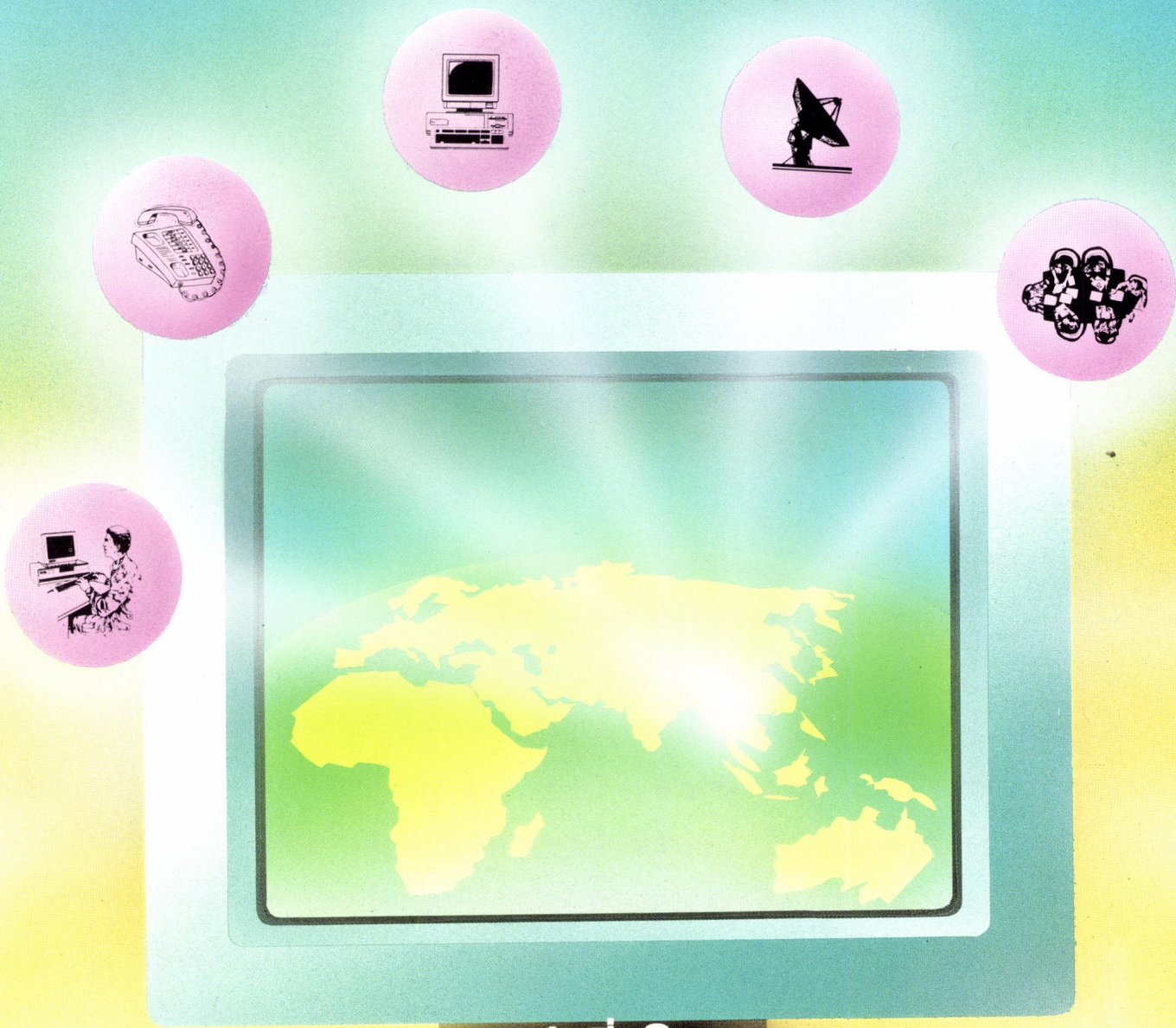
การดำเนินงาน และ การตรวจสอบสถาบันการเงิน ด้านคอมพิวเตอร์



เล่มที่ 3

คอมพิวเตอร์กับการทุจริต

ISBN 974-89418-1-7

เมธา สุวรรณสาร

การดำเนินงาน
และ
การตรวจสอบสถาบันการเงิน
ด้านคอมพิวเตอร์
เล่ม 3

เมธา สุวรรณสาร

คำนำ

1. หนังสือชุด "การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์" ซึ่งเดิมผมเคยประมาณไว้ว่าจะมี 3 เล่มด้วยกัน แต่เมื่อได้รวบรวมและเขียนเพิ่มเติมขึ้นมาใหม่ ก็พบว่ามีเรื่องที่เพิ่มเติมได้อีกหลายเรื่อง รวมทั้งการขยายและอธิบายความที่เคยเขียนในอดีตใหม่ ทำให้หนังสือชุดนี้จะมีอย่างน้อย 4 เล่ม โดยเฉพาะหนังสือเล่ม 3 นี้ มีเรื่องที่ได้เขียนเพิ่มเติมอีกจำนวนมาก เพราะมีความสำคัญที่น่าจะศึกษาโดยเฉพาะตัวอย่าง จุดอ่อนที่อาจจะเกิดการทุจริต รวมทั้งการทุจริตที่ได้เกิดขึ้นแล้ว

2. จุดอ่อนของระบบงานในองค์กรที่ใช้คอมพิวเตอร์มีมากกว่าองค์กรที่ไม่ใช้คอมพิวเตอร์มาก ปัญหาการทุจริตส่วนใหญ่เกิดจากการจัดทำระบบงานที่ขาดความรอบคอบรัดกุม ไม่มีจุดควบคุมและไม่มีผู้ตรวจสอบที่มีประสิทธิภาพเพียงพอ และหรือขาดผู้บริหารที่สนใจด้านนี้

ความเสียหายซึ่งเกิดขึ้นจากระบบงานมีจุดอ่อน อาจก่อให้เกิดความเสียหายให้กับองค์กรอย่างร้ายแรงและคาดไม่ถึง จนถึงขั้นไม่สามารถดำเนินการต่อไปได้ทีเดียว ทั้ง ๆ ที่องค์กรอาจไม่มีปัญหาด้านสภาพคล่อง ซึ่งเป็นเรื่องน่าพิจารณาเป็นอย่างยิ่ง สำหรับผู้บริหารที่ไม่ต้องการให้เกิดปัญหานี้กับองค์กรของตนเอง

3. ธนาคารแห่งประเทศไทยมีหน้าที่กำกับและดูแลความมั่นคงของสถาบันการเงิน ซึ่งมีความสัมพันธ์กันอย่างใกล้ชิดกับความมั่นคงและเสถียรภาพทางเศรษฐกิจโดยรวมของประเทศ ดังนั้นการป้องกันปัญหาก่อนที่ปัญหาจะเกิดขึ้นกับสถาบันการเงิน จึงเป็นทั้งหน้าที่และวิธีการที่กล่าวได้ว่าเหมาะสมโดยเฉพาะอย่างยิ่งการให้ความรู้คำแนะนำในวิธีป้องกันปัญหาล่วงหน้ามากกว่าการให้คำแนะนำให้แก้ไขเมื่อเกิดปัญหาแล้ว

4. การหาทางปรับปรุงแก้ไขและพัฒนางานให้มีประสิทธิภาพอยู่เสมอ ทั้งของธนาคารแห่งประเทศไทย และองค์กรอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งการพัฒนาคนให้มีความรู้เท่าทันเทคโนโลยีใหม่ ๆ จึงเป็นที่มาของการเขียนรวบรวมและเรียบเรียงหนังสือชุดนี้ของผม โดยมีเป้าหมายที่สำคัญคือเพื่อผลประโยชน์ในการปฏิบัติงานของธนาคารแห่งประเทศไทย และสถาบันการเงินที่ธนาคารแห่งประเทศไทยเป็นผู้ดูแล โดยให้การศึกษา ค้นคว้า วิจัยงานด้านคอมพิวเตอร์ ซึ่งมีบทบาทสำคัญยิ่งต่อการพัฒนาระบบการบริหารสถาบันการเงินของไทยในปัจจุบันและในอนาคต

เอกสารชุดนี้ จึงจัดทำขึ้นเพื่อแจกจ่ายให้ผู้ตรวจสอบส่วนกำกับสถาบันการเงินของธนาคารแห่งประเทศไทยเป็นหลัก และสถาบันการเงินต่าง ๆ ในภาคตะวันออกเฉียงเหนือ ทั้งนี้เป็นไปตามแผนงานหนึ่งในจำนวน 19 แผนงานของธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ

5. การที่ผมได้รับมอบหมายจากธนาคารแห่งประเทศไทยให้รับผิดชอบและมีหน้าที่ในการศึกษา ค้นคว้าพัฒนางานตรวจสอบด้านคอมพิวเตอร์ (IT หรือ IS Audit) ในช่วงเวลาที่ผ่านมานั้น ผมได้เสนอและแนะนำให้ธนาคารพาณิชย์รวมทั้งผู้ตรวจสอบภายนอกของธนาคารพาณิชย์ให้ปฏิบัติในหลายเรื่อง ตามที่ปรากฏในบทที่ว่าด้วยเรื่อง

"บทบาทของธนาคารแห่งประเทศไทยกับคอมพิวเตอร์" และ "Role of the bank of Thailand in Banking Computerization" นั้น ทำให้ผมต้องวางมือจากการเป็นผู้สอบบัญชีรับอนุญาตในทุกองค์กร ตั้งแต่ปี พ.ศ. 2524 จนกระทั่งปัจจุบัน (มกราคม 2540) และเข้าใจว่าจะวางมือจากการดำเนินการเป็นผู้สอบบัญชีรับอนุญาตจนกว่าจะออกจากธนาคารแห่งประเทศไทย ทั้งนี้เพราะการออกกฎเกณฑ์บางอย่างกระทบต่อบทบาท ความรู้ ความสามารถ และการเป็นผู้มีคุณสมบัติในการเป็นผู้สอบบัญชีของธนาคารและสถาบันการเงินนั่นเอง ดังนั้นเพื่อความโปร่งใส.....ในเรื่องนี้ผมจึงต้องทำตัวเป็นกลางดังกล่าว

6. หนังสือชุดนี้ไม่มีการจำหน่ายในทุกรูปแบบ เพราะจัดทำขึ้นเพื่อให้การศึกษา ค้นคว้าและวิจัยอย่างแท้จริง โดยหนังสือชุดนี้ได้มาจากการศึกษา แปลและเรียบเรียงจากหนังสือของต่างประเทศเป็นส่วนใหญ่ โดยมีผู้ร่วมงานของผมจำนวนหนึ่งเป็นผู้ช่วยเหลือในฐานะที่เป็นผู้ร่วมงาน โดยมีผมเป็นผู้รับผิดชอบในการศึกษาพัฒนาการตรวจสอบด้านคอมพิวเตอร์ (IS Audit) และการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ (Audit and Control In a Computerized Environment) ตามที่ธนาคารแห่งประเทศไทยได้มอบหมายตั้งแต่แรก

อย่างไรก็ดีหนังสือเล่ม 3 นี้ มีเรื่องใหม่ ๆ ที่ไม่เคยหยิบยกขึ้นมาบรรยายก่อนหน้านี้จำนวนมากที่ได้จัดทำขึ้นใหม่ เพื่อเป็นบทเรียนของผู้ตรวจสอบและสถาบันการเงิน โดยเฉพาะอย่างยิ่งตัวอย่างของจุดอ่อน และการทุจริตที่อาจเกิดขึ้นได้จริง ๆ ถ้าหากไม่มีการป้องกันให้เพียงพอ

7. หนังสือเล่มนี้ได้เน้นถึงเรื่องคอมพิวเตอร์กับการทุจริต มิได้เป็นการชี้โพรงให้กระรอกแต่อย่างใดทั้งสิ้น แต่หากผู้บริหารงานมีความสนใจเรื่องนี้ และมีความเข้าใจเรื่องนี้น้อยกว่าผู้ต้องการทุจริตที่มีความสามารถโดยมีความเข้าใจในจุดอ่อนและมีโอกาสที่จะทุจริตได้แล้ว ผู้บริหารคงต้องทบทวนตนเองด้วยว่าองค์กรควรจะแก้ไขตรงจุดใด

8. การนำคอมพิวเตอร์เข้ามาช่วยในการปฏิบัติงานและให้บริการแก่ลูกค้าประชาชนอย่างแพร่หลายในปัจจุบัน ซึ่งได้เพิ่มประสิทธิภาพแก่องค์กรเป็นอย่างมาก แต่ก็ได้มีการนำเทคโนโลยีเหล่านี้ไปใช้ในทางที่ไม่สุจริตไม่ใช่น้อยและนับวันจะทวีความซับซ้อนขึ้นทุกขณะ ทำให้องค์กรได้รับผลกระทบและความเสียหายมหาศาลภายในเวลาอันรวดเร็ว ซึ่งความเสียหายบางอย่างไม่สามารถวัดได้ด้วยมูลค่าทางการเงิน ดังตัวอย่างที่ได้เกิดขึ้นแล้วทั้งในและต่างประเทศเป็นจำนวนไม่น้อย แต่มักไม่ถูกเปิดเผยเพราะองค์กรเกรงว่าจะมีผลกระทบต่อชื่อเสียงและความน่าเชื่อถือของตน

อย่างไรก็ดีปัจจุบันกรมตำรวจได้ตระหนักถึงปัญหาดังกล่าว และเพื่อเป็นการเตรียมความพร้อมในการแก้ไขปัญหาอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์และเทคโนโลยีชั้นสูงต่อไป กรมตำรวจจึงได้จัดการฝึกอบรมหลักสูตร "สภาพปัญหาและแนวโน้มอาชญากรรมคอมพิวเตอร์" (Computer - Related Crime Issues and Trend) ขึ้นระหว่างวันที่ 24 - 29 พฤศจิกายน 2539 ณ โรงแรมแอมบาสซาเดอร์ซิตี้จอมเทียน อ.สัตหีบ จ.ชลบุรี ตามโครงการความร่วมมือและแลกเปลี่ยนทางวิชาการระหว่างกรมตำรวจกับมหาวิทยาลัยมิชิแกนสเตท สหรัฐอเมริกา (Michigan State University School of Criminal Justice) โดยเชิญวิทยากรและผู้เชี่ยวชาญพิเศษมาบรรยาย อาทิ ศาสตราจารย์ที่สอนเกี่ยวกับอาชญากรรมคอมพิวเตอร์ นักสืบตำรวจฟลอริด้า โคลัมบัส และสารวัตรสืบสวนตำรวจนครบาลกรุงลอนดอน ที่สืบสวนเกี่ยวกับอาชญากรรมคอมพิวเตอร์ และอาชญากรรมข้ามชาติ ทั้งนี้ผู้เข้าร่วมสัมมนา

ส่วนใหญ่เป็นนายตำรวจชั้นผู้ใหญ่ที่เกี่ยวข้อง นอกจากนี้ยังมีผู้แทนส่วนราชการ เช่น ธนาคารแห่งประเทศไทย ศูนย์เทคโนโลยีอิเลกทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) กรมทรัพย์สินทางปัญญา และสำนักงานกฤษฎีกา เป็นต้น ที่ได้รับเชิญให้เข้าร่วมสัมมนาด้วยเพื่อประโยชน์ในการร่วมมือและประสานงานในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ในประเทศไทยต่อไป

9. จากการตื่นตัวของกรมตำรวจในแนวโน้มอาชญากรรมคอมพิวเตอร์โดยการจัดสัมมนาดังกล่าวนั้น นับว่าเป็นเรื่องที่ดีในการเตรียมพร้อมดังกล่าว อย่างไรก็ดี ผมได้มีโอกาสพูดคุยกับนายตำรวจชั้นผู้ใหญ่บางท่าน ก็ได้รับฟังความเห็นและความในใจว่า เรื่องอาชญากรรมคอมพิวเตอร์น่าสนใจมาก แต่น่าเสียดายที่ผู้ที่เกี่ยวข้องจำนวนไม่น้อยไม่มีพื้นฐานทางด้านการบริหารการดำเนินงาน การควบคุมภายใน และระบบงานตลอดจนไม่ค่อยเข้าใจถึงจุดอ่อน การวิเคราะห์จุดอ่อนและกระบวนการปฏิบัติงานด้านคอมพิวเตอร์ ที่เป็นพื้นฐานของการทำความเข้าใจเพื่อประโยชน์ต่อการสืบสวน สอบสวน ที่จะสาวไปถึงการทำอาชญากรรมด้านคอมพิวเตอร์ได้ดีเท่าที่ควร

เรื่องนี้ผมมีความเห็นว่า ทางการน่าจะจัดให้มีการอบรมความรู้เกี่ยวกับคอมพิวเตอร์พื้นฐาน ตลอดจนการควบคุมภายใน การตรวจสอบที่ต้องรู้พื้นฐานของความเสี่ยง จุดอ่อนต่าง ๆ ด้านคอมพิวเตอร์ให้เพียงพอ มิฉะนั้นการสืบสวนสอบสวนอาชญากรรมทางด้านคอมพิวเตอร์หรือเกี่ยวกับคอมพิวเตอร์จะทำได้ไม่สะดวกเลย

10. ปัจจุบันมีหลายองค์กรได้จัดให้มีการอบรมหรือการสัมมนาคอมพิวเตอร์กับการทุจริตปีละหลาย ๆ ครั้ง และทุกครั้งมีผู้สนใจเข้าฟังกันเป็นจำนวนมากเสมอ แสดงถึงความตื่นตัวขององค์กรต่าง ๆ ต่อการป้องกันภัยจากคอมพิวเตอร์ที่เหมาะสมได้ประการหนึ่ง

11. ตัวอย่างหลากหลายที่ท่านจะได้พบจากหนังสือเล่มนี้ ไม่อาจตรวจพบตามปกติได้เป็นส่วนใหญ่ ถ้าไม่มีการสร้างเป้าหมาย ขอบเขต กำหนดวิธีการตรวจสอบตลอดจนการใช้คอมพิวเตอร์เข้าช่วยตรวจสอบที่เหมาะสมในช่วงเวลาที่สมเหตุสมผลรวมทั้งการใช้บุคลากรที่มีความพร้อมในระดับหนึ่งได้ การศึกษาแนวทางการตรวจสอบด้านคอมพิวเตอร์ หรือการศึกษาแนวทางการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ รวมทั้งการใช้คำถามที่ผู้ตรวจสอบควรทราบอย่างเหมาะสม เช่น การตั้งคำถามว่า “What can go wrong” หรือการคาดคะเนข้อผิดพลาด หรือจุดอ่อนที่มีนัยสัมพันธ์ที่อาจเกิดขึ้นในแต่ละกระบวนการปฏิบัติงานทั้งในแบบ Manual และในแบบ Automated ในส่วนที่เกี่ยวข้องทั้งเรื่อง “องค์กร” (Data Center) และเรื่อง “งาน” (Application) ซึ่งเกิดจากความเข้าใจที่ถ่องแท้ของผู้ตรวจสอบในองค์กรที่ใช้คอมพิวเตอร์แล้วจะช่วยให้พบจุดอ่อนที่คาดไม่ถึงได้มาก ซึ่งจะเป็นหนทางป้องกันปัญหาต่าง ๆ ได้ก่อนที่ความเสียหายจะเกิดขึ้น

12. ผมได้เคยบรรยายเรื่อง “คอมพิวเตอร์กับการทุจริต” ให้กับองค์กรต่าง ๆ หลายครั้ง รวมทั้งสถาบันที่จัดให้มีการอบรมเรื่องนี้โดยเฉพาะอย่างยิ่งได้เคยบรรยายร่วมกับ Mr. August Beguai ผู้แต่งหนังสือเรื่อง Cumputer Crime จากประเทศสหรัฐอเมริกา ทุกครั้งมีผู้สนใจรับฟังมากและเรื่องที่ผู้ฟังสนใจมากที่สุด คือ วิธีทุจริตและตัวอย่างเกี่ยวกับการทุจริตต่าง ๆ ที่ได้เกิดขึ้นจริงทั้งในประเทศและต่างประเทศ

ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือที่ผมดูแลสถาบันการเงินต่าง ๆ ทั้ง 19 จังหวัด ก็มีหลายจังหวัดที่ประสบปัญหาการทุจริตด้านคอมพิวเตอร์ แต่ส่วนใหญ่เป็นการทุจริตในลักษณะการใช้ "Off-line" โดยเปลี่ยนข้อมูลใน Report ต่าง ๆ เมื่อผู้บริหารนำไปใช้ตัดสินใจจึงเกิดความเสียหายขึ้น ซึ่งต่างกับการทุจริตที่กรุงเทพฯ ที่มักทุจริตโดยใช้วิธีการแบบ "On-line" โดยผู้ทุจริตอาศัยความเข้าใจในระบบงานและรู้จุดอ่อนเป็นสำคัญ

13. การตรวจสอบด้านคอมพิวเตอร์ที่ได้ผล จึงเป็นการตรวจสอบ Before the fact นั่นคือการตรวจสอบและให้คำแนะนำในเชิงป้องกันก่อนที่ปัญหาจะเกิดขึ้นจริง ๆ ให้ต้องทำการแก้ไข การตรวจสอบลักษณะนี้จะช่วยผู้บริหารและช่วยให้องค์กรสามารถออกระเบียบ กฎเกณฑ์ต่าง ๆ มาใช้ได้อย่างเหมาะสม และลดการทุจริตได้มาก เพราะการทุจริตเกิดจากสาเหตุใหญ่ ๆ 3 ประการ คือ

13.1 มีผู้ทุจริตหรือผู้ไม่หวังดีต่อองค์กร

13.2 องค์กรมีจุดอ่อนในระบบงานและการควบคุมภายใน

13.3 ผู้ปฏิบัติงานที่มีความสามารถมีโอกาสที่จะทุจริตได้

หากจะเพิ่มเหตุผลอีกข้อหนึ่งก็น่าจะไม่ผิด นั่นคือผู้บริหาร ผู้สอบบัญชีทั้ง External Auditor และ Internal Auditor ขาดประสบการณ์ทั้งด้านการบริหาร การตรวจสอบ และไม่อาจให้คำแนะนำในเชิงป้องกันปัญหาที่จะเกิดกับองค์กรได้ล่วงหน้าและมีประสิทธิภาพ ซึ่งส่วนใหญ่เกิดจากผู้ตรวจสอบไม่เข้าใจ "องค์กร" และ "งาน" ที่ตรวจสอบรวมทั้งความเสี่ยงต่าง ๆ ที่เกี่ยวข้องอย่างเพียงพอ หรือมองข้ามจุดที่ควรมีการควบคุมนั่นก็คือกิจกรรมที่ก่อให้เกิดความเสี่ยงได้นั่นเอง

ถ้าหากผู้บริหารระดับสูงได้เข้าใจ "กิจกรรม" ที่ก่อให้ "ความเสี่ยง" ในองค์กรที่ใช้คอมพิวเตอร์จะช่วยป้องกันปัญหาจากการทุจริตได้มาก "ความเสี่ยง" ไม่ได้หมายความถึงการทุจริตเท่านั้น แต่มีความหมายอีกหลายอย่างตามที่ได้กล่าวในสองเล่มแรกมาแล้ว

อย่างไรก็ดี ผู้ที่ทำการทุจริตทุกประเภท ถึงแม้จะประสบความสำเร็จในระยะแรก ๆ ซึ่งอาจซ่อนเร้นความผิดได้หลายปีก็ตาม แต่ในท้ายที่สุดแล้วองค์กรจะจับการทุจริตได้ในที่สุด ดังนั้นจึงขอให้ผู้ที่จะคิดทุจริตโปรดเลิกความคิดและการกระทำดังกล่าวได้

14. หากท่านผู้อ่านใคร่จะทบทวนแนวคิดตลอดจนวิธีการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ ซึ่งในความหมายนี้คลุมไปหมดทั้งเรื่อง Financial Audit และ Computer Audit หรือ IS Audit ซึ่งการตรวจสอบทั้ง 2 เรื่องมีความสัมพันธ์กันอย่างใกล้ชิด เพราะการตรวจสอบ Financial Audit ก็คงต้องพิจารณา Computer Audit ด้วยในฐานะที่องค์กรยุคใหม่ได้นำคอมพิวเตอร์มาใช้ในการปฏิบัติงาน และการควบคุมภายในแล้วทั้งสิ้น ท่านอาจดูข้อสรุปในเล่มนี้ในบทที่เกี่ยวข้องกับการตรวจสอบการทุจริตได้

นอกจากนี้ในเล่มที่ 4 ของหนังสือชุดนี้ผมได้จัดทำบทกรณีศึกษาการตรวจสอบทั้งทางด้าน Data Center และ Application ที่น่าสนใจโดยส่วนใหญ่ได้แนวความคิดและประสบการณ์จากการตรวจสอบด้านภาคปฏิบัติจริง ๆ กรณีศึกษาจะมีบทแนวคำตอบให้ผู้ตรวจสอบได้ติดตามศึกษาด้วย ทั้งนี้เป็นการทบทวนความเข้าใจของผู้ตรวจ

สอบได้ระดับหนึ่ง อย่างไรก็ดีกรณีศึกษาดังกล่าวจะมีประโยชน์มากยิ่งขึ้นถ้าหากผู้ตรวจสอบจะพิจารณาหาแนวคำตอบก่อนที่จะได้ดูบทเฉลยที่เป็นแนวคำตอบจริง ๆ ต่อไป

15. หนังสือชุดนี้ทั้ง 4 เล่ม มีเลขที่ของ ISBN อยู่ด้วย ทั้ง ๆ ที่มีการพิมพ์จำนวนน้อยมาก ทั้งนี้ก็เพื่อใช้ในการศึกษาตามที่เคยกล่าวแล้ว แต่การมีเลขที่ ISBN ด้วยก็เพื่อให้ใช้เป็นที่อ้างอิงสำหรับผู้อ่าน เมื่อหนังสือนี้อยู่ในห้องสมุดของธนาคารแห่งประเทศไทย ที่มีระบบการอ้างอิงเอกสารที่ทันสมัยแล้วเท่านั้น

16. การจัดทำหนังสือชุดนี้ ผมคาดการณ์ผิดหลายประการ นั่นคือ ผมใช้เวลามากกว่าที่คาดไว้แต่เดิมมากมาย จากการจัดทำข้อมูลเพิ่มเติมโดยเฉพาะเล่ม 3 และเล่ม 4 และต้องพิสูจน์ตัวอักษรในบางส่วนพร้อมทำความเข้าใจกับเพื่อนร่วมงานที่ทำหน้าที่พิสูจน์ตัวอักษรไปพร้อมกับอธิบายเรื่องที่เกี่ยวข้องเพราะมีความสับสนในการพิมพ์ด้วย อย่างไรก็ดีเวลาส่วนใหญ่หรือแทบทั้งหมดนี้ผมได้ใช้เวลานอกทำการตามปกติของธนาคาร

ผมบังเอิญได้ไปอ่านศัพท์คอมพิวเตอร์ในห้องสมุดของสาขาภาคฯ ในช่วงเพียงวันหนึ่งได้พบกับศัพท์ที่น่าสนใจมาก และมีความหมายตลอดจนความสำคัญอย่างยิ่งต่อท่านผู้อ่านหรือท่านผู้ตรวจสอบ โดยเฉพาะผู้ที่จะเป็น EDP Auditor หรือ IS Auditor หรือ IS Examiner ก็ตามนั่นคือการแปลคำศัพท์ของคำว่า "Computer audit" จากพจนานุกรมศัพท์คอมพิวเตอร์หลายเล่มได้ให้ความหมายต่างกันเช่น :-

บางเล่มแปลคำนี้ว่า "การตรวจสอบบัญชีด้วยคอมพิวเตอร์"
บางเล่มแปลคำนี้ว่า "การตรวจสอบระบบคอมพิวเตอร์"
บางเล่มไม่ได้ให้ความหมายของคำ ๆ นี้ไว้

ผมรู้สึกหนักใจแทนท่านผู้อ่าน และท่านผู้ตรวจสอบที่กำลังทำความเข้าใจในเรื่องการตรวจสอบ Computer Audit หรือ IT, IS Audit เพราะคำว่า Computer Audit นี้ความหมายที่น่าจะถูกต้องและฟังเข้าใจได้ดีกว่าการตรวจสอบด้านคอมพิวเตอร์ ซึ่งแบ่งการตรวจสอบออกเป็น 2 ส่วนใหญ่ ๆ ได้แก่

ก) การตรวจสอบการบริหารองค์กรทางการด้านคอมพิวเตอร์หรือศูนย์คอมพิวเตอร์ (Data center) ซึ่งเป็นการตรวจสอบ General Controls กับ

ข) การตรวจสอบ "งาน" หรือ Application audit ซึ่งเป็นการตรวจสอบงานแต่ละประเภทแต่ละหน่วยงานขององค์กร เช่น งานด้านเงินฝาก ส่วนงานด้านเงินกู้ งานด้านสินค้าคงคลัง การซื้อ การขาย ฯลฯ ซึ่งจะเน้นการตรวจทางด้าน Input, Processing และ Output ของแต่ละงาน (Application) ที่เกี่ยวข้องกับงานการตรวจสอบทั้ง 2 ด้าน ซึ่งเป็นเรื่อง Computer Audit นี้ เป็นงานใหม่เพิ่มเติมจากการตรวจสอบตามปกติ ซึ่งในระบบบัญชีที่ทำด้วย Manual แบบดั้งเดิมไม่มี

ดังนั้นการแปลคำว่า Computer Audit ตามพจนานุกรมศัพท์คอมพิวเตอร์บางเล่มว่าเป็นการตรวจสอบบัญชีด้วยคอมพิวเตอร์น่าจะมีความหมายเพียงการใช้คอมพิวเตอร์เข้าช่วยในการตรวจสอบ หรือเป็น Computer Assisted Audit Technique อย่างหนึ่งมากกว่าเป็นการตรวจสอบด้านคอมพิวเตอร์ (Computer Audit) จริง ๆ แล้ว ในขณะนี้บางเล่มแปลว่าการตรวจสอบระบบคอมพิวเตอร์ ซึ่งการแปลเช่นนี้มีความหมายที่ใกล้เคียงกับความหมายที่ผม

คิดว่าน่าจะถูกต้องคือ "การตรวจสอบด้านคอมพิวเตอร์" แต่คำว่าการตรวจสอบระบบคอมพิวเตอร์อาจทำให้ผู้อ่านเข้าใจผิดว่า เป็นการตรวจสอบทางด้าน System ของคอมพิวเตอร์หรือเป็นแต่เพียงการตรวจสอบระบบงานใดระบบงานหนึ่งหรือหลายระบบที่ใช้คอมพิวเตอร์ในการประมวลงาน ซึ่งตรงกับคำภาษาอังกฤษว่า "Application Audit" โดยเป็นส่วนหนึ่งของการตรวจสอบทางด้าน Computer Audit ตามที่กล่าวแล้วเท่านั้น หรืออาจมีผู้อ่านบางท่านเข้าใจไขว้เขวไปได้ว่า "เป็นการตรวจสอบระบบคอมพิวเตอร์" ตามคำแปลล้วน ๆ เพียงอย่างเดียวก็ได้ และเข้าใจเช่นนี้ จะคลาดเคลื่อนจากความหมายของคำว่า Computer Audit ตามที่ผมกล่าวในตอนแรก ๆ แล้วว่า การตรวจสอบด้านคอมพิวเตอร์ (Computer Audit) หรือ IS Audit เป็นการตรวจสอบในลักษณะ Total System Approach นั่นคือการตรวจสอบการบริหารงานและการประมวลงานตั้งแต่การพัฒนาระบบงานการนำข้อมูลเข้า การประมวลผลจนกระทั่งได้ข้อมูลผลลัพธ์ทั้งในส่วนที่เป็น Manual ส่วนที่เป็น Automated และส่วนผสมของทั้ง 2 แบบรวมทั้งการใช้ผลลัพธ์จากการประมวลผลตลอดจนถึงการจัดทำเอกสารประกอบระบบงาน ส่วนกระบวนการตรวจสอบ เทคนิคการตรวจสอบ หลักฐานการตรวจสอบ การจัดดูรายงานจะขึ้นอยู่กับเป้าหมาย และขอบเขตการตรวจสอบเป็นสำคัญ ดังนั้นขอได้โปรดศึกษาและทบทวนความหมายและวัตถุประสงค์ในการตรวจสอบ IS Audit ให้ถ่องแท้ก่อนด้วย

หวังว่าคำอธิบายในข้อนี้จะช่วยทำความเข้าใจในเรื่องการตรวจสอบด้านคอมพิวเตอร์ (Computer Audit) ได้บ้างส่วนพอสมควร เพราะหากท่านผู้อ่านเกิดความเข้าใจที่คลาดเคลื่อนแล้ว การศึกษาการบริหารงาน และการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์จะเกิดความสับสนเป็นอย่างยิ่ง ดังนั้นจึงควรทราบว่าการใช้ภาษาไทยในเรื่องของการตรวจสอบด้านคอมพิวเตอร์มีคำศัพท์ที่ใช้คล้าย ๆ กันหลายคำ แต่มีความหมายแตกต่างกันอย่างมีนัยสำคัญมาก สำหรับคำว่า "การตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ก็มีความหมายหลัก ๆ ได้ 2 อย่างคือ การตรวจสอบด้าน IS Audit และ/หรือ Financial Audit ซึ่งขึ้นอยู่กับวัตถุประสงค์ของการตรวจสอบ อย่างไรก็ดี หากเป็นการตรวจสอบ Financial audit ก็หนีไม่พ้นต้องทำการตรวจสอบทางด้าน IS Audit ซึ่งอยู่ในกระบวนการต้น ๆ ของการตรวจสอบ นั่นคือการศึกษาและทำความเข้าใจในระบบงานขององค์กรที่ตรวจสอบก่อนเสมอ (โปรดดูหน้า 30)

17. ขอขอบคุณบรรดาเพื่อนร่วมงานในอดีตทุกท่าน โดยเฉพาะรุ่นบุกเบิกการตรวจสอบงานด้านคอม-พิวเตอร์ ได้แก่ คุณสุขุม ตันตราจิณ คุณสรสิทธิ์ สุนทรเกศ คุณปรีชา ปรมาพจน์ คุณสมศักดิ์ มหินธิชัยชาญ คุณสุภักดิ์ ภูรยานนทชัย คุณวุฒิพงศ์ สมนึก คุณชาตรี วรวณิชชานันท์ และคุณพงศ์เทพ ชินพัฒน์ และเพื่อนร่วมงานรุ่นใหม่ที่เข้ามาเสริมทีมงานในภายหลังที่ไม่อาจระบุชื่อได้ทั้งหมด ซึ่งมีส่วนสำคัญในการช่วยเรียบเรียงเอกสารประกอบการบรรยายในอดีตในหลาย ๆ เรื่อง และทำให้งานตรวจสอบด้านคอมพิวเตอร์แพร่หลายมากขึ้นในปัจจุบัน ขอขอบคุณอีกครั้งสำหรับการมีส่วนร่วมใด ๆ ที่ผ่านมาในกิจกรรมเผยแพร่เอกสารการดำเนินงานการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ ขอขอบคุณเพื่อนร่วมงานในส่วนกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทยสาขาภาคตะวันออกเฉียงเหนือในปัจจุบันที่ช่วยตรวจทานความถูกต้องในการพิมพ์ครั้งนี้

เมธา สุวรรณสาร
ผู้อำนวยการธนาคารแห่งประเทศ สาขาภาคตะวันออกเฉียงเหนือ
30 มกราคม 2540

สารบัญ

หน้า

บทที่ 1 เทคโนโลยีคอมพิวเตอร์กับการควบคุมและตรวจสอบ (บทคัดย่อ)

- ❑ **การทุจริตโดยใช้คอมพิวเตอร์** 3
- ❑ **คอมพิวเตอร์มีผลกระทบต่อการควบคุมและการตรวจสอบ** 4
- ❑ **ความเสี่ยงกับคอมพิวเตอร์** 6
  - ความเสี่ยงคืออะไร 6
  - หลักการวิเคราะห์ความเสี่ยง 7
  - การพิจารณามูลเหตุที่นำไปสู่ความเสียหาย 7
- ❑ **เทคนิคที่ใช้ในการค้นหามูลเหตุแห่งความเสียหาย** 9
- ❑ **การประเมินความเสี่ยงและความเสียหาย** 10
- ❑ **วิธีการที่ใช้ในการประเมินความเสี่ยงและความเสียหาย** 10
- ❑ **การจัดการกับความเสี่ยง** 13
- ❑ **การประกันภัยทางด้านคอมพิวเตอร์** 14
- ❑ **การพิจารณาวิธีการควบคุมความเสี่ยงและความเสียหาย** 14
- ❑ **สิ่งที่ควรพิจารณาเกี่ยวกับการควบคุม** 15
- ❑ **การประเมินประสิทธิภาพของการควบคุม** 17

บทที่ 2 การป้องกันดีกว่าการแก้ไข

- ❑ **ทบทวนมาตรฐานการตรวจสอบและแนวความคิดในการตรวจสอบ เพื่อการบริหารที่มีประสิทธิภาพและป้องกันการทุจริต** 21
  - มาตรฐานการปฏิบัติงาน 23
  - แนวความคิดในการตรวจสอบ 23
  - การศึกษาและประเมินประสิทธิภาพการควบคุมภายในของผู้สอบบัญชี 26
  - ผลของการประมวลผลโดยใช้คอมพิวเตอร์ต่อการศึกษา และประเมินประสิทธิภาพการควบคุมภายใน 29
  - การทดสอบความถูกต้องของยอดคงเหลือ : การเก็บรวบรวมเพื่อให้ได้มาซึ่งหลักฐานที่เพียงพอ 40
  - สรุป 40

หน้า

บทที่ 3 การเข้าใจของผู้บริหารจากผลกระทบของคอมพิวเตอร์ต่อองค์กรก็ช่วยลดการทุจริตได้

- ผลกระทบของคอมพิวเตอร์ที่มีต่อการตรวจสอบ 45
- การควบคุมและการตรวจสอบ 45
- การสอบทานการประมวลผลของเครื่องคอมพิวเตอร์ 47
- ปัญหาที่บรรดาศูนย์คอมพิวเตอร์ต่าง ๆ ส่วนใหญ่ประสบและอาจนำไปสู่การทุจริต 48
- บทบาทของฝ่ายบริหารที่มีต่อคอมพิวเตอร์ และสาเหตุที่ผู้บริหารไม่ให้ความสำคัญต่อผู้ตรวจสอบด้านคอมพิวเตอร์ 49
- อาชญากรรมทางเทคโนโลยี (คอมพิวเตอร์) 50

บทที่ 4 การทุจริตทางคอมพิวเตอร์และการทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือ

- ❑ **การทุจริตทางคอมพิวเตอร์** 55
- ❑ **สาเหตุการทุจริต** 55
- ❑ **การทุจริตโดยใช้คอมพิวเตอร์** 58
- ❑ **การทุจริตเกี่ยวกับคอมพิวเตอร์** 59

บทที่ 5 รูปแบบการทุจริตทางคอมพิวเตอร์ (และตัวอย่างที่เกี่ยวข้อง)

- ❑ **Data Diddling** 63
- ❑ **Trojan Horse** 64
- ❑ **Salermi Techniques** 65
- ❑ **Superzapping** 65
- ❑ **Trap Doors** 66
- ❑ **Logic Bombs** 67
- ❑ **Asynchronous Attacks** 67
- ❑ **Seaverging** 68
- ❑ **Data Leakage** 69
- ❑ **Piggybacking and Impersonation** 70
- ❑ **Wiretapping** 71
- ❑ **Simulation and Modeling** 71

หน้า

บทที่ 6 การทุจริตในวงการคอมพิวเตอร์ (ประสบการณ์ของประเทศต่าง ๆ)

❑ **ตัวอย่างต่าง ๆ ของการทุจริตในวงการคอมพิวเตอร์** 75

- กรณีการเปลี่ยนระบบจาก Manual ไปสู่ Computer System 75
- กรณีการทุจริตโดยการสับเปลี่ยนสมุดคู่ฝากของลูกค้าธนาคารพาณิชย์ 76
- กรณีการ Key เงินฝากลอย ๆ ผ่านเครื่อง Terminal 77
- โกงเงินธนาคารโดยอาศัยเครื่องเทอร์มินัล 79
- การทำรายการเปลี่ยนแปลงแก้ไขวงเงินเบิกเกินบัญชี 81
- ตบตาคณะกรรมการและผู้สอบบัญชีเพื่อตบแต่งงบการเงิน 82
- การทุจริตกับ ATM 83
- การโจรกรรมดอกเบี้ยเงินฝากออมทรัพย์ 84
- เลขที่เช็คนั้นสำคัญไฉน 86
- กำจัดคู่แข่งโดยใช้โปรแกรมคอมพิวเตอร์ 87
- ผู้บริหารสร้าง Input ปลอม 88
- การทุจริตโดยการใช้จุดอ่อนของแบบฟอร์มที่ Input ในระบบอัตโนมัติ (Micr) 89

❑ **การทุจริตทางด้าน INPUT** 89

- เพิ่มรายชื่อผู้มีสิทธิออกเสียงเลือกตั้ง 89
- เพิ่มรายชื่อของผู้สอบผ่านการขอรับใบขับขี่ 90

❑ **การทุจริตทางด้าน PROCESSING** 90

- การใช้โปรแกรมที่ผู้ทุจริตจัดทำขึ้นเพื่อลักลอบแก้ไข หรือ List ข้อมูลที่เก็บในระบบ 90
- ใช้ Password ที่ล่วงรู้มายักยอกเอาวัสดุที่ใช้ติดตั้งโทรศัพท์ไปขาย 90
- โจรกรรมเงินจากเครื่องจ่ายเงินอัตโนมัติ 91

❑ **การทุจริตโดยการขโมยความลับของข้อมูล** 91

- List รายชื่อลูกค้าไปขายให้บริษัทคู่แข่ง 91
- List รายชื่อไปขายให้บริษัทขายสินค้าทางไปรษณีย์ 91
- โจรกรรมโปรแกรมควบคุมการทำงานของคอมพิวเตอร์ 92
- เพิ่มรายชื่อเพื่อรับประโยชน์ TAX Refund 92
- ยักยอกเงินฝากของลูกค้า 93
- การสร้างรายการฝากเงินโดยไม่มีเอกสารประกอบ 93
- ตัวอย่างการทุจริตและการวิเคราะห์โดยย่อ 95
- การทุจริตโดยใช้เลขที่บัญชีและบัตร ATM ของลูกค้า 95

หน้า

บทที่ 7 การค้นหาข้อมูลจากส่วนความจำของคอมพิวเตอร์เพื่อดำเนินคดี

- ❑ **การทุจริตโดยการใช้อุปกรณ์คอมพิวเตอร์ โดยผู้ไม่มีอำนาจหน้าที่** 99
- ❑ **โปรแกรมคอมพิวเตอร์กับการค้นหาข้อมูลเพื่อพิสูจน์การโจรกรรม** 103
- ❑ **การทุจริตทางด้าน INPUT** 105
- ❑ **การปลอม Input เงินฝากโดยใช้ MICR** 108
- ❑ **การควบคุมและการทุจริตทางด้าน Processing** 109
- ❑ **การทุจริตและการควบคุมทางด้าน Output** 111

บทที่ 8 การทุจริตเกี่ยวกับบัตรเครดิตและการป้องกัน การทุจริตและอาชญากรรมคอมพิวเตอร์

- การทุจริตเกี่ยวกับบัตรเครดิต 115
- การป้องกันการทุจริตเกี่ยวกับบัตรเครดิต 115
- กฎหมายเกี่ยวกับบัตรเครดิตในประเทศสหรัฐอเมริกา 116
- กฎหมายเกี่ยวกับบัตรเครดิตในประเทศไทย 116
- กฎหมายการโอนเงินทางอิเล็กทรอนิกส์ 117
  - ประเภทของอาชญากรรมด้านคอมพิวเตอร์ 117
  - การป้องกันอาชญากรรมคอมพิวเตอร์ 118

บทที่ 9 แนวทางปฏิบัติสำหรับผู้บริหารในการรักษาความปลอดภัย ของระบบการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์

- การรักษาความปลอดภัยของระบบการประมวลผลด้วยคอมพิวเตอร์ 121
- ข้อควรปฏิบัติในการสร้างระบบการรักษาความปลอดภัย 122
- ข้อไม่พึงปฏิบัติ 123
- การวิเคราะห์ความเสี่ยง 123
- เทคนิคการควบคุมและการรักษาความปลอดภัย 125
- ขั้นตอนการทำงานและการตอบสนองของระบบ 131

บทที่ 10 สัญญาณการทุจริตหรือจุดอ่อนบางประการในองค์กรที่ใช้คอมพิวเตอร์ 137

หน้า

บทที่ 11 วิธีการกระทำการทุจริตบางประการที่ผู้บริหารควรทราบ

- วิธีการกระทำการทุจริตโดยใช้คอมพิวเตอร์ 141
- รูปแบบของการทุจริตโดยการใช้คอมพิวเตอร์ 141
- ตัวอย่างการทุจริตแบบผสมระหว่างวิธี Manual กับวิธีการใช้คอมพิวเตอร์แบบ Off-line 142
- รายการที่ทำการทุจริตในกรณีต่าง ๆ 143
- การจำแนกวิธีการปรุงแต่งข้อมูลแยกตามลักษณะกิจการ 143
- การแก้ไขคำสั่ง (Program) โดยไม่มีอำนาจ 144

บทที่ 12 ผู้เสียหายจากการทุจริต และการเปิดเผยการทุจริตด้านคอมพิวเตอร์ ซึ่งเป็นเรื่องที่ควรทำโดยผู้บริหาร

- ผู้เสียหายจากการทุจริต 147
- คอมพิวเตอร์กับการทุจริต 147
- เรื่อง การเปิดเผยการทุจริตด้านคอมพิวเตอร์ ซึ่งเป็นการตัดสินใจที่ถูกต้องของผู้บริหาร 149
- เรื่อง OASINO EXTORTION CASE 150
- เรื่อง DUMP BANKS 150

บทที่ 13 การรักษาความปลอดภัยของระบบบริหารข้อมูลหรือโปรแกรมควบคุมระบบงาน

- คำนำ 153
- การรักษาความปลอดภัยภายนอก 153
- การรักษาความปลอดภัยในการปฏิบัติงาน 154
- การควบคุมการรักษาความปลอดภัย 154
- ระบบเตือนภัย 154
- การควบคุมการเก็บ Password 154
- การตรวจสอบ 155
- การป้องกันบุคคลที่ไม่เกี่ยวข้องมาใช้เครื่อง 155
- สิ่งที่ควรระลึกถึงเกี่ยวกับการรักษาความปลอดภัย 155
- การรักษาความปลอดภัยของเครื่อง 156
- ระบบการทำงานด้วยตัวเอง 156
- Capability and Object-Oriented Systems 156
- Movement and Storage Capabilities 157
- Revocation of Capabilities 157
- Case Study : The Object-Oriented Architecture of the IBM System/38 158

หน้า

❑ **การสื่อข้อมูลด้วยรหัส** 159
- A Cryptographic Privacy System and Cryptanalysis 159
- Public Key Systems 159
- Data Encryption Standard (DES) 160
- Operating System Penetration 161

❑ **ข้อบกพร่องทั่วไปของระบบการทำงานของ O/S** 162

❑ **Case Study : Penetrating an Operating System** 168

❑ **Utility Programs** 170

❑ **การประเมินผลการใช้ Utility Programs** 170

❑ **การตรวจสอบการควบคุม Utility Programs** 171

บทที่ 14 ตัวอย่างจุดอ่อนของการดำเนินงานด้านคอมพิวเตอร์ (Data Center หรือ General Controls) ที่อาจก่อให้เกิดการทุจริตได้ พร้อมกับคำแนะนำโดยสรุป

❑ **การจัดการ** 175
- การกำหนดนโยบายและการลงทุนด้านคอมพิวเตอร์ 175
- แผนฉุกเฉินและระบบคอมพิวเตอร์สำรอง 176
- การประกันภัยคอมพิวเตอร์ 180
- คณะกรรมการบริหารงานคอมพิวเตอร์และบุคลากร 181
- การรายงานผลการปฏิบัติงานคอมพิวเตอร์ไม่เป็นลายลักษณ์อักษร 185
- การรักษาความปลอดภัย 187
- อื่น ๆ 187

❑ **การตรวจสอบภายใน** 190

บทที่ 15 ประสบการณ์ (บางส่วน) ในการตรวจสอบการปฏิบัติ "งาน" หรือ Application (Application Audit/Application Controls) ของประเทศต่าง ๆ

❑ **บทนำ** 195

❑ **ระบบงานที่ประมวลผลด้วยคอมพิวเตอร์** 195
- ระบบงานและโปรแกรม 195
- ระบบเงินฝากโดยภาพรวม ๆ 208
- เงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและเงินเบิกเกินบัญชี 233
- เงินฝากออมทรัพย์ 255
- เงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา 270

หน้า

❑ ระบบเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน (ATM) 279
❑ สินเชื่อ 307
- ระบบงานเงินให้สินเชื่อ 307
- ระบบงาน Customer Facility System (CFS) 310
- ระบบบัตรเครดิต 311
❑ ต่างประเทศ 312
- ระบบบัญชีต่างประเทศ 312
- ระบบงาน L/C 313
- ระบบงาน T/R 314
- ระบบงาน SWIFT 316
❑ บัญชี 317
- ระบบงานบัญชี 317
- ระบบงาน Financial Control 318
- ระบบงาน L/G 318
- อื่น ๆ 319

บทที่ 16 ตัวอย่างจุดอ่อนของระบบงาน (Application) ด้านคอมพิวเตอร์ที่อาจก่อให้เกิดการทุจริตได้

❑ บทนำ 323
- จุดอ่อนในระบบงานต่าง ๆ ขององค์กรอันอาจเป็นช่องทางในการกระทำทุจริตได้ 324
❑ ตัวอย่างจุดอ่อนในระบบงาน (Application) ที่อาจได้รับความเสียหายจากการทุจริต 325

บทที่ 17 การตรวจสอบการทุจริตและทบทวนการตรวจสอบจุดอ่อนในระบบงานในองค์กรที่ใช้คอมพิวเตอร์

- คำนำ 335
- ขอบเขตและความถี่ในการตรวจสอบด้านคอมพิวเตอร์ 336
❑ วิธีการตรวจสอบ 337
- การมีส่วนร่วมในการพัฒนาและทดสอบระบบงานของหน่วยงานตรวจสอบ 340
❑ การจัดทำเอกสารและรายงานการตรวจสอบ 342
❑ การรายงานข้อสรุปจากการตรวจสอบ 343
- การวิเคราะห์ความเสี่ยง ผลเสียหาย การควบคุม และการตรวจสอบ 343
- ผลกระทบของคอมพิวเตอร์ต่อการควบคุมทางด้านบัญชี (Accounting Control) บางประการ 344
- ข้อควรคำนึงและพิจารณาในการตรวจสอบ 345

หน้า

- การตรวจสอบกับการควบคุมโดยย่อ 346
- วิธีการตรวจสอบแบบ Total System Approach 347
- จุดที่ควรตรวจสอบและข้อควรคำนึงบางประการในภาพรวม ๆ ของการตรวจสอบ 347
- เทคนิคที่ใช้ในการสร้างคอมพิวเตอร์โปรแกรมเพื่อการตรวจสอบ 349
- แนวทางการตรวจสอบการควบคุมทางบัญชีของระบบงาน 350
- โครงสร้างของการควบคุมในกิจการที่ใช้คอมพิวเตอร์ 351
- ความรับผิดชอบของผู้สอบบัญชีในด้านการตรวจสอบงานที่ประมวลผลด้วยคอมพิวเตอร์ 352
- วิธีการตรวจสอบระบบจะช่วยผู้สอบบัญชีได้อย่างไร 352
- สิ่งที่ผู้ตรวจสอบควรทราบในการตรวจสอบการทุจริต 352
- เข้าใจประเด็นที่ต้องพิจารณาในการเริ่มการตรวจสอบ 353
- เข้าใจถึงการพิจารณาผังทางเดินของกิจกรรมและความสัมพันธ์กับข้อผิดพลาดหรือการควบคุมที่เกี่ยวข้อง 353
- เข้าใจประเด็นคำถามที่เกี่ยวข้องกับองค์ประกอบในการตรวจสอบ 354
- วิธีการตรวจสอบระบบงาน 355
- การทำความเข้าใจในการตรวจสอบทั่วไป 356
- สรุปแนวทางในการตรวจสอบจุดอ่อนในระบบงาน และการทุจริตด้านคอมพิวเตอร์ 357
- แนวการตรวจสอบระบบงานในองค์กรที่ใช้คอมพิวเตอร์ 358
- แนวการตรวจสอบระบบงานด้านคอมพิวเตอร์ 359
- อีกรูปแบบหนึ่งของการกำหนดและวางแผนการตรวจสอบโดยทั่วไป ซึ่งอาจนำมาประยุกต์ใช้กับการตรวจสอบการทุจริตในองค์กรที่ใช้คอมพิวเตอร์ได้ 362
- การป้องกันการทุจริต 366
- สิ่งที่ควรดำเนินการ 366
- สรุป 367

บทที่ 18 ตัวอย่างการตรวจสอบกรณีทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือและความร่วมมือระหว่าง Computer Auditors (IS Auditors) กับ Financial Auditors (ประสบการณ์ของต่างประเทศ)

❑ **บทคัดย่อของการทุจริตในระบบ Refund System และการตรวจสอบโดยย่อ** 371
- การตรวจสอบเบื้องต้น 371
- จุดอ่อนที่พบเบื้องต้น 372
- การค้นพบทุจริต 373
- การประสานงานตรวจสอบ 373
- แบบการตรวจสอบทุจริต 374

หน้า

❑ สรุป 376
- การประสานงาน 376

❑ **การทุจริตและการตรวจสอบกรณีทุจริตเกี่ยวกับคอมพิวเตอร์** 377
- ความเป็นมาขององค์กรที่เกิดการทุจริต 377
- เหตุการณ์ที่ก่อให้เกิดการทุจริต 379
- บทบาทของผู้สอบบัญชี 379
- การตรวจสอบเบื้องต้น 380
- Member Contribution Accounts (MCA) System 380
- Refund System 382
- การควบคุมภายในระบบ MCA 388
- สิ่งที่ค้นพบจากการตรวจสอบเบื้องต้น 390
- การค้นพบการทุจริต 392
- สิ่งที่ต้องทำในการตรวจสอบ 392
- ผลที่ได้จากการตรวจค้นการทุจริต 396
- สรุป 400

บทที่ 19 คำแนะนำในการตรวจสอบ : การควบคุมภายในระบบบัญชีที่ใช้คอมพิวเตอร์

❑ คำนำ 405
- ผลกระทบต่อการควบคุมภายใน 405
- ผลกระทบที่มีต่อหลักฐานในการตรวจสอบ 405

❑ **การควบคุมภายในระบบบัญชีที่ใช้คอมพิวเตอร์** 406

❑ **ความเชื่อมั่นของผู้สอบบัญชีที่มีต่อการควบคุมภายใน** 406

❑ **วิธีการตรวจสอบที่เกี่ยวเนื่องกับการควบคุมภายใน** 407

❑ **การทำเอกสารเกี่ยวกับการตรวจสอบ** 408

❑ **การทดสอบ** 409

บทที่ 20 การป้องกันอาชญากรรมคอมพิวเตอร์ และสิ่งที่ผู้บริหารควรพิจารณาดำเนินการ
- การป้องกันอาชญากรรมคอมพิวเตอร์ 413
- สิ่งที่ผู้บริหารควรพิจารณาดำเนินการ 414

หน้า

บทที่ 21 องค์ประกอบสำคัญในการประมวลข้อมูลโดยระบบคอมพิวเตอร์

- ประกอบด้วย Harware, Software และ Firmware 417
- ตัวอย่างการตรวจสอบขั้นตอนการปฏิบัติงานคอมพิวเตอร์ 418
- คำอธิบายศัพท์และลักษณะการทำงานในระบบคอมพิวเตอร์ที่สำคัญ 418

บทที่ 22 เทคนิคในการนำคอมพิวเตอร์มาใช้ในงานตรวจสอบ (COMPUTER-ASSISTED AUDIT TECHNIQUES)

- การเลือกเทคนิคที่จะใช้ตรวจสอบ 421
  - เทคนิคในการรวบรวมข้อมูล 421
  - เทคนิคที่ใช้ในการตรวจสอบการควบคุมภายใน 423

ภาคผนวก ก

- กรณีศึกษา : การจัดการความรับผิดชอบของพนักงานชั้นบริหาร 439

ภาคผนวก ข

- การกำหนดของธนาคารแห่งประเทศไทยกับระบบรักษาความปลอดภัยของธนาคารพาณิชย์ 441
- การกำหนดของธนาคารแห่งประเทศไทย เรื่อง ขอบเขตการตรวจสอบด้านคอมพิวเตอร์ 444

ภาคผนวก ค

- Check Digit 447
  - วิธีการคำนวณหา Check Digit 447
  - ประโยชน์ของ Check Digit 449
  - รูปแบบความผิดพลาดที่พบ 449

บรรณานุกรม 451

บทที่ 1

เทคโนโลยีคอมพิวเตอร์กับการควบคุมและตรวจสอบ (บทคัดย่อ)

การทุจริตโดยใช้คอมพิวเตอร์

คอมพิวเตอร์เป็นเครื่องมือที่มีประสิทธิภาพในการทำงาน เพียงแต่ต้องอยู่ภายใต้การบงการของมนุษย์ ผู้ใดก็ตามที่เข้าใจภาษาของคอมพิวเตอร์ก็สามารถสื่อสารกับคอมพิวเตอร์ได้ ดังนั้นคอมพิวเตอร์จึงกลายเป็นเครื่องมือที่มีคุณอนันต์กับองค์การ ในกรณีที่จัดทำข้อมูลให้ผู้บริหารองค์การได้ใช้ตัดสินใจ แต่ก็เป็นโทษอย่างมหันต์ต่อองค์การ ถ้ามีผู้ใช้คอมพิวเตอร์เพื่อประโยชน์ทางทุจริตของบุคคลนั้น

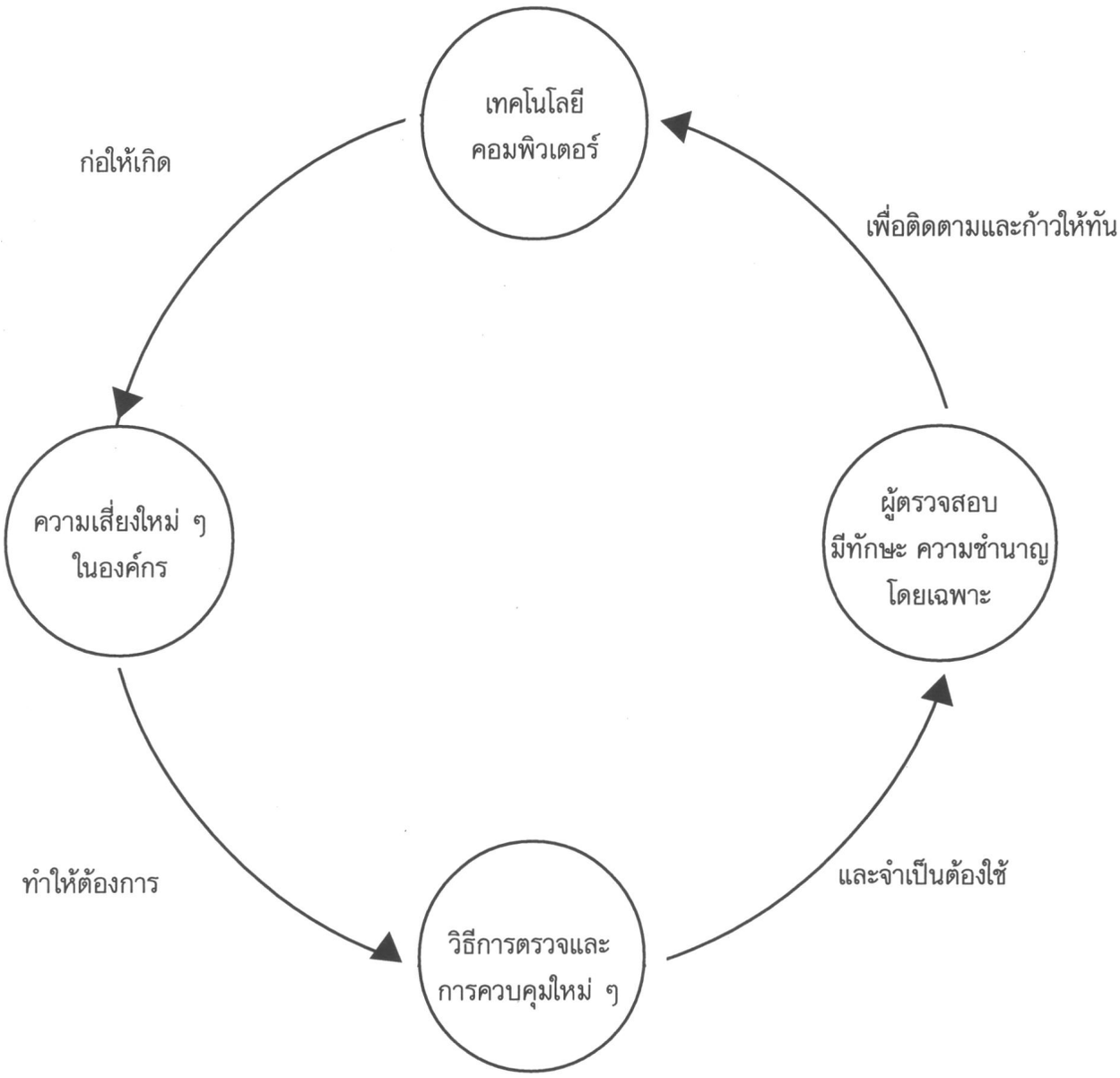
ดังนั้นการศึกษาเรื่องนี้จึงควรทบทวนความเกี่ยวข้องที่สัมพันธ์กันระหว่างเทคโนโลยี ความเสี่ยง วิธีการตรวจสอบและการควบคุม ทักษะของผู้ตรวจสอบ และเป็นที่แน่นอนว่าถ้าผู้ตรวจสอบสามารถวิเคราะห์ความเสี่ยงในลักษณะต่าง ๆ ได้ดี จะทำให้การเข้าถึงจุดควบคุมและการตรวจสอบกระทำได้อย่างมีประสิทธิภาพมากขึ้น โดยเฉพาะอย่างยิ่งการตรวจสอบที่มีเป้าหมายมุ่งไปที่การทุจริต หรือตรวจสอบความเสียหายที่เกิดจากการทุจริตแล้ว เป็นต้น

หนังสือเล่มนี้จึงพยายามวางบทของเนื้อหาให้สัมพันธ์กันเท่าที่จะทำได้เป็นลำดับไป ตามความเข้าใจของผู้เรียบเรียง โดยเฉพาะอย่างยิ่งตัวอย่างการทุจริตต่าง ๆ เป็นสิ่งที่เกิดขึ้นจริง ๆ แล้วทั้งสิ้น ได้เรียบเรียงไว้เป็นบทเรียนของผู้บริหารและผู้พัฒนางานรวมทั้งจุดอ่อนขององค์กรที่ใช้คอมพิวเตอร์ทั้งทางด้าน Data Center และทางด้าน Application ซึ่งมีตัวอย่างจากประสบการณ์จริงของประเทศต่าง ๆ ได้นำมาให้ผู้อ่านได้ศึกษาหลายกรณีด้วยกัน เพื่อให้เป็นแง่คิดของผู้ตรวจสอบการทุจริตในองค์กรที่ใช้คอมพิวเตอร์ต่อ ๆ ไปด้วย

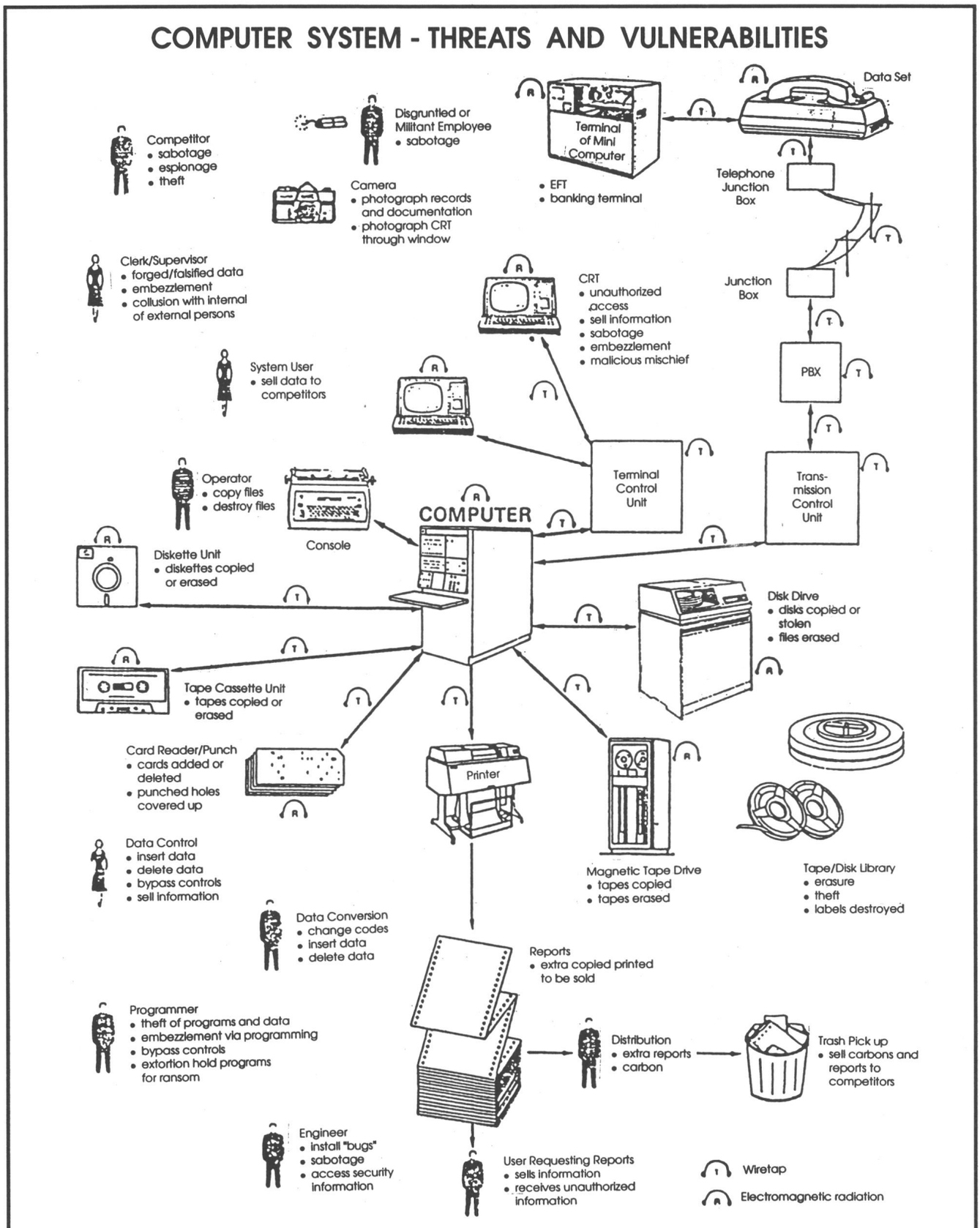
การตรวจสอบการทุจริตในองค์กรที่ใช้คอมพิวเตอร์มีหลักการตรวจสอบเช่นเดียวกับการตรวจสอบระบบคอมพิวเตอร์โดยทั่วไป เพียงแต่มีจุดเน้นหรือเป้าหมายต่างกันไปเท่านั้น หลักการใหญ่ ๆ ได้กล่าวสรุปไว้ในบทที่เกี่ยวข้องในเล่มนี้แล้ว แต่ใคร่ขอทบทวนเพิ่มเติมเล็กน้อยในบทนี้คือ ผู้ตรวจสอบจะต้องเข้าใจเรื่องต่อไปนี้

1. ผู้ตรวจสอบจะมีวิธีเข้าถึงและเข้าใจระบบงานต่าง ๆ ที่มีจำนวนมากมายในแต่ละขั้นตอนขององค์กรที่ใช้คอมพิวเตอร์ได้เพียงใด
2. ผู้ตรวจสอบจะกำหนดความพอเพียงในการรวบรวมเอกสารหลักฐานการตรวจสอบอย่างไร
3. ผู้ตรวจสอบจะระบุจุดควบคุมที่สำคัญหรือไม่ค่อยสำคัญนักเพื่อตัดสินใจทดสอบรายการ และขั้นตอนการควบคุมได้ดีเพียงใด
4. ประสบการณ์ของผู้ตรวจสอบควรจะมีเพิ่มเติมอย่างไรบ้างในการปฏิบัติงานตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ ไม่ว่าจะเป็นการตรวจสอบที่มีเป้าหมายเป็น Financial audit หรือ IS Audit
5. วิธีการตรวจสอบโดยสรุปอีกแบบหนึ่งก็คือ ผู้ตรวจสอบจะ
   - : ตรวจสอบอะไรบ้าง
   - : ต้องการเอกสารหรือต้องเข้าสู่ระบบการประมวลงานอะไรบ้างในการตรวจสอบ
   - : จะตรวจสอบอย่างไร
   - : ผู้ควบคุมงานหรือผู้จัดการฝ่ายตรวจสอบควรตัดสินใจอย่างไรต่อปัญหาที่เกิดขึ้นจากการตรวจสอบ

คอมพิวเตอร์มีผลกระทบต่อการควบคุมและการตรวจสอบ



ปัจจัยที่ผู้บริหารและผู้ตรวจสอบควรทราบ
การตรวจสอบและการควบคุมองค์กรที่ใช้คอมพิวเตอร์ในการประมวลข้อมูล
(ทั้งในกรณีการตรวจสอบตามปกติและการตรวจสอบการทุจริต)



จุดอ่อนและความเสี่ยงที่อาจจะก่อให้เกิดความเสียหายต่อองค์กรที่ใช้คอมพิวเตอร์

ความเสี่ยงกับคอมพิวเตอร์

อาจกล่าวได้ว่าหากกระทำการใดแล้ว ไม่มีเหตุการณ์ที่จะทำให้การกระทำนั้นเกิดความเสียหาย หรือไม่ก็ประสบความสำเร็จตามที่ได้ตั้งใจไว้ ก็ถือว่าการกระทำนั้นไม่มีความเสี่ยง ฉะนั้นการป้องกันหรือการควบคุมใดก็ไม่มีความจำเป็น แต่ตามความเป็นจริง การกระทำต่าง ๆ ที่เกิดขึ้นในโลก ย่อมมีความเสี่ยงด้วยกันทั้งนั้น ไม่มากก็น้อย ตัวอย่างเช่น การเดินข้ามถนน อาจจะเกิดอุบัติเหตุจนถึงแก่ชีวิตฉะนั้นจึงควรป้องกันชีวิตของตนด้วยการมองซ้ายมองขวาก่อนข้ามถนน หรือข้ามถนนบริเวณทางม้าลาย หรือข้ามโดยใช้สะพานลอย เป็นต้น ดังนั้นการป้องกัน และการควบคุมความเสี่ยงจึงเป็นสิ่งที่หลีกเลี่ยงไม่ได้

อย่างไรก็ดีการสร้างระบบการป้องกันและควบคุม ส่วนใหญ่ที่ทำกันมายังไม่ได้มีพื้นฐานมาจากการวิเคราะห์ถึงความเสี่ยงที่อาจเกิดขึ้นทั้งสิ้น จึงทำให้การป้องกันและควบคุมนั้นด้อยประสิทธิผลและประสิทธิภาพ และเป็นการลงทุนที่ให้ผลตอบแทนไม่คุ้มค่า

การวิเคราะห์ความเสี่ยง นอกจากจะเป็นประโยชน์ในการสร้างระบบการป้องกันและควบคุมแล้ว ยังให้ประโยชน์แก่งานด้านการตรวจสอบอีกด้วย กล่าวคือการวิเคราะห์ความเสี่ยง จะทำให้ผู้ตรวจมองเห็นจุดที่ควรทำการตรวจสอบ ซึ่งพิจารณาในแง่ความเสี่ยงก็คือจุดที่อาจก่อให้เกิดความเสียหายนั่นเอง การทราบจุดตรวจสอบที่แน่ชัดจะทำให้การใช้ทรัพยากรตรวจสอบเป็นไปอย่างมีประสิทธผล และประสิทธิภาพ เพราะเป้าหมายของการตรวจสอบที่สำคัญ คือ การค้นหาความผิดพลาดหรือความเสียหายให้ใช้เวลาและเสียค่าใช้จ่ายน้อยที่สุด

การวิเคราะห์ความเสี่ยงที่จะกล่าวในรายละเอียดต่อไปนั้น จะเน้นหนักไปทางด้านการประมวลด้วยคอมพิวเตอร์ (EDP) แต่อย่างไรก็ตาม หลักการนี้ยังสามารถนำไปใช้ในการวิเคราะห์ความเสี่ยงในเรื่องอื่น ๆ ได้อีกด้วย

ความเสี่ยงคืออะไร

ความเสี่ยงคือ เหตุการณ์ที่อาจเกิดขึ้นได้ภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลเสียหายหรือสร้างความล้มเหลวให้แก่ส่วนรวมและส่วนบุคคล ดังนั้นเมื่อกล่าวถึงความเสี่ยงก็ควรระลึกถึง เหตุการณ์ สถานการณ์ และความเสียหายที่อาจเกิดขึ้น ในลักษณะที่มีความสัมพันธ์กัน ตามตัวอย่าง การเดินข้ามถนนข้างต้น ก็ถือว่ามีความเสี่ยง เพราะประกอบด้วยคุณสมบัติ 3 ประการของความเสี่ยงดังนี้

หมายเหตุ : เป็นการทบทวนการวิเคราะห์ที่มาของการควบคุม การสร้างระบบงาน และการตรวจสอบที่เกี่ยวข้องอีกครั้ง เพราะหากท่านผู้อ่านเข้าใจเรื่องนี้ดีแล้ว จะทำให้การบริหารงานด้านคอมพิวเตอร์รวมทั้งกรณีการกำกับงานตรวจสอบองค์กรที่ใช้คอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพเพิ่มขึ้น ไม่ว่าจะเป็นการตรวจสอบทางด้าน IS Audit หรือ Financial Audit ก็ตาม

ก. *เหตุการณ์* ได้แก่ อาจถูกรถยนต์ชน

ข. *สถานการณ์* ได้แก่ เดินสะดุดขาหกล้ม ไม่มีสัญญาณไฟหรือทางข้าม และรถยนต์แล่นด้วยความเร็ว เป็นต้น

ค. *ความเสียหาย* ได้แก่ เสียชีวิตหรือทุพพลภาพ

หลักการวิเคราะห์ความเสี่ยง

การวิเคราะห์ความเสี่ยง คือ การวิเคราะห์ถึงเหตุที่อาจนำไปสู่ความเสียหายหรือความสำเร็จของงานอย่างเป็นระบบ วัฏจักรการวิเคราะห์ฯ ประกอบด้วย 4 ขั้นตอนดังนี้

ก. การพิจารณามูลเหตุที่นำไปสู่ความเสียหาย

ข. การประเมินความเสี่ยงและความเสียหาย

ค. การพิจารณาวิธีการควบคุมความเสี่ยงและความเสียหาย

ง. การประเมินประสิทธิภาพของการควบคุม

การพิจารณามูลเหตุที่นำไปสู่ความเสียหาย

เมื่อกล่าวถึงมูลเหตุที่สร้างความเสียหายให้แก่ EDP หมายถึงเหตุการณ์ อุบัติเหตุ หรือการกระทำที่มีผลกระทบในทางที่เสียหาย คือ Computer System และ Data ซึ่งโดยทั่วไปมักจะถูกเรียกว่า "ความเสี่ยง" แต่แท้ที่จริงแล้วตัว "ความเสี่ยง" หมายถึง โอกาสดีหรือความเป็นไปได้ (Probability) ที่เหตุการณ์นั้นจะเกิดขึ้นภายใต้สถานการณ์ หรือปัจจัยที่นำไปสู่การเกิดเหตุการณ์ที่กล่าว ดังนั้น ความเสี่ยงจึงประกอบด้วยตัวแปร 2 ตัวคือ

1. มูลเหตุที่นำไปสู่ความเสียหาย
2. โอกาสที่จะเกิดเหตุการณ์นั้น

แต่เนื่องจากตัวแปรเกี่ยวกับโอกาสหรือความเป็นไปได้นั้นกำหนดได้ยากหรือไม่สามารถกำหนดได้ ดังนั้นจึงมักจะนิยามความเสี่ยงว่า เป็นมูลเหตุที่นำไปสู่ความเสียหายเท่านั้น

สรุปได้ว่าตัวความเสี่ยงนั้นควบคุมไม่ได้ เพราะฉะนั้นการควบคุมที่ได้ผลต้องควบคุมที่กิจกรรมที่ก่อให้เกิดความเสี่ยงนั้น ๆ

มูลเหตุที่อาจนำไปสู่ความเสียหาย คือ Computer System และ Data แบ่งออกเป็นประเภทใหญ่ ๆ ได้ 6 ประเภทคือ

1. *ภัยธรรมชาติ* เป็นเหตุการณ์ที่ไม่สามารถหลีกเลี่ยงได้ เพราะอยู่เหนือการควบคุมของมนุษย์ เช่น แผ่นดินไหว อายุ น้ำท่วม เป็นต้น แต่มิได้หมายความว่ามนุษย์จะไม่สามารถบรรเทาหรือลดความเสียหาย และฟื้นคืนสภาพปกติได้ การป้องกันที่พอจะทำได้ในกรณีนี้ก็คือ หลีกเลี่ยงพื้นที่ที่คาดว่าจะเกิดเหตุที่กล่าว ดังนั้นข้อมูลทางสถิติเกี่ยวกับภัยพิบัติในพื้นที่ตั้ง Computer จึงมีประโยชน์อย่างมากด้วยการประเมินเหตุการณ์ หรือกำหนด Emergency and Recovery Plans ไว้ล่วงหน้า เพื่อบรรเทาความเสียหายและคืนสภาพปกติได้รวดเร็ว

2. *มนุษย์* กล่าวได้ว่าเหตุการณ์ที่นำไปสู่การเสียหายหรือผิดพลาดทางคอมพิวเตอร์ ส่วนใหญ่เกิดจากการกระทำของมนุษย์ โดยตั้งใจและไม่ได้ตั้งใจกระทำ เช่น เจตนาทำลาย Computer, Data, Files หรือ Programs ให้เสียหายจนใช้งานไม่ได้ หรือ การปฏิบัติงานที่ไม่ถูกต้องไม่เหมาะสมก็อาจนำไปสู่ความเสียหายได้เช่นกัน การป้องกันเหตุร้ายประเภทนี้สามารถทำได้โดยการสร้างระบบการควบคุม และระเบียบการปฏิบัติงานที่รัดกุม

3. *เหตุการณ์* คอมพิวเตอร์มีส่วนทำให้งานยาก หรือที่เป็นไปไม่ได้ให้สามารถทำได้และเป็นไปโดยสะดวก แต่ขณะเดียวกันก็เพิ่มความเสี่ยงใหม่ ๆ ขึ้น เช่น ข้อมูลอาจถูกทำลาย หรือเปลี่ยนแปลง โดยสาเหตุจากความวิบัติของ Hardware และ Software ซึ่งอาจจะเนื่องมาจากตัวของมันเอง หรือจากผู้ใช้ที่ไม่มีความสามารถ การป้องกัน และแก้ไขสามารถทำได้โดยการเข้มงวดการเลือกระบบคอมพิวเตอร์หรือให้มี Maintenance Program เป็นต้น

4. *ระเบียบปฏิบัติงาน* การปฏิบัติงานที่ไม่เป็นไปตามระเบียบและพิธีการที่กำหนด หรือกำหนดระเบียบปฏิบัติงานที่ไม่เหมาะสม เป็นเหตุให้เกิดความผิดพลาดในการปฏิบัติงานได้

5. *การจัดองค์งาน* เกิดจากการมอบหมายอำนาจหน้าที่ความรับผิดชอบ และการติดต่อประสานงานที่ไม่เหมาะสม เช่น สองหน่วยงานมีหน้าที่และความรับผิดชอบเหมือนกัน ผลก็คือไม่มีหน่วยงานใดปฏิบัติหน้าที่ได้อย่างสมบูรณ์ เกิดการผิดพลาดและหลงลืม ทั้งนี้ก็เพราะแต่ละฝ่ายมีความรู้สึกว่าไม่ได้รับผิดชอบงานอย่างเต็มที่จึงมิได้ทำการตรวจสอบและติดตามผลการปฏิบัติงาน เป็นเหตุให้ไม่พบข้อผิดพลาด ดังนั้น การมีข้อบัญญัติเกี่ยวกับอำนาจ หน้าที่และความรับผิดชอบ และการประสานงานที่ดี จะช่วยลดข้อผิดพลาดลงได้

6. *ระบบงาน* มูลเหตุแห่งความเสียหายที่เกิดจากระบบงาน มักมีต้นตอหรือเกี่ยวข้องกับ Functions หรือ Transactions และ Data ของระบบงานนั้น ซึ่งอาจจะมีลักษณะที่คล้ายคลึง หรือแตกต่างจากรายงานอื่นก็ได้ ดังนั้นมูลเหตุเสียหายของระบบงานจึงมีลักษณะเฉพาะ ต่างจากมูลเหตุเสียหายประเภทอื่นที่กล่าวมาแล้ว ตัวอย่างเช่น ระบบเงินฝาก มีมูลเหตุที่อาจนำไปสู่ความเสียหายดังนี้

- บันทึกรายการไม่ถูกต้อง
- บันทึกอัตราดอกเบี้ยไม่ถูกต้อง
- คำนวณดอกเบี้ยจ่ายไม่ถูกต้อง
- จ่ายเงินผิดคนหรือเกินหรือขาด

ฯลฯ

การควบคุมและป้องกันมูลเหตุเสียหายในระบบงานนั้น ปกติมักจะรวมอยู่เป็นส่วนหนึ่งของระบบงาน (Computerized Application) อยู่แล้ว เพื่อให้สามารถป้องกันเหตุร้ายหรือค้นพบได้ในทันทีโดยเฉพาะระบบงานที่มีลักษณะเป็น On-line

เทคนิคที่ใช้ในการค้นหามูลเหตุแห่งความเสียหาย

มูลเหตุของความเสียหายทั้ง 6 ประเภทข้างต้น แสดงให้เห็นเพียงลักษณะกว้าง ๆ เพื่อเป็นพื้นฐานในการวิเคราะห์มูลเหตุที่เป็นจริงของระบบคอมพิวเตอร์ระบบใดระบบหนึ่งภายใต้สถานการณ์ที่แตกต่างกัน การเลือกใช้เทคนิคแบบใดขึ้นอยู่กับความชำนาญ ประสบการณ์ของบุคคลหรือกลุ่มบุคคลที่มีหน้าที่วิเคราะห์ความเสี่ยง เทคนิคฯ แบ่งออกเป็น 3 ประเภทใหญ่คือ

(1) ศึกษาและติดตามจากหนังสือ หรือรายงานที่ออกเป็นประจำ จะทำให้ทราบถึงมูลเหตุความเสียหายที่เกิดขึ้นมาแล้วในองค์การอื่นซึ่งมีสภาพคล้ายคลึงกัน วิธีนี้มีประโยชน์สำหรับผู้ที่มีประสบการณ์น้อยและสะดวก หรือผู้ที่มีเวลาไม่มากนัก หนังสือและรายงานเหล่านี้ได้แก่ Computer Security และ Computer Audit and Controls เป็นต้น

(2) ใช้ Checklists หรือ Questionaire มีหลายองค์กรโดยเฉพาะสำนักงานสอบบัญชีที่ได้ออกแบบ Checklists หรือ Questionaire เกี่ยวกับความเสี่ยงเป็นของตนเอง เพื่อค้นหาจุดหรือแหล่งที่นำไปสู่ความเสียหายทางด้าน EDP ดังนั้นจึงอาจนำมาประยุกต์ใช้กับการค้นหาความเสี่ยงในระบบคอมพิวเตอร์ระบบใดระบบหนึ่งได้ ในบางประเทศหน่วยงานของรัฐซึ่งมีหน้าที่กำกับและควบคุมการใช้คอมพิวเตอร์ในสถาบันการเงิน อาจจะเป็นผู้ที่ออกแบบเครื่องมือชนิดนี้ และถูกนำไปประยุกต์ใช้กันอย่างแพร่หลายทั้งในและนอกประเทศ เช่น EDP Examination Handbook ของ FDIC และ OCC ของประเทศสหรัฐอเมริกา และสำหรับประเทศไทยเรา ธนาคารแห่งประเทศไทยโดยความเห็นชอบของกระทรวงการคลังก็ได้กำหนด Computer Security ขั้นต่ำให้กับธนาคารพาณิชย์ ต้องพึงปฏิบัติตั้งแต่ปี 2528 ก็มีความประสงค์จะลดและป้องกันความเสี่ยงทางด้านคอมพิวเตอร์ของธนาคารพาณิชย์มิให้กระทบไปถึงประชาชนที่เกี่ยวข้อง รวมตลอดไปถึงการป้องกันระบบการเงินให้มีมาตรฐานที่เพียงพอ และสามารถติดตามฐานะของธนาคารที่แท้จริงได้ เป็นต้น

(3) ใช้ทีมงานซึ่งประกอบด้วยบุคคลที่มีประสบการณ์ทางด้านการตรวจสอบ EDP และการรักษาความปลอดภัย ช่วยกันระดมความคิดเกี่ยวกับมูลเหตุเสียหายที่อาจเกิดกับระบบคอมพิวเตอร์ โดยในขั้นแรกนี้ไม่จำเป็นต้องคำนึงถึงว่ามูลเหตุนั้นจะมีเหตุผลหรือไม่มีเหตุผลสนับสนุนก็ตาม ทั้งนี้เพื่อให้ได้ขอบเขตการพิจารณาที่กว้างขวาง หลังจากนั้นจึงค่อยกลับมาพิจารณาคัดเลือกมูลเหตุที่เห็นพ้องต้องกันว่าเหมาะสมหรือเข้ากันได้กับสิ่งแวดล้อมหรือสถานะการณ์ที่เป็นอยู่

ในขั้นตอนนี้นอกจากพิจารณามูลเหตุที่นำไปสู่ความเสียหายแล้ว ผู้ที่นำการวิเคราะห์ความเสี่ยง ควรจะได้พิจารณาเลยไปอีกจุดที่สมควรได้รับการควบคุมด้วยทั้งนี้เพราะการป้องกันให้เกิดมูลเหตุเสียหายนั้นไม่สามารถทำได้โดยตรงกับมูลเหตุ แต่จะสามารถควบคุมกิจกรรมหรืองาน (Activity) และวัตถุ (Resource) ที่เป็นจุดให้เกิดมูลเหตุเสียหาย ดังนั้นเมื่อเสร็จสิ้นงานขั้นตอนนี้แล้วผู้วิเคราะห์ฯ จะได้ข้อมูลเกี่ยวกับความเสี่ยง 2 ตัว คือ มูลเหตุของความเสียหายและจุดที่ควรควบคุม

การประเมินความเสี่ยงและความเสียหาย

หมายถึง การคาดคะเนหรือคำนวณโอกาสที่จะเกิดมูลเหตุฯ ตามที่กล่าวมาแล้ว และความเสียหายที่เป็นผลตามมา ความเสียหายนี้ควรอยู่ในรูปถัวเฉลี่ยโดยวิธีการถ่วงน้ำหนักกับโอกาสที่จะเกิดความเสียหายนั้น (Expected Loss) ทั้งนี้ เพื่อประโยชน์ในการเปรียบเทียบกับความเสียหายที่คาดว่าจะเกิดจากมูลเหตุที่แตกต่างกัน

การประเมินความเสี่ยงและความเสียหาย จะทำให้ผู้วิเคราะห์ฯ ทราบลำดับความสำคัญและขนาดที่แตกต่างกันของความเสี่ยง ซึ่งจะเป็นประโยชน์ในการออกแบบระบบการควบคุมต่อไป ทั้งนี้เพราะการควบคุมให้ได้ทุกจุดหรือมูลเหตุฯ เป็นเรื่องที่กระทำได้ยากและอาจไม่คุ้มค่ากับการลงทุน ดังนั้น จึงควรพิจารณาควบคุมเฉพาะความเสี่ยงและความเสียหายที่มีนัยสำคัญเท่านั้น นอกจากนั้นยังสามารถใช้ข้อมูลที่ได้นี้ประเมินประสิทธิภาพของการควบคุมได้อีกด้วย โดยเปรียบเทียบมูลค่าความเสียหายกับค่าใช้จ่ายในการควบคุมที่เพิ่มขึ้น ถ้าค่าใช้จ่ายสูงกว่าหรือเท่ากับความเสียหายก็แสดงว่าการควบคุมนั้นไม่มีประสิทธิภาพ

วิธีการที่ใช้ในการประเมินความเสี่ยงและความเสียหาย

(1) ใช้ข้อมูลจากเหตุการณ์ที่เกิดขึ้นแล้วในอดีต

คาดการณ์ความเสียหายที่จะเกิดขึ้นในปัจจุบันและอนาคต ความสำเร็จของวิธีนี้ขึ้นอยู่กับความเพียงพอ และความถูกต้องของข้อมูลที่รวบรวมได้ มักใช้ได้ดีกับเหตุการณ์ที่เกิดขึ้นบ่อย ๆ ในการปฏิบัติงานประจำ เช่น การป้อนข้อมูลผิดพลาด, Computer Rerun, Equipment Failures และ Data Rejects เป็นต้น ตัวอย่างเช่น จากข้อมูลในอดีตพบว่าในการป้อนข้อมูล 1,000 รายการ จะมีการผิดพลาด 5 รายการ ความเสียหายเฉลี่ยรายการละ 100 บาท ถ้าปีหนึ่งมีรายการทั้งหมด 1,000,000 ราย ความเสียหายที่คาดว่าจะเกิดขึ้นทั้งปี (Expected Loss) จะเท่ากับ 500,000 บาท (100 x 5/1,000 x 1,000,000) ข้อเสียของวิธีนี้คือไม่สามารถใช้ได้กับเหตุการณ์ที่ยังไม่เกิดขึ้นมาก่อนหรือเกิดขึ้นน้อยมาก เช่น ความเสียหายที่เกิดจากน้ำท่วม แผ่นดินไหว และพายุ เป็นต้น

(2) ใช้สูตรสำเร็จคำนวณหาค่า Expected Loss

โดยการแทนค่าตัวแปรในสูตรซึ่งแบ่งเป็น 2 กลุ่มคือ ตัวแปรเกี่ยวกับความถี่ และตัวแปรเกี่ยวกับมูลค่าเสียหาย วิธีนี้เหมาะสำหรับกรณีที่ไม่สามารถหาข้อมูลในอดีตได้ หรือไม่เคยมีประสบการณ์เกี่ยวข้องกับความเสียหายมาก่อน ดังนั้นการที่สามารถคำนวณมูลค่าเสียหายได้ก็ยังดีกว่าไม่ได้ทำอะไรเลย เนื่องจากวิธีนี้ให้ผลการคำนวณอย่างหยาบ ๆ จึงเหมาะกับการพิจารณาเรื่องที่อาจก่อให้เกิดความเสียหายขนาดใหญ่หรือในแง่ของการรักษาความปลอดภัย สูตรการคำนวณที่ใช้กันอย่างแพร่หลาย คือสูตรของ Robert H. Courtney จาก IBM

$E = P \times V$ ..... (1)

E = Expected Loss

P = Expected Frequency

V = Loss

$P = 10 (p-4)$ หรือ $1/3 \times 10 (p-3)$.....(2)

P = ตัว Parameter ที่มีค่าขึ้นอยู่กับความถี่ของการเกิดเหตุการณ์

$V = 10^{v}$ .....(3)

V = ตัว Parameter ที่มีค่าขึ้นอยู่กับขนาดของความเสียหาย

$E = (1/3) \times 10 (p + v - 3)$ .....(4)

ตัวอย่าง ตารางค่า p และ v

Estimated Frequency				p	Loss	V
1	ครั้งใน	30	ปี	1	100	1
1	“	3	ปี	2	1,000	2
1	“	100	วัน	3	10,000	3
1	“	10	วัน	4	100,000	4
1	“	1	วัน	5	1,000,000	5
10	“	1	วัน	6	10,000,000	6
100	“	1	วัน	7	100,000,000	7

ผู้วิเคราะห์จะต้องเลือกระดับความถี่ และความเสียหายที่เห็นว่าเหมาะสมที่สุด แล้วแทนค่า P และ V ลงในสูตรที่ (4) จะสังเกตเห็นว่าค่าของความถี่และความเสี่ยงภายในตารางข้างบนนั้นมีความแตกต่างกันอย่างเป็นอนุกรม ทำให้ง่ายต่อการเปรียบเทียบเพื่อเลือกความถี่และความเสียหายที่สมเหตุสมผลกว่า ข้อเสียของสูตรนี้ คือ ไม่สามารถพิสูจน์ที่มาของสูตรได้ในเชิงคณิตศาสตร์ ผลลัพธ์ที่ได้จากการคำนวณเป็นตัวเลขหยาบ ๆ ซึ่งอาจก่อให้เกิดการเข้าใจผิดได้ เช่น E = 99,999.99 มิได้หมายความ ความเสียหายจะเท่ากับจำนวนนั้นอย่างแน่นอน นอกจากนั้นค่าของ E คำนวณโดยถือเกณฑ์เฉลี่ยรายปี ซึ่งความเสียหายต่อปีนี้อาจจะมีความสำคัยน้อยเมื่อเทียบกับความเสียหายรวม เช่น ทุก 10 ปีจะเกิดความเสียหาย 100,000 บาทดังนั้นความเสียหายเฉลี่ยปีละ 10,000 บาท ซึ่งพิจารณาแล้วจะเห็นว่าความสำคัญน้อยกว่าถ้าพิจารณาความเสียหายที่เกิดขึ้นทั้งหมดก็จะเห็นถึงความมีนัยสำคัญ

(3) คาดการณ์โดยอาศัยความรู้สึก

อันเกิดาจากประสบการณ์ของผู้วิเคราะห์ จะเห็นได้ว่ามีหลายกรณีที่การตัดสินใจเรื่องสำคัญ ๆ เป็นไปอย่างถูกต้องและแม่นยำ โดยที่ไม่จำเป็นต้องอาศัยข้อมูลในอดีตหรือการคำนวณใด ๆ ทั้งนี้เป็นเพราะผู้ทำหน้าที่ตัดสินใจมีความชำนาญและประสบการณ์สูง ข้อจำกัดของวิธีนี้จึงขึ้นกับความชำนาญและประสบการณ์ของผู้วิเคราะห์

(4) สร้างมโนภาพหรือฉากขึ้นมา

โดยจำลองสถานการณ์ทุกอย่างซึ่งส่งผลในทางลบ ใช้ในกรณีที่ไม่สามารถหาข้อมูลอดีต หรือไม่สามารถคาดคะเนจากความรู้สึกได้ หรือไม่สันทัดกับการใช้สูตรคำนวณ การสร้างมโนภาพหรือฉาก อาจทำได้หลายรูปแบบ แต่ในที่นี้จะกล่าวถึงเฉพาะแบบการบรรยาย

การสร้างมโนภาพแบบบรรยาย คือ การบรรยายสภาพแวดล้อมและความเสียหายที่เป็นไปได้ทั้งหมดจากเหตุการณ์ที่คาดไว้ หรือถ้าเกิดเหตุการณ์ดังกล่าวแล้วจะเสียหายทางใดบ้าง วิธีการนี้ไม่ได้มุ่งหมายจะแสดงความเสี่ยง และความเสียหายในรูปจำนวนที่วัดได้ แต่จะแสดงรูปรวมของความเสียหาย เช่น การสูญเสียความนิยม การถูกดำเนินคดีทางกฎหมาย หรือการทุจริต เป็นต้น ซึ่งก็เป็นแนวทางในการประเมินความเสียหายอย่างหนึ่ง ในขณะที่ไม่มีหรือมีข้อมูลน้อยจนไม่ทราบว่าจะเริ่มต้นทำอะไรดี ข้อดีของวิธีนี้คือ ครอบคลุมเหตุการณ์ที่เป็นไปได้เกือบทั้งหมด และช่วยให้ผู้วิเคราะห์ทราบถึงจุดอ่อนไปด้วยในขณะที่คิดคำนึงถึงมโนภาพ หรือฉาก ข้อเสียคือ ถ้าสร้างมโนภาพหรือฉากที่ไม่สมเหตุผล และเป็นไปได้ยากในทางปฏิบัติองค์กรก็จะเสียค่าใช้จ่ายไปในสิ่งที่ห่างไกลจากความเป็นจริง และหากมโนภาพที่สร้างขึ้นตกไปอยู่ในมือของผู้ที่ประพฤติมิชอบก็จะเป็นอันตรายต่อองค์กร เพราะเท่ากับเป็นพิมพ์เขียวสำหรับการกระทำที่มิชอบต่อคอมพิวเตอร์ ดังนั้นจึงควรเก็บไว้ในที่ปลอดภัยและควบคุมการเข้าถึง

เมื่อจบขั้นตอนที่สอง ก็อาจกล่าวได้ว่าการวิเคราะห์ความเสี่ยงเสร็จสิ้นแล้ว และจะได้ข้อมูล 3 ตัว เพื่อนำไปใช้ในการพินิจพิเคราะห์ การควบคุมต่อไป คือ มูลเหตุ จุดที่เกิดเหตุและความเสียหายแต่อย่างไรก็ตามจากคำบรรยายเทคนิคการประเมินความเสี่ยงและความเสียหายข้างต้น จะเห็นได้ว่าการประเมินความเสียหายในรูปตัวเงินมีข้อจำกัดหลายประการ (แต่ก็ยังเป็นสิ่งที่ควรกระทำหากเป็นไปได้) ดังนั้นความเสียหายในรูปของคำบรรยายจึงอาจนำมาใช้ให้เป็นประโยชน์ในการพิจารณาการควบคุมได้เช่นเดียวกัน นอกจากนั้นในการพิจารณาการควบคุมบางครั้งก็มิได้พิจารณาจากเหตุผลของความเสียหายทางเงินเท่านั้น เช่น การสร้างความพอใจให้ลูกค้า การปรับปรุงประสิทธิภาพในการปฏิบัติงาน เป็นต้น

ความเสียหายอาจแบ่งเป็นประเภทใหญ่ได้ดังนี้

ก. รายการทางการเงินผิดพลาด เกิดจากการบันทึกรายการไม่ตรงตามวันเวลา จำนวนเงินและประเภทบัญชีไม่ถูกต้อง

ข. รายการบันทึกบัญชีไม่เป็นที่ยอมรับเกิดจากการกำหนดนโยบายทางการบัญชีที่ไม่ถูกต้องหรือไม่เหมาะสม

ค. ธุรกิจหยุดชะงัก ในองค์การที่ใช้ระบบคอมพิวเตอร์ในการประมวลผลและปฏิบัติงาน เช่น ธนาคารพาณิชย์ และบริษัทการเงิน เป็นต้น การที่เครื่องคอมพิวเตอร์และโปรแกรมหยุดการทำงาน หรือทำงานอย่างวิปริตโดยไม่ทราบสาเหตุ อาจเป็นเหตุให้การประกอบธุรกิจขององค์การหยุดชะงักชั่วคราว หรือเป็นเวลานานได้ นั่นหมายถึงการสูญเสียธุรกิจและรายได้จำนวนหนึ่ง

ง. การตัดสินใจที่ผิดพลาด เกิดจากการได้รับข้อมูลที่ไม่ถูกต้อง หรือไม่มีข้อมูลในการตัดสินใจ

จ. การทุจริตและฉ้อฉล เกิดจากการนำเงินไปใช้เพื่อประโยชน์ส่วนตัวหรือหลอกลวงผู้อื่น

ฉ. การถูกดำเนินคดีหรือถูกลงโทษโดยทางราชการ เช่น การถูกเปรียบเทียบปรับ เนื่องจากกระทำการฝ่าฝืนกฎหมายเฉพาะที่ควบคุมกิจการนั้น หรือถูกคำพิพากษาให้ชดใช้ค่าสินไหม เป็นต้น

ช. รายจ่ายส่วนเกิน หมายถึง รายจ่ายที่องค์การควรจะหลีกเลี่ยงได้ มิฉะนั้นอาจมีผลต่อการทำกำไรขององค์การ

ซ. ทรัพย์สินสูญหายหรือถูกทำลาย หมายถึง สินทรัพย์ทั่วไป เงินสดและข้อมูลสำคัญ สูญหายหรือถูกทำลายโดยไม่ตั้งใจ

ฌ. ผลเสียต่อการแข่งขันทางการค้า หมายถึง ไม่สามารถสนองความต้องการของตลาดได้ทัน หรือโต้ตอบกับคู่แข่งขันได้อย่างมีประสิทธิภาพ

ญ. ความลับรั่วไหล หมายถึง ความเสียหายโดยส่วนตัวหรือส่วนรวม อันเนื่องจากข้อมูลที่สำคัญถูกนำออกไปใช้โดยไม่ได้รับอนุญาตหรือโดยไม่ตั้งใจ

ฎ. ความต้องการของ User ไม่ได้รับการสนองตอบ หมายถึง วิธีการปฏิบัติงานหรือระบบงานไม่ตรงกับเป้าหมายและความต้องการของ User

ฏ. ภาพพจน์ถูกทำลาย หมายถึง การที่ลูกค้า สาธารณชน และรัฐบาล ขาดความไว้เนื้อเชื่อใจต่อองค์กรความเสียหายตามข้างต้น อาจวัดเป็นจำนวนได้หากผู้วิเคราะห์มีข้อมูลและประสบการณ์เพียงพอ ดังวิธีการประเมินความเสี่ยงและความเสียหายที่กล่าวไปแล้ว

การจัดการกับความเสี่ยง

เมื่อทราบมูลเหตุ ความเสี่ยงและความเสียหายแล้ว ต่อไปก็จำต้องพิจารณาว่าจะจัดการกับมันอย่างไร การจัดการกับความเสี่ยงมี 2 แบบ คือ

1. Risk Control คือการใช้มาตรการทางด้านการควบคุมเพื่อกำจัดหรือลดความเสี่ยงและความเสียหาย ซึ่งจะได้กล่าวเพิ่มเติมในเรื่องของการพิจารณาและประเมินประสิทธิภาพของการควบคุมต่อไป

2. Risk Financing คือ การโอนความเสี่ยงไปให้บุคคลอื่น เช่น การประกันภัย เป็นต้น ปกติการประกันภัยมักจะถูกใช้ควบคู่ไปกับการควบคุมความเสี่ยงเสมอ ทั้งนี้เพราะการควบคุมแต่เพียงอย่างเดียวไม่อาจป้องกันหรือบรรเทาความเสียหายได้ร้อยเปอร์เซ็นต์ หรือได้ทุกกรณี เราไม่อาจเสี่ยงต่อความเสียหายได้ แม้จะมีโอกาสเกิดน้อยก็ตาม เนื่องจากความเสียหายบางอย่างมีมูลค่าสูงเกินกว่าที่จะยอมรับได้ เช่น เครื่องคอมพิวเตอร์ถูกทำลายเสียหายจนใช้การไม่ได้ เป็นต้น

การประกันภัยทางด้านคอมพิวเตอร์

หมายถึง การประกันภัยที่อาจเกิดขึ้นกับ Hardware Software พนักงานและการปฏิบัติงาน ฯลฯ ภัยที่กล่าวได้แก่ ไฟไหม้ น้ำท่วม การทุจริต ภัยธรรมชาติ ไฟฟ้าขัดข้อง การบริการล่าช้า การหยุดชะงักของธุรกิจ และความเสียหายที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ นอกจากนั้นผู้เอาประกันและผู้รับประกันอาจตกลงเงื่อนไขอย่างอื่นเป็นพิเศษก็ได้

สิ่งที่ควรเอาประกันภัยเกี่ยวกับคอมพิวเตอร์

(1) เครื่องคอมพิวเตอร์และอุปกรณ์อื่น ๆ
(2) ความซื่อสัตย์ของพนักงาน
(3) Media ที่เก็บข้อมูลและโปรแกรม
(4) ค่าใช้จ่ายพิเศษที่อาจเกิดขึ้น
(5) ความเสียหายที่เกิดขึ้นจากการหยุดชะงักของธุรกิจเพราะคอมพิวเตอร์
(6) ข้อผิดพลาดและข้อบกพร่องจากการปฏิบัติงาน
(7) การสูญหายของข้อมูล
(8) ความรับผิดชอบที่มีต่อลูกค้าหรือบุคคลที่สาม

การพิจารณาวิธีการควบคุมความเสี่ยงและความเสียหาย

การควบคุมมีความมุ่งหมายเพื่อขจัดหรือลดความเสี่ยงและความเสี่ยงที่อาจเกิดกับองค์กร อย่างน้อยที่สุดหากมีภัยและมีความเสียหายเกิดขึ้น ก็อยู่ในวิสัยที่จะรับได้ หรือทำให้กลับคืนสู่สภาวะปกติได้ แนวคิดในการสร้างระบบการควบคุมมีหลายแนวทาง แต่การวิเคราะห์ความเสี่ยง เป็นแนวทางที่ทำให้การสร้างระบบการควบคุมเป็นไปอย่างรัดกุมและมีประสิทธิภาพมากที่สุด เนื่องจากตั้งอยู่บนพื้นฐานของแนวความคิดที่เป็นระบบและมีเหตุมีผล

จากการวิเคราะห์ความเสี่ยง ผู้วิเคราะห์จะได้ข้อมูลที่นำไปพิจารณาการควบคุมต่อไป

ก. ลักษณะของความเสี่ยง (Description of Risk)
ข. ความเสียหาย (Magnitude of Risk)

สิ่งที่ต้องพิจารณาในขั้นนี้เพื่อกำหนดเป็นนโยบาย และเป้าหมายของการควบคุมก็คือ ความมีนัยสำคัญหรือระดับความเสี่ยงและความเสียหายที่ไม่อาจยอมรับได้จำเป็นต้องมีการควบคุม ทั้งนี้ เพราะการควบคุมความเสียหายให้ได้ทั้งหมดเป็นเรื่องที่ทำได้ยาก หรือหากกระทำได้ก็อาจเป็นการลงทุนที่ไม่คุ้มค่า

สิ่งที่ควรพิจารณาเกี่ยวกับการควบคุม

(1) จุดที่คบคุม

ตามที่กล่าวแล้วว่าเราไม่สามารถควบคุมตัวความเสี่ยงได้โดยตรง แต่เราสามารถควบคุมกิจกรรมที่เกิดความเสี่ยงและความเสียหายได้ ดังนั้นจุดที่เกิดความเสี่ยงและจุดที่มีการควบคุมจึงเป็นจุดเดียวกัน การเลือกจุดที่ควรควบคุมมีอยู่ 2 แนวทาง ซึ่งขึ้นอยู่กับความเสี่ยงว่าเป็นความเสี่ยงของระบบคอมพิวเตอร์ (EDP Resource) หรือระบบงานคอมพิวเตอร์ (EDP Application)

ก. ความเสี่ยงของระบบคอมพิวเตอร์ ส่วนใหญ่จะเกิดกับ Hardware software Data Files และ Operation เป็นต้น จุดที่ควรควบคุมก็คือจุดที่สามารถเข้าถึงสิ่งที่กล่าวมาแล้วได้

ข. ความเสี่ยงของระบบงานคอมพิวเตอร์ ส่วนใหญ่เกิดกับ Transactions หรือ Functions ของระบบงาน อันเนื่องมาจาก

- ข้อมูลถูกเปลี่ยนแปลงแก้ไข
- รายการถูกดึงออกไปจากระบบงาน
- ผู้รับประโยชน์ถูกเปลี่ยนแปลงแก้ไข
- รายการเพิ่มเข้ามาในระบบงาน
- ข้อมูลบางส่วนหายไป

ฯลฯ

ดังนั้นจุดที่ควบคุมก็คือ จุดที่อาจทำให้ Transactions มีการเปลี่ยนแปลงดังกล่าว

(2) ลักษณะของการควบคุม

การควบคุมโดยทั่วไปอาจแบ่งออกได้เป็น 2 ประเภท คือ การควบคุมทางด้านการเงิน (Financial control) และ การควบคุมการปฏิบัติงาน (Operation Control)

การควบคุมทางด้านการเงิน หมายถึง การควบคุมเพื่อให้รายการทางการเงินถูกต้องสมบูรณ์และเป็นไปตามหลักการบัญชีที่ยอมรับกันโดยทั่วไป

การควบคุมการปฏิบัติงาน หมายถึง การควบคุมให้มีการปฏิบัติงานเป็นไปอย่างมีประสิทธิผลและประสิทธิภาพ

นอกจากนั้นการควบคุมอาจแบ่งออกได้เป็น 3 ลักษณะ คือ

ก. การป้องกัน หรือหลีกเลี่ยง มูลเหตุที่นำไปสู่ความเสียหาย (Preventive controls)

ควรใช้กับความเสี่ยงที่ก่อให้เกิดความเสียหายและยากต่อการแก้ไขหรือเสียค่าใช้จ่ายมาก เช่น การป้องกันมิให้เข้าไปในห้องคอมพิวเตอร์ และใช้เครื่องโดยไม่ได้รับอนุญาต เป็นต้น การป้องกันอาจทำได้โดยมียามรักษาการ และออก passward ให้แก่ผู้มีสิทธิใช้เครื่อง เป็นต้น

ข. การตรวจสอบให้พบมูลเหตุ หรือปัญหา ที่อาจนำไปสู่ความเสียหาย (Detection Controls)

ควรใช้กับความเสี่ยงที่ยังไม่เกิดความเสียหายโดยทันที หรืออาจไม่เกิดความเสียหายร้ายแรง หรือถ้าจะคิดป้องกันก็คงทำได้ยากและเสียค่าใช้จ่ายมาก เช่น การป้อนข้อมูล การป้องกันมิให้มีการป้อนข้อมูลผิดพลาด ย่อมทำได้ยากกว่าตรวจสอบว่ามีข้อมูลที่ผิดพลาดหรือไม่ เป็นต้น การควบคุมในลักษณะนี้มักใช้ เพื่อเสริมให้การควบคุมในแบบแรกมีประสิทธิภาพยิ่งขึ้น มีข้อที่ควรระวังก็คือ การควบคุมนี้เป็นเพียงเครื่องมือค้นพบปัญหา แต่หากปัญหานั้นไม่ได้รับการแก้ไขหรือแก้ไขไม่ถูกต้อง ความเสียหายก็ยังเกิดขึ้นได้อีก โดยเฉพาะกรณีที่มีเจตนาละเมิด (Override) การควบคุมนั้น

ค. การตรวจสอบให้พบมูลเหตุหรือปัญหาที่นำไปสู่ความเสียหาย และพร้อมกับกำหนดวิธีการแก้ไขไว้ล่วงหน้า (Detection and Corrective Controls)

การควบคุมแบบนี้ดีกว่าแบบที่สอง เพราะว่าปัญหาที่ตรวจพบจะได้รับการแก้ไขอย่างเหมาะสมและรวดเร็ว เช่น การควบคุมความเสี่ยงอันเกิดจากไฟไหม้ โดยการติดตั้งเครื่อง Fire Alarm แต่เน้นอย่างเดียวยังไม่เพียงพอ เพราะแม้จะได้รับการเตือนว่าเกิดไฟไหม้ขึ้นแล้ว หากไม่สามารถดับไฟได้อย่างรวดเร็ว ความเสียหายก็ยังคงมีอยู่ ฉะนั้นจึงควรติดตั้งเครื่องดับไฟอัตโนมัติที่ควบคู่กันไปด้วย ซึ่งจะทำให้สามารถควบคุมความเสียหายได้ดีขึ้น

(3) เทคนิคที่ใช้ในการควบคุม

หมายถึง วิธีปฏิบัติในการควบคุม อาจแยกออกได้เป็น 7 วิธี

ก. Redundancy Check หมายถึง การกระทำในสิ่งเดียวกันอย่างน้อย 2 ครั้ง แต่ต่างวิธีกัน แล้วเปรียบเทียบผลลัพธ์ที่ได้ เช่น การคำนวณตัวเลขต่าง ๆ เป็นต้น

ข. Verify หมายถึง การตรวจสอบกับหลักฐานที่เชื่อถือได้ เช่น ตรวจสอบเลขที่บัญชีของผู้ฝาก/ถอน กับ Data Base เป็นต้น

ค. Confirmation หมายถึง การให้ยืนยันความถูกต้อง เช่น กำหนดให้ผู้ป้อนรายการข้อมูลในระบบ Online ยืนยันความถูกต้องของข้อมูลที่ปรากฏอยู่บนจอเทอร์มินัล ก่อนที่ข้อมูลจะเข้าสู่ระบบ

จ. Recalculation หมายถึง การคำนวณซ้ำในจุดที่มีการคำนวณปกติจะให้คำนวณด้วยมือ (Manual) แล้วเทียบกับการคำนวณด้วยคอมพิวเตอร์ หรือสลับกันโดยสูตรในการคำนวณเหมือนกัน

ฉ. Limit หมายถึง การกำหนดขอบเขตของหน้าที่ การกระทำหรือรายการไว้แน่นอน ซึ่งสามารถทำได้ทั้งปริมาณ และจำนวนเงิน เวลาและความถี่ เช่นการยินยอมให้ป้อนรหัสประจำตัว (Passward) ผิดพลาดได้ไม่เกิน 3 ครั้ง ติดต่อกัน ครั้งที่ 4 เครื่อง จะยึดบัตร หรือยกเลิกรายการที่จะกระทำต่อไป

ช. Containment หมายถึง การสกัดกั้นมิให้ความเสียหายระบาดหรือลุกลามไปยังที่อื่น เช่น กรณีเครื่องคอมพิวเตอร์ตั้งอยู่ใกล้ ๆ กัน 2 เครื่อง ควรกั้นผนังทนไฟระหว่างเครื่องคอมพิวเตอร์เพื่อป้องกันมิให้ไฟลุกลามจากเครื่องหนึ่งไปอีกเครื่องหนึ่ง เป็นต้น

ซ. Fallback หมายถึง การกำหนดวิธีปฏิบัติหรือระบบสำรองในกรณีเกิดความเสียหายบางส่วนหรือทั้งหมด เพื่อให้สามารถดำเนินงานต่อไปได้ เช่น กรณี Data Base ถูกทำลาย หรือ Memory บางส่วนไม่สามารถใช้งานได้ เป็นต้น

(4) การควบคุมทุกระบบควรมีการแก้ไขควบคู่กันไปด้วย

เพราะการทราบว่ามีปัญหาแต่ไม่ทราบวิธีการแก้ไขที่เหมาะสมย่อมไม่สามารถป้องกันหรือบรรเทาความเสียหายได้

(5) การควบคุมด้วยเครื่องคอมพิวเตอร์หรือเครื่องมือกลอื่น ๆ ย่อมดีกว่าการควบคุมด้วยมือ (Manual Controls)

ถึงแม้ว่าการควบคุมโดยทั่วไปอาจทำได้ทั้งโดยบุคคลและโดยเครื่องมือกล แต่ก็เป็นที่ยอมรับกันว่าการควบคุมโดยเครื่องมือกลมีประสิทธิภาพมากกว่า

(6) การควบคุมที่ดีควรมีหลักฐาน

แสดงให้เห็นว่า ได้ควบคุมจริงและเป็นไปตามระเบียบและกฎเกณฑ์ที่กำหนดไว้

การประเมินประสิทธิภาพของการควบคุม

เป็นขั้นตอนสุดท้ายของวัฏจักรในการวิเคราะห์ความเสี่ยง เพื่อจัดทำข้อมูลสำหรับการตัดสินของฝ่ายบริหารว่าควรมีการควบคุมหรือไม่และอย่างใด

จากการวิเคราะห์ความเสี่ยง ทำให้เราทราบมูลเหตุที่เกิดความเสี่ยงและความเสียหาย ดังนั้น การควบคุมที่ดีหรือที่มีประสิทธิภาพจึงควรเป็นการควบคุมที่สามารถลดความเสียหายลงให้ได้น้อยที่สุด (Minimize Loss) หรืออีกนัยหนึ่งก็คือให้ผลตอบแทนต่อการลงทุนมากที่สุด (Maximize Benefit) วิธีการพิจารณาอย่างง่าย ๆ ก็คือ การเปรียบเทียบระหว่างความเสียหายที่คาดว่าจะเกิดขึ้น (Expected Loss) กับรายจ่ายในการควบคุม (Control Cost) ถ้าหากความเสียหายมากกว่ารายจ่ายในการควบคุมก็แสดงว่าการควบคุมนั้นมีประสิทธิภาพ ในกรณีที่มีหลายทางเลือกให้เลือกการควบคุมแบบที่เสียค่าใช้จ่ายน้อยสุด โดยมีเงื่อนไขว่าการควบคุมทุกแบบสามารถคุ้มครองสามารถคุ้มครองความเสียหายได้เท่าเทียมกัน

ในกรณีที่ไม่ทราบหรือไม่สามารถคำนวณความเสี่ยงในรูปจำนวนเงินได้การตัดสินใจในการควบคุมอาจต้องใช้เกณฑ์อื่น อาทิเช่น การเปรียบเทียบรายจ่ายในการควบคุมกับมูลค่าความเสียหายทั้งสิ้น (Total Loss) สมมุติว่ากิจการมีเงินให้กู้ยืมทั้งสิ้น 1,000 ล้านบาท อาจจะกำหนดเกณฑ์ในการตัดสินใจว่า รายจ่ายในการควบคุมไม่ควรเกินร้อยละ 0.5 ของมูลค่าเงินให้กู้ยืม ซึ่งเท่ากับ 5 ล้านบาท เป็นต้น

อย่างไรก็ตาม การตัดสินใจควบคุมบางอย่างมิได้ขึ้นอยู่กับประสิทธิภาพของการควบคุม แต่จำเป็นต้องมีการควบคุมเพื่อความอยู่รอดของกิจการ เช่น การควบคุมที่เกิดจากระเบียบหรือข้อบังคับของรัฐ เป็นต้น

บทที่ 2

การป้องกันดีกว่าการแก้ไข

ทบทวนมาตรฐานการตรวจสอบและแนวความคิดในการตรวจสอบเพื่อการบริหารที่มีประสิทธิภาพและป้องกันการทุจริต

ผู้สอบบัญชีไม่เพียงแต่ต้องทำความคุ้นเคยกับมาตรฐานเบื้องต้น และแนวความคิดด้านการตรวจสอบเท่านั้น ยังต้องเข้าใจถึงมาตรฐานและแนวความคิดอื่น ๆ เพิ่มเติม โดยเฉพาะอย่างยิ่งในเรื่องวิธีการตรวจสอบระบบการประมวลผลโดยใช้คอมพิวเตอร์ มาตรฐานและแนวความคิดการตรวจสอบพื้นฐานมิใช่เปลี่ยนแปลงไปง่าย ๆ เพียงเพราะ เราเปลี่ยนการประมวลผลข้อมูลทางบัญชีจากระบบที่ทำด้วยมือไปสู่ระบบเครื่องจักรลงบัญชีไปสู่ระบบคอมพิวเตอร์ อย่างไรก็ตามผู้สอบบัญชีมีภาระที่จะต้องเรียนรู้ในเรื่องมาตรฐานและแนวความคิดเพิ่มเติมในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลทางบัญชีโดยใช้คอมพิวเตอร์ ตัวอย่างเช่น แนวความคิดของการแบ่งแยกหน้าที่การบันทึกบัญชีที่ใช้ในการประมวลผลข้อมูลทางบัญชีในระบบที่ทำด้วยมือ ระบบเครื่องจักรลงบัญชี และระบบคอมพิวเตอร์ ซึ่งในการประมวลผลโดยใช้คอมพิวเตอร์นั้น การปรับใช้แนวความคิดมีความยุ่งยากซับซ้อนมากกว่าระบบที่ทำด้วยมือ ผู้สอบบัญชีจะต้องเกี่ยวข้องกับเรื่องการแบ่งแยกหน้าที่บุคลากรภายในฝ่ายบัญชี (accounting department) ซึ่งใช้คอมพิวเตอร์ในการประมวลผลข้อมูลภายในฝ่ายประมวลผลข้อมูลโดยใช้คอมพิวเตอร์ (EDP department) และระหว่างฝ่ายประมวลผลข้อมูลโดยใช้คอมพิวเตอร์กับฝ่ายผู้ใช้งาน (user department)

หากผู้บริหารและผู้สอบบัญชีขององค์กรมีสายตาที่กว้างไกล การเข้าใจระบบของบุคคลภายในทั้งในส่วนที่ใช้คอมพิวเตอร์ และส่วนที่ไม่ใช้คอมพิวเตอร์ จะทำให้มีการวางแผนป้องกันระบบงานได้อย่างรัดกุมและลดช่องว่างของการทุจริตได้ เพราะถ้าองค์กรวางระบบงานไว้ดีพอ โอกาสการทำทุจริตโดยผู้ไม่หวังดีก็จะยากขึ้น

ผู้สอบบัญชีด้านคอมพิวเตอร์ต้องยึดหลักของมาตรฐานการตรวจสอบทั่วไปที่ได้รับการยอมรับแล้ว ซึ่งประกอบด้วยมาตรฐานทั่วไป (general standards) มาตรฐานการปฏิบัติงาน (standards of field work) และมาตรฐานการรายงาน (standards of reporting) ดังนี้

มาตรฐานทั่วไป (General standards)

1) ผู้สอบบัญชีต้องมีความรู้ความสามารถ และมีความชำนาญงานในหน้าที่ผู้สอบบัญชี
2) ผู้สอบบัญชีต้องปฏิบัติหน้าที่ด้วยความอิสระและเที่ยงธรรม
3) ผู้สอบบัญชีต้องตรวจสอบและเสนอรายงานการสอบบัญชีด้วยความระมัดระวังรอบคอบ (และควรคำนึงถึงโอกาสของการทุจริตที่จะเกิดขึ้นได้ แล้วตั้งเป้าหมายการตรวจสอบถ้าต้องการ)

มาตรฐานการปฏิบัติงาน (Standards of field work)

1) ผู้สอบบัญชีต้องวางแผนการตรวจสอบและกำกับควบคุมการปฏิบัติงานของผู้ช่วย (ถ้ามี)
2) ผู้สอบบัญชีต้องประเมินประสิทธิภาพการควบคุมภายในของกิจการที่จะตรวจสอบ เพื่อกำหนดขอบเขตการปฏิบัติงานตรวจสอบให้รัดกุมและเหมาะสม

3) ผู้สอบบัญชีต้องปฏิบัติงานตรวจสอบให้ได้มาซึ่งหลักฐานที่ถูกต้องและเพียงพอโดยใช้วิธีการตรวจสอบ การสังเกต การสอบถาม และการยืนยันรายการ เพื่อให้มีเหตุผลในการให้ความเห็นเกี่ยวกับงบการเงินของกิจการแห่งนั้น ๆ

มาตรฐานการรายงาน (Standards of reporting)

1) ผู้สอบบัญชีต้องระบุว่างบการเงินที่เสนอนั้นเป็นไปตามหลักการบัญชีที่รับรองทั่วไปหรือไม่

2) ผู้สอบบัญชีต้องแสดงความเห็นไว้ในรายงานการสอบบัญชีว่า หลักการบัญชีที่ใช้ถือปฏิบัติเช่นเดียวกับปีก่อนหรือไม่ เพียงใด

3) ข้อความและรายการที่แสดงไว้ในงบการเงินให้ถือว่าครบถ้วนและถูกต้อง เว้นแต่ผู้สอบบัญชีจะรายงานไว้เป็นอย่างอื่นในรายงานการสอบบัญชี

4) รายงานควรระบุความเห็นเกี่ยวกับงบการเงิน ไม่ว่าโดยส่วนรวมหรือโดยระบุส่วนที่ไม่อาจให้ความเห็นได้ ทั้งนี้หากความเห็นโดยส่วนรวมไม่อาจระบุได้ ผู้สอบบัญชีจะต้องระบุเหตุผลไว้ เพราะการรับรองงบการเงินนั้นหมายถึงสิ่งที่แสดงงานการตรวจสอบและความรับผิดชอบของผู้สอบบัญชี

การใช้คอมพิวเตอร์ในการประมวลผลไม่มีผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติ ตามมาตรฐานทั่วไปและมาตรฐานการรายงาน ตัวอย่างเช่น มาตรฐานทั่วไปข้อแรกต้องการให้ผู้สอบบัญชีได้รับการอบรม และได้รับความชำนาญ ซึ่งผู้ตรวจสอบด้านอื่นไม่มี แต่วิธีการที่จะทำให้ได้รับความชำนาญดังกล่าว ซึ่งก็คือการศึกษาและประสบการณ์ในวิชาชีพไม่ได้เปลี่ยนแปลงไป แม้ว่าการศึกษาและประสบการณ์ของผู้สอบบัญชีด้านคอมพิวเตอร์จะแตกต่างกันออกไป ผู้สอบบัญชีทั้งหมดก็จะพัฒนาความชำนาญของเขาด้วยวิธีการศึกษาและการทำงาน อย่างไรก็ตามเมื่อเราตรวจสอบตามมาตรฐานการปฏิบัติงาน สิ่งที่เกิดขึ้นคือ กระบวนการที่สำคัญ ๆ จะมีการเปลี่ยนแปลงไป ในกรณีของมาตรฐานการปฏิบัติงานข้อ 2 ที่ต้องศึกษาและประเมินประสิทธิภาพการควบคุมภายในนั้น ตาม SAS (Statements on Auditing Standards) ฉบับที่ 3 ผู้สอบบัญชีด้านคอมพิวเตอร์ต้องประเมินประสิทธิภาพการควบคุมต่าง ๆ

เนื้อหาสาระในบทความนี้จะกล่าวถึงเรื่องต่าง ๆ ดังนี้

1. มาตรฐานการปฏิบัติงานตรวจสอบ
2. แนวความคิดในประเด็นที่เกี่ยวข้องกับผู้สอบบัญชีด้านคอมพิวเตอร์
3. เรื่องทั่วไปเกี่ยวกับการศึกษาและการประเมินประสิทธิภาพการควบคุมภายในของผู้สอบบัญชี
4. ผลกระทบจากการประมวลผลข้อมูลโดยใช้คอมพิวเตอร์ต่อการศึกษาและการประเมินประสิทธิภาพการควบคุมภายใน และ
5. การเก็บรวบรวมหลักฐานให้ได้เพียงพอ และแนวความคิดในเรื่องบทบาทของคอมพิวเตอร์ในการทดสอบความถูกต้องของยอดคงเหลือ (substantive testing)

สิ่งที่เน้นในบทความนี้คือ การเปลี่ยนแปลงที่เกิดจากระบบที่ประมวลผลข้อมูลโดยใช้คอมพิวเตอร์เปรียบเทียบกับระบบที่ทำด้วยมือหรือระบบเครื่องจักรลงบัญชี การเปลี่ยนแปลงเหล่านี้เป็นเรื่องที่เกี่ยวกับการควบคุมทางบัญชี ร่องรอยการตรวจสอบ และแผนการตรวจสอบ

1. มาตรฐานการปฏิบัติงาน (Standards of field work)

มาตรฐานการปฏิบัติงาน 3 ข้อตามที่ได้กล่าวมาแล้ว เป็นแนวทางให้ผู้สอบบัญชีใช้ในการปฏิบัติงานด้านการตรวจสอบกรณีมีการเปลี่ยนแปลงที่สำคัญในวิธีการตรวจสอบ อันเป็นผลจากการนำคอมพิวเตอร์มาใช้งาน

ลักษณะของการวางแผนการตรวจสอบ และการควบคุมดูแลผู้ช่วยการปฏิบัติงานตามมาตรฐานในข้อแรกกลายเป็นเรื่องที่มีความยุ่งยากมากขึ้นเมื่อมีคอมพิวเตอร์เข้ามาเกี่ยวข้อง ในการวางแผนการตรวจสอบทั้งหมดและกำหนดขอบเขตการตรวจสอบ ผู้สอบบัญชีต้องทำการประเมินประสิทธิภาพและทดสอบด้าน general controls 5 ประเภท และ application controls 3 ประเภท ซึ่งไม่พบในระบบที่ทำด้วยมือหรือระบบเครื่องจักรลงบัญชีการควบคุมดูแลผู้ช่วยปฏิบัติงานมีความยากมากขึ้น เพราะนอกเหนือจากงานโดยตรงทางด้านบัญชีและทางการตรวจสอบผู้ควบคุมอาจต้องดูแลงานที่ประมวลผลด้วยคอมพิวเตอร์ซึ่งมีความสลับซับซ้อนมากมาย

แม้ว่าวิธีที่ทำให้มาตรฐานการปฏิบัติงานสำเร็จลงได้จะประสบความยุ่งยากเมื่อนำ คอมพิวเตอร์เข้ามาใช้เราก็ไม่ต้องเกี่ยวข้องกับวิธีการเหล่านี้มากเกินไป กระบวนการที่ก่อให้เกิดความชำนาญในเรื่องการวางแผนการตรวจสอบและการควบคุมดูแลของผู้สอบบัญชีด้านคอมพิวเตอร์ไม่ได้แตกต่างกันนักในสาระสำคัญกับระบบที่ทำด้วยมือและระบบเครื่องจักรลงบัญชี ซึ่งเป็นเรื่องเกี่ยวกับการศึกษาและประสบการณ์ในวิชาชีพ เพียงแต่การควบคุมดูแลการตรวจสอบด้านคอมพิวเตอร์จำเป็นต้องอาศัยสิ่งที่กล่าวทั้งสองมากขึ้นเท่านั้น

ตามมาตรฐานการปฏิบัติงานข้อ 2 นั้น ผู้สอบบัญชีต้องศึกษาและประเมินประสิทธิภาพการควบคุมภายใน เพราะการนำคอมพิวเตอร์มาใช้ทำให้เกิดความเปลี่ยนแปลงมากมายในการวางแผนการตรวจสอบ ทั้งเรื่องการศึกษาและการประเมินประสิทธิภาพการควบคุมภายใน

การเก็บรวบรวมหลักฐานเพื่อให้ได้มาอย่างเพียงพอตามมาตรฐานการปฏิบัติงานข้อ 3 มีผลกระทบต่อผู้สอบบัญชีด้านคอมพิวเตอร์ 2 เรื่อง คือ ประเภทของหลักฐาน และวิถีทางที่จะได้หลักฐานนั้นมา ประเภทของหลักฐานที่อาจเปลี่ยนแปลงไป เช่น เอกสารเบื้องต้นจะไม่มี แต่มีการใช้เทปแม่เหล็ก (magnetic tape) แทนสมุดรายวันและสมุดแยกประเภท วิถีทางที่จะได้หลักฐานอาจเปลี่ยนแปลงไป เพราะผู้สอบบัญชีอาจต้องใช้คอมพิวเตอร์และโปรแกรมแทนระบบที่ทำด้วยมือหรือระบบเครื่องจักรลงบัญชี

2. แนวความคิดในการตรวจสอบ (Auditing concepts)

มาตรฐานการตรวจสอบให้แนวทางปฏิบัติในการตรวจสอบ ความหมายอย่างกว้าง ๆ ข้อหนึ่งของการตรวจสอบและกระบวนการตรวจสอบ ซึ่งจัดทำโดย American Accounting Association Committee เรื่องแนวความคิดพื้นฐานในการตรวจสอบ (Basic Auditing Concepts - 1971) ระบุว่า ในการปฏิบัติงานผู้สอบบัญชีต้องทำการทดสอบการปฏิบัติตามระบบ (compliance test) และการทดสอบความถูกต้องของยอดคงเหลือ (substantive test) ในการทดสอบทั้ง 2 ชนิดยังคงกระทำอยู่ แต่จะยุ่งยากมากขึ้นเมื่อทำการตรวจสอบด้านคอมพิวเตอร์

2.1 ความหมายอย่างกว้าง ๆ ของการตรวจสอบ (Comprehensive definition of auditing)

สมาคมการบัญชีของสหรัฐอเมริกา หรือ AAA (American Accounting Association) ได้ให้คำจำกัดความคำว่า "การสอบบัญชี" (auditing) ไว้อย่างกว้าง ๆ ครอบคลุมถึงการตรวจสอบภายนอก การตรวจสอบภายใน และการตรวจสอบด้านคอมพิวเตอร์ ดังนี้

การสอบบัญชี คือ กระบวนการปฏิบัติงานที่เป็นระบบ โดยมีวัตถุประสงค์เพื่อให้ได้มาซึ่งหลักฐาน และประเมินหลักฐานในเรื่องเกี่ยวกับธุรกรรมทางการเงิน และเหตุการณ์ต่าง ๆ เพื่อให้ทราบถึงระดับความสอดคล้องกันของหลักฐานที่ตรวจสอบและขอบเขตที่กำหนด และรายงานผลให้ผู้ใช้ประโยชน์ทราบ

แนวความคิดหลาย ๆ แนวในคำจำกัดความข้างต้นนี้ จะอภิปรายในส่วนที่เกี่ยวกับการตรวจสอบด้านคอมพิวเตอร์ ดังนี้

- กระบวนการปฏิบัติงานที่เป็นระบบ (systematic process) มีความหมายว่า การสอบบัญชีมีลักษณะเป็นธุรกรรมที่มีความเคลื่อนไหวในลักษณะที่เป็นเหตุเป็นผลต่อกัน เป็นวิธีการที่สำคัญที่ใช้ในการตรวจสอบระบบทุกระบบ โดยเฉพาะอย่างยิ่งการตรวจสอบระบบคอมพิวเตอร์ ซึ่งไม่สามารถมองเห็นขั้นตอนการประมวลผลและเนื้อหาต่าง ๆ ในแฟ้มข้อมูล วิธีที่เป็นไปตามบุญตามกรรม ไม่มีการวางแผนและไม่มีระบบ ในการตรวจสอบด้านคอมพิวเตอร์นั้นอาจเป็นผลทำให้มีการผ่านหรือข้ามส่วนที่สำคัญในการประมวลผล หรือแฟ้มข้อมูลไปได้

- การได้มาซึ่งหลักฐานและการประเมินหลักฐาน (obtaining and evaluating evidence) ผู้สอบบัญชีด้านคอมพิวเตอร์ต้องเกี่ยวข้องกับความน่าเชื่อถือของระบบการควบคุมภายใน และเนื้อหาในแฟ้มข้อมูลที่สร้างขึ้นโดยใช้คอมพิวเตอร์ในการประมวลผล การเก็บรวบรวมหลักฐานจะกระทำในขณะที่ทดสอบการปฏิบัติตามระบบเพื่อกำหนดว่ามีการปฏิบัติตามระบบการควบคุมภายในที่กำหนดไว้หรือไม่ และทดสอบความถูกต้องของยอดคงเหลือเพื่อกำหนดว่าเนื้อหาในแฟ้มข้อมูลมีความเหมาะสมหรือไม่ เพียงใด

- เพื่อให้ทราบถึงความสอดคล้องกันของหลักฐานที่ตรวจสอบ และขอบเขตที่กำหนด กระบวนการในกรณีนี้คล้ายคลึงกับระบบการลงบัญชีที่ทำด้วยมือและระบบเครื่องจักรลงบัญชี ระดับความสอดคล้องเป็นการตัดสินใจโดยตัวผู้สอบบัญชีเองในลักษณะ subjective เพื่อที่จะดูว่าการไม่ปฏิบัติตามระบบการควบคุมภายในมีนัยสำคัญหรือไม่ หรือการที่ยอดคงเหลือผิดพลาดมีนัยสำคัญหรือไม่ ระบบการควบคุมภายในจะมีความสลับซับซ้อนมากขึ้น ทำให้เป็นการยากที่จะแน่ใจว่าโปรแกรมคอมพิวเตอร์และแฟ้มข้อมูลที่จัดทำให้ผู้สอบบัญชีตรวจสอบนั้นเป็นของจริงหรือสำเนาปลอมที่ไม่ได้ใช้แล้วในการประมวลผล

- การรายงานผล (communicating results) กรณีนี้เช่นเดียวกับผู้สอบบัญชีอื่น ๆ ทั้งหมดที่จะต้องรายงานผลให้กับผู้ใช้งานที่มีความสนใจทราบ ซึ่งบุคคลที่กล่าวนี้หมายความรวมถึงสมาชิกคนอื่น ๆ ในทีมตรวจสอบที่จะต้องรวบรวมประเด็นปัญหาที่ผู้สอบบัญชี ด้านคอมพิวเตอร์ตรวจสอบ และลูกค้า การรายงานผลจะมีความยุ่งยากซับซ้อน เพราะว่าในการประเมินความน่าเชื่อถือของระบบการควบคุมภายในด้านคอมพิวเตอร์ และความถูกต้องของยอดคงเหลือ ต้องนำไปพิจารณารวมกับการประเมินความน่าเชื่อถือของระบบการควบคุมภายในทั้งหมด ไม่ว่าจะเป็นระบบที่ลงบัญชีด้วยมือหรือระบบเครื่องจักรลงบัญชี

2.2 การทดสอบการปฏิบัติตามระบบและความถูกต้องของยอดเงินคงเหลือ (Compliance and substantive testing)

ผู้สอบบัญชีจะต้องศึกษาและประเมินประสิทธิภาพของระบบการควบคุมภายใน เมื่อผู้สอบบัญชีพบจุดแข็งของระบบการควบคุมภายในที่จุดใดก็ตาม ผู้สอบบัญชีจะต้องทดสอบการปฏิบัติว่าเป็นไปตามระบบที่ได้กำหนดไว้หรือไม่ ถ้ามีการปฏิบัติตามแล้ว ผู้สอบบัญชีอาจจะสามารถลดขอบเขตของกระบวนการตรวจสอบลงได้ และเมื่อผู้สอบบัญชีพบจุดอ่อนในระบบ หรือไม่มีการปฏิบัติตามระบบที่กำหนดไว้ หรือไม่เชื่อมั่นจุดแข็งของระบบที่มีอยู่แล้ว ผู้สอบบัญชีจะต้องเพิ่มขอบเขตของกระบวนการตรวจสอบให้มากขึ้น

หลังจากที่ผู้สอบบัญชีศึกษาและประเมินประสิทธิภาพการควบคุมภายในเสร็จสมบูรณ์แล้ว ผู้สอบบัญชีจะต้องกระทำในส่วนที่ 2 ที่เรียกว่า การทดสอบความถูกต้องของยอดคงเหลือ หรือ substantive tests ซึ่งมีอยู่ 2 เรื่อง คือ

1) ทดสอบรายละเอียดของรายการและยอดคงเหลือ
2) สอบทานเชิงวิเคราะห์เกี่ยวกับข้อมูลทางการเงิน

ในการทดสอบรายละเอียดของรายการนั้น ผู้สอบบัญชีด้านคอมพิวเตอร์จะต้องกำหนดว่าโปรแกรมคอมพิวเตอร์สามารถประมวลผลได้อย่างเหมาะสม การทดสอบยอดคงเหลือในบัญชีนั้น ผู้สอบบัญชีด้านคอมพิวเตอร์จะต้องตรวจสอบเนื้อหาในแฟ้มข้อมูลหลัก (master files) และแฟ้มรายการ (transaction files) ที่ผ่านการประมวลผลด้วยคอมพิวเตอร์แล้ว รูปแบบที่สองของ substantive test ก็คือ การสอบทานเชิงวิเคราะห์เกี่ยวกับข้อมูลทางการเงิน ซึ่งสามารถกระทำได้อย่างมีประสิทธิภาพโดยใช้เครื่องคอมพิวเตอร์และเป็นเรื่องเกี่ยวกับการวิเคราะห์อัตราส่วนและแนวโน้มโดยการคำนวณเป็นร้อยละ สำหรับข้อมูลสถิติได้เป็นปริมาณจำนวนมาก ๆ และรวดเร็วกว่าการกระทำโดยบุคคลมาก

2.3 ผลกระทบของคอมพิวเตอร์ต่อกระบวนการสอบบัญชี (Effect of computer on the audit process)

กระบวนการสอบบัญชีทั้งระบบการลงบัญชีที่ทำด้วยมือ ระบบเครื่องจักรของบัญชี และระบบคอมพิวเตอร์ จะคล้าย ๆ กัน เพราะผู้สอบบัญชีจะต้องทดสอบการปฏิบัติตามระบบ (compliance test) ทดสอบความถูกต้องของยอดเงินคงเหลือ (substantive test) และการทดสอบทั้ง 2 สถานะ (dual-purpose) ทั้ง 3 ระบบ ถึงแม้ว่าตามหลักการจะต้องทดสอบการปฏิบัติตามระบบก่อน แล้วจึงทดสอบยอดคงเหลือก็ตาม แต่ในทางปฏิบัติแล้วผู้สอบบัญชีมักจะรวมการทดสอบทั้ง 2 ประเภทเข้าด้วยกัน เรียกว่า dual- purpose tests ตัวอย่างเช่น การทดสอบเพื่อให้แน่ใจว่าการควบคุมการประมวลผลนั้นมีการถือปฏิบัติตามระบบที่กำหนดไว้แล้ว อาจจะมีการคำนวณยอดคงเหลือในบัญชี (ซึ่งเป็นขั้นตอนการ substantive test) ว่าถูกต้องหรือไม่พร้อมกันไปด้วย

ความแตกต่างระหว่างการสอบบัญชีด้านคอมพิวเตอร์และด้านอื่น ๆ อยู่ที่มาตรฐานและกระบวนการต่าง ๆ ที่ใช้กับการสอบบัญชีด้านคอมพิวเตอร์ ในเรื่องมาตรฐานที่เพิ่มขึ้นในการสอบบัญชีด้านคอมพิวเตอร์จะกล่าวถึงในลำดับต่อไป ส่วนกระบวนการต่าง ๆ ในการตรวจสอบด้านคอมพิวเตอร์ที่เพิ่มขึ้นนั้นมีเทคนิคดังต่อไปนี้

1) การตรวจสอบภายนอกคอมพิวเตอร์ (auditing around computer) โดยเน้นถึงข้อมูลนำเข้าและผลลัพธ์ที่ได้จากคอมพิวเตอร์
2) การตรวจสอบผ่านเข้าไปในคอมพิวเตอร์ (auditing through the computer) โดยการทดสอบการปฏิบัติงานของโปรแกรมของคอมพิวเตอร์
3) การตรวจสอบด้วยคอมพิวเตอร์ (auditing with the computer) โดยใช้คอมพิวเตอร์ในการวิเคราะห์เนื้อหาที่อยู่ในแฟ้มข้อมูล

3. การศึกษาและประเมินประสิทธิภาพการควบคุมภายในของผู้สอบบัญชี (The auditor's study and evaluation of internal control)

การศึกษาและประเมินประสิทธิภาพการควบคุมภายในของผู้สอบบัญชีด้านคอมพิวเตอร์ต้องดำเนินการตามหลักการขั้นพื้นฐานในเรื่องการควบคุมภายในที่ใช้กับทุกระบบดังนั้นผู้ตรวจสอบจะต้องปฏิบัติตามหลักการพื้นฐานเหล่านี้ ซึ่งล้วนเกี่ยวข้องกับจุดมุ่งหมายของการศึกษาระบบการควบคุมภายในและการประเมินประสิทธิภาพของการควบคุมคำจำกัดความและแนวความคิดขั้นพื้นฐาน การศึกษาระบบ และการประเมินประสิทธิภาพของระบบ รวมตลอดถึงความสัมพันธ์ของการศึกษาและการประเมินประสิทธิภาพการควบคุมภายในของระบบดังกล่าว กับกระบวนการสอบบัญชีในแนวอื่น ๆ

3.1 จุดมุ่งหมายของการศึกษาและประเมินประสิทธิภาพการควบคุมภายใน (Purpose of internal control study and evaluation)

จุดมุ่งหมายดังกล่าวมีอยู่ 2 ประการ คือ

1) เพื่อตัดสินใจว่าผู้สอบบัญชีสามารถเชื่อมั่นระบบดังกล่าวได้ในขอบเขตเพียงใด หรือกล่าวอีกนัยหนึ่งก็คือ เพื่อที่จะกำหนดลักษณะ ขอบเขต และเวลาการทดสอบที่จะใช้ในการตรวจสอบงบการเงิน
2) เพื่อใช้ในการวางแผนกระบวนการตรวจสอบ

3.2 คำจำกัดความและแนวความคิดขั้นพื้นฐานของการควบคุมภายใน (Definitions and basic concepts of internal control)

คำจำกัดความและแนวความคิดขั้นพื้นฐานมีมากมายที่เกี่ยวข้องกับการควบคุมภายใน ซึ่งจะพบในการศึกษาและประเมินประสิทธิภาพของระบบทุกระบบที่ใช้ในการประมวลผลข้อมูลทางบัญชี ซึ่งรวมถึงคำจำกัดความของคำว่า ระบบการควบคุมภายใน (internal control system) การควบคุมด้านบริหาร (administrative control) การควบคุมด้านบัญชี (accounting control) และแนวความคิดขั้นพื้นฐานที่เกี่ยวข้องกับการควบคุมภายในด้านบัญชี

1) **การควบคุมภายใน**

การควบคุมภายในสามารถให้คำจำกัดความอย่างง่าย ๆ ว่า เป็นวิธีการที่จะใช้ค้นหาข้อผิดพลาดที่เกิดในข้อมูลทางบัญชีและแก้ไขให้ถูกต้อง หรือเพื่อให้เข้าใจง่ายขึ้น อาจกล่าวว่าการควบคุมภายในประกอบด้วยแผนการจัดแบ่งส่วนงาน วิธีการและกระบวนการต่าง ๆ ที่ธุรกิจนำมาใช้ปฏิบัติเพื่อป้องกันทรัพย์สิน เพื่อตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลทางบัญชี ส่งเสริมให้เกิดประสิทธิภาพในการทำงาน และกระตุ้นให้มีการปฏิบัติตามนโยบายที่กำหนด

2) **การควบคุมด้านบริหารและการควบคุมด้านบัญชี**

ระบบการควบคุมภายในประกอบด้วย การควบคุมทั้งในส่วนที่เกี่ยวกับด้านบริหารงานและด้านการบัญชี การควบคุมด้านบริหารงานรวมถึงแผนการจัดแบ่งส่วนงาน วิธีการและกระบวนการต่าง ๆ ที่จะส่งเสริมให้เกิดประสิทธิภาพในการทำงาน และกระตุ้นให้มีการปฏิบัติตามนโยบายที่กำหนด ส่วนการควบคุมด้านบัญชีนั้นรวมถึงแผนการจัดแบ่งส่วนงาน วิธีการและกระบวนการต่าง ๆ ที่นำมาใช้ปฏิบัติเพื่อป้องกันรักษาทรัพย์สิน เพื่อตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลทางบัญชี ผู้สอบบัญชีจะเกี่ยวข้องกับการควบคุมด้านบัญชีเป็นอันดับแรก เพราะการควบคุมในลักษณะนี้เป็นวิธีการพื้นฐานที่จะดูว่าข้อผิดพลาดจากข้อมูลทางบัญชีมีการป้องกันและแก้ไขให้ถูกต้องแล้ว

3) **แนวความคิดขั้นพื้นฐานของการควบคุมภายในทางด้านบัญชี**

แนวความคิดขั้นพื้นฐานดังกล่าวสามารถแบ่งออกได้เป็น 2 ประเภท คือ แนวความคิดทั่วไป (general concepts) และลักษณะพิเศษที่สำคัญ (essential characteristics) ทั้งนี้โดยประเภทแรกอาจสรุปได้ว่าเป็นสภาพแวดล้อมที่มีการควบคุมในทางบัญชี ส่วนประเภทหลังเป็นคุณสมบัติที่จำเป็นต้องมีอยู่ในระบบที่ดี

แนวความคิดทั่วไปของการควบคุมทางบัญชี รวมถึงความรับผิดชอบของฝ่ายบริหาร ความเชื่อมั่นที่มีเหตุมีผล วิธีการประมวลผลข้อมูล และข้อจำกัดที่มีอยู่ ฝ่ายบริหารต้องรับผิดชอบในการกำหนดและดูแลระบบการควบคุมภายใน รวมทั้งการติดตามสอดส่องดูว่าหน้าที่ต่าง ๆ นั้นได้มีการถือปฏิบัติตามที่กำหนดไว้ ผู้สอบบัญชีอาจจะแนะนำการเปลี่ยนแปลงในระบบบางอย่างเมื่อเห็นว่าเหมาะสม และเป็นความรับผิดชอบของฝ่ายบริหารที่จะนำเอาข้อแนะนำไปปฏิบัติ ระบบการควบคุมภายในจะก่อให้เกิดความเชื่อมั่นที่มีเหตุมีผล แต่ไม่สมบูรณ์ทั้งหมด โดยมีวัตถุประสงค์เพื่อป้องกันและแก้ไขข้อผิดพลาดที่พบ ยิ่งกว่านั้นต้นทุนของการควบคุมภายในควรจะต่ำกว่าผลประโยชน์ที่ได้รับ วิธีการประมวลผลข้อมูลจะเป็นตัวกำหนดการควบคุมด้านบัญชีในแต่ละส่วนงาน ถึงแม้ว่าวัตถุประสงค์ของระบบการควบคุมภายในจะเป็นอิสระจากวิธีการประมวลผลข้อมูลก็ตาม การจัดองค์กรและกระบวนการต่าง ๆ ที่จะทำให้บรรลุวัตถุประสงค์ดังกล่าวอาจจะมีผลมาจากวิธีการประมวลผลข้อมูลที่ใช้อยู่ ข้อบกพร่องที่มีอยู่ในระบบการควบคุมภายในนั้น เนื่องมาจากคน เพราะคนจะต้องมีความเหนื่อยล้า ทำผิดพลาด และไม่เข้าใจว่าพวกเขาจะต้องทำอะไร นอกจากนี้ในกรณีที่มีบุคคลบางคนมีเจตนาและสมรู้ร่วมคิดกันที่จะไม่ทำตามระบบการควบคุมแล้ว ก็จะหาวิธีป้องกันได้ลำบากมากขึ้น

ลักษณะพิเศษที่สำคัญของการควบคุมภายในทางบัญชี ซึ่งจะปรากฏให้เห็นได้ในระบบที่ดีในองค์การทั่วไป ดังนี้

- คุณภาพของบุคลากร : เป็นเรื่องที่เกี่ยวกับระบบการควบคุมภายในที่จะต้องป้องกันความประมาทเลินเล่อ ความผิดพลาด และความเข้าใจที่ไม่ถูกต้องของพนักงานที่ได้เกิดขึ้น
- การแบ่งแยกหน้าที่ : เป็นการป้องกันบุคคลไม่ให้นำทรัพย์สินไปใช้โดยมีการปกปิดรายการทุจริต หรือการยักยอกด้วยการบันทึกรายการที่ไม่ถูกต้อง
- รายการที่เกิดขึ้นต้องมีการอนุมัติ : แนวความคิดในเรื่องนี้เป็นระบบการควบคุมภายในที่ป้องกันไม่ให้พนักงานกระทำการที่เกินอำนาจหน้าที่ของตน
- รายการที่เกิดขึ้นจะต้องมีการบันทึกไว้อย่างเหมาะสม : กล่าวคือ จะต้องบันทึกด้วยจำนวนที่เหมาะสม ป้องกันการบันทึกรายการที่ไม่ถูกต้อง
- การนำทรัพย์สินไปใช้ : จะต้องมีการควบคุมเพื่อไม่ให้มีการขโมยทรัพย์สิน
- ตรวจนับทรัพย์สินที่มีอยู่จริงเปรียบเทียบกับที่บันทึกไว้ในบัญชี : กรณีนี้เป็นเรื่องที่มีความจำเป็น เช่น การตรวจนับสินค้าคงคลัง เพื่อที่จะกำหนดว่าระบบดังกล่าวมีความเหมาะสมหรือไม่ เพียงใด

3.3 การศึกษาระบบการควบคุมภายใน (Study of the internal control system)

จุดมุ่งหมายของการศึกษาระบบการควบคุมภายใน ก็เพื่อให้มีความรู้และความเข้าใจในกระบวนการและวิธีการต่าง ๆ ที่กำหนดไว้ รวมทั้งให้เกิดความเชื่อมั่นว่ากระบวนการและวิธีการต่าง ๆ ดังกล่าวมีการใช้งานและปฏิบัติในลักษณะเป็นไปตามแผนที่กำหนดไว้ จุดมุ่งหมายทั้ง 2 ประการดังกล่าวจะสามารถบรรลุผลสำเร็จได้ จะต้องมีการศึกษาระบบใน 2 ส่วน คือ การสอบทานระบบที่เป็นอยู่ และการทดสอบการปฏิบัติตามระบบนั้น ภายหลังจากที่มีความรู้และเข้าใจในขั้นตอนของการสอบทานระบบว่า ระบบการควบคุมภายในควรมีหน้าที่อย่างไร แล้วผู้สอบบัญชีจะต้องทดสอบการปฏิบัติตามระบบว่า ระบบดังกล่าวในทางปฏิบัติทำหน้าที่อย่างไร

3.4 การประเมินประสิทธิภาพของระบบการควบคุมภายใน (Evaluation of the internal control system)

จุดมุ่งหมายของการประเมินประสิทธิภาพของระบบการควบคุมภายใน คือ ต้องกำหนดขอบเขตว่า ระบบดังกล่าวป้องกันข้อผิดพลาดและสิ่งผิดปกติในงบการเงินในส่วนที่มีนัยสำคัญได้เพียงใด มีขั้นตอนอยู่หลายขั้นตอนในการประเมินดังกล่าว คือ

1) ผู้สอบบัญชีต้องกำหนดประเภทของข้อผิดพลาดและสิ่งผิดปกติที่สามารถเกิดขึ้นได้
2) จะต้องระบุถึงกระบวนการควบคุมด้านบัญชีที่ใช้ป้องกันข้อผิดพลาดและสิ่งผิดปกติที่เกิดขึ้น
3) ผู้สอบบัญชีต้องกำหนดว่ามีกระบวนการควบคุมด้านบัญชีที่จำเป็นอยู่ในระบบ และน่าพอใจหรือไม่
4) จุดอ่อนของระบบที่มีสาเหตุจากการขาดกระบวนการควบคุมที่จะใช้ในการป้องกันข้อผิดพลาดและสิ่งผิดปกติที่อาจจะเกิดขึ้นนั้น จะต้องมีการประเมินถึงผลที่จะกระทบต่อลักษณะ เวลา และขอบเขตของกระบวนการตรวจสอบที่จะต้องกระทำในลำดับต่อไป และต้องมีข้อแนะนำเพื่อปรับปรุงระบบดังกล่าวให้ลูกค้าด้วย

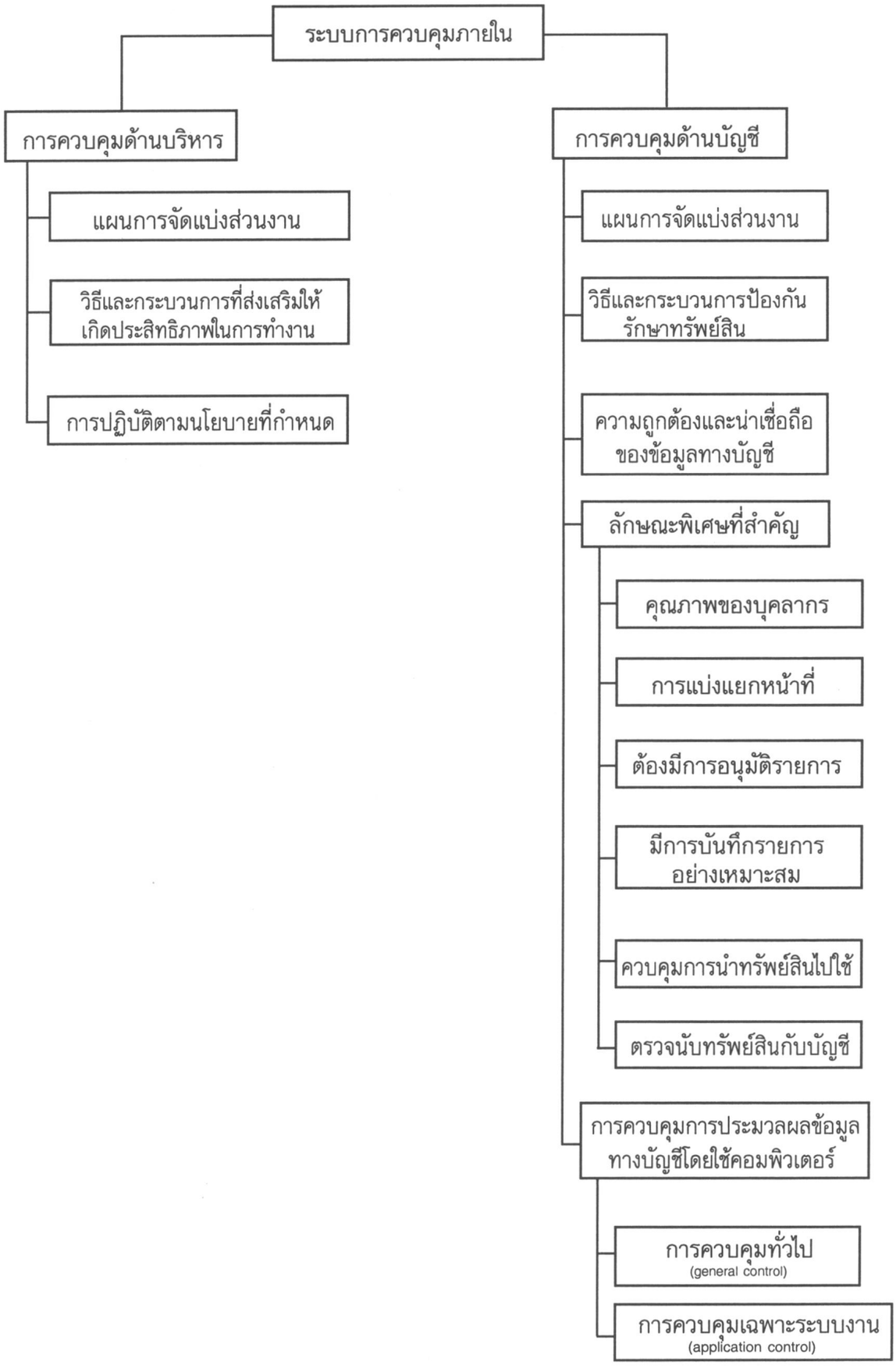
3.4 ความสัมพันธ์ของการศึกษาและการประเมินประสิทธิภาพของระบบการควบคุมภายในกับกระบวนการสอบบัญชีอื่นๆ (Relationship of study and evaluation to other auditing procedures)

การศึกษาและการประเมินประสิทธิภาพการควบคุมภายในที่ระบุไว้ใน มาตรฐานการปฏิบัติงานข้อที่สองนั้น เกี่ยวข้องกับการได้มาซึ่งหลักฐานที่เพียงพอในมาตรฐานดังกล่าวในข้อที่สามที่ว่า การทดสอบความถูกต้องของยอดคงเหลือที่ผู้สอบบัญชีจะกระทำเพื่อให้เป็นไปตามมาตรฐานการปฏิบัติงานนั้น ขึ้นอยู่กับผลของการศึกษาและประเมินประสิทธิภาพการควบคุมภายใน ขอบเขตของการทดสอบความถูกต้องของยอดคงเหลือ สามารถจำกัดให้แคบลงได้ถ้าผู้สอบบัญชีสรุปได้ว่า ระบบการควบคุมภายในน่าเชื่อถือ ในทางตรงกันข้ามถ้าระบบการควบคุมภายในไม่น่าเชื่อถือแล้ว ขอบเขตของการทดสอบอาจจะต้องมีการขยายเพิ่มขึ้นมาก

4. ผลของการประมวลผลโดยใช้คอมพิวเตอร์ต่อการศึกษาและประเมินประสิทธิภาพการควบคุมภายใน (The effects of EDP on the auditor's study and evaluation of internal control)

นอกเหนือไปจากความต้องการโดยทั่วไปในการศึกษาและประเมินประสิทธิภาพการควบคุมภายในทุกระบบของการประมวลผลข้อมูลทางบัญชีนั้น ผู้สอบบัญชียังต้องศึกษาและประเมินการควบคุมอีกมากมายหลายประเภทที่เกี่ยวข้องกับการประมวลผลโดยใช้คอมพิวเตอร์อีกด้วย การควบคุมเกี่ยวกับคอมพิวเตอร์นั้นแบ่งออกเป็น general control และ application control ซึ่งมีความจำเป็นมาก ลำดับขั้นของการควบคุมระบบการประมวลผลโดยใช้คอมพิวเตอร์แสดงให้เห็นดังรูป




ระบบการควบคุมภายใน
การควบคุมด้านบริหาร
แผนการจัดแบ่งส่วนงาน
วิธีและกระบวนการที่ส่งเสริมให้เกิดประสิทธิภาพในการทำงาน
การปฏิบัติตามนโยบายที่กำหนด
การควบคุมด้านบัญชี
แผนการจัดแบ่งส่วนงาน
วิธีและกระบวนการป้องกันรักษาทรัพย์สิน
ความถูกต้องและน่าเชื่อถือของข้อมูลทางบัญชี
ลักษณะพิเศษที่สำคัญ
คุณภาพของบุคลากร
การแบ่งแยกหน้าที่
ต้องมีการอนุมัติรายการ
มีการบันทึกรายการอย่างเหมาะสม
ควบคุมการนำทรัพย์สินไปใช้
ตรวจนับทรัพย์สินกับบัญชี
การควบคุมการประมวลผลข้อมูลทางบัญชีโดยใช้คอมพิวเตอร์
การควบคุมทั่วไป
(general control)
การควบคุมเฉพาะระบบงาน
(application control)

4.1 ผลของการประมวลผลโดยใช้คอมพิวเตอร์ต่อการควบคุมด้านบัญชี (Effects of EDP on accounting control)

การประมวลผลโดยใช้คอมพิวเตอร์มีผลต่อการประมวลผลข้อมูลทางบัญชีอย่างมากมาย ก่อให้เกิดการเปลี่ยนแปลงระบบบัญชี การเปลี่ยนแปลงเหล่านี้ล้วนมีผลกระทบต่อการควบคุมภายในด้านบัญชี และในที่สุดมีผลต่อร่องรอยการตรวจสอบ (audit trail)

การนำเอาคอมพิวเตอร์มาใช้ในระบบบัญชี ก่อให้เกิดการเปลี่ยนแปลงในระบบอย่างมากมาย ดังตัวอย่างต่อไปนี้

1) ธุรกรรมต่าง ๆ ที่มีการกระจายไปให้กันเสมือนหลาย ๆ คนทำงาน อาจจะรวมอยู่ที่คน ๆ เดียว ทำให้การควบคุมภายในเรื่องการแบ่งแยกหน้าที่กระทำไม่ได้ ตัวอย่างเช่น เรื่องเงินเดือน อาจจะทำโดยพนักงานหลายคน เริ่มตั้งแต่การคำนวณเงินเดือนเบื้องต้นตามชั่วโมงที่ทำงาน คูณด้วยอัตราที่ต้องจ่าย คำนวณภาษีหัก ณ ที่จ่าย และรายการหักอื่น ๆ เขียนเช็คเพื่อจ่ายเงินเดือน ผ่านรายการจ่ายดังกล่าวไปยังสมุดบันทึกข้อมูลเกี่ยวกับรายได้ของพนักงาน และสอบทานธุรกรรมด้านต่าง ๆ เหล่านี้

2) การติดตั้งคอมพิวเตอร์มากๆ ก่อให้เกิดปัญหาที่สำคัญในเรื่องขาดเอกสาร เอกสารไม่เพียงพอ กล่าวคือ ผู้สอบบัญชีจะขาดร่องรอยการตรวจสอบ และเป็นการยากที่จะติดตามกระบวนการต่าง ๆ ในแต่ละส่วนได้

3) ผู้สอบบัญชีต้องอาศัยคอมพิวเตอร์และโปรแกรมในการแสดงขั้นตอนการประมวลผลและข้อมูลที่เกี่ยวข้อง ทั้งนี้เนื่องจากกระบวนการในการประมวลผลหรือโปรแกรม และข้อมูลที่จะทำการประมวลผลนั้นจะเก็บอยู่ในรูปของภาษาที่เครื่องสามารถอ่านได้

4) ถึงแม้ว่าในองค์กรต่าง ๆ เป็นจำนวนมากจะว่าจ้างพนักงานเพิ่มขึ้นเมื่อมีการติดตั้งเครื่องคอมพิวเตอร์ก็ตาม แต่พนักงานเหล่านั้นจะเกี่ยวข้องกับการประมวลผลข้อมูลทางบัญชีน้อยลงไป เมื่อเป็นเช่นนี้แล้วทำให้การตรวจสอบเพื่อป้องกันความผิดพลาดของข้อมูลที่อาจจะเกิดขึ้นในระหว่างการประมวลผลกระทำไม่ได้เนื่องจากไม่สามารถมองเห็นได้

5) ในการประมวลผลโดยใช้คอมพิวเตอร์นั้น จะพบข้อผิดพลาดที่เป็นระบบ (systematic errors) ซึ่งมีสาเหตุมาจากรายการที่คล้ายคลึงกันในโปรแกรมเดียวกัน หรือเกิดจากข้อบกพร่องของระบบเอง

6) ในส่วนงานที่ทำหน้าที่ประมวลผลโดยใช้คอมพิวเตอร์นั้น ล้วนแต่เป็นพนักงานที่มีความเชี่ยวชาญทางด้านคอมพิวเตอร์ ดังนั้นผู้สอบบัญชีต้องอาศัยผู้เชี่ยวชาญด้านดังกล่าวในการตรวจสอบขั้นตอนในการประมวลผลของพนักงานในส่วนงานดังกล่าว

7) การควบคุมด้านบัญชีหลาย ๆ อย่างนั้น ผู้สอบบัญชีจะต้องสร้างขึ้นในโปรแกรมคอมพิวเตอร์ ดังนั้นผู้สอบบัญชีด้านคอมพิวเตอร์จึงต้องเข้าไปมีส่วนเกี่ยวข้องด้วยเสมอในขั้นตอนแรกของการออกแบบระบบ

8) ปัญหาและความยุ่งยากต่าง ๆ ที่เกิดขึ้นเมื่อมีการใช้คอมพิวเตอร์ในการประมวลผลข้อมูลนั้นจะแปรผันในทางตรงกันข้ามกับขนาดของระบบคอมพิวเตอร์ที่ติดตั้ง เช่น ในเรื่องการแบ่งแยกหน้าที่ในระบบ

คอมพิวเตอร์ขนาดเล็ก ๆ นั้นไม่สามารถกระทำได้ เนื่องจากขาดบุคลากรที่มีความเชี่ยวชาญ ซึ่งเป็นผลให้คุณภาพของเอกสาร การสั่งงาน และกระบวนการปฏิบัติงานลดลง

ผู้สอบบัญชีต้องตรวจสอบลักษณะพิเศษที่สำคัญของการควบคุมภายในทางบัญชีว่ามีการปฏิบัติตามหรือไม่ ดังนี้

1) เรื่องของการแบ่งแยกหน้าที่ ในกรณีที่ระบบการลงบัญชีที่ทำด้วยมือไม่มีการแบ่งแยกหน้าที่ต่าง ๆ อาจจะมีการรวมไปอยู่ในโปรแกรมคอมพิวเตอร์เพียงโปรแกรมเดียว ดังนั้นการที่บุคคลใดบุคคลหนึ่งจะนำโปรแกรมนี้และแฟ้มข้อมูลอื่น ๆ ที่เกี่ยวข้องไปใช้อาจสามารถเปลี่ยนแปลงโปรแกรมและแฟ้มข้อมูลเพื่อทำการฉ้อฉลได้

2) เนื่องจากระบบคอมพิวเตอร์เป็นจำนวนมากสามารถใช้คำสั่งในการทำรายการต่าง ๆ ได้อย่างอัตโนมัติ เช่น ทำเช็คให้เจ้าหนี้ก่อนวันครบกำหนดชำระ ดังนั้นคอมพิวเตอร์อาจจะถูกสั่งให้กระทำการดังกล่าว ซึ่งเป็นลักษณะของการทำทุจริต ซึ่งเป็นการกระทำที่ไม่ได้รับการอนุมัติ

3) การนำคอมพิวเตอร์เข้ามาใช้ในการประมวลผลข้อมูลทางบัญชี อาจเป็นสาเหตุให้มีการบันทึกบัญชีไม่ถูกต้อง หรือละเลยไม่มีการบันทึกเลยก็ได้

4) ถ้าพนักงานที่ทำหน้าที่ในการประมวลผลข้อมูลมีความรู้และความสามารถแล้ว อาจจะมีการนำเอาทรัพย์สินไปใช้ได้ เช่น สั่งให้คอมพิวเตอร์ออกใบขนส่งสินค้าเพื่อนำสินค้าไปใช้ประโยชน์ส่วนตัวได้

5) อาจจะมีการตรวจนับทรัพย์สินมากเกินความเป็นจริง แล้วใช้คอมพิวเตอร์พิมพ์รายการให้ตรงกัน โดยปิดบังข้อมูลที่ถูกต้องเอาไว้

4.2 ร่องรอยการตรวจสอบในระบบการประมวลผลโดยใช้คอมพิวเตอร์ (The audit trail in an EDP system)

คำว่า "audit trail" นั้น หมายถึง เอกสารที่ใช้ประกอบในการบันทึกรายการเพื่อใช้ในการติดตามแหล่งข้อมูลที่เกิดขึ้นก่อนที่จะมีการสรุปอยู่ในรูปของงบการเงิน มีความหมายรวมถึงเอกสารเบื้องต้นที่ใช้ในการลงบัญชี สมุดรายวันเบื้องต้น บัญชีแยกประเภท กระดาษทดเลข และบันทึกอื่น ๆ ที่ทำขึ้นด้วยมือ ส่วนในระบบคอมพิวเตอร์ ได้แก่ บัตรเจาะรู เทปแม่เหล็ก แผ่นดิสก์ และรายงานที่พิมพ์ออกมา นอกจาก audit trail เป็นสิ่งที่ผู้สอบบัญชีใช้ตรวจติดตามรายการต่าง ๆ ทั้งในลักษณะของ compliance tests และ substantive tests แล้ว ผู้บริหารยังใช้ประโยชน์ในทางปฏิบัติงานตามปกติของตนอีกด้วย ไม่ว่าจะใช้ในการตอบคำถามแก่พนักงานลูกจ้าง ลูกค้า เจ้าหนี้ และหน่วยงานของรัฐ เพื่อให้บุคคลเหล่านั้นทราบถึงสถานภาพในการชำระหนี้ในการส่งสินค้า และเรื่องอื่น ๆ

ระบบการประมวลผลโดยใช้คอมพิวเตอร์มีผลกระทบต่อ audit trail ในหลาย ๆ ทาง ดังต่อไปนี้

1) เอกสารเบื้องต้นที่บันทึกลงไปในสื่อที่ใช้นำเข้าในรูปที่เครื่องคอมพิวเตอร์สามารถอ่านได้นั้น อาจจะถูกเก็บในลักษณะที่จะนำมาใช้ได้ยาก เช่น ในบริษัทหนึ่งที่ใช้ระบบการลงบัญชีด้วยมือนั้น บัตรลงเวลาทุกใบจะส่งไปยังศูนย์รวมที่หนึ่งเพื่อทำการประมวลผลเกี่ยวกับเงินเดือนค่าจ้าง แต่เมื่อบริษัทใช้คอมพิวเตอร์ในลักษณะ on-line แล้ว ข้อมูลจะถูกบันทึกเข้าไปในเครื่องคอมพิวเตอร์โดยผ่านเครื่อง terminal ที่อยู่ในสถานที่คนละแห่ง บัตรลงเวลาดังกล่าวจะถูกเก็บอยู่ในลักษณะกระจายกันหลาย ๆ แห่ง

2) ในคอมพิวเตอร์บางระบบนั้น เอกสารเบื้องต้นอาจจะถูกกำจัด เพราะมีการนำข้อมูลเข้าเครื่องคอมพิวเตอร์โดยตรง (direct input devices) ตัวอย่างเช่น พนักงานขายอาจจะนำคำสั่งซื้อส่งผ่านเข้าไปยัง terminal เลย แทนที่จะให้ทำเป็นใบสั่งซื้อก่อน

3) บัญชีแยกประเภทอาจจะถูกแทนที่ด้วยแฟ้มข้อมูลหลัก (master files) ซึ่งไม่ได้แสดงให้เห็นเป็นจำนวนที่จะนำไปสรุปยอดได้

4) วงจรในการประมวลผลข้อมูลไม่จำเป็นที่จะต้องทำเป็นบัญชีรายละเอียดรายการต่าง ๆ หรือทำเป็นสมุดรายวัน แต่ถ้าจะทำออกมาในรูปดังกล่าวอาจจะต้องเสียค่าใช้จ่ายเพิ่มมากขึ้น

5) ในบางครั้งไม่จำเป็นต้องให้คอมพิวเตอร์พิมพ์รายงานเกี่ยวกับข้อมูลในอดีตออกมา เนื่องจากแฟ้มข้อมูลสามารถเก็บไว้ในสื่อ และจะรายงานให้ทราบเฉพาะกรณีพิเศษ

6) แฟ้มข้อมูลที่เก็บไว้ในสื่อแม่เหล็กนั้นไม่สามารถอ่านได้ นอกจากใช้คอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ เช่น แฟ้มข้อมูลเกี่ยวกับสินค้าคงคลังที่เก็บไว้ในเทปแม่เหล็ก จะต้องใช้คอมพิวเตอร์และโปรแกรมในการพิมพ์ออกมา หรือวิเคราะห์เนื้อหาที่อยู่ในแฟ้มนั้น ๆ

7) ลำดับของข้อมูลที่บันทึกไว้และธุรกรรมที่เกี่ยวกับการประมวลผลนั้น ยากที่จะสังเกตเห็นได้ เพราะว่าข้อมูลและธุรกรรมต่าง ๆ นั้นถูกบรรจุอยู่ภายในระบบคอมพิวเตอร์

4.3 การควบคุมทั่วไปและการควบคุมระบบงานต่าง ๆ (General and application controls)

การควบคุมด้านบัญชีที่มีความจำเป็นเพิ่มขึ้น เมื่อมีการนำเอาคอมพิวเตอร์มาใช้ประมวลผลข้อมูลทางบัญชีนั้น คือ general และ application control ตามที่ระบุไว้ใน SAS ฉบับที่ 3 เรื่อง "ผลของการประมวลผลโดยใช้คอมพิวเตอร์ต่อการศึกษา และประเมินประสิทธิภาพการควบคุมภายใน" นั้น กล่าวไว้ว่า general control ครอบคลุมถึงประเด็นต่าง ๆ ต่อไปนี้

- แผนการจัดองค์กรและการปฏิบัติงานของส่วนงานที่ประมวลผล
- กระบวนการต่าง ๆ เกี่ยวกับเอกสาร การสอบทาน การทดสอบ การอนุมัติต่าง ๆ เกี่ยวกับระบบและโปรแกรม และการเปลี่ยนแปลงต่าง ๆ
- การควบคุมซึ่งผู้ผลิตคอมพิวเตอร์สร้างขึ้นไว้แล้วในเครื่อง โดยทั่วไปหมายถึง hardware control
- การควบคุมในการเข้าถึงอุปกรณ์คอมพิวเตอร์และแฟ้มข้อมูล
- การควบคุมข้อมูลและขั้นตอนอื่น ๆ ที่มีผลต่อการปฏิบัติงานโดยส่วนรวม

ส่วน application controls หมายความรวมถึง

- การควบคุมข้อมูลนำเข้า
- การควบคุมในการประมวลผล
- การควบคุมผลลัพธ์

General control จะมีผลกระทบต่อ application control ในทางลบ ถ้าการควบคุมในด้านนี้อ่อนหรือไม่มี ซึ่งทำให้ผู้สอบบัญชีอาจจะไม่สามารถเชื่อถือระบบการควบคุมทั้งสองประเภทได้ ส่วน application controls นั้นสัมพันธ์กับงานเฉพาะประเภทที่กระทำโดยคอมพิวเตอร์ เช่น ระบบเงินเดือน และสินค้าคงคลัง

4.4 การศึกษาและการประเมินประสิทธิภาพระบบการควบคุมภายใน (Internal control system study and evaluation)

การที่ผู้สอบบัญชีจะต้องศึกษาและประเมินประสิทธิภาพระบบการควบคุมภายในนั้น มีผลกระทบมาจากการควบคุมด้านบัญชีในการประมวลผลโดยใช้คอมพิวเตอร์ audit trail, general controls และ application controls ดังที่ได้กล่าวมาแล้วข้างต้น ถึงแม้ว่าวิธีการทั่วไปที่ใช้ในการศึกษาและประเมินประสิทธิภาพระบบการควบคุมภายในจะมีลักษณะเหมือนกัน ไม่ว่าจะเป็นระบบการลงบัญชีด้วยมือ เครื่องจักร หรือคอมพิวเตอร์ก็ตาม แต่ในเรื่องของคอมพิวเตอร์นั้น การวิเคราะห์ถึงความสัมพันธ์ระหว่างเครื่องคอมพิวเตอร์และผู้ใช้งาน และเรื่องอื่น ๆ ที่เกี่ยวกับระบบบัญชีนั้น มีความสลับซับซ้อนทีเดียว

วิธีการทั่วไปที่ใช้ในการศึกษาและประเมินประสิทธิภาพระบบการควบคุมภายในจะประกอบด้วย การสอบทานระบบการควบคุมภายใน การทดสอบการปฏิบัติตามระบบ และการประเมินผลกระทบดังกล่าว เพื่อให้บรรลุจุดมุ่งหมายของการสอบทาน การทดสอบ และการประเมินผลสำเร็จลงได้ ผู้สอบบัญชีต้องประเมินการควบคุมด้านบัญชีที่ใช้คอมพิวเตอร์ด้วย เพราะการสอบบัญชีด้านคอมพิวเตอร์มิใช่จำกัดแค่ธุรกรรมที่เกี่ยวข้องกับคอมพิวเตอร์เท่านั้น

ผู้สอบบัญชีด้านคอมพิวเตอร์จำเป็นต้องประเมินการควบคุมด้านบัญชีที่ใช้ คอมพิวเตอร์ใน 2 ลักษณะ คือ

1) ผู้สอบบัญชีต้องประเมินการควบคุมด้านบัญชีในเรื่องที่มีนัยสำคัญทุกเรื่องที่กระทำขึ้นโดยบุคคล เครื่องจักร และระบบคอมพิวเตอร์ เช่น ในระบบขายและการเก็บเงินนั้น จะเริ่มจากคนเตรียมใบสั่งขาย เครื่องจักรเตรียมทำใบกำกับสินค้า และปรับปรุงยอดคงค้างของข้อมูลในแฟ้มลูกหนี้ที่เก็บในคอมพิวเตอร์ ดังนั้นในการประเมินประสิทธิภาพการควบคุมด้านบัญชี จะต้องประเมินในส่วนที่ทำโดยบุคคลและเครื่องจักร ซึ่งเป็นส่วนประกอบของการประเมินการประมวลผลโดยใช้คอมพิวเตอร์

2) ผู้สอบบัญชีต้องประเมินการควบคุมด้านบัญชีในส่วนของการประมวลผลโดยใช้คอมพิวเตอร์ในส่วนของผู้ใช้งาน และประเมินทั้งสองส่วนร่วมกัน

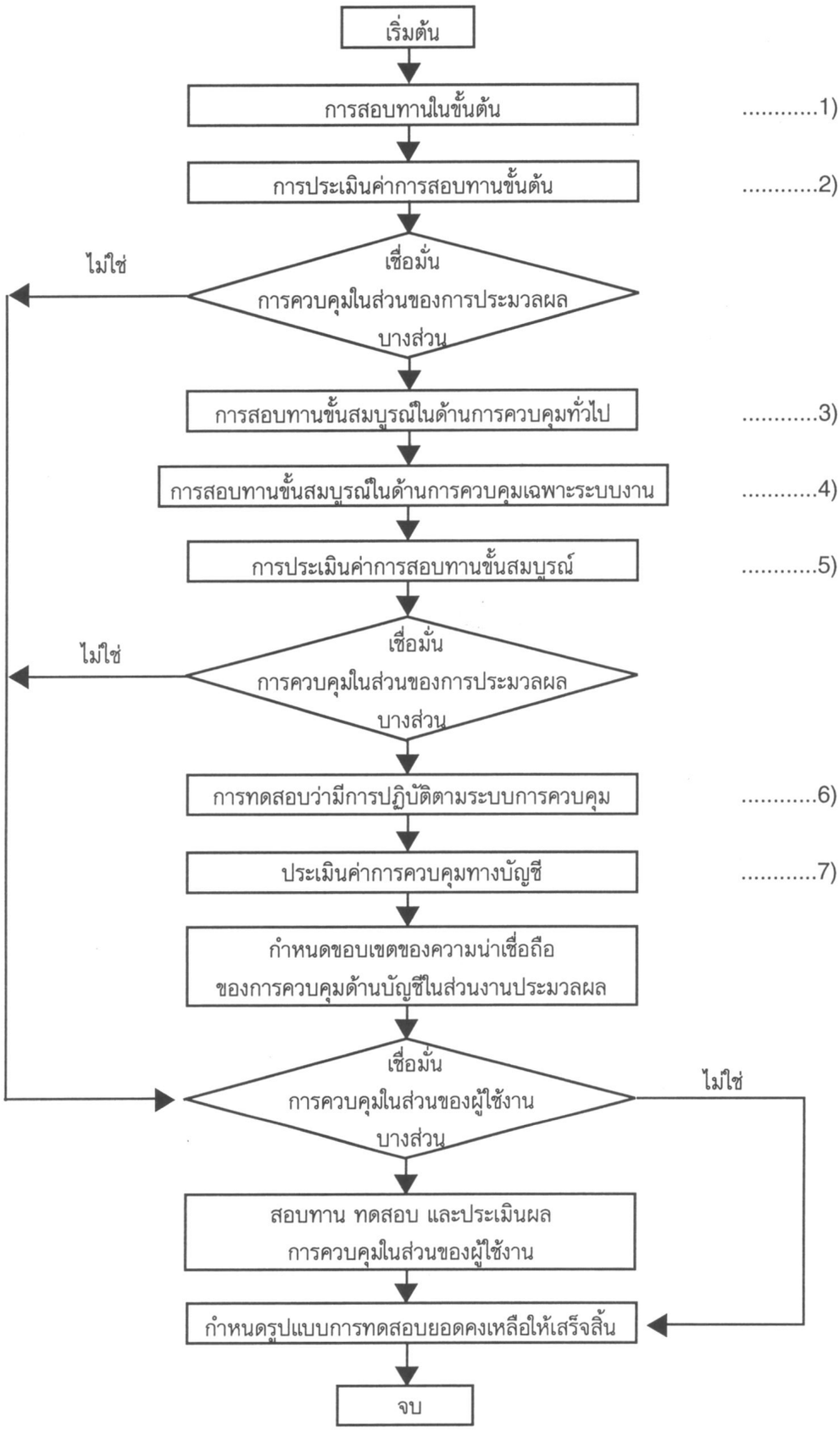
ความสัมพันธ์ระหว่างกันของการควบคุมด้านบัญชีในส่วนของการประมวลผล โดยใช้คอมพิวเตอร์และส่วนของผู้ใช้งาน ปรากฏตามรูปข้างล่างนี้

การควบคุมข้อมูลนำเข้าของผู้ใช้งาน	การควบคุมการประมวลผลของผู้ใช้งาน	การควบคุมผลลัพธ์ของผู้ใช้งาน
	การควบคุมร่วมกันของผู้ใช้งานและส่วนประมวลผล	
	การควบคุมข้อมูลนำเข้า การประมวลผล และผลลัพธ์ของส่วนประมวลผล	
	ข้อมูลนำเข้า การประมวลผล และผลลัพธ์	

การควบคุมการประมวลผลของผู้ใช้งาน

กระบวนการที่ผู้สอบบัญชีด้านคอมพิวเตอร์ใช้ในการประเมินความน่าเชื่อถือ ของการควบคุมด้านบัญชีทั้ง 2 ส่วนนั้น ปรากฏดังรูปต่อไปนี้





ขั้นตอนการตรวจสอบงาน (Application) ในองค์กรที่ใช้คอมพิวเตอร์

ขั้นตอนที่	จุดประสงค์	วิธีการ
1) การสอบทานขั้นต้น (Preliminary phase of reviews)	เข้าใจระบบบัญชีทั้งส่วนที่เป็น EDP และที่ไม่ใช่ EDP - flow ของรายการและความสำคัญของ output - ขอบเขตของการใช้ EDP ในระบบงานบัญชีที่สำคัญๆ - โครงสร้างพื้นฐานของการควบคุมทางบัญชีทั้งใน EDP และ User Control	สอบถาม, discuss, สังเกตการณ์, สอบทานเอกสาร, trace รายการ, ใช้แบบสอบถาม การควบคุม และ checklist
2) การประเมินค่าการสอบทานขั้นต้น (Preliminary review assessment)	- ประเมินความสำคัญของการควบคุมทางบัญชีของ EDP และ ที่ไม่ใช้ EDP - กำหนดขอบเขตที่จะขยายการสอบทานภายใน EDP	ใช้วิจารณญาณ
3) การสอบทานขั้นสมบูรณ์ในด้านการควบคุมทั่วไป (Completion of review general controls)	- ชี้ถึง general controls ที่ให้ความเชื่อมั่นและพิจารณาว่ามีการทำงานอย่างไร - พิจารณาผลกระทบของจุดแข็ง จุดอ่อนที่มีผลต่อการควบคุมเฉพาะระบบ (application control) - พิจารณาการ test compliance จะทำอย่างไร	ตรวจสอบเอกสารในรายละเอียด, สัมภาษณ์ผู้ตรวจสอบภายในบุคลากรด้าน EDP และ User, สังเกตการณ์การปฏิบัติงานเกี่ยวกับ general controls
4) การสอบทานขั้นสมบูรณ์ในด้านการควบคุมเฉพาะระบบงาน (Completion of review application controls)	- ชี้ถึง application controls ที่ให้ความเชื่อมั่นและพิจารณาว่ามีการทำงานอย่างไร - พิจารณาลักษณะของ compliance test ที่จะทำ - พิจารณาผลกระทบของจุดอ่อน จุดแข็งที่อาจมีผลต่อการทำ compliance test	ตรวจสอบเอกสารในรายละเอียด, สัมภาษณ์ผู้ตรวจสอบภายในบุคลากรด้าน EDP และ User, สังเกตการณ์เกี่ยวกับการทำ application control จริงๆ ในแต่ละระบบงานบัญชีที่สำคัญ
5) การประเมินค่าการสอบทานขั้นสมบูรณ์ (Completion of review assessment)	- พิจารณาชนิดของข้อผิดพลาดทั้งที่ตั้งใจและไม่ตั้งใจที่อาจเกิดขึ้น - สามารถชี้ถึงขบวนการควบคุมที่ใช้ prevent, detect ข้อผิดพลาด - ประเมินประสิทธิผลของการควบคุมทางบัญชีของ EDP และที่ไม่ใช้ EDP	ใช้วิจารณญาณ

ขั้นตอนที่	จุดประสงค์	วิธีการ
6) การทดสอบว่ามีการปฏิบัติตามระบบการควบคุม (Tests of compliance)	- เพื่อตัดสินใจว่ามีการกำหนดให้ใช้ระบบการควบคุมที่จำเป็น และมีการปฏิบัติตามอย่างเต็มใจจากพนักงาน - เพื่อยืนยันว่าการควบคุมดังกล่าวใช้ได้เหมาะสม - พิจารณาการควบคุม ขอบเขตความเหมาะสมในการใช้เอกสาร ใช้เมื่อไร ใช้อย่างไร ใช้โดยใคร	ตรวจสอบบันทึกบัญชีต่าง ๆ, ทดสอบขบวนการควบคุม สอบถามและสังเกตการณ์
7) ประเมินค่าการควบคุมทางบัญชี (Evaluation of accounting controls)	สำหรับระบบการบัญชีที่สำคัญแต่ละระบบ - พิจารณาถึงลักษณะของข้อผิดพลาดที่เกิดขึ้นโดยเจตนา และไม่เจตนา - พิจารณาถึงขบวนการควบคุมทางบัญชี ที่จะ prevent หรือ detect ข้อผิดพลาดดังกล่าว - ตัดสินใจว่าขบวนการควบคุมที่จำเป็นดังกล่าวมีการกำหนดให้ปฏิบัติ และมีการปฏิบัติตามอย่างเต็มที่ - ประเมินค่าจุดอ่อน และผลกระทบที่มีต่อลักษณะ ระยะเวลา และขอบเขต ของขบวนการตรวจสอบที่จะนำมาใช้	ใช้วิจารณญาณ

หมายเหตุ ณ จุดใดก็ตามหลังจากสอบทานขั้นต้นที่ผู้สอบบัญชีอาจตัดสินใจไม่เชื่อมั่นต่อระบบการควบคุมทางบัญชี EDP ในทุกระบบงาน (application) หรือบางระบบงานก็ตาม ผู้สอบบัญชีควรจะหันไปทำ **substantive test** โดยสมบูรณ์ ซึ่งประกอบด้วยขบวนการตรวจสอบดังนี้

1) ทดสอบรายละเอียดของรายการและยอดคงเหลือ
2) สอบทานโดยการวิเคราะห์เปรียบเทียบอัตราส่วนที่สำคัญ ๆ แนวโน้มและการตรวจสอบรายการผิดปกติ รายการที่ขึ้นลงมาก หรือรายการที่น่าสงสัย ซึ่งพบจากการวิเคราะห์เปรียบเทียบนั้น

ในช่วงต้นของการสอบทานนั้น จะต้องเก็บรวบรวมข้อมูลและประเมินประสิทธิภาพการควบคุมด้านบัญชีในส่วนของการประมวลผลโดยใช้คอมพิวเตอร์ให้สัมพันธ์กับระบบการควบคุมด้านบัญชีทั้งระบบ ผลลัพธ์ ที่ได้จากการประเมินนั้น ผู้สอบบัญชีจะต้องกำหนดขอบเขตในการสอบทานการควบคุมด้านบัญชีในส่วนของการประมวลผลโดยใช้คอมพิวเตอร์

การกำหนดขอบเขตความน่าเชื่อถือของการควบคุมด้านบัญชี ในส่วนของการประมวลผลโดยใช้คอมพิวเตอร์นั้น ผู้สอบบัญชีจะใช้เป็นหลักในการตัดสินใจว่าจะทำธุรกรรมอะไรต่อไป ซึ่งมีทางเลือกหลัก ๆ 3 ทาง คือ

1) ผู้สอบบัญชีอาจจะสรุปว่า การควบคุมที่มีอยู่มีความน่าเชื่อถือเพียงพอที่จะกำหนดขอบเขตของการทดสอบความถูกต้องยอดคงเหลือให้แคบลง โดยการสอบทานระบบให้เสร็จสิ้นแล้วทดสอบการปฏิบัติตามระบบและกำหนดรูปแบบของการทดสอบความถูกต้องของยอดคงเหลือ

2) ผู้สอบบัญชีอาจจะสรุปว่า การควบคุมที่มีอยู่อ่อนมากเกินกว่าที่จะเชื่อถือได้ ก็จะไม่ทดสอบการปฏิบัติตามระบบ แต่จะใช้วิธีทดสอบความถูกต้องของยอดคงเหลือเพื่อให้บรรลุวัตถุประสงค์ของการสอบบัญชี

3) ผู้สอบบัญชีอาจจะสรุปว่า การควบคุมที่มีอยู่พอจะเชื่อถือได้ แต่ไม่มีประสิทธิภาพพอเวลาที่ใช้ในการสอบทานระบบทั้งหมด และทดสอบการปฏิบัติตามระบบอาจจะไม่คุ้มค่ากับการลดขอบเขตของการทดสอบความถูกต้องของยอดคงเหลือให้แคบลง

นอกจากผู้สอบบัญชีจะต้องคำนึงถึงความน่าเชื่อถือของการควบคุมด้านบัญชีใน ส่วนของการประมวลผลโดยใช้คอมพิวเตอร์แล้ว ยังต้องประเมินการควบคุมด้านบัญชีในส่วนของผู้ใช้งาน และความสัมพันธ์ระหว่างกันอีกด้วย ผู้สอบบัญชีอาจจะตัดสินใจเชื่อถือการควบคุมด้านบัญชีในส่วนของผู้ใช้งานด้วยเหตุผลหลายประการ ดังนี้คือ

1) การควบคุมด้านบัญชีในส่วนของผู้ใช้งานมีความน่าเชื่อถือมากกว่าการควบคุมด้านบัญชีในส่วนของการประมวลผลโดยใช้คอมพิวเตอร์

2) การควบคุมด้านบัญชีในส่วนของการประมวลผลโดยใช้คอมพิวเตอร์มีจุดอ่อน และไม่น่าเชื่อถือ

3) ผู้สอบบัญชีอาจสรุปว่า การควบคุมทั้ง 2 ส่วนจะทำให้ระบบทั้งระบบมีความน่าเชื่อถือ

5. การทดสอบความถูกต้องของยอดคงเหลือ : การเก็บรวบรวมเพื่อให้ได้มาซึ่งหลักฐานที่เพียงพอ (Substantive tesing : the collection of sufficient competent evidential matter)

หลังจากทำการศึกษาและประเมินประสิทธิภาพการควบคุมภายในตามมาตรฐานการปฏิบัติงานในข้อที่ 2 แล้ว ผู้สอบบัญชียังต้องปฏิบัติตามมาตรฐานการปฏิบัติงานในข้อที่ 3 คือ การตรวจสอบให้ได้มาซึ่งหลักฐานที่เพียงพอ เพื่อที่จะสามารถให้ความเห็นในงบการเงินได้ การเก็บรวบรวมหลักฐานดังกล่าวนั้นเป็นเรื่องของการทดสอบความถูกต้องของยอดคงเหลือซึ่งมีส่วนประกอบ 2 ส่วน คือ

1) กระบวนการสอบทานเชิงวิเคราะห์ ครอบคลุมถึงการวิเคราะห์อัตราส่วน แนวโน้ม และความสัมพันธ์ระหว่างกันของข้อมูลที่เกี่ยวข้องกับตัวเงิน และไม่เกี่ยวข้องกับตัวเงิน เครื่องคอมพิวเตอร์สามารถใช้ในการวิเคราะห์ความสัมพันธ์เหล่านี้ได้ เช่น คำนวณการเปลี่ยนแปลงที่เกิดขึ้นจากช่วงเวลาหนึ่งกับช่วงเวลาต่อไปเป็นร้อยละ และคำนวณผลต่างที่เกิดขึ้นระหว่างประมาณการกับผลการดำเนินงานที่เกิดขึ้นจริง

2) ทดสอบยอดคงเหลือตามบัญชี ครอบคลุมถึงการทดสอบรายละเอียดของรายการ และยอดดุลต่าง ๆ ซึ่งคอมพิวเตอร์สามารถทำได้อย่างมีประสิทธิภาพ

คอมพิวเตอร์มีบทบาทที่สำคัญ 2 ประการ ในการตรวจสอบในเรื่องของ substantive testing คือ

1) คอมพิวเตอร์สามารถทดสอบได้ทั้ง compliance และ substantive เช่น กระบวนการทดสอบการปฏิบัติตามระบบนั้น ก็เพื่อให้แน่ใจว่ากระบวนการผ่านรายการจากแฟ้มข้อมูลที่เกี่ยวกับการชำระหนี้มีการบันทึกในแฟ้มข้อมูลของลูกหนี้รายตัวหรือไม่ และทดสอบความถูกต้องของยอดคงเหลือ โดยการสอบทานยอดคงเหลือของบัญชีลูกหนี้รายตัวในแฟ้มข้อมูลลูกหนี้รายตัวได้

2) คอมพิวเตอร์สามารถใช้ทดสอบความถูกต้องของยอดคงเหลือโดยตรงได้อย่างเป็นอิสระจากการทดสอบการปฏิบัติตามระบบ เช่น คอมพิวเตอร์สามารถใช้รวมยอดบัญชีลูกหนี้รายตัวในเทปแม่เหล็ก เพื่อให้แน่ใจว่ายอดรวมดังกล่าวตรงกับบัญชีคุมยอดลูกหนี้

6. สรุป

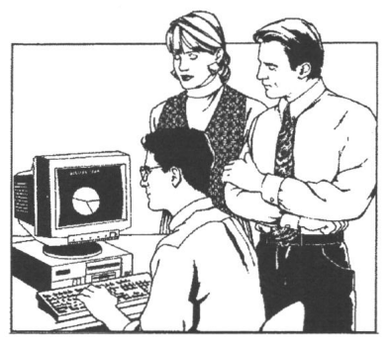
มาตรฐานการปฏิบัติงานทั้ง 3 ข้อนั้น เป็นเรื่องของการศึกษาและประเมินประสิทธิภาพการควบคุมภายใน การทดสอบการปฏิบัติตามระบบ การทดสอบยอดเงินคงเหลือ และการตรวจสอบเพื่อให้ได้มาซึ่งหลักฐานที่เพียงพอเพื่อใช้ในการแสดงความเห็นในงบการเงิน

แนวความคิดและกระบวนการต่าง ๆ ในการศึกษาและประเมินประสิทธิภาพการควบคุมภายในในระบบการลงบัญชีด้วยมือและเครื่องจักร สามารถนำมาประยุกต์ใช้ได้กับกรณีของการประมวลผลโดยใช้คอมพิวเตอร์ จุดมุ่งหมายยังคงเป็นเรื่องของการกำหนดขอบเขตความน่าเชื่อถือของระบบ เพื่อที่จะจำกัดกระบวนการตรวจสอบให้แคบลง และใช้ในการวางแผนการตรวจสอบ ลักษณะขั้นพื้นฐานของระบบการควบคุมภายในก็คือ การแบ่งแยกหน้าที่

ความรับผิดชอบ กระบวนการบันทึกและการอนุมัติ การถือปฏิบัติอย่างถูกต้องเหมาะสม คุณภาพของบุคลากร และระบบการปฏิบัติงานที่เป็นจริง ผู้สอบบัญชีต้องสามารถแยกความแตกต่างระหว่างการควบคุมด้านบริหารและด้านบัญชีออกจากกัน เพื่อที่จะเน้นในเรื่องการควบคุมด้านบัญชีเป็นหลัก การศึกษาระบบการควบคุมภายในจะติดตามมาด้วยการประเมินผลระบบ และเมื่อผู้สอบบัญชีกำหนดขอบเขตความน่าเชื่อถือของข้อมูลแล้ว ก็สามารถกำหนดรูปแบบของการทดสอบความถูกต้องของยอดคงเหลือได้

การนำเอาคอมพิวเตอร์มาใช้ประมวลผลข้อมูลทางบัญชีนั้น มีผลกระทบต่อการควบคุมด้านบัญชีและ audit trail ก่อให้เกิดการเปลี่ยนแปลงมากมายในกระบวนการประมวลผล ผลจากการเปลี่ยนแปลงทำให้ผู้สอบบัญชีต้องประเมินถึงผลที่กระทบต่อลักษณะขั้นพื้นฐานของระบบการควบคุมภายใน ทั้งยังต้องตระหนักถึงการเปลี่ยนแปลงในเรื่อง audit trail จะต้องมีการควบคุมด้าน general controls และ application controls เพิ่มขึ้นในการสอบทานระบบการควบคุมภายใน ผู้สอบบัญชีต้องทดสอบการปฏิบัติตามระบบและประเมินผลระบบดังกล่าว ทั้งยังต้องวิเคราะห์ถึงประสิทธิภาพของ user accounting controls, EDP accounting control และความสัมพันธ์ระหว่างกันอีกด้วย เพื่อจะได้กำหนดขอบเขตความน่าเชื่อถือของระบบการควบคุมภายใน

การทดสอบยอดเงินคงเหลือในเรื่องของการเก็บรวบรวม เพื่อให้ได้มาซึ่งหลักฐานเพียงพอเพื่อใช้ในการแสดงความเห็นต่องบการเงินนั้น กระทำได้โดยการใช้กระบวนการสอบทานเชิงวิเคราะห์ และทดสอบยอดคงเหลือตามบัญชี



บทที่ 3

การเข้าใจของผู้บริหารจาก ผลกระทบของคอมพิวเตอร์ ต่อองค์กรก็ช่วยลดการทุจริตได้

การเข้าใจของผู้บริหารจากผลกระทบของคอมพิวเตอร์ต่อองค์กรก็ช่วยลดการทุจริตได้

มีผู้บริหารและผู้พัฒนางานจำนวนไม่น้อยในหลายองค์กร ที่ไม่ได้ให้ความสำคัญหรือเข้าใจในเรื่องนี้ จึงมักปรากฏจุดอ่อนในระบบงานที่ใช้คอมพิวเตอร์อย่างคาดไม่ถึง ดังนั้นก่อนที่จะพูดกันถึงเรื่องการทุจริตต่อไป ควรทบทวนเรื่องต่อไปนี้เล็กน้อย

1. ผลกระทบของคอมพิวเตอร์ที่มีต่อการตรวจสอบ สรุปได้ดังนี้

1.1 EDP หรือ IS ทำให้ร่องรอยการตรวจสอบเปลี่ยนแปลงไป

1.2 ทำให้วิธีการควบคุมภายใน และการปฏิบัติงานเปลี่ยนแปลงไป

1.3 ทำให้การจัดเก็บข้อมูลและหลักฐานการตรวจสอบเปลี่ยนแปลงไปมาก ข้อมูลบางอย่างไม่อาจติดตามร่องรอยได้ยาก

1.4 จำเป็นต้องใช้ผู้เชี่ยวชาญเฉพาะด้านมากขึ้น

1.5 ทำให้การวางแผนการตรวจสอบเปลี่ยนแปลงไป

1.6 อาจใช้คอมพิวเตอร์เป็นเครื่องมือช่วยในการตรวจสอบได้

2. การควบคุมและการตรวจสอบ

2.1 ผลกระทบต่อระบบการรักษาความปลอดภัย

ตามที่ทราบแล้วว่า Computer Security ประกอบด้วยการค้นหาปัญหาที่อาจจะเกิดขึ้น (detection) การควบคุม (control) และการตรวจสอบ (audit) ดังนั้น เราจึงควรทราบว่าคอมพิวเตอร์จะมีผลกระทบอย่างไรต่อ security เพื่อที่เราจะได้สามารถวางแผนเพื่อการสืบหา (detection) การควบคุม (control) ตรวจสอบ (audit) และแก้ไข (correction) ในภายหลังได้ ดังนั้นสิ่งที่ควรทราบในขั้นแรกก็คือ ช่องทางหรือจุดอ่อนที่เปิดโอกาสให้เกิดความเสียหายทางคอมพิวเตอร์และผลกระทบของคอมพิวเตอร์ที่มีต่อการดำเนินงานของธนาคาร ดังผลกระทบที่อาจจะเกิดขึ้นจากการใช้ข้อมูลไปในทางที่ผิด ดังต่อไปนี้

2.1.1) การใช้ technology ไปในทางที่ไม่ถูกต้อง (improper use of technology)

2.1.2) การบันทึกข้อมูลผิดพลาด (record error)

2.1.3) การปฏิบัติงานไม่เป็นไปตามขั้นตอนที่กำหนดไว้ (illogical processing) ซึ่งจะยกตัวอย่างกรณีเหตุการณ์ที่เกิดขึ้นจริงต่อไปภายหลัง

2.1.4) การไม่สามารถประสานความต้องการของผู้ใช้ให้เข้ากับปัญหาด้านเทคนิค

2.1.5) การไม่สามารถควบคุมเทคโนโลยีได้ (inability to control technology)

2.1.6) การตัดสินใจเกี่ยวกับข้อผิดพลาด (the decision of error)

2.1.7) การป้อนข้อมูลเข้าไม่ถูกต้อง (incorrect entry of data)

2.1.8) การชดเชยข้อมูล (compensation of data)

2.1.9) การไม่สามารถตอบสนองอย่างรวดเร็ว (inability of react quickly)

2.1.10) การไม่สามารถแสดงหลักฐานเกี่ยวกับการปฏิบัติงาน

2.1.11) การทดแทนความรับผิดชอบ

2.2 การตรวจสอบการประมวลผลด้วยคอมพิวเตอร์ (EDP Auditing)

เราจะพบว่า ระบบการควบคุมจะประกอบขึ้นด้วย

- ส่วนที่ควบคุมโดย Manual (Manual Section Segment)
- ส่วนที่ควบคุมโดยระบบคอมพิวเตอร์ (EDP Segment)
- การควบคุมการพัฒนาระบบ (Develope Segment)

เนื่องจากการประมวลผลในบางส่วนเราจะใช้วิธีประมวลผลด้วยคน (Manual) บางส่วนเราจะประมวลผลด้วยคนและด้วยคอมพิวเตอร์ และบางส่วนจะประมวลผลโดยอาศัยคอมพิวเตอร์เพียงอย่างเดียว ทั้งนี้ EDP audit จะเป็นการตรวจสอบและทบทวนถึงระบบการควบคุมต่าง ๆ (Verification of control) ของหน่วยงานที่ตรวจสอบ หลังจากที่มีการศึกษากันอย่างละเอียดในเรื่องต่อไปนี้ คือ

2.2.1 การสอบทานระบบและโปรแกรมเฉพาะงาน (system or application review)

2.2.2 สาเหตุของความเสี่ยงและความเสี่ยงที่เกิดขึ้น (identify risks, cause to exposure)

2.2.3 การประเมินและสรุปผลประสิทธิภาพการควบคุม (evaluate control)

2.2.4 การทดสอบการควบคุม หรือการทดสอบโปรแกรมระบบงาน (test of control or test data (application))

2.2.5 การวิเคราะห์และการสรุปผล (analysis result)

2.2.6 การนำเสนอรายงาน (reporting)

ในเรื่องของการประเมินประสิทธิภาพการควบคุมนั้น เราต้องแยกให้ออกว่า จุดใดบ้างที่เราจะทำการวางจุดควบคุม และจะควบคุมด้วยวิธีใด ในการประเมินประสิทธิภาพการควบคุมนั้น เราอาจใช้ control matrix ช่วยด้วยก็ได้ นอกจากนี้การประเมินการควบคุมยังต้องคำนึงถึงความเสี่ยง ตลอดจนสาเหตุของความเสี่ยงอีกด้วย เพื่อว่าเมื่อเราทราบถึงจุดอ่อนต่าง ๆ ในระบบแล้ว เราจะได้ทำการพิจารณาดูว่ามีจุดควบคุมใดบ้างที่สามารถป้องกันหรือทดแทนจุดอ่อนเหล่านั้นได้ โดยเราจะนำทั้งจุดอ่อนหรือจุดควบคุมมาพิจารณาว่า จุดควบคุมต่าง ๆ ที่มีนั้นมีประสิทธิภาพจริงหรือไม่ มากน้อยเพียงใด และสิ่งที่มีอยู่นั้นจะสามารถป้องกัน แก้ไข ทดแทน จุดอ่อนใดได้บ้าง โดยเราอาจใช้วิธีทดสอบระบบงาน (test data) ช่วยด้วยก็ได้

การทำ test data นั้น เราจะต้องทำการสอบทาน (verify) การประมวลผลของเครื่องคอมพิวเตอร์และผลลัพธ์ที่จะได้ ในการสอบทานหรือการตรวจสอบผลเหล่านี้ เราอาจใช้เทคนิคอื่นช่วยด้วย เช่น การขอคำยืนยันยอด (Confirmation) ทั้งนี้เพื่อติดตามดูความถูกต้องของยอดคงเหลือ (balance) อย่างไรก็ดีวิธีขอคำยืนยันยอดนี้จะไม่สามารถครอบคลุมได้ทั้งหมด เช่น ในสหรัฐอเมริกาเคยมีการทำทุจริตขึ้นโดยที่ไม่สามารถตรวจพบได้ด้วยวิธีการขอคำยืนยันยอดมาแล้ว โดยทางบริษัท Equity Funding Company ได้ออกใบกรมธรรม์ปลอม (fiction Insurance) ซึ่งมีมูลค่าถึง 50 ล้านดอลลาร์ สรอ. เพื่อการแสดงฐานะการดำเนินงานที่ดีขึ้น โดยใช้ computer เป็นเครื่องมือ บริษัทดังกล่าวได้ตั้ง (set) โปรแกรมไว้ว่า ทุกครั้งที่มีการเช็คสอบยอดคงเหลือ (balance) โปรแกรมที่ตั้งไว้จะทำการเช็คสอบว่า ถ้าเป็นรายการที่ใช้ใบกรมธรรม์ปลอม หรือยอดคงเหลือปลอม (fiction insurance of fiction balance) หรือไม่ ถ้าใช่ก็ให้ข้ามไป ทำให้ทุกครั้งที่มีการสุ่มตัวอย่างเพื่อขอคำยืนยันยอดจะสุ่มไม่พบรายการดังกล่าว หรือถ้าสุ่มพบก็จะได้ที่อยู่ที่ผิดจากความจริง จึงไม่ได้รับใบตอบรับจากการสอบถามยืนยันยอด ดังนั้นจึงเป็นการยากมากที่จะพบว่ามีการสร้างใบกรมธรรม์ปลอมซ่อนอยู่ แม้กระทั่งผู้ตรวจสอบของบริษัทเอง ไม่ว่าจะเป็นผู้ตรวจสอบภายในผู้ตรวจสอบภายนอก หรือ EDP auditor ก็หาไม่พบ ซึ่งนับได้ว่าเป็นปัญหา (จุดอ่อน) อย่างหนึ่งของเทคนิคการขอคำยืนยันยอด (confirmation)

3. การสอบทานการประมวลผลของเครื่องคอมพิวเตอร์

มีเทคนิคการตรวจสอบอยู่ 2 แบบ คือ

- EDP auditing by computer ซึ่งก็คือแบบ assisted หรือแบบ through the computer
- EDP auditing without computer ซึ่งก็คือแบบ around the computer

3.1 เทคนิคของการตรวจสอบโดยใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

มีเทคนิคมากมายที่เรียกชื่อแตกต่างกันออกไป แต่สามารถแบ่งได้เป็น เทคนิคหลัก และเทคนิครอง ดังนี้

เทคนิคหลัก ได้แก่ การวิเคราะห์โปรแกรม การทำ TDM (test data method) การแปลภาษา (compile) การเปรียบเทียบ (compare) การใช้ข้อมูลที่ทำขึ้นสำหรับการทดสอบโปรแกรมใหม่ที่จะนำมาใช้งานเพื่อศึกษาการทำงานของโปรแกรมโดยละเอียดทุกขั้นตอน และเพื่อสอบทานความถูกต้องของการประมวลผล โดยนำผลที่ได้จากการประมวลมาเปรียบเทียบกับผลลัพธ์ที่คำนวณไว้ล่วงหน้า (Base case system simulation) การ dump ข้อมูลออกมาตรวจสอบทีละครั้งระหว่างการประมวลผล (snap shot) การพิสูจน์ความถูกต้องของข้อมูลโดยอิสระแยกจากการประมวลผลจริงโดยใช้โปรแกรมอีกชุดหนึ่งของผู้ตรวจสอบ ซึ่งมีลักษณะเหมือนโปรแกรมใช้งาน เพื่อเลียนแบบการประมวลผลและใช้ข้อมูลจริง แล้วนำผลลัพธ์มาเปรียบเทียบกับการประมวลผลจริง (simulation) การควบคุมโดยใช้ผังงาน (control flowchart)

เทคนิครอง ได้แก่

- ITF (integrated test facility) เป็นการทดสอบที่สามารถใช้ทดสอบความถูกต้องของการปฏิบัติงาน ทั้งที่ทำโดยคน และ/หรือทำโดยเครื่องคอมพิวเตอร์ ซึ่งจะเป็นการทดสอบข้อมูลในระหว่างประมวล

ผลจริง โดยผู้ตรวจสอบจะสร้างข้อมูลสำหรับใช้ตรวจสอบ โดยข้อมูลที่สร้างขึ้นจะมีลักษณะเหมือนข้อมูลจริงของหน่วยงานที่ใช้ข้อมูล แล้วป้อนเข้าเครื่องคอมพิวเตอร์ให้ประมวลผลคละไปกับข้อมูลจริง ต่อจากนั้นจึงนำผลลัพธ์ที่ได้จากการประมวลผลมาเปรียบเทียบกับผลลัพธ์ที่คำนวณไว้ล่วงหน้า

- Audit logging คือ การบันทึกการปฏิบัติงานของพนักงานที่เกี่ยวข้องกับการประมวลผล เพื่อใช้เป็นข้อมูลสำหรับการตรวจสอบในเรื่องการใช้แฟ้มข้อมูล ตลอดจนการป้อนข้อมูลผ่านทาง terminal และข้อมูลอ้างอิงเกี่ยวกับตัวผู้ใช้ terminal

- Parallel operation เป็นการสอบทานความถูกต้องของโปรแกรมงานที่จะนำมาใช้ โดยนำโปรแกรมนี้ไปประมวลผลด้วยข้อมูลจริง แต่ยังคงให้มีการทำงานแบบเดิมควบคู่กันไป ทั้งนี้เพื่อนำผลของการประมวลผลมาเปรียบเทียบหาข้อแตกต่าง ตลอดจนจุดบกพร่องที่อาจเกิดขึ้น

4. ปัญหาที่บรรดาศูนย์คอมพิวเตอร์ต่าง ๆ ส่วนใหญ่ประสบ และอาจนำไปสู่การทุจริต

4.1 พึ่งพาอาศัยผู้จำหน่ายคอมพิวเตอร์มากเกินไป

การหวังความช่วยเหลือจากผู้จำหน่ายคอมพิวเตอร์ในการศึกษาและวางระบบงานให้ โดยรักษาผลประโยชน์ของลูกค้าอย่างเต็มที่นั้นไม่มีทางเป็นจริงได้ แต่อย่างไรก็ดีหน่วยงานที่กำลังจะหันมาใช้คอมพิวเตอร์นั้นยากนักที่จะมีทีมงานที่มีความรู้ความสามารถพอที่จะวางแผนและออกแบบระบบงานได้เอง การเพิ่มจำนวนอย่างรวดเร็วของศูนย์คอมพิวเตอร์นั้น ทำให้การให้ความช่วยเหลือด้านต่าง ๆ จากผู้จำหน่ายคอมพิวเตอร์ทำได้ไม่เต็มที่

4.2 วางแผนตระเตรียมจัดตั้งศูนย์คอมพิวเตอร์ไว้ไม่ดีพอ

มีศูนย์คอมพิวเตอร์หลายแห่งที่ดำเนินงานได้อย่างขลุกขลัก เนื่องมาจากศึกษาและวางแผนไว้ง่าย ๆ ไม่กำหนดระบบงานที่จะต้องมีให้แน่ชัด จัดหาเครื่องคอมพิวเตอร์มาก่อนศึกษาระบบงานและหาบุคลากร ขาดการติดตามเอาใจใส่จากฝ่ายบริหาร

4.3 เน้นค่าใช้จ่ายเกี่ยวกับเครื่องคอมพิวเตอร์และบุคลากรด้านนี้มากเกินไป

ให้ความสนใจเฉพาะค่าใช้จ่ายด้านคอมพิวเตอร์ที่เกิดขึ้นตามรายงาน โดยไม่ให้ความสนใจกับค่าใช้จ่ายที่ต้องสูญเสียไปอันเนื่องมาจากระบบงานไม่มีประสิทธิภาพ และการทำงานไม่ได้ตามเป้าหมาย เช่น การทำงานที่มีความสำคัญน้อย ปริมาณงานไม่มากนัก ความต้องการเร่งด่วนไม่มี แต่ผู้จัดการศูนย์ประมวลผลซึ่งอาจเป็นผู้ผูกขาดในการตัดสินใจเพียงผู้เดียวในบางองค์กร ก็ตัดสินใจทำให้เพื่อสนองความต้องการของผู้ใช้ ซึ่งบางครั้งก็ตั้งใจเพียงทดสอบสมรรถภาพของเครื่องคอมพิวเตอร์ เพื่อหาประสบการณ์ให้กับตนเองเพิ่มขึ้นเท่านั้น

4.4 ออกแบบระบบงานง่าย ๆ เพียงระดับพื้นฐาน

มีระบบงานจำนวนมากที่โดยเนื้อแท้แล้วเป็นเพียงการใช้คอมพิวเตอร์ทำงานแบบเดียวกับที่ระบบเดิมเคยทำอยู่แล้ว มากกว่าที่จะออกแบบให้คอมพิวเตอร์ทำงานที่ไม่เคยทำมาก่อน และไม่ได้คำนึงถึงระบบการควบคุม และไม่ได้จัดทำร่องรอยการตรวจสอบ หรือการติดตามงานที่ส่วนต่าง ๆ อย่างมีประสิทธิภาพ ซึ่งเป็นปัจจัยสำคัญนำไปสู่ความเสียหายต่าง ๆ ขององค์กรที่เสียหายมาก ๆ ก็คือ การทุจริต หรือระบบถูกทำลาย

4.5 ผู้สอบบัญชีหรือผู้ตรวจสอบภายในไม่มีบทบาทในการร่วมพัฒนางานมาตั้งแต่ต้น

4.6 ประสบความล้มเหลวเมื่อนำระบบงานออกใช้ หรือใช้ได้ไม่สมบูรณ์

ความยุ่งยากในช่วงนำระบบงานออกใช้นั้น มักจะถูกประเมินต่ำไป เพราะผู้ใช้ข้อมูล (user) ขาดการเอาใจใส่ในช่วงพัฒนาระบบงาน ทำให้ไม่ตระหนักว่าพวกเขาเองก็เป็นส่วนหนึ่งของระบบงาน ผู้มีความคิดเห็นต่อต้านระบบงานใหม่ไม่ได้รับการชี้แจงทำความเข้าใจอย่างเพียงพอ และผู้บริหารระดับสูงไม่ให้ความสนใจเท่าที่ควร

4.7 ประโยชน์ด้านการบริหารงานถูกจำกัด

ผู้วิเคราะห์ระบบงานซึ่งมีความชำนาญด้านเทคนิคด้านคอมพิวเตอร์ด้านเดียว ยากที่จะเข้าใจความต้องการของฝ่ายบริหาร และสิ่งที่จะมีประโยชน์ต่อการบริหารงาน ฝ่ายบริหารก็ไม่ทราบว่าคอมพิวเตอร์จะช่วยงานอะไรได้บ้าง และผู้บริหารระดับสูงบางแห่งกลับไม่ได้รับการพิจารณาว่าเป็นผู้ใช้ข้อมูล (user)

5. บทบาทของฝ่ายบริหารที่มีต่อคอมพิวเตอร์ และสาเหตุที่ผู้บริหารไม่ให้ความสำคัญต่อผู้ตรวจสอบด้านคอมพิวเตอร์

5.1 บทบาทของฝ่ายบริหารที่มีต่อคอมพิวเตอร์

5.1.1 ฝ่ายบริหารระดับสูงส่วนใหญ่มีความเข้าใจเกี่ยวกับคอมพิวเตอร์น้อยมาก แม้ในธนาคารบางแห่งที่ใช้คอมพิวเตอร์เอง ในต่างประเทศเองก็มีปัญหานี้ ทางธนาคารบางแห่งจัดให้มีการอบรมพนักงานบริหารระดับสูง แต่ก็ล้มเหลว เพราะผู้บริหารมักไม่ทนรับฟังคำบรรยายที่ฟังแล้วเกิดอาการง่วงนอน และมีความสับสนในเทคนิคทางด้านคอมพิวเตอร์จนจบ และมักอ้างว่ามีงานอื่นที่สำคัญกว่า

5.1.2 ฝ่ายบริหารมักโยนภาระรับผิดชอบด้านคอมพิวเตอร์ไปให้ผู้จัดการฝ่ายคอมพิวเตอร์ และหวังให้ฝ่ายคอมพิวเตอร์เป็นผู้วางแผนและดำเนินการเอง

5.1.3 ผู้บริหารของหน่วยงานที่ใช้ข้อมูล (user) ไม่ตระหนักว่า ตามปกติแล้วตนต้องรับผิดชอบด้านการปฏิบัติงานและคุณภาพของข้อมูล

5.1.4 ผู้บริหารระดับสูงมักจะอนุมัติหรือไม่อนุมัติโครงการตั้งแต่เริ่มแรกเท่านั้น ไม่กำหนดแนวทางและคอยชี้นำต่อไปอีก

5.2 สาเหตุที่ผู้บริหารไม่ให้ความสำคัญต่อผู้ตรวจสอบด้านคอมพิวเตอร์ คือ

5.2.1 ผู้บริหารไม่เข้าใจถึงระบบการทำงานของเครื่องคอมพิวเตอร์จึงไม่ต้องการเกี่ยวข้องในเรื่องต่าง ๆ ที่เกี่ยวกับระบบคอมพิวเตอร์

5.2.2 ผู้บริหารมีความพอใจในระบบงานที่จัดทำขึ้นโดยผู้พัฒนาระบบงาน และสามารถนำระบบงานนั้นไปใช้งานตามเป้าหมายที่วางไว้ โดยไม่สนใจว่าระบบงานนั้นมีข้อบกพร่องหรือไม่

5.2.3 ผู้บริหารเชื่อมั่นในความรู้ความสามารถของเจ้าหน้าที่ด้านคอมพิวเตอร์มากกว่าผู้ตรวจ-สอบด้านคอมพิวเตอร์ และไม่สนใจว่าระบบงานบางอย่างผู้พัฒนาระบบงานจะต้องมีความรู้ด้านอื่นด้วย เช่น ความรู้ด้านบัญชี เป็นต้น

5.2.4 ผู้บริหารองค์กรมีความเห็นอย่างคลาดเคลื่อนว่า หน้าที่ของผู้ตรวจสอบด้านคอมพิว-เตอร์เพียงเพื่อค้นหาการทุจริตที่เกิดจากการใช้คอมพิวเตอร์เท่านั้น โดยไม่คำนึงถึงวิธีการป้องกันความเสียหายอันเนื่องมาจากการใช้ระบบคอมพิวเตอร์ในการประมวลผลไม่ถูกต้อง หรือเนื่องจากการละเลยขั้นตอนการปฏิบัติงานบางอย่าง ซึ่งก่อให้เกิดความเสียหายได้เช่นกัน

6. อาชญากรรมทางเทคโนโลยี (คอมพิวเตอร์)

การขยายตัวอย่างรวดเร็วของวิทยาการคอมพิวเตอร์ในวงการธุรกิจ โดยเฉพาะธนาคารพาณิชย์และสถาบันการเงิน เป็นความหวังใหม่ที่ผู้บริหารในองค์กรจะเอาชนะใจลูกค้า/ประชาชน โดยการให้บริการที่รวดเร็ว แปลกใหม่ที่องค์กรอื่นที่ประกอบธุรกิจประเภทเดียวกันยังทำไม่ได้

6.1 พัฒนาการทางคอมพิวเตอร์ 3 ประการ ที่ทำให้อาชญากรรมทางเทคโนโลยี เพิ่มขึ้น

6.1.1 การแพร่หลายของเครื่องคอมพิวเตอร์ขนาดเล็กในราคาต่ำ

6.1.2 อัตราเติบโตของการใช้เครื่องคอมพิวเตอร์เป็นไปอย่างกว้างขวาง อาชญากรยุคใหม่ที่มาในคราบของพนักงานระดับสูงในห้องแอร์ก็เพิ่มมากขึ้น โดยเฉพาะคอมพิวเตอร์ระบบรวมศูนย์ที่สามารถใช้ผ่านโทรศัพท์สายตรงติดต่อได้ ยิ่งเปิดโอกาสให้อาชญากรคอมพิวเตอร์สามารถใช้เครื่องคอมพิวเตอร์ส่วนตัวเข้าถึงข้อมูลอันมีค่าอย่างสะดวก

6.1.3 การแพร่หลายของการศึกษาด้านคอมพิวเตอร์ในโรงเรียนสถาบันต่าง ๆ ได้สอนให้คนที่ฉลาดอยู่แล้วฉลาดยิ่งขึ้น และสามารถนำมาใช้ในทางผิด ๆ เช่น เมื่อรู้จุดอ่อนของระบบรักษาความปลอดภัยของคอมพิวเตอร์แล้ว

6.2 คนฉลาดกว่าคอมพิวเตอร์

การที่ใคร ๆ ก็สามารถเป็นเจ้าของเครื่องคอมพิวเตอร์เล็ก ๆ แต่มีประสิทธิภาพสูงได้ง่าย ๆ และส่วนมากก็สามารถพ่วงติดต่อเข้าถึงเครื่องคอมพิวเตอร์ใหญ่ โดยระบบสื่อสารทางสายโทรศัพท์ ทำให้แนวโน้มของผู้ประกอบอาชญากรรมทางด้านคอมพิวเตอร์ลดลงไปถึงระบบเสมียนพนักงานผู้ที่ไม่ซื่อสัตย์ต่อองค์กร อาจเปลี่ยนหรือปลอมแปลงฐานะความมั่นคงของลูกค้าขององค์กร หรือผู้ที่ต้องการได้ หากรู้ถึงระบบงานและจุดอ่อนของการเข้าถึงระบบงานนั้น ๆ

6.3 การควบคุมภายในขาดประสิทธิภาพ

การที่ผู้บริหารระดับสูง และหรือผู้มีส่วนรับผิดชอบในการบริหารงานด้านคอมพิวเตอร์ขาดความเอาใจใส่ในด้านการควบคุมภายในอย่างเพียงพอ ก็มีส่วนสำคัญที่เพิ่มอาชญากรรมทางคอมพิวเตอร์ และนำความสูญเสียอย่างใหญ่หลวงมาให้แก่องค์กรได้ทั้งสิ้น



บทที่ 4

การทุจริตทางคอมพิวเตอร์ และการทุจริตโดยใช้คอมพิวเตอร์ เป็นเครื่องมือ

การทุจริตทางคอมพิวเตอร์และ การทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือ

1. การทุจริตทางคอมพิวเตอร์

ผู้เขียนมีความรู้สึกค่อนข้างลำบากใจในการที่จะเขียนรายละเอียดในเรื่องการ ทุจริตด้านคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งการเขียนจากประสบการณ์ที่ได้เกิดขึ้นจริง ๆ แล้ว หรือโอกาสที่ผู้เขียนค่อนข้างแน่ใจว่าจะเกิดขึ้นได้ในอนาคตภายในองค์กรที่ใช้คอมพิวเตอร์ โดยเฉพาะในเรื่องที่เกี่ยวกับวิธีการทุจริตในสถาบันการเงิน ทั้งในวงการธนาคารพาณิชย์และสถาบันการเงินโดยทั่วไป ทั้งนี้เพราะเรื่องดังกล่าวอาจพิจารณาได้ทั้งในแง่ลบและในแง่บวก กล่าวคือ หากผู้อ่าน ผู้ฟัง มีโอกาสพิจารณานำไปใช้ในทางป้องกันก็เป็นสิ่งดี แต่ในทางตรงกันข้ามผู้ไม่ประสงค์ดีก็อาจนำไปทดลองใช้เป็นแบบอย่างในการทุจริตก็ย่อมจะกระทำได้เช่นกัน โดยเฉพาะอย่างยิ่งในทัศนะของผู้เขียนรู้สึกเป็นห่วงและเป็นกังวลแทนผู้บริหารระดับสูง แต่ในขณะเดียวกันก็มีความเห็นใจต่อผู้บริหารระดับสูงด้วยเช่นกันว่า คอมพิวเตอร์ได้ก้าวเข้ามามีบทบาทในวงการธุรกิจ โดยเฉพาะธนาคารพาณิชย์และสถาบันการเงินในอัตราการเติบโตที่เร็วมาก ผู้บริหารส่วนใหญ่ปรับตัวไม่ทันกับการเปลี่ยนแปลงชนิดนี้ เพราะมีงานประเภทอื่นอีกมากที่ผู้บริหารต้องรับผิดชอบ ครั้นจะให้ความสนใจก็มักจะพบกับความน่าเบื่อหน่ายในเรื่องที่เป็นเทคนิค และระบบงานคอมพิวเตอร์ที่ค่อนข้างเข้าใจได้ไม่ง่ายนัก หากจะศึกษากันให้ถึงขั้นระดับสั่งงานหรือควบคุมงานในด้านนี้ได้โดยตรงและอย่างได้ผล

ดังนั้น โอกาสที่พนักงานระดับปฏิบัติงานจะมีโอกาสกระทำการทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือหรืออาศัยจุดอ่อนของระบบงาน หรือจุดอ่อนของการปฏิบัติงานและการควบคุมภายในองค์กรที่ใช้คอมพิวเตอร์ในทางทุจริตก็มีโอกาสมากกว่าการป้องกันด้านนี้โดย ฝ่ายบริหาร โดยเฉพาะอย่างยิ่งถ้าหากผู้อ่านได้ติดตามอ่านปัญหาของสถาบันการเงินหรือองค์กรอื่นที่ใช้คอมพิวเตอร์ตามที่ได้ลำดับมาในตอนต้น ก็จะพบกับสัญญาณอันตรายของการทุจริตทางคอมพิวเตอร์ในทัศนะของผู้เขียนได้บ้างพอสมควร จึงขอสรุปเรื่องคอมพิวเตอร์กับการทุจริตในวงการสถาบันการเงินโดยใช้เรื่องข้างต้นประกอบเป็นสำคัญ ดังนี้

2. สาเหตุการทุจริต

มีองค์ประกอบที่สำคัญ 3 ประการ คือ

2.1) ความประพฤติส่วนตัวของผู้ไม่รักดี และ

2.2) องค์กรมีจุดอ่อนในด้านระบบงานและการควบคุมภายใน และ

2.3) ผู้ปฏิบัติงานมีโอกาสทุจริตได้

2.1 ความประพฤติส่วนตัวของผู้ไม่รักดี ได้แก่

- การเล่นการพนันและหมกมุ่นในอบายมุข
- ความทะเยอทะยานจนเกินควร

- ใช้จ่ายเกินฐานะ
- ไม่ภักดีต่อองค์กร
- มีความต้องการจะทุจริต หรือต้องการทดลองวิชาในทางที่มิชอบ

2.2 องค์กรมีจุดอ่อนในด้านระบบงานและการควบคุมภายใน

2.2.1) จุดอ่อนในขั้นตอนพัฒนาระบบงาน

- ผู้วิเคราะห์ระบบงานไม่เข้าใจระบบงานที่แท้จริงที่ตนกำลังจะพัฒนาทั้งระบบ
- ไม่ได้ประเมินความเสี่ยงของการปฏิบัติงานไว้ในแต่ละขั้นตอนของการออกแบบงาน
- ไม่ได้กำหนดขั้นตอนการควบคุมและวิธีการตรวจสอบให้แน่ชัดไว้ในแต่ละกระบวนการประมวลข้อมูลและกระบวนการปฏิบัติงาน
- ผู้ใช้และผู้บริหารไม่รู้ความต้องการที่แท้จริงของตนที่จะได้รับจากระบบงานด้านคอมพิวเตอร์ ทำให้ต้องมีการแก้ไขระบบงานกันบ่อย ๆ
- ผู้ตรวจสอบภายในมิได้มีโอกาสร่วมพัฒนาระบบงานตั้งแต่ต้น

2.2.2) จุดอ่อนในขั้นตอนการปฏิบัติงาน

- ผู้ใช้ระบบ เช่น Teller หรือ Supervisor ไม่ทราบว่าตนจะต้องทำอะไรบ้างเมื่อมีปัญหา หรือมีกรณีการปฏิบัติงานที่ผิดไปจากการปฏิบัติงานตามปกติ
- ผู้ใช้เชื่อระบบคอมพิวเตอร์มากเกินไป
- ผู้ใช้เข้าใจผิดว่าความถูกต้องของข้อมูลที่ประมวลด้วยระบบคอมพิวเตอร์ หากมีข้อผิดพลาดขึ้นมาก็ไม่ใช่ความรับผิดชอบของตน
- ผู้ควบคุมไม่เอาใจใส่งานเท่าที่ควร ไม่ปฏิบัติตามกฎเกณฑ์
- ระบบงานที่พัฒนาขึ้นมาใหม่เพื่อใช้คอมพิวเตอร์ถูกนำมาใช้งาน โดยมิได้มีการทดสอบจนเป็นที่พอใจของผู้ใช้และผู้ตรวจสอบก่อนเมื่อนำงานนั้นมาใช้แล้วก็ไม่มีผู้รับผิดชอบโดยตรง

2.2.3) จุดอ่อนในด้านการตรวจสอบ

- ผู้ตรวจสอบขาดความรู้และประสบการณ์ทางด้านการตรวจสอบงานที่ใช้คอม-พิวเตอร์
- ผู้ตรวจสอบอยู่ภายใต้การบังคับบัญชาของผู้พัฒนาระบบงานไม่ว่าทางตรงหรือทางอ้อม
- ไม่ได้เข้าไปมีส่วนร่วมกำหนดจุดควบคุมและวิธีการตรวจสอบในขั้นตอนพัฒนาระบบงาน
- ผู้ตรวจสอบมิได้ติดตามผลและ/หรือปัญหาในการปฏิบัติงานอย่างใกล้ชิด
- ผู้รับผิดชอบไม่กำหนดแผนงานและจัดทำคู่มือการตรวจสอบให้เหมาะสม
- ผู้รับผิดชอบเกรงใจต่อผู้จัดการฝ่ายพัฒนาระบบงาน

2.2.4) จุดอ่อนในการบริหาร

- ขาดการติดตามผลการปฏิบัติงาน
- ไม่ให้ความสำคัญของการตรวจสอบงานด้านคอมพิวเตอร์เท่าที่ควร
- เน้นและให้ความสำคัญต่อการพัฒนาระบบงานใหม่ ๆ เร็วเกินกว่าเวลาที่ควร

2.2.5) ผู้ปฏิบัติงานมีโอกาสทุจริตได้

- การปฏิบัติงานที่ขึ้นอยู่กับการเชื่อใจในความสุจริตของพนักงานเป็นสำคัญ
- ผู้บริหารหรือผู้ควบคุมไม่เข้าใจระบบงานและกฎเกณฑ์การควบคุม
- องค์กรมีจุดอ่อนในด้านระบบงานและการควบคุมภายใน

2.3 จุดที่สามารถจะทุจริตได้

- การทุจริตทางด้าน Input
- การทุจริตทางด้าน Processing
- การทุจริตทางด้าน Output

2.4 ประเภทของการทุจริตทางด้านคอมพิวเตอร์ในวงการสถาบันการเงิน ซึ่งจะมีรายละเอียดพอสมควรประกอบในเรื่องต่อไปนี้ในบทต่อ ๆ ไป คือ

2.4.1) ประเภทการทุจริตทางด้าน Input

- กรณีการทุจริตที่ได้เกิดขึ้นแล้วในประเทศ
- กรณีการทุจริตที่ได้เกิดขึ้นแล้วในต่างประเทศ
- กรณีการทุจริตที่มีโอกาสจะเกิดขึ้นได้ภายในประเทศในอนาคต

2.4.2) ประเภทการทุจริตทางด้าน Processing

- กรณีการทุจริตที่ได้เกิดขึ้นแล้ว
- กรณีการทุจริตที่มีโอกาสจะเกิดขึ้นได้ภายในประเทศในอนาคต

2.4.3) ประเภทการทุจริตทางด้าน Output

- กรณีการทุจริตที่ได้เกิดขึ้นแล้วในประเทศ
- กรณีการทุจริตที่มีโอกาสจะเกิดขึ้นได้ภายในประเทศในอนาคต

2.5 การป้องกันภัยจากการทุจริต

- การป้องกันทางด้านผู้บริหาร
- การป้องกันทางด้านผู้ให้บริการทางด้านคอมพิวเตอร์
- การป้องกันทางด้านผู้ใช้บริการ

2.6 สาเหตุของการทุจริตของพนักงาน

จากรายงานของตำรวจ เอฟ.บี.ไอ. สาขาการธนาคาร (F.B.I. Banking) ได้สรุปพฤติกรรมของพนักงานที่ทุจริตไว้ ดังนี้

ร้อยละ 70 เป็นพนักงานชาย

ร้อยละ 20 เป็นพนักงานหญิง

ร้อยละ 10 เป็นพนักงานสองเพศ (เพราะมีจำนวนน้อย)

สาเหตุที่พนักงานทุจริตแยกได้แต่ละเพศ ดังนี้

พนักงานชาย สาเหตุเรียงตามลำดับความสำคัญไว้ดังนี้

1. เล่นการพนัน 60%
2. เป็นบุรุษเจ้าสำราญ หลงใหลในเพศตรงข้าม 20%
3. ใช้จ่ายเงินเกินตัว รายได้น้อยแต่รสนิยมสูง 7.5%
4. อิทธิพลของเพศตรงข้าม 7.5%
5. ความจำเป็นในการครองชีพ 1.0%
6. สิ่งแวดล้อม พื้นฐานทางครอบครัว และอื่น ๆ 4.0%

พนักงานหญิง จะมีสถิติทุจริตน้อยกว่าพนักงานชาย สาเหตุใหญ่ที่ทำให้พนักงานหญิงทุจริตต่อหน้าที่ เป็นเพราะ

(1) ความจำเป็นในครอบครัว บุตร หรือสามีเจ็บป่วย 60%

(2) ความรักสวยรักงาม และต้องการเป็นคนนำสมัยในด้านแฟชั่น การแต่งกาย เครื่องประดับ และอื่น ๆ ที่ทำให้รู้สึกว่าเป็นบุคคลเด่นในสังคม 20%

(3) อิทธิพลของเพศตรงข้าม 15%

(4) สภาพแวดล้อม พื้นฐานทางครอบครัว 3%

(5) ไม่ทราบสาเหตุ 2%

การทุจริตโดยใช้คอมพิวเตอร์

คอมพิวเตอร์เป็นเครื่องมือที่มีประสิทธิภาพในการทำงาน เพียงแต่ต้องอยู่ภายใต้การบงการของมนุษย์ ผู้ใดก็ตามที่เข้าใจภาษาของคอมพิวเตอร์ก็สามารถสื่อสารกับคอมพิวเตอร์ได้ ดังนั้นคอมพิวเตอร์จึงกลายเป็นเครื่องมือที่มีคุณอนันต์กับองค์การ ในกรณีที่จัดทำข้อมูลให้ผู้บริหารองค์การได้ใช้ตัดสินใจ แต่ก็เป็นโทษอย่างมหันต์ต่อองค์การ ถ้ามีผู้ใช้คอมพิวเตอร์เพื่อประโยชน์ของบุคคลนั้น



การทุจริตเกี่ยวกับคอมพิวเตอร์

1. ยักยอกเวลาและวัสดุอุปกรณ์คอมพิวเตอร์
2. การเปลี่ยนแปลงแก้ไขหรือปลอมแปลงข้อมูลเข้า
3. การปลอมแปลงแก้ไขแฟ้มข้อมูล
4. การปลอมแปลงแก้ไขโปรแกรม
5. การนำโปรแกรมส่วนตัวมาแอบใช้แทนโปรแกรมในระบบ
6. การลักลอบตัดข้อมูลในข่ายโทรคมนาคม
7. การขโมยแฟ้มข้อมูลหรือโปรแรกม
8. การใช้อุปกรณ์คอมพิวเตอร์ในทางทุจริต
9. การใช้คอมพิวเตอร์เป็นแพะรับบาป หรือโฆษณาหลอกลวง
10. การใช้คอมพิวเตอร์เป็นเครื่องมือชู่กรรโชก
    อื่น ๆ



บทที่ 5

รูปแบบการทุจริตทางคอมพิวเตอร์
(และตัวอย่างที่เกี่ยวข้อง)

รูปแบบการทุจริตทางคอมพิวเตอร์ (และตัวอย่างที่เกี่ยวข้อง)

วิธีการทุจริตทางคอมพิวเตอร์ที่จะกล่าวถึงต่อไปนี้ เป็นวิธีการที่ผู้มีความรู้ทางเทคนิคด้านคอมพิวเตอร์นำมาใช้ บางวิธีเป็นเรื่องที่ค่อนข้างยากสำหรับผู้ที่ไม่มีความรู้ถึงระดับเชี่ยวชาญ อย่างไรก็ดี ณ ที่นี้จะไม่กล่าวถึงรายละเอียดที่ซับซ้อนจนเกินไป

การทุจริตทางคอมพิวเตอร์ทุกครั้งจะเป็นเรื่องที่เกี่ยวข้องกับข้อมูลหรือโปรแกรม เช่น การเปลี่ยนแปลง แก้ไข เปิดเผย หรือนำไปใช้ ทำลาย และใช้หรือปฏิเสธการใช้บริการ อุปกรณ์คอมพิวเตอร์ โปรแกรม หรือข้อมูลอย่างใดอย่างหนึ่งในระบบคอมพิวเตอร์

วิธีการทุจริตทางคอมพิวเตอร์อาจสรุปได้ 12 วิธี คือ

1. Data Diddling
2. Trojan Horse
3. Salami Techniques
4. Superzapping
5. Trap Doors
6. Logic Bombs
7. Asynchronous Attacks
8. Seaverging
9. Data Leakage
10. Piggybacking and Impersonation
11. Wiretapping
12. Simulation and Modeling

1. Data Diddling

การทุจริตโดยวิธีนี้เป็นวิธีที่ง่ายที่สุด ลงทุนน้อยที่สุด และมักพบเสมอ ๆ ผู้ทุจริตจะเปลี่ยนแปลงข้อมูลก่อนหรือระหว่างการนำเข้าประมวลผล เช่น

- ปลอมแปลงเอกสารขั้นต้น
- สับเปลี่ยนสื่อข้อมูลนำเข้า เช่น เทป บัตร หรือจานแม่เหล็ก
- ฝ่าฝืนวิธีการตรวจสอบความถูกต้อง เจาะรูบัตรให้แตกต่างจากข้อมูลที่ถูกต้อง หรือหลีกเลี่ยงวิธีการควบคุมที่กำหนดขึ้นสำหรับตรวจสอบความถูกต้องของข้อมูลนำเข้า

ผู้ที่ทำการทุจริตแบบนี้มักจะทำหน้าที่เกี่ยวกับข้อมูลขั้นต้นก่อนการนำเข้า เช่น การจัดทำเอกสารขั้นต้น การบันทึกหรือส่งข้อมูล เข้ารหัสข้อมูล ตรวจสอบความถูกต้องแปลงรูปแบบข้อมูลเพื่อให้คอมพิวเตอร์นำไปประมวลผลได้

วิธีการควบคุมข้อมูลขั้นต้นโดยทั่วไปมักใช้บุคคลควบคุม ได้แก่

ให้มีผู้ลงนามในช่องผู้ทำ ผู้ตรวจ ผู้อนุมัติ ซึ่งต้องแบ่งแยกหน้าที่โดยชัดเจนเพื่อให้การทุจริตทำได้ลำบากยิ่งขึ้น เนื่องจากต้องอาศัยการร่วมมือจากบุคคลหลายฝ่าย หรือโดย

การควบคุมยอดรวมของชุดข้อมูลขั้นต้น โดยบวกยอดรวมชุดข้อมูลด้วยมือและมีผู้เปรียบเทียบกับยอดที่คอมพิวเตอร์รวมให้ เพื่อดูว่ามีผลต่างหรือไม่ นอกจากนี้อาจใช้

check digit เพื่อตรวจสอบหรือใส่ตัวอักษรตัวใดตัวหนึ่งไว้ในฐานข้อมูลเพื่อเช็คสอบกับ field ในข้อมูล (เช่น odd/even number หรือ hash totals)

การให้กำหนดลำดับที่ของข้อมูลหรือเวลานำข้อมูลส่ง เพื่อป้องกันการนำข้อมูลบางส่วนออกจากชุดหรือสลับลำดับข้อมูล

สำหรับกิจการที่มีปริมาณข้อมูลมาก อาจใช้โปรแกรม utility หรือโปรแกรมควบคุมโดยเฉพาะการตรวจสอบการทุจริตโดยวิธีนี้ทำได้โดยเปรียบเทียบกับข้อมูลขั้นต้น

2. Trojan Horse

การทุจริตวิธีนี้เป็นการซ้อนคำสั่งไว้ในโปรแกรม เพื่อให้ทำการตามที่ผู้เขียนโปรแกรมต้องการ โดยโปรแกรมยังคงปฏิบัติงานได้ตามวัตถุประสงค์ที่ระบบกำหนดไว้ ผู้ทุจริตอาจซ่อนคำสั่งไว้ใน production program เพื่อป้องกันมิให้ผู้อื่นล่วงรู้ หรือซ่อนไว้ในส่วนหนึ่งของโปรแกรมที่กำหนดให้ใช้ประมวลผลแฟ้มข้อมูล ซึ่งมีการควบคุมให้ใช้กับส่วนของโปรแกรมนั้นเท่านั้น ผู้เขียนโปรแกรมจะเขียนขึ้นโดยเปิดช่องทางหรือที่ว่างให้สามารถสอดแทรกคำสั่งที่ตนต้องการเข้าไปได้

ตัวอย่างการทำงานของ Trojan Horse แบบง่าย ๆ คือ ผู้ทุจริตซึ่งเป็นพนักงานเขียนโปรแกรมได้ซ่อนคำสั่งไว้ใน utility program เพื่อให้สามารถเข้าถึงและใช้คำสั่งในระบบทุกคำสั่งในทุกส่วนของหน่วยความจำ ซึ่งตามปกติ จะจำกัดให้ทำได้เฉพาะเจ้าหน้าที่ผู้รับมอบอำนาจเท่านั้น

ตามปกติการทุจริตโดยวิธีนี้ไม่สามารถป้องกันหรือตรวจพบได้ โดยเฉพาะในกรณีที่ผู้เขียนโปรแกรมเป็นผู้ที่มีประสบการณ์และความรู้มาก ทั้งนี้เนื่องจากระบบงานทั่ว ๆ ไปจะประกอบด้วยคำสั่งต่าง ๆ และข้อมูลที่มีปริมาณสูงเกินกว่าที่จะทุ่มเทความพยายามค้นหาการทุจริตในลักษณะนี้ได้ Trojan horse อาจซ่อนตัวอยู่ในคำสั่งใน operating system ซึ่งมีอยู่ 5-6 ล้านคำสั่งก็ได้ คำสั่งดังกล่าวใช้เวลาทำงานเพียงไม่กี่ mili-second หลังจากนั้นผู้ทุจริตก็จะนำออกจาก operating system โดยไม่มีร่องรอยให้ติดตามได้เลย นอกจากจะมีเหตุบังเอิญ เช่น ผู้ทุจริตยังคงวางใจว่าไม่มีใครรู้ และแสวงหาผลประโยชน์จนเกิดผลกระทบกับข้อมูลอื่น ทำให้มีการสอบสวนสาว

หลักฐานไปหาตัวบุคคลที่อยู่ในข่ายที่จะทำการทุจริตได้ เช่น พนักงานโปรแกรมที่มีความชำนาญในการแก้ไข utility program ซึ่งอาจเข้าถึงระบบได้ พนักงานของบริษัทที่ให้บริการด้วย software ที่ปรึกษา หรือบุคคลที่เกี่ยวข้องอื่น ๆ

การตรวจสอบวิธีหนึ่งอาจทำโดยการเปรียบเทียบโปรแกรมที่ใช้งานกับชุดต้นฉบับ หรือชุดที่เชื่อว่าจะไม่ถูกแก้ไข สำหรับโปรแกรมชุดสำรองอาจเป็นชุดที่ไม่ทันสมัย ยิ่งไปกว่านั้นอาจถูกผู้ทุจริตลักลอบแก้ไขให้ตรงกับชุดที่ใช้งานจริงแล้วก็ได้ การใช้ utility program เปรียบเทียบโปรแกรมเป็นวิธีที่สะดวกวิธีหนึ่ง แต่จะต้องคำนึงถึงผลกระทบต่อระบบคอมพิวเตอร์ด้วยหากองค์กรใช้วิธีนี้ควรให้ทำได้เฉพาะเจ้าหน้าที่ที่มีความชำนาญจริงและไว้วางใจได้เท่านั้น

การทดสอบโปรแกรมด้วยข้อมูลทดสอบภายใต้เงื่อนไขที่กำหนด อาจช่วยให้พบการทุจริตแบบนี้ได้ แต่โอกาสที่จะพบมีน้อยมาก นอกจากทราบสถานการณ์ล่วงหน้ามาก่อน อย่างไรก็ดีแม้จะทราบว่ามีการทุจริตจริง แต่ก็ไม่สามารถทราบจุดที่คำสั่งนี้ซ่อนตัวอยู่ นอกจากนี้คำสั่ง Trojan horse อาจอยู่ใน source language หรือใน object form ซึ่งจะแทรกเข้าไปใน object form เมื่อมีการ assemble หรือ compile แต่ละครั้งเท่านั้น

3. Salami Techniques

การทุจริตโดยวิธีนี้ เป็นการยักยอกเงิน สินค้าหรือบริการจากหลายแหล่ง ๆ ละเล็กละน้อยซึ่งผลรวมเมื่อเวลาผ่านไปนาน ๆ ก็จะเป็นจำนวนสูง เช่น ระบบบัญชีเงินฝากกระแสรายวัน ซึ่งมีบัญชีเงินฝากของลูกค้าจำนวนมาก ผู้ทุจริตอาจใช้วิธีการแบบ Trojan Horse ลบยอดเงินฝากคงเหลือในบัญชีต่าง ๆ จำนวนหนึ่ง เช่น 10-15 เซนต์ แล้วโอนไปเข้าบัญชีของตนเองเพื่อถอนไปใช้ต่อไป การทุจริตวิธีนี้จะไม่มีผลกระทบต่อยอดรวมเงินฝากและไม่มีการฝ่าฝืนมาตรการควบคุมที่กำหนดไว้ด้วย

วิธีการนี้อาจใช้ในขั้นตอนการคำนวณดอกเบี้ยเงินฝาก โดยอาศัยการปัดเศษ

อย่างไรก็ดีการทุจริตวิธีนี้ไม่สู้จะทำให้เกิดผลเสียหายแก่ผู้ที่เกี่ยวข้องมากนัก และกว่าผู้ทุจริตจะได้รับประโยชน์เป็นจำนวนมาก อาจต้องใช้เวลาหลาย ๆ ปี การตรวจสอบเพื่อค้นหาการทุจริตโดยวิธีนี้ทำได้ 2 วิธี คือ ตรวจดูจากคำสั่งในโปรแกรม หรือคำนวณดอกเบี้ยที่บัญชีของพนักงานเขียนโปรแกรมควรได้รับ (ในกรณีที่ทราบว่าเป็นบัญชีใด) แต่วิธีหลังนี้อาจไม่ได้ผลหากผู้ทุจริตนำยอดที่ปัดเศษไปเข้าไว้ในบัญชีอื่นที่เปิดขึ้นเพื่อการนี้

4. Superzapping

การทุจริตวิธีนี้เรียกชื่อตาม utility program ที่มีอยู่ในระบบ IBM โปรแกรมดังกล่าวชื่อ Superzap ซึ่งสามารถใช้ปรับปรุง (modify) หรือเรียกดูเนื้อหา (content) ทุกส่วนในระบบ โปรแกรมนี้โดยปกติจะไม่มีการนำมาใช้เนื่องจากสามารถหลีกเลี่ยงการควบคุมที่มีอยู่ได้ทั้งหมด การใช้งานจะเกิดขึ้นในกรณีที่เกิดเหตุการณ์ผิดปกติในระบบคอมพิวเตอร์ เช่น คอมพิวเตอร์หยุดทำงาน ทำงานผิดปกติ หรือเกิดปัญหาที่ไม่สามารถเข้าไปได้โดยวิธีการ restart หรือการฟื้นฟูระบบขึ้นใหม่ได้

เนื่องจากโปรแกรมนี้มีประสิทธิภาพสูง และเสี่ยงที่จะเกิดความเสียหายหากไปอยู่ในมือของผู้ทุจริต จึงควรอนุญาตให้ใช้ได้เฉพาะนักโปรแกรมระบบ หรือพนักงานควบคุมเครื่องคอมพิวเตอร์ที่ทำหน้าที่บำรุงรักษาโปรแกรมระบบเท่านั้น โปรแกรมนี้ควรเก็บไว้ในที่ที่ปลอดภัยและจำกัดให้เรียกใช้ได้เฉพาะผู้มีอำนาจเท่านั้น

ในสหรัฐอเมริกาเคยมีธนาคารในรัฐ New Jersey ได้รับความเสียหาย $128,000 เนื่องจากผู้จัดการศูนย์คอมพิวเตอร์ใช้โปรแกรมนี้โอนเงินไปเข้าบัญชีของเพื่อนร่วมทุจริต 3 ราย การทุจริตรายนี้กระทำต่อเนื่องกันเป็นเวลานาน เนื่องจากระบบคอมพิวเตอร์ของธนาคารเกิดปัญหา และผู้จัดการศูนย์คอมพิวเตอร์ได้รับคำสั่งจากฝ่ายบริหารให้ใช้โปรแกรมนี้แก้ไขยอดเงินในบัญชีที่ไม่ถูกต้อง หลังจากแก้ไขเรียบร้อยแล้ว ผู้จัดการศูนย์คอมพิวเตอร์จึงได้พบว่า การใช้โปรแกรมนี้จะไม่ปรากฏหลักฐานให้ตรวจสอบใน journal และไม่ต้องมีการควบคุมใด ๆ จึงนำไปทุจริตดังกล่าว ในที่สุดลูกค้าที่ได้รับความเสียหายเรียกร้องให้ธนาคารสอบสวนจนพบสาเหตุ

5. Trap Doors

ระหว่างการดำเนินการพัฒนาโปรแกรมระบบงาน และโปรแกรมควบคุมระบบขนาดใหญ่ นักพัฒนาโปรแกรมมักจะเขียนรหัสคำสั่งเพื่อช่วยให้สามารถเข้าไปแก้ไขข้อผิดพลาดได้ในภายหลังไว้ในโปรแกรม รหัสดังกล่าวจะทำให้นักพัฒนาโปรแกรมเพิ่มเติมคำสั่ง และให้ออกข้อมูลผลลัพธ์ระหว่างกระบวนการพัฒนาตามที่ต้องการได้ รหัสที่ใช้ช่วยในการแก้ไขดังกล่าว เรียกว่า Trap Doors ตามปกติเมื่อมีการตรวจสอบในขั้นสุดท้าย รหัสดังกล่าวจะถูกนำออกจากโปรแกรม แต่บางครั้งอาจละเลยโดยไม่ตั้งใจ หรือโดยตั้งใจให้คงมีอยู่เพื่อสะดวกในการแก้ไขภายหลัง

นอกจากกรณีข้างต้น อาจมีนักพัฒนาโปรแกรมบางคนเขียน Trap Doors ไว้ เพื่อช่วยในการบำรุงรักษาหรือปรับปรุงระบบภายหลัง หรือนักออกแบบโปรแกรมที่มีขนาดใหญ่และซับซ้อนบางคนเจตนาออกแบบให้ logic ของโปรแกรมมีจุดอ่อนด้วย

บางกรณี Trap Doors อาจเกิดจากวงจรไฟฟ้าของเครื่องคอมพิวเตอร์เอง ในกรณีนี้หากนักพัฒนาโปรแกรมเป็นผู้ที่มีประสบการณ์สูง มักจะพบจุดอ่อนและใช้ประโยชน์ในการทำงานตามปกติ แต่บางคนอาจนำไปใช้ในทางทุจริตได้เช่นกัน นอกจากนี้มีหน้าที่ (function) บางอย่างในระบบคอมพิวเตอร์ซึ่งผู้ผลิตไม่ได้ระบุไว้ หน้าที่นี้เรียกว่า negative specification ซึ่งเกิดจากผู้ออกแบบและผู้จัดทำระบบไม่สามารถทำให้โปรแกรมและ function ต่าง ๆ ทำงานได้ตรงตามข้อกำหนด (specifications) โดยครบถ้วน ปัจจุบันนี้ยังไม่มีผู้ใดสามารถให้คำยืนยันได้ว่า ระบบคอมพิวเตอร์ต่าง ๆ ไม่สามารถทำสิ่งที่อยู่นอกเหนือข้อกำหนดได้

นักวิจัยกำลังพยายามอย่างเต็มที่เพื่อหาวิธีพิสูจน์ความถูกต้องของโปรแกรม และการทำงานของคอมพิวเตอร์ว่าเป็นไปโดยถูกต้องตรงตามข้อกำหนดที่ให้ไว้ แต่คาดกันว่าคงต้องใช้เวลาหลายปีกว่าจะสามารถผลิตเครื่องคอมพิวเตอร์และโปรแกรมที่ปราศจากข้อผิดพลาดได้ ดังนั้นจึงกล่าวได้ว่า Trap Doors ยังคงมีอยู่ในปัจจุบัน

ตัวอย่างการทุจริตโดยคอมพิวเตอร์ที่เกิดจาก Trap Doors คือ Trap Doors นั้นมีจุดอ่อนที่ยินยอมให้ผู้เขียนโปรแกรมสามารถเขียนคำสั่งเคลื่อนย้ายการควบคุมที่ใช้กับโปรแกรมไว้ในเนื้อที่ส่วนที่ใช้เก็บข้อมูล ซึ่งทำให้คอมพิวเตอร์ทำงานตามคำสั่งที่ป้อนเข้าไปในรูปของข้อมูล (data) และสามารถสั่งให้โปรแกรมทำงานนอกเหนือจากที่

กำหนดโดยการนำคำสั่งเข้าในรูปดังกล่าวในขณะที่โปรแกรมกำลังทำงาน เหตุข้างต้นเกิดขึ้นในศูนย์คอมพิวเตอร์ที่แบ่งกันใช้เวลา (commercial time-sharing computer service) นักโปรแกรมระบบจึงสามารถใช้จุดบกพร่องนี้ลักลอบใช้เวลาของคอมพิวเตอร์ โดยไม่ต้องเสียค่าใช้จ่าย และลักลอบนำข้อมูลของผู้ใช้รายอื่นไปหาประโยชน์ส่วนตัวด้วย

ตัวอย่างอีกกรณีหนึ่งเกิดขึ้นที่โรงงานรถยนต์ใน Detroit โดยวิศวกรหลายรายพบว่ามี Trap Doors ในระบบคอมพิวเตอร์แบบแบ่งกันใช้เวลา ซึ่งเปิดโอกาสให้รู้รหัสผ่านที่มีอำนาจสูงสุด (priviledge passwords) โดยสามารถเรียกดูรหัสผ่านของประธานบริษัท Time-sharing ดังกล่าว และนำโปรแกรมลับเฉพาะที่ใช้ในงานธุรกิจไปใช้งานโดยไม่ต้องเสียค่าใช้จ่าย

ทั้ง 2 กรณีข้างต้นเป็นการพบ Trap Doors โดยบังเอิญ และไม่มีใครทราบว่ามีผู้ใช้รายอื่นอีกกี่รายที่แสวงหาผลประโยชน์จากจุดอ่อนนี้ ไม่มีเทคนิคใดที่สามารถนำมาใช้ค้นหา Trap Doors ได้ นอกจากผู้ที่เกี่ยวข้องพบว่ามีเหตุการณ์แวดล้อมที่ส่งให้เห็นว่าน่าจะมีจุดอ่อนในลักษณะนี้เกิดขึ้น ซึ่งจะต้องอาศัยนักโปรแกรมควบคุมระบบและนักโปรแกรมระบบงานที่มีความรู้ความชำนาญถึงขั้นเชี่ยวชาญเท่านั้น

6. Logic Bombs

Logic Bombs คือ โปรแกรมที่ลงมือกระทำการบางอย่างในระบบคอมพิวเตอร์ในช่วงเวลาและภายใต้เงื่อนไขหรือสภาวะการณ์ที่เอื้ออำนวยประโยชน์แก่ผู้ทุจริตได้ เช่น การซ่อนคำสั่งไว้ในโปรแกรมควบคุมระบบ Trojan Horses ที่มีการเรียกออกมาใช้เป็นครั้งคราว คำสั่งที่ซ่อนไว้จะตรวจสอบ ปี วันที่ และเวลา ในระบบคอมพิวเตอร์ทุกครั้ง เมื่อตรงกับที่ผู้ซ่อนคำสั่งกำหนดไว้ Logic Bombs จะสั่งให้อุปกรณ์ในคอมพิวเตอร์ทำงานตามต้องการ

กรณีทุจริตรายหนึ่งเกิดขึ้นในระบบงานเงินเดือน พนักงานเขียนโปรแกรมซ่อน Logic Bombs ไว้โดยสั่งให้ทำลายแฟ้มข้อมูลพนักงานทั้งหมดเมื่อชื่อของตนเองถูกลบออกจากสารบบพนักงาน ซึ่งเป็นการเลิกจ้างนั่นเอง

การใช้ Logic Bomb ในการทุจริตมักอาศัยเทคนิค Trojan Horse ซึ่งอาจสั่งให้ทำการบางอย่างภายใต้เงื่อนไขใด ๆ หรือเมื่อมีข้อมูลบางประเภทปรากฏขึ้น

7. Asynchronous Attacks

asynchronous computer เป็นเครื่องคอมพิวเตอร์ประเภทหนึ่งที่จะเริ่มทำงานเมื่อได้รับสัญญาณบอกผลการปฏิบัติการก่อนหน้านี้ แทนที่จะเริ่มทำงานจากสัญญาณนาฬิกา (clock)

การทุจริตวิธีนี้อาศัยการทำงานแบบ asynchronous ในโปรแกรมควบคุมระบบ ซึ่งพอจะอธิบายได้ดังนี้

โปรแกรมควบคุมระบบของคอมพิวเตอร์ ส่วนใหญ่จะมีการทำงานแบบ asynchronous ซึ่งขึ้นอยู่กับลักษณะของระบบงานที่มีอยู่ในระบบคอมพิวเตอร์นั้น ๆ ตัวอย่างเช่น ในขณะใดขณะหนึ่งมีคำสั่งให้ระบบคอมพิวเตอร์จัดทำรายงานข้อมูลผลลัพธ์จากงานหลาย ๆ งานพร้อมกัน ในกรณีเช่นนี้โปรแกรมควบคุมระบบจะเก็บคำสั่งทั้งหมดไว้

และจะสั่งให้พิมพ์รายงานเมื่ออุปกรณ์ต่าง ๆ พร้อมที่จะทำงานได้ หรือเมื่อมีคำสั่งที่มีลำดับความสำคัญสูงกว่าปรากฏ ซึ่งจะเห็นได้ว่าการทำงานในลักษณะนี้ไม่เป็นไปตามลำดับของคำสั่งที่ได้รับ แต่จะขึ้นอยู่กับความพร้อมของอุปกรณ์

มีวิธีการหลายวิธีที่ต้องอาศัยเทคนิคที่ซับซ้อน เพื่อให้การทำงานของโปรแกรมควบคุมระบบเกิดการสับสน และยินยอมให้มีการฝ่าฝืนข้อกำหนดที่ต้องประมวลผลงานใดงานหนึ่งจนเสร็จสิ้นก่อน ตัวอย่างเช่น การประมวลผลข้อมูลในระบบงานขนาดใหญ่ ซึ่งต้องปฏิบัติงานเป็นเวลานาน ๆ จะต้องมีจุดตรวจสอบและเริ่มต้นใหม่ ขั้นตอนนี้จะต้องอาศัยพนักงานปฏิบัติการคอมพิวเตอร์เป็นผู้เปิด-ปิดสวิตช์เพื่อหยุดการทำงานของโปรแกรมตามจุดหยุดที่กำหนดไว้ล่วงหน้า และจะเริ่มทำงานต่อไปอีกโดยไม่ทำให้ข้อมูลเสียหาย การปฏิบัติงานในช่วงนี้โปรแกรมควบคุมระบบจะทำการสำรอง (save) โปรแกรมและข้อมูลต่าง ๆ ตามที่ปรากฏในขณะนั้นไว้ ตลอดจนค่าตัวแปร (parameters) ซึ่งบอกลักษณะของ mode และระดับของการรักษาความปลอดภัย ณ จุดนั้นด้วย ในขั้นตอนนี้จึงเปิดโอกาสให้พนักงานเขียนโปรแกรมหรือพนักงานปฏิบัติการคอมพิวเตอร์เข้าถึงจุดตรวจสอบ และเริ่มต้นใหม่ที่จะคัดลอกหรือสำเนาโปรแกรมข้อมูลและค่าตัวแปรไว้ได้ ทั้งยังอาจเปลี่ยนแปลงค่าตัวแปรของระบบให้เปลี่ยนไปทำงานในระดับที่หวงห้าม (function at a higher priority security level or priviledge level) และทำให้โปรแกรมเข้าถึงข้อมูลโปรแกรม อื่น ๆ หรือโปรแกรมควบคุมระบบโดยไม่ได้รับอนุญาตได้ แต่ทั้งนี้การหยุดตรวจและเริ่มต้นใหม่ทุกครั้งจะได้รับการบันทึกลงใน console log

การเจาะเข้าไปในระบบคอมพิวเตอร์ยังมีวิธีการที่ซับซ้อนมากกว่าที่อธิบายมาแล้ว แต่เป็นเทคนิคที่ซับซ้อนจนไม่สามารถนำมาอธิบายในที่นี้ ข้อที่ผู้ตรวจสอบพึงระวัง คือ มีความเป็นไปได้เพียงใดที่จะเกิดการเจาะเข้าไปในระบบโดยอาศัย asynchronous attacks เมื่อเกิดความสงสัยผู้ตรวจสอบจำเป็นต้องได้รับการช่วยเหลือจากช่วงเวลาใด เช่น งานที่มีความยุ่งยากทางเทคนิคสูง และต้องอาศัยนักเทคนิคที่ฝึกอบรมมาเป็นพิเศษ เป็นต้น หลักฐานที่พอจะเห็นได้จากผลของ asynchronous attack คือ ข้อมูลผลลัพธ์ประสิทธิภาพ หรือการทำงานของระบบแปรเปลี่ยนไปจากที่กำหนดไว้

8. Seaverging

Seaverging หมายถึง การได้รับข้อมูลที่ผ่านการประมวลผลแล้ว ซึ่งอาจปรากฏในรูปแบบที่ดูได้ด้วยตาเปล่า หรือคงค้างอยู่ในระบบคอมพิวเตอร์ภายหลังจาก ประมวลผลงานหนึ่ง ๆ เสร็จเรียบร้อยแล้ว ตัวอย่างง่าย ๆ คือ ชุดสำเนาของรายงานกระดาษคาร์บอนที่ไม่ต้องการใช้และถูกทิ้งไว้ในถังเก็บเศษกระดาษ หรืออาจเป็นการได้รับข้อมูลที่คงค้างอยู่ในระบบคอมพิวเตอร์ก็ได้

การนำข้อมูลที่คงค้างอยู่ในระบบคอมพิวเตอร์ไปใช้ประโยชน์ เกิดขึ้นจากโปรแกรมควบคุมระบบลงเนื้อที่หน่วยความจำที่พักข้อมูล (buffer) ซึ่งใช้เก็บข้อมูลนำเข้าหรือข้อมูลผลลัพธ์ชั่วคราวไม่หมด ระบบคอมพิวเตอร์บางระบบไม่ลงจานหรือเทปแม่เหล็ก เนื่องจากการทำงานในขั้นตอนนี้ต้องเสียเวลา ดังนั้นสื่อดังกล่าวจึงยังคงเก็บข้อมูลเดิมไว้โดยครบถ้วน ทำให้ผู้ปฏิบัติงานอื่นในขั้นตอนต่อมาสามารถอ่านข้อมูลนั้นได้ บางกรณีอาจเกิดจากการลบข้อมูลในหน่วยความจำไม่เรียบร้อย หรือยังคงเหลือบางส่วน เมื่อผู้ปฏิบัติในลำดับถัดมาทำการอ่านข้อมูลภายหลังจากที่ได้บันทึกข้อมูลใหม่ทับลงไป ข้อมูลเดิมส่วนที่เหลืออยู่จึงถูกอ่านออกมาด้วย

กรณีดังกล่าวเคยปรากฏในศูนย์บริการประมวลผลแบบแบ่งกันใช้เวลาใน Texas ซึ่งมีบริษัทน้ำมันจำนวนหนึ่งเป็นลูกค้า พนักงานปฏิบัติการคอมพิวเตอร์สังเกตเห็นว่าทุกครั้งที่บริษัทแห่งหนึ่งใช้คอมพิวเตอร์ จะขอให้บรรจุเทปใช้งานชั่วคราวไว้ในเครื่องขับเทปทุกครั้ง และเมื่อเขาบรรจุลงไปก็สังเกตเห็นไฟสัญญาณอ่าน (read-tape light) สว่างก่อนไฟสัญญาณบันทึกข้อมูลทุกครั้ง ซึ่งแสดงว่าผู้ใช้กำลังอ่านข้อมูลจากหน่วยความจำชั่วคราวก่อนที่จะบันทึกข้อมูลของตนลงไป เมื่อเกิดเหตุการณ์ทำนองเดียวกันหลาย ๆ ครั้ง พนักงานนั้นจึงเกิดความสงสัยและรายงานให้ฝ่ายจัดการทราบ หลังจากการสอบสวนอย่างง่าย ๆ ก็ได้พบความจริงว่า ลูกค้ารายนั้นลอบจารกรรมข้อมูลของบริษัทน้ำมันรายอื่น ๆ ไปขาย

เคยมีกรณีการลักลอบนำรายงานที่เป็นกระดาษต่อเนื่องไปเปิดเผย และเจ้าหน้าที่ของ FBI สามารถสืบหาตัวผู้ทุจริตได้โดยอาศัยหลักฐานที่มีอยู่ในกระดาษ คือ ชื่อบริษัทผลิตกระดาษ หมายเลขลำดับ ซึ่งทำให้สามารถสืบสาวไปถึงบริษัทคอมพิวเตอร์ที่ใช้กระดาษนั้น และสามารถสืบทราบได้ว่าพิมพ์ออกจากเครื่องพิมพ์ใด จากนั้นก็เป็นการง่ายที่จะค้นหาตัวพนักงานโปรแกรมที่ทำงานเข้าเครื่องคอมพิวเตอร์ โดยตรวจสอบจาก console log

9. Data Leakage

การทุจริตวิธีนี้เป็นการนำข้อมูลออกจากระบบคอมพิวเตอร์ โดยอาศัยวิธีการต่าง ๆ ผู้ทุจริตอาจซ่อนเทคนิคไว้ในระบบคอมพิวเตอร์ แต่ในขั้นตอนการนำข้อมูลออกจะต้องสามารถหลบหลีกการสงสัยจากพนักงานปฏิบัติการคอมพิวเตอร์ หรือพนักงานอื่น ๆ

วิธีการที่อาจใช้ในการทุจริตแบบนี้ อาจมีทั้งการกำหนดให้พิมพ์ข้อมูลออกมาในรายงาน โดยไม่มีลักษณะผิดปกติหรือแตกต่างจากข้อมูลทั่วไป เช่น เพิ่มเข้าไปในกลุ่ม (block) ข้อมูลต่าง ๆ สอดแทรกเข้าไปในข้อมูลอื่น หรืออาจเข้ารหัสให้ผิดจากที่ข้อมูลนั้นควรแสดง ซึ่งอาศัยเทคนิคค่อนข้างซับซ้อน

ตัวอย่างการเข้ารหัส ได้แก่ การกระจายข้อมูลลับที่ต้องการอยู่ตามบรรทัดต่าง ๆ หรือแทรกอยู่ ณ ลำดับที่ที่กำหนดไว้แน่นอนในข้อความ ตัวเลข วรรคตอน ซึ่งต้องถอดรหัสออกมาจึงจะได้ข้อมูลลับนั้น อีกวิธีหนึ่งคือ การควบคุมและสังเกตความเคลื่อนไหวของอุปกรณ์ต่าง ๆ เช่น ม้วนเทปที่เครื่องขับเทปกำลังอ่านอยู่ การเคลื่อนไหวจะมี 2 ลักษณะ คือ ตามเข็มนาฬิกา และทวนเข็มนาฬิกา ซึ่งผู้ที่มีความชำนาญจะทราบว่าเป็นการอ่านตัวเลข 0 หรือ 1 ซึ่งจะต้องนำไปตีความอีกครั้งหนึ่ง บางกรณีอาจใช้เทปบันทึกเสียงทำการบันทึกเสียงพิมพ์ของเครื่องพิมพ์ แล้วนำไปเปิดโดยใช้ความเร็วต่ำลงเพื่อแปลออกมาเป็นเลขฐานสอง

วิธีการที่แปลกซึ่งไม่เคยปรากฏมาก่อน มีในระบบคอมพิวเตอร์ซึ่งมีการรักษาความปลอดภัยอย่างเข้มงวด และการลักลอบนำข้อมูลออกไปมีความเสี่ยงภัยสูง มีรายงานว่าเครื่องคอมพิวเตอร์ที่ใช้ในสงครามเวียดนามหลายเครื่องถูกติดตั้งเครื่องส่งวิทยุขนาดเล็กมากลงไป เครื่องส่งนั้นสามารถส่งสัญญาณเปิดเผยข้อมูลที่มีอยู่ในคอมพิวเตอร์ไปยังเครื่องรับที่อยู่ห่างออกไปได้ ความลับนี้ถูกเปิดเผยหลังจากเครื่องคอมพิวเตอร์ดังกล่าวถูกส่งกลับจากเวียดนามไปยังสหรัฐอเมริกาแล้ว

10. Piggybacking and Impersonation

การทุจริตทั้ง 2 แบบนี้ทำได้ทั้งโดยทางกายภาพและทางอิเล็กทรอนิกส์ ทางกายภาพ คือ การที่ตัวผู้ทุจริตสามารถเข้าไปในบริเวณซึ่งตนเองไม่มีสิทธิเข้าไปได้ ทั้งนี้อาจเป็นบริเวณที่มีการควบคุมด้วยเครื่องอิเล็กทรอนิกส์หรือกลไก (mechanically) ที่ใช้ล๊อกประตูห้อง ที่เกิดขึ้นบ่อย ๆ คือ ปลอมตัวเป็นผู้ทำงานเกี่ยวข้องกับห้องคอมพิวเตอร์ หรือสถานที่หวงห้าม ในมือเต็มไปด้วยอุปกรณ์ต่าง ๆ เช่น ม้วนเทป รอจังหวะที่เจ้าหน้าที่ซึ่งมีอำนาจเข้าไปในสถานที่ที่ต้องการ ก็จะติดตามไปด้วย การป้องกันผู้บุกรุกในลักษณะนี้ทำได้โดยใช้ยามเฝ้าประตู และ/หรือให้มีโทรทัศน์วงจรปิดคอยเฝ้าดู

turnstyle เป็นเครื่องกีดขวางคล้ายทางเข้าซุปเปอร์มาร์เก็ต ซึ่งผู้ผ่านจะต้องใช้ลูกกุญแจ และ/หรือบัตรที่มีแถบแม่เหล็กไป/สอดเข้าไป

mantrap เป็นประตูผ่านซึ่งมี 2 ชั้น ซึ่งจะอนุญาตให้ผ่านเข้าไปได้ครั้งละ 1 คน โดยต้องใช้ลูกกุญแจประกอบ การอาศัยเครื่องกลไกทั้ง 2 แบบนี้จะมีประสิทธิภาพเพียงใด ขึ้นอยู่กับประสิทธิภาพของกลไกและความสังเกตของพนักงานที่เกี่ยวข้องประกอบด้วย

การบุกรุกโดยอาศัยเครื่องอิเล็กทรอนิกส์ อาจอาศัยเครื่องเทอร์มินัลซึ่งแอบพ่วงสายโทรศัพท์คู่สายเดียวกันไว้ เมื่อเครื่องที่ใช้งานจริงเปิดเข้าไปในระบบ ซึ่งจะมีการใช้ระบบคอมพิวเตอร์ตรวจสอบก่อนให้ทำงานได้ เช่น ใช้กุญแจรหัสลับ หรือการต้องทำการบางอย่าง (protocol) ตามที่ตกลง/กำหนดไว้ก่อน หลังจากระบบยอมรับเครื่องเทอร์มินัลที่ใช้งานจริงแล้ว ผู้ทุจริตจะรอจังหวะที่ผู้ใช้เครื่องดังกล่าวไม่อยู่ หรือเครื่องไม่ได้ทำงาน เพื่อการทุจริตต่อไป เนื่องจากเครื่องคอมพิวเตอร์ไม่สามารถแยกแยะได้ว่าเป็นสัญญาณที่มาจากเครื่องใด บางครั้งผู้ทุจริตอาจแอบสวมรอยที่ผู้ใช้ที่แท้จริงในระหว่างที่ผู้ใช้ไม่อยู่ประจำเครื่องเทอร์มินัลและเปิดเครื่องทิ้งไว้ หรือปิดไม่เรียบร้อย เป็นต้น

Impersonation หมายถึง การสวมรอยโดยปลอมแปลงเป็นผู้มีสิทธิเข้าถึง ซึ่งอาจเป็นการเข้าถึงสถานที่ การเข้าไปใช้เครื่องเทอร์มินัล และการเข้าถึงเครื่องคอมพิวเตอร์ผ่านเครื่องเทอร์มินัล โดยสวมรอยใช้หลักฐานของผู้มีสิทธิ์แท้จริง เช่น รหัสลับ ลายนิ้วมือ หรือเสียงของผู้มีสิทธิ์เข้าถึง ผู้ทุจริตที่มีหลักฐานตามที่ระบบกำหนดจะสามารถเข้าถึงเครื่องคอมพิวเตอร์ได้

ตัวอย่างการใช้วิธี impersonation คือ มีชายคนหนึ่งโทรศัพท์ไปหาเจ้าหน้าที่ของบริษัท โทรศัพท์อ้างว่าเป็นผู้เขียนบทความเกี่ยวกับระบบคอมพิวเตอร์ที่บริษัทนั้นใช้อยู่ ต้องการขอทราบรายละเอียดเพื่อนำไปเขียนลงบทความ บริษัทเชิญให้ชายผู้นั้นไปพบและบรรยายสรุปเกี่ยวกับระบบคอมพิวเตอร์ พร้อมทั้งระบบงานต่าง ๆ ให้ทราบ จากข้อมูลที่ได้ไปนั่นเองชายผู้นั้นได้โจรกรรมทรัพย์สิน เครื่องอุปกรณ์โทรศัพท์ ของบริษัทไปกว่า 1 ล้านเหรียญ

อีกกรณีหนึ่งคือ คนร้ายลักบัตร ATM ของผู้เสียหายไป แล้วโทรศัพท์ไปหาเจ้าของบัตร แจ้งว่าตนเป็นพนักงานของธนาคารขอทราบรหัสประจำตัว (PIN) ของเจ้าของบัตร เพื่อทำการอายัดการใช้บัตร ทั้งนี้ทราบว่าบัตรของเขาถูกลักไป ผู้เสียหายหลงเชื่อและแจ้ง PIN ให้คนร้ายรู้ คนร้ายจึงถอนเงินไปเต็มตามวงเงินสูงสุดที่อนุญาตให้ถอนได้

11. Wiretapping

ไม่ปรากฏว่ามีกรณีการลักหรือแก้ไขข้อมูลโดยอาศัยวิธีนี้ ทั้ง ๆ ที่แนวโน้มน่าจะมีมาก เนื่องจากมีการติดต่อสื่อสารส่งผ่านข้อมูลผ่านวงจรสื่อสารหลากหลายรูปแบบ การที่วิธีทุจริตแบบนี้ไม่เป็นที่นิยมเนื่องจากมีวิธีอื่นที่ง่ายกว่า

การทุจริตวิธีนี้ต้องใช้อุปกรณ์มูลค่าประมาณ 200 เหรียญขึ้นไป เพื่อใช้ในการบันทึกและพิมพ์ข้อมูลออกมา ซึ่งสามารถรับโดยตรงจากเครื่องคอมพิวเตอร์ หรือใช้ผ่านเครื่องเทอร์มินัล อย่างไรก็ดีผู้ทุจริตจะไม่รู้ว่าข้อมูลที่รับมานั้นมีสิ่งที่ตนเองต้องการต่อไป สำหรับการลักลอบข้อมูลที่ส่งผ่านระบบไมโครเวฟหรือดาวเทียม ยังเป็นปัญหาสำหรับผู้ทุจริต เนื่องจากเหตุผล 2 ประการ คือ ต้องเสียค่าใช้จ่ายสูง และมักเป็นข้อมูลที่มีการเข้ารหัสไว้

12. Simulation and Modeling

การทุจริตวิธีนี้เป็นการอาศัยประสิทธิภาพของคอมพิวเตอร์เพื่อการวางแผน และสนับสนุนการประกอบอาชญากรรม โดยการจำลองการปฏิบัติงานในระบบคอมพิวเตอร์ เพื่อนำผลที่ได้ไปประกอบการทุจริต

การทุจริตมูลค่านับล้านดอลลาร์รายหนึ่ง เกิดขึ้นจากการกระทำของสมุห์บัญชี ซึ่งมีศูนย์บริการคอมพิวเตอร์ส่วนตัว ผู้ทุจริตได้จำลองระบบบัญชีย่อยและระบบบัญชีแยกประเภทของบริษัทที่เขาทำงานไปแก้ไขปรับปรุงหลังจากนั้นได้นำข้อมูลที่ถูกต้องเข้าไปในระบบบัญชีย่อย เพื่อให้ระบบที่ถูกแก้ไขทำการปรับตัวเลขที่แสดงในระบบบัญชีแยกประเภทตามที่เขาวางแผนไว้ นอกจากนั้นยังสามารถทำการประมวลผลจากระบบแยกประเภทย่อยมายังระบบบัญชีย่อยอีกด้วย จากการทดลองดังกล่าวเขาได้แก้ไขบัญชีเจ้าหนี้และบัญชีลูกหนี้ โดยให้ผลที่แสดงในบัญชีแยกประเภทยังคงเป็นไปตามที่วางแผนไว้ได้

การทุจริตอีกรายหนึ่งเกิดขึ้นที่บริษัทประกันภัยใน Los Angeles ในปี 1973 ผู้ทุจริตได้ใช้ระบบคอมพิวเตอร์จำลองบริษัทใหม่ขึ้นมา และสมมุติให้มีการขายกรมธรรม์ประกันชีวิตไปจำนวนมาก ระบบคอมพิวเตอร์ได้พิมพ์กรมธรรม์ออกมา 64,000 ฉบับ ในรูปแบบที่คอมพิวเตอร์อ่านได้ หลังจากนั้นกรมธรรม์นี้ได้ถูกนำเข้าไปรวมกับระบบที่ใช้จริงแล้วนำกรมธรรม์ไปขายต่อให้แก่บริษัทประกันภัยต่อ (reinsuring companies)

การทุจริตวิธีนี้ผู้ทุจริตต้องใช้เวลาการทำงานของคอมพิวเตอร์มากขึ้นกว่าปกติมาก และต้องพัฒนาโปรแกรมขึ้นมาช่วยด้วย การตรวจสอบอาจทำได้โดยดูจากการใช้บริการประมวลผลที่ผิดปกติเมื่อเทียบกับปริมาณธุรกิจของบริษัทนั้นทำอยู่



บทที่ 6

การทุจริตในวงการคอมพิวเตอร์
(ประสบการณ์ของประเทศต่าง ๆ)

การทุจริตในวงการคอมพิวเตอร์

(ประสบการณ์ของประเทศต่าง ๆ)

ประสบการณ์ของประเทศต่าง ๆ ในวงการคอมพิวเตอร์ ซึ่งจะกล่าวต่อไปนี้ มีบางเรื่องซึ่งเป็นเรื่องของการทุจริตในระบบ Manual ปกติ ซึ่งต่อมาภายหลังจากที่สถาบันการเงินได้เปลี่ยนจากระบบ Manual มาสู่คอมพิวเตอร์แล้วก็มีการทุจริตเกิดขึ้นทั้งก่อนหน้าที่สถาบันการเงินจะเปลี่ยนเป็นระบบคอมพิวเตอร์ และเกิดขึ้นในกรณีคล้าย ๆ กันนี้เมื่อสถาบันการเงินนั้นมาใช้คอมพิวเตอร์ด้วย

ดังนั้นตัวอย่างหลากหลายของการทุจริต ซึ่งส่วนใหญ่เกิดขึ้นในสถาบันการเงินนี้ จึงเป็นตัวอย่างที่เป็นประสบการณ์ของประเทศต่าง ๆ ที่ใช้คอมพิวเตอร์ ซึ่งหวังว่าผู้บริหารของสถาบันการเงินจะได้ใช้เป็นข้อเตือนใจ และเตรียมพร้อมในการป้องกันจุดอ่อนต่าง ๆ ภายในระบบงานด้านคอมพิวเตอร์ของตน อย่างไรก็ดีหากจุดอ่อนต่าง ๆ ที่เกิดขึ้นไม่ได้รับการสนใจจากผู้บริหารอย่างเพียงพอและเหมาะสม สถาบันการเงินที่ใช้คอมพิวเตอร์ก็อาจประสบปัญหาที่ไม่พึงประสงค์ได้

ตัวอย่างต่าง ๆ ของการทุจริตในวงการคอมพิวเตอร์

1. กรณีการเปลี่ยนระบบจาก Manual ไปสู่ Computer System

1.1 มูลเหตุ

เกิดระหว่างการเปลี่ยนระบบงานของเงินฝากประจำ (Fixed Deposit) จาก Manual system ไประบบ Computer system ในระยะนั้นธนาคารทำงานแบบคู่ขนาน (Parallel run) คือ ทำพร้อมกันทั้ง 2 ระบบ สมุดเงินฝากประจำนี้ใช้ในระบบคอมพิวเตอร์แล้ว และรอลูกค้ามาติดต่อเพื่อลงนามด้านหลัง (ธนาคารใช้ระบบ Black light signature) ธนาคารได้วางสมุดคู่ฝากเงินฝากประจำที่ลูกค้ายังไม่มารับที่โต๊ะสมุห์บัญชี

1.2 วิธีการทุจริต

จากข้อ 1 ผู้ทุจริตซึ่งเป็นนักการของสาขานี้ ได้ลักลอบนำสมุดคู่ฝากเงินฝากประจำ และ Transfer paper ของลูกค้าธนาคารไป โดย

1.2.1 ให้เพื่อนนักการลงนามด้านหลังในช่องลายเซ็นลูกค้า

1.2.2 แก้ไขชื่อลูกค้าเป็นชื่อเพื่อนของนักการเอง

1.2.3 ปลอมลายเซ็น Authorized Signature ที่ลงนามรับรองลายมือชื่อลูกค้าด้านหลังและด้านหน้า

1.3 วิธีการเบิกเงิน

เพื่อนนักการไปถอนเงินฝากต่างสำนักงานที่สาขาแถวลาดพร้าว และได้ไปถอนเงินที่สาขาแถวราชเทวี แต่ถูกจับกุมเสียก่อน

1.4 การพบการทุจริต

- การเบิกเงินครั้งแรกที่สาขาแถวลาดพร้าว เจ้าหน้าที่ของสาขาไม่ได้สงสัยลายเซ็น เพราะผู้เบิกเป็นบุคคลคนเดียวกับที่ได้เซ็นลายมือไว้ที่ด้านหลังช่อง Pass book แต่สงสัยว่าชื่อเจ้าของบัญชีที่ถูกแก้ไปนั้นควรมี Authorized Signature เซ็นกำกับการแก้ไขด้วย แต่ก็ไม่ปรากฏ จึงได้โทรศัพท์สอบถามชื่อเจ้าของบัญชีไปยัง Home branch แต่ Home branch คงงานกำลังยุ่ง ตอบกลับมาว่าถูกต้องแล้ว ทั้ง ๆ ที่ไม่ได้เช็คสอบ ผู้ทุจริตจึงเบิกเงินไปได้

- การเบิกเงินครั้งที่ 2 ที่สาขาแถวราชเทวี ผู้ทุจริตโดนจับกุม ทั้งนี้เพราะสาขานี้มีความสงสัยเช่นเดียวกับสาขาแรก จึงได้โทรศัพท์สอบถามไปยัง Home branch เช่นเดียวกัน และได้รับแจ้งว่าชื่อเจ้าของบัญชีตามที่สาขาแจ้งไปไม่ตรงกับชื่อเจ้าของบัญชีที่ปรากฏในทะเบียนของ Home branch ผู้ทุจริตจึงถูกจับกุมในเวลาต่อไป

1.5 การป้องกันการทุจริต

- Pass book ที่เตรียมให้ลูกค้าเก็บเข้าห้องมั่นคงทั้งหมด
- รายการแก้ไขทุกรายการต้องมี Authorized Signature แต่ส่วนมากยกเลิก และทำ Pass book ใหม่ ไม่ให้มีรอยแก้
- Transfer Paper ทำทะเบียนคุมยอดไว้ทุกใบ และมีหมายเลขกำกับไว้

2. กรณีการทุจริตโดยการสับเปลี่ยนสมุดคู่ฝากของลูกค้าธนาคารพาณิชย์

2.1 มูลเหตุ

การทุจริตเกิดจากความสับสนในการรับสมุด Pass book คืนจากธนาคาร กล่าวคือ ในขณะที่ธนาคารเรียกลูกค้ามารับ Pass book คืน บางครั้งมีการสับสนและลูกค้าบางรายรับสมุดของผู้ฝากรายอื่นโดยมิได้เป็นสมุดคู่ฝากของตนเอง ซึ่งเป็นไปได้ทั้งโดยเจตนาและไม่เจตนา และผู้ถือสมุดคู่ฝากที่มิใช่ของตนเองได้ถือโอกาสทุจริตโดยเบิกเงินจากสมุดคู่ฝากเล่มนั้น

2.2 วิธีการทุจริต

- ผู้ทุจริตได้สับเปลี่ยนแผ่นลายเซ็นซึ่งอยู่ใน Pass book ด้านหลังสุดของเจ้าของบัญชีเป็นแผ่นลายเซ็นของตน ทั้งนี้เพราะแผ่นลายเซ็นด้านหลัง Pass book อาจหลุดได้โดยง่าย ถ้าเจ้าของ Pass book เก็บรักษาไม่ดีพอ ซึ่งเป็นเหตุการณ์ที่เกิดขึ้นได้เสมอ ทำให้เจ้าหน้าที่ของธนาคารไม่สังเกตเรื่องนี้

- ผู้ทุจริตทำสลิปเบิกถอน โดยใช้ชื่อเจ้าของบัญชีคนเดิม แต่ใช้ลายเซ็นของตนเอง ซึ่งวิธีดังกล่าวธนาคารไม่อาจตรวจสอบพบความผิดปกติตามลายเซ็นได้ และคอมพิวเตอร์ก็ไม่อาจพบความผิดปกติใด ๆ ได้ เนื่องจากผู้ทุจริตใช้ Pass book ของบัญชีที่มีเงินและมีเลขบัญชีเดิมทุกประการ

2.3 วิธีการเบิกเงิน

- เบิกตามปกติ ในนามของเจ้าของบัญชีคนเดิม แต่ใช้ลายเซ็นของผู้ทุจริต

2.4 การพบการทุจริต

- เจ้าของบัญชีที่แท้จริงมาขอรับ Pass book แต่รับไม่ได้ เพราะมีผู้สวมรอยนำสมุดไปแล้ว และเมื่อเช็คสอบกับ Balance และความเคลื่อนไหวประจำวันในรายงาน และด้านทาง Teller Terminal ก็พบรายการเบิกเงิน และเมื่อตรวจสอบลายเซ็นในสลิปกับลายเซ็นเจ้าของบัญชีที่ให้ไว้ก็ไม่เหมือนกัน

2.5 การป้องกันการทุจริต

ธนาคารให้ Authorized Signature ลงนามด้านหลัง โดยประทับตราและลงนามคาบเกี่ยวระหว่างใบ Pass book แผ่นสุดท้ายกับแผ่นลงนามส่วนหนึ่ง และลงนามคาบเกี่ยวระหว่างปกในด้านหลัง Pass book กับแผ่นลงนามอีกส่วนหนึ่ง เพื่อป้องกันมิให้มีการสับเปลี่ยนแผ่นที่ใช้เช็คสอบลายเซ็นเจ้าของบัญชีที่แท้จริง

3. กรณีการ Key เงินฝากลอย ๆ ผ่านเครื่อง Terminal

3.1 มูลเหตุ

จุดอ่อนในระบบงานและการควบคุม

3.2 วิธีการทุจริต

กระทำโดยพนักงาน ledger หรือ Terminal operator ประจำสาขาธนาคารพาณิชย์แห่งหนึ่ง พนักงานผู้นี้ทำงานที่ธนาคารแห่งนี้มาแล้วประมาณ 10 ปี กระทำการทุจริต ดังนี้

ก) ผู้ทุจริตร่วมกับบุคคลภายนอก ได้ขอเปิดบัญชีเงินฝากสะสมทรัพย์ที่สาขาต่าง ๆ ในเขตกรุงเทพมหานคร เท่าที่ทราบ 10 สาขา เพื่อประกอบการทุจริต

ข) ผู้ทุจริตได้อาศัยงานในหน้าที่ key ยอดเงินฝากโดยไม่มีเอกสารใด ๆ ผ่านเครื่อง Teller Terminal ที่สาขาที่ตนเองทำงานอยู่ ด้วยยอดเงินต่าง ๆ รวม 10 บัญชี จำนวนเงินรวมประมาณ 9 ล้านบาทเศษ ไปยังบัญชีสาขาต่าง ๆ ทั้ง 10 แห่ง ทั้งนี้โดยผู้ทุจริตเริ่ม key เงินฝากในจังหวะงานมาก ๆ ซึ่งวันปฏิบัติงานเป็น วันจันทร์

ค) ผู้ทุจริตได้หลบหนีไปจากสาขาที่ key เงินฝากลอย เมื่อเวลาประมาณ 11.00 น. และหลังจากนั้นได้ร่วมกับบุคคลภายนอกไปเบิกเงินตามสาขาต่าง ๆ ทันที และเบิกเงินไปได้รวมทั้งสิ้น 5 ล้านบาทเศษ

ง) การทุจริตตั้งแต่ต้นจนเบิกเงินไปได้กระทำในวันเดียวกัน

3.3 วิธีการเบิกเงิน

ผู้ทุจริตจะทำสมุดคู่ฝาก (Pass book) ไป Up date ยังสาขาที่จะเบิกเงิน แล้วขอถอนเงินพร้อมกัน

3.4 การพบการทุจริต

เกิดจากการสังเกตและไหวพริบของผู้ช่วยสมุห์บัญชีของธนาคารคนหนึ่ง ซึ่งเป็นสาขาหนึ่งที่ผู้ทุจริตได้ไปเบิกเงิน ตามลำดับเหตุการณ์ดังนี้

ก. ผู้ทุจริตขอเบิกเงินสด 50,000 บาท และ Cashier order อีก 200,000 บาท

ข. รายการเบิกเงินโดยปรากฏชื่อผู้ทุจริตที่บังเอิญผู้ช่วยสมุห์บัญชีจำได้ว่าเป็นพนักงาน Teller ประจำสาขาที่ทำการทุจริต แต่ทำไมจึงต้องมาเบิกเงินที่สาขาของตน ทั้ง ๆ ที่ไม่มีความจำเป็น เนื่องจากจะเบิกจากสาขาที่ตนสังกัดอยู่ก็ได้และสะดวกกว่ามาก

ค. จากการที่ผู้ช่วยสมุห์บัญชีจำได้ว่าผู้ทุจริตเป็นพนักงาน Teller ประจำสาขาแห่งอื่นของธนาคารเดียวกัน จึงได้โทรศัพท์สอบถามมายังสาขาที่ผู้ทุจริตทำงานอยู่เกี่ยวกับการฝากเงินและพฤติการณ์ของผู้ทุจริต เรื่องทั้งหมดจึงถูกเปิดเผยขึ้น เมื่อสาขาที่ผู้ทุจริตได้ตรวจสอบเอกสารกับการ key ข้อมูลผ่านเครื่อง Terminal

3.5 การดำเนินงานของสาขาที่ถูกทุจริตหลังจากได้รับแจ้งสาขาที่สงสัยในพฤติกรรม

ก. เช็คสอบรายการใน Terminal tape กับสลิปทุกรายการทันที ปรากฏว่ามีการ key รายการนำฝากแบบ No-book หลายรายการ จำนวน 10 บัญชี

ข. key ข้อมูลล้างรายการที่ตรวจพบว่ามีการทุจริตทั้งหมดทันที

ค. โทรศัพท์แจ้งอายัดการเบิกเงินจากบัญชีที่พบไปยังสาขาทุกแห่ง

ง. แจ้งให้สำนักงานใหญ่ปิดเครื่องคอมพิวเตอร์ ซึ่งเป็นศูนย์กลางการติดต่อบัญชีแบบ On-line ของสาขาต่าง ๆ ในกรุงเทพฯทั้งหมด

จ. จากการดำเนินการขั้นต้น ๆ ทำให้ธนาคารจับกุมผู้ร่วมทุจริตซึ่งเป็นบุคคลภายนอกได้ในขณะที่นำเช็คธนาคารสาขาอื่นไปเบิกเงินสดที่อีกสาขาหนึ่ง

3.6 การป้องกันการทุจริต

สำนักงานใหญ่ของธนาคารแห่งนี้ได้มีคำสั่งให้มีการสอบถามรายการฝากเงินต่างสำนักงานของบัญชีเงินฝากสะสมทรัพย์ที่มียอดตั้งแต่ 50,000 บาทขึ้นไป และมีการกำหนดวงเงินที่พึงให้เบิกถอนได้ตามระดับของ Authorized code

4. โกงเงินธนาคารโดยอาศัยเครื่องเทอร์มินัล

4.1 ขั้นตอนการปฏิบัติงานเกี่ยวกับการเบิกเงินเกินบัญชี

1) เมื่อลูกค้าสั่งจ่ายเช็คเพื่อถอนเป็นเงินสดหรือหักบัญชีโดยผ่านสำนักหักบัญชี พนักงานประจำเครื่องเทอร์มินัล (Operator) จะบันทึกบัญชี (ป้อนข้อมูล) เพื่อปรับ (update) ยอดคงเหลือในบัญชีของลูกค้าและบัญชีที่เกี่ยวข้องใน Computer file

2) การป้อนข้อมูลนั้น พนักงาน Operator จะใช้จอภาพ Screen General Transfer (Cash Paying) สำหรับกรณีลูกค้าต้องการถอนเป็นเงินสด และจะใช้จอภาพ Screen in-clearing สำหรับกรณีหักบัญชีโดยผ่านสำนักหักบัญชี

3) หลังจากที่ป้อนข้อมูลเสร็จเรียบร้อยแล้วทุกครั้ง เครื่องคอมพิวเตอร์จะพิมพ์รายการลงในกระดาษต่อเนื่อง (Input monitor) จำนวน 2 ฉบับ เป็นต้นฉบับ 1 ฉบับ และสำเนา 1 ฉบับ ต้นฉบับจะนำมาใช้ Checker หรือผู้จัดการแผนกเงินฝากตรวจสอบกับตัวเช็คว่ามีการบันทึกรายการถูกต้องหรือไม่ เช่น เลขที่บัญชี จำนวนเงิน เป็นต้น หากรายการถูกต้องแล้วก็จะทำลาย Input monitor ฉบับนั้นเสีย ส่วนฉบับสำเนาจะเก็บไว้เป็นหลักฐาน

4) กรณีที่ลูกค้าเบิกเงินเกินกว่ายอดคงเหลือในบัญชี หรือวงเงินที่จะเบิกถอนได้โปรแกรมคอมพิวเตอร์จะไม่ยินยอมให้เบิกถอนออกไปได้ โดยจะแสดงข้อความ (Error message) ว่า "Balance short"

5) หากจะยินยอมให้ลูกค้าเบิกเงินเกินกว่ายอดคงเหลือในบัญชี หรือวงเงินที่จะเบิกถอนได้ก็จะต้องให้ผู้จัดการแผนกเงินฝากอนุมัติรายการเสียก่อน ด้วยการป้อนรหัสประจำตัว (Manager's operator code) และรหัสอนุมัติรายการ (Approve code) พนักงาน Operator จึงจะสามารถทำรายการต่อไปได้

6) กรณีที่ลูกค้าต้องการมีวงเงินเบิกเกินบัญชีชั่วคราวหรือถาวร หรือเปลี่ยนแปลงแก้ไขวงเงินจะต้องให้แผนกสินเชื่อเป็นผู้อนุมัติ จากนั้นจึงจะให้แผนกเงินฝากบันทึกรายการเปลี่ยนแปลงแก้ไขดังกล่าว โดยใช้จอภาพ Screen No. DPAC 01 Deposit Account Correction

7) จอภาพ Screen No. DPAC 01 ดังกล่าว นอกจากจะใช้สำหรับแก้ไขวงเงินเบิกเกินบัญชีแล้ว ยังใช้สำหรับแก้ไขอัตราดอกเบี้ยและวันครบกำหนดสัญญาได้อีกด้วย

4.2 จุดอ่อนในระบบงาน

พนักงาน Operator สามารถเรียกใช้จอภาพ Screen No. DPAC 01 ได้โดยอิสระ ไม่มีขอบเขตจำกัดทำให้เปิดโอกาสให้สามารถทำรายการข้ามขั้นตอนการควบคุม (Override) ของพนักงานชั้นบริหารตามที่กล่าวข้างต้นได้

4.3 ความเสี่ยง

เมื่อมีจุดอ่อนในระบบงาน ความเสี่ยงที่จะเกิดการทุจริตย่อมมีขึ้นได้เป็นธรรมดา แม้ว่าธนาคารจะมีความเชื่อมั่นในความซื่อสัตย์สุจริตของพนักงานก็ตาม

4.4 ผู้ทุจริต

ในกรณีนี้ผู้ที่มีโอกาสกระทำการทุจริตมากที่สุด คือ พนักงาน Operator ในแผนกเงินฝากนั่นเอง

4.5 วิธีการทุจริต

1) พนักงาน Operator จะร่วมมือกับลูกค้าเพื่อโกงเงินธนาคาร โดยสั่งจ่ายเช็คให้เกินกว่ายอดคงเหลือในบัญชี หรือวงเงินที่จะเบิกถอนได้ ซึ่งตามขั้นตอนการปฏิบัติงานโปรแกรมคอมพิวเตอร์จะไม่ยินยอมให้เบิกถอนออกไปได้ จนกว่าจะได้รับการอนุมัติรายการจากพนักงานชั้นบริหารด้วยการป้อนรหัส Manager's Operator Code และ Approve Code

2) เพื่อข้ามขั้นตอน (override) การควบคุมดังกล่าว พนักงาน Operator จะใช้จอภาพ Screen No. DPAC 01 Deposit Account Correction เพิ่มเติมหรือเปลี่ยนแปลงแก้ไขวงเงินเบิกเกินบัญชี ทำให้เช็คฉบับนั้นเบิกถอนเงินได้

3) Input Monitor ฉบับที่บันทึกรายการเพิ่มเติมหรือเปลี่ยนแปลงแก้ไขวงเงินเบิกเกินบัญชีนั้น พนักงาน Operator จะทำลายทิ้งเสีย ยกเว้นฉบับสำเนาซึ่งจะไม่ถูกทำลาย เพราะจะเป็นพิรุธได้ง่าย หากฉีกออกจากกระดาษต่อเนื่องทั้งหมดซึ่งเรียงติดต่อกันไป ทำให้พนักงานชั้นบริหารไม่ทราบว่าลูกค้ารายนี้มีการเปลี่ยนแปลงแก้ไขวงเงินเบิกเกินบัญชีโดยมิชอบ

4) สำหรับ Input monitor ฉบับที่แสดงรายการการถอนเงินตามเช็คนั้น จะไม่ปรากฏวงเงินเบิกเกินบัญชี เพียงแต่แสดงเลขที่บัญชี ชื่อบัญชี เลขที่เช็ค จำนวนเงิน และยอดคงเหลือหลังจากหักบัญชีแล้วเท่านั้น เมื่อนำมาใช้ Checker ตรวจสอบกับตัวเช็ค จึงปรากฏว่าถูกต้องตรงกัน

4.6 ความเสียหาย

1) ผู้เสียหาย ได้แก่ ธนาคาร

2) จำนวนเงิน เนื่องจากธนาคารมิได้กำหนดจำนวนเงินที่พนักงาน Operator จะสามารถ Key ได้ อาจทำให้ธนาคารได้รับความเสียหายเป็นจำนวนมาก แม้ว่าปัจจุบันธนาคารจะพยายามป้องกันโดยใช้วิธีสอบถามการสั่งจ่ายเช็คของลูกค้าทางโทรศัพท์ก็ตาม แต่เมื่อลูกค้าร่วมมือกับพนักงานโกงเงินธนาคาร วิธีดังกล่าวก็ย่อมใช้ไม่ได้ผล

4.7 การตรวจสอบ

นำรายงานประจำวันซึ่งแสดงการแก้ไขวงเงินเบิกเกินบัญชีมาตรวจสอบกับ สมุดทะเบียน (OD instruction book) ว่าถูกต้องตรงกันหรือไม่

4.8 การป้องกัน

จำกัดอำนาจของพนักงาน Operator ในการทำรายการดังกล่าว นอกจากจะได้รับอนุมัติจากพนักงานชั้นบริหารเช่นเดียวกับกรณีเกิด "Balance short"

5. การทำรายการเปลี่ยนแปลงแก้ไขวงเงินเบิกเกินบัญชี

การเบิกถอนเงิน โปรแกรมจะควบคุมไม่ให้มีการถอนเงินเกินกว่ายอดคงเหลือ หรือวงเงินที่ลูกค้าจะถอนได้ โดยจะแสดง Error message ว่า "Balance short" ซึ่งพนักงาน Operator จะไม่สามารถทำรายการต่อไปได้หากไม่ได้รับการอนุมัติจากพนักงานชั้นบริหาร (Manager's approval)

5.1 วิธีการทุจริต

1) พนักงาน Operator ทุจริตเอง
   (1) โดยขโมยเช็คของลูกค้า แล้วปลอมลายเซ็น นำมาเบิกเงินจากธนาคารเป็นเงินสด หรือฝากธนาคารอื่นเพื่อส่งมาเรียกเก็บก็ได้
   (2) หากคอมพิวเตอร์แจ้งว่า "Balance short" แสดงว่าบัญชีของลูกค้ามีเงินไม่พอ หรือเกินวงเงินเบิกเกินบัญชีตามที่กล่าวข้างต้น Operator จะใช้วิธีบันทึกรายการเปลี่ยนแปลงแก้ไขวงเงินเบิกเกินบัญชี กล่าวคือ ถ้ามีเงินไม่พอก็แก้ไขให้มีวงเงินเบิกเกินบัญชี ถ้าเกินวงเงินก็แก้ไขเพิ่มวงเงินให้พอเพียงกับจำนวนเงินที่จะถอน

2) พนักงาน Operator ร่วมกับผู้อื่น
   (1) ผู้อื่นในที่นี้ก็คือ บุคคลใกล้ชิดกับลูกค้าหรือทำงานในบริษัทของลูกค้า โดยให้บุคคลนั้นขโมยเช็คของลูกค้ามา แล้วปลอมลายมือชื่อมาเบิกเงินจากธนาคาร
   (2) วิธีการเหมือนข้อ 1 (2)

3) พนักงาน Operator ร่วมกับลูกค้า (เจ้าของบัญชี)
   (1) ตกลงกับลูกค้าให้สั่งจ่ายเช็คมาเบิกเงินจากธนาคาร
   (2) วิธีการเหมือนข้อ 1 (2)

5.2 การตรวจสอบ

ธนาคารสามารถตรวจพบวิธีการทุจริตดังกล่าวได้จากรายงานต่อไปนี้

1) Specification list of non-financial transaction (A/C corrected) แสดงบัญชีที่มีการแก้ไขวงเงินเบิกเกินบัญชี อัตราดอกเบี้ย และวันครบกำหนดสัญญา
2) Deposit balance list of loan customer แสดงยอดคงค้างของบัญชีที่เป็นลูกค้าแผนก Loan รวมทั้งวงเงินเบิกเกินบัญชี อัตราดอกเบี้ย และวันครบกำหนดสัญญา

รายงานที่กล่าวนำมาเช็คสอบกับสมุดทะเบียนอนุมัติสินเชื่อเงินเบิกเกินบัญชี (OD instruction book) หรือสัญญาต่าง ๆ ซึ่งจะทราบผลอย่างเร็วก็เป็นสิ้นวันหรือเช้าวันรุ่งขึ้น ซึ่งอาจไม่ทันกาล

5.3 การป้องกัน

1) ธนาคารใช้วิธีสอบถามเจ้าของบัญชีโดยทางโทรศัพท์ กรณีเช็คสั่งจ่ายมีจำนวนเงินตั้งแต่ 50,000 บาทขึ้นไป ดังนั้นกรณีข้อ 5.1 และ 5.2 ผู้ทุจริตจะได้เงินไปไม่เกิน 50,000 บาทต่อบัญชี

2) จำกัดอำนาจของพนักงาน Operator ในการปรับปรุงเปลี่ยนแปลงแก้ไขวงเงินเบิกเกินบัญชี อัตราดอกเบี้ย และวันครบกำหนดสัญญา โดยให้พนักงานชั้นบริหารอนุมัติรายการก่อน โดย Key รหัสของผู้บริหาร พนักงาน Operator จึงจะสามารถทำรายการต่อไปได้ เช่นเดียวกับกรณีที่เบิกถอนเงินแล้วเกิด Error Message ว่า "Balance short"

6. ตบตาคณะกรรมการและผู้สอบบัญชีเพื่อตบแต่งงบการเงิน

6.1 มูลเหตุ

การถอน No-Book

6.2 วิธีการทุจริต

เบิกเงินฝากประจำแบบ No-Book แล้วไม่ลงรายการทางบัญชี

6.3 วิธีการเบิกเงิน

ผู้ทุจริตเป็นผู้จัดการมีอำนาจลงนามถอนเงิน ได้ขอถอนเงินจากบัญชีเงินฝากประจำแบบ No-Book หลายล้านบาท โดยแจ้งกับธนาคารว่าจะนำสมุดคู่ฝากมาให้ Up date ในวันหลัง เงินที่เบิกไปนำไปใช้ส่วนตัว คณะกรรมการของกิจการคิดว่าเงินฝากประจำที่ธนาคารยังคงอยู่ เพราะสมุดคู่ฝากยังคงแสดงยอดเงินฝากครบเต็มจำนวน

6.4 การพบทุจริต

ผู้ทุจริตทำทุจริตหลายด้านแล้วหลบหนี คณะกรรมการติดต่อธนาคารขอถอนเงินตามสมุดคู่ฝาก แต่ธนาคารแจ้งว่าเงินฝากดังกล่าวถูกเบิกไปหมดแล้ว

6.5 การป้องกันการทุจริต

ศึกษาโครงสร้างการรับฝากและให้ถอนเงินของธนาคารที่ติดต่อด้วย หากธนาคารยอมให้ถอน No-book ได้ จะต้องขอคำยืนยันยอดต่อธนาคารตามมาตรฐานการสอบบัญชีแทนการดูยอดเงินคงเหลือจากสมุดคู่ฝากเท่านั้น

7. การทุจริตกับ ATM

7.1 มูลเหตุ

รายละเอียดในบัตร ATM และรหัส PIN หาได้ง่าย

7.2 วิธีการทุจริต

1. อุปกรณ์ที่จำเป็น คือ เครื่องอ่านและเขียนข้อมูลบนบัตร ATM
2. ยืนสังเกตดูการถอนเงินจาก ATM ของบุคคลอื่น แล้วจำรหัสที่กด (สามารถมองเห็นได้โดยง่าย หากทำทีเป็นว่ารอใช้เครื่อง ATM อยู่)
3. เมื่อบุคคลอื่นตาม 2 ถอนเงินเสร็จแล้วทิ้งบัตรบันทึกรายการไว้ เก็บบัตรนั้นมาจดรหัสที่จำไว้ด้วยกัน (รายใดไม่ทิ้งบัตรบันทึกรายการไว้ให้ก็ผ่านไป)
4. นำข้อมูลเลขที่บัตรจากบัตรบันทึกรายการไปทำข้อมูลใส่บัตร (ตัวบัตรอาจหาได้จากการขอใช้ ATM กับบัญชีของผู้ทุจริตเอง จากธนาคาร แล้วนำมาเปลี่ยนข้อมูล) โดยใช้เครื่องเขียนข้อมูลบนบัตร ATM

7.3 วิธีการเบิกเงิน

นำบัตร ATM ที่เปลี่ยนข้อมูลแล้วไปเบิกเงินจาก ATM โดยใช้รหัสที่จดจำมาแล้วนำบัตร ATM ไปเปลี่ยนข้อมูลใหม่เพื่อเบิกจากบัญชีอื่นต่อไป

7.4 การพบทุจริต

ลูกค้าธนาคารหลายรายแจ้งว่ายอดในบัญชีถูกถอนโดยบุคคลอื่น

7.5 การป้องกันการทุจริต

1. ลูกค้าไม่ควรทิ้งบัตรบันทึกรายการไว้กับเครื่อง ATM
2. ธนาคารไม่ควรให้เครื่อง ATM พิมพ์เลขที่บัตรหรือข้อมูลอื่นใด ๆ ในบัตร ATM ให้ปรากฏใน "บัตรบันทึกรายการ"
3. เวลาใช้ ATM พยายามระวังบุคคลอื่นเห็นการกดรหัส

7.6 กลุ่มผู้ที่อาจทุจริต

1. พนักงานธนาคารที่มีโอกาสใช้เครื่องอ่าน-เขียนข้อมูลบนบัตร ATM
2. พนักงานของบริษัทที่ขายเครื่องอ่าน-เขียนข้อมูลบนบัตร ATM

8. การโจรกรรมดอกเบี้ยเงินฝากออมทรัพย์

8.1 การคำนวณดอกเบี้ย

ธนาคารได้ใช้โปรแกรมสำหรับการคำนวณดอกเบี้ยในระบบงานเงินฝากออมทรัพย์ โดยมีสูตรดังนี้

$$\text{ดอกเบี้ย} = \frac{\text{เงินต้น x จำนวนวัน x อัตราดอกเบี้ย}}{36{,}500}$$

สำหรับจำนวนวันนั้นเป็นผลที่ได้จากการนำจำนวนวันที่คำนวณดอกเบี้ยถึงปัจจุบัน หรือวันที่มีรายการเคลื่อนไหว (Today Int. Date) หักด้วยจำนวนวันที่คำนวณดอกเบี้ยครั้งหลังสุด (Last calculated Int. Date) ซึ่งปกติ Today Int. Date จะมีค่ามากกว่า Last calculated Int. Date เสมอ เว้นแต่ในช่วงระยะเวลาคาบเกี่ยวระหว่างปลายปีเก่ากับต้นปีใหม่

กรณีที่ Today Int. Date มีค่าน้อยกว่า Last calculated Int. Date จำนวนวันที่ได้จะมีค่าน้อยกว่า 0 (ผลลบ) ซึ่งตามขั้นตอนการทำงานของโปรแกรมจะนำค่า 365 ไปบวกกับผลลบนั้น แล้วจึงนำผลลัพธ์ที่ได้ไปเข้าสูตรคำนวณดอกเบี้ยดังกล่าว

8.2 การใช้โปรแกรมสำหรับปรับจำนวนดอกเบี้ยค้างจ่าย

โดยปกติธนาคารจะใช้โปรแกรม Int 01 สำหรับปรับจำนวนดอกเบี้ยค้างจ่ายตอนสิ้นงวด การบัญชีมีผลทำให้ Accrued interest ใน Master saving file เพิ่มขึ้น แล้วจึงทำการ Post ดอกเบี้ยลงในการ์ดบัญชีให้แก่ลูกค้าแต่ละราย อย่างไรก็ตามโปรแกรมนี้สามารถคำนวณดอกเบี้ยล่วงหน้าจนถึงวันที่ต้องการได้ โดยเพียงแต่ป้อนเลขที่บัญชีและวันสิ้นสุดที่ต้องการ ดอกเบี้ยค้างจ่ายของบัญชีนั้นก็จะเพิ่มขึ้น

8.3 วิธีการโจรกรรม

1) ต้องทราบขั้นตอนการทำงานของโปรแกรมสำหรับคำนวณดอกเบี้ยประจำวัน
2) ต้องทราบชื่อโปรแกรม วิธีการเลือกใช้ ตลอดจนการใช้โปรแกรม
3) เมื่อทราบรายละเอียดการทำงานของโปรแกรมทั้งสองที่กล่าวข้างต้นแล้ว จะพบว่ามี จุดอ่อนหรือช่องทางในการกระทำทุจริตได้ กล่าวคือ ภายหลังจากใช้โปรแกรมปรับดอกเบี้ยค้างจ่าย Int 01 สำหรับคำนวณดอกเบี้ยล่วงหน้าแล้ว ในวันเดียวกันนั้นเองหากบัญชีนั้นมีรายการเคลื่อนไหว ไม่ว่าฝากหรือถอน จะมีผลทำให้ Today Int. Date น้อยกว่า Last calculated Int. Date และจำนวนวันที่ได้จะมีค่าเป็นผลลบ จากนั้นการคำนวณดอกเบี้ยจะเป็นไปตามเงื่อนไขในโปรแกรมตามที่กล่าวไว้ในข้อ 1 จำนวนดอกเบี้ยที่ได้รับจะเพิ่มขึ้นผิดปกติ ทั้งนี้เพราะจำนวนวันเพิ่มขึ้นมากเกินไปนั่นเอง

4) เมื่อผู้ทุจริตพบจุดอ่อนในระบบเงินฝากออมทรัพย์ตามข้อ 3.3) แล้ว ก็ให้ผู้ฝากเงินซึ่งเป็นพรรคพวกกับผู้ทุจริต (อาจเป็นพนักงานบัญชีประจำเครื่อง Banking Terminal) เปิดบัญชีกับธนาคารไว้

5) ผู้ทุจริตเรียกใช้โปรแกรมปรับดอกเบี้ยค้างจ่ายตอนสิ้นงวด คือ โปรแกรม Int 01 สำหรับคำนวณดอกเบี้ยล่วงหน้า (แม้ล่วงหน้า 1 วันก็ได้ แต่จะต้องมาเคลื่อนไหวบัญชีก่อนวันนั้น) โดยป้อนเลขที่บัญชีและวันที่สิ้นสุดการคำนวณดอกเบี้ย

6) ในวันเดียวกันนั้นก็ให้พรรคพวกนำเงินมาฝากหรือถอนเงินออกไป เพื่อให้เกิดรายการเคลื่อนไหวนั้น ซึ่งจะมีผลให้เกิดการคำนวณดอกเบี้ยประจำวันตามที่กล่าวไว้ในข้อ 8.3

7) เมื่อถึงวันสิ้นงวดการบัญชีก็จะทำการ Post ดอกเบี้ยค้างจ่าย (Accrued interest) ให้แก่บัญชีลูกค้าแต่ละราย เหมือนเช่นเคยปฏิบัติในระบบ Manual ซึ่งจะทำให้ยอดคงเหลือในบัญชีเพิ่มขึ้นเท่ากับจำนวนดอกเบี้ย

8) เมื่อ Post ดอกเบี้ยเสร็จแล้ว ก็ให้พรรคพวกถอนเงินออกไปจนเกือบหมด หรือปิดบัญชีแล้วแต่กรณี

8.4 การตรวจพบ

การโจรกรรมดอกเบี้ยด้วยวิธีดังกล่าว ไม่สามารถตรวจพบได้ง่าย ๆ เนื่องจาก

1) การเรียกใช้โปรแกรมปรับดอกเบี้ยค้างจ่ายตอนสิ้นงวด Int 01 มิได้ถูกบันทึกไว้เป็นหลักฐานในที่แห่งใดเลย

2) รายงาน Saving A/C Balance Listing ซึ่งแสดงยอดเงินคงเหลือ ยอดดอกเบี้ยสะสม (Accrued interest) ยอดรวมสุทธิ รหัสการค้ำประกันสินเชื่อ วันที่มาติดต่อกับธนาคารหลังสุด และจำนวนวันที่คำนวณดอกเบี้ยครั้งหลังสุด (Last calculated Int. Date) มิได้พิมพ์ทุกวัน แต่จะพิมพ์ทุกสิ้นเดือน (รายที่มีการคำนวณดอกเบี้ยล่วงหน้า Last calculated Int. Date) จะมากกว่ารายการอื่น ๆ ที่มีการเคลื่อนไหวในวันที่พิมพ์รายการดังกล่าว

3) ธนาคารมิได้ทดสอบการคำนวณดอกเบี้ยมาหลายปีแล้ว

8.5 การป้องกัน

1) แยกโปรแกรมปรับดอกเบี้ยค้างจ่ายตอนสิ้นงวด Int 01 ออกต่างหากจากแผ่นที่บรรจุโปรแกรมใช้งานประจำวัน
2) กำหนดเจ้าหน้าที่ผู้มีอำนาจเก็บรักษาและควบคุมการใช้โปรแกรมดังกล่าวอย่างเคร่งครัด
3) แก้ไขโปรแกรมดังกล่าวมิให้มีการปรับดอกเบี้ยเป็นกรณีล่วงหน้าได้

9. เลขที่เช็คนั้นสำคัญไฉน

9.1 มูลเหตุ

ธนาคารมีการเปลี่ยนการ์ดบัญชีเงินฝากรายตัว โดยมีกำหนดแน่นอน เช่น ทุกสิ้นเดือน พร้อมทั้งลอกรายการเบิกเช็คของลูกค้าไว้ตอนบนบัญชีเงินฝากรายตัว C/A ซึ่งเมื่อดูจากบัญชีรายตัวที่ยกยอดมาจะไม่ทราบว่าเช็คฉบับเลขที่เท่าไรได้เบิกไปแล้วบ้าง

9.2 วิธีการทุจริต

หลังวันเปลี่ยนการ์ดบัญชีรายตัว ผู้ทุจริตได้ปลอมเช็คของลูกค้าธนาคารหลายราย โดยให้เลขที่เช็คอยู่ในกลุ่มที่ลูกค้าแต่ละรายได้เบิกไป เมื่อนำไปเบิกเงิน ธนาคารเห็นว่าลายมือชื่อถูกต้อง ยอดเงินที่ขอเบิกอยู่ในวงเงิน และเลขที่เช็คตรงกับกลุ่มเช็คที่จ่ายให้ลูกค้า ธนาคารจึงผ่านรายการให้

9.3 วิธีการเบิกเงิน

1. นำเช็คไปเบิกเงินสด
2. นำเช็คไปฝากเข้าบัญชีที่ธนาคารอื่น ซึ่งได้เปิดบัญชีไว้ โดยใช้หลักฐานแสดงตัวผู้ฝากปลอม เมื่อเรียกเก็บเงินได้แล้วจึงเบิกเงินสดไปภายหลัง

9.4 การพบการทุจริต

เมื่อครบรอบเปลี่ยนการ์ดบัญชีกระแสรายวัน (Current Account) รายตัวครั้งต่อมาธนาคารได้ส่ง Statement ให้ลูกค้าแต่ละรายปรากฏว่ามีลูกค้ารายใหญ่หลายรายได้ทักท้วงมาว่า เช็คที่ธนาคารนำมาหักบัญชีนั้นไม่ใช่เช็คที่กิจการได้จ่ายไป และเลขที่เช็คบางรายการได้หักบัญชีไปแล้วในเดือนก่อน ๆ ธนาคารจึงได้เช็คสอบรายการและพบการทุจริต

9.5 การป้องกันการทุจริต

1. ทำบัตรซึ่งมีรายละเอียดเลขที่เช็คทุกฉบับที่ธนาคารจ่ายให้ลูกค้า เพื่อใช้ทำเครื่องหมายว่าเลขที่ใดได้ผ่านบัญชีแล้ว
2. ในกรณีที่มีการเบิกเงินจำนวนสูง ๆ เช่น 200,000 บาทขึ้นไป ให้โทรถามผู้สั่งจ่ายเพื่อขอคำยืนยัน
3. ใช้ตรายางประทับลงบนขอบเช็ค โดยให้ตรายางติดบนขอบเช็คบางส่วน และส่วนที่เหลือติดบนกระดาษอื่นก่อนที่จะจ่ายเช็คให้ลูกค้า เพื่อว่าเมื่อธนาคารได้รับเช็คสั่งจ่ายมา เมื่อใดก็จะนำมาต่อรอยดูว่าตรายางที่ประทับตรงกันหรือไม่ โดยอาจเช็คสอบเฉพาะเช็คที่มีจำนวนสูง ๆ

9.6 ใช้คอมพิวเตอร์ [1]

ในกรณีที่ธนาคารใช้คอมพิวเตอร์มักจะใช้คอมพิวเตอร์ตรวจสอบเลขที่เช็คของลูกค้าที่สั่งจ่ายมา หากลูกค้าเป็นผู้ที่ใช้เช็คมาก ๆ กล่าวคือ สมุดเช็คที่เบิกไปจากธนาคารเล่มก่อน ๆ ยังกลับมาหักบัญชีไม่ครบทุกฉบับ ถ้าลูกค้ามาขอเบิกสมุดเช็คใหม่อีก และเนื้อที่เก็บข้อมูลเลขที่เช็คเต็ม ธนาคารจะใช้วิธีการตัดเลขที่เช็คบางชุดออก ดังนั้น หากเช็คฉบับใดมีเลขที่อยู่ในกลุ่มเลขที่ที่ถูกตัดออก แต่เพิ่งนำมาเบิกเงินก็จะไม่สามารถผ่านรายการได้ เว้นแต่ผู้มีอำนาจจะ Key รหัสลับให้คอมพิวเตอร์ผ่านให้หลังจากที่ตรวจสอบเลขที่เช็คแล้ว ซึ่งส่วนใหญ่จะใช้วิธีดูทะเบียนจ่ายเช็คว่าได้จ่ายให้ไปหรือไม่ จึงอาจเกิดการทุจริตในทำนองเดียวกันได้ หากเช็คดังกล่าวเป็นเช็คปลอมตามแบบอย่างข้างต้น

9.7 การป้องกัน

1) ทำรายละเอียดเลขที่เช็คที่ยังไม่มาผ่านบัญชี แต่ถูกตัดออกจากระบบคอมพิวเตอร์แล้วให้อยู่ในความรับผิดชอบของผู้มีอำนาจ เพื่อใช้ตรวจสอบเมื่อมีเช็คดังกล่าวมาขอผ่านบัญชี
2) ธนาคารใดให้คอมพิวเตอร์ตรวจสอบแบบเป็นช่วง เช่น เช็คที่มาเบิกเงินเลขที่ 10004 อยู่ในช่วงของเลขที่ 10001 ถึง 10020 ที่ธนาคารจ่ายให้ลูกค้า ควรเพิ่มเป็นการควบคุมเลขที่รายฉบับ และการควบคุมรายฉบับนี้หากควบคุมได้ยิ่งมากโอกาสทุจริต ก็จะยิ่งน้อยลง

10. กำจัดคู่แข่งโดยใช้โปรแกรมคอมพิวเตอร์

10.1 มูลเหตุ

กำจัดคู่แข่งทางธุรกิจ

10.2 วิธีการ

สายการบินบรานิฟของสหรัฐซึ่งเลิกกิจการเมื่อต้นปี 2525 ได้แจ้งต่อคณะกรรมการการบินพลเรือนและคณะลูกขุนกลาง ที่เมืองฟอร์ดเวิร์ธ ว่า สายการบินอเมริกันแอร์ไลน์ โดย นายโรเบิร์ต แครนแดลล์ ประธานบริษัท ได้ใช้ "ระบบจองตั๋วเครื่องบินแบบเซเบอร์ (Sabre-Reservation System)" ซึ่งเป็นระบบที่ทันสมัยมากที่สุดของวงการท่องเที่ยว ในการลบชื่อหรือยกเลิกการจองตั๋วเที่ยวบินของสายการบินบรานิฟ

การที่ นายโรเบิร์ต แครนเดลล์ ประธานสายการบินอเมริกันแอร์ไลน์ ทำเช่นนั้นได้ ก็เพราะเป็นผู้เชี่ยวชาญด้านคอมพิวเตอร์ และเป็นผู้พัฒนาระบบการจองตั๋วเครื่องบินเซเบอร์ขึ้นเอง

---

[1] เมื่อธนาคารเปลี่ยนระบบจาก Manual ไปสู่ระบบ Computer แล้ว ถึงแม้ระบบจะมีการตรวจสอบเลขที่เช็คอัตโนมัติ ก็มีการทุจริตได้โดยมีตัวอย่างเกิดขึ้นจริง ๆ แล้ว

10.3 ความเสียหาย

300 ล้านเหรียญสหรัฐ และเลิกกิจการ

10.4 การป้องกัน

-

10.5 ข้อพึงสังวร

ธนาคารหรือธุรกิจที่ใช้คอมพิวเตอร์ประเภทที่ใช้สายสื่อสาร เช่น ใช้โทรศัพท์ อาจถูกกลั่น-แกล้ง ทุจริต จากบุคคลต่อไปนี้

ก. บุคคลที่สามที่รับพัฒนาระบบให้

ข. บุคคลภายในองค์การที่เป็นผู้พัฒนาระบบเอง

ทั้งนี้เพราะการกระทำดังกล่าวไม่จำเป็นที่จะต้องเข้าใกล้เครื่องมืออุปกรณ์ หรือคอมพิวเตอร์ขององค์การเลย แต่ใช้โทรศัพท์ติดต่อแทน

11. ผู้บริหารสร้าง Input ปลอม

11.1 ผู้ทุจริต

ประธานกรรมการบริษัท Equity Fund Corp.

11.2 ผู้เสียหาย

ผู้ลงทุนซื้อหุ้นของบริษัท บริษัทรับช่วงซื้อกรมธรรม์

11.3 สาเหตุ

เพื่อสร้างฐานะของบริษัทให้เจริญเติบโตกว่าความเป็นจริง ทำให้หุ้นมีมูลค่าสูงขึ้น และขายกรมธรรม์ปลอมให้แก่บริษัทรับช่วงได้มากขึ้น

11.4 วิธีการ

สร้างกรมธรรม์ปลอม Input สู่ระบบโดยใช้รหัสว่า Issued by Department 99' และเมื่อผู้สอบบัญชีให้สุ่มตัวอย่างเพื่อตรวจสอบ ก็จะแฝงคำสั่งให้ข้ามขั้นตอนการ List รหัสข้างต้น

11.5 การค้นพบ

พนักงานของบริษัทที่ถูกไล่ออกได้ไปแจ้งการทุจริตที่เกิดขึ้นต่อ New York State Insurance Department และ New York Stock Exchange

11.6 การลงโทษ

ผู้บริหารได้รับการตัดสินให้ถูกจำคุก

12. การทุจริตโดยการใช้จุดอ่อนของแบบฟอร์มที่ Input ในระบบอัตโนมัติ (Micr)

12.1 ผู้ทุจริต

ลูกค้าของธนาคาร

12.2 ผู้เสียหาย

ธนาคารแห่งหนึ่ง

12.3 สาเหตุ

เนื่องจากจุดอ่อนของแบบฟอร์มใบรับฝากที่ใช้ Micr ที่ได้ออกให้กับลูกค้าไว้ล่วงหน้า และการปฏิบัติงานที่เตรียมไว้กรณีลูกค้าลืมนำใบนำฝากมา

12.4 วิธีการ

ผู้ทุจริตใช้ใบรับฝากที่มีเลขที่บัญชีของตนไปปนกับใบนำฝากที่ลูกค้าต้องใช้หากลืมนำใบรับฝากมา เมื่อพนักงานเห็นใบรับฝากมีเลขที่บัญชีแล้ว ก็จะพิมพ์จำนวนเงินด้วย Micr ให้ผ่านไปได้

12.5 การค้นพบ

ไม่ได้กล่าวถึง

12.6 การลงโทษ

ผู้ทุจริตไม่ถูกลงโทษ เนื่องจากได้ถอนเงินทั้งสิ้นในเวลาใกล้ปิดทำการและหลบหนีไป

การทุจริตทางด้าน INPUT

13. เพิ่มรายชื่อผู้มีสิทธิออกเสียงเลือกตั้ง

ผู้ทุจริต	พนักงาน Data Entry
ผู้เสียหาย	Board of Election, New York
สาเหตุ	หวังผลทุจริตในการเกี่ยวข้อง
วิธีการ	เพิ่มรายชื่อผู้ที่ยังไม่มีสิทธิออกเสียงเลือกตั้งหลายร้อยชื่อใน File ผู้มีสิทธิออกเสียง
การค้นพบ	ไม่ได้กล่าวถึง
การลงโทษ	ไม่ได้กล่าวถึง

14. เพิ่มรายชื่อของผู้สอบผ่านการขอรับใบขับขี่

ผู้ทุจริต พนักงาน Data Entry
ผู้เสียหาย board of Election, New York
สาเหตุ ได้รับค่าจ้างรายละ $200-400 (ทำให้เขามีรายได้ถึง $300,000)
การค้นพบ ไม่ได้กล่าวถึง
การลงโทษ ไม่ได้กล่าวถึง

การทุจริตทางด้าน PROCESSING

15. การใช้โปรแกรมที่ผู้ทุจริตจัดทำขึ้นเพื่อลักลอบแก้ไข หรือ List ข้อมูลที่เก็บในระบบ

ผู้ทุจริต TRW Credit Data of Anaheim ซึ่งเป็นกิจการที่ให้บริการด้านข่าวสารและข้อมูลประวัติด้านสินเชื่อ
ผู้เสียหาย กิจการ Credit Card
สาเหตุ ได้รับค่าจ้างในการเปลี่ยนประวัติประมาณร้อยละ $300-1,500
การค้นพบ กิจการ Credit Card ร้องเรียน และคณะลูกขุนได้ฟ้องร้องแก่พนักงาน TRW
การลงโทษ ไม่ได้กล่าวถึง

16. ใช้ Password ที่ล่วงรู้มายักยอกเอาวัสดุที่ใช้ติดตั้งโทรศัพท์ไปขาย

ผู้ทุจริต Schneider
ผู้เสียหาย บริษัท Pacific Telephone & Telegraph Company
สาเหตุ ผู้ทุจริตเห็นแบบฟอร์มการขอเบิกพัสดุโทรศัพท์และคู่มือการขอเบิกพัสดุทิ้งในถังขยะ ทำให้สามารถเชื่อมโยงระบบ password ในการเบิกพัสดุได้ทั้งหมด
วิธีการ ผู้ทุจริตซื้อ Terminal แบบเดียวกับที่ผู้เสียหายใช้ และทดสอบการส่ง password เพื่อขอเบิกพัสดุให้ส่งไปยังจุดที่นัดหมาย
การค้นพบ Schneider ให้พนักงานผู้หนึ่งออกจากงาน และพนักงานผู้นั้นได้นำเรื่องไปแจ้งตำรวจ
การลงโทษ ค่าเสียหายประมาณหลายล้านเหรียญสหรัฐ แต่อัยการหาหลักฐานพิสูจน์ได้เพียง $5,000 ศาลสั่งลงโทษจำคุก 60 วัน แต่ถูกขังจริงเพียง 40 วัน

17. โจรกรรมเงินจากเครื่องจ่ายเงินอัตโนมัติ

ผู้ทุจริต วิศวกรไฟฟ้าชาวฝรั่งเศส

ผู้เสียหาย ธนาคารแห่งหนึ่ง

สาเหตุ ผู้ทุจริตสนใจและพยายามศึกษาเพื่อปลอมบัตร

วิธีการ ผู้ทุจริตศึกษา pattern ของข้อมูลที่บรรจุในแถบแม่เหล็ก และหลอกถามเลขที่บัญชีจากลูกค้าของธนาคาร

การค้นพบ เครื่องจ่ายเงินอัตโนมัติเครื่องหนึ่งขัดข้อง ไม่คืนบัตรให้ผู้ทุจริต ต่อมาพนักงานธนาคารค้นพบและดักซุ่มรอจับตัวเมื่อผู้ทุจริตได้กลับมาทดลองถอนเงินใหม่

การลงโทษ ไม่ได้กล่าวถึง (ค่าเสียหายประมาณ F. Fr 60,000)

การทุจริตโดยการขโมยความลับของข้อมูล

18. List รายชื่อลูกค้าไปขายให้บริษัทคู่แข่ง

ผู้ทุจริต พนักงานควบคุมเครื่องของบริษัทเอง

ผู้เสียหาย บ. Encyclopedia britanica

สาเหตุ ไม่ได้กล่าวถึง

วิธีการ List รายชื่อลูกค้าไปขายให้แก่บริษัทคู่แข่ง และบริษัทที่ขายสินค้าทางไปรษณีย์

การค้นพบ ไม่ได้กล่าวถึง

การลงโทษ ไม่ได้กล่าวถึง (ค่าเสียหายประมาณไม่ต่ำกว่า $1 ล้าน)

19. List รายชื่อไปขายให้บริษัทขายสินค้าทางไปรษณีย์

อีก 2 Case เกิดขึ้นในทำนองเดียวกัน

ผู้ทุจริต พนักงานควบคุมเครื่องของบริษัทเอง

ผู้เสียหาย Illinois Driver Registration Bureau

สาเหตุ ได้รับสินบนจากบุคคลภายนอกเป็นเงิน $10,000

วิธีการ ไม่ได้กล่าวถึง

การค้นพบ ไม่ได้กล่าวถึง

การลงโทษ ไม่ได้กล่าวถึง

20. โจรกรรมโปรแกรมควบคุมการทำงานของคอมพิวเตอร์

ผู้ทุจริต University Computing Company (U.C.C.) Inc. ซึ่งเป็นคู่แข่งกับ I.S.D.

ผู้เสียหาย Information System Design Inc. (I.S.D.)

สาเหตุ เนื่องจากบริษัท I.S.D. สามารถพัฒนาระบบ Plot/Trans ซึ่งสามารถ Plot graph ด้วยเทอร์มินอลธรรมดา และสามารถให้บริการอันรวดเร็วแก่ลูกค้าที่อยู่ห่างไกล U.C.C. ก็พยายามที่จะพัฒนาระบบนี้ แต่ยังไม่ประสบผลสำเร็จ

มูลเหตุจูงใจที่สำคัญคือ ทั้ง 2 บริษัทต่างแข่งขันในการให้บริการแก่ลูกค้ารายเดียวกัน

วิธีการ พนักงานพัฒนาโปรแกรมอาวุโสของ U.C.C. ได้ใช้ Terminal ที่ U.C.C. ทำการ Access เพื่อดึงความลับของโปรแกรม plot/trans ของ I.S.D. มาพิมพ์ที่ Terminal ของ U.C.C.

ผู้ทุจริตได้เข้าไปตีสนิทกับพนักงานของลูกค้า I.S.D. เพื่อทราบหมายเลขโทรศัพท์คู่สายและ password

การค้นพบ การขโมยความลับดังกล่าวจากบันทึกใน control loan ของ I.S.D. เพื่อเรียกเก็บเงินจากลูกค้าปรากฏว่าลูกค้าปฏิเสธการจ่ายเงิน เนื่องจากไม่เคยใช้บริการในลักษณะนี้มาก่อน I.S.D. เพ่งเล็งความสนใจมาที่ U.C.C. และต่อมา I.S.D. ได้ขอความร่วมมือกับเจ้าหน้าที่ตำรวจเพื่อตรวจค้นข้อมูลในส่วนความจำ และอุปกรณ์จัดเก็บข้อมูลของระบบคอมพิวเตอร์ของ U.C.C. ปรากฏว่าได้พบโปรแกรมที่ขโมยมา ถูกถ่ายทอดเก็บไว้ในเทปแม่เหล็ก

การลงโทษ พนักงานพัฒนาโปรแกรมของ U.C.C. ถูกปรับ $5,000 รอลงอาญา 3 ปี ขณะที่ U.C.C. ถูกฟ้องในฐานะจำเลยร่วม และต้องชดใช้ค่าเสียหายเป็นเงิน $300,000

21. เพิ่มรายชื่อเพื่อรับประโยชน์ TAX Refund

ผู้ทุจริต พนักงาน Data Entry ของ IRS (Internal Revenue Service)

ผู้เสียหาย -

สาเหตุ ผู้ทุจริตเป็นหลานของสตรีชราผู้หนึ่ง ซึ่งยังชีพด้วยเงินสวัสดิการประกันสังคม

วิธีการ เพิ่มรายชื่อใน File ของผู้มีสิทธิได้รับ TAX Refund และพิมพ์เช็คสั่งจ่ายพร้อมหลักฐานการขอรับเงิน

การค้นพบ พนักงานธนาคารจำได้ว่าสตรีผู้นี้ยังชีพด้วยเงินสวัสดิการสังคมเพียงอย่างเดียว จึงไม่ควรที่จะได้รับ Tax Refund อีก จึงรายงานข้อสงสัยไปยัง IRS

การลงโทษ ไม่ได้กล่าวถึง

22. ยักยอกเงินฝากของลูกค้า

ผู้ทุจริต พนักงาน Teller ของ Union Dime Saving Bank

ผู้เสียหาย ลูกค้าของธนาคารและธนาคาร

สาเหตุ เกิดจากจุดอ่อนในระบบการควบคุมที่ยินยอมให้ผู้มีหน้าที่รับเงินเป็นผู้บันทึกรายการรับเงินเองทุกวัน นอกจากนี้ยังมีจุดอ่อนในการพิมพ์ใบยืนยันยอดให้ลูกค้าที่พิมพ์บัญชีเงินฝากออมทรัพย์และบัญชีเงินฝากประจำต่างวันกัน

วิธีการ เมื่อลูกค้ามาฝากจะลงรายการใน passbook ตามปกติ แต่เมื่อลูกค้ากลับไปจะทำรายการ Reverse และบันทึกรายการฝากในจำนวนที่น้อยกว่า

เมื่อลูกค้ามาถอนจะนำเงินที่ยักยอกมาบางส่วนจ่ายให้ลูกค้าไปการพิมพ์ใบยืนยันยอดต่างวัน ทำให้ผู้ทุจริตสามารถโอนเงินจากบัญชีหนึ่งมายังบัญชีที่ยักยอก เพื่อให้ยอดคงเหลือในใบยืนยันยอดเท่ากับยอดใน passbook

การค้นพบ ตำรวจจับเจ้ามือการพนันและพบรายชื่อผู้ทุจริตในฐานะลูกค้ารายใหญ่ จึงเกิดความสงสัย เนื่องจากผู้ทุจริตไม่อยู่ในฐานะที่จะทำเช่นนั้นได้

การลงโทษ ผู้ทุจริตถูกศาลสั่งจำคุก 20 เดือน ในข้อหายักยอกเงิน $1.5 ล้าน แต่ถูกขังจริงเพียง 15 เดือน เนื่องจากความประพฤติเรียบร้อย

23. การสร้างรายการฝากเงินโดยไม่มีเอกสารประกอบ

1. ผู้ทุจริต : เพศหญิง สมรสแล้ว (ไม่ได้จดทะเบียน) ตำแหน่งพนักงานระดับ Supervisor ของสาขาธนาคารพาณิชย์แห่งหนึ่งในกรุงเทพฯ

2. สาเหตุ :
   - ด้านองค์กร
     - 2.1) การป้อนรหัสประจำตัว (ID) และรหัสผ่าน (Password) ของผู้อนุมัติรายการ ต้องกระทำที่เครื่อง Terminal เดียวกับเครื่องที่พนักงาน Teller บันทึกรายการ เป็นโอกาสให้ผู้อื่นสังเกตเห็นและแอบจดจำรหัสดังกล่าวไว้ได้
     - 2.2) มีจุดอ่อนในการควบคุมการปฏิบัติงาน โดยผู้อนุมัติรายการมักจะค้างหรือทิ้งกุญแจไว้ที่เครื่อง Terminal อันเป็นช่องทางให้ผู้ทุจริต สามารถทำการทุจริตได้โดยการอนุมัติรายการให้ผ่านไปได้

3. ระยะเวลา : ระหว่างเวลา 8.00-15.00 น. ของวันทำการ 1 วัน

4. วิธีการ : ผู้ทุจริตได้สร้างรายการฝากเงินในลักษณะที่ไม่มีเอกสารประกอบ (Key ลอย) ด้วยรหัสรายการฝากด้วยบิล (เช่น Demand Draft, Mail Transfer, Telegraphic transfer หรือ Inter-office Payment เป็นต้น) ซึ่งจะไปเพิ่มยอดคงเหลือที่สามารถถอนได้ในบัญชีเงินฝากทันที โดยใช้รหัสผ่านที่ถูกต้องจากจุดอ่อนข้างต้น ทั้งสองประการ แล้วตระเวนถอนเงินสดตามสาขาต่าง ๆ จนหมดเวลาทำการของธนาคารพาณิชย์ในวันนั้น

5. มูลค่าความเสียหาย : ประมาณ 8,000,000 บาท (เตรียมการไว้ 15,000,000 บาท แต่ถูกจับกุมก่อน)

6. การค้นพบ : จากการตรวจสอบบัญชีประจำวันของสาขา พบว่าไม่มีหลักฐานเอกสารการนำเงินเข้าบัญชีเงินฝาก ดังปรากฏในคอมพิวเตอร์ พร้อมกับการหายตัวของผู้ทุจริต

7. จุดจบ :
- ยังไม่สามารถจับกุมตัวผู้ทุจริตได้
- เจ้าหน้าที่ตำรวจได้จับกุมตัวสามีซึ่งเชื่อว่ามีส่วนรู้เห็นและควบคุมตัวไว้เป็น ผู้ต้องหา ตั้งแต่วันที่ 31 สิงหาคม 2531

8. การป้องกันและแก้ไข :

8.1) ควรปรับปรุงระบบงานโดยเปลี่ยนแปลงให้ผู้อนุมัติรายการป้อนรหัสประจำ ตัว (ID) และรหัสผ่าน (Password) ที่เครื่อง Terminal อื่นแยกต่างหากจากเครื่อง Terminal ที่พนักงาน Teller บันทึกรายการ เพื่อป้องกันมิให้ผู้อื่นแอบสังเกตเห็น และจดจำรหัสได้ในขณะที่กำลังป้อนข้อมูล

8.2) กำชับให้ผู้อนุมัติรายการบิดกุญแจปิด และดึงกุญแจออกทุกครั้งหลังจากอนุมัติรายการเสร็จแล้ว



24. ตัวอย่างการทุจริตและการวิเคราะห์โดยย่อ

การทุจริตโดยใช้เลขที่บัญชีและบัตร ATM ของลูกค้า

1. ผู้ทุจริต : พนักงานสาขาธนาคารพาณิชย์ผู้มีหน้าที่เกี่ยวกับระบบงานเงินฝาก

2. สาเหตุ : องค์กรมีจุดอ่อนในการควบคุมจัดเก็บ :
   - 2.1 บัตรและใบแจ้งรหัส ATM ที่ยังมิได้จ่ายให้ลูกค้า
   - 2.2 เช็ครอเรียกเก็บ
   - 2.3 ใบนำฝากเข้าบัญชี

3. ระยะเวลา : อย่างต่ำ 1 วันทำการ และขึ้นกับการรอรับคืนบัตร ATM จากบริษัทลูกค้า

4. วิธีการ : ยักยอกบัตรและรหัส ATM ของลูกค้าที่บริษัทส่งกลับคืนมาเนื่องจากลูกค้าลาออกแล้ว และยักยอกเช็คที่ธนาคารรับไว้เพื่อเรียกเก็บเงินในวันรุ่งขึ้น พร้อมทั้งแก้ไขเลขที่บัญชีเงินฝากมาเป็นของรายที่ได้ยักยอกบัตร ATM ไว้ แล้วจึงถอนเงินจากเครื่อง ATM หลังจากเช็คผ่านการเรียกเก็บแล้ว

5. มูลค่าความเสียหาย : 13,000 บาท

6. การค้นพบ : เมื่อวันที่ 28 ธันวาคม 2531 เจ้าของบัญชีที่แท้จริงมาแจ้งว่าไม่มีเงินเข้าบัญชี พร้อมทั้งแสดงใบนำฝากเช็คเข้าบัญชีเป็นหลักฐาน ซึ่งผู้จัดการสาขาตรวจสอบใบนำฝากแล้วเห็นว่าถูกต้อง จึงนำเงินเข้าบัญชีให้ และได้แจ้งให้ฝายบริหารกิจการสาขา สำนักงานใหญ่ทราบเพื่อดำเนินการสอบสวนต่อไป

7. จุดจบ : สำนักงานใหญ่ได้ดำเนินการสอบสวนพนักงาน 3 คน คือ
   - 7.1 พนักงานระดับสอง ผู้รับเช็คเข้าบัญชีของลูกค้าที่แท้จริง และเป็นผู้นำเช็คส่งให้สมุห์บัญชี
   - 7.2 พนักงานระดับประจำสาขา ผู้ทุจริต และผลจากการสอบสวนยอมสารภาพว่าได้นำบัตร ATM ไปถอนเงินจริง

7.3 พนักงานธุรการ เป็นผู้นำบัตร ATM ไปถอนเงินให้ผู้ทุจริต สำนักงานใหญ่ให้ผู้ทุจริตและพนักงานธุรการลาออก

8. **การป้องกันและแก้ไข** :

8.1 ธนาคารแจ้งบริษัทให้เปลี่ยนการขอเปิดบัญชีโดยตัวแทนบริษัทขอเปิด มาเป็นให้พนักงานแต่ละคนเปิดบัญชีและรับบัตร ATM ด้วยตนเอง

8.2 เพิ่มความระมัดระวังในการพิจารณาการขอเปิดบัญชีโดยขอดูบัตรประจำตัว และหลักฐานอื่นอย่างเข้มงวด

8.3 การเก็บรักษาบัตร ATM ของลูกค้ารายที่ยังไม่มารับบัตรควรอยู่ในความดูแลของเจ้าหน้าที่ระดับบริหารอย่างใกล้ชิด



บทที่ 7

การค้นหาข้อมูลจากส่วนความจำของคอมพิวเตอร์เพื่อดำเนินคดี

การค้นหาข้อมูลจากส่วนความจำของคอมพิวเตอร์เพื่อดำเนินคดี

บทนำ

การทุจริตในหลาย ๆ กรณีตามที่ได้กล่าวมาโดยสรุปในบทก่อน ๆ หน้านั้น ในบางเรื่องมีรายละเอียดที่น่าสนใจสำหรับท่านผู้อ่าน จึงได้นำข้อมูลบางส่วนมากล่าวทบทวนเพิ่มเติมในบทนี้

การทุจริตโดยการใช้อุปกรณ์คอมพิวเตอร์โดยผู้ไม่มีอำนาจหน้าที่

ข้อที่ควรระวังของการใช้ระบบ Password ก็คือ Password อาจรั่วไหลได้ง่ายซึ่งถ้าผู้ใดก็ตามสามารถล่วงรู้ Password ย่อมสามารถสั่งให้คอมพิวเตอร์ปฏิบัติงานเท่ากับผู้เป็นเจ้าของ Password ทุกประการ Password อาจรั่วไหลได้ด้วยเหตุต่อไปนี้

1. เกิดจากความไม่ระมัดระวังในการเก็บรักษา Password

ในกรณีตัวอย่าง นักเรียน High School วิทยาลัยแห่งหนึ่งในสหรัฐอเมริกา พบกระดาษจด Password ของพนักงานพัฒนาระบบประจำวิทยาลัยในถังขยะ จึงได้ใช้ Password นั้นใช้เวลาของคอมพิวเตอร์จำนวนมากในการเล่น Computer Game

2. กรณีน่าศึกษาและ Pacific Telephone Telegraph Company ในเรื่อง Password

เกิดจากความสนิทสนมส่วนตัวระหว่างผู้ที่ทราบ Password และผู้ที่ต้องการจะทราบ Password หรือบางครั้งผู้ที่ต้องการทราบ Password อาจเชื่อมโยง Password ในแบบ Jigsaw Puzzle ดังเช่นตัวอย่างในกรณี Jerry and Schneider ได้เดินผ่านที่ทิ้งขยะของ Pacific Telephone & Telegraph Company (PT & TC) ใน Los Angeles ตั้งแต่เป็นนักเรียน High School เขาสังเกตเห็นแบบฟอร์มการขอเบิกพัสดุโทรศัพท์ ตลอดจนคู่มือการเบิกพัสดุทิ้งอยู่ จึงพยายามศึกษาวิธีการขอเบิกพัสดุทางโทรศัพท์

ระบบการเบิกพัสดุของบริษัทฯเป็นระบบอัตโนมัติ ผู้ได้รับมอบหมายให้เบิกพัสดุจะแจ้ง Password ไปยังศูนย์คอมพิวเตอร์ของบริษัทฯ โดย Remote Terminal ผ่านสายโทรศัพท์ไปยังคอมพิวเตอร์ IBM 360 คอมพิวเตอร์จะตรวจสอบ Password ซึ่งถ้าถูกต้องก็จะให้ผู้ที่มี Password แจ้งรายการอุปกรณ์โทรศัพท์ที่ขอเบิกตลอดจนสถานที่และเวลาส่งของ จากนั้นคอมพิวเตอร์จะส่งรายการขอเบิกนี้พิมพ์แจ้งไปยังหน่วยพัสดุ ซึ่งจะจัดพัสดุที่ขอเบิกส่งไปยังสถานที่และเวลาซึ่งนัดหมายไว้ต่อไป ราคาพัสดุที่เบิกจะลงบัญชีโครงการ (Project) ที่เจ้าของ Password สังกัดอยู่ระบบการเบิกพัสดุนี้บริษัทฯ กล่าวว่าช่วยให้การดำเนินงานตามโครงการติดตั้งโทรศัพท์ครอบคลุมทั้งรัฐ California ของบริษัทฯ ดำเนินไปอย่างมีประสิทธิภาพและรวดเร็ว

ต่อมา Schneider เข้าศึกษาในคณะวิศวกรรมศาสตร์ใน University of California at Los Angeles (UCLA) ทำให้เข้าถึงกลไกของระบบคอมพิวเตอร์และระบบรหัสลับมากขึ้น เขาพยายามสนิทสนมกับพนักงานของบริษัทฯ ตลอดจนสัมภาษณ์พนักงานเหล่านั้นในฐานะนักศึกษาเตรียมเขียนวิทยานิพนธ์ในหัวข้อเรื่อง Computerized Warehouse System ทำให้ Schneider สามารถเชื่อมโยงระบบ Password ในการเบิกพัสดุได้ทั้งหมด

ในเดือนมิถุนายน ค.ศ. 1971 Schneider ซื้อ Terminal แบบเดียวกับที่บริษัทใช้ และทดสอบส่ง Password เพื่อขอเบิกพัสดุโทรศัพท์มีมูลค่า $300,000 ให้ส่งไปยังจุดที่นัดหมาย ซึ่งปรากฏว่าได้ผล

Schneider ได้ตั้งบริษัทชื่อ Los Angeles Telephone & Telegraph Company เพื่อขายอุปกรณ์โทรศัพท์ซึ่งยักยอกจาก PT & TC ผ่านทางระบบการเบิกโดยใช้ Password ตลอดมา และกิจการได้ขยายขึ้นจนมีโกดังเก็บของขนาด 6,000 ตารางฟุตและมีพนักงานในสังกัด 10 คน

ในเดือนมกราคม ค.ศ. 1972 Schneider ให้พนักงานผู้หนึ่งออกจากงานพนักงานผู้นั้นได้นำเรื่องไปแจ้งตำรวจ จากการสอบสวนพบว่าพัสดุโทรศัพท์ที่ Schneider ยักยอกในช่วงเวลา 2 ปีที่ผ่านมา มีมูลค่าประมาณหลายล้านเหรียญสหรัฐ แต่พนักงานอัยการสามารถหาหลักฐานพิสูจน์ต่อศาลได้เพียง $5,000 ศาลพิพากษาลงโทษจำคุก 60 วันแต่เขาถูกจองจำเพียง 40 วัน เนื่องจากประพฤติดี

หลังจากพ้นโทษ Schneider ได้ตั้งบริษัทที่ปรึกษาทางด้านรักษาความปลอดภัยของระบบข้อมูลคอมพิวเตอร์ และยังได้แต่งหนังสือเกี่ยวกับอาชญากรรมที่ได้กระทำ ซึ่งบริษัทสร้างภาพยนตร์ขอซื้อลิขสิทธิ์เพื่อนำไปสร้างภาพยนตร์ โดยให้ค่าตอบแทนที่สูง

3. ระบบ Password อาจรั่วไหลเนื่องจากจุดอ่อนในโปรแกรม Operating System เอง

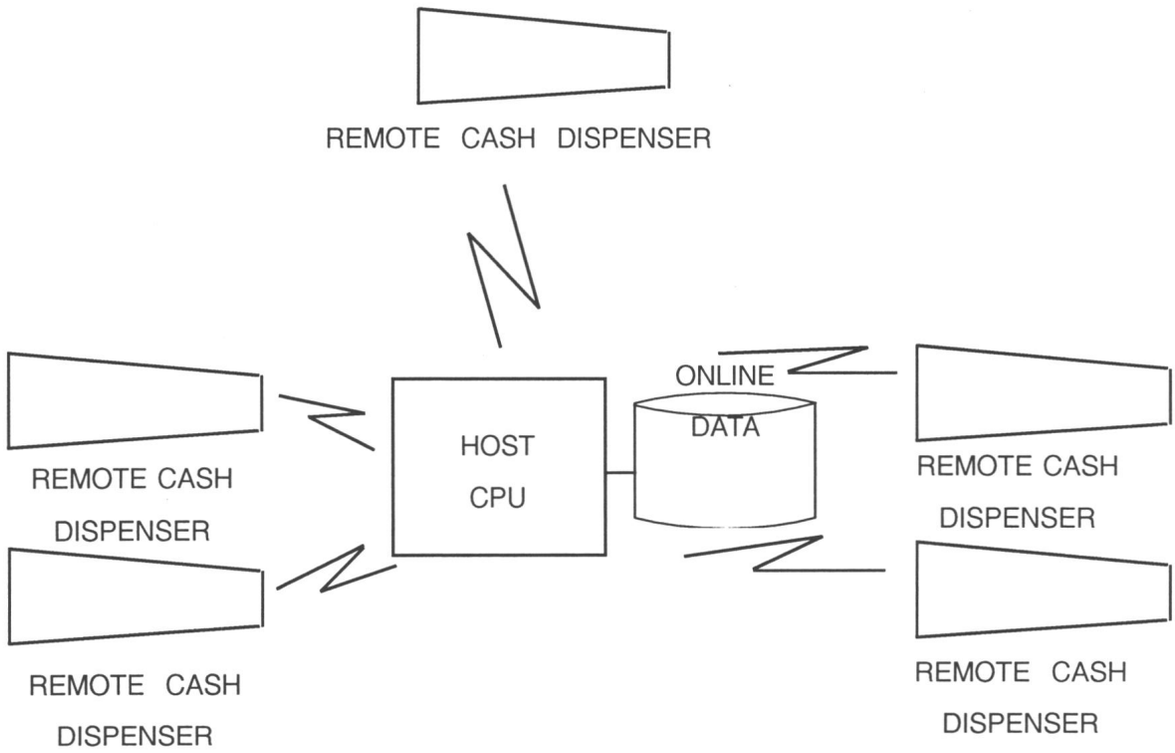
ตัวอย่างเช่น ระบบการใช้ Authorized Table ที่ผ่านมา เนื่องจาก Authorized Table ถูกจัดเก็บในแผ่นจานแม่เหล็ก ดังนั้นผู้ที่ต้องการทราบ Password อาจใช้ Utility Routine ทำการ Dump ข้อมูลในแผ่นจานแม่เหล็กเพื่อทราบถึง Password ที่บันทึกใน Table หรืออาจใช้ Routine ที่ใช้ Maintenance Table ทำการแก้ไข Authorized Table เพื่อผลในทางทุจริต เช่น เพิ่ม Password สำหรับผ่านเข้าสู่ระบบ แล้วแก้ไข Security Level ของ บาง Password

เนื่องจากการใช้ระบบ Password เพื่อ Identify ผู้ใช้ต่อระบบคอมพิวเตอร์มีจุดอ่อนในด้านที่รั่วไหลได้ง่าย ในระบบที่มีการระมัดระวังอย่างเคร่งครัด จึงนิยมใช้วิธีอื่นประกอบด้วย เช่น

- ใช้ Badge/Card Reader ซึ่งอ่านเครื่องหมายและบัตรที่ออกให้ผู้ใช้แต่ละราย และตรวจสอบว่า Badge/Card Reader นั้นถูกต้องหรือไม่
- ตรวจคุณสมบัติทางร่างกายของผู้ใช้ เช่น ลายนิ้วมือหรือคลื่นเสียง แล้วเปรียบเทียบกับข้อมูลเกี่ยวกับผู้ใช้ที่จัดเก็บไว้ว่าตรงกัน

ข้อที่ควรสังวรณ์ก็คือ ไม่ว่าจะมีระบบป้องกันการ Access อุปกรณ์คอมพิวเตอร์รัดกุมเพียงใดก็ตาม ผู้ที่จงใจทุจริตย่อมหาทางผ่านมาตรการป้องกันโดยวิธีที่แยบยลได้เสมอ

ในปี ค.ศ. 1974 วิศวกรไฟฟ้าชาวฝรั่งเศสผู้หนึ่งถูกจับในข้อหาขโมยเงินประมาณ F.Fr. 60,000 จากเครื่องจ่ายเงินอัตโนมัติในเมืองใหญ่ของฝรั่งเศส 4 เมือง



แผนภาพ การถอนเงินผ่าน
เครื่องจ่ายเงินอัตโนมัติ

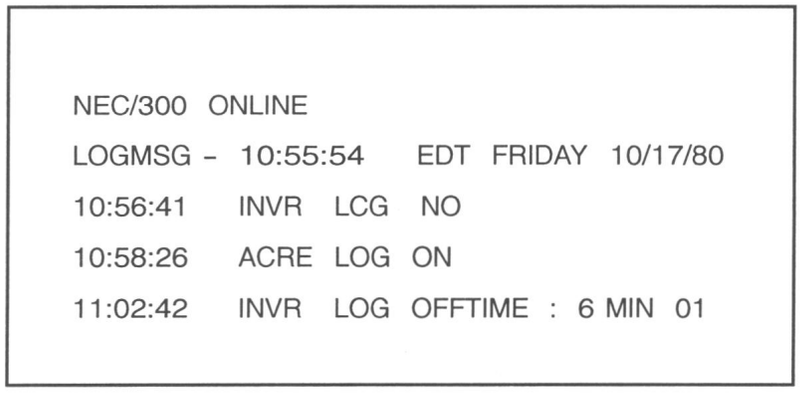
เครื่องจ่ายเงินอัตโนมัติมีสภาพคล้ายกับ Terminal ติดตั้งอยู่ในย่านชุมนุมชน เพื่ออำนวยความสะดวกให้ลูกค้าธนาคารสามารถถอนเงินในวันสุดสัปดาห์ หรือเมื่อมีความจำเป็นต้องใช้เงินกระทันหันโดยไม่ต้องไปเบิกเงินที่ธนาคาร เมื่อลูกค้าต้องการเบิกเงินจะต้องสอดบัตรที่ธนาคารออกให้เฉพาะบุคคล ในบัตรจะมีเครื่องหมายรหัสลับซึ่งเครื่องจ่ายเงินอัตโนมัติจะตรวจจับ Pattern ของรหัส แล้วส่งข้อมูลไปยังศูนย์คอมพิวเตอร์เพื่อตรวจว่า Pattern นั้นถูกต้องหรือไม่ ถ้า Pattern ไม่ถูกต้อง คอมพิวเตอร์จะส่งสัญญาณกลับมายังเครื่องจ่ายเงินให้เก็บบัตรใบนั้นไว้ แต่ถ้าพบว่าเป็นบัตรที่ถูกต้องก็จะส่งสัญญาณให้เครื่องจ่ายเงินอัตโนมัติคืนบัตรให้ลูกค้า และส่งสัญญาณให้ลูกค้า Key รหัสลับของบัญชีเงินฝาก ข้อมูลจะถูกส่งไปยังคอมพิวเตอร์ตรวจสอบว่ายอดคงเหลือในบัญชีลูกค้ามีพอหรือไม่ ถ้ายอดคงเหลือมีเพียงพอ เครื่องจะปลดปล่อยซองบรรจุเงินประมาณ F.Fr. 80-100 ตามที่ลูกค้าเบิกให้แก่ลูกค้า และ Update ยอดคงเหลือในบัญชีเงินฝาก

ผู้ทุจริตได้ขอเปิดบัญชีเงินฝากที่ให้บริการดังกล่าว เพื่อให้ได้รับบัตรถอนเงิน ผู้ทุจริตพยายามศึกษา Pattern ของรหัสจนเข้าใจระบบรหัสที่ใช้ และทำบัตรปลอมขึ้น ผู้ทุจริตได้ใช้วิธีการเพื่อที่จะทราบถึงตัวเลขรหัสลับของบัญชีเงินฝากที่ธนาคารออกให้แก่ลูกค้าแต่ละราย โดยโทรศัพท์ถึงลูกค้ารายใหญ่ของธนาคารที่คาดว่าจะมีเงินคงเหลือในบัญชีจำนวนมาก และอ้างว่าเป็นพนักงานของธนาคารต้องการเปลี่ยนเลขหมายรหัสลับของบัญชีลูกค้าใหม่เพื่อเหตุผลในด้านรักษาความปลอดภัย การเปลี่ยนหมายเลขใหม่จะกระทำโดยเพิ่มหมายเลขพิเศษขึ้นอีก 1 หลักต่อท้ายหมายเลขเดิม จากนั้นผู้ทุจริตจะแกล้งซักซ้อมความเข้าใจถึงตัวเลขรหัสใหม่กับลูกค้า โดยให้ลูกค้าอ่านหมายเลขรหัสทั้งหมด ผลปรากฏว่าทุกครั้งที่ทำการสอบถามลูกค้าทุกรายได้ให้ความร่วมมือในการแจ้งรหัสลับของตนเป็นอย่างดี

ด้วยการใช้บัตรปลอมที่จัดเตรียมและรหัสลับของบัญชีเงินฝากที่สอบถามจากลูกค้า ผู้ทุจริตได้ทำการเบิกเงินจากเครื่องจ่ายเงินอัตโนมัติในเมืองใหญ่ ๆ ของฝรั่งเศส 4 เมือง ในที่สุดผู้ทุจริตถูกจับได้เนื่องจากเครื่องจ่ายเงินอัตโนมัติเครื่องหนึ่งขัดข้องไม่คืนบัตรปลอมให้ผู้ทุจริต พนักงานควบคุมของธนาคารพบบัตรปลอมในเครื่อง จึงได้ดักซุ่มอยู่บริเวณเครื่องจ่ายเงินอัตโนมัตินั้น วันรุ่งขึ้นผู้ทุจริตได้กลับไปเพื่อทดลองใหม่และถูกจับกุมดำเนินคดี

การลักลอบใช้อุปกรณ์คอมพิวเตอร์เพื่อผลประโยชน์ในทางทุจริต มักเกิดจากบุคคลภายในศูนย์คอมพิวเตอร์เอง ซึ่งอาจมีอำนาจหน้าที่ในการใช้คอมพิวเตอร์ หรือทราบจุดอ่อนของระบบ Password ดีอยู่แล้ว เช่น ตัวอย่างกรณีที่อดีตพนักงานของ Manufacturing Data System Inc. แห่ง Ann Arbor, Michigan ซึ่งทำกิจการ Computer Service Center ได้ใช้รหัสลับที่ทางบริษัทออกให้ลูกค้าใช้เวลาของคอมพิวเตอร์ทำการประมวลผลข้อมูลให้ W & R Tool เป็นการส่วนตัวเป็นเวลาทั้งสิ้น 143 ชั่วโมง คิดเป็นค่าใช้จ่าย $15,000 ซึ่งต่อมาถูกจับและถูกดำเนินคดี

มาตรการที่นิยมใช้ในการป้องกันการใช้อุปกรณ์คอมพิวเตอร์เพื่อประโยชน์ในทางทุจริตอีกประการหนึ่งก็คือ Run Control Log โดยกำหนดให้คอมพิวเตอร์บันทึกไว้ว่าได้ปฏิบัติอะไรให้แก่ผู้ใด ตั้งแต่เวลาใดถึงเวลาใด รายงานนี้อาจพิมพ์ออกสู่ภายนอกโดย Console Printer ตลอดเวลา หรือบันทึกไว้ในแผ่นจานแม่เหล็ก เพื่อรอการ List ออกมาในภายหลังก็ได้



แผนภาพ Control Log Report

ผู้มีหน้าที่ควบคุมจะต้องตรวจตรา Control Log Report มิให้มีการแก้ไขเปลี่ยนแปลง และตรวจสอบว่าผู้ใช้แต่ละรายมีหน้าที่ในการใช้คอมพิวเตอร์ในช่วงเวลาที่ปรากฏในรายงานจริงหรือไม่ ช่วงเวลาที่ใช้ปฏิบัติงานดังกล่าวนานกว่าที่ควรจะเป็นหรือไม่

4. การควบคุมด้านการรักษาความลับของข้อมูล

การขโมยรายชื่อลูกค้าไปขาย การขโมยข้อมูลซึ่งเป็นความลับที่บันทึกไว้ในระบบคอมพิวเตอร์เพื่อนำไปหาผลประโยชน์ได้ เป็นพฤติกรรมที่แพร่หลายในปัจจุบัน เช่น พนักงานควบคุมเครื่องคอมพิวเตอร์ 3 คน ของบริษัทขาย Encyclopedia Britanica ได้ร่วมมือ List รายชื่อลูกค้า และนำไปขายให้บริษัทคู่แข่งและบริษัทประเภทขายสินค้าทางไปรษณีย์ (Mailing List) ทั่วไป ซึ่งเจ้าหน้าที่ของบริษัทผู้เสียหายได้ประเมินราคาของข้อมูลว่าไม่ต่ำกว่า $1 ล้าน ใน ค.ศ.1973 พนักงานผู้คุมเครื่องคอมพิวเตอร์ของ Illinois Driver Registration Bureau ได้รับการติดสินบนจากบุคคลภายนอกเป็นเงิน $10,000 ให้ลักลอบ List รายชื่อและที่อยู่ของผู้ขับขี่ยานพาหนะ ซึ่งมีมูลค่าต่อธุรกิจขายสินค้าทางไปรษณีย์ประมาณ $70,000

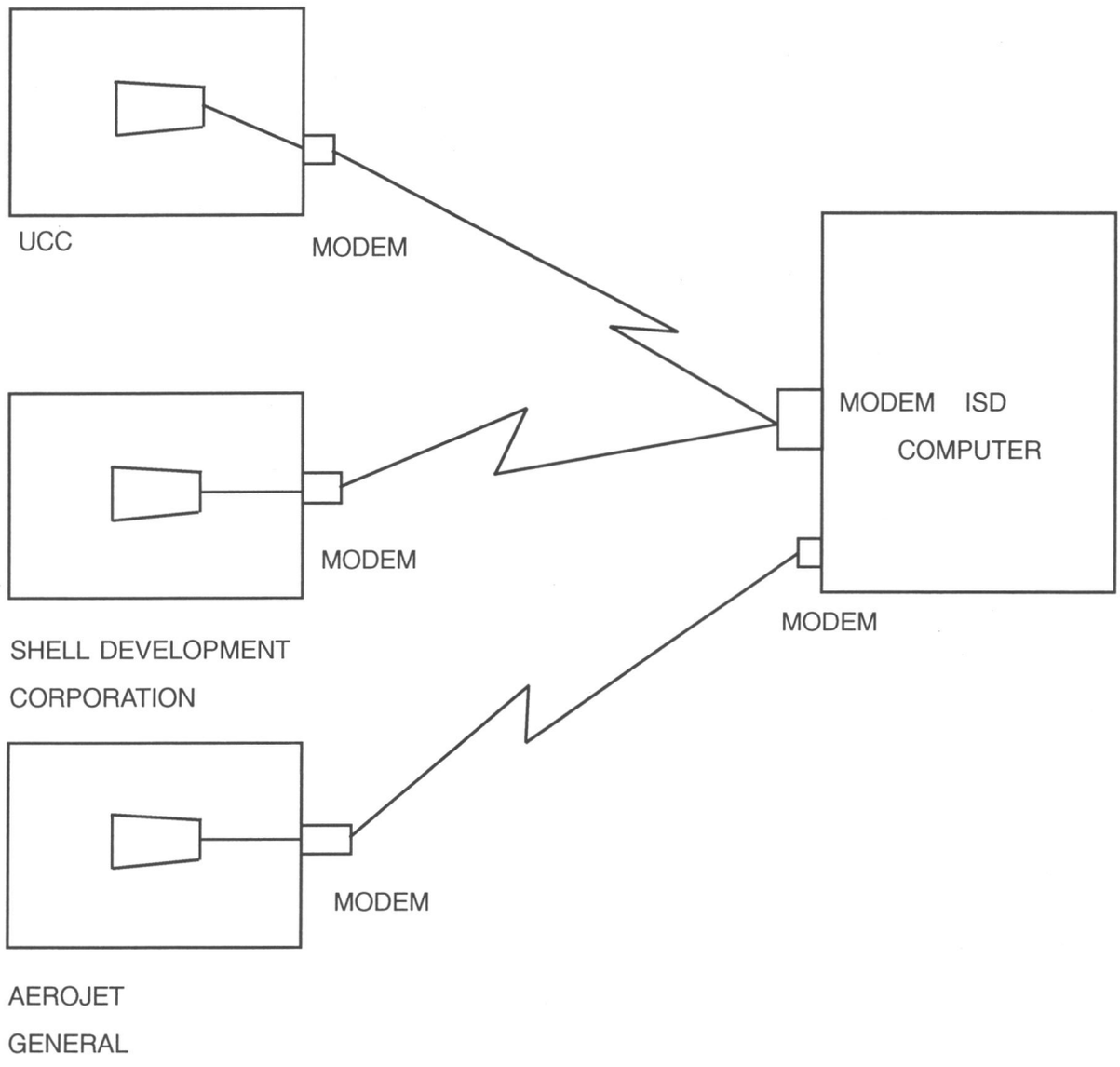
ใน ค.ศ.1971 พนักงานตำรวจในชิคาโกถูกจับในข้อหา List ข้อมูลอาชญากรรมจากศูนย์คอมพิวเตอร์ National Crime Information Center ของ F.B.I. เพื่อนำไปขายให้นักสืบเอกชนและสำนักงานทนายความ

ในประเทศนอร์เวย์ พนักงานควบคุมเครื่องคอมพิวเตอร์ของ Health Service ถูกจับในข้อหา List ข้อมูลเกี่ยวกับผู้ป่วยเรื้อรังเพื่อขายให้พนักงานขายของบริษัทผลิตยาไปติดต่อผู้ป่วย

โปรแกรมคอมพิวเตอร์กับการค้นหาข้อมูลเพื่อพิสูจน์การโจรกรรม

นอกจากข้อมูลที่เป็นความลับจะเป็นเป้าหมายของการทุจริตเพื่อหาผลประโยชน์แล้ว โปรแกรมควบคุมการทำงานของคอมพิวเตอร์ก็เป็นเป้าหมายของการทุจริตด้วย ตัวอย่างเช่น บริษัท University Computing Company (U.C.C.) แห่ง Palo Alto, California ประกอบธุรกิจประเภท Computer Service Center ให้บริการเช่าเวลาคอมพิวเตอร์แก่กิจการทั่วไป มีรายได้ประมาณปีละ $100 ล้าน U.C.C. มีคู่แข่งที่สำคัญที่ดำเนินธุรกิจประเภทเดียวกัน คือ บริษัท Information System Design Inc. (I.S.D.) แห่ง Oakland, California บริษัท I.S.D. นับเป็นบริษัทที่ก่อตั้งภายหลังมีรายได้ประมาณปีละ $1 ล้าน แต่มีความสามารถพัฒนาโปรแกรม PLOT/TRANS โปรแกรมนี้สามารถ Plot graph จากผลการคำนวณทางวิศวกรรมซึ่งลูกค้าที่ใช้บริการส่งมาจาก Remote Terminal โดยใช้ Remote Terminal แห่งนั้นเอง ระบบ PLOT/TRANS ช่วยอำนวยความสะดวกและลดค่าใช้จ่ายในการประมวลผลข้อมูลให้แก่ลูกค้า เพราะสามารถ Plot graph ด้วย Terminal ธรรมดา และให้บริการที่รวดเร็วแก่ Terminal ของลูกค้าที่อยู่ห่างไกล ดังนั้นระบบนี้จึงช่วยให้เทคนิคของ I.S.D. ก้าวหน้ากว่า U.C.C. จึงพยายามพัฒนาระบบเช่นนี้เช่นกัน แต่ยังไม่ประสบผลสำเร็จ บริษัททั้งสองแข่งขันการให้บริการแก่ลูกค้าสำคัญ คือ Shell Development Corporation แห่ง Emerryville และ Aerojet General แห่ง Sacramento แต่ I.S.D. อยู่ในฐานะได้เปรียบในการแข่งขันการให้บริการลูกค้าเนื่องจากระบบ PLOT/TRANS ดังกล่าว

พนักงานพัฒนาโปรแกรมอาวุโสของ U.C.C. คือ Eli Bart พยายามที่จะดึงความลับของโปรแกรม PLOT/TRANS โดยใช้ Terminal ที่ U.C.C. ทำการ Access ระบบคอมพิวเตอร์ของ I.S.D. การที่จะติดต่อกับระบบคอมพิวเตอร์ของ I.S.D. ได้ประการแรกจะต้องทราบหมายเลขโทรศัพท์ที่ I.S.D. กำหนดให้ลูกค้าแต่ละรายใช้ติดต่อระหว่าง Terminal ของลูกค้ากับคอมพิวเตอร์ของ I.S.D. และหมายเลขนี้ไม่ปรากฏในสมุดโทรศัพท์ ประการที่สองจะต้องทราบ Password ของลูกค้าที่ I.S.D. กำหนดให้ลูกค้าแต่ละราย และประการที่สามจะต้องทราบชื่อรหัสของโปรแกรม PLOT/TRANS เพื่อสามารถเรียกใช้โปรแกรม



แผนภาพการเรียกใช้โปรแกรมงานจาก Remote Terminal

Eli Bart ทราบความลับของหมายเลขโทรศัพท์คู่สายระหว่าง Terminalของบริษัท Shell Development Corporation และ Password ซึ่ง I.S.D. ออกให้บริษัท Shell โดยการเข้าไปสนิทสนมกับพนักงานของบริษัท Shell ซึ่งเป็นลูกค้าของทั้ง U.C.C. และ I.S.D. สำหรับชื่อรหัสของโปรแกรม PLOT/TRANS ปรากฏว่า Eli Bart ได้จากเพื่อนซึ่งทำงานในบริษัท Aerojet General ซึ่งเป็นลูกค้าของ I.S.D. และใช้ระบบ PLOT/TRANS

ในวันที่ 19 มกราคม ค.ศ. 1970 Eli Bart ได้ใช้ Terminal ในสำนักงานใหญ่ของ U.C.C. ทำการ Access คอมพิวเตอร์ของ I.S.D. โดยทำเสมือนเป็น Terminal ของบริษัท Shell Development Corporation และสั่งให้คอมพิวเตอร์ของ I.S.D. ส่งโปรแกรม PLOT/TRANS มาพิมพ์ ณ Terminal ของ U.C.C.

ถึงแม้ความพยายามของ Eli Bart ในการได้ความลับของโปรแกรม PLOT/TRANS จะเป็นผลสำเร็จ แต่รายการนี้ได้ถูกบันทึกใน Control Log ของคอมพิวเตอร์ I.S.D. เพื่อเรียกเก็บเงินจากบริษัท Shell Development Corporation เป็นค่าบริการใช้คอมพิวเตอร์ ซึ่งบริษัท Shell Development Corporation ได้ปฏิเสธการจ่ายเงินตามรายการดังกล่าว เนื่องจากไม่เคยใช้บริการในลักษณะนี้มาก่อน

พนักงานของบริษัท I.S.D. ได้ดำเนินการสอบสวนกรณีดังกล่าว และเพ่งเล็งมายัง U.C.C. ในวันที่ 19 กุมภาพันธ์ ศกเดียวกัน เจ้าหน้าที่ตำรวจและพนักงานของบริษัท I.S.D. ใช้หมายค้นทำการตรวจสอบข้อมูลในส่วนความจำและอุปกรณ์จัดเก็บข้อมูลของระบบคอมพิวเตอร์ บริษัท U.C.C. นับว่าเป็นหมายค้นส่วนความจำของคอมพิวเตอร์ครั้งแรกในประวัติศาสตร์ หลังจากใช้เวลา List ข้อมูล 9 ชั่วโมง จึงได้พบว่าโปรแกรม PLOT/TRANS ที่ขโมยมาจากบริษัท I.S.D. ได้ถูกถ่ายทอดเก็บไว้ในเทปแม่เหล็ก และตรวจพบเอกสารลายมือของ Eli Bart เขียนบันทึกวิธีการ Access ระบบคอมพิวเตอร์ของ I.S.D.

Eli Bart ถูกฟ้องศาลในข้อหาขโมยความลับทางการค้า ซึ่งประเมินว่ามีมูลค่าไม่ต่ำกว่า $1 ล้าน และได้รับโทษปรับ $5,000 รวมทั้งรอลงอาญา 3 ปี บริษัท U.C.C. ถูกฟ้องในฐานะจำเลยร่วม และต้องชดใช้ค่าเสียหายให้บริษัท I.S.D. เป็นเงิน $300,000

การทุจริตทางด้าน INPUT

การทุจริตทางด้าน Input มักเกิดจากการแก้ไขรายการ Input และรายการ Input ปลอม ดังกรณีตัวอย่างต่อไปนี้

1. ในปี ค.ศ. 1972 พนักงาน Data Entry ของ Board of Election, New York ถูกจับในข้อหาเพิ่มรายชื่อผู้ที่ยังไม่มีสิทธิออกเสียงเลือกตั้งหลายร้อยชื่อใน File ของผู้ที่มีสิทธิออกเสียง เพื่อร่วมมือทุจริตในการเลือกตั้ง

2. ในปี ค.ศ.1974 พนักงานศูนย์คอมพิวเตอร์ของ New York Department of Motor Vehicle ได้ถูกจับในข้อหาเพิ่มชื่อของผู้สอบผ่านการขอรับใบขับขี่ File รายชื่อที่เพิ่มส่วนมากเป็นผู้อพยพต่างชาติ ซึ่งไม่ผ่านการทดสอบสายตา ข้อเขียน และการทดสอบขับขี่ในถนน (Road Test) ผู้กระทำผิดสารภาพว่าร่วมมือกับโรงเรียนสอนขับรถยนต์ และได้รับค่าจ้างประมาณ $200-400 ต่อราย ทำให้มีรายได้จากการทุจริตประมาณ $300,000

3. สตรีชราผู้หนึ่งนำเช็ค Tax Refund ของ Internal Revenue Service (IRS) ไปขอเบิกเงินที่ธนาคารแห่งหนึ่งใน Southern California โดยมีหลักฐานการขอรับเงินไปแสดงอย่างครบถ้วน อย่างไรก็ตามพนักงานของธนาคารจำได้ว่าสตรีชราผู้นั้นยังชีพด้วยเงินสวัสดิการประกันสังคม จึงไม่ควรที่จะได้รับ Tax Refund อีก ดังนั้นพนักงานได้รายงานข้อสงสัยไปยังสำนักงาน IRS จากการสอบสวนพบว่า หลานของสตรีชราผู้นั้นซึ่งทำงานในฐานะพนักงาน Data Entry ของสำนักงาน IRS California ได้เพิ่มชื่อของสตรีชราผู้นั้นใน File ผู้มีสิทธิได้รับ Tax Refund และส่งไปพิมพ์เช็คสั่งจ่ายที่ศูนย์คอมพิวเตอร์ของสำนักงานใหญ่ IRS ใน West Virginia

การทุจริตทางด้าน Input ทั้ง 3 ราย กระทำโดยเพิ่มข้อมูลใน File โดยไม่มีเอกสารเบื้องต้นสนับสนุน ดังนั้นถ้ามีการพิมพ์ (List) รายการที่ทำการ Input สู่คอมพิวเตอร์นำมาตรวจสอบกับเอกสารเบื้องต้นอย่างรอบคอบแล้ว ย่อมสามารถตรวจพบการทุจริตในกรณีดังกล่าว

4. การแก้ไขรายการแล้ว Input ข้อมูลใหม่เพื่อการทุจริต บางกรณีการทุจริตทางด้าน Input ได้กระทำอย่างซับซ้อน เช่น ในกรณีตัวอย่าง Stephen Nattner พนักงาน Teller แห่ง Union Dime Saving Bank สาขา Park Avenue, New York ยักยอกเงินลูกค้าเงินฝากในระหว่างปี ค.ศ. 1970 - 1973 เป็นจำนวนเงิน $1.5 ล้าน Stephen Nattner ดำเนินการยักยอกเงินจากบัญชีเงินฝากประจำที่ลูกค้านำมาเปิดบัญชี โดยในครั้งแรกจะ Input ข้อมูลเข้าเครื่องคอมพิวเตอร์ตรงตามจำนวนที่ลูกค้านำฝาก เพื่อให้คอมพิวเตอร์พิมพ์รายการในสมุดคู่ฝาก จากนั้นเมื่อลูกค้ากลับไปแล้ว Stephen Nattner จะลงรายการยกเลิก (Reverse) รายการฝากนี้ และแก้ไขยอดเงินนำฝากให้น้อยลง เช่น ถ้าลูกค้านำเงินมาฝาก $10,000 จะยกเลิกรายการฝากนี้โดยทำการ Reverse และ Input รายการใหม่เป็น $1,000 ซึ่งทำให้ดูเสมือนการ Input ครั้งแรกเป็นรายการที่ผิดพลาด เนื่องจากพิมพ์ตัวเลขผิดพลาด Stephen Nattner จะบันทึกรายการที่ยักยอกไว้อย่างละเอียด ซึ่งถ้าลูกค้าที่ถูกยักยอกมาถอนเงิน ก็จะนำเงินที่ยักยอกไว้บางส่วนจ่ายให้แก่ลูกค้า อย่างไรก็ตามรายการถอนเงินมีน้อยมาก เนื่องจากลูกค้าที่ถูกยักยอกส่วนใหญ่เป็นคนชราซึ่งฝากเงินบำเหน็จบำนาญเพื่อหวังดอกเบี้ยเลี้ยงชีพ ในวันสิ้นงวดบัญชีซึ่งต้องมีการพิมพ์ใบยืนยันยอดเงินคงเหลือในบัญชีแจ้งไปยังลูกค้า Stephen Nattner อาศัยจุดอ่อนในระบบการพิมพ์ใบยืนยันยอดเงินฝากธนาคาร ซึ่งกำหนดให้ทำการพิมพ์ใบยืนยันยอดบัญชีเงินฝากออมทรัพย์ต่างวันกับการพิมพ์ใบยืนยันยอดเงินฝากประจำ คือ เงินฝากออมทรัพย์จะถือยอด ณ วันสิ้นงวดและเงินฝากประจำจะถือยอด 2 วันหลังจากวันสิ้นงวด เขาทำการโอนยอดเงินจากบัญชีเงินฝากออมทรัพย์ของลูกค้าบางรายมาเป็นรายการฝากในบัญชีเงินฝากประจำที่ได้ทำการยักยอกเพื่อให้ยอดเงินในใบยืนยันยอดคงเหลือในสมุดคู่ฝาก ซึ่งหลังจากที่พิมพ์ใบยืนยันยอดแล้ว เขาจะทำการโอนกลับไปยังบัญชีออมทรัพย์ดังเดิม

หลังจากที่ทำการยักยอกเงินจากลูกค้าในช่วงเวลา 3 ปี เป็นจำนวนเงินมากกว่า $1.5 การทุจริตได้ถูกเปิดเผย เนื่องจากเจ้าหน้าที่ตำรวจจับเจ้ามือการพนันจากการค้นตัวเจ้ามือการพนันพบรายชื่อลูกค้ารายใหญ่ซึ่งมีชื่อของ Stephen Nattner รวมอยู่ด้วย จากรายละเอียดการรับแทง ปรากฏว่า Stephen Nattner เป็นผู้ที่เสียพนันมากที่สุด บางวันเสียพนันถึง $30,000 ทั้งนี้ทำให้เจ้าหน้าที่ตำรวจสงสัยว่า Stephen Nattner นำเงินจากที่ใดมาเล่นการพนัน จึงทำการสอบสวนและสามารถเปิดเผยการทุจริตครั้งนี้

ต่อมา Stephen Nattner ได้รับคำตัดสินจำคุก 20 เดือน ในข้อหายักยอกเงิน $1.5 ล้าน แต่จำคุกจริงเพียง 15 เดือน เนื่องจากประพฤติดี

กรณีทุจริตของ Stephen Nattner เกิดขึ้นโดยอาศัยจุดอ่อนในระบบการควบคุมที่ยินยอมให้ผู้มีหน้าที่รับเงินเป็นผู้บันทึกรายการรับเงินเองทุกสิ้นวัน

ในด้านการแบ่งแยกหน้าที่ เมื่อทำการพิมพ์รายละเอียดรายการ (List Transaction) ประจำวัน ผู้ควบคุมไม่ได้ให้ความสนใจกับรายการ Reverse รายการรับฝากเงินของพนักงานรายนี้ ซึ่งมีรูปแบบการ Reverse ที่ผิดปกติเกิดขึ้นเป็นประจำ นอกจากนั้นวิธีการพิมพ์ใบยืนยันยอดเงินฝากยังหละหลวม โดยยินยอมให้มีการพิมพ์ใบยืนยันยอดเงินฝากออมทรัพย์และเงินฝากประจำต่างวันกัน เป็นการเปิดโอกาสให้สามารถโอนยอดเงินระหว่างกัน

สิ่งที่ต้องระวังเป็นพิเศษก็คือ การแก้ไขยอดคงเหลือใน Record ที่บันทึกในระบบคอมพิวเตอร์ สามารถทำได้อย่างรวดเร็วและไม่ทิ้งร่องรอยใด ๆ ไว้ ทั้งนี้ต่างจากระบบการบันทึกข้อมูลในแผ่นบัญชี ซึ่งทำได้ยากกว่าและมีร่องรอย Audit Trail ปรากฏอยู่ง่ายต่อการตรวจสอบความผิดปกติ

5. การสร้าง Input ปลอมตบแต่งฐานะขององค์กร กรณี Equity Funding Corporation

บางครั้งผู้บริหารของกิจการเป็นผู้สร้าง Input ปลอมเพื่อใช้เป็นเครื่องมือแสดงฐานะของกิจการให้ดูมั่นคงกว่าข้อเท็จจริง หรือเพื่อหลอกลวงบริษัทอื่นที่เกี่ยวข้องเช่น กรณีตัวอย่างที่เกิดใน Equity Funding Corporation, New York ระหว่างปี ค.ศ. 1969 - 1973 Equity Funding Corp. เป็นบริษัทดำเนินกิจการประกันชีวิต เมื่อขายประกันได้จะขายกรมธรรม์บางรายต่อให้บริษัทอื่นรับช่วงในฐานะ Reinsurance ในการขายกรมธรรม์ต่อให้บริษัทอื่น Equity Funding Corp. ได้ค่าธรรมเนียมจากบริษัทที่รับช่วง อย่างไรก็ตามถึงแม้จะขายกรมธรรม์ให้บริษัทรับช่วงไปแล้ว แต่การจ่ายเงินค่าประกันประจำปีลูกค้าที่เอาประกันยังจ่ายต่อ Equity Funding Corp. ซึ่งจะนำส่งผลประโยชน์ที่ได้ให้กับบริษัทรับช่วงอีกต่อหนึ่ง

นับแต่ปี ค.ศ. 1969 Standley Goldblum ประธานกรรมการของบริษัทฯสั่งให้พนักงานสร้างกรมธรรม์ปลอม Input สู่ระบบคอมพิวเตอร์ โดยใช้รหัสว่ากรมธรรม์จัดเตรียมโดย Department 99 ทั้งนี้เพื่อให้ฐานะของบริษัทเจริญเติบโตกว่าความเป็นจริง ซึ่งมีผลให้หุ้นของบริษัทฯมีมูลค่าสูงขึ้นในตลาดหลักทรัพย์ และให้ขายกรมธรรม์ปลอมนั้นต่อให้บริษัทรับช่วง ทำให้ได้ค่าธรรมเนียมและผลประโยชน์ตอบแทนอื่น ๆ เป็นเงิน $1,175,000 เฉพาะในปี ค.ศ. 1972 กรมธรรม์ปลอมทั้งสิ้นมีมูลค่าทางบัญชีสูงถึง $14.5 ล้าน (จากกรมธรรม์ทั้งหมด 97,000 รายการ เป็นกรมธรรม์ปลอม 64,000 รายการ)

ในเดือนมีนาคม ค.ศ. 1973 Raynond Birk อดีตพนักงานของ Equity Funding Corp. ซึ่งถูกไล่ออก ได้แจ้งการทุจริตที่เกิดขึ้นต่อ New York State Insurance Department และ New York Stock Exchange หลังการสอบสวนผู้บริหารของ Equity Funding Corp. ได้รับการตัดสินให้จำคุก

ข้อที่น่าสังเกตก็คือ การปิดบังการทุจริตมิให้ผู้ควบคุมจาก New York State Insurance และผู้สอบบัญชีตรวจพบกระทำโดยเตรียมการตั้งแต่ขั้น Input ข้อมูล ทั้งนี้รายการที่เป็นกรมธรรม์ปลอมจะมีรหัสกำกับว่า "Issued by Department 99" เมื่อผู้ควบคุมจาก New York State Insurance หรือผู้ตรวจสอบบัญชีมาตรวจสอบมักกำหนดให้ทำการ List กรมธรรม์ตามเงื่อนไขที่กำหนดเพื่อนำไปสุ่มตรวจสอบกับผู้เอาประกันโปรแกรม List รายการกรมธรรม์ที่ Equity Funding Corp. จัดเตรียมจะแฝงไว้ด้วยคำสั่งที่ให้ข้ามรายการซึ่ง "Issued by Department 99" ทำให้รายการกรมธรรม์ปลอมไม่มีโอกาสถูก List ออกมาตรวจสอบ

อนึ่งในปัจจุบันกิจการต่าง ๆ มีแนวโน้มที่จะใช้ระบบการ Input ข้อมูลในลักษณะกึ่งอัตโนมัติเพื่อความรวดเร็วในการปฏิบัติงาน เช่น การใช้ระบบ MICR (Magnetic Ink Character Reader) โดยการพิมพ์ข้อมูลที่จะ MICR เข้าสู่ระบบคอมพิวเตอร์ในลักษณะที่เครื่องอ่าน MICR สามารถอ่านข้อมูลที่พิมพ์อยู่ได้โดยตรง บางครั้งการใช้ระบบ Input ข้อมูลในลักษณะดังกล่าวโดยไม่ทำการตรวจสอบอย่างรอบคอบ อาจกลายเป็นช่องทางให้ผู้ทุจริตดำเนินการฉ้อโกงได้

การปลอม Input เงินฝากโดยใช้ MICR

ชายผู้หนึ่งเปิดบัญชีเงินฝากกระแสรายวันกับธนาคารแห่งหนึ่งใน Washington D.C. สหรัฐอเมริกา เพื่อให้ได้สมุดเช็คและใบนำฝากเงินจำนวนมาก ในใบนำฝากเงินและสมุดเช็คด้านล่างจะมีรหัสตัวเลขซึ่งพิมพ์ในระบบ MICR แสดงหมายเลขบัญชี หลังจากที่ได้ศึกษาระบบรหัสและรูปแบบของใบนำฝากเงินเป็นอย่างดีแล้ว ชายผู้นั้นได้พิมพ์ใบนำฝากเงินปลอมซึ่งมีลักษณะเหมือนกับใบนำฝากที่ธนาคารเตรียมไว้ที่เคาน์เตอร์สำหรับผู้ที่มีความประสงค์จะฝากเงิน แต่มิได้นำใบนำฝากเงินที่ธนาคารได้ให้ไว้มาด้วย ใบนำฝากเงินแบบนี้จะไม่มี MICR หมายเลขบัญชีบันทึกไว้ ซึ่งถ้าลูกค้านำฝากโดยใช้ใบนำฝากเงินแบบนี้พนักงานของธนาคารจะใช้เครื่องพิมพ์ MICR พิมพ์หมายเลขบัญชีเพิ่มให้ ในเวลาที่ทำการพิมพ์จำนวนเงินในใบนำฝากและนำใบนำฝากไปเข้าเครื่องอ่าน MICR เพื่อทำการ Update ยอดเงินในบัญชีของลูกค้ารายนั้น

ผู้ทุจริตได้พิมพ์ใบนำฝากเงินปลอมโดยบันทึกหมายเลขบัญชีของผู้ทุจริตในแบบ MICR กำกับอยู่ด้วย และลอบนำไปวางรวมกับใบนำฝากที่ธนาคารเตรียมไว้ให้ลูกค้าที่เคาน์เตอร์ เมื่อลูกค้าที่ต้องการจะฝากเงินแต่ไม่ได้นำใบฝากเงินของตนมา ก็จะหยิบใบนำฝากเงินปลอมนี้กรอกจำนวนเงินที่จะนำฝาก และส่งให้พนักงานเคาน์เตอร์นับเงินและประทับตราลงนามรับรอง พร้อมทั้งคืนสำเนาให้ลูกค้า ใบนำฝากเงินจะถูกส่งต่อให้แก่พนักงานซึ่งจะใช้เครื่องพิมพ์ MICR พิมพ์จำนวนเงินและเลขที่บัญชี ถ้าใบนำส่งเงินฝากนี้ไม่มีหมายเลขบัญชีพิมพ์ด้วย MICR ปรากฏอยู่ ปรากฏว่าในขั้นตอนของการพิมพ์จำนวนเงิน พนักงานที่พิมพ์ตรวจดูใบนำฝากเงินนั้นมีหมายเลขบัญชีของผู้ทุจริตพิมพ์อยู่แล้ว จึงพิมพ์ MICR เฉพาะจำนวนเงินฝากในใบนำฝาก และส่งเข้าสู่เครื่องอ่าน MICR เพื่อทำการ Update ยอดคงเหลือในบัญชีของลูกค้า ดังนั้นผลที่เกิดขึ้นก็คือ จำนวนเงินในใบนำฝากปลอมจะถูกส่งไป Update เพิ่มยอดคงเหลือของผู้ทุจริต ซึ่งผู้ทุจริตได้ถอนเงินทั้งสิ้นในเวลาใกล้ปิดทำการและหลบหนีไป

7. การใช้จุดอ่อนของ Input ในระบบอัตโนมัติโดยใช้ MICR อีกแบบหนึ่ง

กรณีเช่นนี้เกิดขึ้นใน New York และ Boston ในช่วงเวลาใกล้เคียงกัน

การทุจริตโดยอาศัยจุดอ่อนของระบบ Input ในแบบอัตโนมัติอีกกรณีหนึ่งเกิดขึ้นกับธนาคารใน New York ชายผู้หนึ่งเปิดบัญชีกระแสรายวันกับธนาคารหลายแห่งในเวลาใกล้เคียงกัน ต่อมาผู้ทุจริตได้ซื้อเครื่องพิมพ์เช็คซึ่งสามารถพิมพ์ MICR เพื่อพิมพ์เช็คปลอมของ Chemical Bank, New York แต่ในส่วนที่เป็นหมายเลข MICR ซึ่งแสดงว่าเป็นเช็คของธนาคารใด ผู้ทุจริตได้พิมพ์หมายเลขประจำของ Bank of American, Los Angeles ไว้แทน

ต่อมาผู้ทุจริตได้กรอกจำนวนเงินในเช็คปลอมเหล่านั้น และนำฝากเข้าบัญชีกับธนาคารที่เปิดบัญชีไว้ พนักงานธนาคารที่รับฝากจะลงรายการเป็นเช็คเคลียริ่งของ Local Area ซึ่งจะถอนเงินได้ในวันทำการถัดไปถ้าเช็คนั้นไม่ถูกคืนจาก Chemical Bank

เช็คปลอมได้ถูกส่งไปยัง Federal Reserve Bank เพื่อทำการ Clearing เครื่องแยกเช็คของ Federal Reserve Bank ซึ่งแยกเช็คโดยการอ่าน MICR ได้แยกเช็คปลอมเพื่อส่งไปเรียกเก็บเงินจาก Bank of America, Los Angeles ตามหมายเลขธนาคารที่พิมพ์ในระบบ MICR แทนที่จะเป็น Chemical Bank เช็คปลอมได้ถูกส่งไปยัง Los Angeles ซึ่งจะใช้เวลาประมาณ 2 วัน เมื่อเช็คถูกส่งไปถึง Bank of America พนักงานธนาคารได้ตรวจพบว่าเป็นเช็คของ Chemical Bank, New York ทำให้เข้าใจว่าคงจะเกิดความผิดพลาดในการแยกเช็ค จึงส่งเช็คปลอมกลับไปยัง Federal Reserve Bank ที่ New York ซึ่งใช้เวลาอีก 2 วัน

เนื่องจากเช็คไม่ได้ถูกคืนจาก Chemical Bank ในวันทำการถัดไปนับจากวันนำฝาก ดังนั้นธนาคารซึ่งผู้ทุจริตนำเช็คฝากเข้าบัญชีจึงถือว่าเช็คนั้นเป็นเช็คที่เรียกเก็บเงินได้ หลังจากผู้ทุจริตเบิกเงินนำฝากตามเช็คปลอมเป็นจำนวนกว่า $1 ล้านแล้วได้หลบหนีไป

การควบคุมและการทุจริตทางด้าน Processing

ความมุ่งหมายของการควบคุมในด้านนี้ ก็เพื่อให้การปฏิบัติข้อมูลกระทำโดยผู้มีอำนาจหน้าที่ และใช้โปรแกรมที่ผ่านการทดสอบความถูกต้องและได้รับการรับรองแล้วเท่านั้น ทั้งนี้เพื่อป้องกันมิให้มีการใช้โปรแกรมที่ถูกสร้างหรือดัดแปลงแก้ไขจากโปรแกรมเดิมทำการปฏิบัติข้อมูลเพื่อผลในทางทุจริต

การทุจริตทางด้านการปฏิบัติข้อมูลเนื่องมาจากโปรแกรมซึ่งมักเกิดขึ้นเสมอ ได้แก่

1. การทุจริตเกิดขึ้นจากการใช้โปรแกรมที่ผู้ทุจริตจัดทำขึ้นเพื่อลักลอบแก้ไข หรือพิมพ์ List ข้อมูลที่จัดเก็บในระบบ

กรณีที่เกิดขึ้นใน TRV Credit Data of Anaheim, California สหรัฐอเมริกา ซึ่งเป็นบริษัทที่ดำเนินกิจการในด้านรวบรวมข้อมูลเกี่ยวกับฐานะการเงิน (Credit Stated) ของประชากรประมาณ 50 ล้านคนในสหรัฐอเมริกา เพื่อให้บริการด้านข่าวสารและข้อมูลประวัติทางด้านสินเชื่อของบุคคลต่าง ๆ แก่ธนาคารแก่กิจการ Credit Card ซึ่งเป็นสมาชิก โดยเฉพาะอย่างยิ่ง American Express และ Master Charge ต่อมาคณะลูกขุนแห่ง Los Angeles ได้ฟ้องพนักงานของ TRV Credit Data of Anaheim ข้อหารับแก้ไขประวัติทางด้านสินเชื่อของบุคคลที่มีประวัติไม่เป็นที่น่าพึงพอใจ ให้กลายเป็นบุคคลที่มีประวัติทางด้านสินเชื่อดี โดยได้รับค่าจ้างประมาณรายละ $300- 1,500 ซึ่งผลจากการแก้ไขประวัติด้านสินเชื่อได้ก่อให้เกิดหนี้สูญในกิจการ Credit Card จำนวนมหาศาล

ในระหว่างปี ค.ศ.1968-1972 พนักงานในศูนย์คอมพิวเตอร์ของ F.B.I. ถูกสอบสวนในข้อหาว่ามีการรับจ้างแก้ไขประวัติอาชญากรรมของบุคคลต่าง ๆ ที่จัดเก็บไว้

2. การทุจริตเกิดขึ้นจากการใช้โปรแกรมที่ผู้ทุจริตสร้างขึ้น หรือดัดแปลงจากโปรแกรมเดิมเพื่อหักเงินจากบัญชีอื่นครั้งละจำนวนน้อย และนำมาเข้าบัญชีของผู้ทุจริตหรือเรียกวิธีการนี้ว่า Salami

2.1 ผู้ทุจริตเป็นพนักงานศูนย์คอมพิวเตอร์ของธนาคารได้จัดทำโปรแกรมเพื่อหักเงินจากบัญชีกระแสรายวันของลูกค้าธนาคารเฉพาะรายที่เป็นเอกชนครั้งละไม่เกิน $1 มาเข้าบัญชีของผู้ทุจริต โปรแกรมได้รับการออกแบบให้ทำการตรวจเช็คมิให้บัญชีใดถูกหักเงินเกินกว่าปีละ 3 ครั้ง การทุจริตนี้ได้ดำเนินไปเป็นเวลานาน เนื่องจากการหักบัญชีกระทำโดยไม่ทิ้งร่องรอยใด ๆ เลย และลูกค้าที่เป็นเอกชนทั่วไปมักไม่สนใจเงินจำนวนน้อยที่ขาดหายไปเพราะคิดว่าเป็นค่าบริการที่ธนาคารหักจากบัญชี และไม่คุ้มค่าที่จะไปธนาคารเพื่อสอบถาม คนส่วนมากมักเชื่อคอมพิวเตอร์และคิดว่าตนเองคำนวณยอดเงินคงเหลือผิด

2.2 พนักงานของโรงงานตัดเย็บเสื้อผ้าที่ New York ได้โปรแกรมให้คอมพิวเตอร์หักภาษี ณ ที่จ่าย ออกจากเช็คเงินเดือนของพนักงานทุกคนในบริษัทเกินกว่าปกติ และให้นำเงินที่หักนี้ส่งเป็นภาษีของผู้ทุจริต ซึ่งเมื่อสิ้นปีผู้ทุจริตจะได้รับเงินจาก Internal Revenue Service จำนวนมากในรูปของภาษีคืน (Tax Refund)

2.3 พนักงานพัฒนาโปรแกรมของบริษัทขายสินค้าทางไปรษณีย์ ได้โปรแกรมให้คอมพิวเตอร์หักบัญชีค่านายหน้าของพนักงานขายคนอื่นคนละจำนวนน้อย ไปเข้าบัญชีปลอมในชื่อ Zwana (เหตุที่ใช้ชื่อ Zwana เนื่องจากในการปฏิบัติข้อมูลเพื่อคำนวณค่านายหน้าที่พนักงานแต่ละคนจะได้รับในรอบเดือน จะทำเรื่องตามลำดับชื่อ ซึ่ง Zwana จะเป็นชื่อสุดท้าย) การทุจริตได้ดำเนินไปอย่างราบรื่นเป็นเวลา 3 ปี จนในที่สุดได้ถูกเปิดเผย เนื่องจากบริษัทได้จัดงานเลี้ยงพนักงานขาย และจะแจกรางวัลพิเศษแก่พนักงานขายชื่อแรกและชื่อสุดท้ายในบัญชีรายชื่อปรากฏว่า Zwana ซึ่งเป็นชื่อสุดท้ายไม่มีตัวตน

3. การทุจริตเกิดขึ้นจากผู้ทุจริตแฝงคำสั่งให้คอมพิวเตอร์ข้ามขั้นตอนในโปรแกรมเพื่อผลในทางทุจริต หรือที่เรียกว่า Trojan Horse

พนักงานพัฒนาโปรแกรมแห่ง National City Bank, New York สหรัฐอเมริกา ซึ่งได้รับมอบหมายให้พัฒนาโปรแกรมปฏิบัติข้อมูลเงินฝากกระแสรายวัน ได้แฝงคำสั่งประเภท Condition Branch ในโปรแกรมเพื่อให้คอมพิวเตอร์ปฏิบัติงานข้ามขั้นตอนการตรวจเช็คจำนวนคงเหลือในบัญชี ถ้าเป็นการเบิกเงินจากบัญชีซึ่งผู้ทุจริตเปิดไว้ทำให้ผู้ทุจริตสามารถสั่งจ่ายเงินจากบัญชีนั้นในจำนวนเกินกว่ายอดคงเหลือจำนวนเท่าใดก็ได้ การทุจริต ได้ถูกเปิดเผยเนื่องจากระบบคอมพิวเตอร์ขัดข้อง จึงต้องทำการ Update ยอดคงเหลือด้วยมือ ทำให้เสมียนธนาคารคนหนึ่งสังเกตพบการทุจริต

การป้องกันการทุจริตทางด้านการปฏิบัติข้อมูล ต้องใช้มาตรการหลายด้านประกอบกันเพื่อป้องกันมิให้ผู้ทุจริตมีโอกาสใช้โปรแกรมที่จัดเตรียมลักลอบทำการปฏิบัติข้อมูลเพื่อผลทางทุจริต จะต้องมีการควบคุมด้านการป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับมอบหมายอย่างเคร่งครัด โดยใช้มาตรการดังได้กล่าวแล้วในตอนต้น โปรแกรมใช้งานจะต้องได้รับการ List ออกมาตรวจเทียบกับโปรแกรมที่ผ่านการทดสอบความถูกต้องและได้รับการรับรอง เพื่อค้นหาข้อแตกต่างที่ผู้ทุจริตอาจทำการแก้ไขอยู่เสมอ และการตรวจสอบควรจะกระทำในลักษณะไม่แจ้งให้ทราบล่วงหน้า (Surprise Request)

การทุจริตและการควบคุมทางด้าน Output

จุดมุ่งหมายของการควบคุมทางด้าน Output ก็เพื่อให้แน่ใจว่าผู้มีหน้าที่เกี่ยวข้องที่ได้รับมอบหมายเท่านั้นที่ได้รับรายงานที่เป็น Output ในช่วงเวลาที่เหมาะสม

การทุจริตทางด้าน Output ที่มักเกิดขึ้นอยู่เสมอก็คือ รายงานที่เป็น Output ได้รับการบิดเบือนแก้ไขเพื่อปิดบังการทุจริต หรือทำให้ผู้ใช้รายงานเข้าใจผิดในข้อเท็จจริง รายงานที่เป็น Output ถูกทำลาย หรือถูกนำไปขายแก่บุคคลอื่นที่ต้องการทราบความลับ

มาตรการที่ใช้ในการควบคุมด้าน Output ประกอบด้วย

เอกสาร Output ที่มีความสำคัญ เช่น เช็คเงินเดือนที่พิมพ์โดยคอมพิวเตอร์ การพิมพ์หมายเลขลำดับล่วงหน้า และมีทะเบียนคุมหมายเลข ซึ่งสามารถตรวจสอบความสัมพันธ์ระหว่างหมายเลขในทะเบียนคุมและหมายเลขเอกสารที่ถูกนำไปพิมพ์เป็น Output อยู่เสมอ

บทที่ 8

การทุจริตเกี่ยวกับบัตรเครดิต และการป้องกันการทุจริต และอาชญากรรมคอมพิวเตอร์

การทุจริตเกี่ยวกับบัตรเครดิต และการป้องกันการทุจริตและอาชญากรรมคอมพิวเตอร์

1. การทุจริตเกี่ยวกับบัตรเครดิต

สามารถเกิดขึ้นได้จากกลุ่มบุคคล 3 กลุ่ม คือ

1.1 กลุ่มบุคคลที่มีวัตถุประสงค์กระทำการทุจริตด้วยวิธีการ เช่น

1.1.1 ปลอมแปลงบัตรเครดิต แล้วนำบัตรเครดิตไปหลอกใช้กับร้านค้ารับบัตร

1.1.2 ปลอมแปลงบัตรเครดิต แล้วสมคบกับร้านค้ารับบัตร

1.1.3 ปลอมแปลงบัตรเครดิตที่หมดอายุแล้ว มาลบรหัสและอักษรตัวนูนด้วยเตารีด หรือความร้อนอื่น แล้วพิมพ์ข้อมูลใหม่ทับเข้าไปแล้วนำบัตรปลอมนี้ไปใช้

1.1.4 นำบัตรเครดิตจากผู้ถือบัตรที่เป็นชาวต่างประเทศที่ฝากไว้ตามที่พักไปใช้

1.1.5 ขโมยบัตรเครดิตในระหว่างทางที่มีการส่งบัตรเครดิตทางไปรษณีย์

1.2 ร้านค้ารับบัตร กระทำการทุจริตโดย

1.2.1 ร่วมมือกับพนักงานโรงแรมปลอมแปลงบัตรเครดิต โดยวิธีนำข้อมูลส่วนที่เป็นตัวนูน (Embossing) ไปพิมพ์บนบัตรขาว (White card) โดยไม่มีแถบแม่เหล็กหลังบัตร แล้วนำบัตรขาวไปใช้

1.2.2 รูดบัตรเครดิตซ้ำ ขณะที่เจ้าของบัตรเผลอ

1.3 ผู้ถือบัตรหรือเจ้าของบัตร กระทำการทุจริตโดย

1.3.1 โกงเอง โดยอ้างว่าไม่ได้ใช้บัตรเครดิต

1.3.2 ร่วมมือกับผู้ทุจริต โดยการขายหรือให้ใช้บัตรเครดิตของตนเพื่อการทุจริต

2. การป้องกันการทุจริตเกี่ยวกับบัตรเครดิต

ทุกฝ่ายที่เกี่ยวข้อง ได้แก่ ผู้ถือบัตร ร้านค้ารับบัตร และผู้ออกบัตร (ธนาคารพาณิชย์ หรือบริษัทผู้ออกบัตรเครดิต) จะต้องร่วมมือกันโดยใกล้ชิด

ในส่วนของธนาคารพาณิชย์ ได้มีการป้องกันการทุจริตเกี่ยวกับบัตรเครดิตไว้หลายวิธี เช่น

2.1 ออกแบบและผลิตบัตรเครดิตให้ยากต่อการปลอมแปลง

2.2 ใช้เครื่อง Verify ในการตรวจสอบบัตรและอนุมัติรายการ

2.3 เรียกเก็บและทำลายบัตรเครดิตที่หมดอายุต่อหน้าผู้เป็นเจ้าของบัตร

2.4 ควบคุมการจ่ายบัตรเครดิตให้แก่ผู้ถือบัตรโดยตรง ไม่ผ่านไปรษณีย์

2.5 พิจารณาคัดเลือกผู้ถือบัตรและร้านค้าผู้รับบัตรอย่างเข้มงวด

2.6 ขอความร่วมมือจากผู้ถือบัตรในการแจ้งให้ธนาคารพาณิชย์ (ผู้ออกบัตร) ทราบทันทีที่บัตรสูญหาย

2.7 ประกันภัยเพื่อชดเชยหรือบรรเทาความเสียหายที่เกิดจากการทุจริต

3. กฎหมายเกี่ยวกับบัตรเครดิตในประเทศสหรัฐอเมริกา

ในหมวด 16 มาตรา 1601 ของประมวลกฎหมายแพ่งสหรัฐอเมริกา อธิบายว่า ข้อกำหนดต่าง ๆ ตามหมวดนี้ ซึ่งสามารถเรียกว่า "พระราชบัญญัติบัตรเครดิตปลอม พ.ศ. 2527" (Credit Card Fraud Act of 1984) มีสาระสำคัญโดยสรุป ดังนี้

ลักษณะการปลอมแปลงหรือการกระทำความผิดในเรื่องนี้ อาจจะกระทำโดย

บุคคลคนเดียว หรือ

กลุ่มบุคคลตั้งแต่ 2 คนขึ้นไปก็ได้

ในกฎหมายนี้กำหนดบทลงโทษไว้โดยแบ่งตามประเภทของการทุจริต หรือกระทำความผิดให้มีโทษ

ปรับ

จำคุก หรือ

ทั้งจำทั้งปรับ

(ปรับไม่เกิน 10,000 - 100,000 เหรียญสหรัฐ จำคุก 10 - 20 ปี)

4. กฎหมายเกี่ยวกับบัตรเครดิตในประเทศไทย

ในขณะนี้ยังไม่มีกฎหมายเรื่องบัตรเครดิตโดยเฉพาะกำหนดไว้

เพียงแต่สามารถอนุโลมนำประมวลกฎหมายอาญา มาตรา 265 มาใช้ตัดสินได้ว่า

ผู้ปลอมบัตรเครดิตมีความผิดฐานปลอมเอกสารสิทธิ์ มีโทษจำคุกตั้งแต่ 6 เดือน ถึง 5 ปี และปรับตั้งแต่ 1,000 บาท ถึง 10,000 บาท



5. กฎหมายการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Fund Transfer Act - EFT)

สำหรับกฎหมายของสหรัฐอเมริกาในเรื่องการโอนเงินทางอิเล็กทรอนิกส์ (EFT) นั้น ครอบคลุมเกี่ยวกับเรื่องการโอนเงินโดย

ATM

POS

บัตรเดบิต

บัตรเครดิต และ

สำนักหักบัญชีอัตโนมัติ (ACH) ด้วย

จะเห็นได้ว่าบัตรเครดิตเป็นส่วนหนึ่งของ EFT Act อยู่แล้ว ถ้ามีการร่างกฎหมายนี้ขึ้น

ประเภทของอาชญากรรมด้านคอมพิวเตอร์

1. ยักยอกวัสดุอุปกรณ์และเวลาคอมพิวเตอร์
2. การเปลี่ยนแปลงแก้ไขหรือปลอมแปลงข้อมูลเข้า
3. การปลอมแปลงแก้ไขแฟ้มข้อมูล (Master file)
4. การปลอมแปลงแก้ไขโปรแกรม
5. การนำโปรแกรมส่วนตัวมาแอบใช้แทนโปรแกรมในระบบ
6. การลักลอบคัดลอกข้อมูลในข่าวโทรคมนาคม
7. การขโมยแฟ้มข้อมูลหรือโปรแกรม
8. การใช้อุปกรณ์คอมพิวเตอร์ในทางทุจริต
9. การใช้คอมพิวเตอร์เป็นแพะรับบาป หรือโฆษณาหลอกลวง
10. การใช้คอมพิวเตอร์เป็นเครื่องมือขู่กรรโชก



การป้องกันอาชญากรรมคอมพิวเตอร์

1. การใช้คอมพิวเตอร์ทำให้ข้อมูลมารวมกันอยู่ที่จุดเดียวหมด
   - ควรป้องกัน File Library ให้รัดกุม

2. การใช้คอมพิวเตอร์ช่วยให้ซุกซ่อนความผิดได้ง่าย
   - ข้อมูลอยู่ในจานแม่เหล็กมองไม่เห็นด้วยตาเปล่า จึงต้องมีโปรแกรมตรวจสอบอย่างดี

3. การใช้คอมพิวเตอร์ช่วยให้สามารถแก้ไขโปรแกรมและข้อมูลโดยไม่ทิ้งร่องรอยไว้มาก
   - จะต้องจัดให้มีรหัสลับสำหรับผู้ที่จะมีสิทธิแก้ไขข้อมูลและโปรแกรม
   - จัดให้คอมพิวเตอร์บันทึกการแก้ไขเอาไว้เป็น Exception Report

4. การใช้คอมพิวเตอร์ช่วยให้สามารถทำลายหลักฐานได้ง่ายดาย
   - แก้ไขได้โดยการจัดทำ Back up copy และมีการตรวจสอบ Back up copy เป็นระยะ ๆ

5. การใช้คอมพิวเตอร์ในระบบ On-Line มักจะมีการตรวจสอบข้อมูลน้อยกว่าระบบธรรมดา
   - ใช้บุคคลควบคุมในการส่งข้อมูลเข้า
   - ใช้ program ควบคุมในการส่งข้อมูลเข้า
   - ใช้ pass word ควบคุม

6. การใช้คอมพิวเตอร์ทำให้ชาวบ้านเชื่อถือมากเกินไป
   - แก้ไขโดยการประชาสัมพันธ์ให้ผู้ใช้ทั่วไปทราบว่า คอมพิวเตอร์ก็ผิดได้ ถ้ามีคนสั่งทำให้ผิด

7. การใช้คอมพิวเตอร์ทำให้ควบคุมข้อมูลลำบาก
   - ข้อมูลที่เก็บเป็นจานแม่เหล็กบางชุดอาจต้องอยู่ในสถานที่คอมพิวเตอร์เรียกใช้ตลอดเวลา (On-Line) ผู้ที่มี Terminal อาจติดต่อหรือคัดลอกข้อมูลได้ แก้ไขได้โดยการแปลข้อความเป็นรหัส

8. การใช้คอมพิวเตอร์บางแห่งทำให้ไม่มีการแยกความรับผิดชอบ
   - แก้ได้โดยการจัดแบ่งหน้าที่พนักงานเตรียมข้อมูล ไม่ให้คนเดียวมีสิทธิทำได้ทุกอย่าง

9. การออกแบบระบบคอมพิวเตอร์มักจะไม่คำนึงถึงการตรวจสอบ
   - จัดให้มีผู้ตรวจสอบร่วมพัฒนาระบบงานด้วย

บทที่ 9

แนวทางปฏิบัติสำหรับผู้บริหารในการรักษาความปลอดภัยของระบบการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์

แนวทางปฏิบัติสำหรับผู้บริหารในการรักษาความปลอดภัยของระบบการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ (EDP Security - A Practical Approach for Managers)

1. การรักษาความปลอดภัยของระบบการประมวลผลด้วยคอมพิวเตอร์ (Security and EDP Security)

1.1 ความเสี่ยง (Risk)

ในการกำหนดแนวทางในการรักษาความปลอดภัยของระบบประมวลผลด้วยคอมพิวเตอร์นั้น ผู้บริหารจะต้องทราบก่อนว่ามีความเสี่ยง (Risk) หรือภัยอะไรบ้างที่จะต้องทำการควบคุมป้องกัน การรักษาความปลอดภัยจะเกี่ยวข้องกับความเสี่ยงภัยที่อาจเกิดขึ้น แนวความคิดในการสร้างระบบรักษาความปลอดภัยมีดังนี้คือ

- Make infiltrators task difficult คือ จะต้องพยายามหาจุดอ่อนที่ทำให้เกิดความเสี่ยงหรือภัย แล้วพยายามทำให้ภัยนั้นเกิดขึ้นได้ยาก
- Focus on both prevention and detection การรักษาความปลอดภัยจะต้องมีทั้งวิธีการป้องกัน (Prevention) ไม่ให้เกิดภัยขึ้น และถ้าหากภัยเกิดขึ้นกับระบบงานแล้วจะมีวิธีการแก้ไข (Detect and Recovery) ให้ระบบสามารถทำงานต่อไปได้อย่างไร
- Ensure cost is reasonable ต้นทุนค่าใช้จ่ายที่เกิดขึ้นในการรักษาความปลอดภัยต้องเหมาะสม

1.2 หลักการของระบบการรักษาความปลอดภัย (Security Axioms)

จุดประสงค์ของระบบการรักษาความปลอดภัย คือ ต้องทำให้ภัยเกิดขึ้นได้ยากที่สุด และความเสียหายเกิดขึ้นน้อยที่สุด โดยการจัดให้มีการควบคุมด้านต่าง ๆ ได้แก่ System Controls, Physical Controls, Administrative Controls, Social Controls เป็นต้น ซึ่งการควบคุมที่ดีจะต้องสามารถครอบคลุมความเสี่ยงที่อาจเกิดขึ้นได้มากกว่าหนึ่งอย่าง



2. ข้อควรปฏิบัติในการสร้างระบบการรักษาความปลอดภัย (What Should You Do)

ขั้นที่ 1 : Preliminary

2.1 ผู้บริหารจะต้องตระหนักว่าข้อมูล (Information) นั้น เป็นเสมือนทรัพย์สินที่สำคัญของบริษัท หากข้อมูลสูญหายหรือถูกทำลายอาจไม่สามารถหาข้อมูลมาทดแทนได้เหมือนทรัพย์สินอย่างอื่น

2.2 ต้องกำหนดให้บุคคลใดบุคคลหนึ่ง หรือกลุ่มบุคคล ทำหน้าที่รับผิดชอบระบบการรักษาความปลอดภัยของระบบการประมวลผลด้วยคอมพิวเตอร์ (EDP Security)

ขั้นที่ 2 : Diagnostic

2.3 กำหนดข้อผิดพลาด (Exposure) ที่จะเกิดขึ้นกับข้อมูล อันได้แก่ การใช้ข้อมูลอย่างไม่ถูกต้อง การเปลี่ยนแปลงข้อมูล การขโมยข้อมูล และการทำลายข้อมูล เป็นต้น

2.4 ประเมินผลวิธีการรักษาความปลอดภัยเพื่อป้องกัน และวิธีการรักษาความปลอดภัยของข้อมูลที่ใช้อยู่ในปัจจุบัน

2.5 ระบุผลแตกต่างระหว่างผลที่ได้จากระบบการรักษาความปลอดภัยที่มีอยู่และต้นทุนในการขจัดหรือลดภัย

2.6 กำหนดวิธีการเพื่อปรับปรุงวิธีการรักษาความปลอดภัย โดยเสียค่าใช้จ่ายคุ้มค่า (Cost Effective Improvements)

ขั้นที่ 3 : Implementation

2.7 ทำการปรับปรุงวิธีการรักษาความปลอดภัย

2.8 ควรทำการทดสอบความเหมาะสมของระบบรักษาความปลอดภัยเป็นระยะ ๆ อย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงวิธีการควบคุมและรักษาความปลอดภัย



3. ข้อไม่พึงปฏิบัติ (What Not To Do)

3.1 ไม่มีการกำหนดผู้รับผิดชอบในการรักษาความปลอดภัยระบบการประมวลผลด้วยคอมพิวเตอร์

3.2 มุ่งทำการป้องกัน (Protection) ภัย แต่ลืมกำหนดวิธีการแก้ไข (Detection/Recovery) เพราะถึงจะมีระบบการป้องกันรักษาความปลอดภัยที่ดีที่สุด ก็ยังอาจเกิดความเสียหายขึ้นได้ ดังนั้นจะต้องคำนึงถึงว่าถ้าเกิดความเสียหายขึ้นจะมีวิธีการแก้ไข หรือฟื้นฟูให้ระบบงานดำเนินต่อไปได้อย่างไร

3.3 ละเลยการรักษาความปลอดภัยในบาง Area ที่เป็นจุดอ่อน

3.4 ระวังเฉพาะภัยที่เกิดจากการกระทำโดยเจตนา ละเลยการป้องกันภัยที่อาจเกิดขึ้นโดยบังเอิญ

3.5 ทำการป้องกันเฉพาะภัยที่เกิดขึ้นจากการทำลายจากภายนอกบริษัท โดยลืมป้องกันภัยที่อาจเกิดขึ้นภายในสำนักงาน

4. การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นวิธีการที่ช่วยผู้บริหารในการกำหนดความเสี่ยง ประเมินผลระบบการรักษาความปลอดภัย และชี้ให้เห็นถึงต้นทุนที่เหมาะสม (Cost Effective) ในการปรับปรุงวิธีการรักษาความปลอดภัย ตัวอย่างการวิเคราะห์ความเสี่ยงที่จะกล่าวถึงต่อไป เป็นวิธีวิเคราะห์ความเสี่ยงที่ The Touche Ross (Australia) ใช้

4.1 ขั้นตอนการวิเคราะห์ความเสี่ยง (Risk Analysis Methodology)

ขั้นที่ 1 : รวบรวมข้อมูล

ขั้นที่ 2 : วิเคราะห์ความเสี่ยง โดยจัดทำแผนฉุกเฉินล่วงหน้า (Precontingency Planning) คือ

- กำหนดและวิเคราะห์ภัยที่อาจเกิดขึ้นได้ ระบุว่ามีภัย (Threats) อะไรบ้าง
- จัดทำ Control Metric
- ระบุค่าของภัย (Threat Coefficients)
- ประมาณความเสียหายที่อาจเกิดขึ้นเป็นจำนวนเงิน

ขั้นที่ 3 : วิเคราะห์ต้นทุน/กำไร (Cost/Benefit Analysis)

โดยจัดลำดับของภัย (Ranking of Threats) การวิเคราะห์ความเสี่ยงจะต้องครอบคลุม Facilities ต่าง ๆ ในระบบคอมพิวเตอร์ ได้แก่ อุปกรณ์ บุคลากร ฐานข้อมูล ระบบ Back up/Recovery ระบบการติดต่อสื่อสาร เป็นต้น นอกจากนี้ยังต้องครอบคลุมถึงแต่ละระบบงาน (Application Area) ได้แก่ Area ที่เป็นผังเครื่องคอมพิวเตอร์ วิธีการเข้าถึง วิธีการประมวลผล วิธีปฏิบัติของ User เอกสารหลักฐานต่าง ๆ และวิธีการ Recovery เป็นต้น

ขั้นที่ 4 : กำหนดแนวทางของแผนฉุกเฉิน (Contingency Planning Guidelines)

ขั้นที่ 5 : กำหนดแนวทางของแผนฟื้นฟูระบบ (Disaster Recovery Guidelines)

ขั้นที่ 6 : Post Contingency Planning

4.2 แบบของการวิเคราะห์ความเสี่ยง (Risk Analysis Model) ประกอบด้วย

ส่วนที่เป็น Input ของการวิเคราะห์ความเสี่ยง มีดังนี้

- การกำหนดภัยที่อาจเกิดขึ้นได้ (Potential Threats) โดยคำนึงถึงภัยต่าง ๆ ที่สามารถทำลายระบบเครื่องคอมพิวเตอร์ได้ ได้แก่ ภัยที่เกิดจากการกระทำของมนุษย์ ภัยที่เกิดจากเครื่องคอมพิวเตอร์ ภัยธรรมชาติ เป็นต้น ซึ่งภัยเหล่านี้จะเกี่ยวข้องโดยตรงกับระบบการควบคุมที่มีอยู่
- ต้นทุนความเสียหายถ้าเกิดภัยขึ้น (Equipment Damage Costs) ได้แก่ ต้นทุนการซื้ออุปกรณ์ใหม่มาใช้แทนอุปกรณ์ที่เสียหายหรือถูกทำลายไป
- ปัจจัยที่ทำให้ Users ล่าช้าเมื่อมีภัยเกิดขึ้น (Factors Relating to Delays)
- แผนฉุกเฉิน (Contingency Plan) ที่กำหนดขึ้น มีต้นทุนหรือค่าใช้จ่ายเท่าไร

ส่วนที่เป็น Output คือ ผลที่เกิดขึ้นถ้าเกิดภัย หมายถึง ผลเสียหายจากอุปกรณ์ ผลเสียหายที่เกิดจากความล่าช้าของ Users ผลเสียหายรวม Cost-Benefit Gap (คือ ต้นทุนหรือค่าใช้จ่ายในการขจัดภัยที่อาจเกิดขึ้น หักด้วยผลเสียหายที่เป็นจำนวนเงินถ้าเกิดภัยนั้น ๆ ขึ้น) และระยะเวลาคืนทุน (Payback Years)

4.3 สิ่งที่ผู้บริหารควรปฏิบัติหลังจากการวิเคราะห์ความเสี่ยง คือ

- กำหนดความรับผิดชอบให้ผู้ที่เกี่ยวข้อง
- พัฒนามาตรฐานหรือนโยบายการรักษาความปลอดภัย ได้แก่ มาตรฐานของ Users, มาตรฐานของ EDP Facilities ข้อมูล ข่ายงาน ระบบ Back up นโยบายด้านบุคคล มาตรฐานของระบบงาน เป็นต้น
- ดำเนินการวิเคราะห์ความเสี่ยงต่อไป

4.4 สรุป (Conclusions)

การสร้างระบบรักษาความปลอดภัยนั้น ผู้บริหารจะต้องคำนึงถึงกฎการลดน้อยถอยลงของผลตอบแทน (Law of Diminishing Returns) ดังนั้นระบบการรักษาความปลอดภัยที่ควรนำมาใช้จะต้องเป็นระบบที่ให้ผลตอบแทนคุ้มค่ากับต้นทุนที่เสียไปเท่านั้น



5. เทคนิคการควบคุมและการรักษาความปลอดภัย (Technique of Security and Control)

5.1 ความทั่วไป

การสร้างระบบการรักษาความปลอดภัยของระบบคอมพิวเตอร์นั้น มีความสัมพันธ์กับความเสี่ยง (Risk) ที่จะเกิดขึ้นกับระบบคอมพิวเตอร์ กล่าวคือ จะต้องกำหนดความเสี่ยงที่อาจเกิดขึ้นได้ก่อน แล้วจึงกำหนดวิธีการควบคุม รวมทั้งเทคนิคในการควบคุม เพื่อป้องกันไม่ให้เกิดความเสี่ยงนั้น ๆ ขึ้น

ในการติดต่อสื่อสาร (Communication) กับระบบคอมพิวเตอร์นั้น จะมีความเสี่ยงในการติดต่อสื่อสาร คือ ผู้ส่งข้อมูลจะแน่ใจได้อย่างไรว่าผู้รับข้อมูล (Receiver) เป็นบุคคลคนเดียวกับคนที่เราต้องการส่งข้อมูลไปให้

เนื่องจากวิวัฒนาการด้านเทคโนโลยีต่าง ๆ เจริญไปอย่างรวดเร็ว ทำให้เกิดบริการทางการเงินแบบใหม่ ได้แก่ บริการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Transfer) ธนาคารทางอิเล็กทรอนิกส์ (Electronic Banking) และ Home Banking เป็นต้น ซึ่งเทคโนโลยีเหล่านี้ช่วยอำนวยความสะดวกรวดเร็วในการให้บริการของธนาคารและสถาบันการเงิน ในขณะเดียวกันก็ทำให้เกิดความเสี่ยงแบบใหม่ขึ้นด้วย

5.2 เทคนิคในการป้องกันการเข้าถึงระบบคอมพิวเตอร์ (Access Control Techniques) มีดังนี้

5.2.1 การใช้รหัสลับ (Password)

Password เป็นเทคนิคอย่างหนึ่งที่ใช้เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์ ผู้ที่ทราบรหัส Password เท่านั้นจึงจะเข้าถึงระบบคอมพิวเตอร์ได้ โดยกำหนดให้ผู้ใช้ต้องป้อนรหัส Password เข้าเครื่องคอมพิวเตอร์ เพื่อตรวจสอบรหัส Password ว่าเป็นบุคคลที่มีสิทธิเข้าถึงระบบจริงหรือไม่ การสร้างรหัสลับควรใช้ความระมัดระวังให้มาก และควรมีการควบคุมที่จำเป็น เพื่อป้องกันรหัสลับ Password ไม่ให้ตกไปอยู่ในมือของบุคคลที่ไม่ได้รับมอบหมาย

5.2.2 Cryptographic

เนื่องจากข่าวสาร (message) ต่าง ๆ ที่ส่งไปมาใน network ต้องการ privacy มาก (privacy problem คือ การป้องกันบุคคลภายนอกลักลอบอ่านข้อมูลจาก network) ดังนั้นทุกครั้งที่มีการส่งข่าวสารต่าง ๆ ควรมีการใช้เทคนิคการแปลงหรือถอดรหัสข้อมูล

เทคนิคการแปลงหรือถอดรหัสข้อมูล (cryptographic) นั้น ถือได้ว่าเป็น system impact ขั้นต่ำเลยทีเดียว เพื่อความปลอดภัยของข้อมูล เราควรทำการแปลงหรือถอดรหัสข้อมูลในทุกครั้งที่มีการส่งข่าวสาร

ลักษณะการทำงานของการแปลงหรือถอดรหัสข้อมูล อาจแบ่งได้เป็น 2 ลักษณะ

- การแปลงรหัสข้อมูล (encryption)
- การถอดรหัสข้อมูล (decryption)

เมื่อผู้ใช้ข้อมูลทำการส่งข่าวสารเขาจะทำการ encrypt ข่าวสารนั้น ๆ ให้เป็นข้อความที่มีการสลับหรือแทนที่ด้วยรหัส (cryptogram) ก่อนที่จะส่งผ่านไปตามข่ายการสื่อสาร และก่อนที่ข้อมูลถึงผู้รับ (receiver) จะมีการถอดรหัส (decrypt) ให้กลายเป็นข้อมูลธรรมดา ด้วยวิธีนี้แม้จะมีผู้ลักลอบต่อสายดักสัญญาณข้อมูล (tap) ก็จะไม่สามารถล่วงรู้รหัสการแปลข้อมูลของเขา และจะอ่านข้อความไม่ออก

ในการแปลงรหัสข้อมูลนั้น เราไม่จำเป็นต้องแปลงข้อมูลทั้งหมด เราควรจะเลือกแปลงเฉพาะที่สำคัญ ๆ เท่านั้น เช่น ในเรื่องของการโอนเงิน เราอาจเลือกแปลงข้อมูลเฉพาะส่วนที่เป็นเลขที่บัญชีและจำนวนเงิน ส่วนที่อยู่และชื่อบัญชีนั้นไม่จำเป็น เราสามารถส่งไปแบบธรรมดาได้

ข้อมูลที่เราทำการส่งไปหลังจากที่แปลงข้อมูลแล้วนั้น เรียกว่า cryptogram ส่วนข้อมูลที่เราส่งไปโดยไม่แปลง คือ ส่งไปแบบธรรมดา เราเรียกว่า plain text

ในเรื่องของการแปลงและถอดรหัสข้อมูล เราควรจะเริ่มแปลงข้อมูลตั้งแต่จุดเริ่มส่งข้อมูล และทำการถอดรหัส ณ จุดรับข้อมูล ไม่ควรให้มีการส่งข้อมูลที่สำคัญ ๆ ในแบบ plain text ไปตามสายสื่อสาร

อย่างไรก็ดี แม้ว่าเราจะมีการแปลงและถอดรหัสข้อมูล แต่ก็ไม่ได้หมายความว่าระบบของเราจะปลอดภัย เพราะการแปลงและถอดรหัสข้อมูลเป็นเพียงการทำให้ผู้ที่ลักลอบดักสัญญาณข้อมูลไม่อาจเข้าใจข้อมูลและข่าวสารที่เราส่งไปมาเท่านั้น แต่ไม่ได้ป้องกันการลอบส่งหรือแก้ไขข้อมูลเข้ามายังระบบของเรา ซึ่งนับว่าอันตรายมากเช่นกัน เช่น ถ้านาย ก. ต้องการโอนเงินจากธนาคาร A ไปยังธนาคาร B ถึงแม้จะมีการ encrypt ข้อมูลแล้วก็ตาม ถ้านาย ข. เป็นผู้ลอบดักสายอยู่ และสามารถดักข้อมูลนี้ไปได้ แม้นาย ข. จะไม่เข้าใจข้อมูลที่ดักได้นี้ แต่เขาก็จะสามารถแก้ไขข้อมูลได้เป็นอย่างอื่น เป็นอะไรก็ได้เขาไม่สนใจ แต่ทว่ารายการและข้อมูลที่นาย ก. ส่งไปก็เปลี่ยนไปแล้ว เงินของนาย ก. ก็ไม่ไปที่ธนาคาร B จำนวนเงินจะผิดไปจากข้อเท็จจริงเท่าใด? ข้อมูลที่ได้รับจะกลายเป็นเช่นไร? ธนาคารจะได้รับความเสียหายมากน้อยเพียงใด? เป็นเรื่องที่ธนาคารต้องคำนึงถึงเช่นกัน

5.2.3 Authentication

คือ การพิสูจน์ผู้ใช้ข้อมูลว่ามาจากเครื่องและบุคคลที่ควรจะเป็นหรือไม่ ทั้งนี้เพื่อให้ผู้รับส่งข้อมูล (sender and receiver) มั่นใจว่าข้อมูลที่รับส่งนั้นถูกต้อง ปลอดภัย

การ authentication นี้อาจทำได้โดยใช้วิธีแปลงและถอดรหัสข้อมูล (cryptographic) ช่วย โดยอาจแปลงทีละ block ทีละ block ไป หรืออาจทำโดยใช้รหัสสอดแทรกเข้าไปในข้อมูล โดยอาศัยหมายเลขลำดับของข้อมูลเป็นหลัก ซึ่งอาจมีการคำนวณหรือใช้สูตรคณิตศาสตร์ร่วมกับข้อมูลที่ใช้ในการพิสูจน์ผู้ใช้ข้อมูล (identifier) ด้วย

ในเรื่องของการ authenticate user นั้น อาจทำได้โดยเมื่อมีการส่งข้อมูลที่แสดงถึง identity ของผู้ส่งผ่านเครือข่ายไปยัง host ผู้รับกำหนดให้ host ตอบกลับมาในระยะเวลาอันควร ด้วยวิธีนี้ข้อมูลจะถูกส่งเข้าทางเครื่องเทอร์มินอลใดก็ได้ที่มีอยู่ในระบบ โดยส่งข้อมูลผ่านมายังเครือข่ายสู่ host ที่เป็นเจ้าของเรื่อง เมื่อ host ได้รับก็จะส่งผ่านให้ controller ทำการเช็คสอบ password ความถูกต้องของข้อมูล ความถูกต้องของผู้ใช้ข้อมูล และส่งคำตอบกลับไปยังแหล่งที่มาของข้อมูล โดยการตอบกลับไปครั้งนี้จะเป็นการเช็คเพิ่มเติมด้วยว่ามาจากเครื่องเทอร์มินอลที่ถูกต้องอีกด้วย และอาจมีการเช็คสอบตัวผู้ใช้เพิ่มเติมอีกก็ได้

Authentication นั้นบอกเราได้ว่า ข้อมูลที่ถูกส่งไปและรับกลับมาแต่ละครั้งมาจากจุดใดและโดยใคร แต่ทั้งนี้ก็ต้องขึ้นอยู่กับระบบและการวางรูปแบบของ Key Management ด้วยว่าเป็นอิสระมากน้อยเพียงใด คือถ้าให้แต่ละ key เป็น key ที่ unique ไม่ว่าจะเป็น terminal's key, token หรือแม้กระทั่ง PIN การ authentication ก็จะยิ่งทำได้ง่าย สะดวกรวดเร็วยิ่งขึ้น ความปลอดภัยก็จะดีขึ้น

5.2.4 Key Management

ใน network หนึ่ง ๆ นั้นเราจำเป็นต้องจัดให้รหัสรายการแต่ละรายการ แต่ละประเภทของรายการ มีรหัสแยกต่างหากจากกัน ทั้งนี้ก็เพื่อความสะดวกในการจัดการ (manage) และเพื่อประโยชน์ในการควบคุม (control) แต่ทว่าด้วยวิธีนี้เองทำให้เราประสบปัญหาการมี key จำนวนมากมาย ดังนั้นเราจึงต้องนำ key management มาใช้อย่างจริงจัง

เช่น ถ้าเราออกบัตรเครดิต 100 ใบ โดยให้สามารถใช้กับระบบ Point of Sales (POS) ได้โดยเรามี terminal ตามร้านค้าต่าง ๆ อยู่ถึง 1,000 เครื่อง ซึ่งถ้าลูกค้าทุกคนใช้บริการเพียงคนละ 1 ครั้งต่อ terminal 1 เครื่อง เราก็จะมีรายการเข้ามาถึง 100 รายการ หรือถ้าลูกค้าใช้คนละ 2 ครั้งต่อ terminal 1 เครื่อง (ลูกค้าทำรายการที่ terminal เดิมทั้ง 2 ครั้ง) เราก็จะมี key เข้ามาถึง 200 keys อะไรจะเกิดขึ้นถ้าลูกค้าแต่ละคนใช้ บริการถึง 10 หรือ 20 ครั้ง และมีการใช้ข้าม terminal สลับไปมา เราอาจมี key เข้ามาเป็นแสน ๆ keys เลยก็ได้

จะเห็นได้ว่ามันมากมายเกินกว่าที่จะจัดทำด้วยวิธีแบบเดิม (manual) นอกจากนี้ข่าวสารต่าง ๆ (information & message) ที่ส่งไปมานั้นถือเป็นเรื่องสำคัญเป็นความลับควรปกปิด (privacy and confidential) ดังนั้นเราจึงหันมาใช้เครื่องมือทางอิเล็กทรอนิกส์ (electronic equipments) ช่วยในการทำ key management แทน

Key System

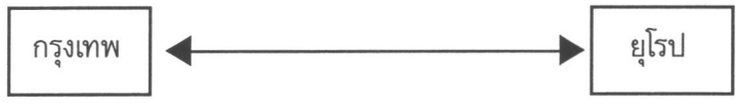
ในระบบ network ที่ใหญ่มาก ๆ เช่น ระบบ ATM, EFT (Electronic Fund Transfer) มักเกิดปัญหายุ่งยากในการ manage key เนื่องจากในธุรกิจที่ใหญ่ ๆ มักมีการร่วมมือกัน (cooperate) ฉะนั้นจะเห็นได้ว่ารายการต่าง ๆ ที่ส่งเข้ามายังศูนย์จะยิ่งยุ่งยากซับซ้อนเพิ่มมากขึ้นอีกหลายเท่าตัว จึงจำเป็นต้องมีระบบ key system ที่ดี แยกเป็นแต่ละประเภท แต่ละรายการ แต่ละระบบงาน และแต่ละบริษัท และยังจะต้อง

แยกอีกว่าเป็นขั้นตอนงานใด เช่น authentication หรือ encryption นอกจากนี้ในการส่งข้อมูลข่าวสารแต่ละครั้ง ผู้ส่ง (sender) และผู้รับ (receiver) จะต้องมี key ที่เหมือนกัน ฉะนั้นในทุก ๆ วัน ทุก ๆ เดือน ทุก ๆ ปี จะมี key ที่ต้องจัดการ (manage) อยู่มากมายเกือบจะตลอดเวลา นับได้เป็นล้าน ๆ keys

การสร้าง key ต่าง ๆ เราอาจทำได้โดยเลือกจากชุดของตัวเลข โดยวิธีสุ่ม เมื่อสุ่มตัวเลขได้จะนำมาแปลงอีกที อาจจะโดยใช้สูตรทางคณิตศาสตร์ เมื่อแปลงเสร็จจึงจะส่งไปยังผู้รับร่วมไปกับข้อมูลที่ต้องการส่งไป ผู้รับก็จะมีวิธีการเช่นเดียวกันกับผู้ส่งในอันที่จะถอดรหัสข้อมูลที่ได้รับให้เหลือเพียงข้อมูลที่แท้จริง

Key Distribution

Network



การส่งข้อมูลและข่าวสารไปตาม network ต่าง ๆ นั้น เราจะต้องมี key ที่เหมือนกันทั้งผู้รับและผู้ส่ง กล่าวคือ การที่กรุงเทพฯ และที่ยุโรปจะติดต่อกันได้นั้น ข้อมูลที่ส่งไปจะต้องมีวิธีการ generate key ที่เหมือนกัน สามารถถอดและแปลงรหัสซึ่งกันและกันได้

ดังนั้นในแต่ละ host (ศูนย์คอมพิวเตอร์) จะต้องมีการเก็บ key ที่ generate ไว้ใน key storage และจะต้องรู้ด้วยว่า key แต่ละ key เป็นของ transaction ใด บริษัทใด

Public Key และ Private Key

ขั้นตอนการทำงานของ public key นั้นยุ่งยากและซับซ้อนมาก แต่ทว่าวิธีการใช้นั้นง่ายมาก (simple use) public key คือ การใช้ key ร่วมกัน (key are share) และจากที่ได้เคยกล่าวมาตั้งแต่ต้นแล้วว่าในระบบหนึ่ง ๆ นั้นมี key มากมายที่เราจะต้อง manage ดังนั้นเพื่อลดปัญหานี้ลงเราจึงใช้ระบบ public key ช่วยได้

ในขั้นตอนการส่งและรับข้อมูลโดยปกตินั้น เราจะมีการแปลงรหัสข้อมูลขณะส่งข้อมูล และจะมีการถอดรหัสในขณะรับข้อมูล ในเรื่องของ public key นั้น หน้าที่การทำงานของ key ที่ใช้แปลงรหัสข้อมูล (encrypt) จะต่างกับ key ที่ใช้ถอดรหัสข้อมูล โดย key ที่ใช้แปลงรหัสข้อมูลนั้นผู้ส่งข้อมูลทุกคน (sender) มีสิทธิใช้ส่งข้อมูล key นี้จึงเรียกว่า public key ส่วน key ที่ใช้ในการถอดรหัสข้อมูลนั้นมีผู้มีหน้าที่เกี่ยวข้องเพียงไม่กี่คนเท่านั้นที่ทราบวิธี เราจึงเรียกว่า private key

Key Destruction

การสร้าง key ขึ้นมาใช้นั้น เมื่อใช้เสร็จหรือไม่ต้องการใช้แล้วเราก็ควรทำลายเสีย และทุกครั้งที่มีการทำลายจะต้องให้แน่ใจด้วยว่า key ที่ต้องการทำลายได้ถูกทำลายไปจริง

Transaction Key

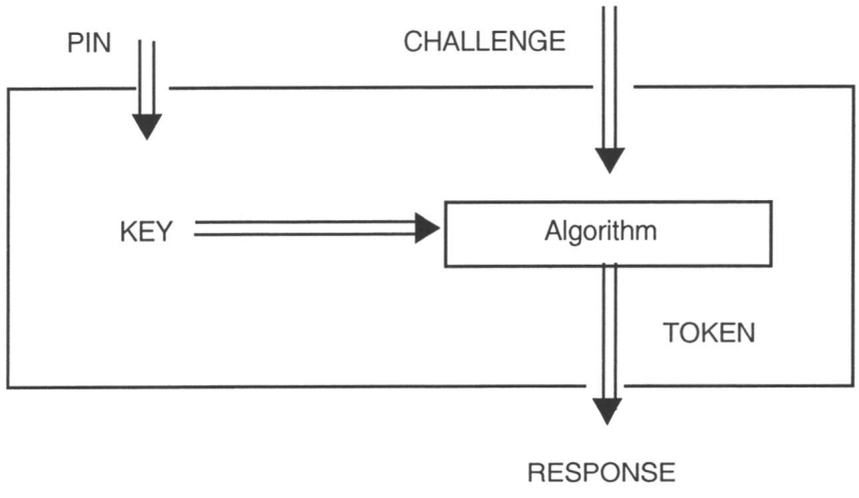
เป็น key ที่สร้างขึ้นสำหรับระบบข้อมูลที่มี Database มักใช้กันในเรื่องของ Credit Card และ ATM

Key System Approve

เมื่อเราจะพิจารณาระบบอะไรก็ตาม เราต้องดูภาพรวมของทั้งระบบด้วยว่าเป็นอย่างไร สามารถตอบสนองความต้องการในปัจจุบันได้ครบถ้วนหรือไม่ อย่างไร time skill เป็นเช่นไร ความปลอดภัย (security) มีพอเพียงหรือไม่ มีความคล่องตัวยืดหยุ่น (flexibility) มากน้อยเพียงใด มีมาตรฐานหรือไม่ (standard) ง่ายต่อการใช้งาน (easy of use) หรือไม่ ตลอดจนมีการวางแผนและการเตรียมการสำหรับการเจริญเติบโต (growth) และการรักษาความปลอดภัย (security) ในอนาคตหรือไม่อย่างไร นอกจากนี้เรายังต้องเตรียมการแก้ปัญหาในกรณีที่ system down อีกด้วย กล่าวคือ จะต้องมีแผนฟื้นฟูระบบ (Recovery Process) ที่ดี สามารถกู้สถานการณ์ให้กลับคืนสู่สภาพปกติได้ในเวลาอันรวดเร็ว เนื่องจากถ้าระบบเกิดการหยุดชะงักขึ้น (system down) นั่นหมายถึงเกิดการสูญเสียขึ้นอย่างใหญ่หลวง องค์การอาจสูญเงินจำนวนมหาศาล ยิ่งเสียนานเท่าใดองค์การก็จะยิ่งเสียหายมากเท่านั้น

5.2.5 Dynamic Access Control System

ในระบบนี้รหัสที่ใช้ควบคุมจะถูกเปลี่ยนแปลงไปตลอดเวลา เช่น ในการควบคุมโดย Dynamic Password ซึ่งเป็นระบบที่ password จะถูกเปลี่ยนทุกครั้งที่มีการส่งข้อมูล ซึ่งการเปลี่ยนแปลงนี้สามารถทำโดยใช้วิธีการแปลงและถอดรหัสข้อมูล (cryptographic) ช่วย ดังรูปต่อไปนี้



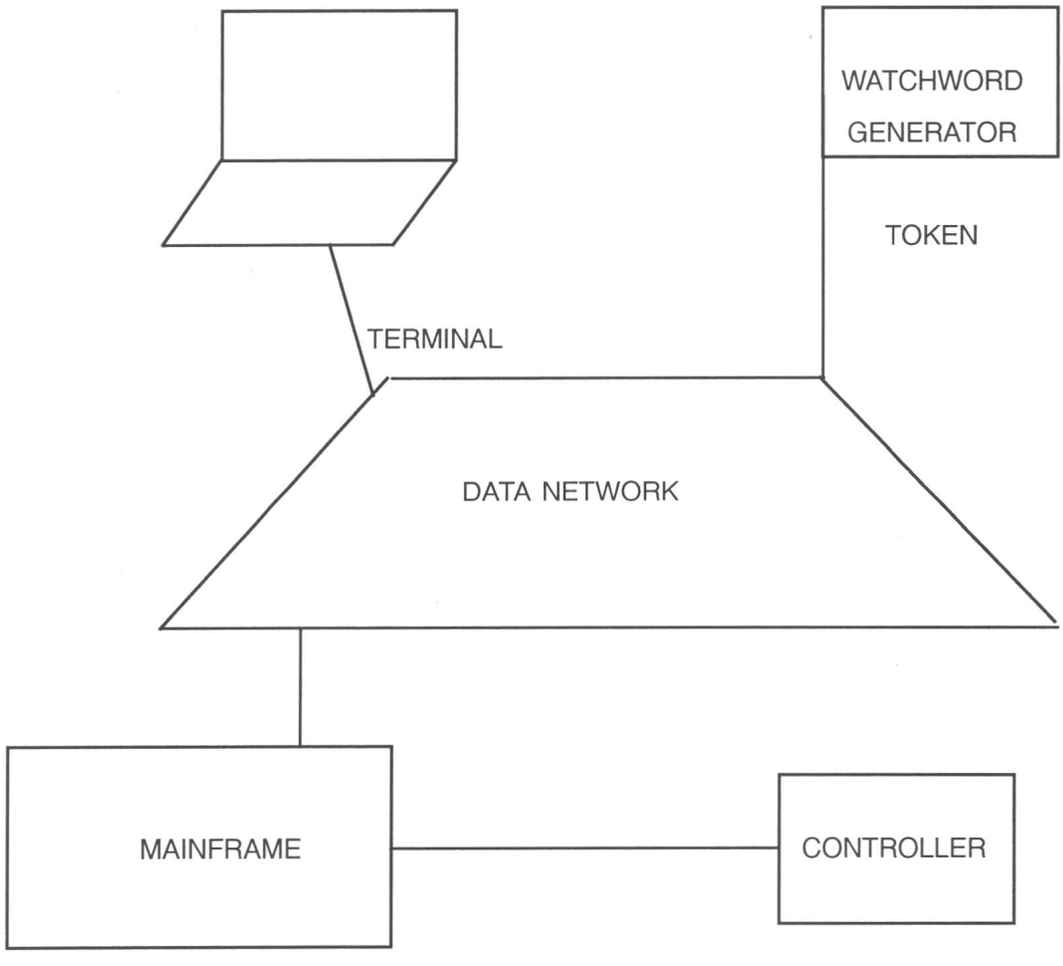
TOKEN : คือ รหัสหรือสิ่งที่เรารู้ เป็นสิ่งที่เรามีอยู่
USER'S TOKEN : คือ รหัสหรือสิ่งที่เป็นของเรา เรารู้ และจะไม่มีใครรู้อีกเลย
TOKEN จะเป็นตัวที่ทำให้ password เปลี่ยนไป

ในเรื่องของการควบคุมการเข้าถึงข้อมูล (access control) จริง ๆ แล้วมี access control facilities มากมายให้เลือกใช้ และสามารถที่จะเลือกจุดควบคุมว่าจะให้ควบคุมที่ host ณ EDP center เลย หรือให้วางจุดควบคุมไว้ที่ตัว terminal เองในแต่ละระบบงานก็ได้

Watchword controller ทำหน้าที่ต่อไปนี้คือ

- เก็บข้อมูลของผู้ใช้และ keys (maintains list of users and keys)
- สร้างรหัสตอบโต้ (generate challenges)
- การพิสูจน์ความถูกต้องของข้อมูลที่ได้รับจากผู้ใช้ (verifies responses)
- จัดเตรียมเอกสารการตรวจ (provides audit trail)

5.2.6 Dynamic Password Scenario



User's token มีลักษณะหน้าที่ดังต่อไปนี้

- generate response
- PIN ที่ใช้เป็นของ user ซึ่ง user จะรู้แต่เพียงผู้เดียว
- key จะต้อง unique

(PIN จะเป็นแนวทางไปสู่ key ที่ถูกต้อง ซึ่งนับได้ว่าเป็น unique key)
ความสามารถในการป้องกัน (protection) การเข้าถึงระบบ จะขึ้นอยู่กับ

- การบริหารงานของระบบงาน (system management)
- ความสามารถของ user (user awareness)
- ความสามารถของ token นั้น ๆ (token forgeability)

ขั้นตอนการทำงานและการตอบสนองของระบบ

ถ้าเราได้รับข้อมูลที่ลอบส่งเข้ามา หรือข้อมูลที่ผิดปกติ หรือสิ่งที่ไม่คาดคิดมาก่อน token จะพยายามจำกัดความเสี่ยงให้ลดลง อย่างไรก็ตามการทำงานจะได้ดีมากน้อยเพียงใดนั้น ขึ้นอยู่กับ user's token และ user's knowledge ด้วย

ANSI X3.92

เป็นมาตรฐานอย่างหนึ่งที่ The American National Standard Institute กำหนดขึ้น ANSI X 3.92 นี้ใช้กันอย่างแพร่หลายมากในธุรกิจการเงินและการธนาคาร เนื่องจากการใช้ระบบที่เป็นมาตรฐานจะทำให้เราสามารถติดต่อสื่อสารกับผู้อื่นที่ใช้อุปกรณ์ที่ base on DEA (ANSI X3.92) ได้มาก นอกจากนี้อุปกรณ์ (device) ที่มีระบบ ANSI X3.92 โดยมากจะสามารถต่อเชื่อมกับอุปกรณ์ประกอบ (device) ได้หลายชนิด เช่น electronic terminal, dumb terminal, telephone ฯลฯ แต่ประสิทธิภาพการทำงานและการตอบสนอง (response) จะขึ้นอยู่กับตัวอุปกรณ์นั้น ๆ เอง และระบบต่าง ๆ ที่ติดตั้งไว้ในอุปกรณ์นั้น ๆ

Watchword Controller

จะทำหน้าที่ป้องกันและจัดให้มีการควบคุมการเข้าถึงข้อมูล (perimeter access control) watchword controller นี้จัดว่าเป็น intelligent peripheral อย่างหนึ่ง

ในการทำงาน watchword controller จะช่วยลดงานของ host ลงอย่างมาก โดยมันจะรับงานบางอย่างมาทำแทน เช่น การเช็คสอบ password การเช็คสอบความถูกต้องของข้อมูล กล่าวคือ ถ้ามีผู้ต้องการจะเข้าถึงระบบคอมพิวเตอร์ที่ host โดยอาจทำที่ EDP center เอง หรือโดยผู้ต้องการ access ทำการ key คำสั่ง ผ่าน terminal ส่งไปยัง host เมื่อถึงขั้นตอนการเช็คสอบ password และความถูกต้องของข้อมูล คำสั่งหรือข้อมูลดังกล่าวส่งผ่านไปยัง watchword controller เพื่อให้ทำการตรวจสอบความปลอดภัยของ password แทน

โดยปกติแล้วในระบบการสื่อสารหนึ่ง ๆ นั้น เราต้องมีอุปกรณ์อย่างน้อย 2 ชุด เพื่อทำการสื่อสารถึงกัน เช่น ธนาคารบางแห่งอนุญาตให้ลูกค้าทำรายการในระบบ on-line โดยใช้เครื่อง terminal ของตนเชื่อมกับเครื่องคอมพิวเตอร์ของธนาคารได้ โดยลูกค้าเพียงแต่แจ้งความประสงค์การขอใช้บริการมายังธนาคาร ธนาคารก็จะจัดช่องทางหรือสายสื่อสารให้ลูกค้าทำการติดต่อกับธนาคารได้

การทำงานของระบบจะเริ่มจากการที่ Host เริ่มทำงานในระบบ network โดย host อาจจะได้รับข้อมูล ข่าวสาร password คำสั่ง หรืออะไรบางอย่างที่แสดงถึง user's identifiers เช่น ID ชื่อ รหัสจาก terminal ที่ส่งผ่านมาทาง network เมื่อ host รับข่าวสารนั้น ๆ เข้ามาแล้ว จะทำการส่งต่อไปยัง controller เพื่อทำการเช็คสอบ password และความถูกต้องของข้อมูล และทำการตอบสนองกลับไปยังแหล่งที่มา

สรุปลักษณะของ Dynamic Password

- user ไม่ต้องยุ่งเกี่ยวกับการจัดการ key (key management)
- user สามารถเลือก PIN ได้
- generator จะเป็นตัวควบคุมการเข้าถึงข้อมูล (generator access control)
- จะมีการตอบสนองจากเครื่องคอมพิวเตอร์เสมอ
- ข่าวสารข้อมูลต่าง ๆ ที่เกี่ยวกับการรักษาความปลอดภัย จะเก็บอยู่ใน controller
- เป็นระบบที่สร้างภายใต้มาตรฐาน ANSI X3.92
- มีการบันทึก audit trail โดยครบถ้วน (full audit trail)

PCC Security Card Bit

อาจกล่าวได้ว่าเป็นระบบของ IBM หรือ IBM compatible ได้ เนื่องจากโลกถือว่า IBM เป็นบริษัทที่มีเครื่อง PC ที่เป็นมาตรฐานที่สุด โดยมักจะใช้ระบบ ANSI X9.9 หรือ ANSI X9.19 ซึ่งถือเป็นมาตรฐานของ PC เพื่อช่วยในการติดต่อสื่อสารกันในระหว่าง PC (inter-access) ถ้าเรามี security card เราสามารถกำหนดให้เครื่องคอมพิวเตอร์ติดต่อกับ security card นั้นเองได้ และ security card นี้จะช่วยในการรักษาความปลอดภัยระบบสื่อสาร โดยรวมเข้าด้วยระบบอิเล็กทรอนิกส์ (electronic system) แต่จะไม่แยกรักษาความปลอดภัยเฉพาะจุดใดจุดหนึ่ง หรือบุคคลใดบุคคลหนึ่ง

Security card bit นี้จะทำงานโดยมันจะพยายามป้องกันการทุจริต การจารกรรม โดยเราจะต้องสร้าง algorithm ของ signature หรือ algorithm ที่สามารถตรวจสอบบุคคลผู้ใช้ได้ แล้วนำมาต่อเข้ากับเครือข่ายเพื่อจะได้ส่งข้อมูลและข่าวสารต่าง ๆ ผ่านขั้นตอน algorithm นี้ โดยให้ algorithm ทำการพิสูจน์ข้อมูลและข่าวสารต่างๆ (authenticate) ก่อนที่จะอนุญาตให้ติดต่อกับระบบงานได้ ซึ่งทำให้วิธีการอนุญาตให้ติดต่อกับระบบและการตรวจสอบข้อมูลทำได้สะดวกและรวดเร็วมาก

ทุกครั้งที่มีการเข้าสู่ข่าวการสื่อสาร ควรจะต้องทำการตรวจสอบข้อมูลทุกครั้ง โดยอาจทำเป็นทอด ๆ จากแหล่งหนึ่งไปสู่อีกแหล่งหนึ่งจนกว่าจะถึงที่หมาย เพื่อให้แน่ใจว่าข้อความที่ส่งไปและรับมานั้นถูกต้อง

ระบบการรักษาความปลอดภัยนั้นมีอยู่ 2 แหล่ง คือ

- Software Package
- Hardware ซึ่งได้แก่ terminal, electronic machine,

dumb terminal, telephone, controller

โดยที่อุปกรณ์หนึ่ง ๆ อาจมีการใช้ทั้ง 2 แบบ เช่น อาจมีการใช้ PIN, TOKEN, challenge และมี software package ช่วยในเรื่องระบบการรักษาความปลอดภัยของข้อมูลวิ่งอยู่บนเครื่องอีกทีหนึ่งก็ได้

การใช้ PC security card นี้ง่ายและสะดวกมาก เราอาจใช้การ์ดนี้แทนการใช้ PIN หรืออาจใช้ทั้ง 2 อย่างก็ได้ โดยเราเพียงแต่สอดการ์ดนี้เข้าไปในเครื่องคอมพิวเตอร์ โดยเครื่องคอมพิวเตอร์จะนำข้อมูลจากการ์ดนี้เป็นแนวทาง (trial) ไปสู่ key และส่งต่อไปยังข่ายการสื่อสาร เพื่อไปยัง host ทั้งนี้ในขั้นตอนนี้อาจมีการแปลงรหัสข้อมูลก่อน เพื่อเพิ่มการรักษาความลับขึ้นอีกชั้นหนึ่ง เพราะถ้ามีการลอบดักสายก็จะไม่สามารถเข้าใจข้อมูลของเราได้ นอกจากนี้เมื่อข้อมูลถูกส่งไปยัง host แล้ว ที่ host อาจมีการตอบกลับไปยังแหล่งที่ส่งข้อมูลอีกทีเพื่อตอบรับว่าได้รับคำสั่งเรียบร้อยแล้ว หรือถ้าระบบนั้นต้องการความปลอดภัยมาก ๆ ก็อาจให้ host ส่งสัญญาณถาม (require) ข้อมูลยืนยันผู้ใช้เพิ่มเติม หรือให้ผู้ใช้ยืนยันอีกครั้ง โดยที่ทุกครั้งที่ host ติดต่อกลับเพื่อขอข้อมูลเพิ่มเติมหรือเพื่อให้ยืนยัน password นั้น ตัวผู้ใช้เองไม่จำเป็นต้องยุ่งยากเลย เพราะเครื่องจะไป access card เอาเอง ซึ่งจะเห็นได้ว่าง่ายและสะดวกมาก

อาจกล่าวได้ว่า key จะถูก access โดย PIN หรือ card โดยการที่จะเข้าถึง key ได้ ต้องรู้ PIN หรือใช้ card เสียก่อน แต่ที่จริงแล้ว key ที่พูดถึงกันนั้นไม่ใช่ key จริง ๆ แต่เป็นขั้นตอนการ process key โดยใช้ PIN เป็นแนวทางไปสู่ข้อมูลจริง และ key ไม่ใช่เป็นตัวเลขที่เก็บไว้ตายตัวแต่อย่างใด อาจเป็นเพียง algorithm หรือสูตรคำนวณทางคณิตศาสตร์เท่านั้น โดย PIN หรือ card ที่ได้รับมาจะเปลี่ยนแปลงไม่ได้ เพราะถ้าเปลี่ยนแปลงเครื่องจะคำนวณหา key ไม่ได้ ทำให้ไม่อาจจะใช้งานกับเครื่องได้

ดังนั้นในกรณีที่เรากำหนดให้การ์ดแต่ละใบใช้ได้เฉพาะกับเครื่อง terminal บางเครื่องเท่านั้น เราก็นำการ์ดนั้นไปใช้กับ terminal อื่นไม่ได้ และในกรณีที่บัตรถูกขโมย แม้ผู้ขโมยจะมี card หรือ PIN ถ้าเขาเข้าไม่ถึงเครื่อง terminal ของเรา เขาก็ไม่สามารถเข้าถึงข้อมูลได้ อย่างไรก็ดีถ้าการ์ดหาย หรือหากจะเปลี่ยน PIN ให้แจ้ง security manager ให้ดำเนินการให้ได้



บทที่ 10

สัญญาณการทุจริต หรือจุดอ่อนบางประการในองค์กรที่ใช้คอมพิวเตอร์

สัญญาณการทุจริตหรือจุดอ่อนบางประการในองค์กรที่ใช้คอมพิวเตอร์

มีสัญญาณการทุจริตหรือจุดอ่อนในระบบงานโดยทั่ว ๆ ไป ซึ่งจะชี้ให้ฝ่ายจัดการรู้ล่วงหน้าได้ ถ้าหากฝ่ายจัดการมีความเอาใจใส่ในการบริหารงานอย่างใกล้ชิดและมีประสิทธิภาพ และมีสัญชาตญาณของนักบริหารที่จะรู้ถึงปัญหาหรือภัยที่เกิดจากการทุจริตในองค์กรของตนได้ล่วงหน้า ซึ่งจะสามารถป้องกันปัญหาได้ก่อนที่จะต้องสูญเสียและต้องแก้ไขปัญหากันในภายหลัง

สัญญาณนี้ก็ไม่จำเป็นจะต้องใช้ความรู้ทางเทคนิค หรือการฝึกฝนแต่อย่างไร อย่างไรก็ตามหากผู้ตรวจสอบภายในหรือผู้สอบบัญชีภายนอก สามารถแจกแจงสัญญาณเตือนภัยเหล่านี้ได้ จะช่วยให้ฝ่ายจัดการขององค์กรสามารถทำหน้าที่ที่สำคัญในการป้องกันการทุจริตหรือทราบจุดอ่อนในระบบงานด้านคอมพิวเตอร์ขององค์การได้อย่างมีประสิทธิภาพเพิ่มขึ้น

ตัวอย่างสัญญาณการทุจริตหรือจุดอ่อนในระบบงาน ได้แก่

- พนักงานให้คำอธิบายอย่างมีพิรุธต่อการหายไปของอุปกรณ์ ทรัพย์สิน หรือเงิน
- บันทึกข้อมูลถูกเขียนขึ้นใหม่โดยไม่มีเหตุผลอันควร
- บันทึกข้อมูล (Record) ถูกแก้ไขเปลี่ยนแปลง เพิ่มเติม ลบล้าง หรือทำลาย โดยผิดขั้นตอน หรือไม่ปฏิบัติตามขั้นตอนที่กำหนดไว้
- ลายมือบนเอกสารสำคัญถูกปลอมแปลง
- บันทึกข้อมูลที่มีอยู่ปรากฏว่าเป็นของปลอม
- สินค้าคงคลังมักขาดจำนวน
- พนักงานในระบบงานสำคัญมีการทำงานล่วงเวลาบ่อย ๆ
- บันทึกข้อมูลไม่มีการปรับปรุงให้ทันเวลา
- บุคลากรในแผนกที่สำคัญรู้สึกลังเลในการให้ความร่วมมือต่อการควบคุมการบันทึกข้อมูล หรือลังเลใจในการให้ความร่วมมือต่อการถูกตรวจสอบ ไม่ว่าจากการตรวจสอบภายในหรือจากบุคคลที่สาม
- พนักงานในศูนย์คอมพิวเตอร์หรือผู้ที่เกี่ยวข้อง แสดงความสนใจระวังต่อคำถามทั่ว ๆ ไปมากเป็นพิเศษ
- คำร้องเรียนของลูกค้า ผู้ขาย ผู้ซื้อ และบัญชีอื่น ๆ มีลักษณะยืดเยื้อ
- คำร้องเรียนของพนักงานในส่วนที่เกี่ยวข้องกันมีจำนวนมากเกินสมควร
- คำร้องเรียนเกี่ยวกับพฤติกรรมการทุจริตถูกละเลยไม่สนใจ
- การกระทำที่ไม่ถูกต้องไม่เป็นไปตามระเบียบ และขาดศักยภาพถูกซ่อนเร้นไว้
- พนักงานในระบบงานสำคัญปฏิเสธการเลื่อนตำแหน่ง หรือการหยุดพักผ่อน
- พนักงานมักจะเถลไถลออกไปนอกแผนกของตนเอง
- ข้อมูลทางการเงินที่เป็นความลับมักจะถูกนำมาใช้เพื่อผลประโยชน์ทางการเงินส่วนตัว

- ข้อมูลภายในรั่วไหลสู่เพื่อนหรือญาติโดยบุคคลภายใน เพื่อผลประโยชน์ด้านการลงทุน
- ความลับทางการค้าถูกลักลอบนำไปขายแก่กิจการที่เป็นคู่แข่ง
- ขบวนการในการตัดสินใจถูกนำออกเผยแพร่แก่บุคคลภายนอกที่ไม่มีหน้าที่เกี่ยวข้อง
- โปรแกรมถูกลักลอบถ่ายสำเนาและนำออกขายแก่บุคคลภายนอก
- รายชื่อลูกค้าถูกถ่ายสำเนาและขายโดยพนักงาน
- ไม่มีเอกสารประกอบระบบงานและคู่มือที่เพียงพอและทันกาล ในการปฏิบัติงานด้านคอมพิวเตอร์
- ไม่มีการทดสอบและประเมินงานควบคุมภายใน โดยบุคคลภายนอกองค์กรที่มีประสิทธิภาพ
- มีการกระทำผิดระเบียบอื่น ๆ

การหลีกเลี่ยงและการป้องกันการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เป็นสิ่งที่ทุกองค์กรจะต้องเกี่ยวข้อง จึงเป็นสิ่งที่จะหลีกเลี่ยงมิได้ที่ฝ่ายจัดการจะต้องเข้าใจสภาพแวดล้อมที่จะก่อให้เกิดมีการกระทำผิดหรือมีจุดอ่อนดังกล่าว ผู้บริหารในปัจจุบันจึงต้องได้รับการศึกษาและอบรมทั้งในด้านความสามารถในการบ่งชี้ปัญหา และการแก้ไขปัญหาดังกล่าว แต่ไม่ถึงกับต้องเป็นผู้ชำนาญในด้านคอมพิวเตอร์ อย่างไรก็ดีนับว่าเป็นโชคร้ายที่องค์กรจำนวนมากเข้าใจว่าถ้าเขาปิดตาเสียบ้างปัญหาดังกล่าวก็จะไม่เกิดขึ้น ซึ่งที่จริงกลับเป็นสิ่งอำนวยความสะดวกให้เกิดการทุจริตหรือจุดอ่อนที่อาจมีปัญหาร้ายแรงตามมาได้



บทที่ 11

วิธีการกระทำการทุจริตบางประการที่ผู้บริหารควรทราบ

วิธีการกระทำการทุจริตบางประการที่ผู้บริหารควรทราบ

วิธีการกระทำการทุจริตโดยใช้คอมพิวเตอร์

รูปแบบการทุจริตแม้ว่าจะมีอยู่มากมาย แต่วิธีการจัดทำกระบวนการต่าง ๆ เพื่อการทุจริตพอจะจำแนกได้เพียง 3 ลักษณะ คือ

1. การปรุงแต่งข้อมูลที่นำเข้าบันทึกในคอมพิวเตอร์
2. การแก้ไขคำสั่ง (program) โดยไม่มีอำนาจ
3. การแก้ไขหรือสับเปลี่ยนข้อมูลในแหล่งเก็บข้อมูล (file alternation and substitutions) หรือการเปลี่ยนแปลงข้อมูลใน Hard Copy หรือ Reports ต่าง ๆ ที่ผู้บริหารหรือผู้ใช้ในการตัดสินใจและดำเนินการโดยเฉพาะการใช้วิธี Off-line แก้ไข Output จากระบบงานบางประเภทที่อาจใช้วิธีนี้ได้ (ประสบการณ์ของไทยจากภาคตะวันออกเฉียงเหนือ)

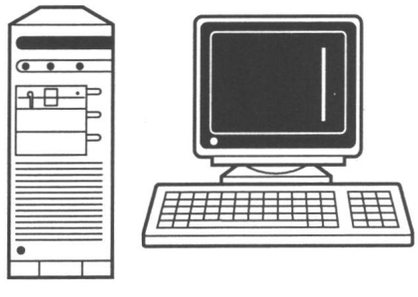
รูปแบบของการทุจริตโดยการใช้คอมพิวเตอร์ อาจจะจัดเป็นกลุ่มได้ดังนี้

1. ยักยอกเวลาของคอมพิวเตอร์ หรือขโมยทรัพยากรของคอมพิวเตอร์ เช่น เทปบันทึกลูกหนี้ สินค้าคงคลัง เป็นต้น
2. ใช้คอมพิวเตอร์เป็นผู้รับบาป (คือ ป้อนความผิดปกติให้คอมพิวเตอร์)
3. ปรุงแต่งข้อมูลที่นำเข้าบันทึก หรือเจตนาบันทึกข้อมูลที่ไม่ถูกต้อง
4. คัดลอกข้อมูลจากฐานบันทึกข้อมูล (Data Base)
5. ดัดแปลงคำสั่งหรือนำโปรแกรมที่ไม่ถูกต้องมาใช้แทนโปรแกรมที่ถูกต้อง
6. ตัดข้อมูลบางส่วนในระบบสื่อสาร



ตัวอย่างการทุจริตแบบผสมระหว่างวิธี Manual กับวิธีการใช้คอมพิวเตอร์แบบ Off-line

ช่วงเวลา	:	ระหว่างปี 2534 ถึงปี 2537
ผู้ทุจริต	:	พนักงานตำแหน่งพิธีการสินเชื่อสาขา ซึ่งรับผิดชอบเกี่ยวกับการรับซื้อลดตั๋วเงินได้ ทำการทุจริตหลายกรณี ดังนี้
การทุจริตแบบ Manual	:	กรณีที่ 1 ปลอมแปลงลายมือชื่อลูกค้าเงินฝากประจำรวม 3 ราย ทำหนังสือยินยอมมอบเงินฝากเป็นประกันเพื่อขอสินเชื่อประเภทเงินให้กู้และตั๋วเงินในนามของลูกค้าผู้ฝากเงินและโอนเงินกู้ที่ได้รับฝากเข้าบัญชีเงินฝากออมทรัพย์ในนามของลูกค้าที่ผู้ทุจริตเตรียมการเปิดบัญชีรอไว้ล่วงหน้า และถอนไปใช้ประโยชน์ส่วนตัวในภายหลัง
การทุจริตโดยใช้คอมพิวเตอร์	:	กรณีที่ 2 แก้ไขข้อมูลการให้สินเชื่อในกรณีที่ 1 เกี่ยวกับภาระหนี้คงค้างและวงเงินอนุมัติการให้สินเชื่อในเครื่องคอมพิวเตอร์ เพื่อแสดงผลเป็นเท็จหลอกลวงผู้บริหารให้หลงเชื่ออนุมัติให้ไถ่ถอนเงินฝากที่อายัดเป็นประกัน และอนุมัติให้กู้เงินเพิ่มเติมอีกจำนวนหลายรายการ และภายหลังได้แก้ไขข้อมูลในเครื่องคอมพิวเตอร์กลับคืนเพื่อให้ภาระหนี้ตรงกับข้อเท็จจริง แต่ไม่มีหลักประกัน เนื่องจากได้รับอนุมัติให้ไถ่ถอนไปแล้ว
การทุจริต	:	กรณีที่ 3 ปลอมแปลงลายมือชื่อของลูกค้าเพื่อเปิดบัญชีเงินฝากประจำในนามของลูกค้าคนหนึ่ง และพิมพ์ยอดเงินฝากในสมุดคู่ฝากเป็นเท็จ เพื่อนำมาเป็นประกันการให้สินเชื่อประเภทเงินให้กู้ทั่วไปในนามของลูกค้าที่เกี่ยวข้องวงเงิน 20 ล้านบาท แล้วนำเงินออกไปใช้ประโยชน์ส่วนตัว



รายการที่ทำการทุจริตในกรณีต่าง ๆ

วิธีการปรุงแต่งข้อมูล	รายจ่ายแก่พนักงานและผู้อื่น	การควบคุมสินค้าคงคลังและการเบิกเงินชดเชย	การเก็บเงินการนำฝาก	อื่น ๆ
เพิ่มรายการหรือแก้ไขรายการ	40	44	17	0
ลบรายการ	2	3	2	0
แก้ไขรายการที่เก็บไว้ในแหล่ง-เก็บข้อมูล	6	3	1	2
แก้ไขคำสั่ง (Program)	2	7	5	0
การปฏิบัติการที่ไม่เหมาะสม	4	1	0	0
อื่น ๆ	2	11	2	2
	56	69	27	4

การจำแนกวิธีการปรุงแต่งข้อมูลแยกตามลักษณะกิจการ จะเป็นดังนี้

วิธีการปรุงแต่งข้อมูล	บริษัททั่วไป	สถาบันการเงิน	องค์การของรัฐ	ภาครัฐบาล
เพิ่มรายการ	16	9	9	48
แก้ไขรายการ	8	12	0	
ลบรายการ	3	4	0	0
แก้ไขรายการที่เก็บไว้ในแหล่ง-เก็บข้อมูล	5	3	5	0
แก้ไขคำสั่ง	6	8	0	0
การปฏิบัติการที่ไม่เหมาะสม	4	0	1	0
อื่น ๆ	4	1	1	11
	46	37	16	59

การแก้ไขคำสั่ง (program) โดยไม่มีอำนาจ

วิธีการที่ผู้จะกระทำการทุจริตจากการแก้ไขคำสั่ง มีดังนี้

- การกระจายยอด (Breakage)
- กำหนดรหัสสำหรับรายการที่ไม่มีเอกสาร
- ปรุงแต่งยอดคงเหลือ
- จงใจให้ผ่านรายการผิด
- ดัดแปลงแหล่งเก็บข้อมูล
- ทำให้การคุมยอดไร้ผล (Fudging control totals)

การคำนวณรายการต่าง ๆ โดยใช้คอมพิวเตอร์ที่ทำให้การแก้ไขคำสั่งสามารถใช้เป็นวิธีการทุจริตที่ได้ผล มักได้แก่รายการต่อไปนี้

- ค่าบริการที่เกิดจากการใช้ทรัพย์สินหรือบริการ
- ส่วนลดต่าง ๆ
- ค่าแรง
- รางวัลการขาย
- ผลประโยชน์เมื่อออกจากงาน
- ดอกเบี้ยบัญชีเงินฝากสะสมหรือเงินฝากประจำ
- เงินสวัสดิการ ค่ารักษาพยาบาล



บทที่ 12

ผู้เสียหายจากการทุจริต และการเปิดเผยการทุจริตด้านคอมพิวเตอร์ ซึ่งเป็นเรื่องที่ควรทำ โดยผู้บริหาร

ผู้เสียหายจากการทุจริต และการเปิดเผยการทุจริตด้านคอมพิวเตอร์ซึ่งเป็นเรื่องที่ควรทำโดยผู้บริหาร

ผู้เสียหายจากการทุจริต

30% เป็นบริษัทการเงินและบริษัทประกันภัย
มากกว่า 20% เป็นกิจการประเภทขายส่งและโรงงาน
22% เป็นกิจการประเภทขายปลีก
13% เป็นกิจการที่ให้บริการ หรือกิจการสาธารณูปโภค

สิ่งเหล่านี้แสดงให้เห็นว่า การฉ้อฉลทางด้านคอมพิวเตอร์สามารถที่จะเกิดขึ้นได้กับทุกองค์การค้า
- มีจุดอ่อนในการควบคุมเกิดขึ้นในระบบคอมพิวเตอร์
- จุดอ่อนมักเกิดจากตัวพนักงาน หรือบุคคลภายนอก ผู้พยายามที่จะเข้าถึงระบบ

คอมพิวเตอร์กับการทุจริต

วิธีการ

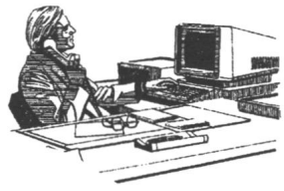
ที่นิยมใช้กันคือ การปลอมแปลงเอกสารขั้นตอนที่ใช้ในการประมวลผล

ผู้กระทำผิด

ส่วนใหญ่เป็นพวกเสมียน (Clerical personnel)

วิธีการตรวจพบ

- ลูกค้าร้องเรียน
- ลูกค้าสอบถาม
- พบโดยบังเอิญ
- ได้รับการบอกเล่า
- พบโดยระบบการควบคุมที่มีอยู่
- การตรวจสอบตามปกติ (พบมากที่สุด) ในธุรกิจการธนาคาร การร้องเรียนของลูกค้าทำให้ค้นพบการทุจริตมากที่สุด



ผู้ค้นพบการทุจริต

- ผู้บริหารระดับกลาง
- ผู้ตรวจสอบภายใน
- ลูกค้า
- ผู้สอบบัญชีภายนอก
- พนักงานคนอื่น ๆ

ปรากฏว่าแหล่งที่ค้นพบการทุจริตที่ใหญ่ที่สุดคือ จากพนักงานอื่น ๆ (other employers)

คอมพิวเตอร์กับการทุจริต

การลงโทษผู้กระทำผิด

- ผู้กระทำผิดมักจะไม่ถูกลงโทษ เนื่องจากขาดหลักฐานที่เพียงพอ
- ผู้กระทำผิดส่วนใหญ่มักจะถูกภาคทัณฑ์ เนื่องจากเป็นความผิดครั้งแรก

สิ่งที่จะตามมาในอนาคต

- การทุจริตโดยใช้คอมพิวเตอร์ หรือเกี่ยวกับคอมพิวเตอร์จะมีมากขึ้น
- จะมีองค์กรผู้เสียหายมากขึ้น
- ทนายความและการพิพากษาคดีคอมพิวเตอร์จะมีปัญหาในการสืบคดี และการพิจารณามาก

สิ่งที่ควรดำเนินการ

- ผู้ตรวจสอบภายในด้านคอมพิวเตอร์จะต้องมีบทบาทมากขึ้น ในด้านการป้องกันการทุจริต และจะต้องเพิ่มขึ้นอย่างเร่งด่วน
- การแลกเปลี่ยนทักษะระหว่างหน่วยงานในศูนย์คอมพิวเตอร์เป็นสิ่งจำเป็น
- บริษัทขนาดเล็กหรือที่ใช้เครื่องคอมพิวเตอร์ขนาดเล็กควรจะระมัดระวังเป็นพิเศษ

คอมพิวเตอร์กับการทุจริต

การป้องกันการทุจริต

1. ความเอาใจใส่และความเข้าใจระบบงาน การประมวลข้อมูลด้วยคอมพิวเตอร์
2. การเข้าใจระบบงานขององค์การอย่างแท้จริงของผู้วิเคราะห์ และผู้พัฒนาระบบงาน (ดูสาเหตุการทุจริต พิจารณาถึงโอกาสที่จะทุจริตได้)
3. การควบคุมและการตรวจสอบที่มีประสิทธิภาพ (หากป้องกันไม่ได้ องค์กรควรทราบถึงสิ่งผิดปกติเร็วที่สุด)
4. ผู้ใช้ข้อมูลที่เอาใจใส่ในข้อมูลที่เกี่ยวข้อง

เรื่อง การเปิดเผยการทุจริตด้านคอมพิวเตอร์ ซึ่งเป็นการตัดสินใจที่ถูกต้องของผู้บริหาร

The right way to treat computer crime

ในวันที่ 5 มิถุนายน 1980 บริษัท Leds and Northrup ใน Pennsyllvama ได้ไล่พนักงานของเขา คือ Joseph Harshman ซึ่งเป็น Computer project leaders/programmer ออก และแทบจะทันทีทันใดก็ได้ล้างโปรแกรม Pacavoids ของ Harshman ออกจาก File แต่กลับต้องประหลาดใจเมื่อพบว่าข้อมูลที่เกี่ยวกับ Move 1 ขึ้นเป็น computer control program ถูกล้างออกหมด จากการสอบสวนจึงพบว่า Harshman ได้ฉวยโอกาสขณะที่เขายังมี Password อยู่ในการ Access ข้อมูล และทำลายข้อมูลเสีย แต่ขณะที่ได้รับคำบอกกล่าวให้ออก บริษัท Leds and Northrup ได้ตัดสินใจต่างกับแห่งอื่น ๆ ที่ถูกทุจริตในด้านนี้ คือ เขายอมเปิดเผยความจริงโดยฟ้อง Harshman ในศาล Montgomery ด้วยเหตุผล 2 ประการ คือ เพื่ออาศัยขบวนการทางกฎหมายให้ทราบว่าข้อมูลอื่นอย่างไรบ้างที่ถูกทำลายไป และเพื่อการข่มขู่พนักงานอีกที่อาจจะคิดทำเช่นนี้

จากเหตุการณ์นี้บ่งเห็นว่าในการปฏิบัติต่อการทุจริต เพื่อความแน่นอนในการสอบสวนต้องระมัดระวังการเปิดเผยและการลงโทษไว้ด้วยตามกรณีนี้ควรเป็นอุทาหรณ์ได้ว่าเขาควรจะได้ล้าง Password ของ Harshman ทันที และก่อนจะบอกให้เขาทราบถึงการไล่ออก

นาย Daoid Reginald Allan อายุ 45 ปี พนักงานธนาคารผู้หนึ่ง ซึ่งมีประวัติการทำงานที่ไม่ด่างพล้อยมาเป็นเวลากว่า 30 ปี ลูกลงโทษในเดือนมีนาคมนี้โดยศาล Birmingham Crown Court ในข้อหาฉ้อโกงนายจ้าง (National Weatminoter Bank Limited) เกินกว่า $7,000 นาย Allan ถูกลงโทษในความผิดรวม 7 กระทง ทั้งกรณีขโมย และตกแต่งบัญชีโดยถูกกล่าวหาว่าได้กระทำความผิดตั้งแต่ปี 1972 จนถึงปี 1979 เมื่อถูกจับอัยการได้บรรยายว่าจำเลยได้เปิดบัญชีปลอม ซึ่งเขายอมให้มีการเบิกเกินบัญชีได้เสร็จแล้วเอาเงินออกไปและทำการหมุนยอดหนี้ระหว่างงวดบัญชีต่าง ๆ และกับบัญชีต่าง ๆ

นาย Allan ถูกลงโทษจำคุก 2 ปี และให้ใช้เงิน $7,150 ซึ่งอาจถือว่าเป็นเพราะการโชคร้ายเนื่องจากการมีนักโทษมากจนคุกแน่น จึงมีแนวโน้มไม่ให้ศาลลงโทษจำคุกสำหรับนักโทษที่ไม่ได้คดีรุนแรง

ต้องมองถึงความสมดุลของความเสี่ยงในการทำอาชญากรรมทางคอมพิวเตอร์เทียบกับผลที่จะเกิดขึ้น ประการแรกผู้ทุจริตจะสามารถเลือกได้ว่าจะทำเมื่อไร และอย่างไร ซึ่งนับว่าได้เปรียบมาก และโอกาสถูกจับก็น้อย และถ้าถูกจับได้บริษัทก็มักไม่ให้ข้อเท็จจริงในการสอบสวน และทางบริษัทจะให้ข้อเท็จจริงก็ยังมีโอกาสอีกเกินกว่า 50% ที่จะพ้นผิด และถึงแม้จะถูกลงโทษก็ยังนับว่ามีโอกาสที่น้อยมากจริง ๆ ที่จะถูกจำคุกจากผลได้ผลเสียดูจะเป็นสิ่งที่น่าชักจูงใจให้เกิดการกระทำผิด จึงอาจคาดได้ว่าอาชญากรรมที่ไม่มีความรุนแรงไม่มีการทำลายเช่นนี้จะเป็นอาชญากรรมในอนาคต โดยเฉพาะเมื่อเทียบกับภาวะความลำบากทางเศรษฐกิจและเงินเฟ้อเช่นนี้

เรื่อง OASINO EXTORTION CASE

เรื่องปรากฏว่ามีคน 2 คนเข้าไปในโรงแรม Haroeys Hotel and Casino โดยบอกว่าเป็นผู้ชำนาญทางคอมพิวเตอร์ พร้อมกับถือกล่องที่ไม่มีใครเข้าใจว่าเป็นกล่องอะไรโดยอ้างว่าเป็นอุปกรณ์คอมพิวเตอร์ จากนั้นเจ้าของโรงแรมก็ได้รับคำขู่ว่าให้แลกเงิน $3,000,000 กับการระเบิดโรงแรม ซึ่งผลที่สุดผู้ชำนาญการทางระเบิดและ FBI ก็แก้ไขไม่ได้เกิดการระเบิดเสียหายมากมาย

แม้จะเป็นข่าวธรรมดาแต่เป็นข้อเตือนว่ามันไม่เป็นข้อเท็จจริงหรือที่ใครคนหนึ่งที่ถือกระเป๋าที่มีตรา IBM, ICL, Honeyoell หรือไปรษณีย์ มักจะสามารถเดินผ่านด้านรักษาความปลอดภัยได้โดยง่ายดาย ซึ่งนั่นหมายความว่าเมื่อมีการเชื่อเครื่องแบบ ระบบควบคุมที่แสนดีก็บอกได้เพียงว่าเมื่อไรบุรุษไปรษณีย์หรือพนักงานเหล่านั้นมา

เรื่อง DUMP BANKS

นาย Muir เป็น Transport Contractor (ผู้รับจ้างขนส่ง) อายุ 31 ปี ถูกลงโทษในคดีฉ้อโกง 8 กระทง และอาชญากรรมอื่นอีก 64 กระทง โดยเหยื่อของเขาล้วนเป็นกิจการใหญ่ เช่น National Westnenster Bank, Barclays Bank, Midland Bank และ Yorkshire Bank

จุดอ่อนก็คือ Muir ได้รับเช็คเล่มใหม่ของบัญชีของบุคคลอื่นได้โดยง่าย ๆ เพียงแต่บอกเลขบัญชีที่ถูกต้อง และขอรับสมุดเช็ด หลังจากนั้นเขาก็รีบจ่ายเงิน (ถอน) กว่า 10,000 จากบัญชีนั้นก่อนที่คอมพิวเตอร์ของธนาคารจะจับเขาได้

ศาล Hewitt กล่าวว่า "นี้คือสัญญาณเตือนว่าระบบของธนาคารขาดประสิทธิภาพ"



บทที่ 13

การรักษาความปลอดภัยของระบบบริหารข้อมูลหรือโปรแกรมควบคุมระบบงาน

การรักษาความปลอดภัยของระบบบริหารข้อมูล หรือโปรแกรมควบคุมระบบงาน (OPERATING SYSTEM SECURITY)

คำนำ

ระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์ได้รับการพัฒนาเป็นลำดับ อาทิเช่น มีการแบ่งเวลาใช้งานสำหรับเครื่องคอมพิวเตอร์ขนาดใหญ่ให้กับผู้ใช้งานหลาย ๆ คน (Single Computer Time Sharing System) มีการนำระบบ Remote Access มาใช้งาน เป็นต้น นอกจากนี้คอมพิวเตอร์ยังถูกนำไปใช้ปฏิบัติงานในด้านการติดต่อธุรกิจที่มีความเสี่ยงภัยสูง เช่น การโอนเงินโดยระบบอิเล็กทรอนิกส์ หรือแม้แต่การควบคุมหอบังคับการเครื่องบิน ณ ท่าอากาศยานต่าง ๆ ก็จำเป็นต้องอาศัยการสื่อสารโดยระบบคอมพิวเตอร์ที่มีประสิทธิภาพควบคู่ไปกับการประมวลผลแบบ Microprocessor นอกจากนี้ ยังช่วยในการทำงานด้านอื่นพร้อมกันไป จึงจำเป็นอย่างยิ่งที่จะต้องมีการรักษาความปลอดภัยในการสื่อข้อมูลโดยระบบต่าง ๆ เหล่านี้อย่างรัดกุม ในบทนี้จะได้กล่าวถึงการรักษาความปลอดภัยของโปรแกรมควบคุมระบบงาน (Operating System) และการป้องกันความเสียหายอันจะเกิดขึ้นกับ Hardware

การรักษาความปลอดภัยที่ดีควรครอบคลุมไปทุกด้าน โดยเฉพาะโปรแกรมควบคุมระบบงาน (Operating System) ทั้งนี้เพราะระบบคอมพิวเตอร์ในปัจจุบันมีการติดต่อแลกเปลี่ยนข้อมูลกันได้โดยผ่านเครื่องมือสื่อสารซึ่งส่วนมากนิยมใช้โทรศัพท์ การรักษาความปลอดภัยทางกายภาพที่เคยปฏิบัติในอดีตไม่เพียงพอที่จะคุ้มครอง โดยเฉพาะเมื่อมีการใช้ Remote terminal ด้วย อย่างไรก็ดี ระดับของความปลอดภัยในแต่ละระบบงานจะแตกต่างกันไป บางครั้ง ข้อมูลที่รั่วไหลอาจจะไม่มีความสำคัญต่อผู้พบเห็น แต่กลับถือเป็นเรื่องเสื่อมเสียสำหรับผู้บริหารที่รับผิดชอบได้

นอกจากการรักษาความปลอดภัยของโปรแกรมควบคุมระบบงานแล้ว ยังมีด้านอื่นที่ควรให้ความสำคัญ คือ การรักษาความปลอดภัยภายนอก (External Security) ที่จะกล่าวถึงต่อไป และการรักษาความปลอดภัยภายใน (Internal security) ซึ่งเกี่ยวข้องกับการควบคุมต่าง ๆ ภายใน Hardware และ Operating system เพื่อให้การทำงานเป็นที่เชื่อถือได้และต่อเนื่องไม่หยุดชะงัก

การรักษาความปลอดภัยภายนอก (External Security)

ความปลอดภัยภายนอกเป็นความปลอดภัยทางกายภาพ การป้องกันภัยพิบัติและการรุกล้ำโดยบุคคลภายนอกเป็นสิ่งที่จำเป็น ซึ่งกระทำได้ด้วยวิธีการต่าง ๆ ได้แก่ ใช้เครื่องจับควัน (Smoke detector) เครื่องตรวจจับระดับความร้อน การติดตั้งอุปกรณ์ในการตรวจสอบรูปพรรณหรือหลักฐาน (Identification control) ของผู้มีสิทธิเข้าในเขตหวงห้ามภายในห้องคอมพิวเตอร์ เช่น บัตรผ่านพร้อมรูปถ่ายและลายเซ็น หรือการตรวจสอบลายนิ้วมือ เป็นต้น

การรักษาความปลอดภัยในการปฏิบัติงาน (Operational Security)

ผู้บริหารองค์กรมีหน้าที่วางนโยบายและระเบียบข้อบังคับเพื่อรักษาความปลอดภัยในด้านการปฏิบัติงาน โดยกำหนดว่าบุคคลใดมีสิทธิใช้เครื่องคอมพิวเตอร์ภายในขอบเขตอย่างไร ทั้งนี้โดยพิจารณาว่า ข้อมูลใดไม่พึงเปิดเผยกับเจ้าหน้าที่ระดับใดและบุคคลใดสามารถเก็บความลับไว้ได้ ควรยึดถือหลักการในการแบ่งแยกหน้าที่ (Division of responsibilities) โดยให้แต่ละคนปฏิบัติหน้าที่ต่าง ๆ กัน ไม่จำเป็นต้องรู้งานทั้งระบบ และพยายามให้เกิดความร่วมมือกันในพนักงานทุกฝ่ายด้วย ดังตัวอย่างเช่น Operators มีสิทธิที่จะเข้าไปในห้องเครื่องได้ Programmers เป็นผู้เขียนโปรแกรม แต่ทั้ง Operators และ Programmers ไม่จำเป็นต้องรู้งานซึ่งกันและกัน การป้อนข้อมูลเข้าควรที่จะได้รับการตรวจสอบโดยชุดทำงานคณะหนึ่ง โดยมีอีกคณะหนึ่งเป็นผู้ตรวจทานงาน Output เป็นต้น

การควบคุมการรักษาความปลอดภัย (Surveillance)

การควบคุมการรักษาความปลอดภัย ได้แก่การควบคุมด้วยอุปกรณ์ การว่ากล่าวตักเตือน การตรวจสอบตลอดจนการอนุมัติผู้มีสิทธิใช้เครื่อง แต่บางครั้งการควบคุมด้วยอุปกรณ์รักษาความปลอดภัยอาจไม่ได้ผลนัก เช่น การใช้ระบบบันทึกเสียงผู้มีสิทธิเข้าในห้องคอมพิวเตอร์ ถ้าพนักงานผู้นั้นเป็นหวัดเสียงก็อาจจะเปลี่ยนไป คอมพิวเตอร์จะไม่ยอมให้ประตูเปิด เพราะเสียงปัจจุบันไม่ตรงกับเสียงที่เคยบันทึกไว้

ระบบเตือนภัย (Threat Monitoring)

วิธีรักษาความปลอดภัยอีกวิธีหนึ่ง คือการกำหนดระบบงานที่สามารถควบคุมการปฏิบัติงานได้หลายระดับ เช่น แทนที่จะปล่อยให้ User มีอำนาจควบคุมการทำงานของเครื่องเองในกรณีที่ User ต้องการใช้ File ที่สำคัญ (Critical file) ซึ่งระบบการทำงานของคอมพิวเตอร์บางประเภทจะอนุญาตให้ User เรียก File ทุก File มาใช้งานได้เท่ากับ User กลายเป็นผู้ควบคุมระบบโปรแกรมควบคุมข้อมูล เพราะฉะนั้นจึงมีการคิดค้นวิธีการควบคุมการเข้าถึง File ข้อมูล เรียกว่าระบบเตือนภัย (Threat monitoring) ขึ้นมา

การควบคุมการเก็บ Password (Password Protection)

วิธีการที่จะแสดงตัวต่อการควบคุมโดยคอมพิวเตอร์แบ่งออกเป็น 3 ประเภท คือ

1) ใช้ลักษณะส่วนบุคคล เช่น ลายนิ้วมือ เสียง รูปร่างหน้าตา และลายมือชื่อ เป็นต้น
2) ใช้สิ่งที่บุคคลนั้นเป็นเจ้าของ เช่น เหรียญตรา บัตรแสดงตัว และกุญแจ เป็นต้น
3) ใช้สิ่งที่บุคคลนั้นรู้คนเดียว เช่น Password รหัสตู้เซฟ เป็นต้น

การใช้ Password เป็นวิธีการที่นิยมใช้กันโดยทั่วไป ไม่ควรใช้ Password ที่ยาว เพราะจะทำให้ยากแก่การจดจำ ผู้ที่จะเข้าถึงเครื่อง Terminal ได้จะต้องพยายามผ่าน Password ก่อน และการที่จะต้องเดา Password ให้ถูกต้องนั้น ต้องใช้ความพยายามเป็นอย่างมาก เพราะฉะนั้นในโปรแกรมควบคุมระบบงานควรกำหนดจำนวนครั้งของการกด Password และความยาวของ Password ด้วย

อีกวิธีหนึ่งที่สามารถใช้ควบคุม Password ให้รัดกุมยิ่งขึ้น คือการ Encrypt ข้อมูล หมายถึงการสลับที่ข้อความหรือการแทนที่ข้อความด้วยรหัสในการส่งข่าวสารที่เป็นความลับเพื่อมิให้ผู้อื่นเข้าใจความหมาย โดยจะมีเจ้าหน้าที่เพียง 2-3 คนเท่านั้นที่พอจะทราบรหัสและแปลงรหัสกลับเป็นข้อมูลธรรมดาได้ (Decrypt)

นอกจากนี้ ควรกำหนดจำนวนครั้งที่ User สามารถ Key รหัสประจำตัวในขณะที่ Log in ด้วย เพื่อป้องกัน User ฉวยโอกาสลองกดรหัสของผู้อื่น ดังนั้น เมื่อมีผู้พยายามลองกดรหัสของผู้อื่น หรือเมื่อมีผู้พยายามกดรหัสเกินจำนวนครั้งที่กำหนด เครื่องจะหยุดการติดต่อหรือส่งสัญญาณเตือนภัยทันที

การตรวจสอบ (Auditing)

ในการควบคุมการรักษาความปลอดภัยด้วยการตรวจสอบ ผู้ตรวจสอบจะทำการตรวจสอบเพื่อดูว่าจะมีข้อมูลเท็จแอบแฝงอยู่ในระบบงานหรือไม่ รวมทั้งตรวจสอบการประมวลผลข้อมูลในปัจจุบันอีกด้วย

ทะเบียนบันทึกผลการตรวจสอบ (Audit log) ใช้บันทึกเหตุการณ์สำคัญที่เกิดขึ้นในระบบคอมพิวเตอร์ โดยเครื่องจะทำการบันทึกทุกครั้งที่มีการประมวลผลข้อมูล และเก็บรักษาไว้ในที่ปลอดภัยจากการเข้าถึงโดยบุคคลภายนอก อย่างไรก็ดี ทะเบียนบันทึกผลการตรวจสอบแต่เพียงอย่างเดียวไม่สามารถประกันระบบรักษาความปลอดภัยที่ดีได้ จำเป็นจะต้องมีการตรวจสอบติดตามผลอยู่เสมอ ซึ่งบางครั้งอาจใช้วิธีการตรวจสอบแบบสุ่มตัวอย่างเพื่อพิจารณาสิ่งผิดปกติที่อาจเกิดขึ้นด้วย

การป้องกันบุคคลที่ไม่เกี่ยวข้องมาใช้เครื่อง (Access Controls)

การรักษาความปลอดภัยที่สำคัญ คือการป้องกันบุคคลที่ไม่เกี่ยวข้องเข้าถึงข้อมูลที่เก็บไว้ โดยการอ่าน (Read access) การเขียน (Write access) และการทำงานตามคำสั่ง (Execute access) สิ่งเหล่านี้ควบคุมได้โดยใช้ Access control matrix แบบ 2 มิติ (Two-dimensional matrix) ซึ่งจะบันทึกหัวข้อระบบงานและวัตถุประสงค์ของการทำงานในแต่ละครั้งไว้เป็นหลักฐาน

สิ่งที่ควรระลึกถึงเกี่ยวกับการรักษาความปลอดภัย (Security Kernels)

ถ้ามีการสร้างระบบรักษาความปลอดภัยไว้ในตัวเครื่องตั้งแต่แรกเริ่มแล้ว จะทำให้การควบคุมการรักษาความปลอดภัยรัดกุมยิ่งขึ้น ดังนั้น ทุกครั้งที่มีการพัฒนาระบบ ควรเน้นในด้านการรักษาความปลอดภัยเป็นสำคัญด้วย

การรักษาความปลอดภัยของโปรแกรมควบคุมระบบงาน ขึ้นอยู่กับการควบคุมดูแลการทำงานของ Access control logging รวมทั้งการติดตามผลการบริหารหน่วยข้อมูลใน Real storage, Virtual storage ตลอดจนการจัดระบบการทำงานของ File แต่ทุกวันนี้ได้มีการพัฒนาโครงสร้างของระบบโดยพยายามที่จะจำกัดขอบเขตความสำคัญของการทำงานให้น้อยลง

การรักษาความปลอดภัยของเครื่อง (Hardware Security)

ในขณะที่ Hardware มีราคาลดลงตามขนาดของตัวเครื่องที่ถูกสร้างให้กะทัดรัดขึ้นนั้น ได้มีการพัฒนาระบบการรักษาความปลอดภัยของเครื่องควบคู่กันไปกับการทำงานและสถาปัตยกรรม ซึ่งสามารถควบคุมการทำงานในโปรแกรมต่าง ๆ ช่วยให้การทำงานเร็วและมีประสิทธิภาพมากขึ้น สามารถติดตามผลได้ตลอดเวลา

ระบบการทำงานด้วยตัวเอง (Survival Systems)

การทำงานด้วยตัวเองในระบบคอมพิวเตอร์ คือการที่เครื่องทำการประมวลผลต่อไปเรื่อย ๆ ในขณะที่ส่วนประกอบบางส่วนไม่ทำงาน ในระบบ On-line การทำงานด้วยตัวเองนี้เป็นสิ่งจำเป็น เช่น ในบริษัทการบินที่ไม่มีระบบการทำงานด้วยตัวเอง ทุกอย่างจะหยุดชะงักถ้าคอมพิวเตอร์ไม่สามารถปฏิบัติงานได้ เนื่องจากไม่มีหลักฐานยืนยันในการสำรองที่นั่งและหลักฐานในการซื้อบัตรผู้โดยสาร เป็นต้น การที่มีระบบการทำงานด้วยตัวเองจะช่วยให้การทำงานไม่หยุดชะงัก เพราะเมื่อเครื่องที่ทำการประมวลผลแบบ On-line หยุดอย่างกะทันหัน อีกเครื่องจะสามารถประมวลผลข้อมูลต่อไปได้ หรือสามารถทำงานในระบบ Off-line เสมือนเป็นเครื่องสำรอง อันเป็นสาเหตุหนึ่งที่ทำให้มีการ Pool เกิดขึ้น เพื่อช่วยในการทำงาน

ในปัจจุบันมีการออกแบบ Microprocessor ให้มี Fail-safe ไปในตัว โดยจัดทำทางเดินสำหรับนำสัญญาณไฟฟ้าให้ไหลผ่านจากจุดหนึ่งไปยังอีกจุดหนึ่งไว้ด้วย เพื่อช่วยการทำงานในระบบ Multiprocessing ซึ่งจะต้องอาศัยระบบการทำงานด้วยตัวเองดังกล่าวประกอบกันไป สำหรับลักษณะการทำงานด้วยตัวเองนี้ สรุปได้คือ

- รวบรวมกลไกของ Fail-safe ไว้ในการทำงานของ Hardware มากกว่า Software
- ใช้ Transparent multiprocessing ช่วยให้การทำงานปรับตัวเองโดยไม่ต้องเปลี่ยนตัว Software
- ใช้ระบบย่อย T/O หลายแบบ
- รวบรวมระบบการทำงานไว้ใน Hardware
- รวบรวมกลไกในการตรวจสอบความผิดของระบบ Hardware-software

Capability and Object-Oriented Systems

ระบบการทำงานแบบ Capabilities and object-oriented system กำลังเป็นที่สนใจของ System engineer เพราะเป็นส่วนที่คอยเช็คสอบการรักษาความปลอดภัยของระบบคอมพิวเตอร์

ในที่นี้การทำงานของ Access right จะช่วยให้ Subject ทำงานประสานกับ Object ตามขั้นตอนโปรแกรมที่เขียนไว้ Object คืออุปกรณ์ขั้นพื้นฐานที่สร้างขึ้นมาเพื่อให้ระบบทำงานควบคู่กันไป ประกอบด้วย Files, Programmes, Directories, Terminals, Channels controllers devices, Disk tracks และ Primary storage block เป็นต้น Subject ประกอบด้วย Jobs หรือ Applications คืองานชิ้นหนึ่งที่เครื่องคอมพิวเตอร์ทำการประมวลผลครั้งหนึ่งหรือหลายครั้ง Process คือกระบวนการทำงานของเครื่องคอมพิวเตอร์ และ Procedure คือส่วนของโปรแกรมซึ่งมีคำสั่งเป็นขั้นตอนในการแก้ปัญหาต่าง ๆ และถูกเรียกใช้โดยโปรแกรมหลักหรือส่วนของโปรแกรมอื่น

ในขณะที่ Subject และ Object ทำงานประสานกัน ก็จะทำให้เกิดระบบงานขึ้นใหม่ขึ้นเรื่อย ๆ Capability คือการที่มีสัญญาณหลาย ๆ สัญญาณและมีลักษณะการทำงานไม่ขึ้นกับ Host หรือ Mastercomputer โดยส่งสัญญาณพร้อม ๆ กันบนช่องสื่อสารเพียงช่องเดียว

Capability เป็นตัวสื่อในการทำงานระหว่าง Subject กับ Object ในขณะเดียวกัน ส่วนที่ทำหน้าที่ของ Protection domain จะกำหนดขอบเขตการเข้าถึงข้อมูลว่า Subject เดียวอาจจะเข้าถึงส่วนของ Object ได้หลายจุด โดยมี Capabilities เป็นสื่อในการที่ Subject ต้องการติดต่อกับ Object ตัวใดเป็นพิเศษ จำต้องสั่งให้ Capability ทำงาน

หลักใหญ่ของการป้องกันคือ ให้มีการเข้าถึงเฉพาะผู้มีสิทธิเท่านั้น ปัญหาหลักที่สำคัญก็คือ จะเกิดอะไรขึ้น ถ้า Capabilities ตัวสุดท้ายถูกลบทิ้งไป การที่จะนำสิ่งที่ถูกลบทิ้งให้เข้าสู่สภาพเดิมนั้นจะยากลำบากมาก ดังนั้น Capabilitis ควรมีการทำสำเนาทุกครั้ง

Movement and Storage Capabilities

การควบคุมการทำสำเนาและความเคลื่อนไหวของ Capabilities เป็นงานค่อนข้างยาก ระบบการทำงานโดยทั่วไปนั้น Users ไม่สามารถบังคับทำงานของ Capabilities ได้โดยตรง แต่เป็นหน้าที่ของ Operating Systems ที่ทำหน้าที่บังคับการทำงานแทน Users หน้าที่ที่สำคัญของ O/S คือเป็นผู้ติดตามความเคลื่อนไหวของ Capabilities เป็นการยากที่ O/S พยายามควบคุมการเคลื่อนไหวของตัว Capabilities ในระบบการประมวลผลข้อมูลแบบ Multiprocessing จึงจำเป็นต้องมีโครงสร้างของ Directory ที่ทำหน้าที่ควบคุมการทำงานของ Capabilities ทั้งระบบ

Revocation of Capabilities

การนำ Capabilities กลับมาใช้งาน บางครั้ง User มีความจำเป็นที่จะเอา Capabilities กลับมาใช้งานอีก ถ้า Directory ของระบบงานทำหน้าที่ควบคุม Capabilities การนำ Capabilities มาใช้งานก็จะทำได้ง่ายขึ้น

เทคนิคในการเลือกตัว Capabilities ที่ต้องการเพื่อนำกลับมาใช้งานอีกนั้นคือการสร้าง Primary Capability จาก Object Primary Capability แล้วจึงเลือก Capability ตัวที่ต้องการมาใช้งาน และตัว Capabilities ที่ใช้งานสำหรับ I/O Device อาจต้องมีการปรับตัวต่าง ๆ กันไป แล้วแต่ประเภทของ Device ตัวอย่างเช่น Capability สำหรับ Tape Drive Object อาจจะต้อง Rewind ในขณะที่ตัว Capability ของ Card Reader ไม่ต้องทำอะไรเลย



Case Study : The Object-Oriented Architecture of the IBM System/38

การทำงานของ IBM System/38 จะอยู่ภายใต้การควบคุมของโปรแกรมระบบงาน (O/S) ชื่อ Control Program Facility (CPF) โครงสร้างของ IBM System/38 ประกอบด้วย Object-Oriented หน่วยข้อมูลที่สำคัญ Uniformly Addressable และหน่วยเก็บข้อมูลขนาดใหญ่ Object ต่าง ๆ ของระบบงานเป็น Storage Resident และ System Storage ถูกจัดโดย Device-Independent ซึ่งมีกลไกในการรวม File และตรวจสอบรหัส นอกจากนี้ System/38 ยังสามารถออกคำสั่งควบคุมการทำงานของ Object โดยตรง โดยมี CPF (Control Program Facility) เป็นตัวประสานงานใน Object-Oriented ระบบงานทำหน้าที่เกี่ยวกับการอนุมัติ (Authorization) การเคลื่อนไหว (Moving) การเปลี่ยนชื่อ (File Renaming) การ Dump ข้อมูล การ Lock เครื่อง การ Save ข้อมูล และการสร้างข้อมูลขึ้นมาใหม่ (Restore) ดังจะอธิบายในลำดับต่อไป ดังนี้

เมื่อตัว Object ถูกสร้างขึ้น โปรแกรม CPF จะตั้งชื่อ Object ลงในเครื่องเรียกว่า Context ซึ่ง Users เห็นจากจอภาพในรูปของ Libraries หรือ Catalog ของ Object

โปรแกรม CPF ใช้ Machine Object เพื่อสร้าง User-Oriented Object เรียก Database file โดยโปรแกรม CPF จะรวม Data Space Index Cursor และ Space ใน Database File นอกจากนี้ยังมี Higher-Level Object ที่สร้างจาก Machine Object เรียก Composite Object แต่ละตัวประกอบด้วยโปรแกรมประกอบงานและ Space ที่สัมพันธ์กัน แต่ Space Object ไม่มีโปรแกรมประกอบงาน เนื่องจากเป็นโปรแกรมที่ทำหน้าที่จัดหาหน่วยเก็บข้อมูลให้เข้ากับ Buffers, Pointers Control Blocks และข้อมูลอื่น ๆ

System/38 มีตัว Capability-Based เคลื่อนที่ผ่านระบบ System Pointer ที่ชี้แหล่งของ Object และขอบเขตของการเข้าถึงข้อมูล System Pointer นี้จะรับคำสั่งจากโปรแกรมควบคุมระบบ System/38 เท่านั้น User ไม่มีสิทธิเข้าถึงโดยตรง นอกจากนี้ยังมี Unresolved System Pointer ที่ทำหน้าที่ระบุชื่อ Object ก่อนการหาแหล่งของข้อมูล (Location) เรียก Resolved

เครื่องมีระบบรักษาความปลอดภัยของข้อมูลโดยทำการตรวจสอบผู้มีสิทธิเข้าถึงข้อมูล ถ้ามีการพยายามใช้เครื่องโดยผู้ไม่มีสิทธิ เครื่องจะไม่รับติดต่อสื่อสารด้วย System/38 จะรวมข้อมูลเข้าไว้ใน Object Access Mechanism เพื่อป้องกันการเข้าถึงข้อมูลจากหลายงานพร้อมกัน กล่าวคือ เมื่อโปรแกรมหนึ่งทำหน้าที่เขียน อีกโปรแกรมจะเริ่มทำการอ่านส่วนโปรแกรมอื่นก็จะทำการ Process ต่อไป

สำหรับผู้ที่ได้รับมอบหมายหน้าที่เป็น Security Administrator จะมีสิทธิเข้าถึง Object ในระบบงานทั้งหมด IBM ได้เตรียมมาตรฐานของ User ไว้ในโปรแกรม CPF โครงสร้างสำหรับ Security Administrator นั้นครอบคลุมถึงการอนุมัติเข้าถึง Object ทั้งหมด ซึ่งรวมทั้งการอนุมัติการสร้าง Profile ใหม่ และการปรับปรุงโครงสร้างของเก่าที่มีอยู่แล้ว

การสื่อข้อมูลด้วยรหัส (Cryptography)

แต่เดิมนั้นการใช้รหัสเป็นที่นิยมใช้ในหมู่ทหารในการสื่อสาร มาจนถึงปัจจุบันนี้การสื่อข้อมูลด้วยรหัสเป็นปัจจัยสำคัญในการประมวลผลด้วยระบบคอมพิวเตอร์และการโอนเงินโดยระบบคอมพิวเตอร์ได้เจริญก้าวหน้าขึ้นอย่างรวดเร็ว การสื่อข้อมูลด้วยรหัส คือการใช้คำสั่งที่บุคคลภายนอกไม่สามารถล่วงรู้ได้

ในการส่งข้อมูลด้วยรหัสนี้ เกี่ยวข้องกับ 3 เรื่อง คือ

1) Privacy Problem
2) Authentication Problem
3) The Problem of Dispute

Privacy Problem เป็นการป้องกันบุคคลภายนอกลับลอบเก็บข้อมูลจากข่ายสื่อสาร Authentication Problem เป็นการป้องกันการใส่ข้อมูลผิด และ Problem of dispute เป็นการยืนยันข้อมูลที่ผู้รับได้รับให้ตรงกับข้อมูลที่ส่งมา และปัจจุบันนี้ National Bureau of Standards ได้จัดทำ Data Encryption Standard (DES) ในการส่งข้อมูลลับของทางราชการ

A Cryptographic Privacy System and Cryptanalysis

ในการแปลงรหัสข้อมูลจะกระทำได้เฉพาะผู้ที่ทราบหลักเกณฑ์การแปลงรหัส คือ ผู้ส่งและผู้รับเท่านั้น ซึ่งการแปลงรหัสในระบบคอมพิวเตอร์จะเกี่ยวข้องกับ

1) Sender ผู้ส่งข้อมูล
2) Receiver ผู้รับข้อมูล
3) Plaintext ข้อมูลที่ส่งเป็นข้อมูลธรรมดา
4) Ciphertext or Cryptogram ข้อความที่มีการสลับที่หรือมีการแทนที่ด้วยรหัส ในกรณีส่งข่าวสารที่เป็นความลับซึ่งไม่ต้องการให้ผู้อื่นเข้าใจความหมาย
5) Eavesdropper ผู้ลักลอบต่อสายดักสัญญาณข้อมูล

ซึ่งในเรื่องนี้มักจะไม่มีการตรวจสอบคู่สายว่าถูกดักสัญญาณหรือไม่ เมื่อ Sender ส่งข้อมูลในรูปของ Plaintext ไปยัง Receiver โดยผ่านหน่วยที่แปลงข้อมูลเพื่อให้เป็น Ciphertext ก่อนส่งถึงผู้รับ กรณีมีผู้ลักลอบต่อสายดักสัญญาณข้อมูลจะไม่สามารถล่วงรู้รหัสได้ นอกจากเป็นบุคคลที่เกี่ยวข้องกับการส่งข้อมูล การใช้ระบบแปลงรหัสลับในการส่งข้อมูลเป็นระบบการรักษาความปลอดภัยในการส่งข้อมูลที่สำคัญ

Public Key Systems

เพื่อความปลอดภัยในการส่งข้อมูลผ่านข่ายสื่อสาร จะต้องมีการแปลงรหัส ซึ่งมีระบบการทำงานแยกเป็น 2 Functions คือ การแปลงข้อมูลธรรมดาให้เป็นรหัส และจากรหัสให้เป็นข้อมูลธรรมดา ทั้งนี้รหัสที่ใช้ต้องควบคุมอย่างเข้มงวด ซึ่งบางครั้งก็ไม่รัดกุมเท่าที่ควรหรือไม่ได้ผลตามที่ต้องการ จึงมีการใช้ระบบ Public Key ขึ้น เพื่อขจัดปัญหาการกระจายรหัส ดังกล่าว (Key Distribution)

ในระบบ Key System มี Function ของการแปลงข้อมูล (Encrypering) คือการสลับที่ข้อความหรือการแทนที่ข้อความด้วยรหัส และ Function การถอดรหัสที่เขียนสลับที่กันให้เป็นข้อความที่สามารถอ่านเข้าใจได้นั้น เป็นระบบการทำงานที่แยกจากกัน Key ที่ใช้สำหรับการแปลงข้อมูลเป็นรหัสก่อนการส่ง จะต่างกับ Key ที่ใช้ถอดรหัสให้เป็นข้อมูล โดย Key ที่ใช้สำหรับการแปลงข้อมูลเป็นรหัส ผู้ส่งข้อมูลทุกคนที่เป็น User มีสิทธิส่งข้อมูล Key นี้จึงเรียกว่า Public Key ในขณะที่การถอดรหัสกลับเป็นข้อมูลนั้นจะมี User บางคนที่รับผิดชอบเท่านั้นที่รู้วิธีการถอดรหัส จึงเรียกว่า Private Key จะเห็นได้ว่า Public Key และ Private Key มีหน้าที่ต่างกัน แต่ทำงานสัมพันธ์กัน

Data Encryption Standard (DES)

การแปลงรหัสข้อมูลสามารถทำได้ 2 แบบ คือ

1) แบบ DES (Data Encryption Standard)
2) แบบ RSA (Rivest Shamir and Adleman)

ทั้ง 2 แบบมีลักษณะในการแปลงรหัสข้อมูลต่างกันคือ การแปลงรหัสแบบ DES เป็นแบบ Symmetric กล่าวคือ Key รหัสกลุ่มเดียวสามารถได้ทั้งการ Encrypt และ Decrypt ข้อมูล ส่วนการแปลงรหัสแบบ RSA เป็นแบบ Asymmetric ใช้ Key ต่างกันในการ Encrypt และ Decrypt ข้อมูล

ประโยชน์ของการใช้ระบบ Encryption อย่างแพร่หลายกับ O/S คือช่วยป้องกันการรั่วไหลของ Password list และข้อมูลใน File ทำให้บุคคลภายนอกไม่สามารถใช้งานได้แม้แต่ System Administrator ซึ่งเป็นผู้ที่มีสิทธิเข้าถึงข้อมูลทุกระดับในระบบงาน การแปลงรหัสของแฟ้มข้อมูล (File Encryption) ช่วยให้ User มีความเชื่อมั่นในด้านการรักษาความปลอดภัยของข้อมูลยิ่งขึ้น

เมื่อมีการ Encrypt แล้ว อุปกรณ์สำรองที่ใช้ในการประมวลผล (Back up) เช่น Tapes และ Disks ก็ไม่จำเป็นต้องควบคุมอย่างเข้มงวดต่อไปอีก นอกจากนี้ การสื่อสารโดยใช้ระบบคอมพิวเตอร์ที่มีวิธี Encrypt ข้อมูลใน Link Encryption กล่าวคือ ข่ายสื่อสารมีหน้าที่รับผิดชอบในการแปลงรหัสข้อมูลที่ Terminal ต้นทาง และถอดรหัสที่ปลายทาง หลังจากนั้นเมื่อต้องการส่งข้อมูลต่อไปยัง Terminal อื่น ก็จะทำการ Encrypt ต่อไปเป็นช่วง ๆ การ Encrypt ข้อมูลอีกลักษณะคือ End-to-end Encryption คือการ Encrypt ข้อมูลที่ต้นทางและจะ Decrypt เมื่อถึงปลายทางเท่านั้น นอกจากนี้ยังสามารถ Encrypt ใน Password Log-in ได้อีกด้วย โดยใช้วิธีเรียกว่า Challenge and Response Procedure ให้การรับรองว่าเป็น User ที่ถูกต้องในขณะที่เริ่ม Log-in โดยที่ไม่จำเป็นต้องป้อนข้อมูลอื่นเพิ่มเติม ผู้ที่จะลักลอบดักสัญญาสื่อสารนี้ต้องใช้เวลาในการถอดรหัส และจะต้องใช้ผู้เชี่ยวชาญทางการสื่อสารจึงจะสามารถแปลงข้อมูลกลับได้



Operating System Penetration

ระบบการควบคุมรักษา Operating System ควรจะมีประสิทธิภาพ เพื่อป้องกัน User ที่ไม่มีสิทธิเกี่ยวข้องกับการใช้ O/S รวมทั้งบุคคลภายนอก ฝ่ายบริหารจำเป็นต้องมีมาตรการป้องกันการลักลอบเข้าถึงระบบ (O/S Penetration Studies) เพื่อประเมินว่าผู้ที่ต้องการลักลอบเข้าถึงระบบการทำงานของ O/S จะต้องใช้ความพยายามมากเท่าใด ด้วยวิธีใดและต้องลงทุนเท่าใด ถ้าพบข้อบกพร่องจะได้ทำการแก้ไขปรับปรุงแผนป้องกันนี้ต่อไป

I/O Control เป็นจุดที่มีจุดอ่อนมากที่สุด เนื่องจาก I/O Code เป็นเรื่องสลับซับซ้อน กว่าจะค้นพบข้อผิดพลาดได้ต้องใช้เวลาในการตรวจสอบ เนื่องจาก I/O Channel หรือช่องสื่อสารสำหรับติดต่อข้อมูลกันระหว่างเครื่อง Terminal กับอุปกรณ์ประกอบ มีสิทธิเข้าถึง Primary Storage ได้โดยตรง และสามารถเปลี่ยนแปลง System Information ที่สำคัญได้ นอกจากนี้ I/O Channel จะถูกบังคับให้ทำงานในลักษณะของ Infinite loop และไม่ยอมรับข่ายสื่อสารของ I/O ให้ทำงานตามระบบงานได้ ผลกระทบนี้จะทำให้ระบบการทำงานเสียหายอย่างมาก

แผนทดสอบการลักลอบเข้าถึง O/S จะถูกกำหนดขึ้นเพื่อประเมินว่าจะต้องใช้ความพยายามมากเท่าใด ลงทุนทางด้านไหนบ้าง และมากน้อยเท่าใด จึงจะทำให้บุคคลภายนอก (Potential Penetrator) สามารถล่วงล้ำในหน่วยสารนิเทศของระบบงาน (System Resources) ได้ ทั้งนี้ กุญแจสำคัญของกลไกในการรักษาความปลอดภัยคือทำให้ระบบนี้ดูใหญ่ แต่ไม่ให้ใหญ่มากเท่ากับการทำงานของ System Designer



ข้อบกพร่องทั่วไปของระบบการทำงานของ O/S
(Generic System Functional Flaws)

จุดอ่อนที่พบใน O/S	จุดบกพร่อง	การตรวจสอบ/ข้อเสนอแนะ
Legality Checking	- Authentication : การตรวจสอบดูว่าผู้ที่กำลังติดต่อหน้าจอคอมพิวเตอร์นั้นเป็นผู้มีสิทธิจริงหรือไม่ เนื่องจากในระบบคอมพิวเตอร์หลายระบบ User ส่วนมากไม่อาจทราบได้ว่าเครื่องและโปรแกรมที่กำลังทำงานอยู่นั้นเป็นเครื่องที่ใช้งานจริงหรือไม่ เพราะผู้ที่ลักลอบเข้าถึงระบบการทำงานอาจจะทำสายสื่อสารขึ้นใหม่โดยที่ User ไม่รู้ตัวว่ากำลังพิมพ์ Password ของตัวเองลงใน File ปลอม ซึ่งแสดงให้เห็นว่า ระบบการรับรอง Password ยังไม่รัดกุมอย่างเพียงพอ	- การตรวจสอบดูว่า User ผู้นั้นมีสิทธิใช้เครื่องได้จริงหรือเปล่า โดยทำการตรวจสอบ Parameter ของ User
	- Encryption : การแปลงรหัส ซึ่งโดยทั่วไปแล้ว Master list Password ทั้งหมดควรเก็บไว้ในรูปของรหัส และฝ่ายบริหารส่วนมากไม่ได้ให้ความสำคัญในเรื่องการดูแลรักษาความปลอดภัย	- ควรมีการจัดทำแผนการตรวจว่ามีผู้พยายามลักลอบใช้ข่ายสื่อสารลักลอบข้อมูลหรือไม่ และอย่างไร เพราะบางครั้งการลักลอบเข้าถึงข่ายสื่อสารนั้นอาจจะไม่ต้องการข้อมูลก็ได้ หรือข้อมูลที่ได้ไปก็อาจจะไม่เป็นประโยชน์ต่อการโจรกรรม อาจเป็น เพียงแผนการที่แสดงให้เห็นว่าผู้บริหารยังไม่ให้ความสำคัญอย่างเพียงพอในเรื่องการรักษาความปลอดภัยในระบบสื่อสาร

จุดอ่อนที่พบใน O/S	จุดบกพร่อง	การตรวจสอบ/ข้อเสนอแนะ
	- Password : การลองกด Password หลาย ๆ ครั้ง อาจจะทำให้เดา Password ถูกได้ เพราะฉะนั้นควรมีการเปลี่ยน Password เป็นระยะ	- ตรวจดูว่าฝ่ายบริหารมีมาตรการในการจัดให้ใช้ Password อย่างไร มีระยะเวลาเปลี่ยน Password หรือไม่
	- Privilege : การใช้สิทธิพิเศษของโปรแกรม เพราะระบบงานบางระบบมีโปรแกรมพิเศษหลายโปรแกรม ซึ่งโดยทั่วไปแล้วควรจะเก็บจำนวนโปร-แกรมพิเศษไว้ให้น้อยที่สุด	- มีการเช็คสอบโปรแกรมระบบงานว่ามีปะปนกับโปรแกรมที่ใช้งานพิเศษหรือไม่ และควรจัดระเบียบขั้นตอนในการเก็บโปรแกรมพิเศษอย่างไร
	- Program Confinement : การขอยืมใช้โปรแกรมในระหว่าง User ด้วยกัน อาจจะทำให้เกิดการเปลี่ยนโปรแกรมของ User ได้	- ควรมีการวางกฎข้อบังคับที่ User ห้ามใช้ File บางประเภท และ File นั้นจะต้องเป็น File ที่ User บางคนรับผิดชอบโดยเฉพาะเจ้าหน้าที่ระดับบริหารควรออกระเบียบข้อบังคับให้มีการเช็คสอบผู้ใช้ File พิเศษ และมีการทำทะเบียนบันทึกรายละเอียดไว้
	- Clandestine Code : การลักลอบเข้าถึงข้อมูลโดยรหัสลับ อาจจะแทรกซึมเข้าในรูปของ Patching หรือส่วนคำสั่งที่เขียนเพิ่มเติมให้กับโปรแกรมเพื่อแก้ไขส่วนผิดพลาด หรือเปลี่ยนแปลงบางอย่างใน O/S ซึ่งรหัสนี้สามารถจะเรียกมาใช้งานได้แม้ว่ารหัสผ่านต่าง ๆ จะเปลี่ยนแปลงไปหมดแล้วก็ตาม	- การตรวจสอบ Log เพื่อดูว่ามีงานอื่นที่ผิดปกติมาประมวลผลใน File หรือไม่ เป็นการตรวจสอบขั้นต้น

จุดอ่อนที่พบใน O/S	จุดบกพร่อง	การตรวจสอบ/ข้อเสนอแนะ
	- Masquerade : การหาผลประโยชน์จากเครื่องคอมพิวเตอร์โดยใช้รหัสผ่าน (Password) และรหัสบัญชี (User ID) หรือบุกรุกค้นหา Privileged ข้อมูลในระบบคอมพิวเตอร์หรือลักลอบเข้าถึงระบบงานโดยใช้วิธีล่อล่วง Operator ในการล้ำเขตของ Security - Piggyback : คือการหาผลประโยชน์จากระบบคอมพิวเตอร์โดยอาศัยสิทธิของผู้อื่น โดยใช้ Terminal เพื่อดักขโมยข้อมูลจากสายสื่อสารระหว่าง User กับ Processor และจากนั้นจะทำการเปลี่ยนแปลงข้อมูลตามใจชอบ	
Implementation	- ทางฝ่ายบริหารได้จัดวางแผนการรักษาความปลอดภัยไว้อย่างดี แต่ไม่มีการปฏิบัติตาม	- ดูว่ามีการ Review แผนรักษาความปลอดภัย และมีการฝึกซ้อมในความพร้อมเพียงอย่างไรบ้าง หรือมีการปรับปรุงแผนรักษาความปลอดภัยให้ทันกับระบบงานในปัจจุบันอย่างไร
	- Time Sharing : คือการแบ่งเวลาใช้งานเครื่องคอมพิวเตอร์ขนาดใหญ่ให้กับผู้ใช้งานหลาย ๆ คน ระบบงานอาจจะนำเอา System information ที่สำคัญไปไว้ใน Address ของ User โดยไม่ได้ตั้งใจ เนื่องจากจุดบกพร่องของการแบ่งเวลาใช้งานของเครื่องคอมพิวเตอร์	- ตรวจสอบโดยเช็ค System log จะเป็นในรูปการสุ่มตัวอย่างก็ได้

จุดอ่อนที่พบใน O/S	จุดบกพร่อง	การตรวจสอบ/ข้อเสนอแนะ
	- Implicit trust : ความเคยชินในการทำงานในระบบงาน โดยที่คิดว่าระบบงานเดิมนั้นดีอยู่แล้ว ไม่จำเป็นต้องมีการปรับปรุงเปลี่ยนแปลง	- ควรมีการออกระเบียบในการพัฒนาปรับปรุงระบบงานสม่ำเสมอให้ทันต่อความต้องการของการทำงานในช่วงนั้น
	- Operator Carelessness : โดยที่ผู้พยายามลักลอบการเข้าถึงเครื่องอาจจะล่อลวงให้ Operator ทำ O/S Disk Pack ปลอมอีกชุดหนึ่งได้	- O/S Disk Pack ควรเก็บในตู้เซฟ มีการเปิดใช้เป็นเวลา และควรมีทะเบียนบันทึกรายชื่อผู้มีสิทธิใช้ Disk นี้
	- Residue : การทิ้งกระดาษที่พิมพ์แล้วโดยไม่มีการทำลายซึ่งข้อความที่พิมพ์บางอย่างอาจมีความสำคัญ เช่น รายชื่อ Password เพราะฉะนั้นข้อมูลที่มีความสำคัญเมื่อไม่ใช้แล้วควรทำลายทิ้งทุกครั้ง	
	- ผู้ลักลอบเข้าถึงระบบงานพยายามป้อนคำสั่ง SEND/RECEIVE เพื่อทดลองในสิ่งที่เป็นไปได้ เช่น พยายามลองใช้ Password และบังเอิญตรงกับ Password ที่มีอยู่ใน List เป็นต้น	- ควรตรวจดูว่ามีการจัดทำ Penetrator entrapment หรือไม่ ซึ่งเป็นแผนตรวจจับผู้พยายามลักลอบเข้าถึงระบบงาน เป็นการป้องกันขั้นต้นไว้ด้วย แต่ระบบคอมพิวเตอร์ส่วนใหญ่มักจะละเลยในเรื่องนี้
	- Implied sharing : ระบบงานอาจจะนำเอา System information ที่สำคัญไปไว้ใน Address ของ User โดยไม่ได้ตั้งใจ เนื่องจากจุดบกพร่องของการแบ่งเวลาใช้งานของเครื่องคอมพิวเตอร์ และเมื่อ User ทำงานเสร็จ	- การตรวจโดยใช้วิธีจำกัดจำนวน Log-in ของเครื่อง เมื่อเกินจำนวนครั้งที่กำหนด Terminal จะ Log-out ไปเอง และจะมีสัญญาณแจ้งไปที่ System administrator แต่ระบบคอมพิวเตอร์ส่วนมากไม่มี

จุดอ่อนที่พบใน O/S	จุดบกพร่อง	การตรวจสอบ/ข้อเสนอแนะ
	ผู้ลักลอบจะรีบสวมรอยทำงานต่อไปก่อนที่สายสื่อสารจะหยุดทำงาน การลักลอบดักข้อมูลระหว่างสายสื่อสารอาจกระทำได้โดยเชื่อมสายกับสายสื่อสารของ User terminal ที่ไม่ได้ใช้งานอยู่ตลอดเวลา นอกจากนี้ การประมวลผลข้อมูลแบบต่อเนื่อง (Interacting synchronized process) ด้วยความเร็วสูง สามารถส่งข้อมูลไปยังที่ต่าง ๆ ได้ และยากที่จะติดตามผลงาน	ความรัดกุมเพียงพอในการรักษาความปลอดภัยเช่นนี้ นอกจากนี้ควรเข้มงวดในการจัดให้ Line disconnect ทันทีที่ User ทำงานเสร็จ เพื่อป้องกันผู้อื่นสวมรอยทำงานต่อไป - การป้องกันคลื่นรบกวน Shilding โดยการติดตั้งเครื่องป้องกันคลื่นโดยระบบ Electronic ที่สามารถป้องกันในขณะส่งข้อมูลมิให้คลื่นไฟฟ้ากระจายรอบสายสื่อสาร ตามปกติการส่งข้อมูลจะมีคลื่นไฟฟ้ากระจายรอบสายสื่อสาร ซึ่งก่อให้เกิดสนามแม่เหล็ก ซึ่งทำให้ดักฟังข่ายสื่อสารหรือระบบคอมพิวเตอร์ได้ง่าย
Parameter Passing	- Parameter passing by reference VS by value : การส่ง Parameter โดยชี้แจงถึงแหล่งและการส่งผ่านโดยตรง บางโปรแกรมระบบงานถูกเขียนให้ Register เป็นผู้ชี้ Location ของ Parameter แทนที่จะส่งโดยตรง และอีกจุดคือ Unexpected parameter โดยการทำลายระบบงานโดยการป้อนค่า Parameter ผิด Supervisor call และจะใช้เวลานานกว่าจะตรวจสอบพบ ซึ่งเป็นช่องว่างของระบบการรักษาความปลอดภัยในระบบงาน	- จะเป็นการปลอดภัยที่จะผ่าน Parameter โดยตรงถึง Register (หน่วยความจำชั้นเล็ก ๆ ขนาด 1 Byte ใช้เก็บข้อมูลหรือหมายเลขตำแหน่งข้อมูลไว้ชั่วคราวขณะทำการประมวล) แทนที่จะให้ Register เป็นผู้ชี้ Location ของ Parameter เพราะการใช้ Register เป็นตัวชี้ตำแหน่งข้อมูล ซึ่งสามารถนำไปถึง Address ของ User ทำให้เกิดการชี้ช่องทางในการเข้าถึง O/S ได้

จุดอ่อนที่พบใน O/S	จุดบกพร่อง	การตรวจสอบ/ข้อเสนอแนะ
	- Asynchronous : คือการส่งสัญญาณข้อมูลโดยมีรหัสเริ่มส่ง (Start) และรหัสสุดท้าย (Stop) รวมอยู่ด้วยทุกครั้งเป็นการสื่อสารที่มีความเร็วค่อนข้างต่ำการจู่โจมในขณะที่ทำการประมวลผลแบบ Multiple process เป็นช่วงว่างในการส่งข้อมูลที่ผิดในขณะที่ตัว Process ทำ Validity check ง่ายต่อการแทรกแซงและทำการตรวจสอบได้ยาก - Denial of access : การกลั่นแกล้งให้ระบบงานเสียหายโดยการที่ User เขียนโปรแกรมที่ทำงานแบบ Infinite loop หรือทำหน้าที่ควบคุมระบบงานทั้งหมดเพื่อไม่ให้ User ผู้มีสิทธิจริงทำงานได้ - Trojan Horse : คือวิธีลักลอบเข้าถึงระบบงานเพื่อทำลายระบบข้อมูลด้วยการใช้รหัสหรือคำสั่งที่ซ่อนอยู่ในโปรแกรมขนาดใหญ่ เพื่อรบกวนการทำงานของโปรแกรม Trojan Horse นี้อาจจะอยู่ใน System ตลอดไป จะทำงานต่อเมื่อมีการทำงานครั้งสำคัญ และเมื่อผู้ลักลอบใช้งานเสร็จแล้วอาจจะลบร่องรอยของการลักลอบใช้งานนี้ได้	- ควรมีการตรวจสอบ Programe code เป็นครั้งคราว เพื่อป้องกันการลับลอบใช้โปรแกรม และเพื่อความคล่องตัวในการประมวลผลข้อมูล ระบบงานส่วนใหญ่จะอนุญาตให้มีการ Interrupt งานที่กำลังทำอยู่ เพื่อทำงานที่เร่งด่วนก่อน เมื่อเสร็จจากงานด่วนจึงกลับมาทำงานเดิมต่อไป ซึ่งผู้พยายามลักลอบเข้าถึงระบบงานจะพยายามเข้าครอบ-ครองระบบการควบคุมการทำงาน ณ จุดนี้

Case Study : Penetrating an Operating System

ได้มีการทำการทดสอบการลักลอบเข้าถึง System Operation โดยกลุ่มนักศึกษาระดับปริญญาโทขึ้นไปของ University of Michigan ในเมือง Ann Arbor และประสบความสำเร็จ กล่าวคือ

หัวข้อของการลักลอบเข้าถึงระบบงาน จะเน้นในการรักษาความปลอดภัยของ Software เป็นหลัก

วัตถุประสงค์

พยายามเข้าถึง File ที่ User ต้องใช้สิทธิพิเศษในการใช้ File และทำให้ System เสียหายได้

ระบบงานที่เกี่ยวข้อง

MTS (Michigan Terminal System) ที่ใช้งานได้กับเครื่อง IBM 360/370 และสามารถประมวลผลได้ทั้งระบบ Batch และระบบที่มีการโต้ตอบกันระหว่างเครื่องคอมพิวเตอร์กับผู้ใช้งาน (Interactive Computation) ประกอบด้วยระบบการจัด File ที่ใหญ่พอสำหรับ Sharing และสามารถ Maintain รายการ (User Accounts) ได้ 25,000 รายการ นอกจากนี้ MTS สามารถที่จะรับระบบการทำงานแบบ Interactive ได้พร้อมกัน 250 Users

ขั้นตอนในการทำงาน

คณะทำงานประกอบด้วยผู้ใช้ (User) ตามปกติของ MTS และได้รับสิทธิพิเศษในการเข้าถึงเอกสารประกอบภายในของตัวเครื่อง ลักษณะการทำงานต้องทำ Comprehensive Analysis คือการวิเคราะห์ระบบงานตามจุดต่าง ๆ และเขียนรายงานเกี่ยวกับข้อบกพร่องตามวิธีการตั้งข้อสมมติฐานในการหาจุดบกพร่องของระบบงานที่บริษัท System Development Corporation เป็นผู้พัฒนาขึ้นตามหัวข้อดังต่อไปนี้

1) Flaw Hypothesis Generation การตรวจหาจุดบกพร่องทั่วไปของระบบงาน โดยคณะทำงานจะทำการตรวจสอบและรายงานจุดบกพร่องที่กล่าวให้ทราบ

2) Flaw Hypothesis Confirmation จะยืนยันจุดบกพร่องในระบบงานตามข้อสมมติฐานที่ตั้งไว้ โดยการทำ Teat Run เพื่อให้แน่ใจว่าจุดบกพร่องที่ตั้งข้อสงสัยไว้เป็นจุดบกพร่องที่แท้จริง

3) Flaw Generalization จุดบกพร่องที่ตรวจสอบพบและจัดอยู่ในข้อบกพร่องทั่วไปของระบบงาน ถือได้ว่าเป็นจุดอ่อนในโครงสร้าง (Design weaknesses) ของระบบงานหรือไม่ ถ้าเป็นก็จะต้องค้นหาสาเหตุข้อแก้ไข

คณะทำงานได้ค้นพบจุดบกพร่องในการรักษาความปลอดภัยของ Software ดังต่อไปนี้

1) มีจุดบกพร่องบางจุดในระบบ Subroutines
2) กลไกในการตรวจเช็ค Parameter ยังไม่รัดกุม กล่าวคือ เกิด Arbitrary bit Sequences ลำดับของ bit ที่ถูกเก็บใน System Segment ประกอบด้วยระบบการควบคุมสารสนเทศของงาน (System's Control Information about a task)

3) มีจุดบกพร่องในระบบงาน เปิดช่องให้ User สามารถเปลี่ยนแปลง System Accounting Information และเปลี่ยนลำดับความสำคัญของ User ได้ด้วย

4) ระบบการควบคุมและป้องกันการเข้าถึงสารสนเทศของ MTS ได้ถูกบรรจุใน System Segment และอาจถูกแก้ให้หมดประสิทธิภาพในการคุ้มครองระบบงาน

5) User สามารถเปลี่ยนระบบจาก User mode หรือวิธีการปฏิบัติงานของ User มาเป็นวิธีการปฏิบัติงานของระบบงาน และจะทำการปฏิบัติงานตามคำสั่งของโปรแกรมที่ User มีสิทธิพิเศษเรียกใช้งาน

Supervisor call อาจจะทำลายระบบการควบคุม Hardware Storage ที่จะช่วยให้ User ได้ปรับปรุงและเปลี่ยนแปลงหน่วยความจำสำรอง (Storage Segment) เมื่อ Supervisor core ของ MTS อาศัยใน Shared Segments และ User สามารถเปลี่ยนจากระบบการทำงานของเครื่องมาเป็นระบบควบคุมการปฏิบัติงาน (Supervisor State) และสามารถเข้าถึงส่วนใดของ Supervisor และ Software ได้ตามใจชอบ

ขั้นตอนในการลักลอบเข้าควบคุมระบบการทำงานของ Software สามารถทำได้สำเร็จตามเป้าหมาย และชี้ให้เห็นถึงจุดบกพร่องต่าง ๆ ดังนี้

จุดบกพร่องในกลไกการตรวจสอบ Parameter จะพบหลังจากที่ System ใช้งานแล้ว ซึ่งจะเป็นการเปิดช่องว่างให้ User ทำการเปลี่ยนแปลง Parameter ก่อนที่ System จะทำการตรวจสอบได้ ผู้ลักลอบสามารถนำจุดบกพร่องเกี่ยวกับ Parameter ไปแสวงหาประโยชน์ด้วยการเปลี่ยน Address Parameter ให้ไปสู่ System Segment แทนที่จะไปยัง User Storage ตามปกติ ซึ่งแสดงให้เห็นความสำคัญขณะทำการสื่อสารระหว่างการเช็คสอบ Parameter Routines กับ Routines ที่ใช้งานปัจจุบันของ Parameter โดยระบบ Synchronous นั้นจะยังมีจุดบกพร่องอยู่ ซึ่งคณะทำงานได้มีความเห็นพ้องต้องกันในขณะที่ใช้ระบบ MTS

จุดบกพร่องอีกข้อหนึ่ง แสดงให้เห็นถึงโปรแกรมบางส่วนของระบบงานอาจถูกบังคับให้เก็บข้อมูลที่สำคัญ ในหน่วนเก็บข้อมูลสำหรับ User ทั่วไป (User Accessible Segments) จากนั้น User ทั่วไปสามารถสั่งงานจาก User-Accessible Segments โดยจะได้รับการแบ่งเวลาใช้งานเครื่องได้ตามใจชอบ (Free Computer Time) และสามารถจะทำลายระบบงานได้ด้วยการบังคับโปรแกรม Supervisors ให้อยู่ใน Infinite loop

การควบคุมจะต้องประสานกลไกในการรักษาความปลอดภัยของ O/S เข้าด้วยกันเพราะเมื่อทุกฝ่ายให้ความร่วมมือกันในด้านการรักษาความปลอดภัยแล้ว ไม่เพียงแต่ระบบงานจะถูกควบคุมอย่างรัดกุมเท่านั้น แม้แต่ระดับ Higher Privileged Levels ก็จะสามารถควบคุมได้ด้วย



Utility Programs

Utility Programs เป็นโปรแกรมสำเร็จรูปที่บริษัทผู้ผลิตเครื่องคอมพิวเตอร์ส่วนใหญ่จัดทำขึ้น มีหน้าที่ควบคุมระบบการทำงานตามลักษณะต่าง ๆ กัน ได้แก่

: เปลี่ยนตัวกลางที่ใช้บันทึกข้อมูล เช่น จากเทปมาเป็นแผ่น Diskette เป็นต้น
: ปรับข้อมูลให้ทันสมัยอยู่เสมอ โดยเปลี่ยนหรือลบ Record ที่ไม่ใช้ทิ้งไป
: สร้างหรือลบ File เก่าทิ้งไปเมื่อหมดความจำเป็นในการใช้งาน
: เปลี่ยน Password ของ File ต่าง ๆ
: พิมพ์ File เพื่อใช้ประโยชน์ในการตรวจสอบ
: จัดเรียง File ใหม่ให้สะดวกในการใช้งาน

หน้าที่ของ Utility Program ดังกล่าวข้างต้นนี้ ผู้ตรวจสอบสามารถอาศัยประโยชน์ในการทำ Compliance test และ Substantive test ตลอดจนศึกษาถึงระบบต่าง ๆ รวมทั้งช่วยสนับสนุนการตรวจสอบโปรแกรมระบบงาน (Software Application) อาทิ

- จัดเรียง File ให้เป็นไปตามลำดับขั้นตอนการทำงาน
- คัดลอกตัวอย่าง File เพื่อนำไปทดสอบ
- ลบล้าง File ที่หมดความจำเป็นในการใช้งาน
- พิมพ์ Internal file label สำหรับใช้เปรียบเทียบกับ Actual file label ว่ามีโปรแกรมนอกระบบงานแปลกปลอมบ้างหรือไม่
- พิมพ์ Record ของ File ที่ต้องการตรวจสอบ
- คัดลอก File จาก Disk มาบันทึกลงบนเทปเพื่อทำการประมวลผลตามที่ต้องการ

การประเมินผลการใช้ Utility Programs

Utility Programs บางประเภทหาได้ง่าย และสามารถทำงานได้เช่นเดียวกับ Audit Software Package อย่างไรก็ดี Utility Programs ที่ถูกสร้างขึ้นสำหรับ Operator และ Programmers เพื่อช่วยประมวลผลข้อมูล โดยเฉพาะผู้ตรวจสอบอาจนำไปใช้สนับสนุนการตรวจสอบได้ไม่คล่องตัวเท่าที่ควร เนื่องจากมิได้ออกแบบมาเพื่อการตรวจสอบโดยตรง

โดยทั่วไปประโยชน์ที่จะได้รับจากการใช้ Utility Program ในการตรวจสอบ คือช่วยลดขั้นตอนการสั่งงานของโปรแกรมได้มากกว่าการใช้ Audit Software ธรรมดา โดยเฉพาะถ้าผู้ตรวจสอบได้รับความร่วมมือจากบริษัทผู้ผลิตและขาย Utility Programs ก็จะทำให้การตรวจสอบมีประสิทธิผลยิ่งขึ้น อย่างไรก็ดี มีข้อจำกัดในการใช้ Utility Programs ช่วยในการตรวจสอบที่พึงระวัง 2 ประการ คือ

1) การควบคุม Parameter อาจจะใช้รหัสที่ผู้ตรวจสอบไม่สามารถล่วงรู้ได้
2) การใช้ Utility Program ช่วยในการตรวจสอบจะไม่มี Audit trail

การตรวจสอบการควบคุม Utility Programs

ในการใช้ Utility Programs ช่วยตรวจสอบ ผู้ตรวจสอบควรกำหนดขอบเขตไว้เช่นเดียวกับการตรวจสอบโปรแกรมระบบงาน (Applications) และตรวจสอบคู่มือตลอดจนรายละเอียดเกี่ยวกับ Utility Programs รวมทั้งการจัด Parameters สำหรับการใช้ Utilities ว่าเหมาะสมตามลักษณะงานของโปรแกรมนั้น ๆ หรือไม่ นอกจากนี้ ควรตรวจสอบดูการบันทึกทะเบียนการประมวลผลข้อมูลของ System Console's log หรือ Job Accounting Information เพื่อทบทวนดูว่าไม่มีระบบงานอื่นแปลกปลอมเข้ามาในระหว่างที่เครื่องทำการประมวลผลงานประจำ

ตัวอย่างของการใช้ Utility Program ช่วยในการตรวจสอบ

ผู้ตรวจสอบอาจนำ Utility Programs มาใช้ในการตรวจสอบดังต่อไปนี้

1) พิมพ์รายการใน File

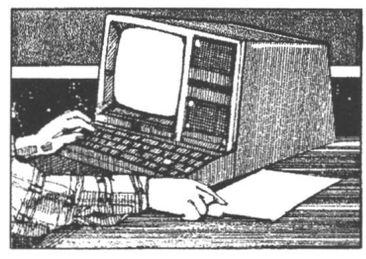
ผู้ตรวจสอบสามารถใช้คำสั่งใน Utility Program ให้พิมพ์ Records ทั้งหมดใน File ออกมา เพื่อตรวจหา Records ที่ผิดไปจากรายชื่อ Records ที่ได้ถูกบันทึกใน File

2) ทดสอบการบันทึกรายการ

ผู้ตรวจสอบสามารถใช้ Utility Program ในการหาข้อมูลจาก File แล้วนำมาเปรียบเทียบดูว่า Field ใน File และ Records ใน File จะมีจำนวนเท่ากันกับรายการ Records ที่บันทึก ในกรณีที่จำนวน Records สำหรับใช้งานปัจจุบันรวมแล้วมีจำนวนมากกว่าที่ได้ถูกบันทึกใน File ผู้ตรวจสอบเก็บรวบรวมรายชื่อ Record ออกมาเพื่อตรวจสอบว่า Records ที่เพิ่มขึ้นนั้นเป็นงานที่เกี่ยวข้องกันหรือไม่

3) ช่วยเสริมสร้างความเข้าใจในโปรแกรมระบบงาน

เนื่องจาก Utility Program สามารถสั่งให้พิมพ์ Source Programs ออกมาจาก Disk library ได้ ผู้ตรวจสอบจึงอาจตรวจสอบโปรแกรมที่ใช้งานปัจจุบันของ Source code ได้ด้วย



บทที่ 14

ตัวอย่างจุดอ่อนของการดำเนินงาน ด้านคอมพิวเตอร์ (Data Center หรือ General Controls) ที่อาจก่อให้เกิดการทุจริตได้ พร้อมกับคำแนะนำโดยสรุป

ตัวอย่างของระบบงานที่มีต่อทางด้านการตรวจสอบ Data Center

1. การจัดการ

1.1 การกำหนดนโยบายและการลงทุนด้านคอมพิวเตอร์

(1) ไม่มีการกำหนดนโยบายและแผนงานคอมพิวเตอร์

องค์กรไม่มีนโยบายและแผนงานคอมพิวเตอร์ที่ชัดเจน การดำเนินงานด้านคอมพิวเตอร์ขององค์กรส่วนใหญ่เป็นการแก้ปัญหาเฉพาะหน้า เช่น การนำระบบคอมพิวเตอร์เข้ามาใช้งานเมื่อต้องการนำอุปกรณ์หรือเครื่องมือทันสมัยเข้ามาบริการลูกค้า โดยไม่ได้เตรียมการด้านบุคลากรที่เกี่ยวข้องอย่างเพียงพอ เป็นผลให้การปฏิบัติงานด้านคอมพิวเตอร์ของสถาบันการเงินไม่ได้รับประโยชน์จากการใช้คอมพิวเตอร์อย่างเต็มที่

นอกจากนี้องค์กรยังไม่ได้กำหนดอำนาจหน้าที่และความรับผิดชอบของคณะอนุกรรมการคอมพิวเตอร์ไว้อย่างชัดเจน และไม่มีการรายงานผลการดำเนินงานด้านคอมพิวเตอร์ทุกระยะ จึงมีผลทำให้การพัฒนางานด้านนี้ขององค์กรไม่ก้าวหน้าเท่าที่ควร

ข้อแนะนำ

1) เพื่อให้การดำเนินงานขององค์กรโดยส่วนรวมมีประสิทธิภาพดีขึ้น องค์กรควรกำหนดนโยบาย เป้าหมาย แผนงานคอมพิวเตอร์ระยะสั้นและระยะยาว และจัดลำดับความสำคัญของแต่ละโครงการอย่างชัดเจน
2) ควรจัดทำงบประมาณในการจัดหาเครื่องคอมพิวเตอร์ อุปกรณ์ประกอบ โปรแกรมระบบงาน และบุคลากร ในอัตราส่วนที่เหมาะสมกับแผนงานที่วางไว้ในแต่ละปี

(2) การลงทุนด้านคอมพิวเตอร์

องค์กรไม่ได้กำหนดระเบียบและวิธีการจัดซื้อเครื่องคอมพิวเตอร์ไว้ชัดเจน จึงทำให้การพิจารณาตัดสินใจและการจัดทำสัญญาสั่งซื้อเครื่องคอมพิวเตอร์ แต่ละครั้งมีความแตกต่างกัน โดยเฉพาะอย่างยิ่งการจัดซื้อเครื่องคอมพิวเตอร์ที่มีจำนวนเงินสูง และองค์กรไม่ได้จัดตั้งงบประมาณไว้ก่อน ย่อมจะมีผลกระทบถึงแผนการใช้จ่ายในด้านอื่น ๆ ขององค์กรด้วย

ในกรณีที่องค์กรเริ่มนำระบบคอมพิวเตอร์มาใช้งาน และมีการลงทุนเพิ่มอีก ทำให้องค์กรมีภาระค่าใช้จ่ายด้านคอมพิวเตอร์ ได้แก่ ค่าเสื่อมราคา ค่าเช่า Software และค่าบำรุงรักษาเครื่อง นอกจากนี้ยังทำให้องค์กรเสียโอกาสในการให้สินเชื่อหรือลงทุนในสินทรัพย์อื่นที่ก่อให้เกิดรายได้แก่องค์กร อันจะเป็นผลกระทบต่อการดำเนินงานในอนาคต โดยเฉพาะในช่วงอัตราดอกเบี้ยเงินให้กู้ยืมมีแนวโน้มลดลง จึงอาจกล่าวได้ว่าองค์กรจะมีกำไรลดลงในอนาคตอย่างมีนัยสำคัญ ซึ่งสาเหตุหนึ่งมาจากค่าใช้จ่ายในการดำเนินงานด้านคอมพิวเตอร์ที่มีแนวโน้มสูงขึ้นมาก

แผนการลงทุนด้านคอมพิวเตอร์ในโครงการต่าง ๆ ขององค์กรยังขาดรายละเอียดเกี่ยวกับการพัฒนากำลังคน ค่าใช้จ่าย อุปกรณ์ที่จะใช้ และผลกระทบต่อฐานะทางการเงิน และการดำเนินงานด้านต่าง ๆ ซึ่งอาจมีผลต่อโครงสร้างของรายจ่ายและประสิทธิภาพในการทำกำไรขององค์กรในอนาคต

ข้อแนะนำ

1) องค์กรเพิ่มความระมัดระวังการลงทุนในสินทรัพย์ประจำด้านคอมพิวเตอร์ ซึ่งต้องใช้เงินลงทุนค่อนข้างสูง การจัดทำแผนการลงทุนด้านนี้ทั้งในระยะสั้นและระยะยาว นอกจากจะมีรายละเอียดการดำเนินงานตามโครงการและการพิจารณาตัดสินใจเลือกแนวทางการลงทุนแล้ว ควรมีรายละเอียดการวิเคราะห์ผลกระทบจากการลงทุนที่มีต่อฐานะและการดำเนินงานขององค์กร การเสียโอกาสลงทุนในสินทรัพย์อื่น และเรื่องอื่น ๆ ที่เป็นประโยชน์ในการพิจารณาลงทุนตามควรแก่กรณี โดยพิจารณาควบคู่กับแผนการเสริมสร้างรายได้และกำไรขององค์กรเพื่อให้การดำเนินงานโดยส่วนรวมขององค์กรสามารถดำเนินต่อไปได้ด้วยความมั่นคง

2) องค์กรควรทบทวนสัญญาการสั่งซื้อเครื่องคอมพิวเตอร์ และการชำระเงินให้สอดคล้องกับความสามารถทางการเงินขององค์กร หากเห็นว่าเกินความสามารถก็ควรเปลี่ยนแปลงสัญญา เพื่อสั่งซื้อเครื่องคอมพิวเตอร์ให้เหมาะสมและจำเป็นเท่านั้น หรืออาจพิจารณาจัดหาแหล่งอื่น หรือองค์กรอื่นที่ต้องการเปลี่ยนระบบงาน โดยมีเครื่องคอมพิวเตอร์และอุปกรณ์ที่องค์กรสามารถนำมาใช้ทดแทนได้ในราคาถูกกว่า

1.2 แผนฉุกเฉินและระบบคอมพิวเตอร์สำรอง

(1) องค์กรไม่ได้จัดทำแผนปฏิบัติงานฉุกเฉินไว้ปฏิบัติการในกรณีที่ไม่สามารถใช้เครื่องคอมพิวเตอร์ประมวลผลข้อมูลได้ตามปกติ ด้วยเหตุใด ๆ ก็ตาม อาจทำให้การดำเนินงานและการให้บริการหยุดชะงักเป็นที่เสียหายแก่องค์กรและประชาชนทั่วไปได้

ข้อแนะนำ

องค์กรควรจัดทำแผนฉุกเฉิน (Emergency Plan) แผนปฏิบัติงานชั่วคราว และกำหนดวิธีการปรับปรุงแก้ไขข้อมูลที่ได้รับความเสียหายให้กลับคืนสู่สภาพปกติ (Contingency Plan หรือ Disaster/Recovery Plan) เป็นลายลักษณ์อักษร และฝึกหัดพนักงานให้คุ้นเคยกับวิธีปฏิบัติงานตามแผนฉุกเฉิน พร้อมทั้งจัดให้มีการทดสอบการปฏิบัติตามแผนดังกล่าวเป็นครั้งคราว ทั้งนี้แผนฉุกเฉินควรประกอบด้วย

- วิธีเผชิญเหตุการณ์ร้ายแรงเพื่อจำกัดขอบเขตความเสียหาย และให้สามารถปฏิบัติงานต่อไปได้อย่างรวดเร็ว
- แผนการอพยพเคลื่อนย้ายพนักงานออกจากสถานที่เกิดเหตุ
- ระเบียบปฏิบัติสำหรับพนักงานเมื่อไฟไหม้ น้ำท่วม มีผู้บุกรุก ถูกวางระเบิด หรือมีเหตุการณ์ร้ายแรงอื่น ๆ
- ความปลอดภัยของสถานที่เก็บแฟ้มข้อมูลและเอกสาร
- ระเบียบปฏิบัติในการปิดเครื่องคอมพิวเตอร์

- ระเบียบการปฏิบัติงานประมวลผลซ้ำ เพื่อปรับปรุงแก้ไขข้อมูลให้มีสภาพใช้งานได้ตามปกติ เมื่อเครื่องจักรขัดข้องหรือเสียหาย

นอกจากนี้เพื่อไม่ให้การดำเนินงานและการให้บริการของธนาคารหยุดชะงัก จึงควรกำหนดขั้นตอนในการปฏิบัติงานชั่วคราวในระหว่างที่ยังใช้ศูนย์คอมพิวเตอร์ไม่ได้ โดยกำหนดให้ครอบคลุมบางหัวข้อหรือทุกหัวข้อในเรื่องต่อไปนี้ แล้วแต่กรณี

- กำหนดหน้าที่และความรับผิดชอบของพนักงานแต่ละคนในการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน
- กำหนดความสำคัญของเอกสารและอุปกรณ์ที่จำเป็นต้องขนย้ายตามความสำคัญก่อนหลังและวิธีการขนย้าย
- กำหนดความสำคัญของขั้นตอนการปฏิบัติงานตามลำดับก่อนหลังเมื่อเกิดเหตุฉุกเฉิน
- กำหนดสถานที่ที่จะต้องใช้ปฏิบัติงานชั่วคราว
- กำหนดหน้าที่และความรับผิดชอบของพนักงานที่จะปฏิบัติงานในศูนย์คอมพิวเตอร์ชั่วคราว
- กำหนดวิธีการปฏิบัติงาน อุปกรณ์และเอกสารที่จำเป็นที่จะต้องใช้ที่ศูนย์คอมพิวเตอร์ชั่วคราว
- กำหนดความสำคัญของงานที่จะต้องประมวลผลก่อนหลัง และระยะเวลาที่จะต้องปฏิบัติงานให้เสร็จสมบูรณ์
- กำหนดวิธีการแจกจ่ายเอกสารที่ได้จากการประมวลผลไปยังหน่วยงานที่เกี่ยวข้อง
- กำหนดวิธีปฏิบัติงานด้าน Manual แทนระบบ On-line โดยใช้รายงานที่ได้รับ
- กำหนดขั้นตอนในการปฏิบัติงานเพื่อกลับเข้าปฏิบัติงานในศูนย์คอมพิวเตอร์ที่เสียหาย
- กำหนดวิธีการแก้ไขปัญหาที่ศูนย์คอมพิวเตอร์ที่เสียหายแล้วแต่กรณี ให้กลับสู่สภาวะปกติ

(2) แผนฉุกเฉินไม่ครบถ้วนและไม่เป็นปัจจุบัน

- องค์กรมิได้ปรับปรุงรายชื่อและหน้าที่ความรับผิดชอบของพนักงานผู้เกี่ยวข้องในการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน และมิได้จัดทำทะเบียนควบคุมเอกสารและคู่มือชุดสำรองที่เก็บไว้ภายนอกศูนย์คอมพิวเตอร์ พร้อมทั้งติดตามปรับปรุงเอกสารให้เป็นปัจจุบัน

ข้อแนะนำ

เพื่อให้การแก้ไขเหตุฉุกเฉินเป็นไปอย่างถูกต้อง เหมาะสม และทันกาล องค์กรควรทบทวนและปรับปรุงรายชื่อ หน้าที่ความรับผิดชอบของพนักงานซึ่งมีหน้าที่ปฏิบัติตามแผนฉุกเฉิน รวมทั้งปรับปรุงเอกสารคู่มือให้เป็นปัจจุบันอยู่เสมอ

(3) องค์กรไม่มีระบบกระแสไฟฟ้าสำรองเพื่อให้แสงสว่างเพียงพอ

ในการปฏิบัติงานในห้องเครื่อง และสำหรับป้อนเครื่องคอมพิวเตอร์ นอกจากระบบไฟฟ้าสำรอง UPS อันจะทำให้องค์กรไม่สามารถปฏิบัติงานและให้บริการได้อย่างต่อเนื่อง

ข้อแนะนำ

ควรจัดให้มีระบบกระแสไฟฟ้าสำรอง เพื่อให้องค์กรสามารถปฏิบัติงานและให้บริการได้อย่างต่อเนื่อง

(4) ควรจัดให้มีระบบคอมพิวเตอร์ชุดสำรอง (Backup)

ปัจจุบันองค์กรยังไม่มีระบบคอมพิวเตอร์สำรองไม่มีการจัดเก็บโปรแกรมชุดสำรองและแฟ้มข้อมูลสำรอง ทั้งในสำนักงานและนอกสำนักงาน

ข้อแนะนำ

องค์กรควรจัดให้มีอุปกรณ์คอมพิวเตอร์ โปรแกรม และแฟ้มข้อมูลชุดสำรอง ไว้นอกอาคารที่ทำการของศูนย์คอมพิวเตอร์ หรือทำสัญญากับบุคคลภายนอกที่มีเครื่องคอมพิวเตอร์ซึ่งมีประสิทธิภาพใกล้เคียงกัน สำหรับใช้ปฏิบัติงานในกรณีเครื่องคอมพิวเตอร์ขององค์กรเสียหายใช้การไม่ได้ทั้งหมด หรือเมื่อเกิดเหตุฉุกเฉิน เพื่อไม่ให้การดำเนินงานขององค์กรหยุดชะงัก

นั่นคือ ควรมีแผนงานเกี่ยวกับระบบคอมพิวเตอร์สำรอง ซึ่งควรประกอบด้วย

- การเตรียมหาศูนย์ประมวลผลสำรองเตรียมไว้ทดแทน
- การมอบหมายหน้าที่ในการสร้างข้อมูลที่ได้รับความเสียหายขึ้นมาใหม่ และหน้าที่ในการประมวลผลนอกสถานที่
- กรณีจำเป็นต้องประมวลผลนอกสถานที่ด้วยคอมพิวเตอร์ชุดสำรอง (Backup Site)
- การพิจารณาตัดสินใจและความรับผิดชอบในการใช้ Backup Site
- ขั้นตอนที่พนักงานต้องปฏิบัติในการเสนอขอใช้ Backup Site
- วิธีแจ้งการขอใช้ Backup Site ตามข้อตกลงหรือสัญญาที่ได้กระทำไว้กับผู้อื่น
- แฟ้มข้อมูล โปรแกรม และเอกสารที่จำเป็นต้องนำไปใช้ที่ Backup Site และวิธีการขนย้ายวัสดุอุปกรณ์
- ลำดับความสำคัญในการประมวลผล
- พลังงานสำรอง (Reserve Supplies)
- สิ่งอำนวยความสะดวกในการประมวลผล และข้อมูลที่สำคัญชุดสำรอง

(5) การจัดเก็บแฟ้มข้อมูลและโปรแกรมชุดสำรอง

องค์กรไม่มีระเบียบกำหนดอายุการเก็บข้อมูลแต่ละประเภทใน เทป และการบันทึกข้อความลงใน label ที่ติดบนเทปไม่ครบถ้วน

- การบันทึกรายละเอียดในทะเบียนเทปบางหัวข้อไม่เป็นมาตรฐานเดียวกัน
- ตู้ที่ใช้เก็บเทปชุดสำรองภายนอกสถานที่ และกระเป๋าที่ใช้ขนย้ายเทป ไม่สามารถป้องกันคลื่นแม่เหล็กได้

ข้อแนะนำ

องค์กรควรดำเนินการแก้ไขข้อบกพร่องข้างต้นต่อไป

(6) การเก็บรักษาแฟ้มข้อมูลชุดสำรองไม่เหมาะสม

ปัจจุบันสถาบันการเงินเก็บแฟ้มข้อมูลชุดสำรองรวมกับแฟ้มข้อมูลชุดจริงในห้องคอมพิวเตอร์ หากเกิดเหตุฉุกเฉินห้องคอมพิวเตอร์ได้รับความเสียหาย จะทำให้แฟ้มข้อมูลชุดจริงและชุดสำรองถูกทำลายไปพร้อมกัน และส่งผลให้องค์กรมีปัญหาในการปฏิบัติงานและให้บริการลูกค้า

ข้อแนะนำ

องค์กรควรแยกเก็บแฟ้มข้อมูลชุดสำรองไว้ที่แห่งอื่นนอกศูนย์คอมพิวเตอร์ หรืออาจแยกเก็บไว้ที่สาขาใกล้เคียง

(7) การควบคุมการขนย้ายเทปข้อมูลชุดสำรองไม่รัดกุม

การขนย้ายเทปข้อมูลชุดสำรองไปเก็บไว้ที่สาขาอื่น โดยไม่มีภาชนะที่แข็งแรงปิดมิดชิด อาจทำให้ข้อมูลเสียหายใช้งานไม่ได้ และการจัดทำทะเบียนรับ-ส่งยังไม่ครบถ้วน ประกอบกับพนักงานรักษาความปลอดภัยมิได้ลงลายมือชื่อรับทราบการนำเทปดังกล่าวออกนอกศูนย์คอมพิวเตอร์ทุกครั้ง

ข้อแนะนำ

ควรจัดทำทะเบียนรับ-ส่งเทปข้อมูลชุดสำรองให้ครบถ้วน และจัดหาภาชนะที่แข็งแรงปิดมิดชิด เพื่อป้องกันมิให้ข้อมูลเสียหายใช้การไม่ได้

(8) ข้อมูลชุดสำรองที่นำไปเก็บนอกสถานที่ยังไม่เป็นปัจจุบัน

ข้อมูลชุดสำรองของระบบงานบางระบบที่นำไปฝากเก็บที่สาขาอื่นไม่เป็นชุดล่าสุด หากเกิดเหตุฉุกเฉินทำให้ข้อมูลที่ใช้งานอยู่นั้นเสียหาย องค์กรจะไม่มีชุดสำรองที่เป็นปัจจุบันที่สุดนำมาใช้เพื่อให้การบริการลูกค้าสามารถดำเนินต่อไปอย่างรวดเร็ว และข้อมูลชุดสำรองของวันศุกร์และวันเสาร์เก็บไว้ในตู้นิรภัยที่สาขาตลอดแล้ว โดยไม่ได้นำข้อมูลชุดสำรองดังกล่าวไปเก็บที่สาขาอื่น

ข้อแนะนำ

ควรกำหนดให้มีการนำเทปข้อมูลชุดสำรองไปเก็บที่สาขาอื่นให้ครบทุกวัน และควรเป็นข้อมูลชุดล่าสุด

(9) ไม่มีเอกสารสนับสนุนการปฏิบัติงานชุดสำรอง

ปัจจุบันองค์กรมีเพียงเอกสารสนับสนุนการปฏิบัติงานสำหรับใช้ภายในศูนย์คอมพิวเตอร์เท่านั้น ไม่มีการจัดทำสำเนาเอกสารสนับสนุนการปฏิบัติงาน และนำมาจัดเก็บในสถานที่จัดเก็บแฟ้มข้อมูลชุดสำรอง (Backup file)

ข้อแนะนำ

องค์กรควรดำเนินการให้มีเอกสารสนับสนุนการปฏิบัติงานชุดสำรองต่อไป

1.3 การประกันภัยคอมพิวเตอร์

(1) จากการที่องค์กรได้จัดหาเครื่องและอุปกรณ์คอมพิวเตอร์มาใช้งานเพิ่มขึ้นเรื่อย ๆ จึงความพิจารณาจัดให้มีการประกันภัยความเสียหายอันจะเกิดกับคอมพิวเตอร์ให้ครบถ้วนทุกรายการด้วย เพื่อให้ได้รับความคุ้มครองอย่างเพียงพอ

(2) การประกันภัยเครื่องคอมพิวเตอร์และอุปกรณ์ไม่ครอบคลุมความเสี่ยงภัยบางด้าน

องค์กรประกันภัยเครื่องคอมพิวเตอร์และอุปกรณ์เฉพาะอัคคีภัย และประกันการสูญเสียเฉพาะความเสียหายที่เกิดจากการชิงทรัพย์ ปล้นทรัพย์ หรือความพยายามกระทำการดังกล่าว ซึ่งยังไม่คุ้มครองความเสี่ยงด้านอื่น ๆ ที่อาจทำให้องค์กรได้รับความเสียหายจากการดำเนินงานและให้บริการด้านคอมพิวเตอร์ เช่น การทุจริต เป็นต้น

ข้อแนะนำ

องค์กรควรจัดให้มีการประกันภัยที่คุ้มครองเครื่องคอมพิวเตอร์ให้ครบถ้วนทุกรายการ โดยให้คุ้มครองความเสี่ยงทุกด้าน เพื่อลดความเสียหายที่องค์กรอาจได้รับจากการใช้ระบบคอมพิวเตอร์

(3) การติดตั้งเครื่องคอมพิวเตอร์ในสถานที่อื่นไม่เป็นไปตามกรมธรรม์ประกันภัย

องค์กรได้ประกันภัยความเสียหายอันอาจเกิดขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์ โดยระบุสถานที่ตั้งหรือเก็บทรัพย์สินที่เอาประกันภัยไว้ในกรมธรรม์เป็นชั้นที่ 1-5 แต่ในบางขณะองค์กรได้ย้ายเครื่องคอมพิวเตอร์สำหรับพนักงานผู้เขียนโปรแกรมขึ้นไปอยู่ที่ชั้น 11 ของอาคารเดียวกัน ซึ่งองค์กรอาจได้รับความเสียหายเนื่องจากกรมธรรม์ประกันภัยดังกล่าวไม่ครอบคลุมถึง

ข้อแนะนำ

องค์กรควรติดตั้งเครื่องคอมพิวเตอร์ที่ได้ประกันภัยความเสียหายไว้ตามสถานที่ที่ได้ระบุไว้ในกรมธรรม์

(4) กรมธรรม์ประกันภัยขาดความสมบูรณ์

กรมธรรม์ประกันภัยคอมพิวเตอร์ที่องค์กรได้ทำไว้กับบริษัทประกันภัยขาดความสมบูรณ์ในการลงนามรับรองเอกสาร คือ

- รายละเอียดของรายการเครื่องและอุปกรณ์คอมพิวเตอร์ที่เอาประกันภัยไว้มีการประทับตรา แต่มิได้ลงนามกำกับไว้
- เงื่อนไขและความคุ้มครองของ "Computer All Risks" ซึ่งแนบเพิ่มเติมสัญญาไม่มีการประทับตราและลงนามกำกับ

ข้อแนะนำ

องค์กรควรพิจารณาปรับปรุงแก้ไขกรมธรรม์ประกันภัยคอมพิวเตอร์ให้ถูกต้องและสมบูรณ์ และกรณีทำสัญญาประกันภัยในครั้งต่อไปควรพิจารณาความถูกต้องและสมบูรณ์ของสัญญาประกันภัยด้วย

1.4 คณะกรรมการบริหารงานคอมพิวเตอร์และบุคลากร

(1) การจัดองค์การไม่เหมาะสม

ศูนย์คอมพิวเตอร์ขององค์กรเป็นหน่วยงานอิสระ มีฐานะเทียบเท่าฝ่าย ขึ้นตรงต่อผู้บริหารระดับสูงขององค์กร ซึ่งองค์กรมอบหมายให้ควบคุมดูแลเฉพาะการปฏิบัติงานของศูนย์คอมพิวเตอร์และฝ่ายบริหารการเงิน และให้จัดทำรายงานเสนอคณะจัดการ (Management Committee) ซึ่งมีกรรมการผู้จัดการใหญ่เป็นประธาน ดังนั้นการกำหนดเป้าหมาย แผนงาน และการควบคุมการดำเนินงานคอมพิวเตอร์จึงเกิดมาจากแนวความคิดทางสายงานคอมพิวเตอร์ฝ่ายอื่น ๆ ซึ่งอยู่ในฐานะผู้ใช้ข้อมูลและประโยชน์จากคอมพิวเตอร์มิได้มีส่วนร่วมและรับผิดชอบในการจัดการดังกล่าว จึงอาจก่อให้เกิดการทำงานที่ไม่ประสานระหว่างศูนย์คอมพิวเตอร์ ฝ่ายผู้ใช้ประโยชน์จากคอมพิวเตอร์และฝ่ายตรวจสอบ ซึ่งจะส่งผลถึงความก้าวหน้าของการพัฒนาระบบงาน และความน่าเชื่อถือต่อระบบงานที่ใช้คอมพิวเตอร์

ข้อแนะนำ

องค์กรควรกำหนดให้ฝ่ายงานต่าง ๆ ที่เป็นผู้ใช้ข้อมูลและประโยชน์จากคอมพิวเตอร์มีส่วนร่วมและรับผิดชอบในการกำหนดเป้าหมาย แผนงาน และการควบคุมการดำเนินงานคอมพิวเตอร์ร่วมกับฝ่ายคอมพิวเตอร์ (หรือศูนย์คอมพิวเตอร์) เพื่อให้มีการทำงานที่ประสานกันระหว่างศูนย์คอมพิวเตอร์ ผู้ใช้ประโยชน์จากคอมพิวเตอร์และฝ่ายตรวจสอบ เพื่อความก้าวหน้าของการพัฒนาระบบงานและความน่าเชื่อถือต่อระบบงานที่ใช้คอมพิวเตอร์

(2) ไม่มีการแต่งตั้ง EDP Steering Committee

องค์กรไม่มีการแต่งตั้งคณะกรรมการนโยบายการใช้คอมพิวเตอร์หรือคณะกรรมการบริหารงานคอมพิวเตอร์ (EDP Steering Committee) เพื่อเข้าร่วมพิจารณาและกำหนดนโยบาย เป้าหมาย แผนงาน และการควบคุมการดำเนินงานด้านคอมพิวเตอร์ ซึ่งอาจทำให้การดำเนินงานด้านคอมพิวเตอร์ขององค์กรไม่สอดคล้องกับการปฏิบัติงานของส่วนงานต่าง ๆ หรือผู้ใช้งาน (User) และไม่ได้ใช้คอมพิวเตอร์เป็นเครื่องมือที่ช่วยเสริมให้การพัฒนาปรับปรุงงานและบริการให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ

ข้อแนะนำ

1) องค์กรกำหนดให้คณะกรรมการดำเนินงานด้านคอมพิวเตอร์ปฏิบัติหน้าที่อย่างครบถ้วน ดังนี้
   - พิจารณาและกำหนดนโยบาย เป้าหมาย และแผนการใช้คอมพิวเตอร์ในอนาคตทั้งระยะสั้น และระยะยาวที่ชัดเจน เพื่อให้ส่วนงานที่เกี่ยวข้องให้ความร่วมมือและยึดถือเป็นแนวทางในการปฏิบัติงาน
   - ให้ความเห็นชอบต่อโครงการคอมพิวเตอร์ซึ่งริเริ่มโดยส่วนงานต่าง ๆ

- จัดอันดับความสำคัญของโครงการคอมพิวเตอร์ รวมทั้งดูแลการใช้งานให้เป็นไปตามนโยบาย เป้าหมาย และแผนงานที่กำหนด
- จัดสรรทรัพยากรให้แก่โครงการต่าง ๆ
- กำหนดมาตรการในการรักษาความปลอดภัยและการควบคุมภายใน
- ให้ความเห็นชอบในการศึกษาและวิจัยเพื่อพัฒนางานคอมพิวเตอร์
- ให้ความเห็นชอบงบประมาณด้านคอมพิวเตอร์
- ติดตามขจัดปัญหาข้อขัดข้องเพื่อให้การดำเนินงานสำเร็จตามเป้าหมายอย่างมีประสิทธิภาพ

2) ควรกำหนดให้ศูนย์คอมพิวเตอร์จัดทำรายการสรุปผลการดำเนินงานของศูนย์ฯ แก่คณะกรรมการดำเนินงานด้านคอมพิวเตอร์ เพื่อให้ทราบถึงสถานะของโครงการต่าง ๆ พร้อมทั้งปัญหาและอุปสรรคที่เกิดขึ้น และผลกระทบที่ติดตามมา เพื่อหาวิธีการแก้ไขให้สามารถดำเนินการได้ตามเป้าหมาย

3) ควรกำหนดให้ศูนย์คอมพิวเตอร์จัดทำรายงานเสนอผู้บริหารของศูนย์ฯ เพื่อให้ผู้บริหารทราบผลการปฏิบัติงานในห้องคอมพิวเตอร์ การพัฒนาระบบงาน และเรื่องทั่ว ๆ ไป ซึ่งเป็นประโยชน์ต่อการควบคุมการปฏิบัติงานต่าง ๆ ของศูนย์ฯ ให้เป็นไปตามแผนงานที่วางไว้ และดำเนินงานได้อย่างราบรื่น

4) ควรจัดทำระเบียบหรือมาตรฐานการปฏิบัติงาน ซึ่งเป็นเอกสารที่สำคัญใช้อ้างอิงในการปฏิบัติงานให้ครบถ้วนทุกหน่วยงาน เช่น ระเบียบเกี่ยวกับระบบงานและโปรแกรมในเรื่องการออกแบบระบบงานและโปรแกรม การจัดทำโปรแกรม การทดสอบระบบงานและโปรแกรม เป็นต้น

5) การมอบหมายงานและการกำหนดระเบียบปฏิบัติ ควรกระทำเป็นลายลักษณ์อักษรไว้เป็นหลักฐานในการอ้างอิงและปฏิบัติงาน และหากเป็นงานที่ต้องใช้เวลานาน ควรให้มีการจัดทำรายงานผลความก้าวหน้าของงานนั้นเป็นระยะ ๆ ด้วย เพื่อให้การปฏิบัติเป็นไปอย่างถูกต้อง มีประสิทธิภาพ และสามารถควบคุมติดตามงานให้บรรลุตามเป้าหมาย

6) องค์กรควรบันทึกบัญชีสินทรัพย์ให้ถูกต้อง เพื่อจะได้ทราบผลการดำเนินงานที่แท้จริง ซึ่งสามารถใช้เป็นข้อมูลในการตัดสินใจต่อการบริหารงานในปัจจุบันและอนาคตได้ถูกต้องและเหมาะสม

7) สำนักงานใหญ่ควรกำหนดระเบียบปฏิบัติเกี่ยวกับการแก้ไขโปรแกรมเป็นลายลักษณ์อักษรให้มีรายละเอียดครบถ้วน เพียงพอ และชัดแจ้ง

8) องค์กรควรกำหนดระเบียบให้สาขาทำการปรับปรุงแก้ไขโปรแกรมชุดสำรองพร้อมกับชุดปฏิบัติงานจริง และให้จัดเก็บแผ่น Diskette ที่ใช้ในการแก้ไขโปรแกรมแล้วไว้ในที่ปลอดภัย เพื่อใช้เป็นหลักฐานในการอ้างอิงและตรวจสอบการแก้ไขโปรแกรมทุกครั้งด้วย

(3) ขาดการวางแผนบุคลากรที่ดี

องค์กรยังมิได้กำหนดคุณสมบัติของพนักงาน และจัดทำรายละเอียดลักษณะงาน (Job Description) ของพนักงานปฏิบัติการคอมพิวเตอร์ (Computer Operator) ซึ่งอาจมีผลให้องค์กรขาดแนวทางที่เหมาะสมในการสับเปลี่ยนโยกย้ายงาน การฝึกอบรมเพื่อเพิ่มพูนความรู้และความชำนาญให้แก่พนักงาน และอาจมีผลให้พนักงานขาดแนวทางในการควบคุมและปฏิบัติงานที่เหมาะสมได้

องค์กรยังมิได้กำหนดตัวพนักงานผู้ที่จะปฏิบัติงานทดแทนในด้านโปรแกรมหรือการบริหารงานคอมพิวเตอร์ ในกรณีที่ผู้จัดการฝ่ายบริการทางเทคนิค (Technical Service Department) ไม่สามารถปฏิบัติหน้าที่ได้ ซึ่งอาจมีผลให้การดำเนินงานขององค์กรล่าช้าหรือหยุดชะงัก นอกจากนี้องค์กรอยู่ระหว่างเตรียมการนำเครื่องคอมพิวเตอร์ที่มีขีดความสามารถในการประมวลผลสูงกว่าปัจจุบันมาใช้ในงานขององค์กรและธุรกิจในเครือ ซึ่งมีวิธีการปฏิบัติงานแตกต่างไปจากปัจจุบัน จึงมีความจำเป็นที่จะต้องเตรียมการและกำหนดตัวพนักงานผู้ปฏิบัติหน้าที่ทดแทนไว้ล่วงหน้า

องค์กรได้โยกย้ายสับเปลี่ยนพนักงานชั้นบริหารในฝ่ายคอมพิวเตอร์ค่อนข้างมาก การปฏิบัติดังกล่าวอาจมีผลกระทบต่อการดำเนินงานด้านคอมพิวเตอร์ได้

ข้อแนะนำ

องค์กรควรมีการวางแผนบุคลากรที่ดี โดยกำหนดคุณสมบัติของพนักงาน และจัดทำรายละเอียดลักษณะงาน (Job Description) ของพนักงานด้านคอมพิวเตอร์ และควรพิจารณาคัดเลือกพนักงานที่เหมาะสมเข้ารับการฝึกอบรมงานด้านโปรแกรมและการบริหารงานคอมพิวเตอร์ เพื่อให้สามารถปฏิบัติงานทดแทนผู้บริหารได้เมื่อจำเป็น

(4) ไม่มีการแบ่งแยกการปฏิบัติหน้าที่ของพนักงานให้เป็นไปตามหลักการควบคุมภายในที่ดี

องค์กรไม่ได้แยกหน้าที่ของเจ้าหน้าที่ที่ทำหน้าที่เปิดปิดและสั่งงานเครื่องคอมพิวเตอร์ (Operator) โดยให้มี User ID และ Password สำหรับการป้อนข้อมูลปรับปรุงหรือแก้ไขรายการในแฟ้มข้อมูลหลักของลูกค้าระบบงาน (application) ต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อองค์กรได้ หากมีการป้อนรายการผิดพลาด หรือทำรายการโดยไม่ได้รับอนุญาตจากพนักงานชั้นบริหาร เนื่องจากระบบงานไม่สามารถควบคุมและป้องกันการเข้าถึงแฟ้มข้อมูลการเงินที่สำคัญ รวมถึงอาจกระทบต่อความเชื่อถือได้ของข้อมูลจากระบบงานคอมพิวเตอร์ได้

ข้อแนะนำ

องค์กรควรแยกพนักงานที่ทำหน้าที่ป้อนข้อมูลในระบบงานต่าง ๆ ออกจากพนักงานที่ทำหน้าที่เปิดปิดและสั่งงานเครื่องคอมพิวเตอร์ และควรให้พนักงานรับทราบ User ID และ Password เฉพาะระบบงานที่ตนเองรับผิดชอบเท่านั้น เพื่อประโยชน์ในการควบคุมการปฏิบัติงานตามขั้นตอน และอยู่ภายใต้การควบคุมและอนุมัติรายการจากพนักงานชั้นบริหาร อีกทั้งยังเป็นการป้องกันข้อผิดพลาดของการป้อนข้อมูลและการสูญหายของเอกสารหลักฐานเมื่อมีการเคลื่อนย้ายจากแผนกงานหนึ่งไปยังอีกแผนกหนึ่งด้วย

องค์กรไม่ได้แบ่งแยกหน้าที่บุคลากรปฏิบัติงานป้อนข้อมูลเข้า เครื่องจักรและบัญชี จากผู้ที่ทำหน้าที่รวบรวมและกระทบยอด Slip ในตอนสิ้นวัน และการกระทบยอดรวมสิ้นวันไม่มีการสอบทานและตรวจสอบความสมบูรณ์ของ Slip อีกครั้ง ซึ่งอาจเป็นช่องทางให้เกิดการรวมเอา Slip ที่ยังไม่ได้ผ่านการอนุมัติและตรวจสอบการบันทึกรายการโดยผู้มีอำนาจ และอาจเป็นเหตุให้สถาบันการเงินเสียหายได้

ข้อแนะนำ

ควรแบ่งแยกหน้าที่ป้อนข้อมูลเข้าเครื่องจักรกับบัญชี หรือเครื่องคอมพิวเตอร์ ซึ่งองค์กรกำลังจะนำเข้ามาใช้ในอนาคต ออกจากผู้มีหน้าที่รวบรวมและกระทบยอดรวม Slip ในตอนสิ้นวัน และในการรวมยอด Slip สิ้นวัน ควรมีการสอบทานและตรวจสอบความสมบูรณ์ของ Slip อีกครั้งหนึ่ง

สาขาได้ให้พนักงานเทลเลอร์ ซุปเปอร์ไวเซอร์ด้านการบัญชีและการเงินจำนวน 3 คน หมุนเวียนกันไปทำหน้าที่ด้านการประมวลผลและด้านการเก็บรักษาอุปกรณ์ต่าง ๆ คนละ 1 วัน แต่ในระหว่างเวลาที่พนักงานที่รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลและเก็บรักษาอุปกรณ์ในห้องคอมพิวเตอร์ขณะนั้นก็ยังไปช่วยปฏิบัติงานติดต่อกับลูกค้าที่ Counter ของสาขาในบางเวลาด้วย ซึ่งไม่สอดคล้องกับหลักการควบคุมภายใน และหน้าที่ที่กำหนดไว้ในคำสั่งและระเบียบปฏิบัติงานขององค์กร

ข้อแนะนำ

ในกรณีที่จำเป็นต้องให้พนักงานที่หมุนเวียนไปทำหน้าที่ด้านการประมวลผลและเก็บรักษาอุปกรณ์ ไปปฏิบัติหน้าที่อื่นในขณะใดขณะหนึ่ง ก็ควรให้อยู่ในความดูแลของพนักงานบริหารสาขาโดยใกล้ชิด

จากการตรวจสอบการปฏิบัติงานขององค์กร พบว่าหน้าที่สำคัญบางด้านมีการใช้พนักงานไม่เหมาะสม เช่น องค์กรได้ให้พนักงาน Clearing พนักงานทำความสะอาด และพนักงานเดินเอกสาร มาให้บริการด้านเงินฝากกับลูกค้า และพนักงานแผนก Forex ซึ่งมีหน้าที่ในการจัดทำเอกสารเบื้องต้น มาทำหน้าที่ด้านการป้อนข้อมูลที่แผนกบัญชีและคอมพิวเตอร์ด้วย การปฏิบัติดังกล่าวอาจเกิดจุดอ่อนด้านการควบคุมภายใน และอาจทำให้องค์กรได้รับความเสียหายด้านการเงินได้

ข้อแนะนำ

องค์กรควรประเมินและกำหนดให้พนักงานปฏิบัติงานตามหน้าที่ ให้เหมาะสมกับตำแหน่งงานโดยไม่ขัดต่อหลักการควบคุมภายในที่ดี

(5) ปัญหาจากการดำเนินงานด้านคอมพิวเตอร์ที่เกิดจากการช่วยเหลือโดยบุคคลภายนอก

- การช่วยเหลือในการพิจารณาจัดซื้อเครื่องคอมพิวเตอร์ไม่เหมาะสม เป็นผลให้องค์กรต้องซื้อเครื่องคอมพิวเตอร์ชุดใหม่เพิ่มขึ้น
- ต้องอาศัยเอกสารสนับสนุนระบบงานจากบุคคลภายนอกซึ่งมีไม่ครบถ้วนสมบูรณ์ ซึ่งในระยะแรกองค์กรมีความจำเป็นต้องอาศัยความช่วยเหลือด้านคอมพิวเตอร์จากบุคคลภายนอก

ข้อแนะนำ

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นจากการใช้เอกสารสนับสนุนระบบงานที่ไม่ถูกต้อง องค์กรควรดำเนินการปรับปรุงแก้ไขเอกสารสนับสนุนระบบงานที่ได้รับจากบุคคลภายนอกให้ถูกต้องครบถ้วนสมบูรณ์ สอดคล้องกับโปรแกรมระบบงานที่องค์กรได้นำมาใช้โดยเร็ว

1.5 การรายงานผลการปฏิบัติงานคอมพิวเตอร์ไม่เป็นลายลักษณ์อักษร

(1) ไม่มีการมอบหมายงาน การรายงานผลการดำเนินงาน และการกำหนดระเบียบปฏิบัติงานเป็นลายลักษณ์อักษร

- การมอบหมายงานส่วนใหญ่จะสั่งการด้วยวาจา ทำให้ขาดหลักฐานอ้างอิง ไม่สามารถควบคุมและติดตามการปฏิบัติงานได้เท่าที่ควร ความเข้าใจระหว่างผู้บังคับบัญชาสั่งการกับผู้รับคำสั่งอาจคลาดเคลื่อนไม่ถูกต้องตรงกัน และเกิดข้อผิดพลาดในการปฏิบัติงาน นอกจากนี้ผู้มอบหมายงานอาจหลงลืมไม่ติดตามงานที่ได้มอบหมายซึ่งจะทำให้องค์กรได้รับความเสียหายได้

- ฝ่ายคอมพิวเตอร์รายงานผลการปฏิบัติงานโดยตรงต่อผู้บริหารระดับสูงที่รับผิดชอบด้วยวาจาอย่างไม่เป็นทางการ และไม่มีระเบียบข้อบังคับเป็นลายลักษณ์อักษรกำหนดให้ผู้ปฏิบัติงานด้านคอมพิวเตอร์ จัดทำรายงานผลการดำเนินงาน ของศูนย์คอมพิวเตอร์ในแต่ละเรื่องเสนอแก่ผู้บริหารศูนย์คอมพิวเตอร์ ซึ่งจะมีผลทำให้องค์กรไม่ได้รับทราบปัญหาและอุปสรรคในการดำเนินงานด้านนี้เป็นลายลักษณ์อักษร และไม่ทราบว่าได้มีการแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นเพียงใด นอกจากนี้ทำให้องค์กรไม่มีเอกสารและหลักฐานในการพิจารณาประกอบการตัดสินใจ อันจะเป็นประโยชน์ต่อการติดตามการควบคุม เปลี่ยนแปลง แก้ไข และการวางแผนการใช้คอมพิวเตอร์ขององค์กรในอนาคต

- องค์กรไม่ได้กำหนดระเบียบการปฏิบัติงานด้านคอมพิวเตอร์ ทำให้ผู้ปฏิบัติงานขาดแนวทางในการปฏิบัติงาน องค์กรต้องพึ่งพาอาศัยตัวบุคคลที่คุ้นเคยสำหรับในแต่ละด้านค่อนข้างมาก ไม่สามารถสับเปลี่ยนพนักงานให้ปฏิบัติงานทดแทนกันได้ นอกจากนี้หากมีปัญหาในการปฏิบัติงานในกรณีที่มีผู้ปฏิบัติงาน ไม่เคยมีประสบการณ์มาก่อน การดำเนินการแก้ปัญหาโดยไม่มีแนวทางที่แน่ชัด อาจทำให้ข้อมูลทางการเงินมีข้อผิดพลาดและก่อให้เกิดความเสียหายต่อองค์กรได้

ข้อแนะนำ

องค์กรควรมีระเบียบข้อบังคับเป็นลายลักษณ์อักษรเกี่ยวกับการกำหนดให้ฝ่ายคอมพิวเตอร์จัดทำรายงานเสนอผู้บริหารที่รับผิดชอบงานด้านคอมพิวเตอร์ เช่น รายงานประจำสัปดาห์ รายเดือน รายงวด เป็นต้น

รายงานที่ควรจัดทำเสนอผู้บริหาร ได้แก่

1) รายงานเหตุการณ์หรือความเสียหายที่เกิดจากโปรแกรมสั่งงาน หรือเครื่องมือต่าง ๆ
2) รายงานเวลาที่ใช้ในการจัดทำโปรแกรมขึ้นใหม่ การปรับปรุงแก้ไข และการทดสอบโปรแกรม
3) รายงาน Down time ของเครื่องคอมพิวเตอร์
4) รายงานการใช้ Utility program แก้ไขข้อผิดพลาดของโปรแกรมและข้อมูล

5) รายงานจำนวนรายงานที่ให้เครื่องคอมพิวเตอร์จัดทำขึ้นเป็นพิเศษ

6) รายงานแสดงการเปรียบเทียบความก้าวหน้าในการพัฒนาระบบงานและโปรแกรมกับโครงการที่ธนาคารวางไว้

7) รายงานการทำงานล่วงเวลา

(2) **ไม่มีระเบียบปฏิบัติเกี่ยวกับการรายงานปัญหาและอุปสรรคในการประมวลผลข้อมูล**

สำนักงานใหญ่ไม่ได้กำหนดระเบียบปฏิบัติในการรายงานปัญหา และอุปสรรคในการประมวลผลข้อมูล เป็นผลให้สาขาขาดแนวทางในการปฏิบัติในเรื่องที่เกี่ยวข้อง เช่น

- เมื่อเกิดปัญหาในการใช้ Audit Trail Utility ทำให้สาขาหยุดใช้ Utility ดังกล่าว เป็นผลให้ธนาคารขาดข้อมูลที่ใช้ในการควบคุมและตรวจสอบการปฏิบัติงานด้านคอมพิวเตอร์
- ผู้ใช้ข้อมูลเปลี่ยนแปลงแบบฟอร์มข้อมูลนำเข้า (Input Form) ด้วยตนเอง เป็นผลให้ไม่สามารถตรวจสอบความถูกต้องของข้อมูลตามแบบฟอร์มมาตรฐานขององค์กรได้

ข้อแนะนำ

สำนักงานใหญ่ควรกำหนดระเบียบปฏิบัติให้สาขารายงานปัญหาที่เกิดขึ้นเพื่อเป็นแนวทางปฏิบัติในแต่ละกรณี ในระหว่างที่ยังไม่มีระเบียบปฏิบัตินี้ สาขาควรแจ้งปัญหาด้านคอมพิวเตอร์ที่เกิดขึ้นเป็นลายลักษณ์อักษรให้ทางสำนักงานใหญ่ทราบ เพื่อกำหนดวิธีการแก้ไขปัญหาให้สาขาโดยเร็ว

(3) **ไม่มีระเบียบปฏิบัติเกี่ยวกับการแก้ไขโปรแกรมเป็นลายลักษณ์อักษร**

- สาขาได้รับแจ้งจากสำนักงานใหญ่ด้วยวาจาว่า ห้ามมิให้สาขาแก้ไขโปรแกรมระบบงาน A ทำให้พนักงานสาขาเข้าใจว่าสามารถแก้ไขโปรแกรมอื่นนอกเหนือจาก A ได้
- ในกรณีที่มีการแก้ไขโปรแกรม A ทางสำนักงานใหญ่จะจัดส่งโปรแกรมที่แก้ไขไว้ในแผ่น Diskette เพื่อให้สาขาทำการแก้ไขโปรแกรมชุดปฏิบัติงานจริง แต่มิได้กำหนดให้ทำการแก้ไขโปรแกรมชุดสำรอง (Program Backup) พร้อมกันไปด้วย และไม่ได้จัดเก็บแฟ้ม Diskette ดังกล่าวไว้ในที่ปลอดภัย
- การแก้ไขโปรแกรมตามที่ทางสำนักงานใหญ่ส่งมาให้ทำนั้น เมื่อพนักงานปฏิบัติงานได้แก้ไขแล้ว จะเก็บคำสั่งนั้นเข้าแฟ้มได้ แต่มิได้บันทึกการแก้ไขนั้นไว้เป็นหลักฐานเพื่อใช้สอบทานการปฏิบัติงานภายหลังที่ได้แก้ไขอะไรบ้างแล้ว ใครเป็นผู้แก้ไข และแก้ไขเมื่อใด



1.6 การรักษาความปลอดภัย

ไม่มีการติดตั้งเครื่องเตือนภัยและอุปกรณ์ดับเพลิง

ภายในห้องคอมพิวเตอร์ขององค์กรไม่ได้ติดตั้งอุปกรณ์และเครื่องมือ เตือนภัยเบื้องต้นที่จำเป็น เช่น เครื่องจับควันไฟ (Smoke Detector) เครื่องจับความร้อน (Heat Detector) เครื่องวัดความชื้น และอุปกรณ์ดับเพลิง เป็นต้น ประกอบกับโดยปกติแล้วไม่มีพนักงานประจำห้องคอมพิวเตอร์ และจะปิดประตูล็อคกุญแจไว้ ซึ่งจากสภาพดังกล่าวจะมีความเสี่ยงที่จะเกิดไฟไหม้ห้องคอมพิวเตอร์ ทำให้อุปกรณ์คอมพิวเตอร์ และ Data File เสียหายในเกณฑ์สูง

ข้อแนะนำ

องค์กรควรติดตั้งระบบ Heat/Smoke Detector ไว้ในห้องคอมพิวเตอร์เช่นเดียวกับห้องอื่น ๆ ของธนาคาร และในโอกาสต่อไปหากมีการปรับปรุงห้องคอมพิวเตอร์ควรใช้อุปกรณ์และวัสดุทนไฟ

1.7 อื่น ๆ

(1) **การควบคุมการรับ-ส่งเอกสารไม่รัดกุม**

- ในการรับเอกสารจากสาขาต่าง ๆ เพื่อทำการเตรียมข้อมูลเกี่ยวกับชื่อ ที่อยู่ของลูกค้า สาขาไม่มีการบันทึกรับเอกสารที่ได้รับจากสาขาต่าง ๆ ซึ่งอาจทำให้มีข้อมูลบางส่วนขาดหายไป
- การจัดส่งรายงานทางการเงินโดยบรรจุในซองกระดาษ และไม่มีพนักงานควบคุมการจัดส่งรายงานอย่างใกล้ชิด อาจเป็นช่องทางให้ข้อมูลทางการเงินซึ่งเป็นความลับของลูกค้า รั่วไหลหรือสูญหายได้โดยง่าย เนื่องจากมิได้ทำข้อตกลงในการรับส่งเอกสารไว้เป็นลายลักษณ์อักษร
- การส่งรายงานให้สาขา ใช้วิธีบรรจุซองแล้วนำไปฝากรถแท็กซี่ โดยให้คนขับรถเป็นคนเซ็นรับ อาจไม่ปลอดภัย และไม่จัดทำทะเบียนรับ-ส่งรายงานระหว่างสาขาต่าง ๆ นอกจากนี้ยังปรากฏการส่งรายงานบางประเภทผิดสาขาด้วย เช่น ในรายงานของสาขาหนึ่งมีรายงานของสาขาอื่นรวมอยู่ด้วย

ข้อแนะนำ

องค์กรควรกำหนดระเบียบควบคุมการรับ-ส่งเอกสารต่างๆ ระหว่างสาขาและสาขากับสำนักงานใหญ่ พร้อมทั้งจัดทำทะเบียนรับ-ส่งรายงานให้ครบทุกสาขา

(2) **การควบคุมเอกสารบางประเภทไม่รัดกุม**

องค์กรไม่ได้กำหนดประเภทของเอกสารคอมพิวเตอร์ เช่น คู่มือ (Manual) ต่าง ๆ ที่ได้รับจากบริษัทผู้ขายเครื่องคอมพิวเตอร์ ว่าเล่มใดสมควรให้พนักงานผู้ปฏิบัติหน้าที่ใดขอยืมไปอ่านได้ ซึ่งไม่สอดคล้องกับหลักการควบคุมภายในเท่าที่ควร อาจมีผลกระทบต่อการรักษาความปลอดภัยของระบบคอมพิวเตอร์

(3) **การควบคุมการแก้ไขข้อมูลไม่รัดกุม**

พนักงานผู้รับผิดชอบในการแก้ไขข้อมูลไม่ได้ลงนามกำกับการแก้ไขข้อมูลในใบ Input form ให้ครบถ้วนทุกรายการ เพื่อแสดงว่าได้มีการควบคุมดูแลการแก้ไขข้อมูลโดยใกล้ชิด

(4) **การปฏิบัติงานด้านเงินฝากและบัญชีเดินสะพัด** (CIS-DEPOSIT)

ในระบบ On-line ของธนาคาร ปัจจุบันจำเป็นต้องใช้พนักงานถึง 2 คนต่อเครื่อง Terminal 1 เครื่อง โดยมีพนักงาน Checker ควบคุมดูแลการปฏิบัติงานของพนักงาน Teller อยู่ตลอดเวลา ทำให้การปฏิบัติงานไม่คล่องตัวเท่าที่ควร และทำให้ต้นทุนหรือค่าใช้จ่ายในการทำรายงานอยู่ในเกณฑ์ค่อนข้างสูง

(5) **การควบคุมการอนุมัติรายการโดยมอบบัตรให้พนักงานชั้นบริหาร**

การอนุมัติรายการโดยมอบบัตรให้พนักงานชั้นบริหารถือไว้สำหรับใช้อนุมัติการผ่านรายการแทน Supervisor key ยังมีปัญหาในทางปฏิบัติเช่นเดียวกัน โดยพนักงานชั้นบริหารอาจมอบบัตรให้ผู้ปฏิบัติงานถือได้ตลอดเวลา ซึ่งจะมีผลคล้ายกับการเสียบกุญแจ Supervisor ลงเครื่อง Terminal และไม่มีพนักงานชั้นบริหารรับรู้การปฏิบัติงานตามระเบียบขององค์กรอย่างแท้จริง ทำให้เกิดจุดอ่อนในการควบคุมภายใน

ข้อแนะนำ

ควรปรับปรุงระบบควบคุมการใช้บัตรของพนักงานชั้นบริหารในการอนุมัติรายการให้รัดกุมยิ่งขึ้น

(6) **การปฏิบัติงานของศูนย์คอมพิวเตอร์ยังไม่เป็นไปตามลักษณะงานของส่วนงานที่องค์กรกำหนด**

โดยรวมงานควบคุมและปฏิบัติการเข้ากับงานพัฒนาระบบงาน และไม่ได้แยกหน้าที่ operator ออกจาก programmer อย่างชัดเจน อันเป็นจุดอ่อนในการควบคุมด้านคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งในระบบ on-line

(7) **องค์กรไม่ได้กำหนดมาตรฐานหรือระเบียบปฏิบัติการด้านต่าง ๆ เพื่อใช้เป็นแนวทางในการปฏิบัติงานและควบคุมงานได้อย่างมีประสิทธิภาพ**

ข้อแนะนำ

องค์กรควรจัดทำระเบียบและคู่มือที่จำเป็นสำหรับการดำเนินงานคอมพิวเตอร์ ดังนี้

- การปฏิบัติการคอมพิวเตอร์ (Operation)
- การรักษาความปลอดภัย (Security)
- การปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan)
- การปรับปรุงแก้ไขระบบคอมพิวเตอร์และข้อมูลที่ได้รับความเสียหายให้กลับคืนสู่ภาวะปกติ (Recovery Plan)

(8) **ความถูกต้องของเอกสารสัญญา**

- การอ้างอิงในเอกสารสัญญาไม่ถูกต้องครบถ้วน เช่น เอกสารสัญญาซ่อมบำรุงเครื่องได้อ้างถึงข้อ 7.5 แต่ไม่ปรากฏข้อ 7.5 ดังอ้างถึง ซึ่งอาจทำให้สัญญาข้อที่มีการกล่าวถึงและ/หรืออ้างอิง ไม่มีผลใช้บังคับตามกฎหมาย
- กรมธรรม์ประกันภัยแบบ Co-Insurance ระบุวงเงินรับผิดไม่ตรงกัน

(9) **เอกสารสนับสนุนการปฏิบัติงานขาดรายละเอียดที่จำเป็นต่อการปฏิบัติงานไม่เป็นปัจจุบัน และการเก็บรักษาไม่รัดกุม**

เอกสารสนับสนุนการปฏิบัติงานขาดรายละเอียดเกี่ยวกับผังทางเดินของระบบงาน (Work Flow) ซึ่งแสดงขั้นตอนการทำงานของระบบงานต่าง ๆ ตั้งแต่จุดกำเนิดข้อมูล การเตรียมข้อมูล การนำข้อมูลเข้าประมวลผล การจัดเก็บข้อมูล และการจัดส่งรายงานให้ผู้ใช้ข้อมูล และมิได้ติดตามปรับปรุงเอกสารสนับสนุนการปฏิบัติงานของระบบงานให้เป็นปัจจุบันตลอดเวลา ทำให้ไม่สามารถใช้เป็นแนวทางในการควบคุมและสนับสนุนการปฏิบัติงานอย่างมีประสิทธิภาพ รวมทั้งใช้ฝึกอบรมพนักงานเมื่อมีการสับเปลี่ยนหรือโยกย้ายได้ และยังทำให้ขาดหลักฐานและไร้ร่องรอยหรือแนวทางในการควบคุมและตรวจสอบติดตามได้ในที่สุด นอกจากนี้การเก็บรักษาเอกสารยังมีข้อบกพร่องบางประการดังนี้

มิได้กำหนดประเภทความสำคัญของเอกสารที่พนักงานระดับใดบ้างสามารถใช้งานได้ เพื่อป้องกันการเข้าถึงระบบงานที่อาจทำให้องค์กรได้รับความเสียหาย

- องค์กรเก็บเอกสารสนับสนุนการปฏิบัติงานและคู่มือต่าง ๆ ที่ได้รับจากผู้ขายไว้ในห้องเก็บพัสดุ ซึ่งพนักงานทั่วไปสามารถเข้าถึงได้ นอกจากนี้ยังเก็บเอกสารเกี่ยวกับการรักษาความปลอดภัยของระบบงานไว้ในห้องคอมพิวเตอร์ ซึ่งอาจมีผู้นำไปใช้โดยมิได้รับอนุญาต และเข้าถึงระบบงานโดยผ่านระบบป้องกันและรักษาความปลอดภัยไปได้
- มิได้จัดทำทะเบียนควบคุมการยืมและคืนเอกสารตามที่กล่าวข้างต้นไว้เป็นหลักฐาน

ข้อแนะนำ

นอกจากองค์กรจะได้กำหนดและจัดประเภทความสำคัญของ เอกสารที่พนักงานระดับต่าง ๆ สามารถเข้าถึงและใช้ได้ พร้อมทั้งจัดทำทะเบียนควบคุมการนำไปใช้และคืน โดยมีพนักงานรับผิดชอบโดยเฉพาะแล้ว องค์กรควรจัดเก็บเอกสารสนับสนุนการปฏิบัติงานไว้ในที่ปลอดภัยด้วย เช่น ล็อคกุญแจ เป็นต้น

(10) **ไม่มีหนังสือรับรองความถูกต้องของข้อมูลก่อนนำมาใช้ประมวลผลในระบบคอมพิวเตอร์**

ศูนย์คอมพิวเตอร์มิได้กำหนดรูปแบบการรับรองความถูกต้องในการเปลี่ยนแปลงระบบข้อมูลในระบบคอมพิวเตอร์จากหน่วยงานที่เกี่ยวข้อง ได้แก่ ตัวแทนจากฝ่ายตรวจสอบ ศูนย์คอมพิวเตอร์ และสาขาที่จะใช้ข้อมูลในระบบคอมพิวเตอร์ อันอาจมีผลต่อความถูกต้องของข้อมูล ตลอดจนการแบ่งแยกความรับผิดชอบเมื่อเกิดปัญหาในการปฏิบัติงาน

ข้อแนะนำ

ควรจัดให้มีหนังสือตรวจรับการเปลี่ยนระบบข้อมูลสาขา เพื่อนำเข้าระบบคอมพิวเตอร์จากหน่วยงานที่เกี่ยวข้อง เพื่อแบ่งแยกความรับผิดชอบเมื่อเกิดปัญหาในการปฏิบัติงาน

(11) **ไม่มีหลักฐานแสดงแหล่งที่มาของข้อมูล**

องค์กรเตรียมข้อมูลการจ่ายเงินเดือนตำรวจ โดยเจ้าหน้าที่เตรียมข้อมูลรับเอกสารจากกอง-บัญชาการตำรวจนครบาลโดยตรง ไม่ผ่านเจ้าหน้าที่ผู้รับมอบอำนาจขององค์กร และเมื่อเตรียมข้อมูลเสร็จ องค์กรได้คืนเอกสารรายการเงินเดือนให้กองบัญชาการตำรวจนครบาลทั้งหมด หากมีปัญหาข้อโต้แย้งเกิดขึ้นภายหลัง องค์กรอาจเสียหายได้

(12) **การควบคุมและประเมินผลการใช้เครื่องคอมพิวเตอร์ขนาดเล็ก**

ปัจจุบันองค์กรมีเครื่องคอมพิวเตอร์ขนาดเล็ก (Micro computer) เป็นจำนวนมากกระจัดกระจายอยู่ตามหน่วยงานต่าง ๆ รวมทั้งผู้บริหารระดับสูงขององค์กร อีกทั้งแนวโน้มในอนาคตแสดงให้เห็นว่าจะมีการนำคอมพิวเตอร์ขนาดเล็กมาใช้กันมากขึ้น ซึ่งจะส่งผลกระทบกับการดำเนินงานขององค์กรได้ หากไม่มีการกำหนดมาตรการในการควบคุมดูแลและติดตามการลงทุน การปฏิบัติงาน การรักษาความปลอดภัย และการควบคุมภายใน ก็อาจส่งผลให้องค์กรได้รับความเสียหายได้

1.2 การตรวจสอบภายใน

(1) ไม่มีการตรวจสอบภายในด้านคอมพิวเตอร์

องค์กรไม่มีการตรวจสอบและประเมินผลการควบคุมภายในของระบบงานคอมพิวเตอร์อย่างสม่ำเสมอ อันอาจทำให้การปฏิบัติงานเกิดข้อผิดพลาดได้

ข้อแนะนำ

องค์กรควรจัดให้มีการตรวจสอบและประเมินระบบการควบคุมภายใน ของระบบงานคอมพิวเตอร์เป็นครั้งคราวอย่างน้อยปีละหนึ่งครั้ง

(2) การตรวจสอบภายในไม่ครอบคลุมงานคอมพิวเตอร์อย่างเพียงพอ

การตรวจสอบภายในด้านคอมพิวเตอร์ขององค์กรไม่ครอบคลุมงานด้านคอมพิวเตอร์อย่างเพียงพอ ไม่เป็นไปตามประกาศ/ข้อกำหนดที่เกี่ยวข้อง เนื่องจากการพัฒนาผู้ตรวจสอบงานด้านนี้ยังล่าช้ากว่าการพัฒนาด้านคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนในการควบคุมงานด้านนี้

ข้อแนะนำ

องค์กรควรกำหนดขอบเขตการตรวจสอบภายในให้ครอบคลุมงานด้านคอมพิวเตอร์อย่างเพียงพอตามประกาศ/ข้อกำหนดที่เกี่ยวข้อง และเร่งพัฒนาผู้ตรวจสอบด้านคอมพิวเตอร์อย่างจริงจัง

(3) ไม่มีการจัดทำแผนการตรวจสอบด้านคอมพิวเตอร์

องค์กรไม่ได้กำหนดให้ส่วนงานที่รับผิดชอบในการตรวจสอบด้านคอมพิวเตอร์จัดทำแผนการตรวจสอบ และงบประมาณการตรวจสอบประจำปีเสนอฝ่ายบริหาร เพื่อพิจารณาความเหมาะสมและสอดคล้องกับนโยบายการพัฒนา และการขยายงานด้านคอมพิวเตอร์ขององค์กร โดยไม่ได้กำหนดระยะเวลาและขอบเขตการตรวจสอบอย่างชัดเจน เพื่อให้ครอบคลุมการปฏิบัติงานของส่วนงานต่าง ๆ ไม่ได้กำหนดหลักเกณฑ์ที่ใช้ในการคัดเลือกงานตรวจสอบความถี่ของการตรวจสอบและการจัดลำดับความสำคัญของงานที่ตรวจสอบ สำหรับใช้เป็นแนวทางในการวางแผนงานตรวจสอบ ทำให้การตรวจสอบไม่ครอบคลุมในบางเรื่อง เช่น

- การเข้าร่วมพัฒนาระบบงานและโปรแกรมในโครงการต่าง ๆ
- การตรวจสอบการปรับปรุงแก้ไขระบบงานและโปรแกรม
- การตรวจสอบการปฏิบัติงานตามระเบียบ คำสั่ง และข้อกำหนดของระบบงานของพนักงานสาขาในเครือข่ายระบบ on-line ซึ่งเป็นผู้ใช้ระบบที่สามารถเข้าถึงข้อมูลที่สำคัญของลูกค้าได้โดยตรง



บทที่ 15

ประสบการณ์ (บางส่วน) ในการตรวจสอบการปฏิบัติ “งาน” หรือ “Application” (Application Audit/Application Controls) ของประเทศต่าง ๆ

ประสบการณ์ (บางส่วน) ในการตรวจสอบการปฏิบัติ "งาน" หรือ "Application" (Application Audit/Application controls) ของประเทศต่าง ๆ

1. บทนำ

การตรวจสอบ "งาน" (Application) ในองค์กรที่ใช้คอมพิวเตอร์นั้นเป็นหัวใจของ Internal Auditor ไม่ว่าจะเป็น IS Auditor หรือ Regular Auditor เพราะการตรวจสอบ "งาน" (Application) นั้น ผู้ตรวจสอบเข้าใกล้กับเป้าหมายการตรวจสอบหลักของ Auditor นั่นคือ การตรวจ Compliance Audit ที่เน้นการตรวจสอบการปฏิบัติตามนโยบายคำสั่ง ระเบียบ วิธีการปฏิบัติงาน ฯลฯ ขององค์กร รวมทั้งการนำ Substantive Test ที่เป็นการตรวจสอบรายการทางการเงิน ประกอบตามความจริงเป็นบางส่วน เพื่อสนับสนุนการตรวจ Compliance Audit นั้นเป็นการเข้าใกล้คนและงานภายในองค์กรมากที่สุด

หลักการตามที่ผมได้กล่าวไว้ในเรื่องประสบการณ์ของประเทศต่าง ๆ ในการดำเนินงานด้านคอมพิวเตอร์ (Data Center/General Controls) ในบทก่อนนั้นสามารถนำมาใช้กับกรณีการตรวจสอบ "งาน" (Application) ได้เป็นส่วนใหญ่ จึงไม่ขอกล่าวซ้ำอีกแต่ใคร่ขอเน้นว่า "จุดอ่อน" ของงานหรือระบบงาน หากไม่แก้ไขในเวลาอันควรหลังจาก ได้รับคำแนะนำจากผู้ตรวจสอบแล้ว อาจเป็นภัยที่ถึงองค์กรและก่อให้เกิดความเสียหายทั้งกรณีปกติและกรณี "ทุจริต" ได้เสมอ เพราะจากประสบการณ์นั้น มีหลายกรณีที่ผู้ตรวจสอบเคยแนะนำองค์กรให้แก้ไขแล้ว แต่องค์กรไม่ได้แก้ไขในเวลาอันควร จุดอ่อนนั้น ๆ ก็มีผู้ไม่หวังดีปฏิบัติการ "ทุจริต" จริง ๆ ที่ก่อให้เกิดความเสียหายหลายกรณีต่อองค์กรในเวลาต่อมา

ต่อไปนี้ เป็นประสบการณ์ในช่วง พ.ศ. 2525 - 2532 ในการตรวจสอบทางด้าน "งาน" (Application) โดยพยายามจัดลำดับเป็นหมวดหมู่ของ "งาน" ที่เกี่ยวข้อง

2 ระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ (Application)

2.1 ระบบงานและโปรแกรม

1) มาตรฐานการพัฒนาระบบงานและโปรแกรมไม่สมบูรณ์

ส่วนวิเคราะห์และพัฒนาระบบ ซึ่งมีหน้าที่รับผิดชอบในการพัฒนาระบบงานใหม่และปรับปรุงระบบงานได้เริ่มกำหนดมาตรฐานเป็นการภายในสำหรับควบคุมการพัฒนาระบบงาน คือ แบ่งงานพัฒนาระบบงานออกเป็นขั้นตอนมาตรฐาน 4 ขั้นตอน ได้แก่ การวิเคราะห์ระบบ การออกแบบระบบ การจัดทำและทดสอบโปรแกรม และการนำระบบออกใช้ปฏิบัติงาน และให้เจ้าหน้าที่ผู้รับผิดชอบแต่ละขั้นตอนรายงานผลการปฏิบัติงานทุกเดือน สิ่งที่ยังขาดอยู่ก็คือ มาตรฐานเกี่ยวกับวิธีปฏิบัติและเอกสารที่จะต้องจัดทำขึ้นประกอบการปฏิบัติงานในขั้นตอนต่าง ๆ ตามที่ได้กำหนดข้างต้น

ข้อแนะนำ

ในการควบคุมการพัฒนาระบบงานให้ได้ประสิทธิภาพนั้น นอกจากจะมีการแบ่งแยกงานออกเป็นงานย่อย เพื่อสะดวกและง่ายต่อการปฏิบัติงานและการรายงานแล้ว ควรจะมีการกำหนดมาตรฐานเกี่ยวกับวิธีปฏิบัติซึ่งผู้รับผิดชอบจะได้ใช้เป็นแนวทางในการปฏิบัติงานตามที่ได้รับมอบหมาย นอกจากนี้ยังสามารถใช้เป็นเครื่องมือในการวัดผลการปฏิบัติงานด้วยว่าตรงกับที่กำหนดไว้ และทันกับแผนงาน

ระเบียบและวิธีปฏิบัติในรายละเอียดที่ศูนย์คอมพิวเตอร์ควรพิจารณากำหนดขึ้น ได้แก่ ระเบียบและวิธีปฏิบัติในการวิเคราะห์ระบบ การออกแบบระบบ การจัดทำโปรแกรม การทดสอบระบบ การนำระบบออกใช้งาน และการปรับปรุงแก้ไขโปรแกรม

2) **มีข้อบกพร่องเกี่ยวกับมาตรฐานในการจัดทำระบบงานและโปรแกรม**

สถาบันการเงินไม่ได้กำหนดมาตรฐานระเบียบปฏิบัติงานหรือคู่มือเกี่ยวกับการพัฒนาระบบงาน (System Development Standard) เป็นลายลักษณ์อักษร ซึ่งเป็นส่วนสำคัญของการดำเนินงานด้านคอมพิวเตอร์ เพื่อให้พนักงานที่มีหน้าที่ในการพัฒนาระบบงานและโปรแกรมยึดถือเป็นแนวทางในการปฏิบัติงาน และจัดทำเอกสารสนับสนุนระบบงานในขั้นตอนต่าง ๆ ให้มีรูปแบบเดียวกัน หรือในบางกรณีมีมาตรฐานดังกล่าวแต่ไม่ได้กล่าวถึงเรื่องที่สำคัญบางเรื่อง คือ

- หลักเกณฑ์การพิจารณาจัดหาโปรแกรมสำเร็จรูป
- การจัดทำโปรแกรมตรวจสอบความถูกต้องของข้อมูลนำเข้า
- การจัดให้มีข้อมูล และหลักฐานที่ควรมีไว้ตรวจสอบ (Audit trail)
- การกำหนดให้มีจุดตรวจสอบ (Check Point) และจุดตั้งต้นประมวลผลได้ใหม่ (Restart) ในระบบงาน
- การปรับปรุงแก้ไขโปรแกรมกรณีเร่งด่วนเป็นการชั่วคราว

ข้อแนะนำ

สถาบันการเงินควรจัดทำคู่มืออันเป็นมาตรฐานของระบบงาน เพื่อใช้เป็นแหล่งอ้างอิงหรือแนวทางสำหรับการพัฒนาระบบงาน การบำรุงรักษาระบบงาน หรือการปรับปรุงระบบงานคอมพิวเตอร์ให้ดีขึ้น ระเบียบการพัฒนาระบบงานและโปรแกรมโดยทั่วไป ควรมีหัวข้อดังนี้

- การควบคุมโครงการ
- มาตรฐานการพัฒนาระบบงานโดยทั่วไป
- กระบวนการพัฒนาระบบงาน
- การจัดหาหรือจัดทำโปรแกรมสำเร็จรูป

หมายเหตุ หากข้อใดไม่มีข้อแนะนำ ขอให้เข้าใจว่าข้อบกพร่องหรือจุดอ่อนที่เป็นข้อสังเกตในการตรวจสอบนั้นชัดเจนและเป็นข้อแนะนำในตัวแล้ว

- มาตรฐานการเขียนโปรแกรม
- มาตฐานการทดสอบระบบงานและโปรแกรม
- มาตรฐานการนำระบบงานใหม่ออกใช้งาน
- การตรวจสอบผลการนำระบบงานใหม่ออกใช้งาน
- การรักษาความปลอดภัยเกี่ยวกับ OS (Operating System)
- การควบคุมการปฏิบัติงานของผู้เขียนโปรแกรมระบบงาน
- การรักษาความปลอดภัยโปรแกรมที่ใช้ประมวลผล
- การควบคุมการปรับปรุงแก้ไขโปรแกรม
- การควบคุมการปรับปรุงแก้ไขโปรแกรมในกรณีเร่งด่วนเป็นการชั่วคราว
- การจัดทำข้อมูลและหลักฐานที่ควรมีไว้ตรวจสอบ
- การจัดให้มีจุดตรวจสอบและจุดตั้งต้นประมวลผลได้ใหม่ไว้ในระบบงาน

3) **การบริหารโครงการพัฒนาระบบงานมีจุดอ่อน**

สถาบันการเงินมีจุดอ่อนในการบริหารโครงการพัฒนาระบบงาน คือ

- ไม่มีการศึกษาความเหมาะสมของโครงการ (Feasibility Study) การวิเคราะห์ต้นทุนและผลตอบแทนที่จะได้รับจากโครงการ (Cost – Benefit Analysis) และการจัดลำดับความสำคัญของโครงการ
- การกระจายกำลังคนไปพัฒนางานพร้อม ๆ กันหลายโครงการ โดยไม่คำนึงถึงลำดับความสำคัญ อาจทำให้โครงการต่าง ๆ ล่าช้า ไม่เป็นไปตามแผนที่วางไว้

ข้อแนะนำ

สถาบันการเงินควรมีนโยบายให้มีการพัฒนาระบบงานที่มีคุณภาพ โดยกำหนดให้มีการศึกษาความเป็นไปได้ของโครงการ (Feasibility Study) การวิเคราะห์ต้นทุนและผลตอบแทนที่จะได้รับจากโครงการ (Cost – Benefit Analysis) การจัดลำดับความสำคัญของโครงการ พร้อมทั้งจัดกำลังคนในการพัฒนางาน โดยคำนึงถึงลำดับความสำคัญของโครงการด้วย

4) **เอกสารประกอบระบบงานมีข้อบกพร่องบางประการ**

การจัดทำเอกสารประกอบระบบงานของสถาบันการเงินมีข้อบกพร่องบางประการ ดังนี้

- เอกสารประกอบระบบงานที่พัฒนาเสร็จและนำออกใช้งานแล้ว ยังคลาดเคลื่อนต่อความเป็นจริงไม่สมบูรณ์ อันเนื่องมาจากสถาบันการเงินไม่ได้กำหนดมาตรฐานของเอกสารประกอบระบบงาน ซึ่งอาจทำให้ไม่สามารถประเมินความถูกต้องและสมบูรณ์ของระบบงานได้ และเป็นผลให้การปฏิบัติงานผิดพลาดได้ในภายหลัง อันอาจเกิดผลเสียต่อการควบคุมและการปฏิบัติงานของผู้ใช้งานและศูนย์คอมพิวเตอร์ โดยผู้ปฏิบัติงานอาจหาวิธีการแก้ไขปัญหาการปฏิบัติงานด้วยตนเอง หรือผู้ใช้ข้อมูลอาจละเลยไม่สามารถตรวจสอบบางชนิดที่จำเป็นต้องตรวจสอบก่อนนำไปใช้งาน อีกทั้งเจ้าหน้าที่ที่ย้ายเข้ามาปฏิบัติงานใหม่ อาจไม่มีคู่มือในการศึกษา และอาจปฏิบัติงานไม่ถูกต้อง

ข้อแนะนำ

สถาบันการเงินควรจัดให้มีมาตรฐานการพัฒนาระบบงานและโปรแกรม เพื่อให้พนักงานที่มีหน้าที่ในการพัฒนาระบบงานและโปรแกรมยึดถือเป็นแนวทางในการปฏิบัติงาน และจัดทำเอกสารสนับสนุนระบบงานในขั้นตอนต่าง ๆ ให้มีรูปแบบเดียวกัน และปรับปรุงให้ครบถ้วน ถูกต้อง ทันเวลา และสมบูรณ์อยู่เสมอทั้งนี้เพราะเอกสารดังกล่าวเป็นแหล่งข้อมูลที่จะนำไปใช้ประโยชน์ในการตรวจสอบความถูกต้องของระบบก่อนนำออกไปใช้งาน การแก้ไขและปรับปรุงระบบการปฏิบัติงานตามระบบ และยังช่วยให้การติดต่อและประสานงานระหว่างศูนย์คอมพิวเตอร์ และฝ่ายอื่น ๆ เป็นไปอย่างมีประสิทธิภาพ เอกสารสนับสนุนระบบงานควรจะครบถ้วนสมบูรณ์ และได้รับการทดสอบแล้วก่อนที่จะมีการอนุมัติให้ใช้ระบบงานใหม่ และภายหลังจากที่มีการแก้ไขแล้วทุกครั้ง

เอกสารที่สถาบันการเงินควรจัดทำขึ้นเพื่อสนับสนุนระบบงาน ได้แก่

1. ผลการศึกษาและวิเคราะห์โครงการ
2. คำบรรยายเกี่ยวกับระบบงาน
3. คำบรรยายเกี่ยวกับโปรแกรม
4. คู่มือหรือวิธีการปฏิบัติงานสำหรับพนักงานประจำเครื่องคอมพิวเตอร์ โดยควรจัดทำเป็นภาษาอังกฤษหรือภาษาไทย
5. คู่มือหรือวิธีการปฏิบัติงานสำหรับผู้ใช้ข้อมูล
6. ผลการตรวจรับระบบก่อนนำออกใช้งาน

เอกสารประกอบระบบงานยังขาดรายละเอียดที่สำคัญ เช่น

1) Record Layout ของแต่ละระบบ (Application) ยังขาดความสมบูรณ์เกี่ยวกับการอธิบายความหมายของแต่ละ field เพิ่มเติม นอกเหนือจากลักษณะและความยาวของข้อมูล
2) Program Specification ของแต่ละระบบ (Application) บางโปรแกรมของผังการปฏิบัติงาน ขั้นตอนและวิธีควบคุมต่าง ๆ

ข้อแนะนำ

เอกสารสนับสนุนการปฏิบัติงานด้านคอมพิวเตอร์ที่ดีและสมบูรณ์ ย่อมจะช่วยให้การดูแลและการเปลี่ยนระบบงานเดิมเป็นระบบงานใหม่ทำได้ง่ายและมีประสิทธิภาพ สถาบันการเงินจึงควรจัดให้มีเอกสารประกอบระบบงานที่มีประสิทธิภาพ ดังนี้

1) รายละเอียดระบบงาน (System Specification) ในหมวดที่ว่าด้วย Record Layout ควรจะมีคำอธิบายความหมายของแต่ละ field เพิ่มเติม
2) รายละเอียดโปรแกรมงาน (Program Specification) ในกรณีที่สถาบันการเงินจ้างบริษัทภายนอกพัฒนาระบบงานให้ ก็ควรขอให้บริษัทจัดทำเอกสารประกอบการพัฒนาโปรแกรมให้ด้วย โดยเฉพาะ Program Flowchart

3) คู่มือสำหรับผู้ใช้ข้อมูล (User Manual) ควรมีคำอธิบายโดยละเอียดของการทำงานทุกขั้นตอน โดยเฉพาะจุดที่ต้องมีการควบคุมความถูกต้องของการปฏิบัติงาน

4) ในกรณีที่สถาบันการเงินต้องการพัฒนาระบบงานใหม่เอง โดยไม่พึ่งพาบุคคลภายนอก สถาบันการเงินควรกำหนดระเบียบหรือคู่มือมาตรฐานที่ระบุขั้นตอนของการพัฒนาระบบงานอย่างชัดเจน

เอกสารสนับสนุนระบบงาน และการใช้คอมพิวเตอร์ไม่สอดคล้องกับการปฏิบัติงานจริง เช่น

1) จากเอกสารสนับสนุนระบบงาน กำหนดให้พิมพ์รายงาน Proof List ออกมาให้แก่ User ทำการตรวจสอบความถูกต้องก่อนที่จะทำการ Update Master File แต่จากการปฏิบัติงานจริง ฝ่ายคอมพิวเตอร์จะทำการพิมพ์ Proof List แล้ว Update Master File เลย

2) จากคู่มือสำหรับผู้ใช้ระบบงาน ATM ระบุว่า ในกรณีที่กระแสไฟฟ้าดับนานเกินกว่า 16 ชั่วโมง Key ต่าง ๆ ที่เก็บไว้ที่เครื่อง ATM จะลบหายไป แต่เมื่อเครื่องหยุดทำงานจริง ปรากฏว่า Key ต่าง ๆ ได้ลบหายไปภายในเวลาที่เร็วกว่า 16 ชั่วโมง

3) ตามคู่มือปฏิบัติงาน ATM กำหนดไว้ว่า หากธนบัตรที่มีอยู่ในกล่องเหลือถึงจำนวน 20 ฉบับแล้ว เครื่องจะเตือนว่าเป็น Close out และปิดการให้บริการแก่ลูกค้าทันที แต่ในทางปฏิบัติพบว่าบางครั้งเงินสดคงเหลืออยู่ในกล่องจำนวนมากกว่า 20 ฉบับ เครื่องก็จะตัดหรือหยุดการให้บริการทำให้ผู้ใช้คู่มือเกิดความสับสนในการปฏิบัติงาน

ข้อแนะนำ

สถาบันการเงินควรปรับปรุงให้เอกสารสนับสนุนระบบงานและการปฏิบัติงานจริงสอดคล้องกัน

- เอกสารสนับสนุนระบบงานแสดงข้อมูลไม่เป็นปัจจุบันและไม่ครบถ้วน สถาบันการเงินดำเนินการและควบคุมการจัดทำเอกสารสนับสนุนระบบงาน (Documentation) ของทุกระบบงานขาดความรัดกุม เป็นผลให้มีเอกสารสนับสนุนระบบงาน ทั้งด้านโปรแกรม User และ Operation ไม่เพียงพอต่อการควบคุมและสนับสนุนการปฏิบัติอย่างมีประสิทธิภาพ ดังนี้

1) ข้อมูลบางส่วนมีการแก้ไขแล้ว แต่ในเอกสารประกอบระบบงานไม่มีการแก้ไข
2) มีข้อมูลบางส่วนระบุไว้ในเอกสารประกอบระบบงาน แต่ไม่ทราบความหมายที่แท้จริงของข้อมูลนั้น
3) โปรแกรมระบบงานสามารถทำงานได้มากกว่าที่ระบุไว้ในเอกสารประกอบระบบงาน
4) เอกสารประกอบระบบงานยังขาดรายละเอียดที่สำคัญ เช่น Program Specification และ Program Flowchart และทุกระบบงาน
5) ไม่ได้จัดทำคู่มือในการปฏิบัติงานด้าน Conversion ซึ่งใช้ในการเปลี่ยนข้อมูลในระบบ Manual ให้อยู่ในรูปแบบของระบบคอมพิวเตอร์

ดังนั้น เมื่อถึงคราวจำเป็นต้องใช้เอกสารอ้างอิง ก็ไม่สามารถนำเอกสารสนับสนุนระบบงานดังกล่าว มาใช้ปฏิบัติงานได้ทันที สถาบันการเงินจะต้องอาศัยตัวบุคคลเป็นหลักในการจดจำรายละเอียดของระบบงาน ซึ่งจะสร้างปัญหาให้กับสถาบันการเงินได้เมื่อมีการโยกย้าย สับเปลี่ยน หรือพนักงานลาออกจากสถาบันการเงิน

ข้อแนะนำ

สถาบันการเงินกำหนดระเบียบการจัดทำและบำรุงรักษาเอกสารประกอบระบบงาน และให้มีการควบคุมตามระเบียบโดยเคร่งครัด

- ไม่มีคู่มือสำหรับผู้ใช้ข้อมูล

สถาบันการเงินไม่ได้จัดทำคู่มือสำหรับผู้ใช้ข้อมูล ซึ่งเป็นสิ่งจำเป็นในการช่วยให้ผู้ใช้ข้อมูลเข้าใจเชื่อถือ ยอมรับระบบงาน และป้องกันความเสียหายที่อาจเกิดจากผู้ใช้ข้อมูลหาวิธีแก้ไขปัญหาด้วยตนเอง หรือผู้ใช้ข้อมูลอาจไว้วางใจข้อมูลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์จนเกินไป ทำให้ละเลยไม่ตรวจสอบข้อมูลบางชนิดที่จำเป็นต้องตรวจสอบก่อนนำไปใช้

ข้อแนะนำ

สถาบันการเงินควรจัดทำคู่มือปฏิบัติงานให้เสร็จและใช้ได้ทันก่อนเริ่มปฏิบัติงานและมีการฝึกอบรมการใช้คู่มือ

๕) การจัดเก็บ การบำรุงรักษา และการควบคุมการใช้เอกสารสนับสนุนการปฏิบัติงานมีข้อบกพร่องบางประการ

๖) การควบคุมการแก้ไขโปรแกรมไม่เหมาะสม

- สถาบันการเงินไม่ได้กำหนดระเบียบปฏิบัติเกี่ยวกับการปรับปรุงแก้ไขโปรแกรมใช้งานอาจทำให้สถาบันการเงินไม่สามารถควบคุมและเป็นเหตุให้เกิดความเสียหายได้

ข้อแนะนำ

สถาบันการเงินควรกำหนดระเบียบในการแก้ไขโปรแกรมระบบงาน และให้มีการควบคุมการแก้ไขตามระเบียบที่กำหนดไว้โดยเคร่งครัด

- ผู้เขียนโปรแกรมไม่ได้มีการจัดทำรายละเอียดการแก้ไขโปรแกรม และไม่มีการทำหนังสือขออนุมัติแก้ไขโปรแกรมจากผู้ที่มีส่วนเกี่ยวข้อง และผู้รับผิดชอบก่อนดำเนินการ

ข้อแนะนำ

สถาบันการเงินควรควบคุมดูแลให้มีการปฏิบัติตามมาตรฐานของระบบงานโดยทั่วไปที่สถาบันการเงินจะจัดทำขึ้น และควรเร่งรัดติดตามเอกสารสนับสนุนระบบงานบางประเภทจากบริษัทผู้ขายเครื่องคอมพิวเตอร์ให้สถาบันการเงิน

- สำเนาหนังสือขออนุมัติปรับปรุงแก้ไขโปรแกรมที่ฝ่ายคอมพิวเตอร์จัดส่งให้ฝ่ายตรวจสอบ เฉพาะกรณีที่การแก้ไขโปรแกรมมีผลกระทบต่อข้อมูลทางการเงินเท่านั้น ยังไม่เป็นการเพียงพอเพราะการปรับปรุงแก้ไขโปรแกรมในส่วนที่ไม่น่าจะเกี่ยวข้องกับข้อมูลทางการเงินในบางกรณี อาจมีผลกระทบต่อฐานะและการดำเนินงานของสถาบันการเงินได้เช่นเดียวกัน

ข้อแนะนำ

ฝ่ายคอมพิวเตอร์ควรส่งสำเนาหนังสือขออนุมัติที่ปรับปรุงแก้ไขโปรแกรมให้ฝ่ายตรวจสอบทุกกรณี

- ในการแก้ไขโปรแกรมงาน โปรแกรมเมอร์ไม่ได้แก้ไขโปรแกรมและแฟ้มข้อมูลที่ได้รับผลกระทบจากการเปลี่ยนแปลงแก้ไขโปรแกรมระบบงานหรือแฟ้มข้อมูลอื่น ๆ ในระบบคอมพิวเตอร์ ซึ่งส่งผลให้พนักงานควบคุมเครื่อง (Operator) มีรายละเอียดขั้นตอนงานที่ต้องปฏิบัติตามตารางปฏิบัติงาน (Job Run Sheet) คลาดเคลื่อนไป เช่น

1) การเรียกใช้โปรแกรมที่ถูกต้องออกจากระบบไปแล้ว
2) แฟ้มข้อมูลที่ใช้ออกรายงาน Job Run Sheet ไม่ได้ปรับปรุงให้สอดคล้องกับขั้นตอนงานที่เพิ่มขึ้นมา ซึ่งจะแสดงใน Job Control Report

ข้อแนะนำ

ควรควบคุมให้โปรแกรมเมอร์ทำการปรับปรุงโปรแกรมและแฟ้มข้อมูลที่ถูกกระทบจากการเปลี่ยนแปลงส่วนต่าง ๆ ในระบบงานให้ทันต่อเวลาและถูกต้องอยู่เสมอ

- ในใบคำขออนุมัติปรับปรุงแก้ไขโปรแกรมที่รายละเอียดไม่ครบถ้วน เช่น ไม่ระบุวัตถุประสงค์และสาเหตุในการขอแก้ไข ไม่มีรายละเอียดการแก้ไขทั้งก่อนและหลังการปรับปรุงและไม่ได้แจ้งให้ส่วนตรวจสอบงานคอมพิวเตอร์ทราบทุกครั้งที่มีการปรับปรุงแก้ไขโปรแกรม ซึ่งอาจมีปัญหาในด้านความปลอดภัยของระบบข้อมูลทางการเงิน ทำให้ประสิทธิภาพของการควบคุมภายในบกพร่องและขาดหลักฐานในการใช้ติดตามความถูกต้องและปัญหาที่อาจเกิดขึ้นในอนาคต

ข้อแนะนำ

ในใบคำขออนุมัติแก้ไขโปรแกรมตามแบบฟอร์ม ควรระบุรายละเอียดเกี่ยวกับปัญหาหรือเหตุผลของการแก้ไขให้ครบถ้วนทุกโปรแกรม

- สถาบันการเงินมิได้จัดทำทะเบียนประวัติการเปลี่ยนแปลงแก้ไขโปรแกรม ซึ่งอาจส่งผลกระทบต่อความครบถ้วนและการติดตามกรณีที่เกิดปัญหาในการประมวลผล ตลอดจนเป็นอุปสรรคในการบันทึกรายละเอียดการแก้ไขโปรแกรมเพื่อติดตามผลต่อเนื่องในการเปลี่ยนแปลงแก้ไขโปรแกรมทุกระยะ

ข้อแนะนำ

สถาบันการเงินควรจัดทำทะเบียนประวัติการแก้ไขโปรแกรมของศูนย์คอมพิวเตอร์

7) **แผนการทดสอบเพื่อตรวจรับระบบงานใหม่ไม่ครอบคลุมปัญหาหรือเงื่อนไขสำคัญ**

แผนการทดสอบเพื่อตรวจรับระบบงานใหม่ยังไม่ครอบคลุมเงื่อนไขของการเกิดรายการโดยสถาบันการเงินจะเลือกบัญชีเก่าทั้งที่เป็นบัญชีเงินฝากกระแสรายวันและเป็นเงินเบิกเกินบัญชีที่มีรายการเคลื่อนไหวทุกประเภทรายการมาป้อนข้อมูลผ่านเครื่องคอมพิวเตอร์และเปรียบเทียบผลลัพธ์กับการ์ดบัญชีโดยสถาบันการเงินไม่ได้กำหนดการทดสอบการป้อนข้อมูลผิดพลาดหรือผิดเหตุผลที่อาจเกิดขึ้นเป็นกรณีพิเศษ เช่น กรณีการป้อนข้อมูลผิดพลาดที่อาจเกิดขึ้นได้ หรือกรณีการป้อนข้อมูลถูกต้องแต่ผิดเวลา เป็นต้น ซึ่งอาจทำให้รายการผิดพลาดเหล่านี้ผ่านไป และอาจก่อให้เกิดผลเสียหายแก่สถาบันการเงินได้

ข้อแนะนำ

สถาบันการเงินควรจัดทำข้อมูลทดสอบในการตรวจรับระบบงานให้ครอบคลุมรายการที่อาจเกิดขึ้นได้ทุกประเภท ทั้งกรณีปกติและกรณีพิเศษ และกำหนดการควบคุมในจุดที่ระบบงานไม่มีการควบคุมหรือควบคุมได้ไม่รัดกุมให้สอดคล้องกันด้วย

8) **การพัฒนาโปรแกรม**

สถาบันการเงินยินยอมให้ที่ปรึกษาของสถาบันการเงินรับโอนงานพัฒนาโปรแกรมงานแทนบริษัทซึ่งเป็นผู้รับจ้างพัฒนาโปรแกรมครั้งแรก โดยไม่มีการดำเนินการเป็นลายลักษณ์อักษรกับบริษัทว่ายินยอมให้ที่ปรึกษากระทำการแทนบริษัทได้ ซึ่งอาจเกิดปัญหาความรับผิดชอบในภายหลังได้

ข้อแนะนำ

สถาบันการเงินควรกำหนดให้มีข้อตกลง หรือการโอนงานระหว่างองค์กรเป็นลายลักษณ์อักษร

9) **ไม่มีการทดสอบโปรแกรมการใช้งานแล้วเป็นครั้งคราว**

นับแต่มีการนำระบบงานเงินกู้เพื่อที่อยู่อาศัยออกใช้ สถาบันการเงินไม่ได้ทำการทดสอบโปรแกรมการคำนวณดอกเบี้ยของลูกค้าและรายการอื่น ๆ อีกครั้งหนึ่ง

ข้อแนะนำ

สถาบันการเงินควรจัดให้มีการทดสอบโปรแกรมที่นำออกใช้งานแล้ว เพื่อทดสอบความถูกต้องในการประมวลผลข้อมูลเป็นครั้งคราว

10) **การรวบรวมเอกสารที่ได้จากการทดสอบระบบงานก่อนนำไปใช้งาน**

สถาบันการเงินไม่ได้กำหนดระเบียบให้มีการรวบรวมข้อมูลและผลจากการทดสอบระบบงานที่นำออกใช้ใหม่ไว้เป็นหลักฐาน เพื่อใช้ประโยชน์ในการทบทวนการทดสอบที่นำออกใช้ใหม่ไว้เป็นหลักฐาน เพื่อใช้ประโยชน์ในการทบทวนการทดสอบที่ได้นำไปนั้นว่าครอบคลุมการทำงานทุกขั้นตอนของระบบงานหรือไม่

ข้อแนะนำ

สถาบันการเงินควรกำหนดระเบียบเกี่ยวกับการทดสอบระบบงานให้มีการรวบรวมกระดาษทำการ ข้อมูลทดสอบ และผลจากการทดสอบ ไว้เป็นหมวดหมู่ตามระบบงาน เพื่อใช้ประโยชน์ในการปฏิบัติงานต่อไป

11) **มิได้กำหนดระเบียบปฏิบัติเกี่ยวกับการทดสอบโปรแกรมการปฏิบัติงานคู่ขนาน (Parallel Test)**

ในการทดสอบโปรแกรมงานแบบการปฏิบัติงานคู่ขนานกับระบบงานเดิม เพื่อให้แน่ใจว่าสามารถใช้โปรแกรมการปฏิบัติงานจริงอย่างสมบูรณ์ แต่สถาบันการเงินมิได้กำหนดระเบียบปฏิบัติงานคู่ขนาน ทำให้บางระบบงานมีการปฏิบัติงานคู่ขนานเกินกว่า 6 เดือนขึ้นไป อาจเกิดผลกระทบต่อเป้าหมายและแผนงานการใช้คอมพิวเตอร์ของสถาบันการเงิน

ข้อแนะนำ

สถาบันการเงินควรพิจารณาและกำหนดหลักเกณฑ์ในการปฏิบัติงานแบบคู่ขนาน เช่น ระยะเวลาสูงสุดในการปฏิบัติงานคู่ขนาน การรายงานผล และการยกเลิกการปฏิบัติงานคู่ขนาน และควรเร่งรัดให้มีการจัดทำคู่มือปฏิบัติงานให้เสร็จสิ้นและฝึกอบรมการใช้คู่มือด้วย ก่อนที่จะเริ่มปฏิบัติงานคู่ขนาน

12) **การนำระบบงานใหม่ออกใช้แทนระบบงานเดิม (System Inplementation)**

จากการตรวจสอบวิธีปฏิบัติในการนำระบบงานที่ผ่านการทดสอบแล้วมาใช้แทนระบบงานเดิม ไม่ปรากฏว่ามีหลักฐานแสดงการอนุมัติของสถาบันการเงิน และวันที่ที่เริ่มใช้ระบบงานใหม่ทำให้ขาดหลักฐานสำคัญที่แสดงถึงความพร้อมเพรียง และความรับผิดชอบของฝ่ายต่าง ๆ ที่เกี่ยวข้อง ก่อนที่สถาบันการเงินจะอนุมัติให้ใช้ระบบงานใหม่แทนระบบงานเดิมได้

ข้อแนะนำ

ในการอนุมัติให้ใช้ระบบงานใหม่ ควรมีหลักฐานแสดงการรับรองจากหน่วยงาน ดังนี้

- หลักฐานที่แสดงว่าฝ่ายงานผู้ใช้ข้อมูลได้ตรวจสอบผลงานที่ได้จากระบบงานแล้วใช้ได้และถูกต้องตามที่กำหนดไว้
- หลักฐานที่แสดงว่าสำนักผู้ตรวจสอบภายในได้ทดสอบระบบงานและวิธีการควบคุมภายในจนเป็นที่พอใจแล้ว
- หลักฐานที่แสดงว่าฝ่ายผู้ใช้ข้อมูลได้ตรวจทานคู่มือในการปฏิบัติงานแล้วเห็นว่าเรียบร้อยและสมบูรณ์ สามารถนำไปใช้เป็นแนวทางในการปฏิบัติงานจริงได้
- หลักฐานที่แสดงว่าหน่วยปฏิบัติการคอมพิวเตอร์ได้ตรวจทานคู่มือการปฏิบัติงาน ความพร้อมเพรียงของโปรแกรมและเครื่องคอมพิวเตอร์แล้ว

หลักฐานที่กล่าวข้างต้น สถาบันการเงินควรเก็บรวบรวมไว้เพื่อเป็นส่วนหนึ่งของเอกสารประกอบระบบงานที่สถาบันการเงินอนุมัติให้ใช้ปฏิบัติงานแทนระบบเดิมด้วย

13) การใช้เครื่อง Terminal ที่ทำหน้าที่ควบคุมการทำงานของระบบคอมพิวเตอร์ (console) ไม่รัดกุม

สถาบันการเงินไม่ได้กำหนดให้มีการใช้ Password เพื่อตรวจสอบผู้มีสิทธิใช้ Console ในการติดต่อกับเครื่องคอมพิวเตอร์ เป็นการเปิดโอกาสให้บุคคลที่ไม่เกี่ยวข้องซึ่งสามารถเข้าถึงเครื่องคอมพิวเตอร์ และอาจทำการแก้ไขข้อมูลการเงินที่สำคัญไปในทางที่ก่อให้เกิดผลเสียหายต่อสถาบันการเงิน นอกจากนี้สถาบันการเงินยังจัดเก็บโปรแกรมที่ใช้ในการแก้ไขข้อมูลไว้ในเครื่องคอมพิวเตอร์ซึ่งสามารถใช้งานได้ตลอดเวลาด้วย

ข้อแนะนำ

สถาบันการเงินควรกำหนดให้มี Password เพื่อควบคุมการใช้เครื่อง Console นอกจากนี้ควรกำหนดระเบียบการใช้โปรแกรมแก้ไขข้อมูล และควรนำโปรแกรมที่ใช้ในการแก้ไขข้อมูลออกจากเครื่องเมื่อเลิกใช้งานแล้ว

14) ไม่ได้จัดให้มีพนักงานควบคุมเครื่องคอมพิวเตอร์ในขณะประมวลผลงาน Batch

ในขั้นตอนการประมวลผลงาน Batch ซึ่งเป็นการทำงานในช่วงเวลากลางคืนจนเสร็จสิ้นงานประจำวัน สถาบันการเงินได้มอบหมายให้ยามรักษาการณ์เป็นผู้ถือกุญแจห้องคอมพิวเตอร์และดูแลการประมวลผลเป็นครั้งคราว ถ้าหากเกิดปัญหาในการประมวลผลให้แจ้งพนักงานผู้รับผิดชอบโดยตรงทราบ

ในกรณีที่เกิดปัญหาอาจไม่สามารถแก้ไขปัญหาในการประมวลผลได้ทันท่วงที ซึ่งอาจมีผลกระทบต่อการดำเนินงานของสถาบันการเงินในวันทำการถัดไป และอาจเป็นช่องทางให้บุคคลที่ไม่เกี่ยวข้องเปลี่ยนแปลงข้อมูลโดยไม่มีใครทราบ

ข้อแนะนำ

สถาบันการเงินควรจัดให้มีเจ้าหน้าที่ผู้รับผิดชอบควบคุมดูแลการประมวลผลให้เสร็จสิ้นตามขั้นตอนของโปรแกรมระบบงานในแต่ละวัน

15) รายงานการออกแบบระบบงานของสถาบันการเงินแสดงข้อมูลไม่ครบถ้วน

จากการตรวจสอบรายงานการออกแบบระบบงานของสถาบันการเงิน พบว่ารายงานดังกล่าวประกอบด้วยข้อมูล 3 ส่วน คือ

1) สรุปงานที่สำคัญของสถาบันการเงินทั้งหมดที่จะใช้คอมพิวเตอร์
2) ลักษณะของงานที่ปฏิบัติในแต่ละระบบงาน
3) รูปแบบของรายงานต่าง ๆ ตามความต้องการของผู้ใช้งาน

ข้อมูลเหล่านี้เพียงแต่แสดงถึงหน้าที่หรือกิจกรรมหลักทั่วไปของสถาบันการเงินและรายงานที่ผู้ใช้ต้องการเท่านั้น ไม่ได้แสดงวิธีปฏิบัติและการควบคุมภายในกิจกรรมหลักโดยละเอียดอย่างเหมาะสม ก่อนที่จะผ่านไปสู่ขั้นตอนการออกแบบโดยละเอียดเพื่อจัดทำโปรแกรมงาน (System Specification)

ข้อแนะนำ

1) กำหนดให้ผู้ออกแบบระบบงานใหม่ ๆ จัดทำแผนภูมิแสดงวิธีปฏิบัติงานและการควบคุมภายใน (Procedural Flowchart) ด้วย

2) ก่อนส่ง System Specification ให้ผู้ออกแบบระบบงาน ควรมอบให้ฝ่ายงานที่ใช้ข้อมูลและสำเนาผู้ตรวจสอบภายในตรวจสอบความสมบูรณ์ของเอกสารและลงนามรับรองเป็นลายลักษณ์อักษร และเก็บรักษาต้นฉบับ หรือถ่ายสำเนาเก็บไว้อย่างน้อย 1 ฉบับ

3) System Specification ควรประกอบด้วย System Flowchart, Processing Procedures & Logic, Input Formats, Output Formats, Control Paints, และ User Procedures

16) การจัดเก็บเอกสารประกอบระบบงานและโปรแกรมไม่เหมาะสม

สถาบันการเงินไม่ได้กำหนดระเบียบปฏิบัติเกี่ยวกับการจัดเก็บเอกสารประกอบระบบงานและโปรแกรมเป็นผลให้ผู้ปฏิบัติงานไม่ทราบถึงความสำคัญของเอกสารดังกล่าว จึงจัดวางไว้ในที่ไม่ปลอดภัย อาจเป็นช่องทางให้ผู้ไม่มีหน้าที่เกี่ยวข้องสามารถเข้าถึงเอกสารได้โดยง่าย และอาจก่อให้เกิดผลกระทบต่อความปลอดภัยของระบบงานโปรแกรม หรือข้อมูลของสถาบันการเงินได้

ข้อแนะนำ

สถาบันการเงินควรกำหนดระเบียบเกี่ยวกับการจัดเก็บเอกสารประกอบระบบงานและโปรแกรม กำหนดตัวบุคคลที่ธนาคารอนุญาตให้ใช้เอกสารบางประเภทที่มีผลกระทบต่อการศึกษาความปลอดภัยของระบบคอมพิวเตอร์ และควรจัดสถานที่เก็บเอกสารที่เหมาะสม พร้อมทั้งควบคุมการใช้เอกสารดังกล่าวให้รัดกุม

17) การจัดเก็บ Authentication Keys File ไม่รัดกุม

สถาบันการเงินจัดเก็บแผ่น diskette ซึ่งบันทึก Authentication Keys File ที่ตู้เก็บเอกสารภายในห้องเครื่อง SWIFT หากเครื่อง SWIFT และข้อมูลในแผ่น Authentication Keys File ถูกทำลายพร้อมกัน จะเป็นผลให้สถาบันการเงินไม่มีแผ่น Authentication Keys File เพื่อที่จะสามารถดำเนินงานตามปกติภายในระยะเวลาที่เหมาะสมได้

ข้อแนะนำ

ควรจัดเก็บแผ่น Authentication Keys File ไว้ต่างหากในที่ปลอดภัย

18) การทบทวนโครงการภายหลังการนำระบบงานออกใช้

การประเมินผลและการวัดความสำเร็จของโครงการในลักษณะ Post – implementation review ยังไม่ได้มีการดำเนินงานอย่างจริงจังเท่าที่ควร ทำให้ไม่ทราบว่าโครงการคอมพิวเตอร์ที่ใช้อยู่ในปัจจุบันบรรลุวัตถุประสงค์หรือไม่ มีปัญหาในการปฏิบัติงานมากน้อยเพียงใด

ข้อแนะนำ

หลังจากนำระบบงานใหม่ออกใช้งานไประยะเวลาหนึ่งแล้ว ควรมีการประเมินผลและวัดความสำเร็จของโครงการในลักษณะ Post – implementation review โดยพิจารณาถึงเรื่องต่าง ๆ ดังต่อไปนี้

- ระยะเวลาและค่าใช้จ่ายที่กำหนดไว้ตามโครงการ เปรียบเทียบกับระยะเวลาและค่าใช้จ่ายที่เกิดขึ้นจริง
- ผลการใช้ระบบงานใหม่บรรลุวัตถุประสงค์เพียงใด
- ผลประโยชน์ที่สถาบันการเงินได้รับจากการใช้ระบบงานใหม่
- ปัญหาการปฏิบัติงาน
- ความคุ้มค่าในการลงทุน

19) การควบคุมการซ่อมบำรุงเครื่องคอมพิวเตอร์ไม่รัดกุม

สถาบันการเงินได้ให้พนักงานของบริษัทผู้ให้เช่าเครื่องคอมพิวเตอร์มาซ่อมบำรุงรักษาเครื่อง โดยมิได้กำหนดเวลาการซ่อมและบำรุงรักษาเครื่องจักรที่เหมาะสมไว้ล่วงหน้า เพื่อป้องกันไม่ให้อุปกรณ์ในระบบคอมพิวเตอร์เสียและสามารถใช้ประมวลผลได้อย่างต่อเนื่อง นอกจากนี้สถาบันการเงินได้ให้พนักงานที่มาทำการซ่อมบำรุงปฏิบัติงานได้โดยอิสระ ขาดการควบคุมจากเจ้าหน้าที่ของสถาบันการเงิน

ข้อแนะนำ

สถาบันการเงินควรให้บริษัทผู้ให้เช่าจัดทำตารางการบำรุงรักษาเครื่องคอมพิวเตอร์ที่แน่นอนและแจ้งให้สถาบันการเงินทราบ นอกจากนี้ควรให้มีเจ้าหน้าที่ของสถาบันการเงินควบคุมการซ่อมบำรุงโดยใกล้ชิด

20) ไม่มี Journal Tape ควบคุมการใช้เครื่อง Terminal

ระบบงานที่ประมวลผลด้วยเครื่องคอมพิวเตอร์ สถาบันการเงินไม่ได้กำหนดให้มีการพิมพ์รายละเอียดของรายการประจำวัน (Listing) สำหรับการใช้แทนสมุดลงรายการขั้นต้น (Journal) และไม่มี Journal Tape เพื่อควบคุมการป้อนรายการความครบถ้วนของ Slip และการติดตามปัญหาซึ่งอาจพบในภายหลัง โดยเฉพาะในกรณีที่จอ Display ถูกใช้ไปในงานอื่น

ข้อแนะนำ

ควรจัดให้พิมพ์รายงานสำหรับใช้แทนสมุดลงรายการขั้นต้น (Journal) และรายงาน Journal Tape เพื่อเก็บไว้เป็นหลักฐานการติดตามรายการและควบคุมกรณีที่เกิดมีปัญหาขึ้นในภายหลังด้วย

21) ไม่มีข้อกำหนดการรักษาความต่อเนื่องของ Journal Roll จากเครื่อง Authorized Workstation

จากการตรวจสอบพบว่าพนักงานฉีกกระดาษ Journal Roll ที่พิมพ์จากเครื่อง Authorized Work station ในระหว่างวัน ทำให้ไม่สามารถควบคุมความครบถ้วนของเอกสารหลักฐานและติดตามรายการได้

ข้อแนะนำ

ในกรณีที่มีเหตุจำเป็นที่ Journal Roll ในวันเดียวกันไม่ต่อเนื่องกันควรนำมาติดกันและประทับตราที่รอยต่อโดยผู้บริหารหรือผู้ได้รับมอบอำนาจ เพื่อมิให้ฉีกขาดหรือตกหล่นหรือขาดข้อมูลบางส่วนไป และควรกำหนดให้มีการตรวจสอบ Journal Roll โดยผู้บริหาร

22) การควบคุมการแก้ไขข้อผิดพลาดไม่ครบถ้วน

ในระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ รายการแก้ไขข้อผิดพลาดของรายการที่ป้อนวันเดียวกันนั้นไม่ต้องผ่านการอนุมัติจากเจ้าหน้าที่ผู้ได้รับมอบอำนาจ

ข้อแนะนำ

ควรกำหนดให้การทำรายการแก้ไขข้อผิดพลาดของรายการที่เกิดขึ้นในวันนั้นต้องผ่านการอนุมัติ (Override) จากเจ้าหน้าที่ผู้ได้รับมอบอำนาจ

23) ไม่มีรายงานควบคุมการเปลี่ยนแปลงข้อมูล

การเปลี่ยนแปลงแก้ไขข้อมูลใน Main File ไม่แสดงการเปลี่ยนแปลงหรือแก้ไขข้อมูลอื่นที่เกี่ยวข้องด้วย อาจเป็นจุดอ่อนในการควบคุมการเปลี่ยนแปลงแก้ไขข้อมูลที่สำคัญและอาจเกิดปัญหาในการปฏิบัติงานต่อไปได้

ข้อแนะนำ

ควรกำหนดให้มีรายงานการเปลี่ยนแปลงข้อมูล แสดงรายละเอียดการแก้ไขเปลี่ยนแปลง โดยแสดงทั้งข้อมูลเก่าและข้อมูลใหม่ที่เปลี่ยนแปลง

24) ไม่มีการพิมพ์วันที่ที่ทำรายงาน

การพิมพ์รายงาน (Report) ของระบบงานที่ประมวลผลด้วยคอมพิวเตอร์สถาบันการเงินไม่ได้กำหนดให้พิมพ์วันที่ที่เครื่องคอมพิวเตอร์ทำการพิมพ์รายงานนั้น ๆ เพียงแต่พิมพ์วันที่ของข้อมูลเท่านั้นอาจทำให้ผู้ปฏิบัติงานนำข้อมูลจากรายงานไปใช้ผิดพลาดได้

ข้อแนะนำ

ควรกำหนดให้พิมพ์วันที่ของข้อมูลหรือรายงาน และวันที่ที่เครื่องคอมพิวเตอร์พิมพ์รายงาน (Report) นั้น ในหน้ารายงานทุกหน้า

2.2 ระบบเงินฝากโดยภาพรวม ๆ

(1) จุดอ่อนของ Check Digit

เลขที่บัญชีลูกค้าที่สถาบันการเงินใช้ประกอบด้วยเลข 12 หลัก แยกเป็นกลุ่มตัวเลขได้ 5 กลุ่ม คือ x-xx-xxxxx-x-xxx

x	หมายถึง	Check Digit ที่ได้จากการถ่วงน้ำหนักตัวเลขกลุ่มที่ 2 และ กลุ่มที่ 3
xx	หมายถึง	รหัสประเภทเงินฝาก
xxxxx	หมายถึง	เลขที่บัญชีลูกค้าแต่ละประเภทเงินฝาก
x	หมายถึง	Branch Digit เป็นรหัสคุมอีกตัวหนึ่งที่ใช้ป้องกันข้อผิดพลาดของรายการต่างสาขา ได้จากการถ่วงน้ำหนักตัวเลขกลุ่มที่ 1 กลุ่มที่ 2 กลุ่มที่ 3 และกลุ่มที่ 5
xxx	หมายถึง	รหัสสาขาของสถาบันการเงิน

จากโครงสร้างเลขที่บัญชีลูกค้าข้างต้น อาจทำให้เกิดข้อผิดพลาดได้ ดังนี้

1) การทำรายการรับฝากเงินและถอนเงินภายในสาขาเดียวกัน อาจผิดบัญชีได้ เพราะเลขที่บัญชีที่ต่างกัน 50 หมายเลข จะมี Check Digit และ Branch Digit เหมือนกัน

2) การทำรายการรับฝากเงินและถอนเงินภายในสาขาเดียวกัน อาจผิดบัญชีและผิดสำนักงานสาขาได้ เพราะ Branch Digit สถาบันการเงินใช้ป้องกันการป้อนเลขที่สำนักงานสาขาผิดพลาดนั้นซ้ำซ้อนกันหลายสำนักงานสาขา

ข้อแนะนำ

สถาบันการเงินควรปรับปรุงระบบ Check Digit และ Branch Digit ให้มีประสิทธิภาพสามารถป้องกันข้อผิดพลาดที่อาจเกิดจากการรับฝากเงินหรือถอนเงินผิดบัญชีและผิดสำนักงานสาขาได้อย่างแท้จริง

(2) การคำนวณ Check Digit

จากรายงานรายละเอียดบัญชีเงินฝากออมทรัพย์ พบว่า บางบัญชีมี Check Digit ผิดปกติ เช่น บัญชีเลขที่ 3-001-001938 และ 3-001-052292 เป็นต้น ทั้งนี้เพราะซ้ำกับ Check Digit ของบัญชีที่เรียงอยู่ติดกันคือบัญชีเลขที่ 3-001-001928 และ 3-001-052282 เมื่อทดลองป้อนข้อมูลบัญชีที่ผิดปกติทั้งสอง จะเกิด Error Message ทางจอภาพว่า "Error Check Code Reentry" ซึ่งแสดงว่า Check Digit ของบัญชีทั้งคู่ไม่ถูกต้อง ควรจะเป็น 0 และ 3 ตามลำดับ เมื่อทดสอบป้อนเลขที่บัญชีโดยใช้ Check Digit ที่ถูกต้อง ปรากฏว่าเกิด Error Message สำหรับบัญชี 3-001-001930 ว่า "A/C # Not Found" หรือไม่มีบัญชีนี้ในแฟ้มข้อมูลของสถาบันการเงินที่เป็นเช่นนี้ก็เพราะว่าเลขที่บัญชีใน Master Saving File และ Record Pointer File (Index) ยังคงเป็น 3-001-001938 อยู่ จึงทำให้ไม่สามารถ Update หรือ Retrieve บัญชีนี้ได้

ข้อแนะนำ

สถาบันการเงินควรให้สำนักผู้ตรวจสอบภายในตรวจสอบความถูกต้องของเลขที่บัญชีเงินฝากทั้งหมดและแก้ไขให้ถูกต้อง

(3) สูตรคำนวณ Check Digit ไม่เหมาะสม

การควบคุมความถูกต้องในการป้อนข้อมูลเลขที่บัญชีนั้น สถาบันการเงินใช้เลข 5 เป็นค่าถ่วงน้ำหนักเลขที่บัญชีหลักที่ 6 ในการคำนวณ Check Digit ของเลขที่บัญชีเงินฝากทุกประเภท ซึ่งถ้าหากมีการป้อนเลขที่และบัญชีในหลักนี้ไม่ถูกต้อง เป็นเลขอื่นที่เป็นเลขคี่หรือเลขคู่เหมือนกัน ก็จะคำนวณได้ Check Digit เลขที่เดียวกัน ซึ่งหากผู้รับมอบอำนาจไม่ได้ใช้ความระมัดระวังแล้ว อาจทำให้มีการเข้าบัญชีลูกค้าผิดรายได้ โดยเฉพาะกรณีที่ไม่มีการพิมพ์หรือเขียนชื่อลูกค้าใน Slip เพื่อให้ตรวจสอบด้วย

นอกจากนี้ พบว่ามี Slip จำนวนมากมิได้เขียนชื่อบัญชีลูกค้า และเช็คที่สถาบันการเงินมอบให้ลูกค้าเพื่อลงนามสั่งจ่ายเงินจากบัญชีเงินฝากของตนไม่มีการพิมพ์ชื่อบัญชีในเช็คนี้ด้วย การควบคุมการป้อนเลขที่บัญชีผิดจึงเห็นว่ามีส่วนสำคัญมาก

ข้อแนะนำ

สถาบันการเงินควรกำหนดให้มีมาตรการควบคุมความถูกต้องของข้อมูล โดย :

1) กำชับและควบคุม Checker หรือ พนักงาน Authorized ตรวจสอบรายการเข้าบัญชี โดยเฉพาะเลขที่บัญชี ชื่อบัญชี และจำนวนเงิน ใน Slip หลังป้อนรายการให้ถูกต้องทุกครั้ง
2) ควรมีข้อแนะนำให้ลูกค้าเขียน Slip ให้สมบูรณ์ทั้งเลขที่บัญชีและชื่อบัญชี

(4) ไม่มีการตรวจสอบความครบถ้วนและความถูกต้องของเลขที่บัญชี

โปรแกรม Maintenance MASCUR ไม่มีการตรวจสอบความครบถ้วนของเลขที่บัญชีที่ป้อนเข้าสู่ระบบ โดยการกำหนดให้ Picture ของเลขที่บัญชีเป็น x (Alphanumeric) ซึ่งถือว่าเลขที่บัญชีของลูกค้าในตำแหน่งใดก็ตามที่ไม่มีข้อมูลหรือเป็นช่องว่าง (Blank) จะมีค่าเท่ากับศูนย์ (0) เป็นผลให้บัญชีที่มีตัวเลข Check Digit เป็นศูนย์กับบัญชีที่ Check Digit เป็น Blank จะมีค่าเท่ากัน ซึ่งอาจเกิดข้อผิดพลาดได้

ข้อแนะนำ

สถาบันการเงินควรกำหนดให้มีการตรวจสอบความครบถ้วนของเลขที่บัญชีที่ป้อนเข้าสู่ระบบและห้ามมิให้ใช้โปรแกรมประมวลผลงานที่มีค่า blank และศูนย์มีค่าเท่ากัน

(5) องค์กรกำหนดเงื่อนไขในระบบงานเงินฝากให้รับทำรายการฝากได้โดยพนักงาน Teller

พนักงาน Teller จะป้อนเลขที่บัญชีเงินฝากครบ 10 หลักหรือไม่ก็ได้ โดยเครื่องคอมพิวเตอร์จะเติมเลขที่สาขา Home Branch หรือเติมศูนย์ให้สำหรับค่าข้างหน้าที่มิได้ป้อนนั้น ทำให้องค์กรมิได้รับประโยชน์จากการควบคุมด้วย Check Digit เท่าที่ควร และหากพนักงานเข้าใจระบบงานไม่ดีพอ หรือเผลอเรอนำไปใช้กับการป้อนรายการฝากถอนต่างสาขา ก็อาจก่อให้เกิดการเข้าผิดบัญชีผิดสาขา และองค์กรอาจได้รับความเสียหายได้

(6) ในกรณีที่มีรายการฝาก-ถอนหลายรายการในบัญชีเดียวกัน พนักงานสามารถใช้รหัสรายการเป็น

Multiple เพื่อยกเว้นไม่ต้องป้อนเลขที่บัญชีได้นั้น อาจทำให้ตัดบัญชีหรือเข้าบัญชีเงินฝากแก่ลูกค้าผิดรายการได้โดยง่าย เนื่องจาก Check digit ของเลขที่บัญชีลูกค้าของสาขาหลายแห่งในเขตกรุงเทพมหานครซ้ำกัน

ข้อแนะนำ

ควรปรับปรุงแก้ไขระบบเงินฝากและการควบคุมภายในที่เกี่ยวข้อง ให้สามารถป้องกันข้อผิดพลาดในการถอนผิดบัญชีผิดสำนักงานสาขาในกรณีที่กล่าวข้างต้นได้อย่างเหมาะสมและเพียงพอตามควรแก่กรณี

(7) การคำนวณดอกเบี้ยจ่าย

โปรแกรมคำนวณดอกเบี้ยบัญชีเงินฝากผิดพลาด กล่าวคือ จากการทดสอบการคำนวณดอกเบี้ยจ่ายผู้ฝากรายตัว จำนวน 13 ราย พบว่า มีการบันทึกดอกเบี้ยจ่ายเกินกว่าที่พึงจ่าย 2 ราย ซึ่งอาจก่อให้เกิดการปฏิบัติที่ไม่ชอบด้วยกฎหมายได้ หากสถาบันการเงินจ่ายดอกเบี้ยให้ลูกค้าในอัตราสูงสุดตามที่กฎหมายกำหนดอยู่แล้ว และอาจทำให้สถาบันการเงินมีค่าใช้จ่ายสูงกว่าที่ควรอีกด้วย

จากการค้นหาสาเหตุของข้อผิดพลาดแล้ว ปรากฏว่า เกิดจากรายการเช็คคืนโดยโปรแกรมคำนวณดอกเบี้ยจะไม่ลดจำนวนดอกเบี้ยลงตามจำนวนเงินของเช็คที่คืน มีผลทำให้ดอกเบี้ยจ่ายสูงกว่าความเป็นจริง

ข้อแนะนำ

สถาบันการเงินควรกำหนดให้มีการทดสอบความถูกต้องของการคำนวณดอกเบี้ยเป็นครั้งคราวอย่างน้อย 1 ครั้ง

(8) ไม่สามารถยกเลิกรายการเรียกเก็บดอกเบี้ยที่คำนวณด้วย manual ได้

จากการทดสอบรายการ Reverse interest charge พบว่า รายการที่กล่าวไม่สามารถยกเลิกหรือล้างข้อมูล Accrued interest ที่ถูกบันทึกไว้ในแฟ้มข้อมูลด้วย รายการ Interest charge ได้อย่างแท้จริง ผู้ใช้ข้อมูลที่ทราบในภายหลังที่ดอกเบี้ยที่คำนวณด้วยมือ (Manual) ซึ่งบันทึกบัญชีด้วยรายการ Interest Cherge ไปแล้วมีข้อผิดพลาด และดำเนินการแก้ไขข้อผิดพลาดด้วยรายการ Reverse interest charge จะหลงเข้าใจผิดว่า จำนวน

ดอกเบี้ยที่เรียกเก็บจากลูกค้าไม่ถูกต้องนั้นโปรแกรมคอมพิวเตอร์ดำเนินการล้างรายการให้แล้ว อาจป้อนดอกเบี้ยจำนวนใหม่เข้าไปอีกเป็นผลให้สถาบันการเงินเรียกเก็บดอกเบี้ยจากลูกค้าซ้ำซ้อนและผิดพลาด

ข้อแนะนำ

สถาบันการเงินควรปรับปรุงแก้ไขข้อผิดพลาดในระบบงาน ให้สามารถใช้รายการต่าง ๆ ได้อย่างแท้จริง

(9) การปิดบัญชีโดยไม่บันทึกรายการดอกเบี้ย

การปิดบัญชีสามารถกระทำโดยข้ามขั้นตอนการบันทึกดอกเบี้ยได้ โดยไม่ต้องทำรายการ Interest/Tax Inquiry เพื่อบันทึกดอกเบี้ยเงินฝากและหักภาษีเงินได้หัก ณ ที่จ่ายก่อนปิดบัญชีด้วยรายการ A/C Closed Confirmation ซึ่งผู้ปฏิบัติงานอาจหลงลืมได้ เนื่องจากไม่มีข้อความใด ๆ (message) เตือนผู้ปฏิบัติงานให้ทราบว่าจะต้องทำรายการโอนดอกเบี้ยสะสมเข้าบัญชีลูกค้า

ข้อแนะนำ

สถาบันการเงินควรกำหนดให้ระบบมีข้อความเตือน (Message) ให้ผู้ทำรายการต้องบันทึกรายการดอกเบี้ยสะสมเข้าบัญชีให้ลูกค้าก่อนปิดบัญชี และในกรณีที่ต้องปิดบัญชีโดยมีดอกเบี้ยค้างอยู่ ควรให้ผู้มีอำนาจเป็นผู้อนุมัติรายการ

(10) การปรับปรุงโปรแกรมการคำนวณดอกเบี้ยตามอัตราใหม่

จากการทดสอบการคำนวณดอกเบี้ยจ่ายแก่ผู้ฝากเงิน ปรากฏว่าสถาบันการเงินใช้อัตราในการคำนวณดอกเบี้ยไม่ถูกต้อง กล่าวคือยังคงใช้อัตราดอกเบี้ยเดิมในการคำนวณดอกเบี้ยสำหรับเงินฝาก ไม่ได้เปลี่ยนอัตราดอกเบี้ยใหม่ตามที่ประกาศไว้

ข้อแนะนำ

สถาบันการเงินควรกำหนดขั้นตอนให้มีการควบคุมและตรวจสอบปรับปรุงอัตราดอกเบี้ยตามที่ประกาศใหม่โดยเคร่งครัด

(11) การกำหนดจำนวนวันที่ใช้คำนวณดอกเบี้ยเช็คคืนมากเกินความจำเป็น

การกำหนดจำนวนวันที่ใช้คำนวณดอกเบี้ยเช็คคืนถึง 3 หลัก (999 วัน) นั้นเกินความจำเป็นในการปฏิบัติงาน และอาจทำให้สถาบันการเงินได้รับความเสียหาย หากมีการป้อนข้อมูลจำนวนวันเช็คคืนผิดพลาด

ข้อแนะนำ

ควรกำหนดจำนวนวันที่ใช้คำนวณดอกเบี้ยเช็คคืนให้อยู่ในช่วงที่เหมาะสมและสอดคล้องกับการปฏิบัติงาน

(12) **ระบบงานคำนวณดอกเบี้ยคลาดเคลื่อนไปจากความเป็นจริง ในกรณีมีเช็คคืนบัญชีเดียวกันหลายฉบับ**

การคำนวณดอกเบี้ยเช็คคืน ระบบจะคำนวณให้โดยอัตโนมัติในงาน On - line ถ้ากรณียอดคงเหลือสิ้นวันก่อนมียอดเป็นเงินฝาก ระบบงานจะนำยอดเช็คคืนมาหักกับยอดคงเหลือก่อนแล้วจึงนำยอดที่เป็นเงินเบิกเกินบัญชีไปคำนวณดอกเบี้ย กรณีที่ทำรายการเช็คคืนบัญชีเดียวกันหลายฉบับ เช็คคืนฉบับแรกระบบจะคำนวณดอกเบี้ยถูกต้อง แต่เช็คคืนฉบับต่อไป การคำนวณดอกเบี้ยจะคลาดเคลื่อนไปจากความเป็นจริงเพราะระบบงานจะนำยอดคงเหลือสิ้นวันก่อนมาหักออกจากยอดเช็คคืนทุกครั้งที่ทำรายการ แล้วจึงนำไปคำนวณดอกเบี้ย ซึ่งจะทำให้สถาบันการเงินได้รับดอกเบี้ยน้อยกว่าความเป็นจริง

ข้อแนะนำ

ควรมีข้อความ (Message) เตือนให้พนักงานทราบกรณีมีการทำรายการเช็คคืนหลายฉบับในบัญชีเดียวกัน

(13) **การกำหนดจำนวนหลักของตัวเลขต่าง ๆ ไม่สอดคล้องกัน**

13.1) บัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและเงินเบิกเกินบัญชี ซึ่งกำหนดให้ยอดคงเหลือตามบัญชีมีหลักเป็นพันล้านบาท หากมีการทำรายงานที่ทำให้ยอดคงเหลือตามบัญชีเป็นหลักหมื่นล้านบาทจะมีผลทำให้การทำรายการในลำดับต่อไปไม่ถูกต้องด้วย เพราะระบบไม่สามารถนำยอดคงเหลือที่ถูกต้องไปใช้ประมวลผลต่อไปได้

13.2) บัญชีเงินฝากออมทรัพย์

- การทำรายการฝาก-ถอน เครื่องสามารถรับได้สูงสุดเป็นหลักพันล้านแต่จำนวนเงินฝาก-ถอนแต่ละรายการที่พิมพ์ในสมุดคู่ฝาก (Pass Book) พิมพ์ได้สูงสุดเพียงหลักสิบล้าน
- ยอดเงินคงเหลือในบัญชีลูกค้า เครื่องสามารถรับได้สูงสุดเป็นหลักพันล้าน แต่ยอดเงินคงเหลือที่พิมพ์ในสมุดคู่ฝาก พิมพ์ได้สูงสุดเพียงหลักร้อยล้าน

13.3) มีการตัดจำนวนหลักตัวเลขอ้างอิงในการทำรายการซึ่งมีอยู่ 8 หลักมาพิมพ์ในรายงาน Daily Transaction เพียง 7 หลัก ซึ่งจะทำให้เกิดความสับสนและเป็นปัญหาในการใช้ข้อมูลอ้างอิง

13.4) จากการทดสอบรายการ Change Passbook Number เพื่อเปลี่ยนเลขที่สมุดคู่ฝากซ้ำกันหลายครั้ง จากเลขที่ 00000000 เป็นเลขที่ 22222222 และ จากเลขที่ 22222222 เป็นเลขที่ 23232323 พบว่าเลขที่ของสมุดคู่ฝากก่อนเปลี่ยนครั้งหลังสุดคือ เลขที่ 22222222 ถูกพิมพ์ในรายงานเป็นเลขที่ 02222222 ซึ่งไม่ถูกต้องเนื่องจากการเก็บข้อมูลดังกล่าวจะเก็บไว้เพียง 7 หลัก แต่พิมพ์ในรายงาน 8 หลัก จึงทำให้เกิดปัญหาดังกล่าวขึ้น

ข้อแนะนำ

องค์กรควรปรับปรุงแก้ไขหลักเกณฑ์ในการกำหนดจำนวนหลักของตัวเลขต่าง ๆ ในระบบงานเงินฝากให้ถูกต้องและสอดคล้องซึ่งกันและกัน เพื่อป้องกันข้อผิดพลาดในการประมวลผลข้อมูล และการนำข้อมูลไปใช้งาน

(14) ความน่าเชื่อถือของข้อมูล

ผู้ทำรายการสามารถป้อนตัวเลขข้อมูลได้มากกว่าจำนวนหลักที่กำหนดไว้ในคู่มือปฏิบัติงานจะมีผลทำให้ผู้ใช้ข้อมูลเกิดความสับสนและไม่แน่ใจว่าข้อมูลดังกล่าวที่เก็บอยู่ในระบบงานมีความถูกต้อง

ข้อแนะนำ

ควรให้ระบบคอมพิวเตอร์ปฏิเสธ Status และอัตราดอกเบี้ยที่ป้อนเข้าสู่ระบบมากกว่าจำนวนหลักที่กำหนดไว้ เพื่อป้องกันข้อผิดพลาดในการป้อนข้อมูล

(15) การควบคุมเงินสดในมือพนักงาน Teller ยังไม่รัดกุม

- องค์กรมิได้กำหนดปริมาณเงินสดในมือของพนักงาน teller เพื่อจำกัดความรับผิดชอบของพนักงาน teller ให้อยู่ภายในขอบเขตที่เหมาะสม ทั้งนี้เพื่อลดความเสี่ยงภัยในการรับจ่ายเงินสดระหว่างวัน

ข้อแนะนำ

องค์กรควรกำหนดวงเงินสดในมือพนักงาน teller ก็ต้องทำหน้าที่ควบคู่กัน 2 ด้าน คือ ด้านการเงินและด้านการบัญชี เพื่อทดแทนการแบ่งแยกหน้าที่พนักงานซึ่งเป็นวิธีการควบคุมภายในที่เคยใช้ในระบบเดิม นอกจากนี้ยังช่วยลดความเสี่ยงภัยในการรับ-จ่ายเงินสดระหว่างวันของพนักงาน teller ด้วย

- การทำรายการรับและส่งคืนเงินสดซึ่งจะต้องป้อนเครื่องนั้น พนักงานออเธอไรส์เทลเลอร์สามารถทำรายการได้โดยไม่ต้องผ่านการอนุมัติรายการจากพนักงานระดับเทลเลอร์ซุปเปอร์ไวเซอร์ เพียงแต่ลงนามในใบแสดงการรับ-ส่งเงินสด เมื่อเงินสดในมือพนักงานออเธอไรส์เทลเลอร์เต็มวงเงินที่กำหนดไว้ เครื่องจะไม่ให้ทำรายการต่อ พนักงานออเธอไรส์เทลเลอร์ก็สามารถทำรายการส่งคืนเงินสดได้ โดยที่ยังไม่ได้ส่งคืนเงินจริง ซึ่งเป็นวิธีปฏิบัติที่ไม่ปลอดภัยและอาจเกิดความเสียหายต่อองค์กรได้

ข้อแนะนำ

ควรปรับปรุงระบบงานให้มีการผ่านรายการโดยพนักงานเทลเลอร์ซุปเปอร์ไวเซอร์ ในกรณีที่รายการรับและส่งคืนเงินสด เพื่อให้การควบคุมเงินสดในมือพนักงานรัดกุมยิ่งขึ้น

(16) ไม่มีการจำกัดอำนาจการทำรายการที่มีจำนวนเงินสูง

องค์กรให้อำนาจพนักงาน Teller บันทึกรายการฝาก-ถอนจำนวนเงินได้โดยไม่มีพนักงานผู้รับมอบอำนาจอนุมัติรายการก่อน ประกอบกับมิได้กำหนดวงเงินสดที่อนุญาตให้พนักงาน teller ถือไว้ในมือหากมีข้อผิดพลาดในการปฏิบัติงานหรือการทุจริตเกิดขึ้น องค์กรจะเสียหายมาก

ข้อแนะนำ

องค์กรควรกำหนดให้มีการควบคุมการบันทึกรายการฝาก-ถอนที่มีจำนวนเงินสูง ๆ เป็นพิเศษ เช่น กำหนดให้คอมพิวเตอร์ตรวจสอบรายการฝาก-ถอนจำนวนเงินสูง โดยผ่านการอนุมัติจากผู้ได้รับมอบอำนาจก่อน

(17) การปรับปรุงยอดดอกเบี้ยโดยไม่จำกัดจำนวนเงินสูงสุด

การอนุญาตให้พนักงาน Teller ปรับปรุงยอดดอกเบี้ยของลูกค้าด้วยรหัสรายการ INTEREST ADJUST โดยไม่จำกัดจำนวนเงินสูงสุด ประกอบกับการปรับปรุงยอดดอกเบี้ยจะไม่ปรากฏในการกระทบยอดตอนสิ้นวันทำการ และลูกค้ามีสิทธิถอนดอกเบี้ยที่เกิดจากรายการดังกล่าว หลังจากที่ระบบคอมพิวเตอร์ได้ผ่านดอกเบี้ยเข้าบัญชีแล้วได้ทันที อาจทำให้องค์กรได้รับความเสียหาย

ข้อแนะนำ

ควรควบคุมการทำรายการปรับปรุงดอกเบี้ยของลูกค้าที่มีจำนวนเงินสูง ๆ โดยให้ผ่านการอนุมัติของผู้รับมอบอำนาจก่อน

(18) การเปิดบัญชีใหม่ด้วยเลขที่บัญชีเก่าย้อนหลังได้

รายงานเงินฝากทุกประเภทไม่มีการป้องกันการเปิดบัญชีด้วยเลขที่บัญชีเก่าย้อนหลังได้ วิธีปฏิบัติดังกล่าวไม่มีประโยชน์ต่อการปฏิบัติงานประจำวัน เพราะมีโปรแกรมอื่นที่จะทำการเปิดบัญชีที่ปิดผิดบัญชีได้ใหม่อยู่แล้ว

ข้อแนะนำ

ควรจะแก้ไขระบบเพื่อป้องกันปัญหาการใช้เลขที่บัญชีเก่าให้รัดกุมยิ่งขึ้น นอกจากนี้เพื่อป้องกันปัญหาในกรณีที่ purge ออกไปแล้ว ควรกำหนดให้ใช้เลขที่บัญชีเรียงตามลำดับจากน้อยไปหามากเสมอ และไม่ยอมให้มีการเลือกใช้เลขที่บัญชีย้อนหลัง

(19) ขั้นตอนในการจัดทำบัตร CD (Cash Dispensor) ให้ลูกค้า มีการควบคุมไม่รัดกุม

ในปัจจุบันองค์กรได้ว่าจ้างบุคคลภายนอกจัดทำบัตร CD ให้ แต่ไม่ได้กำหนดขั้นตอนในการควบคุมการจัดทำบัตรให้รัดกุม กล่าวคือ เนื่องจากอุปกรณ์ในการจัดทำบัตร CD ของบริษัทผู้จัดทำบัตรให้จะต้องอาศัยเครื่องอ่านเทปแม่เหล็กในการอ่านข้อมูลเข้าระบบจัดทำบัตร CD แต่องค์กรไม่มีเครื่องบันทึกข้อมูลของลูกค้าที่จะใช้บริการ CD เก็บไว้ในเทปแม่เหล็ก พนักงานขององค์กรจะต้องนำข้อมูลดังกล่าวไปประมวลผลให้มีการจัดเก็บข้อมูลไว้ในเทปแม่เหล็กที่บริษัทผู้ขายเครื่อง CD ให้องค์กร หลังจากนั้นพนักงานองค์กรนั้นจะจัดส่งไปยังบริษัทผู้จัดทำบัตร CD เพื่อทำบัตรต่อไป

ข้อแนะนำ

จากขั้นตอนข้างต้น องค์กรไม่สามารถควบคุมได้ว่าข้อมูลจะตกค้างอยู่ในเครื่องคอมพิวเตอร์ของบริษัทผู้ขายเครื่อง CD ให้องค์กรหรือไม่ และในขั้นตอนการจัดทำบัตร CD องค์กรก็ไม่สามารถควบคุมการจัดทำบัตร CD ได้ โดยเฉพาะจำนวนบัตร องค์กรจึงควรพิจารณาปรับปรุงแก้ไขปัญหาดังกล่าวโดยการสั่งซื้อเครื่องมาทำบัตร CD เอง

(20) **การโอนบัญชี Active ไปเป็นบัญชี Unclaimed เป็นผลให้รายการเงินสดไม่ถูกต้อง**

จากการทดสอบพบว่า การโอนบัญชีที่เคลื่อนไหวไปเป็นบัญชีที่ไม่เคลื่อนไหว ปรากฏว่าโปรแกรมจะผ่านรายการโอนปิดบัญชีที่เคลื่อนไหวด้วยรายการเงินสด (Transaction Code "C") แล้วไปเปิดบัญชีที่ไม่เคลื่อนไหวด้วยรายการยอดยกมา (Transaction Code "B/F") เป็นผลให้รายการปิดบัญชีที่เคลื่อนไหวไปรวมยอดในรายงาน "สรุปยอดสลิปแยกตามประเภท" และรายงาน "สรุปใบสำคัญประจำวัน" ในรายการเงินสดซึ่งผิดหลักการบัญชี เพราะรายการดังกล่าวไม่ใช่รายการเงินสด นอกจากนี้การโอนบัญชีที่เคลื่อนไหวไปเป็นบัญชีที่ไม่เคลื่อนไหวนั้น จะมีข้อมูลแสดงในรายงาน "รายงานบัญชีที่ปิด" แสดงว่าบัญชีที่ถูกโอนนั้นเป็นบัญชีที่ปิดแล้ว ซึ่งเป็นข้อมูลที่ไม่ถูกต้อง เพราะบัญชีที่กล่าวเป็นบัญชีที่ยังเปิดอยู่

ข้อแนะนำ

ควรบันทึกรายการที่เกิดขึ้นให้ตรงกับข้อเท็จจริง และถูกต้องตามหลักการบัญชี

(21) **การควบคุมบัญชีที่ไม่เคลื่อนไหวขาดการติดต่อจากลูกค้า**

ระบบเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและระบบเงินฝากออมทรัพย์ มีบัญชีเงินฝากที่ไม่เคลื่อนไหวรวมอยู่กับบัญชีเงินฝากที่เคลื่อนไหว และอนุญาตให้พนักงาน Teller ผ่านรายการในบัญชีที่ไม่เคลื่อนไหวได้โดยไม่ต้องผ่านการอนุมัติรายการจากพนักงานผู้ถือบัตร SUPERVISOR ก่อน

ข้อแนะนำ

ควรแยกเงินฝากที่ไม่เคลื่อนไหวขาดการติดต่อ เป็นระยะเวลานานออกจากบัญชีเงินฝากที่เคลื่อนไหว และหากมีรายการเคลื่อนไหวของบัญชีดังกล่าว ก็ควรให้ผ่านการอนุมัติรายการจากพนักงานผู้ถือบัตร SUPERVISOR ก่อนทุกครั้ง

(22) **บัญชีเงินฝากที่ขาดการติดต่อ**

องค์กรได้โอนบัญชีเงินฝากที่ขาดการติดต่อนานเกินกว่า 2 ปี และมียอดคงค้างต่ำกว่า 100 บาท ออกจาก Master File ทุกสิ้นปี ไปพักไว้ในบัญชี Unclaimed Balance Account รวมกับบัญชี Cashier' order ที่ไม่มีผู้มารับเงิน และจะบันทึกรายละเอียดบัญชีเหล่านี้ไว้ใน Floppy Disk เพื่อใช้ในการจัดทำรายงานรายละเอียดบัญชีที่ขาดการติดต่อตอนสิ้นงวดบัญชี โดยออกยอดสุดท้ายรวมกัน

ในรายงานดังกล่าวมิได้มีการแยกแสดงยอดรวมของเงินฝากแต่ละประเภทไว้ และประกอบกับได้จัดทำบัญชีคุมยอดย่อย (Sub-Ledger) บัญชีเงินฝากที่ขาดการติดต่อ จึงทำให้ไม่สามารถทราบยอดรวมของเงินฝากที่ขาดการติดต่อแต่ละประเภทในแต่ละวันได้ ซึ่งจะส่งผลให้การจัดทำรายงานการดำรงเงินสดสำรอง และรายงานอื่น ๆ คลาดเคลื่อนจากความเป็นจริง

ข้อแนะนำ

ควรกำหนดให้การจัดทำรายงานรายละเอียดบัญชีที่ขาดการติดต่อ แยกแสดงยอดรวมของเงินฝากแต่ละประเภท พร้อมทั้งจัดทำบัญชีคุมยอดย่อย (Sub - Ledger) ด้วย

(23) **การควบคุมการผ่านรายการ**

เงินฝากทุกประเภทขององค์กรยินยอมให้ Operator ผ่านรายการที่สำคัญได้ โดยไม่ต้องขออนุมัติจากพนักงานชั้นบริหาร ได้แก่

- การผ่านรายการเปิดบัญชีใหม่
- การผ่านรายการเงินฝากได้โดยไม่จำกัดจำนวนเงินฝาก
- ทำการแก้ไขรายการฝากถอนที่ผ่านเข้าระบบคอมพิวเตอร์แล้ว
- การป้อนเลขที่เช็คซึ่งใช้ในการควบคุมการผ่านรายการถอนด้วยเช็คผิดบัญชี

หรือมีการอนุญาตให้พนักงานเทเลอร์ทำรายการที่มีผลกระทบต่อแฟ้มข้อมูลหลักได้โดยลำพัง เช่น

- Clearing deposit
- Cash a cheque
- Transfer withdrawal cheque
- Electric cheque nobook
- Telephone cheque nobook
- Waterwork cheque nobook
- Comission debit nobook
- Clearing cheque deposit nobook

ข้อแนะนำ

องค์การควรพิจารณาวิธีปรับปรุงแก้ไขการควบคุมการผ่านรายการให้รัดกุมยิ่งขึ้น และกำหนดให้มีพนักงานชั้นบริหารควบคุมดูแลพนักงานเทลเลอร์ทำรายการที่สำคัญ หรือ รายการที่มีผลกระทบต่อแฟ้มข้อมูลหลักโดยใกล้ชิด

(24) **การควบคุมรายการที่ทำผ่านเครื่องเทอร์มินอล**

ระบบเงินฝากที่ใช้อยู่ในปัจจุบัน เปิดโอกาสให้พนักงาน Teller สามารถทำรายการที่สำคัญโดยไม่มีระบบป้องกันหรือข้อห้ามการทำรายการแต่อย่างใด ซึ่งอาจทำให้องค์กรได้รับความเสียหาย ดังนี้

1) พนักงาน Teller สามารถลงรายการล้างข้อมูลในแฟ้มข้อมูลหลัก (Master File) ทั้งจากสาขานั้นเองหรือจากต่างสาขาได้ อาจเป็นสาเหตุให้มีการล้างข้อมูลของลูกค้าออกไปได้โดยปราศจากร่องรอยหรือหลักฐาน เนื่องจากไม่มีการพิมพ์รายงานแสดงรายละเอียดของการทำรายการให้พนักงานชั้นบริหารตรวจทานเป็นพิเศษ

2) พนักงาน Teller สามารถสั่งเครื่องคอมพิวเตอร์ให้ปิดระบบการให้บริการเงินฝากแก่ลูกค้าได้ตลอดเวลา อาจทำให้บริการขององค์กรหยุดชะงักลงได้

3) พนักงาน Teller สามารถเปลี่ยนสภาพหรือปลดการอายัดรายการฝากเช็คเรียกเก็บ จึงอาจทำให้องค์กรเสียหายได้ เพราะจะทำให้ยอดเงินที่ฝากด้วยเช็คซึ่งยังไม่ทราบผลการเรียกเก็บที่ถูกอายัดไว้ เปลี่ยนเป็นยอดเงินที่สามารถถอนได้ทันที

ข้อแนะนำ

องค์กรควรควบคุมและป้องกันมิให้ทำรายการที่สำคัญ ๆ ผ่านเครื่องเทอร์มินอลของสาขาที่เป็นระบบ On-line ควรให้ทำได้เฉพาะศูนย์คอมพิวเตอร์สำนักงานใหญ่เท่านั้น เช่น

- DELETE MASTER FILE
- CLOSE SYSTEM
- CHANGE SYSTEM BIT

(25) การใช้บัตรควบคุมการผ่านรายการไม่รัดกุม

องค์กรไม่มีระเบียบเกี่ยวกับการกำหนดตัวพนักงานของสำนักงานใหญ่ที่มีสิทธิใช้บัตรควบคุมการผ่านรายการเป็นที่แน่ชัด กล่าวคือ

1) ยินยอมให้พนักงาน Teller ใช้บัตรผ่านรายการระดับ ASC (Assistant Supervisor Card) ซึ่งสามารถทำรายการที่สำคัญได้ เช่น การเปิดบัญชี การแก้ไขรายการ เป็นต้น

2) ยินยอมให้พนักงาน Teller คนใดคนหนึ่ง เซ็นรับและส่งคืนบัตรควบคุมการผ่านรายการระดับต่าง ๆ แทนพนักงานอื่นซึ่งเป็นผู้ใช้บัตร ในตอนเช้าและตอนเลิกงานประจำวัน

3) พนักงาน Checker มอบบัตรควบคุมการผ่านรายการระดับ SC (Supervisor Card) ให้พนักงานอื่นทำแทนในระหว่างที่ตนไม่อยู่

ข้อแนะนำ

องค์กรไม่ควรยินยอมให้พนักงาน Teller ถือบัตรผ่านรายการของผู้มีอำนาจ ส่วนพนักงาน Checker ให้ถือบัตรผ่านรายการระดับ ASC และให้พนักงานผู้มีอำนาจลงนาม (Authorized) ถือบัตรผ่านรายการระดับ SC นอกจากนี้ ให้ผู้มีอำนาจถือบัตรผ่านรายการแต่ละคนเซ็นชื่อรับและส่งคืนบัตรเมื่อเริ่มและเสร็จสิ้นปฏิบัติงานประจำวัน และหากมอบบัตรผ่านรายการให้บุคลอื่นทำรายการแทนในระหว่างที่ตนไม่สามารถปฏิบัติงานได้ ก็ควรบันทึกในทะเบียนไว้เป็นหลักฐาน

(26) การควบคุมการใช้บัตรอนุมัติรายการ และกุญแจเทลเลอร์ซุปเปอร์ไวเซอร์ไม่รัดกุม

มีการมอบหมายบัตรอนุมัติรายการให้กับพนักงาน Teller หรือมีการเสียบกุญแจคาไว้ที่ Keyboard ตลอดเวลา ซึ่งอาจเป็นสาเหตุให้ไม่สามารถยืนยันและค้นหาผู้รับผิดชอบในกรณีมีปัญหาในการปฏิบัติงานได้

ข้อแนะนำ

เพื่อให้การควบคุมรายการมีความรัดกุมยิ่งขึ้น องค์กรควรห้ามมิให้มีการมอบบัตรอนุมัติรายการให้กับพนักงาน teller หรือไม่ให้เสียบกุญแจเทลเลอร์ซุปเปอร์ไวเซอร์คาไว้ที่ Keyboard แล้วแต่กรณี

(27) การถือบัตรอนุมัติรายการ

การมอบบัตรอนุมัติรายการชั้นอื่นระดับอื่นให้แก่พนักงานที่ถือบัตรอนุมัติรายการชั้น 8 ระดับ 8 อยู่แล้ว จะมีผลทำให้การควบคุมการผ่านรายการบางประเภทไม่รัดกุมเท่าที่ควร ซึ่งเรื่องนี้มีปัญหาที่พนักงานผู้ควบคุมจะปฏิบัติตามที่ได้กำหนดไว้หรือไม่ ซึ่งในบางครั้งก็จำเป็นต้องไว้ใจพนักงานด้วยกัน

ข้อแนะนำ

เพื่อประโยชน์ในการควบคุมการผ่านรายการบางประเภท องค์กรไม่ควรมอบบัตรอนุมัติรายการชั้นอื่นระดับอื่นให้แก่พนักงานที่ถือบัตรอนุมัติรายการชั้น 8 ระดับ 8 อยู่แล้ว

(28) ระบบงานยินยอมให้สามารถใช้บัตรอนุมัติรายการเปิดเครื่องเทอร์มินอล

การยินยอมให้ใช้บัตรอนุมัติรายการ (Supervisor Card) ทำการเปิดเครื่องเทอร์มินอล (Sign on) แทนบัตรพนักงาน Teller ส่งผลให้การทำรายการบางประเภทที่ต้องใช้บัตรอนุมัติรายการสามารถผ่านรายการได้ และโดยเหตุที่พนักงานระดับที่มีอำนาจหน้าที่ในการอนุมัติรายการนั้นมิได้ประจำเครื่องเทอร์มินอล อาจทำให้การอนุมัติการทำรายการเป็นไปโดยไม่เหมาะสม

ข้อแนะนำ

เพื่อป้องกันมิให้เกิดจุดอ่อนในระบบควบคุมการอนุมัติรายการ ไม่ควรอนุญาตให้ผู้อนุมัติรายการหรือพนักงานซึ่งทำหน้าที่ควบคุมดูแลการปฏิบัติงานของพนักงาน Authorize Teller เป็นผู้เปิดเครื่องเทอร์มินอล

(29) การรักษาความปลอดภัย Password ของพนักงานชั้นบริหาร

Operator อาจทราบ Password ของพนักงานชั้นบริหารได้โดยง่าย เพราะการปฏิบัติงานในบางกรณี พนักงานชั้นบริหารจำเป็นต้องป้อน Password ที่จอภาพของ Operator เปิดโอกาสให้ Operator รู้เห็น Password ของพนักงานชั้นบริหาร ซึ่งจะมีผลทำให้การควบคุมการใช้ Card ของพนักงานชั้นบริหารซึ่งเป็นเครื่องมือที่ใช้ในการควบคุมการปฏิบัติงานประจำวันไม่ได้ผลเท่าที่ควร

ข้อแนะนำ

องค์กรควรแนะนำให้พนักงานชั้นบริหารเพิ่มความระมัดระวังในการป้อน Password หรือ ปรับปรุงระบบคอมพิวเตอร์ให้แยกจอการอนุมัติรายการออกจากจอบันทึกรายการของ Operator นอกจากนี้ควรกำหนด ให้มีการเปลี่ยนแปลง Password เป็นครั้งคราว เพื่อป้องกันมิให้พนักงานอื่นที่ไม่เกี่ยวข้องทราบได้ง่าย

(30) การรักษาความปลอดภัยเกี่ยวกับรหัสประจำตัวพนักงาน Teller ยังไม่รัดกุม

ในกรณีที่พนักงาน Teller ลืมรหัสประจำตัว ผู้ช่วยผู้อำนวยการฝ่ายการธนาคาร หรือผู้จัดการสาขา สามารถเรียกดูรหัสประจำตัวของพนักงานของผู้นั้นโดยผ่านเครื่อง Terminal ที่พนักงาน Teller ใช้ปฏิบัติงานได้ ซึ่งรหัสประจำตัวของพนักงาน Teller ทุกคนของสำนักงานที่เรียกดู จะปรากฏขึ้นที่จอภาพ อาจเป็นช่องทางให้พนักงาน Teller ในสำนักงานนั้นล่วงรู้รหัสประจำตัวซึ่งเป็นความลับของผู้อื่นได้

ข้อแนะนำ

องค์กรควรยกเลิกรหัสรายการ Inquiry Password Station หากพนักงาน Teller ลืมรหัสประจำตัว สามารถสอบถามได้จากผู้จัดการสาขาหรือผู้ช่วยผู้อำนวยการฝ่ายการธนาคาร ซึ่งเป็นผู้กำหนด Teller Password ได้อยู่แล้ว

(31) โปรแกรมระบบงานบางส่วนใช้ข้อมูลจากแฟ้มข้อมูลข้ามระบบงานโดยไม่ถูกต้อง

จากรายงานการทดสอบรายงาน "Daily Stopped Cheque Report" แสดงรายการระงับเช็คของบัญชีเงินฝากประจำ ซึ่งไม่ถูกต้องเพราะบัญชีเงินฝากประจำไม่มีการใช้เช็คในการถอนเงินจากบัญชี

ข้อแนะนำ

องค์กรควรแก้ไขโปรแกรมการประมวลผลงานให้ถูกต้อง

(32) ไม่มีการตรวจสอบ Journal Roll เป็นครั้งคราว

องค์กรไม่ได้กำหนดให้ผู้รับมอบอำนาจตรวจสอบ Journal Roll ซึ่งเป็นเอกสารสำคัญในการติดตามและตรวจสอบรายการที่ทำผ่านเครื่องคอมพิวเตอร์ เพื่อทบทวนการปฏิบัติงานผ่านเครื่องเทอร์มินอลเป็นครั้งคราว

ข้อแนะนำ

องค์กรควรกำหนดให้ผู้รับมอบอำนาจตรวจสอบ Journal Roll เป็นครั้งคราว

(33) การเก็บรักษา Journal Roll ไม่มีความปลอดภัยเท่าที่ควร

การจัดเก็บ Journal Roll ที่บันทึกรายละเอียดในการปฏิบัติงานผ่านเครื่อง Terminal ซึ่งเป็นหลักฐานที่มีความสำคัญต่อการควบคุมและตรวจสอบ ยังไม่เรียบร้อยครบถ้วนและไม่ได้กำหนดระเบียบปฏิบัติในเรื่องนี้ไว้เป็นลายลักษณ์อักษร เอกสารดังกล่าวอาจสูญหายหรือถูกทำลายได้

ข้อแนะนำ

ควรจัดเก็บ Journal Roll ให้ครบถ้วน และมีการควบคุมการใช้ Journal Roll เช่นเดียวกับสมุดบัญชี เพื่อให้มีเอกสารหลักฐานที่จำเป็นต้องใช้ในการควบคุมและตรวจสอบการปฏิบัติงานผ่านเครื่อง Terminal อย่างเพียงพอ

(34) จุดอ่อนในการทำรายการอายัดเงินฝาก

1) พนักงานสามารถทำรายการอายัดเงินฝากได้เป็นจำนวนมากกว่ายอดเงินฝากคงเหลือที่พึงถอนได้ (Avaliable Balance) หรือยอดคงเหลือตามบัญชี (Ledger Balance) หรืออายัดเงินฝากส่วนที่เป็นเช็คเคลียริ่งซึ่งยังไม่ทราบผลการเรียกเก็บเงินได้ โดยไม่ตรวจสอบยอดคงเหลือก่อน

2) พนักงานทำรายการแก้ไขรายการฝากเงินที่เคยถูกอายัดไว้แล้ว แต่มิได้ล้างรายการคู่ที่อายัดให้สอดคล้องกับยอดเงินฝากที่ลดลงทั้งสองกรณีดังกล่าว ทำให้จำนวนเงินที่อายัดไว้เพื่อเป็นหลักประกันในการให้สินเชื่อแก่ลูกค้าแสดงมูลค่าสูงกว่าความเป็นจริง

ข้อแนะนำ

องค์กรควรแก้ไขโปรแกรมไม่ให้มีการอายัดเงินฝากเกินกว่ายอดคงเหลือที่พึงถอนได้ และยอดคงเหลือตามบัญชี หรืออายัดเงินฝากที่เป็นเช็คเคลียริ่งซึ่งยังไม่ทราบผลการเรียกเก็บเงิน และกำชับให้พนักงานล้างการอายัดเงินฝากทุกครั้งที่มีรายการแก้ไขลดยอดเงินฝาก เพื่อให้มูลค่าของหลักประกันถูกต้องและน่าเชื่อถือได้

(35) ข้อมูลของลูกค้าสูญหาย

การลบล้างข้อมูลลูกค้าออกจาก Master File ในกรณีที่ยอดคงเหลือในบัญชีเป็นศูนย์ ผ่านเครื่อง Terminal ของสาขาเจ้าของบัญชีหรือต่างสาขา มีผลทำให้ข้อมูลของลูกค้าใน Master File และรายการเคลื่อนไหวในวันนั้นสูญหายไปโดยไม่ปรากฏหลักฐานในการทำรายการในรายงานใด ๆ ซึ่งจะทำให้องค์กรต้องเสียเวลาติดตามรายการดังกล่าวจาก Journal Roll นอกจากนี้ ลูกค้าไม่สามารถมาฝากเงินเข้าบัญชีได้ทั้งที่ยังไม่ได้ปิดบัญชี

ข้อแนะนำ

องค์กรควรควบคุมและป้องกันไม่ให้มีการลงล้างข้อมูลโดยใช้รหัสรายการ Delete Master File เพื่อป้องกันมิให้ข้อมูลของลูกค้าสูญหายไป และเกิดความยุ่งยากในการติดตามรายการ

(36) การควบคุมการแก้ไขข้อความบนเอกสารสำคัญไม่รัดกุม

จากการตรวจสอบปรากฏว่าองค์กรได้ใช้วิธีขูด ลบ หรือใช้น้ำยาสีขาวป้ายข้อความเดิมบนเอกสารสำคัญ เช่น สัญญาต่าง ๆ หรือทะเบียนบันทึกที่เกี่ยวข้องกับจำนวนเงิน แล้วเขียนหรือพิมพ์ข้อความใหม่ทับลงไป ซึ่งทำให้ไม่ทราบว่าการแก้ไขข้อความนั้นกระทำไปโดยชอบธรรมหรือไม่

ข้อแนะนำ

ควรใช้วิธีขีดฆ่าหรือบันทึกบัญชีกลับรายการ (Reverse) ที่ผิด แล้วบันทึกสิ่งที่ถูกต้องใหม่ โดยกำหนดให้พนักงานชั้นบริหารลงนามกำกับรายการแก้ไขทั้งหมดด้วย

(37) **การเก็บรักษาเอกสารสำคัญไม่เรียบร้อย**

การจัดเก็บ Journal Roll ที่บันทึกรายละเอียดในการปฏิบัติงานผ่านเครื่อง Terminal ยังมิได้ให้พนักงานชั้นบริหารลงนามในตอนต้นและสิ้นสุดของวัน และมิได้แยกเก็บเอกสารเป็นรายวันตามระเบียบการปฏิบัติงาน ทำให้การควบคุมเอกสารดังกล่าวไม่เรียบร้อยเท่าที่ควร

ข้อแนะนำ

ควรกำหนดให้มีการดูแลควบคุมการเก็บรักษาเอกสารสำคัญโดยพนักงานชั้นบริหาร

(38) **ความสมเหตุสมผลของข้อมูล**

ข้อมูลต่าง ๆ ที่ป้อนเข้าสู่ระบบคอมพิวเตอร์ตามข้อกำหนดในการทำรายการบางประเภทไม่ได้มีการทดสอบความเป็นไปได้ของข้อมูล เพื่อป้องกันความผิดพลาดเท่าที่ควร ซึ่งข้อผิดพลาดในบางกรณีจะมีผลกระทบต่อความถูกต้องเชื่อถือได้ในการประมวลผลข้อมูล

ในระบบงานขององค์กรโดยทั่วไปจะมีการตรวจสอบข้อมูล (Edit) หลายประเภทอยู่แล้ว แต่ไม่สามารถตรวจสอบได้ครบ 100% จึงต้องให้พนักงานเป็นผู้ตรวจสอบความถูกต้องในการทำรายการประกอบด้วย

ข้อแนะนำ

ควรมีการทดสอบความเป็นไปได้ของข้อมูลบางประเภทก่อนที่จะยอมรับเก็บไว้ในระบบคอมพิวเตอร์

(39) **ไม่มีการควบคุมการใช้รหัสรายการ Convert ข้อมูลในการปฏิบัติงาน On line**

การปล่อยรหัสรายการ CONVERSION NEW ACCT. ซึ่งใช้เพียงครั้งเดียวในกรณีเมื่อต้องการนำข้อมูลบัญชีของลูกค้าจากระบบเงินฝากเดิม เข้าไปเก็บในเครื่องคอมพิวเตอร์ของระบบใหม่ในช่วงที่มีการเปลี่ยนระบบงาน ไว้ในระบบงานเหมือนเป็นรายการปกตินั้น จากการทดสอบการทำรายการดังกล่าวพบว่า ในรายงาน Daily Current Account Transaction ไม่แสดงรายละเอียดของรายการดังกล่าว และไม่รวมอยู่ในยอดคงเหลือ ณ สิ้นวันที่ทำรายการด้วย ดังนั้น หากมีการนำรหัสรายการดังกล่าวมาใช้งานภายหลังจากที่มีการเปลี่ยนแปลงระบบแล้ว อาจทำให้รายงานแสดงข้อมูลคลาดเคลื่อนจากความเป็นจริง

ข้อแนะนำ

องค์กรควรยกเลิกรหัสรายการ Conversion New Acct. ภายหลังการนำระบบงานคอมพิวเตอร์ออกใช้แล้ว เพื่อป้องกันข้อผิดพลาดอันอาจเกิดจากการใช้รหัสรายการดังกล่าว

(40) **การพิมพ์รายการฝากถอนต่างสำนักงานเมื่อสมุดคู่ฝากหมดเล่ม**

ตามระเบียบกรณีสมุดคู่ฝากหมดเล่ม ให้สาขาพิมพ์รายการ No – book ที่เหลือไว้ด้านหลังสมุดคู่ฝาก และถ้ายังไม่พอให้พิมพ์ไว้ด้านหน้า หรือพิมพ์ทับรายการของเดิมที่มีอยู่จนหมดรายการ

การ Update สมุดคู่ฝากโดยยินยอมให้มีการพิมพ์ทับรายการของเดิมเช่นนี้ มีผลให้ข้อมูลของรายการเก่าที่ถูกพิมพ์ทับ และข้อมูลของรายการใหม่ที่พิมพ์ทับ เสียหาย ไม่สามารถดูและตรวจสอบการเคลื่อนไหวของรายการได้

ข้อแนะนำ

ควรปรับปรุงวิธีการพิมพ์รายการฝากถอนต่างสำนักงานเมื่อสมุดคู่ฝากหมดเล่ม ให้สามารถป้องกันการพิมพ์ข้อมูลใหม่ทับข้อมูลเดิม

(41) **การควบคุมสมุดคู่ฝากที่ยังไม่ได้ใช้**

การจ่ายสมุดคู่ฝากโดยไม่ได้จัดทำทะเบียนควบคุมการจ่ายสมุดคู่ฝากให้แก่ลูกค้า สมุดคู่ฝากอาจสูญหายโดยไม่มีผู้ใดทราบ

ข้อแนะนำ

ควรกำหนดให้มีการจัดทำทะเบียนควบคุมการจ่ายสมุดคู่ฝากให้ลูกค้า

(42) **การแบ่งแยกหน้าที่ในการเก็บสมุดคู่ฝากและการบันทึกข้อมูลลงในแถบแม่เหล็กของสมุดคู่ฝาก**

การยินยอมให้พนักงาน Operator ซึ่งเก็บสมุดคู่ฝากที่ยังไม่ได้ใช้ สามารถทำการบันทึก (Write) ข้อมูลลงในแถบแม่เหล็กของสมุดคู่ฝากลูกค้าได้โดยไม่มีพนักงาน Authorized หรือพนักงานอื่นควบคุมดูแลโดยใกล้ชิด เป็นจุดอ่อนในการควบคุมภายในที่อาจก่อให้เกิดความเสียหายได้

ข้อแนะนำ

ไม่ควรยินยอมให้พนักงาน Operator ซึ่งทำหน้าที่บันทึกข้อมูลลงในแถบแม่เหล็กของสมุดคู่ฝากเป็นผู้เก็บรักษาสมุดคู่ฝากที่ยังไม่ได้ใช้

(43) **การควบคุมสมุดคู่ฝากที่ลูกค้ารายที่ไม่ต้องการทำรายการต่างสาขาไม่รัดกุม**

กรณีลูกค้าบางรายแจ้งความประสงค์ว่า ไม่ต้องการทำรายการต่างสาขา องค์กรไม่ได้ประทับตรายกเลิกในหน้าหลังของสมุดคู่ฝากที่ใช้บันทึกตัวอย่างลายมือชื่อลูกค้าที่ใช้เป็นหลักฐานในการถอนเงินต่างสาขา

ข้อแนะนำ

องค์กรควรกำหนดระเบียบให้ประทับตรา “ห้ามทำรายการต่างสาขา” บริเวณหน้าหลังของสมุดคู่ฝากที่ใช้บันทึกตัวอย่างลายมือชื่อ พร้อมกับลงลายมือชื่อโดยผู้รับมอบอำนาจกำกับด้วย

(44) **การควบคุมการทำรายการแบบไม่มีสมุดคู่ฝากจากต่างสาขาไม่รัดกุม**

1) การยินยอมให้โอนหรือถอนเงินสดโดยไม่มีสมุดคู่ฝากจากต่างสาขา อาจเป็นจุดอ่อนที่ก่อให้เกิดความเสียหายแก่องค์กรได้ เนื่องจากสาขาที่ทำรายการไม่สามารถตรวจสอบลายมือชื่อของลูกค้าได้

2) การยินยอมให้ฝากย้อนวันที่โดยไม่มีสมุดคู่ฝากจากต่างสาขา และไม่มีการระบุไว้ในคู่มือการปฏิบัติงาน รวมทั้งการทำรายการนี้จากต่างสาขาจะไม่ปรากฏในรายงาน Daily Inter-Branch Transaction by Other Branches อาจเป็นจุดอ่อน เนื่องจากสาขาเจ้าของบัญชีอาจไม่ทราบว่ามีสาขาใดบ้างทำรายการให้ และลูกค้ามีสิทธิถอนเงินฝากที่เกิดจากรายการดังกล่าวผ่านเครือข่ายงาน On - line ได้ทันที

ข้อแนะนำ

องค์กรควรหามาตรการและวิธีการควบคุมการทำรหัสรายการต่างสาขาของรายการต่อไปนี้อย่างรัดกุมและเหมาะสม เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นภายหลังจากที่นำระบบงานฝากถอนต่างสาขาออกใช้แล้ว ได้แก่

- CASH WITHDRAW NO BOOK
- TRANSFER WITHDRAW NO BOOK
- BACK DATE TRANSFER DEPOSIT NO BOOK

(45) **การสอบถามข้อมูลที่สำคัญของลูกค้าของระบบงานเงินฝากจากต่างสาขา**

โปรแกรมระบบงานยินยอมให้ทำรหัสรายการต่อไปนี้ต่างสาขาได้

- CUSTOMER INQUIRY	เพื่อสอบถามข้อมูลเกี่ยวกับชื่อที่อยู่ของลูกค้า
- LAST TRANS. INQUIRY	เพื่อสอบถามรายการเดินบัญชีครั้งสุดท้ายของลูกค้า
- ACTIVITY INQUIRY	เพื่อสอบถามรายการเคลื่อนไหวของลูกค้า
- DETAIL INQUIRY	เพื่อสอบถามรายละเอียดของลูกค้าเกี่ยวกับเช็ค เช็คอายัด วงเงิน O/D และ TEMP O/D
- TELLER INQUIRY	เพื่อสอบถามรายละเอียดของลูกค้าสำหรับ TELLER
- SUP. INQUIRY 1	เพื่อสอบถามรายละเอียดของลูกค้าสำหรับ SUPERVISOR 1
- INQUIRY MISC. CODE	เพื่อการสอบถามรายละเอียดต่าง ๆ ของลูกค้า
- SUP. INQUIRY 2	เพื่อสอบถามรายละเอียดของลูกค้า SUPERVISOR 2

นอกจากนั้น การทำรายการบางรหัสรายการไม่ต้องผ่าน SUPERVISOR CARD เพื่ออนุมัติการทำรายการก่อน

ข้อแนะนำ

องค์การควรกำหนดให้สามารถทำรายการสอบถามข้อมูลลูกค้าต่างสาขาได้เพียงบางรายการที่จำเป็นเท่านั้น และให้การทำรหัสรายการดังกล่าวอยู่ในความควบคุมของเจ้าหน้าที่ผู้รับมอบอำนาจหรือต้องผ่านการอนุมัติรายการโดย SUPERVISOR CARD ทุกครั้ง กำหนดอำนาจการทำรายการของพนักงานระดับต่าง ๆ ไว้ด้วย

(46) ไม่มีทะเบียนบันทึกรายละเอียดการฝากถอนเงิน (Teller Sheet)

องค์กรขาดการควบคุมเกี่ยวกับรายละเอียดการรับฝาก-ถอนเงินหน้าเคาน์เตอร์ (Counter) ทำให้

- ไม่มีหลักฐานใช้ในการติดตามรายการที่มีปัญหา
- ไม่มีหลักฐานใช้ตรวจสอบความถูกต้องของการทำรายการแก้ไข
- ไม่มีหลักฐานใช้ในการควบคุมความครบถ้วนของจำนวนสลิปที่เกิดขึ้นในแต่ละวัน

ข้อแนะนำ

องค์กรควรจัดทำบันทึกรายละเอียดการฝาก-ถอนเงิน (Teller Sheet) โดยมีรายละเอียดเกี่ยวกับรายการฝาก-ถอนเงินที่หน้าเคาน์เตอร์ทุกรายการทั้งหมด และกำหนดให้ผู้มีหน้าที่รับผิดชอบกระทบยอดจำนวนสลิปกับบันทึกรายละเอียดการฝาก-ถอนเงิน

(47) การควบคุมการแก้ไขรายการ (Correction) ไม่รัดกุม

การอนุญาตให้ทำการแก้ไขรายการฝากเงินสดและรายการโอนฝากจากบัญชีที่ถูกถอนเงินออกไปบางส่วนหรือถูกนำไปประกันหนี้ อาจมีผลทำให้เกินยอดเงินฝากคงเหลือที่สามารถถอนได้ หรือวงเงินประกันหนี้ที่ลูกค้าทำไว้น้อยกว่าความเป็นจริง

ข้อแนะนำ

องค์กรควรกำหนดให้มีข้อความเตือนก่อนให้ทำรายการต่อไปได้ และควรให้มีการอนุมัติรายการโดยผู้รับมอบอำนาจ เมื่อการแก้ไขรายการฝากเงินสดและรายการโอนฝากที่จะมีผลทำให้บัญชีเงินฝากออมทรัพย์ มียอดติดลบ หรือทำให้วงเงินประกันหนี้ผิดพลาดได้

(48) การ Post รายการฝากถอนให้ลูกค้าผิดบัญชี โดยเฉพาะรายการฝากผ่านสาขาอื่น ยังมีข้อผิดพลาดมาก

เนื่องจากไม่มีการตรวจสอบชื่อบัญชีลูกค้าก่อนทำรายการ และใช้วิธี Repeat เลขที่บัญชีทดแทนการป้อนเลขที่บัญชีซ้ำ ทำให้ไม่มีการป้อนเลขที่บัญชีเพื่อสอบทานความถูกต้องก่อนยินยอมให้ผ่านรายการ

ข้อแนะนำ

ในกรณีที่จำเป็นต้องใช้วิธี Repeat เลขที่บัญชีทดแทนการป้อนเลขที่บัญชีซ้ำ องค์กรควรกำหนดให้มีผู้ตรวจทานความถูกต้องอย่างเข้มงวด

(49) ความสมเหตุผลของข้อมูล

ข้อมูลต่าง ๆ ที่ป้อนเข้าสู่ระบบคอมพิวเตอร์ตามข้อกำหนดในการทำรายการบางประเภทมิได้มีการตรวจสอบความถูกต้องและเป็นไปได้ของข้อมูล ซึ่งข้อผิดพลาดในบางกรณีจะมีผลต่อความถูกต้องเชื่อถือได้

ข้อแนะนำ

ควรแก้ไขระบบงานให้สามารถตรวจสอบความถูกต้อง ความสมเหตุสมผล และความเป็นไปได้ เพื่อป้องกันมิให้มีการอายัดเพื่อค้ำประกันผิดประเภทบัญชี สำหรับการกำหนดรหัสเงื่อนไขโดยไม่ทราบความหมายนั้น ควรให้แน่ใจว่าจะไม่ส่งผลกระทบต่อเงื่อนไขการทำรายการใด ๆ ของลูกค้า

(50) ไม่มีการตรวจสอบคู่รายการก่อนดำเนินการแก้ไขข้อผิดพลาด

ระบบยินยอมให้มีการแก้ไขรายการโดยไม่มีคู่รายการมาก่อน (Original Transaction) ซึ่งวิธีปฏิบัติดังกล่าวอาจทำให้มีการแก้ไขผิดบัญชีหรือผิดรายการ ซึ่งองค์กรอาจได้รับความเสียหายได้

ข้อแนะนำ

องค์กรควรแก้ไขให้ระบบมีการ check สอบคู่รายการก่อนที่จะให้บันทึกรายการแก้ไข (Correction Transaction) ได้

(51) การป้องกันการฝาก No Book ผิดบัญชี

การรับฝากเงินกรณีไม่ได้ใช้สมุดคู่ฝาก (No Book) โดยไม่เรียกชื่อบัญชีซึ่งเป็นข้อมูลที่เก็บไว้ในระบบคอมพิวเตอร์นำมาพิมพ์ลงในแบบฟอร์มรับฝากเงินให้ลูกค้าตรวจสอบความถูกต้องในการรับฝากเงินนั้น หากลูกค้าแจ้งเลขที่บัญชีไม่ถูกต้องหรือมีข้อผิดพลาดในการป้อนเลขที่บัญชี อาจทำให้ลูกค้าได้รับความเสียหายจากการนำเงินฝากเข้าบัญชีให้ลูกค้าผิดบัญชี

ข้อแนะนำ

การรับฝากเงินกรณีไม่ได้ใช้สมุดคู่ฝากประกอบการทำรายการ ควรเรียกชื่อบัญชีซึ่งเป็นข้อมูลที่เก็บไว้ในระบบคอมพิวเตอร์นำมาพิมพ์ลงในแบบฟอร์มการรับฝากเงินให้ลูกค้าตรวจสอบความถูกต้องหรือมีวิธีการอื่นทดแทน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการนำเงินฝากเข้าบัญชีให้ลูกค้าผิดบัญชี

(52) การบำรุงรักษาอุปกรณ์คอมพิวเตอร์

เครื่องพิมพ์ Journal Roll บางเครื่อง ไม่ได้รับการบำรุงรักษาให้อยู่ในสภาพที่ใช้งานได้ดีมีการพิมพ์ซ้ำหยุดอยู่กับที่จนอ่านข้อมูลไม่ได้ พนักงาน Teller ของสาขาแต่ละแห่งอาจละเลยไม่เอาใจใส่ในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์เท่าที่ควร ซึ่งผู้บริหารขององค์กรก็ได้พยายามดูแลอยู่แล้ว แต่อาจไม่ทั่วถึงทุกแห่ง เพราะมีสาขาเป็นจำนวนมาก

ข้อแนะนำ

ควรบำรุงรักษาเครื่องพิมพ์ Journal Roll ให้อยู่ในสภาพที่ใช้งานได้ดี ไม่พิมพ์ซ้ำหยุดอยู่กับที่จนอ่านข้อมูลไม่ได้

(๕๓) **คู่มือการปฏิบัติงานไม่เป็นปัจจุบันและไม่สอดคล้องกัน**

ระดับของการผ่านรายการฝากเช็คโดยป้อน Hold day เป็น 0 (ศูนย์) ในคู่มือปฏิบัติงานไม่ตรงกัน ในคู่มือการปฏิบัติงานเกี่ยวกับ Financial transactions current account กำหนดให้ระดับผู้จัดการซึ่งเป็นระดับ 9 เป็นผู้อนุมัติรายการไว้ในหัวข้อหนึ่ง ในขณะที่ในคู่มือเล่มเดียวกันกำหนดให้พนักงานระดับ 6 เป็นผู้อนุมัติรายการในหัวข้อเดียวกัน นอกจากนี้ ในคู่มือการปฏิบัติงานยังกำหนดวิธีการปฏิบัติงานไม่ครบถ้วน เช่น ไม่กำหนดวิธีการทำรายการเช็คคืนของบัญชีเงินฝากออมทรัพย์ หลังจากวันที่ Post ดอกเบี้ยแล้ว ซึ่งจะทำให้ผู้ปฏิบัติงานเกิดความสับสนในการปฏิบัติงานได้

ข้อแนะนำ

ควรปรับปรุงให้คู่มือการปฏิบัติงานครบถ้วนเป็นปัจจุบันข้อมูลเรื่องเดียวกันที่ปรากฏต่างที่กันสอดคล้องซึ่งกันและกัน และสอดคล้องกับการปฏิบัติงานจริง

(๕๔) **มีข้อผิดพลาดในการแก้ไขรายการโดยใช้วันที่ย้อนหลัง**

ในกรณีที่มีการเปลี่ยนแปลงอัตราดอกเบี้ยและมีการบันทึกรายการย้อนหลัง โดยย้อนไปก่อนวันเปลี่ยนแปลงอัตราดอกเบี้ย การคำนวณดอกเบี้ยของเครื่องคอมพิวเตอร์จะใช้อัตราดอกเบี้ยปัจจุบันซึ่งเป็นอัตราใหม่ไม่แบ่งคิดเป็น 2 อัตรา คือ อัตราดอกเบี้ยเก่าและอัตราดอกเบี้ยใหม่ ตามระยะเวลาที่เป็นจริง

ข้อแนะนำ

ควรดำเนินการแก้ไขให้โปรแกรมคำนวณดอกเบี้ยโดยใช้อัตราดอกเบี้ยที่ถูกต้องตามช่วงเวลาที่มีการเปลี่ยนแปลง

(๕๕) **ไม่มีทะเบียนควบคุมเช็คลงวันที่ล่วงหน้า**

เช็คลงวันที่ล่วงหน้า (Post Date Cheque) ที่สาขารับจากลูกค้า สาขาจะเก็บเช็คแยกตามรายธนาคารและตามวันที่ที่เช็คถึงกำหนด โดยมิได้จัดทำทะเบียนบันทึกรายละเอียดเช็คลงวันที่ล่วงหน้า ทำให้ไม่สามารถตรวจสอบได้ทันทีว่ามีเช็คอยู่ครบถ้วนหรือไม่ ซึ่งเป็นจุดอ่อนของการควบคุมภายใน

ข้อแนะนำ

เพื่อเป็นประโยชน์ในการควบคุมและการตรวจสอบ ควรจัดทำทะเบียนเช็คลงวันที่ล่วงหน้า

(๕๖) **การป้อนข้อมูลเพื่อปรับปรุงรายการย้อนหลัง Operator สามารถกระทำได้โดยตรง**

โดยการป้อน "ปี เดือน วัน" ลงใน Field "Val. Date" พร้อมกับข้อมูลที่ต้องการในจอภาพ (Menu) ของการทำรายการนั้น ซึ่งการปรับปรุงรายการย้อนหลังดังกล่าวโดยตรง อาจก่อให้เกิดข้อผิดพลาดในการปฏิบัติงานได้

ข้อแนะนำ

องค์กรควรใช้การทำรายการ "Val. Date" เฉพาะการปรับปรุงแก้ไขรายการที่มีข้อผิดพลาดและเป็นรายการเดียวกับรายการที่เคยบันทึกรายการหรือตั้งบัญชีไว้ก่อนแล้ว ไม่ควรปรับปรุงรายการย้อนหลังด้วยรายการที่เกิดขึ้นเป็นรายการแรกหรือรายการใหม่

(57) **การป้อนรายการ Type 'C' เพื่อยกเลิก (Cancel) รายการที่มีข้อผิดพลาด (Error)**

จากการป้อนข้อมูลของ Operator มีจุดอ่อนในการควบคุมการปฏิบัติงาน เช่น สามารถยกเลิกการอายัดเช็คด้วยการป้อน Type 'C' โดยไม่มีข้อจำกัดของพนักงานที่มีอำนาจในการใช้เครื่อง Terminal จึงทำให้ขั้นตอนการควบคุมโดย Managers' Approval ถูกหลีกเลี่ยงและข้ามขั้นตอนไป

ข้อแนะนำ

1) ควรกำหนดหรือจำกัดขอบเขตการทำรายการ Type 'C' โดยต้องขออนุมัติจากเจ้าหน้าที่ชั้นบริหารก่อน หรือกำหนดรหัสเพื่อการทำ Type 'C' โดยเฉพาะและให้อยู่ในความรับผิดชอบของพนักงาน Operator ที่ได้รับมอบหมายเท่านั้น

2) ควรตรวจสอบรายงานเกี่ยวกับ Non - Financial Transaction โดยเฉพาะการยกเลิกรายการด้วย Type 'C' เพราะอาจกระทบต่อข้อมูลทางด้านการเงิน ซึ่งอาจก่อให้เกิดความเสียหายกับองค์กรได้

ข้อแนะนำ

องค์กรควรปรับปรุงให้การพิมพ์ข้อความใน Journal Roll ถูกต้องและครบถ้วน

(59) **พนักงานเทลเลอร์มิได้บันทึกรายละเอียด** วัน/เดือน/ปี/เวลา การใช้เครื่องเทอร์มินัลในสมุดทะเบียนเทอร์มินัล

ข้อแนะนำ

ในกรณีที่องค์กรมีระเบียบกำหนดให้พนักงานเทลเลอร์ต้องบันทึกรายละเอียดการใช้เครื่องเทอร์มินัลไว้ในสมุดทะเบียน ก็ควรดูแลและควบคุมให้มีการปฏิบัติตามโดยเคร่งครัด

(60) **การอายัดเงินฝากโดยอ้างอิงเลขที่เช็ค เปิดโอกาสให้สามารถนำเช็คที่เคยผ่านบัญชีลูกค้ามาผ่านบัญชีซ้ำอีกได้**

การอายัดเงินฝากด้วยรายการ Departmental hold และการถอนอายัดเงินฝากด้วยรายการ Release departmental hold ซึ่งอนุญาตให้ผู้ปฏิบัติงานเลือกปฏิบัติ โดยจะป้อนเลขที่เช็คสำหรับใช้เป็นข้อมูลอ้างอิงหรือไม่ต้องป้อนเลขที่เช็คก็ได้นั้น อาจเป็นปัญหาในการปฏิบัติงานและทำให้เกิดจุดอ่อนในระบบงานได้ หากผู้ปฏิบัติงานเลือกใช้วิธีป้อนเลขที่เช็คเป็นข้อมูลอ้างอิง

การป้อนเลขที่เช็คฉบับที่ยังไม่มาผ่านบัญชีลูกค้าเป็นข้อมูลอ้างอิงในกรณีอายัดเงินฝากจะเป็นผลให้เช็คฉบับนั้นถูกอายัด ถึงแม้ว่าลูกค้าจะไม่ต้องการอายัดเช็คฉบับนั้นก็ตาม ซึ่งจะเป็นปัญหาในการปฏิบัติงานหากมีเช็คฉบับนั้นมาผ่านบัญชี สำหรับกรณีถอนอายัดเงินฝาก หากผู้ปฏิบัติงานเลือกปฏิบัติโดยป้อนเลขที่เช็คฉบับที่เคยผ่านบัญชีลูกค้าแล้วเป็นข้อมูลอ้างอิง จะเกิดจุดอ่อนในการควบคุมการผ่านเช็คที่มาตัดบัญชีลูกค้า เพราะระบบจะยินยอมให้ผู้ปฏิบัติงานสามารถผ่านเช็คฉบับนั้นซึ่งเคยผ่านบัญชีลูกค้าไปแล้วได้

ข้อแนะนำ

ควรปรับปรุงวิธีการอายัดเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามในส่วนที่ทำให้ระบบควบคุมเช็คที่มาผ่านบัญชีลูกค้ามีจุดอ่อนตามควรแก่กรณี

(61) ไม่มีการป้องกันการใช้รหัสบางประเภทที่ไม่ถูกต้อง

องค์กรไม่ได้กำหนดวิธีการป้องกันข้อผิดพลาด หรือกำหนดให้ระบบคอมพิวเตอร์ปฏิเสธการใช้รหัสการอายัด (Miscellaneous Code) และรหัสประจำฝ่าย (Department Code) ที่ไม่ถูกต้อง หากผู้ปฏิบัติงานใช้รหัสซึ่งไม่ได้กำหนดไว้ใช้งานป้อนเข้าระบบคอมพิวเตอร์ จึงทำให้ข้อมูลคลาดเคลื่อนไปจากความเป็นจริง

ข้อแนะนำ

ควรมีวิธีการป้องกันข้อผิดพลาดที่อาจเกิดขึ้นจากการใช้รหัสไม่ถูกต้อง

(62) ระยะเวลาการออกรายงานแสดงยอดคงเหลือทุกบัญชีของเงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม

ซึ่งตามปกติจะออกทุกสิ้นเดือน และรายงานแสดงยอดคงเหลือทุกบัญชีของเงินฝากออมทรัพย์ซึ่งปกติจะออกตอนสิ้นงวดนั้น อาจก่อให้เกิดความไม่สะดวกในการปฏิบัติงานของสาขาได้ในกรณีที่ติดต่อกับสำนักงานใหญ่ไม่ได้หรือไฟดับ การติดตามรายการเคลื่อนไหวของลูกค้าที่มาขอถอนเงินย้อนกลับไปอาจเสียเวลาในการค้นหานาน

ข้อแนะนำ

ควรออกรายงานที่สามารถช่วยผู้ปฏิบัติงานให้ทราบยอดคงเหลือของลูกค้าทุกรายได้โดยเร็ว เพื่อลดงานในการติดตามรายการเคลื่อนไหวของลูกค้าในกรณีที่ไฟดับหรือเครื่องคอมพิวเตอร์ขัดข้อง

(63) การพิมพ์วันที่ในรายงานไม่ถูกต้อง

รายงานบางรายงาน วันที่ที่นำมาพิมพ์รายงานเป็นวันที่ของ System Date ซึ่งจะเปลี่ยนเป็นวันถัดมาเมื่อถึงเวลา 24.00 น. โดยอัตโนมัติ ในกรณีที่การประมวลข้อมูลเลยเวลา 24.00 น. รายงานที่ใช้ System Date เป็นหลักในการพิมพ์วันที่ จะเป็นวันที่ถัดมาจากวันที่ทำรายการซึ่งไม่ถูกต้อง

ข้อแนะนำ

รายงานต่าง ๆ ควรใช้วันที่ของ Transaction Date ซึ่งเป็นวันทำการที่เกิดรายการจริง

(64) ไม่มีการพิมพ์รายงานพิเศษที่ใช้ในการควบคุมภายใน

องค์กรมิได้จัดทำรายงานพิเศษเพื่อควบคุมการโอนบัญชีเงินฝากที่ไม่เคลื่อนไหวไปเป็นบัญชี Sleeping Account และรายงานแสดงการแก้ไขรายการที่ผิดพลาด รวมทั้งยอดรวมรายการแก้ไขข้อผิดพลาดประจำวัน (Error Transaction Report) ทำให้ไม่มีรายละเอียดที่ใช้ในการควบคุมบัญชีเงินฝาก และใช้ตรวจสอบความถูกต้องของการทำรายการแก้ไข

ข้อแนะนำ

ควรจัดทำรายงานพิเศษเพิ่มเติมเพื่อใช้ในการควบคุมภายใน ดังนี้คือ

1) รายงานการโอน Active Account ไปเป็น Sleeping Account
2) รายงานแสดงการแก้ไขรายการที่ผิดพลาด รวมทั้งยอดรวมรายการแก้ไขข้อผิดพลาดประจำวัน (Error Transaction Report) เพื่อตรวจสอบและควบคุมความถูกต้องของการทำรายการแก้ไข

(65) ไม่มีรายงานแสดงการเปลี่ยนแปลงข้อมูลของลูกค้า

การเปลี่ยนแปลงข้อมูลบางประเภทของลูกค้า เช่น รหัสประเภทของลูกค้า การ delete ข้อมูลจาก Master File เป็นต้น มิได้แสดงไว้ในรายงานใด ๆ อาจทำให้การติดตามและตรวจสอบความถูกต้องของรายการดังกล่าวไม่สะดวก

ข้อแนะนำ

การทำรายการเปลี่ยนแปลงข้อมูลของลูกค้า เช่น การ delete Master File หรือการ Change Field ซึ่งแก้ไขรหัสประเภทของลูกค้า ควรให้ปรากฏหลักฐานการทำรายการไว้ในรายงาน Daily Transaction Miscellaneous หรืองานอื่น เพื่อประโยชน์ในการควบคุมและตรวจสอบความถูกต้องของรายการดังกล่าว

(66) การคำนวณยอดเงินคงเหลือที่พึงถอนได้อาจไม่ถูกต้องในกรณีระบุคอมพิวเตอร์ขัดข้อง

รายงาน Daily current own branch transaction report แสดงข้อมูลที่อาจเป็นปัญหาต่อการปฏิบัติงาน ดังนี้

นำวงเงินเบิกเกินบัญชีที่ครบกำหนดอายุสัญญาแล้ว แสดงเป็นยอดเงินคงเหลือที่พึงถอนได้ หากระบบคอมพิวเตอร์ขัดข้องเสียหายไม่สามารถให้บริการ Online ได้ตามปกติ ผู้ปฏิบัติงานอาจยินยอมให้ลูกค้าถอนเงินตามยอดเงินคงเหลือที่พึงถอนได้ที่ปรากฏในรายงาน ซึ่งในบางกรณีจะทำให้องค์กรได้รับความเสียหายได้

สำหรับกรณีที่ระบบคอมพิวเตอร์สามารถให้บริการ Online ได้ตามปกติ จะไม่มีปัญหาดังกล่าว เนื่องจากยอดเงินคงเหลือที่พึงถอนได้ที่แสดงทางจอภาพเมื่อสอบถามด้วยรายการ Balance Inquiry เป็นยอดที่ถูกต้อง

ข้อแนะนำ

องค์กรควรแก้ไขให้รายงานดังกล่าว แสดงข้อมูลที่ถูกต้อง

(67) รายงานไม่ถูกต้องสมบูรณ์

ข้อมูลที่แสดงในรายงานคลาดเคลื่อนไปจากความเป็นจริง ดังนี้

- ค่า O/D MAX ในรายงานผิดจะพิมพ์ค่าน้อยกว่า 1 โดยค่าที่ถูกต้องใน Master File เป็น 0
- การนับจำนวนบัญชีของลูกค้าโดยไม่นับบัญชีที่มียอดคงเหลือเป็น 0 (ศูนย์) จะมีผลทำให้ยอดรวมจำนวนบัญชีทั้งหมดน้อยกว่าความเป็นจริง
- เลขที่บัญชีที่มี Check Digit เป็น 0 (ศูนย์) ในรายงานจะไม่พิมพ์เลข Check Digit
- "รายงานปิดบัญชี" ในกรณีปิดบัญชีผิดแล้วทำการ Maintenance ให้มีการเปิดบัญชีใหม่ในวันเดียวกัน รายงานที่กล่าวยังแสดงข้อมูลของบัญชีนั้นเป็นบัญชีที่ปิดแล้ว
- "Current A/C Special Rate Listing" ได้แสดงข้อมูลของบัญชีที่ปิดแล้วออกมาด้วย
- "เงินให้สินเชื่อแยกตามประเภทธุรกิจ" แสดงข้อมูลบางรายการไม่ถูกต้อง
- "รายการเคลื่อนไหวสลิปทุกประเภท" ในวันที่มีการผ่านดอกเบี้ย โปรแกรมจะทำการบวกยอด และพิมพ์ดอกเบี้ยที่ผ่านบัญชีเรียบร้อยแล้วซ้ำอีกครั้งหนึ่ง เป็นผลให้รายงานที่กล่าวแสดงรายการดอกเบี้ย และยอดคงเหลือไม่ถูกต้อง
- รายงานประจำวันของสาขาแสดงยอด Before Active - Accrued Int. มีจำนวน 160,000.00 บาท ไม่สอดคล้องกับยอด Today Active - Accrued Int. ที่ปรากฏในรายงานเดียวกันของวันก่อน คือ 120,000.00 เนื่องจากองค์กรต้องการแสดงให้เห็นว่ามีการปรับปรุงหรือเปลี่ยนแปลงยอดจากวันก่อน ซึ่งจะให้ประโยชน์ในการติดตามรายการทางบัญชีได้ในภายหลัง
- จำนวนหลักที่พิมพ์ไม่เพียงพอ เช่น

รายงาน Daily Current Account Transaction แสดงยอดรวมรายการฝากและรายการถอนได้สูงสุดหลักร้อยล้านบาท ทั้งที่การทำรายการฝากและถอนแต่ละครั้งเป็นหลักร้อยล้านบาท

รายงาน Daily Transaction of Saving A/C รายงาน Daily Inter-office Balance for Home Branch และรายงาน Daily Inter-branch Balance Sheet for Accounting Deposit แสดงยอดฝากถอนและยอดรวมของรายการดังกล่าวได้สูงสุดหลักสิบล้านบาท แต่ทำรายการฝากและถอนแต่ละครั้งได้ถึงหลักร้อยล้านบาท

สมุดคู่ฝากออมทรัพย์ แสดงยอดเงินฝากคงเหลือได้สูงสุดหลักร้อยล้านบาท แต่ใน Master File เก็บค่าได้ถึงหลักพันล้านบาท

การพิมพ์ยอดคงเหลือ (Balance) ในรายงาน (Report) ต่าง ๆ ในระบบงานเงินฝากได้กำหนดเนื้อที่สำหรับพิมพ์ยอดคงเหลือไม่เท่ากัน ซึ่งอาจเป็นเหตุให้การแสดงยอดเงินฝากหรือเงินเบิกเกินบัญชีของลูกค้าไม่ถูกต้อง กล่าวคือ อาจพิมพ์ยอดเงินฝากและเงินเบิกเกินบัญชีต่ำกว่าที่เป็นจริง เนื่องจากเครื่องคอมพิวเตอร์

ตัดหลักที่เกินเนื้อที่ที่จะพิมพ์ได้ออก ซึ่งกระทบความถูกต้องเชื่อถือได้ของรายงานและข้อมูลทางการเงิน และอาจก่อให้เกิดปัญหาในการควบคุมของผู้บริหาร (เช่น ขณะที่ป้อนข้อมูลได้ตาม Transaction file ถึง 12 หลัก เป็นต้น)

รายงาน Daily Accounts Closed และรายงาน Daily Summary Transaction Report แสดงการปิดบัญชีไม่ถูกต้อง โดยรวมบัญชีที่ถูกยกเลิกการปิดบัญชีไว้ด้วยทั้งจำนวนบัญชีและจำนวนเงิน เป็นการปิดบัญชีซ้ำ 2 ครั้ง

รายงาน Daily Debit/Credit Transaction Over 100,000 Baht ไม่ได้แสดงรายการฝากและถอนย้อนวันที่ (Conversion Deposit และ Conversion Withdraw) ที่มีจำนวนเงินมากกว่า 100,000 บาท

รายงาน Monthly Total Depostit By Type of Customer/Deposit ไม่ถูกต้องเนื่องจากโปรแกรมระบบงานไม่ได้ทดสอบความเป็นไปได้ของข้อมูล โดยสามารถป้อนรหัสประเภทของลูกค้าที่ไม่ได้กำหนดให้ทำรายการได้

รายงาน Report of Increase/Decrease in O/D Line แสดงยอดวงเงินเบิกเกินบัญชีผิดพลาดในกรณีที่มีการเพิ่มวงเงินไม่ผิดแล้วยกเลิก และเพิ่มวงเงินใหม่ที่ถูกต้อง สำหรับบัญชีที่ยังไม่เคยมีวงเงินมาก่อน โดยแสดงยอดรวมของวงเงินเดิมที่ผิดพลาดกับวงเงินใหม่ที่ถูกต้อง แทนที่จะแสดงยอดวงเงินใหม่ที่ถูกต้องเพียงวงเงินเดียวเท่านั้น

รายงาน Master File Report of Current A/C ไม่ได้แสดงรายละเอียดเกี่ยวกับวงเงินเบิกเกินบัญชี วันที่ครบกำหนด อัตราดอกเบี้ยของลูกค้าที่ทำสัญญาใหม่ และที่มีการเปลี่ยนแปลงวงเงินเดิมในระหว่างเดือน

รายงาน Master File Report of Saving ไม่ได้รวมบัญชีลูกค้าที่มีสถานะถึงแก่กรรมแล้วในยอดสรุปของจำนวนเงินและจำนวนบัญชี

รายงาน Monthly Balance Saving A/C บัญชีลูกค้าที่มียอดคงเหลือและดอกเบี้ยค้างจ่ายเป็นลบใน Master File แต่ในรายงานนี้แสดงเป็นค่าบวก นอกจากนี้ ยังได้คำนวณ รวมดอกเบี้ยค้างจ่ายเป็นลบใน Master File แต่ในรายงานนี้แสดงเป็นค่าบวก นอกจากนี้ ยังได้คำนวณรวมดอกเบี้ยค้างจ่ายบวก ทำให้ยอดรวมของดอกเบี้ยค้างจ่ายมากไป

- รายงาน Daily Hold and No-Book Saving A/C ปรากฏว่ายอดคงเหลือในบัญชีของลูกค้าแต่ละราย และยอดรวมของยอดเหลือที่พึงถอนได้ มีค่าเป็นลบ แต่ในรายงานนี้แสดงค่าเป็นบวก
- รายงาน Statement of Saving Account ไม่ได้แสดงรายการปิดบัญชีของลูกค้าบางบัญชีที่ปิดแล้ว
- รายงาน Daily New Accout และรายงาน Daily Account Closed แสดงยอดจำนวนเงินรวมไม่ถูกต้อง เนื่องจากได้รวมรายการเปิดบัญชีและรายการปิดบัญชีที่มีการแก้ไขแล้วทำให้ยอดจำนวนเงินรวมสูงกว่าความเป็นจริง

- รายงาน Daily Saving Transaction แสดงยอดจำนวนเงินรวมของรายการฝาก (Credit Amount) ไม่ถูกต้อง เพราะในกรณีที่มีรายการฝากหรือถอนด้วยจำนวนเงินที่เป็นหลักร้อยล้าน รายงานจะไม่สามารถแสดงยอดรวมที่เกินหลักร้อยล้านได้

การพิมพ์รายงานยังไม่ถูกต้อง กล่าวคือ ถ้าวันรุ่งขึ้นเป็นวันหยุดทำการของธนาคาร เช่น รายงานประจำวันศุกร์ จำนวนเงินของเช็คที่ฝากผ่านพนักงานเทลเลอร์จะไปแสดงเป็นจำนวนเงินของเช็คที่ฝากผ่านเครื่อง ATM ทำให้การดูรายงานอาจผิดพลาดได้

- **รายงานแสดงรายการเคลื่อนไหวประจำวันนอกเหนือจากรายการฝากถอน**

การพิมพ์รายงานในส่วนที่เป็นรายการของเงินฝากออมทรัพย์ที่ทำให้สาขาอื่น จะพิมพ์ขึ้นหน้าใหม่โดยมิได้ระบุว่าเป็นสาขาใด เพียงแต่พิมพ์เลขที่บัญชี 7 หลักเท่านั้น ทำให้การติดตามดูรายงานไม่สะดวกและไม่ได้ผลเท่าที่ควร

- **รายงานแสดงรายการเคลื่อนไหวของบัญชีเงินฝากออมทรัพย์ประจำวัน**

การพิมพ์วันที่เคลื่อนไหวครั้งสุดท้ายไม่ถูกต้องในกรณีที่มีรายการเช็คคืน หรือรายการแก้ไขการฝากเงินสดผ่านเครื่อง ATM หรือรายการฝากเงินสดผ่านเครื่อง ATM โดยระบบงานจะนำวันที่ซึ่งทำรายการไปพิมพ์เป็นวันที่เคลื่อนไหวครั้งสุดท้าย

- **รายงานสรุปยอดเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามแยกตามประเภทลูกค้า**

องค์กรไม่ได้หักหนี้สูญที่ได้อนุมัติให้ตัดบัญชีไปแล้วทั้งจำนวนหรือบางส่วน 6 รายเป็นเงิน 11,071,306.44 บาท ออกจากแฟ้มข้อมูลหลัก ทำให้ยอดรวมของเงินเบิกเกินบัญชีตามรายงานนี้ไม่ถูกต้องตรงกับยอดเงินเบิกเกินบัญชีตามงบทดลอง นอกจากนี้ อาจทำให้รายงานอื่น ๆ ที่ใช้ข้อมูลจากแฟ้มข้อมูลหลักแสดงข้อมูลคลาดเคลื่อนไปด้วย

- **รายงานแสดงรายละเอียดของบัญชีเงินฝากออมทรัพย์ที่ปิดบัญชี**

ไม่พิมพ์ชื่อลูกค้าที่ปิดบัญชีโดยเว้นที่ว่างไว้ในรายงาน ทั้ง ๆ ที่ในแฟ้มข้อมูลหลักมีชื่อลูกค้ารายนั้น ๆ อยู่

ข้อแนะนำ

ควรปรับปรุงแก้ไขรายงานที่แสดงข้อมูลคลาดเคลื่อนไปจากความเป็นจริงให้ถูกต้อง เพื่อป้องกันข้อผิดพลาดจากการนำรายงานไปใช้

(๖๘) การยืนยันความถูกต้องของข้อมูลในรายงานต่างชุดกัน ไม่สอดคล้องกัน

ข้อมูลจำนวนบัญชีที่มียอดเงินฝากคงเหลือไม่เกิน 50,000.00 บาท ที่ปรากฏในรายงาน Customer account balance report และรายงาน Summary classified current balance report ยังมีข้อแตกต่างกัน

ข้อแนะนำ

ควรปรับปรุงแก้ไขข้อมูลจำนวนบัญชีเงินฝากของลูกค้าที่มียอดเงินฝากคงเหลือไม่เกิน 50,000.00 บาท ให้ถูกต้องและสอดคล้องกัน

(69) **ความเข้าใจรายงานคลาดเคลื่อน**

สาขาเข้าใจไม่ถูกต้องเกี่ยวกับยอด Balance ที่แสดงในรายงาน โดยเข้าใจว่าเป็นจำนวนเงินที่ขอเปิดบัญชีในวันนั้น แต่ถ้าลูกค้ามีการทำรายการในวันที่ขอเปิดบัญชี ยอดที่ปรากฏในรายงานจะเป็นยอดคงเหลือ ณ สิ้นวัน มิใช่จำนวนเงินที่ขอเปิดบัญชี

สาขาชี้แจงว่า จะใช้รายงาน Open Account Report เพียงเพื่อดูว่าในแต่ละวันมีลูกค้ามาเปิดบัญชีมีรายชื่อใครบ้าง ส่วนยอดคงเหลือสิ้นวันจะดูจากรายงาน Outstanding Report

ข้อแนะนำ

ควรปรับปรุงแก้ไขรายงาน Open Account Report ให้แสดงยอด Balance เป็นจำนวนเงินที่ขอเปิดบัญชี และควรจัดทำคู่มือการใช้รายงานส่งให้สาขา เพื่อที่จะได้สามารถใช้รายงานได้

(70) **รายงานที่เลิกใช้**

รายงานต่าง ๆ ของระบบเงินฝากที่ปรากฏในระบบ มีบางรายงานที่สำนักงานสาขาไม่ใช้งานและไม่ได้ปรับปรุง Menu ต่าง ๆ ให้เป็นไปตามที่ใช้งานจริง

ข้อแนะนำ

ควรปรับปรุง Menu ที่ใช้พิมพ์รายงานในระบบเงินฝาก ให้เป็นไปตามที่ใช้งานจริง

2.2.1 เงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและเงินเบิกเกินบัญชี

(1) **การควบคุมเกี่ยวกับเช็คที่มีคำสั่งระงับการจ่ายเงินไม่รัดกุม**

1) ระบบงานสามารถยกเลิกคำสั่งระงับการจ่ายเงินตามเช็คที่ถูกระงับการจ่ายเงินเมื่อผู้ป้อนข้อมูลกด ENTER ซ้ำอีกครั้งหนึ่ง

2) ระบบงานมิได้กำหนดให้ป้อนเลขที่เช็คจากน้อยไปหามาก เมื่อมีคำสั่งระงับการจ่ายเงินตามเช็คเป็นช่วง หากผู้ป้อนข้อมูลป้อนเลขที่เช็คที่มีคำสั่งระงับการจ่ายเงินจากมากไปหาน้อยจะมีผลทำให้ระบบคอมพิวเตอร์ระงับจ่ายเงินเฉพาะเช็คฉบับสุดท้ายและฉบับแรกเท่านั้น

3) เช็คที่คำสั่งระงับการจ่ายเงินของลูกค้าที่ปิดบัญชีไปแล้วเป็นจำนวนมาก องค์กรมิได้ลบล้างข้อมูลเช็คเหล่านั้นออกไปด้วย ทำให้เสียเนื้อที่ในแฟ้มข้อมูล

(2) **การควบคุมความครบถ้วนของการคืนเช็ค**

องค์กรมิได้กำหนดวิธีการควบคุมและตรวจสอบการคืนเช็คประจำวันของแผนกบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามที่บันทึกไว้ในสมุดทะเบียน กับรายงาน Interim Moved Excess Report เพื่อป้องกันข้อผิดพลาดและความเสียหายที่เกิดจากการคืนเช็คไม่ถูกต้องและครบถ้วน

(3) **การแบ่งแยกหน้าที่ระหว่างการจัดเตรียมเอกสารขั้นต้นและการป้องกันข้อมูล**

ไม่มีการแบ่งแยกหน้าที่ระหว่างการจัดเตรียมเอกสารขั้นต้นและการนำข้อมูลเข้าเครื่องคอมพิว-เตอร์ เพื่อประโยชน์ในการควบคุมภายในเท่าที่ควร พนักงานรับ-ส่งเช็คคืน มีรหัสประจำตัวที่สามารถทำรายการนำเข้าข้อมูล เป็นจุดอ่อนในการควบคุมภายใน เนื่องจากใช้ป้อนข้อมูลเกี่ยวกับการเคลื่อนไหวทางบัญชีอื่น ๆ ได้

(4) **การนำข้อมูลเข้าเครื่องคอมพิวเตอร์ไม่ถูกต้อง**

1) มีการนำรหัสพนักงานสินเชื่อเข้าเครื่องคอมพิวเตอร์ไม่ถูกต้องตามตำแหน่ง (Field) ที่กำหนดทำให้รายงาน Limit Review Full List ซึ่งได้จากระบบงานคอมพิวเตอร์สำหรับใช้ในการพิจารณาต่ออายุวงเงินสินเชื่อ ไม่มีข้อมูลเกี่ยวกับวงเงิน วันอนุมัติ วันครบกำหนดของลูกค้ารายนั้น ๆ เป็นผลให้พนักงานสินเชื่อไม่สามารถควบคุมและติดตามลูกหนี้รายที่รับผิดชอบได้

2) รายงานแสดงยอดเงินฝากแยกประเภทธุรกิจไม่ถูกต้องตามความเป็นจริง

ข้อแนะนำ

เพื่อให้ระบบงานเป็นประโยชน์แก่ผู้ใช้ข้อมูล และสามารถใช้ควบคุมการให้สินเชื่อแก่ลูกหนี้ได้อย่างมีประสิทธิภาพ ศูนย์คอมพิวเตอร์ควรสอบถามปัญหาหรือข้อขัดข้องในการใช้รายงานผลลัพธ์ประเภทต่าง ๆ จากผู้ใช้ข้อมูลเป็นครั้งคราว เพื่อใช้เป็นแนวทางในการพิจารณาปรับปรุงระบบงานที่ใช้อยู่ในปัจจุบัน รวมทั้งเพิ่มเติมข้อกำหนดในระบบงานใหม่ ซึ่งอยู่ระหว่างเตรียมการนำมาใช้ตามความเหมาะสมต่อไป

(5) **การควบคุมรายการแก้ไขข้อผิดพลาดไม่รัดกุม**

1) ผู้ปฏิบัติงานสามารถทำรายการแก้ไขข้อผิดพลาด (Reverse) ที่มีผลทำให้บัญชีมียอดบัญชีเกินวงเงิน หรือยอดเบิกเงินเกินบัญชีชั่วคราวได้ โดยไม่ต้องผ่านการอนุมัติจากเจ้าหน้าที่ผู้มีอำนาจอนุมัติวงเงินเบิกเกินบัญชีชั่วคราว เนื่องจากระบบงานไม่มีการตรวจสอบยอดเงินที่ลูกค้ามีสิทธิถอนได้ (Available balance) อาจทำให้องค์กรได้รับความเสียหายได้

2) ระบบงานอนุญาตให้ผู้ปฏิบัติงานทำรายการแก้ไขข้อผิดพลาด (Reverse) โดยไม่มีการทำรายการผิดพลาดมาก่อนได้ อาจทำให้มีการแก้ไขผิดบัญชี เนื่องจากไม่มีคู่รายการสำหรับการเช็คสอบความถูกต้องของการแก้ไข

3) องค์กรไม่ได้กำหนดให้มีการจัดทำทะเบียนควบคุมรายการแก้ไข เพื่อไว้ใช้ตรวจสอบความถูกต้องของการแก้ไขข้อผิดพลาดในภายหลัง

ข้อแนะนำ

การทำรายการแก้ไขข้อมูลทุกครั้ง (Reverse) ควรให้มีการตรวจสอบยอดเงินที่ลูกค้ามีสิทธิถอนได้ (Available balance) ด้วย และควรควบคุมทั้งจำนวนเงินและเลขที่บัญชีให้ตรงกับรายการที่ได้ทำไปแล้ว

(6) **การควบคุมเลขที่เช็คที่มาตัดบัญชีไม่รัดกุม**

ระบบงานไม่มีการป้องกันข้อผิดพลาดในการป้อนเลขที่เช็ค ระบบงานจึงไม่มีการตรวจสอบว่าจำเป็นต้องป้อนเลขที่เช็คสำหรับรายการตัดบัญชีดังกล่าวด้วย ซึ่งถ้าพนักงานเทลเลอร์หลงลืมไม่ป้อนเลขที่เช็ค เช็คที่เคยผ่านบัญชีไปแล้วและตัดบัญชีไปแล้วจะตัดบัญชีซ้ำได้อีก และอาจมีการผ่านรายการผิดบัญชีได้

ข้อแนะนำ

การทำรายการถอน House Cheque และ Branch Cheque ด้วยรหัสรายการเดียวกับรายการโอนหักบัญชีภายในควรตรวจสอบ Bill Code ว่าเป็นรายการที่ต้องป้อนเลขที่เช็ค

(7) **รายการที่มีผลทำให้การคำนวณดอกเบี้ยเงินเบิกเกินบัญชีที่เรียกเก็บจากลูกค้าผิดพลาดได้**

1) การปิดบัญชีเงินเบิกเกินบัญชีองค์กรจะคำนวณดอกเบี้ยและตัดบัญชีลูกค้าทันที หากในวันเดียวกันนั้นมีการแก้ไขเพื่อเปิดบัญชีใหม่ และผู้ปฏิบัติงานหลงลืมไม่ทำรายการคืนดอกเบี้ยให้ลูกค้าจะมีผลให้ลูกค้าต้องเสียดอกเบี้ยในจำนวนที่ถูกตัดบัญชีไปแล้วอีกในขั้นตอนบันทึกรายการดอกเบี้ยประจำเดือน (Post) เนื่องจากจำนวนดอกเบี้ยที่ตัดบัญชีลูกค้าไปแล้วนั้น ยังคงแสดงว่าเป็นดอกเบี้ยคงค้างสำหรับบัญชีนั้น ๆ อยู่ อาจทำให้องค์กรเรียกเก็บดอกเบี้ยจากลูกหนี้เกินกว่าอัตราดอกเบี้ยสูงสุดที่ทางการกำหนด

2) การทำรายการยกเลิกวงเงินเบิกเกินบัญชีทั้งหมด ระบบงานจะนำดอกเบี้ยที่ค้างอยู่มาตัดบัญชีลูกค้าทันที แม้ว่ายังไม่ถึงวันที่ทำการบันทึกรายการดอกเบี้ย (Post) ประจำเดือนก็ตาม ซึ่งถ้าภายในเดือนนั้นลูกค้ายังไม่ชำระหนี้และสภาพบัญชีเป็นเงินเบิกเกินบัญชีอยู่ จะมีผลทำให้มีการคำนวณดอกเบี้ยของดอกเบี้ยที่ตัดบัญชีลูกค้าแล้วในสิ้นเดือนนั้น การปฏิบัติดังกล่าวอาจทำให้องค์กรเรียกเก็บดอกเบี้ยจากลูกหนี้เกินกว่าอัตราดอกเบี้ยสูงสุดที่ทางการกำหนดได้

ข้อแนะนำ

1) การทำรายการแก้ไขการปิดบัญชี ถ้าทำรายการบันทึกดอกเบี้ยไปแล้วก่อนปิดบัญชีควรกำชับให้พนักงานทำรายการแก้ไขการบันทึกดอกเบี้ยด้วย

2) การทำรายการยกเลิกวงเงินเบิกเกินบัญชีทั้งหมด ไม่ควรให้มีการบันทึกรายการ (Post) ดอกเบี้ยเงินเบิกเกินบัญชีก่อนวันที่กำหนดให้มีการบันทึกรายการดอกเบี้ยประจำเดือน

(8) **การปรับปรุงวันที่เคลื่อนไหวครั้งสุดท้าย (Date of last transaction) ไม่ถูกต้อง**

เมื่อมีการทำรายการยกเลิกวงเงินทั้งหมด และภายในวันเดียวกันนั้นมีรายการแก้ไขการยกเลิกวงเงินดังกล่าว จะมีผลทำให้วันที่เคลื่อนไหวครั้งสุดท้ายของบัญชีผิดพลาด เนื่องจากระบบงานได้ทำการปรับปรุงวันที่เคลื่อนไหวครั้งสุดท้ายเป็นวันที่ทำการปัจจุบัน โดยเปรียบเสมือนว่ามีการเคลื่อนไหวในวันทำการนั้น ทำให้การโอนบัญชีเป็น Inactive account ไม่ถูกต้อง ซึ่งอาจมีผลให้การจัดชั้นหนี้สำหรับบัญชีเงินเบิกเกินบัญชีผิดพลาดได้

ข้อแนะนำ

ควรแก้ไขโปรแกรมให้ทำการปรับปรุง Date of last transaction ของรายการแก้ไขการยกเลิกวงเงินให้ถูกต้อง

(9) **ระบบงานยินยอมให้ป้อนอัตราดอกเบี้ยเงินเบิกเกินบัญชีสูงกว่าอัตราที่ทางการกำหนด**

ระบบงานยินยอมให้ป้อนอัตราดอกเบี้ยเงินเบิกเกินบัญชีโดยไม่ได้ตรวจสอบกับอัตราสูงสุดของดอกเบี้ยที่กำหนดได้

ข้อแนะนำ

ควรกำหนดขั้นตอนการควบคุมโดยโปรแกรมใช้งาน เพื่อป้องกันมิให้มีการป้อนอัตราดอกเบี้ยสูงกว่าอัตราที่ทางการกำหนด ซึ่งอาจเกิดความผิดพลาดได้

(10) **การควบคุมเช็คลงวันที่ล่วงหน้า (Post Dated Cheque) ไม่รัดกุม**

องค์กรบันทึกรายการเช็คลงวันที่ล่วงหน้าไว้ปะปนในทะเบียนคุมเช็คที่ส่งเรียกเก็บไม่ทัน (Cheque too late) และเช็คเรียกเก็บต่างจังหวัด (Collection Cheque) เรียงตามวันที่ที่ได้รับเช็ค โดยมิได้แยกบันทึกในทะเบียนเช็คลงวันที่ล่วงหน้าโดยเฉพาะ ทำให้ไม่สามารถตรวจสอบได้ทันทีว่ามีเช็คอยู่ครบถ้วนหรือไม่ และอาจเป็นช่องทางให้เช็คสูญหายได้โดยง่าย

ข้อแนะนำ

องค์กรควรแยกทะเบียนบันทึกเช็คลงวันที่ล่วงหน้าออกจาก Cheque too late เพื่อประสิทธิภาพในการควบคุมความครบถ้วนของเช็ค

(11) **ไม่มีการเก็บเลขที่เช็คที่จ่ายให้ลูกค้าไว้ในระบบคอมพิวเตอร์**

ระบบงานเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและเงินเบิกเกินบัญชี ไม่มีการบันทึกเลขที่เช็คที่ออกให้กับลูกค้าไว้ในระบบงาน และไม่มีการตรวจสอบเลขที่เช็คก่อนตัดบัญชีลูกค้า เป็นจุดอ่อนในการปฏิบัติงานอย่างยิ่ง เปิดโอกาสให้ลูกค้าหรือพนักงานสามารถนำเช็คเลขที่เดียวกันมาผ่านบัญชีได้หลายครั้งหรือนำเช็คที่ไม่ได้ออกให้กับบัญชีนั้นมาผ่านบัญชีได้

(12) **ไม่มีการตรวจสอบความถูกต้องในการกำหนดวันที่ใช้คำนวณดอกเบี้ยเช็คคืน**

จากการทดสอบวิธีการกำหนดวันที่สำหรับใช้ในการคำนวณดอกเบี้ย (Value date) กรณีเช็คคืนจากธนาคารอื่น พบว่าระบบคอมพิวเตอร์ไม่ได้ตรวจสอบความถูกต้องของข้อมูลที่กล่าวเท่าที่ควร หากผู้ปฏิบัติงานใช้วันที่ทราบผลการคืนเช็คจากธนาคารอื่น เป็นวันที่สำหรับใช้คำนวณดอกเบี้ยเช็คคืน แทนวันที่ลูกค้านำเช็คฝากเข้าบัญชีจะมีผลทำให้การคำนวณดอกเบี้ยเงินเบิกเกินบัญชีคลาดเคลื่อนไปจากความเป็นจริงได้

ข้อแนะนำ

ควรกำหนดให้มีการตรวจสอบความถูกต้องในการกำหนดวันที่สำหรับใช้คำนวณดอกเบี้ยเช็คคืนก่อนนำเข้าระบบคอมพิวเตอร์ โดยให้ระบบคอมพิวเตอร์เตือนผู้ปฏิบัติงานให้ทำการยืนยันความถูกต้องในการทำรายการหากมีการใช้วันที่ทราบผลการคืนเช็คจากธนาคารอื่นเป็นวันที่สำหรับใช้คำนวณดอกเบี้ยเช็คคืน

(13) **ทำรายการเช็คคืนได้โดยไม่จำเป็นต้องมีเช็คนำฝากเข้าบัญชีในวันก่อน**

จากการทดสอบทำรายการเช็คคืนพบว่า ระบบคอมพิวเตอร์ยินยอมให้ผู้ปฏิบัติงานทำรายการเช็คคืนในบัญชีของลูกค้าได้โดยไม่จำเป็นต้องมีเช็คนำฝากเข้าบัญชีของลูกค้ารายเดียวกันนั้นในวันก่อน ซึ่งเป็นจุดอ่อนของระบบงาน เนื่องจากไม่มีการป้องกันผู้ปฏิบัติงานทำรายการเช็คคืนผิดบัญชี และเตือนให้ผู้ปฏิบัติงานทราบถึงข้อผิดพลาดที่กล่าวก่อนนำข้อมูลเข้าระบบคอมพิวเตอร์

ข้อแนะนำ

ควรกำหนดให้มีการป้องกันข้อผิดพลาดในการทำรายการเช็คคืนผิดบัญชี โดยให้ระบบคอมพิวเตอร์ยอมรับรายการเช็คคืนเฉพาะกรณีที่มีเช็คนำฝากเข้าบัญชีลูกค้าในวันก่อน ถ้าหากยังตรวจสอบรายฉบับไม่ได้ก็ควรให้ตรวจสอบจำนวนเงินของรายการเช็คคืนกับจำนวนเงินที่นำฝาก และให้เครื่องคอมพิวเตอร์เตือนผู้ปฏิบัติงานให้ทำการยืนยันความถูกต้องในการทำรายการเช็คคืนทุกครั้ง

(14) **มีข้อผิดพลาดในการปฏิบัติงานของพนักงาน** Operator เกี่ยวกับการป้อนข้อมูลเพื่อควบคุมรายการหักบัญชีเงินฝากกระแสรายวันหรือเงินเบิกเกินบัญชีของลูกค้าโดยไม่มีเช็ค (No Cheque) หรือรายการหักบัญชีก่อนล่วงหน้า แล้วให้ลูกค้าส่งเช็คมาให้องค์กรภายหลัง (Cheque Will Follow) เพื่อองค์กรจะได้เก็บไว้เป็นหลักฐานการหักบัญชีของลูกค้า และเพื่อล้างเลขที่เช็คของลูกค้าออกจากแฟ้มควบคุมเช็คลูกค้ารายตัว (Cheque Number File) ซึ่งพนักงาน Operator มักสับสน โดยทำรายการ No Cheque เป็นรายการ Cheque Will Follow หรือทำรายการกลับกันในทางตรงกันข้าม ทำให้เกิดความยุ่งยากและมีจุดอ่อนในการควบคุมและตรวจสอบ

ข้อสังเกต

ธนาคารได้ปรับปรุงแก้ไขวิธีการควบคุมและเช็คสอบการทำรายการดังกล่าวแล้ว โดยมีแผนก Comptroller และแผนกบัญชีเป็นผู้รับผิดชอบ

(15) การอายัดเงินฝากเกินกว่ายอดเงินที่พึงถอนได้

ระบบยินยอมให้ทำรายการกันเงินฝากได้มากกว่าจำนวนเงินที่ลูกค้าพึงถอนได้ (Available Balance) ซึ่งอาจจะทำให้ผู้ใช้ข้อมูลเกี่ยวกับการกันเงินฝากไว้เป็นประกันเกิดความสับสน และอาจเข้าใจผิด ซึ่งอาจทำให้องค์กรได้รับความเสียหายได้

(16) การคิดดอกเบี้ยนอกเหนือจากอัตราดอกเบี้ยที่แท้จริง

อัตราดอกเบี้ยสูงสุดของบัญชีเงินเบิกเกินบัญชีที่ระบบคอมพิวเตอร์แจ้งให้ทราบ จะเป็นข้อมูลครั้งหลังสุดที่มีการเปลี่ยนแปลงอัตราดอกเบี้ยสูงสุดของบัญชีลูกหนี้เงินเบิกเงินบัญชีแต่ละราย ซึ่งอาจไม่ใช่อัตราดอกเบี้ยสูงสุดที่แท้จริงที่ใช้คำนวณดอกเบี้ย หาก Effective Date ซึ่งเป็นวันที่มีผลบังคับใช้อัตราดอกเบี้ยสูงสุดที่เปลี่ยนแปลงครั้งหลังสุด เป็นวันก่อนหน้า Effective Date ของการเปลี่ยนแปลงอัตราดอกเบี้ยสูงสุดในครั้งก่อน ๆ

จุดอ่อนที่กล่าวข้างต้นเป็นจุดอ่อนที่สามารถซ่อนเร้นข้อผิดพลาดที่อาจเกิดขึ้นโดยเจตนาหรือไม่เจตนาได้อย่างดี และมีผลกระทบต่อความน่าเชื่อถือของข้อมูลดอกเบี้ยเงินเบิกเกินบัญชีที่เรียกเก็บจากลูกค้าแต่ละราย

ข้อสังเกต

ในการเปลี่ยนแปลงดอกเบี้ยทุกครั้ง สำนักงานใหญ่จะมีหนังสือสั่งการเกี่ยวกับการเปลี่ยนแปลงดอกเบี้ยและวันที่มีผลบังคับใช้ ซึ่งตามปกติจะไม่มีการเปลี่ยนแปลงย้อนหลังเกิน 1 เดือน

(17) การคำนวณดอกเบี้ยเงินเบิกเกินบัญชีไม่ถูกต้อง

1) การปรับปรุงดอกเบี้ยเช็คคืน

เช็คเคลียริ่งที่ลูกค้านำมาเข้าบัญชีเพื่อลดยอดหนี้เงินเบิกเกินบัญชี แต่เป็นเช็คคืนในวันรุ่งขึ้น โปรแกรมที่ทำการปรับปรุงดอกเบี้ยจะใช้อัตราดอกเบี้ย Maximum Rate (อัตราร้อยละ 15 ต่อปี) มาคำนวณดอกเบี้ยที่เรียกเก็บเพิ่มจากลูกค้าเพราะเป็นเช็คคืน โดยไม่คำนึงถึงยอดหนี้คงค้างและอัตราดอกเบี้ยของแต่ละวงเงินตามสัญญาเงินเบิกเกินบัญชี ซึ่งไม่ถูกต้อง

2) การคำนวณดอกเบี้ยก่อนบันทึกดอกเบี้ยไม่ถูกต้อง

ในวันที่มีการบันทึก (POST) ดอกเบี้ยในตอนเย็นภายหลังจากการทำ DAY END PROCESS แล้วนั้น ก่อนที่โปรแกรมจะทำการบันทึกดอกเบี้ย โปรแกรมจะคำนวณดอกเบี้ยประจำวันจนถึงวันทำการถัดไป (NEXT PROCESSING DATE) ให้ก่อน (ซึ่งถ้าเป็นวันที่ไม่มีการ POST ดอกเบี้ย การคำนวณดอกเบี้ยดังกล่าวจะคำนวณตอนที่ทำ GOOD MORNING PROCESS ในวันทำการถัดมา) ด้วยอัตราดอกเบี้ยร้อยละ 15 ต่อปี ซึ่งเป็น Maximum Rate โดยไม่คำนึงถึงอัตราดอกเบี้ยที่กำหนดไว้ตามสัญญาเงินเบิกเกินบัญชีของแต่ละวงเงิน ซึ่งไม่ถูกต้อง

ข้อแนะนำ

องค์กรควรปรับปรุงแก้ไขวิธีการคำนวณดอกเบี้ยเงินเบิกเกินบัญชีในกรณีที่กล่าวข้างต้นให้ถูกต้องตามหลักความเป็นจริงหรือ Logic ของการคำนวณดอกเบี้ยที่ยอมรับกันโดยทั่วไป

(18) ไม่มีการป้องกันข้อผิดพลาดในการเปลี่ยนประเภทบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามของพนักงาน และการเปลี่ยนประเภทบัญชีสาขาอื่นให้เป็นบัญชีเงินเบิกเกินบัญชี

โปรแกรมแก้ไขวงเงินและอัตราดอกเบี้ยขององค์กรเปิดโอกาสให้ผู้ปฏิบัติงานกำหนดวงเงินและอัตราดอกเบี้ยสำหรับบัญชีพนักงานและบัญชีสาขาอื่น ซึ่งจะมีผลทำให้บัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามของพนักงานและบัญชีของสาขาอื่นในธนาคารเดียวกันสามารถเปลี่ยนประเภทบัญชีเป็นบัญชีเงินเบิกเกินบัญชีได้โดยไม่มีการควบคุม

ข้อแนะนำ

จุดอ่อนของระบบงานนี้ สามารถสร้างปัญหาและช่องทางทุจริตที่อาจก่อความเสียหายให้กับธนาคารได้มาก ดังนั้นธนาคารควรแก้ไขโปรแกรมมิให้มีการปฏิบัติงานเช่นนี้ได้ (ตามตัวอย่างนี้ ธนาคารไม่เคยทราบมาก่อนเลยว่าระบบงานหรือโปรแกรมเปิดโอกาสให้พนักงานใช้จุดอ่อนดังกล่าวในองค์กรของตน)

(19) วิธีการป้อนอัตราดอกเบี้ยที่เรียกเก็บจากลูกค้ายังไม่รัดกุม

ในการป้อนอัตราดอกเบี้ยที่เรียกเก็บจากลูกค้านั้น องค์กรใช้วิธีเพิ่มหรือลดจากอัตราดอกเบี้ยที่กำหนดไว้ตามประเภทของหลักประกัน เช่น องค์กรเรียกเก็บดอกเบี้ยจากลูกค้าที่มีเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาเป็นหลักประกันในอัตราร้อยละ 10 ต่อปี จะต้องลดอัตราดอกเบี้ยจากที่กำหนดไว้ร้อยละ 11 ต่อปี ลงร้อยละ 1 ต่อปี อย่างไรก็ดี หากผู้ปฏิบัติงานลดอัตราดอกเบี้ยเป็นจำนวนมากกว่าอัตราดอกเบี้ยที่กำหนดไว้ จะเป็นผลให้อัตราดอกเบี้ยที่ป้อนเข้าระบบมีค่าเป็นลบ แต่ในรายงาน Monthly O/D Line of C/A แสดงอัตราดอกเบี้ยดังกล่าวเป็นค่าบวก และอัตราดอกเบี้ยที่เรียกเก็บจริงจะสูงกว่าอัตราดอกเบี้ยที่ระบุไว้ตามสัญญา

ข้อแนะนำ

ควรกำหนดให้มีการควบคุมการป้อนอัตราดอกเบี้ยที่เรียกเก็บจากลูกค้าให้รัดกุม เช่น กำหนดให้เครื่องคอมพิวเตอร์เช็คสอบความถูกต้องเบื้องต้นของอัตราดอกเบี้ย (Rate Amount) เป็นต้น

(20) จุดอ่อนในการทำรายการย้อนวันที่ (Back Date)

1) สามารถทำรายการฝากถอนโดยป้อนวันที่ล่วงหน้าได้ ซึ่งไม่สอดคล้องกับลักษณะของการทำรายการย้อนวันที่และการบันทึกรายการทางการเงิน

2) หากทำรายการย้อนวันที่กับบัญชีเงินเบิกเกินบัญชี จะทำให้การคำนวณดอกเบี้ยสะสมไม่ถูกต้อง เนื่องจากโปรแกรมระบบงานไม่สามารถคำนวณยอดคงเหลือในบัญชีของแต่ละวันย้อนหลังเพื่อนำมาใช้ในการปรับปรุงดอกเบี้ยได้

3) สามารถใช้รายงานถอนย้อนวันที่เพื่อหลีกเลี่ยงหรือข้ามขั้นตอนในการอนุมัติรายการเบิกเงินเกินบัญชีจากผู้จัดการสาขาหรือพนักงานชั้นบริหารได้

4) ในรายการ Daily Current Account Transaction ไม่ได้แสดงการทำรายการเปิดบัญชีใหม่โดยย้อนวันที่

ข้อแนะนำ

ควรกำหนดให้มีการควบคุมการทำรายการย้อนวันที่ให้รัดกุม เช่น กำหนดให้มีการตรวจสอบข้อมูลเบื้องต้นของวันที่ย้อนหลัง มีข้อความเตือนก่อนยอมให้ทำรายการถอนย้อนวันที่ ซึ่งจะมีผลให้ยอดคงเหลือของบัญชีมียอดติดลบ และหลีกเลี่ยงการใช้รหัสรายการฝากถอนย้อนวันที่กับบัญชีเงินเบิกเกินบัญชีเป็นต้น

(21) การรักษาความลับของลูกค้ายังไม่ปลอดภัยเพียงพอ

ระบบงานยินยอมให้สาขาที่มิใช่เจ้าของบัญชี เรียกดูข้อมูลสำคัญบางประเภทของลูกค้าสาขาอื่น เช่น ยอดคงเหลือในบัญชี เลขที่เช็คที่จ่ายให้ลูกค้า วงเงินเบิกเกินบัญชี ผ่านทางเครื่อง Terminal อาจก่อให้เกิดความเสียหายแก่ลูกค้าได้ หากมีการเปิดเผยข้อมูลที่เป็นความลับของลูกค้าแก่บุคคลภายนอก

ข้อแนะนำ

การสอบถามข้อมูลของลูกค้าควรกระทำผ่านสาขาเจ้าของบัญชีเท่านั้น เพื่อป้องกันการเปิดเผยข้อมูลซึ่งเป็นความลับของลูกค้าแก่บุคคลอื่นซึ่งมิใช่เจ้าของบัญชี

(22) โปรแกรมระบบงานนับจำนวนบัญชีเงินฝากไม่ถูกต้อง

เนื่องจากโปรแกรมระบบงานนับจำนวนบัญชีของเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามของลูกค้าที่มียอดคงเหลือในบัญชีเป็นศูนย์ เป็นจำนวนบัญชีของเงินเบิกเกินบัญชี ทำให้การนับจำนวนบัญชีเงินฝากไม่ถูกต้องตรงกับความเป็นจริง

ข้อแนะนำ

ควรแก้ไขโปรแกรมระบบงานให้นับจำนวนบัญชีที่มียอดคงเหลือเป็นศูนย์ เป็นของบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม แทนที่จะเป็นของบัญชีเงินเบิกเกินบัญชี เพื่อให้การนับจำนวนบัญชีถูกต้อง

(23) ไม่ได้แยกเก็บหรือทำลายรายงานที่ผิดพลาด

ผู้ปฏิบัติงานยังคงจัดเก็บรายงานชุดที่ผิดพลาดรวมอยู่กับรายงานชุดที่ถูกต้อง

ข้อแนะนำ

ควรประทับตรายกเลิก และแยกรายงานชุดที่ผิดพลาดไว้ต่างหาก เพื่อป้องกันความสับสนในการใช้รายงาน

(24) **บัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามแต่ถูกจัดขึ้นเป็นหนี้ในรายงาน**

ลูกหนี้เงินเบิกเกินบัญชีรายที่มีการจัดขึ้นเปลี่ยนสภาพเป็นเงินฝาก และถ้าไม่มีการล้าง Status การจัดชั้นหนี้ของลูกหนี้ออกไปจากระบบงานแล้ว รายงานจะยังคงแสดงชื่อบัญชีลูกค้ารายที่มียอดคงเหลือตามบัญชีเป็นเงินฝาก เป็นลูกหนี้จัดชั้นอยู่ ซึ่งคลาดเคลื่อนไปจากความเป็นจริง

ข้อสังเกต

ในการแก้ไขสถานการณ์จัดชั้นหนี้ ปกติสาขาจะต้องได้รับอนุมัติจากสำนักงานใหญ่ ซึ่งสาขาจะต้องป้อนรหัสข้อมูลเข้าไปแก้ไขการจัดชั้นทุกครั้งที่ได้รับคำสั่งอนุมัติ ดังนั้น สาขาควรตรวจสอบติดตามรายงาน และแจ้งให้สำนักงานใหญ่ทราบเพื่อขออนุมัติให้เป็นไปตามขั้นตอนด้วย

(25) **รายงานที่มีข้อผิดพลาด**

1) Total Available Balance ไม่ถูกต้อง
2) รายงาน C/A Outstanding Report และรายงาน Daily Trial Balance แสดงข้อมูลไม่ตรงกัน

ข้อแนะนำ

(1) คู่มือการปฏิบัติงานเป็นเอกสารอ้างอิงที่สำคัญในการดำเนินงานขององค์กร จึงควรจัดทำให้ถูกต้อง ชัดเจน และเป็นปัจจุบัน เพื่อให้สามารถใช้ประโยชน์ได้อย่างแท้จริง ในกรณีรหัสรายการใดที่ไม่มีการใช้งานก็ควรยกเลิกออกจากระบบงาน เพื่อไม่ให้เกิดความสับสนในการปฏิบัติงาน และป้องกันปัญหาการทำรายการผิดพลาด

(2) ควรกำหนดให้โปรแกรมตรวจสอบอัตราดอกเบี้ยของแต่ละวงเงิน มิให้เกินอัตราสูงสุดตามประกาศของทางการ

(3) ควรให้โปรแกรมตรวจสอบจำนวนเงินฝากที่จะกันไว้เป็นประกัน มิให้มากกว่ายอดเงินคงเหลือที่ลูกค้าพึงถอนได้ (Available Balance) เพื่อเป็นการป้องกันความเสียหายที่อาจจะเกิดขึ้น

(4) ในกรณีที่ลูกค้ามีหลายวงเงิน สาขาควรระมัดระวังในการเลือกใช้อัตราดอกเบี้ยในการคำนวณดอกเบี้ยเช็คคืนให้ถูกต้อง

(5) ควรปรับปรุงแก้ไขระบบงานคอมพิวเตอร์ให้สามารถป้องกันการซ่อนเร้นอัตราดอกเบี้ยที่แท้จริงที่เรียกเก็บจากลูกหนี้เงินเบิกเกินบัญชี โดยให้รหัสรายการ Contract Inquiry แสดงอัตราดอกเบี้ยที่ถูกต้องและเป็นอัตราเดียวกับที่เรียกเก็บจากลูกหนี้

(6) ควรปรับปรุงรายงาน C/A Classified O/D Account Report ให้แสดงเฉพาะลูกหนี้เงินเบิกเกินบัญชีรายที่มีการจัดชั้นเท่านั้น และควรมีข้อความบอกให้ทราบว่า บัญชีใดบ้างที่ยังไม่ได้ทำการเปลี่ยน Status ให้ถูกต้องในรายงานอื่นที่เกี่ยวข้อง เพื่อที่จะทำการแก้ไขให้ถูกต้อง

(7) ควรยกเลิก Miscellaneous Code ที่ไม่เกี่ยวข้องกับบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและบัญชีเงินเบิกเกินบัญชี เพื่อไม่ให้เกิดความสับสน

(8) ควรปรับปรุงแก้ไขรายงานที่มีข้อผิดพลาดให้ถูกต้อง

(26) ไม่มีการควบคุมการเปิดบัญชีเท่าที่ควร

การควบคุมการเปิดบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามยังไม่รัดกุมเท่าที่ควร โดยยินยอมให้พนักงาน Teller ทำรายการเปิดบัญชีให้ลูกค้าด้วยจำนวนเงินฝากต่ำกว่า 10,000.00 บาท หรือทำรายการเปิดบัญชีเงินเบิกเกินบัญชีได้โดยไม่มีพนักงานชั้นบริหารสอบทานการปฏิบัติงานโดยใกล้ชิด

ข้อสังเกต

ธนาคารได้แก้ไขตามคำแนะนำแล้ว

(27) รายงานที่ออกโดยคอมพิวเตอร์ไม่ถูกต้องตามความเป็นจริง

1) Statement ที่จัดส่งให้ลูกค้า

ยอดคงเหลือยกไป (C/F) ที่แสดงใน Statement ที่องค์กรจัดส่งให้ลูกค้ายังคลาดเคลื่อนไปจากความเป็นจริง เนื่องจากองค์กรใช้ยอดคงเหลือของ Record ต่อไปใน Deposit Statement File มาพิมพ์แทนยอดคงเหลือที่ถูกต้อง

2) รายงานแสดงการปิดบัญชี

ในกรณีที่ Customer Service ให้เลขที่บัญชีสำหรับบัญชีที่เปิดใหม่ถูกต้องจะต้องทำ Customer History Maintenance โดยเปลี่ยน Active Code เป็น "C" เพื่อปิดบัญชีที่ใช้เลขที่บัญชีไม่ถูกต้องนั้นเสีย แต่อย่างไรก็ดี ในรายงานแสดงการปิดบัญชีได้นับบัญชีที่มีอยู่ทั้งสิ้นในปัจจุบันด้วย ซึ่งไม่ถูกต้อง เพราะรายการแก้ไขที่กล่าวข้างต้นได้ปรากฏอยู่ในรายงานการแก้ไขประวัติลูกค้าแล้ว

3) รายงานยอดคงเหลือ

วันที่ที่มีรายการเคลื่อนไหวครั้งสุดท้ายของบัญชีลูกค้าที่ปรากฏอยู่ในยอดคงเหลือ (บัญชีกระแสรายวัน) ยังไม่ถูกต้อง เพราะองค์กรนำวันที่ทำการ Set up มาพิมพ์แทนวันที่เคลื่อนไหวครั้งหลังสุด ทั้ง ๆ ที่บัญชีลูกค้ามีรายการเคลื่อนไหวหลังจากวัน Set up แล้ว

4) รายงานการให้สินเชื่อแยกตามประเภทธุรกิจ

แสดงยอดคงค้างไม่ถูกต้อง โดยใช้ยอดคงค้างของบัญชีต่าง ๆ ที่มี Business Code เดียวกัน ซึ่งมีทั้งด้านเดบิตและเครดิต มาหักกลบลบกัน เอายอดสุทธิมาออกรายงาน แทนที่จะใช้เฉพาะยอดรวมด้านเดบิต (มีภาระเป็นลูกหนี้ขององค์กรในวันออกรายงาน) ของแต่ละบัญชีที่มี Business Code เดียวกันมาออกรายงาน

5) รายงานที่ออกครั้งแรกหลังวันที่ทำการ Set up ข้อมูลจากระบบเก่าเข้าสู่ระบบคอมพิวเตอร์

- รายงานแสดงยอดคงเหลือแยกตาม Segment (บัญชีกระแสรายวัน)

ในวันทำการวันแรกหลังจากการ Set up ยอดของ "ยอดคงเหลือเดิม" ในรายงานแสดงยอดเป็น 0.00 ไม่ได้ยกยอดบัญชีที่ทำการ Set up เข้าไป มาแสดงไว้ จึงทำให้ยอด "เพิ่มขึ้น/ลดลง" ในรายงาน แสดงยอดที่ไม่ถูกต้องเฉพาะวันทำการวันแรกหลังจากการ Set up เท่านั้นวันต่อ ๆ มาจะถูกต้อง

- รายงานยอดเบิกเกินบัญชีแยกตามอัตราดอกเบี้ย (บัญชีกระแสรายวัน) ดอกเบี้ยสะสมในตอน Set up และดอกเบี้ยของวันทำการก่อนจนถึง TODAY DATE ซึ่งเป็นดอกเบี้ยที่คำนวณตอนที่ทำ GOOD MORNING PROCESS ไว้ด้วย

ข้อสังเกต

ธนาคารได้แก้ไขตามคำแนะนำของผู้ตรวจสอบแล้ว สำหรับปัญหาการออกรายงานครั้งหลังธนาคารได้กำชับให้เจ้าหน้าที่ใส่วันที่ ๆ จะ Set up ด้วย

(28) โปรแกรมระบบงานไม่มีการตรวจสอบรายการเช็คคืนของบัญชีเงินฝากที่ไม่มีการฝากด้วยเช็คเคลียริ่ง

โปรแกรมระบบงานไม่มีมาตรการป้องกันความผิดพลาดในการบันทึกรายการเช็คคืนที่ลูกค้านำฝากด้วยเช็คเคลียริ่ง เป็นผลให้มีการบันทึกรายการเช็คคืนผิดบัญชี และมีผลทำให้ยอดเงินฝากคงเหลือในบัญชีลูกค้าและการคำนวณดอกเบี้ยไม่ถูกต้อง ได้แก่

1) กรณีทำรายการเช็คคืนผิดประเภทบัญชี (Account Type) แต่เป็นของลูกค้ารายเดียวกัน หากไม่มีการแก้ไขข้อผิดพลาดดังกล่าว จะเป็นผลทำให้มีการคำนวณดอกเบี้ยของเงินฝากออมทรัพย์ให้แก่รายการที่ไม่มีการฝากจริง

2) กรณีทำรายการเช็คคืนผิดเลขที่บัญชี (Account Root) และเป็นบัญชีของลูกค้าคนละราย อาจก่อให้เกิดผลเสียหายแก่ลูกค้าที่พนักงานทำรายการเช็คคืนผิดบัญชี เนื่องจากยอดเงินฝากลดลง หรือเงินเบิกเกินบัญชีเพิ่มขึ้น และไม่ได้รับดอกเบี้ยจากเงินฝากของตน หรือถูกคิดดอกเบี้ยจากเงินเบิกเกินบัญชีในจำนวนเงินที่ลูกค้าไม่ได้ถอนเงินไปจริง นอกจากนี้องค์กรอาจเสียหายได้หากลูกค้าผู้นำเช็คเคลียริ่งเข้าฝากแล้วเป็นเช็คคืน ถอนเงินจำนวนดังกล่าวไป และองค์กรได้จ่ายดอกเบี้ยให้หรือไม่ได้คิดดอกเบี้ยเงินเบิกเกินบัญชีจากบัญชีดังกล่าวด้วย

ข้อแนะนำ

เพื่อป้องกันข้อผิดพลาดในการคำนวณดอกเบี้ยและรักษาผลประโยชน์ของกิจการ ควรกำชับพนักงานที่เกี่ยวข้องให้เพิ่มความระมัดระวังในการจัดเตรียมและตรวจสอบความถูกต้องของรายการเช็คคืนทุกครั้งก่อนนำไปบันทึกรายการ หากองค์กรมีการพัฒนาระบบงานเพิ่มเติม ควรกำหนดให้โปรแกรมระบบงานสามารถทำการเช็คสอบรายการเช็คคืนให้ถูกต้องด้วย เพื่อช่วยให้การปฏิบัติงานของพนักงานมีความถูกต้องมากขึ้น

(29) การแก้ไขรายการฝากเช็คย้อนหลังไม่ถูกต้อง

จากการตรวจสอบพบว่ามีการจ่ายดอกเบี้ยไม่ถูกต้อง เนื่องจากการแก้ไขรายการเช็คคืนและรายการฝากด้วยเช็คซึ่งเข้าผิดบัญชี ของลูกค้ารายเดียวกัน โดยการย้อนหลัง (Back Date) มากไป 4 วัน

จากข้อผิดพลาดดังกล่าวข้างต้น หากองค์กรจ่ายดอกเบี้ยให้ลูกค้าในอัตราสูงสุดตามที่กฎหมายกำหนดไว้แล้ว อาจทำให้องค์กรจ่ายดอกเบี้ยเกินอัตราที่กฎหมายกำหนดได้

ข้อแนะนำ

ควรกำหนดให้พนักงานผู้รับผิดชอบตรวจสอบและระมัดระวังการแก้ไขรายการย้อนหลังโดยรัดกุม

(30) ไม่มีการจำกัดอำนาจในการผ่านรายการของพนักงานป้อนข้อมูล

โปรแกรมระบบงานที่องค์กรใช้ในการเตรียมข้อมูลนำเข้า ไม่มีการจำกัดอำนาจพนักงานป้อนข้อมูลเพื่อควบคุมการป้อนข้อมูลบางรายการ เช่น การผ่านรายการถอนเงินจากบัญชีที่ถูกอายัดเป็นต้น ซึ่งอาจก่อให้เกิดความเสียหายต่อองค์กรได้

ข้อแนะนำ

ควรกำหนดให้โปรแกรมระบบงานแบ่งแยกระดับของพนักงาน ทำหน้าที่อนุมัติรายการเพื่อให้การควบคุมการป้อนข้อมูลรัดกุมยิ่งขึ้น

(31) การป้อน Interest Statement Date ผิดพลาด

มีการป้อน Interest Statement Date ผิดพลาด โดยป้อนเป็นวันที่ 27 กันยายน และ 26 มกราคม แทนที่จะเป็นวันที่ 26 พฤษภาคม และ 26 กุมภาพันธ์ ตามลำดับ ทำให้การบันทึกดอกเบี้ยประจำเดือนเป็นไปโดยไม่ถูกต้อง

(32) ไม่มีการควบคุมเลขที่เช็ครายฉบับ

โปรแกรมระบบงานเงินฝากซึ่งธนาคารจะนำมาใช้ใหม่นั้น จะตรวจสอบเลขที่เช็คของลูกค้าที่มาตัดบัญชีกับ Cheque Range ของแต่ละบัญชีเท่านั้น ไม่มีการบันทึกเลขที่เช็ครายฉบับที่ได้ผ่านบัญชีไปแล้ว ฉะนั้นหากมีข้อผิดพลาด เช่น ป้อนเลขที่เช็คที่เคยผ่านบัญชีไปแล้วซ้ำอีก หรือมีเช็คปลอมมาตัดบัญชีโปรแกรมงานจะไม่มีการตรวจสอบข้อผิดพลาดในกรณีดังกล่าว ซึ่งอาจก่อให้เกิดความเสียหายแก่ลูกค้าและธนาคารได้ ซึ่งธนาคารชี้แจงว่าปัจจุบันยังไม่มีปัญหาที่กล่าว และรับจะพิจารณาหามาตรการป้องกันต่อไป

ข้อแนะนำ

ควรพิจารณาเพิ่มการควบคุม โดยการบันทึกเลขที่เช็ครายฉบับทุกเล่มที่จ่ายให้ลูกค้าเพื่อตัดเลขที่เช็คที่ลูกค้านำมาผ่านบัญชีแล้ว เพื่อป้องกันการผ่านเช็คเลขที่ซ้ำกัน นอกจากนี้การ Delete Cheque Range แต่ละ Range ควรให้โปรแกรมงานพิมพ์รายงานเลขที่เช็คทุกฉบับที่ยังไม่มาผ่านบัญชีเพื่อให้เจ้าหน้าที่ใช้ตรวจสอบก่อนการอนุมัติให้ตัดเช็คได้ เมื่อมีเช็คเลขที่ที่ถูก Delete Cheque Range มาขอผ่านบัญชี

(33) ไม่มีการตรวจสอบข้อมูลก่อนทำการล้างรายการ (Reverse Entries)

ระบบงานไม่เช็คสอบการล้างรายการต่าง ๆ ออกจากบัญชีเงินฝากของลูกค้าว่ามีรายการที่ ผิดพลาดบันทึกไว้ในบัญชีของลูกค้ารายนั้นอยู่ก่อนแล้ว เช่น การทำรายการเช็คคืน การแก้ไขข้อผิดพลาดของรายการ Cash, Transfer และ House Cheque เป็นต้น ซึ่งอาจทำให้มีการล้างรายการผิดบัญชีได้ ซึ่งระบบไม่สามารถป้องกันการผิดพลาดในลักษณะต่าง ๆ ดังกล่าว แต่ผู้ใช้ข้อมูลจะพบข้อผิดพลาดในวันทำการถัดไป โดยตรวจสอบความถูกต้องในการบันทึกบัญชีจากรายงานกับ Slip

ข้อแนะนำ

(1) เพื่อป้องกันข้อผิดพลาดในการคำนวณดอกเบี้ยและรักษาผลประโยชน์ขององค์กร ควรกำชับพนักงานที่เกี่ยวข้องให้เพิ่มความระมัดระวังในการจัดเตรียมและตรวจสอบความถูกต้องของแบบฟอร์ม Account Maintenance Form ทุกครั้งก่อนนำไปบันทึกรายการ

(2) เพื่อป้องกันมิให้มีการป้อนรายการถอนเงินด้วยเช็คผิดบัญชี องค์กรควรป้อนเลขที่เช็คที่จ่ายให้แก่ลูกค้าเข้าเครื่องคอมพิวเตอร์ เพื่อให้โปรแกรมทำการเช็คสอบก่อนยินยอมให้มีการถอนเงินจากบัญชี

(3) เพื่อป้องกันการล้างรายการ (Reverse Entries) ผิดบัญชีองค์กรควรแก้ไขโปรแกรมให้มีการตรวจสอบการป้อนรายการเช็คคืนหรือรายการแก้ไขข้อผิดพลาดต่าง ๆ โดยินยอมให้ป้อนได้ต่อเมื่อมีรายการ Clearing Cheque Hold หรือรายการที่ผิดพลาดบันทึกอยู่แล้วเท่านั้น

(34) โปรแกรมประมวลผลและคำนวณดอกเบี้ยเงินเบิกเกินบัญชีประจำวันของระบบงานเงินฝากกระแสรายวันและเงินเบิกเกินบัญชี มีข้อผิดพลาดในการประมวลผล ซึ่งมีผลให้องค์กรเรียกเก็บดอกเบี้ยจากบัญชีเงินเบิกเกินบัญชีไม่ถูกต้อง

(35) มีข้อผิดพลาดในการปฏิบัติงาน เนื่องจากการทำรายการเพื่อยกเลิกวงเงินเบิกเกินบัญชีด้วย Deposit Accout Correction โปรแกรมคำสั่งงานจะล้างรายการดอกเบี้ยสะสมในแฟ้มข้อมูลให้มียอดคงเหลือเป็นศูนย์ (0) และถ้าพนักงานที่รับผิดชอบไม่ได้เรียกเก็บหรือหักบัญชีลูกค้าเป็นค่าดอกเบี้ยเงินเบิกเกินบัญชีก็จะถูกยกเลิก ซึ่งทำให้องค์กรสูญเสียรายได้ที่พึงได้รับ

(36) ไม่ได้ควบคุมและตรวจสอบรายละเอียดผลของการป้อนข้อมูล เพื่อควบคุมและตรวจสอบความถูกต้อง

(37) จุดอ่อนของการทำ Cheque Issued/Collected

1) องค์กรไม่ได้ควบคุมและป้องกันการบันทึกรายการ Cheque Collected Type "C" เพื่อยกเลิกหรือล้างหมวดเลขที่เช็คทั้งหมดออกจากบัญชีของลูกค้าในแฟ้มข้อมูล (File) ซึ่งทำให้มีเนื้อที่ว่างพอที่จะบันทึกเลขที่เช็คหมวดใหม่เข้าไปได้

ในการทำรายการดังกล่าว มีผลให้เลขที่เช็คที่เคยเบิกถอนเงินไปแล้ว แสดงสถานะในแฟ้มข้อมูลว่ายังไม่เคยเบิกถอนเงินออกไป และถ้ามีเช็คที่เคยหักบัญชีไปแล้ว โดยมีเลขที่เช็คซ้ำกับเลขที่เช็คเดิมซึ่งเคยเบิกถอนเงินไปแล้วมาเบิกถอนเงินอีก โปรแกรมควบคุมและตรวจสอบเลขที่เช็คจะไม่สามารถตรวจสอบได้ และจะสามารถเบิกถอนเงินจากบัญชีของลูกค้านั้นไปได้อีกครั้งหนึ่ง ซึ่งอาจนำความเสียหายมาสู่องค์กรได้

2) องค์กรไม่ได้กำหนดให้มีการอนุมัติจากเจ้าหน้าที่ชั้นบริหารขององค์กรในการควบคุมหรือจำกัด ขอบเขตการป้อนข้อมูลเพื่อบันทึกรายการ Cheque Issued ของลูกค้า เพื่อป้องกันเช็คของผู้อื่นหรือเช็คที่เคยหักบัญชีไปแล้วมาเบิกถอนเงินจากบัญชีของลูกค้า ซึ่งอาจจะก่อให้เกิดความเสียหายขึ้นได้

ข้อแนะนำ

องค์กรควรพิจารณาและปรับปรุงแก้ไขจุดอ่อนข้างต้น ดังนี้คือ

1) ควรควบคุมหมวดเลขที่เช็คที่ถูกทำด้วยรายการ Cheque collected Type "C" ด้วยความระมัดระวังเป็นพิเศษ เพื่อป้องกันมิให้มีเลขที่เช็คซ้ำกันผ่านบัญชีได้อีก

2) ควรมีการตรวจสอบความถูกต้องของเลขที่เช็คที่ยังค้างอยู่ในแฟ้มข้อมูลลูกค้าโดยเฉพาะรายใหญ่เป็นครั้งคราว

(38) องค์กรมิได้ใช้คอมพิวเตอร์ควบคุมการเบิกถอนเงินโดยใช้เช็คฉบับที่ลูกค้าสั่งอายัดในระหว่างวัน

ดังนั้น หากไม่มีการควบคุมทางด้าน Manual ที่รัดกุม อาจก่อให้เกิดความเสียหายต่อองค์กรได้ เนื่องจากเมื่อพนักงานประจำ Counter ได้รับแจ้งการอายัดเช็คจากลูกค้า พนักงานจะจัดทำตั๋ว Stop Payment/Hold สั่งให้ Data Processing Center (DPC) ทำการ Capture ขณะเดียวกันก็จะบันทึกหมายเลขเช็คที่ลูกค้าสั่งอายัดลงเทปกระดาษติดไว้ที่จอ เพื่อใช้ในการตรวจสอบเช็คอายัดในระหว่างเวลาทำการ ซึ่งเทปกระดาษดังกล่าวอาจสูญหายไปได้ และเป็นเหตุให้มีการเบิกจ่ายเงินจากเช็คฉบับที่ถูกสั่งอายัดแล้ว

ข้อแนะนำ

องค์กรควรจัดให้มีการควบคุมเพื่อป้องกันการเบิกถอนเงินโดยใช้เช็คที่ถูกอายัดในระหว่างวันให้รัดกุมยิ่งขึ้น โดยให้พนักงานตรวจสอบเช็คที่ถูกทำอายัดแล้วกับทะเบียนคำสั่งอายัดทุกครั้ง

(39) จากการตรวจสอบและทดสอบโปรแกรมระบบงาน Ledger Accounting ขององค์กร พบว่า มิได้มีการควบคุมป้องกันการทำ Stop Payment/Hold ด้วยเลขที่เช็คซ้ำหมายเลขกัน ซึ่งอาจเกิดจากการจัดทำตั๋ว Delete รายการ Stop Payment ดังกล่าว ปรากฏว่าสามารถ Delete ได้เพียงฉบับเดียวยังคงอยู่ใน File-Stop Payment อีก 1 ฉบับ อาจก่อให้เกิดผลดังนี้

1) เมื่อลูกค้าสั่งยกเลิกการอายัดเช็คแล้ว ก็ยังไม่สามารถผ่านบัญชีเช็คฉบับนั้น และเป็นเหตุให้ผู้ทรงเช็คไม่ได้รับเงินตามเช็คฉบับที่กล่าว

2) กรณีที่มีการสั่งอายัดเช็คเรียงติดกันหลายฉบับและเกิดการอายัดซ้ำ เป็นเหตุให้มีเลขที่เช็คบางฉบับไม่ได้รับการอายัด เมื่อเช็คฉบับนั้นมาคอยตัดบัญชีหรือถูกนำมาขึ้นเงิน องค์กรก็อาจเกิดความเสียหายได้

ข้อแนะนำ

1) ควรกำหนดให้มีการตรวจสอบการสั่งอายัดเช็คซ้ำ รวมทั้งการ Delete

2) ก่อนที่จะทำการ Stop Payment ควรตรวจสอบรายงาน Complete Stop Payment เพื่อดูว่ามีรายการที่อาจซ้ำกันหรือไม่

(41) การควบคุมการเบิกจ่ายเงินโดยเช็คที่มีหมายเลขซ้ำกับหมายเลขเช็คที่ถอนเงินไปแล้ว

ระบบงานเงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม สามารถเก็บหมวดหมายเลขเช็คได้ครั้งละหนึ่งหมวด แต่ละหมวดสูงสุด 999 ฉบับ เพื่อใช้ตรวจสอบหมายเลขเช็คที่ลูกค้านำมาถอนเงิน หากหมายเลขเช็คนั้นมิได้อยู่ในหมวดที่บันทึกไว้ จะมี Message เตือนว่า "CHQ NO. NOT IN CHQ. RANGE" เพื่อให้เจ้าหน้าที่รับมอบอำนาจระมัดระวังการอนุมัติรายการ แต่ระบบงานจะไม่ตรวจสอบหมายเลขเช็คซ้ำได้

(42) ไม่มีการควบคุมและเช็คสอบการแก้ไขรายการในโปรแกรมระบบงาน

จากการทดสอบ (Test) การทำรายการแก้ไขการรับฝากเงินโดยรายการโอนเงินปรากฏว่าโปรแกรมไม่มีการตรวจสอบรหัสรายการที่ทำผิดพลาด และไม่ตรวจสอบจำนวนเงินที่ป้อนเพื่อแก้ไขว่าตรงกับยอดที่ป้อนฝากครั้งแรกหรือไม่ ทำให้บัญชีเงินฝากดังกล่าวมีสภาพเป็นเงินเบิกเกินบัญชี ซึ่งอาจมีผลกระทบต่อความถูกต้องน่าเชื่อถือของข้อมูลทางการเงิน และอาจเป็นจุดอ่อนของระบบการควบคุมเนื่องจากเสมือนกับการทำรายการถอนเงินสด ซึ่งปกติจะมีการตรวจสอบยอดเงินที่ลูกค้ามีสิทธิถอนได้ (Available balance) และมีการตรวจสอบอำนาจของสาขาในการให้เงินเบิกเกินบัญชี เมื่อมีการเบิกเงินเกินกว่ายอดเงินฝาก (Available balance) หรือมีการเบิกเงินเกินบัญชีเกินกว่าอำนาจของสาขา จะมี Message เตือน หากมีการเลี่ยงมาใช้รหัสรายการอื่นทำรายการแทน เครื่องคอมพิวเตอร์จะผ่านรายการให้โดยข้ามขั้นตอนการตรวจสอบ และไม่มี Message ใด ๆ เตือนให้ทราบ แม้จะมีการตรวจสอบวงเงินตามอำนาจผู้ทำรายการ (Teller Level) ก็ตาม แต่ผู้ทำการ Override ก็อาจไม่ทราบข้อเท็จจริงกับกรณีที่จะเกิดขึ้นได้

อนึ่ง ในทำนองเดียวกัน รหัสรายการที่ใช้ในการแก้ไข (Correction) รายการถอนเงินสดและรายการเช็คคืนโดยไม่มีการตรวจสอบยอดเงินกับรายการ เป็นจุดอ่อนในการแก้ไขรายการที่ Key ผิดพลาด เพราะอาจได้ผลตรงข้าม คือแทนที่จะลบล้างข้อมูลที่ผิดพลาด กลับกลายเป็นการเพิ่มยอด Available balance

ข้อแนะนำ

องค์กรจะแก้ไขระบบงานไม่ให้มีการ Correction เกินกว่ายอด Available balance ถ้าเกิน จะต้องให้ Supervisor Override รายการเสียก่อนจึงจะทำให้ สำหรับการเช็คสอบรหัสรายการ จำนวนเงิน และเลขที่บัญชีของรายการที่ต้องการจะ correct กับรายการแรกที่ตั้งนั้น ระบบงานควรมีการเช็คสอบว่าจะต้องมีรายการที่ทำวันนี้ก่อน จึงจะทำรายการ Correction ได้ และเช็คสอบ Limit ของเจ้าหน้าที่ Teller รวมทั้งการควบคุมด้าน Manual โดยเจ้าหน้าที่ Supervisor

(34) ระบบงานยินยอมให้เปิดบัญชีเงินฝากต่างสาขาได้

จากวิธีการปฏิบัติองค์กรไม่ให้มีการเปิดบัญชีของสาขาใดสาขาหนึ่งโดยสาขาอื่น ๆ แต่จากการทดสอบพบว่า โดยระบบงาน พนักงาน Teller สามารถทำรายการเปิดบัญชีของสาขาอื่นได้ โดยสาขาเจ้าของบัญชีอาจไม่ทราบ ซึ่งเป็นจุดอ่อนในการควบคุมภายใน

ข้อแนะนำ

1) ควรเพิ่มมาตรการในการควบคุมการเบิกจ่ายเงินโดยเช็คที่มีหมายเลขซ้ำกับหมายเลขเช็คที่ถอนเงินไปแล้ว ให้รัดกุมยิ่งขึ้น เพื่อป้องกันการทุจริตอันเกิดจากการนำเช็คปลอมที่มีหมายเลขซ้ำกับเช็คฉบับจริงที่ถอนเงินไปแล้ว มาเบิกถอนเงินซ้ำอีก

2) ควรกำหนดมาตรการควบคุมความถูกต้องของรายการ Correction ไม่ให้ทำรายการได้เกินกว่าอำนาจของสาขา

3) ควรควบคุมให้ทำรายการเปิดบัญชีได้เฉพาะสาขาของเจ้าของบัญชีเท่านั้น

(44) รหัสรายการ Convert withdraw ไม่มีการตรวจสอบยอดเงินคงเหลือในบัญชีลูกค้าหรือวงเงินเบิกเกินบัญชีกับจำนวนเงินที่ถอนก่อนยินยอมให้ผ่านรายการ ซึ่งผู้ปฏิบัติงานอาจใช้รหัสรายการที่ผ่านรายการให้ลูกค้าและหลีกเลี่ยงการขออนุมัติวงเงินเบิกเกินบัญชีชั่วคราวได้

(45) กรณีรับฝากและทำรายการถอนลงวันที่ย้อนหลังให้ลูกค้าในวันเดียว เครื่องคอมพิวเตอร์จะคำนวณดอกเบี้ยเงินเบิกเกินบัญชีเฉพาะรายการถอนด้วยรหัสรายการถอนโดยลงวันที่ย้อนหลังเท่านั้น ได้คำนึงถึงยอดเงินคงเหลือตามบัญชีเมื่อสิ้นวัน ทำให้การคำนวณดอกเบี้ยคลาดเคลื่อนไปจากความเป็นจริง

(46) รหัสรายการ Convert deposit ซึ่งใช้ทำรายการรับฝากเงิน กรณีที่ต้องการลงวันที่ย้อนหลังให้ลูกค้าที่เคยฝากเงินมาแล้วนั้น หากมีการลงวันที่ผิดพลาด เช่น ลงวันที่ล่วงหน้าอาจตรวจไม่พบ ซึ่งจะทำให้การคำนวณดอกเบี้ยเงินเบิกเกินบัญชีคลาดเคลื่อนไปจากความเป็นจริงเช่นเดียวกัน

ข้อแนะนำ

(1) องค์กรควรกำหนดให้มีการขออนุมัติจากพนักงานชั้นบริหารก่อนยินยอมให้ใช้รหัสรายการ Convert withdraw เพื่อป้องกันผู้ปฏิบัติงานหลีกเลี่ยงการขออนุมัติวงเงินเบิกเกินบัญชีชั่วคราว

(2) การนำรหัสรายการ Convert deposit และรหัสรายการ Convert withdraw มาใช้ทำรายการฝากถอนเงินในระบบ On-line ควรปรับปรุงวิธีการคำนวณดอกเบี้ยเงินเบิกเกินบัญชีให้ถูกต้องด้วย

(3) การนำรหัสรายการ Convert deposit มาใช้ทำรายการรับฝากเงินกรณีที่ต้องการลงวันที่ย้อนหลังให้ลูกค้า ควรมีวิธีการป้องกันการลงวันที่ย้อนหลังให้ลูกค้าผิดพลาดด้วย ทั้งนี้เพราะการลงวันที่ย้อนหลังให้ลูกค้าผิดพลาดจะทำให้การคำนวณดอกเบี้ยเงินเบิกเกินบัญชีคลาดเคลื่อนไปจากความเป็นจริง และในบางกรณีอาจมีผลทำให้อัตราดอกเบี้ยที่เรียกเก็บจากลูกหนี้สูงเกินกว่าอัตราดอกเบี้ยตามที่กฎหมายกำหนด

(47) การควบคุมเลขที่สมุดเช็คที่จ่ายให้ลูกค้า

การทำรายการ Issue check book เพื่อป้อนเลขที่เช็คฉบับที่มอบให้ลูกค้าเก็บไว้ในระบบคอมพิวเตอร์สำหรับควบคุมและป้องกันการตัดเช็คผิดบัญชี ซึ่งอนุญาตให้พนักงาน Teller ทำรายการนี้ได้โดยไม่ต้องใช้บัตรอนุมัติรายการ (Authorized card) และไม่มีพนักงานอื่นสอบทานการป้อนข้อมูลดังกล่าวนั้น เป็นจุดอ่อนในการควบคุมภายใน ผู้ที่ทราบจุดอ่อนสามารถทำรายการ Issue check book เพื่อให้ระบบคอมพิวเตอร์ยอมผ่านเช็คฉบับที่ต้องการตัดบัญชีของลูกค้าได้ทุกบัญชี

ข้อแนะนำ

ควรจัดให้มีการใช้บัตรอนุมัติรายการควบคุมการทำรายการ Issue check book เพื่อป้องกันข้อผิดพลาดในการป้อนเลขที่เช็คฉบับที่องค์กรมอบให้ลูกค้าเก็บไว้ในระบบคอมพิวเตอร์สำหรับควบคุมเช็คที่มาตัดบัญชี

(48) Total Available Balance ถูกหักด้วยยอดที่เบิกเกินวงเงิน

โปรแกรมที่ออกรายงาน C/A outstanding report ซึ่งนำเอาส่วนที่ลูกค้าเบิกเกินวงเงิน มาหักออกจากยอดรวมของวงเงินที่ลูกค้ามีสิทธิถอนทั้งสิ้น จะมีผลทำให้ยอดรวมของวงเงินที่ลูกค้ามีสิทธิถอนไม่ถูกต้อง

ข้อแนะนำ

ควรปรับปรุงแก้ไขโปรแกรมที่ใช้ออกรายงาน C/A outstanding report โดยไม่นำวงเงินที่ลูกค้ามีสิทธิถอน (Available balance) ที่มีค่าติดลบมาหักออกจากยอดรวมของวงเงินที่ลูกค้ามีสิทธิถอน เพื่อให้รายงานที่กล่าวแสดงยอดรวมของวงเงินที่ลูกค้ามีสิทธิถอนที่ถูกต้อง

(49) ไม่มีการตรวจสอบความถูกต้องของข้อมูล

1) การป้อนข้อมูลอัตราดอกเบี้ยของบัญชีลูกค้า ระบบงานไม่ได้ตรวจสอบอัตราดอกเบี้ย ซึ่งอาจเกินกว่าที่กฎหมายกำหนด หรือต่ำกว่าอัตราดอกเบี้ยตามปกติ เนื่องจากระบบงานกำหนดให้ผู้ปฏิบัติงานป้อนเลขหลังจุดทศนิยม 2 ตำแหน่ง โดยไม่ต้องป้อนจุดทศนิยม จึงมีการป้อนข้อมูลอัตราดอกเบี้ยผิดพลาด

ข้อแนะนำ

ควรปรับปรุงระบบงานให้ตรวจสอบอัตราดอกเบี้ยที่ป้อนเข้าเครื่องว่าอยู่ในช่วงที่เหมาะสมหรือไม่

2) การป้อนข้อมูล Expiry date ระบบงานใหม่ได้ตรวจสอบว่า Expiry date นั้นเป็นวันที่ก่อน System date หรือไม่ ในกรณีที่พลั้งเผลอป้อน Expiry date เป็นวันที่ก่อน System date จะมีผลทำให้คำนวณดอกเบี้ยโดยใช้ Standard rate ซึ่งเป็นอัตราดอกเบี้ยสูงสุดในขณะนั้น และลูกค้าต้องจ่ายดอกเบี้ยมากกว่าอัตราดอกเบี้ยที่กำหนดตามสัญญาเงินเบิกเกินบัญชี

ข้อแนะนำ

ควรมีการตรวจสอบ Expiry date ให้เป็นวันที่หลังจาก System date

3) การป้อนข้อมูล Over limit 4 คือ กรณีที่จะให้เงินเบิกเกินวงเงินที่มีอยู่นั้นใช้อัตราดอกเบี้ยเท่ากับอัตราสูงสุดในขณะนั้น (หรือ Standard rate) สาขาไม่จำเป็นต้องป้อนอัตราดอกเบี้ยไว้ใน Over limit 4 แต่จากการตรวจสอบรายงานพบว่าได้มีการป้อน Over limit 4 เท่ากับร้อยละ 15 ต่อปี ไว้หลายบัญชี ซึ่งถ้ามีการประกาศเปลี่ยนแปลงอัตราดอกเบี้ยสูงสุด อัตราดอกเบี้ยที่ใช้คำนวณดอกเบี้ยจะคลาดเคลื่อนไปจากความเป็นจริง

ข้อแนะนำ

ไม่ควรป้อนอัตราดอกเบี้ยของ Over limit 4 ในกรณีที่ต้องการใช้อัตราดอกเบี้ยสูงสุด (Standard rate) กับลูกค้ารายนั้น

4) การป้อนวงเงินระบบงานไม่ได้ตรวจสอบว่าการป้อนวงเงินนั้น อัตราดอกเบี้ยจะต้องเรียงลำดับจากต่ำไปสูง ซึ่งหากมีการป้อนวงเงินแรกด้วยอัตราดอกเบี้ยสูงกว่าวงเงินที่สอง ระบบงานก็จะคำนวณดอกเบี้ยโดยใช้อัตราดอกเบี้ยจากวงเงินแรกเรียงตามลำดับ อันอาจจะทำให้ลูกค้าต้องจ่ายดอกเบี้ยสูงกว่าความเป็นจริง

ข้อแนะนำ

ควรมีข้อความ (Message) เตือนให้ทราบว่า วงเงินที่ป้อนเข้าระบบงานนั้นไม่ได้เรียงวงเงินจากอัตราดอกเบี้ยต่ำไปหาสูง

(50) จุดอ่อนของ Check Digit

วิธีการคำนวณ Check Digit เลขที่บัญชีแบบที่องค์กรใช้มีข้อยกเว้นว่า ถ้าบัญชีใดมีเศษเป็น 1 Check Digit บัญชีนั้นจะเท่ากับ 0 ซึ่งก็จะเท่ากับบัญชีที่มีเศษ 0 ผลก็คือ ทำให้มีกลุ่มเลขที่บัญชีที่มี Check Digit 0 เหมือนกันเกินสมควร และเป็นเหตุให้การป้องกันการฝาก-ถอนผิดบัญชีอันเนื่องมาจากการให้หรือ Key เลขบัญชีผิดโดยมิได้ตั้งใจไม่มีประสิทธิภาพเท่าที่ควร

(51) การปฏิบัติเกี่ยวกับการบันทึกรายการตัดบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามด้วยเช็คของลูกค้าที่ธนาคารอื่นส่งมาเรียกเก็บไม่เหมาะสม

เช็คของลูกค้าบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามหรือเงินเบิกเกินบัญชีที่ธนาคารอื่นส่งมาเรียกเก็บ องค์กรจะบันทึกการตัดบัญชีทันทีโดยไม่ตรวจสอบยอดคงเหลือในบัญชีของลูกค้าก่อน หากผู้บริหารไม่อนุมัติให้ตัดบัญชี องค์กรจะคืนเช็คและบันทึกรายการแก้ไขย้อนหลังในวันรุ่งขึ้น

ข้อแนะนำ

องค์กรควรบันทึกการแก้ไขรายการตัดบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและเงินเบิกเกินบัญชีด้วยเช็คที่ธนาคารอื่นส่งมาเรียกเก็บ ซึ่งไม่ได้รับการอนุมัติตัดบัญชีให้เสร็จสิ้นภายในวันเดียวกัน

(๕๒) **การคำนวณดอกเบี้ยที่มีรายการเช็คคืนหลังวันผ่านดอกเบี้ยประจำเดือนของเงินเบิกเกินบัญชีไม่ถูกต้อง**

จากการทดสอบด้วยข้อมูลทดสอบ โดยใช้บัญชีเงินเบิกเกินบัญชี มีวงเงิน 2 วงเงิน วงเงินแรก 200,000 บาท อัตราดอกเบี้ยร้อยละ 15 ต่อปี วงเงินที่สอง 100,000 บาท อัตราดอกเบี้ยร้อยละ 14.5 ต่อปี จากการทดสอบ ยอดคงเหลือของบัญชีนี้เป็นยอดตัวแดง ณ วันที่ 28 สิงหาคม 2538 จำนวน 300,000 บาท และในวันที่ 22 พฤศจิกายน 2538 มีรายการฝากด้วยเช็คเคลียริ่ง 2 ฉบับ จำนวนเงินฉบับละ 350,000 บาท ทำให้ยอดคงเหลือของบัญชีดังกล่าวมียอดเป็นตัวดำ จำนวน 400,000 บาท หากวันที่ 22 พฤศจิกายน 2538 เป็นวันศุกร์ตามกำหนดของทางการองค์กรจะต้องทำการคำนวณดอกเบี้ยถึงวันที่ 24 พฤศจิกายน 2538 จึงมีการผ่านรายการดอกเบี้ยในเย็นวันที่ 22 พฤศจิกายน 2538 โดยผ่านดอกเบี้ยให้บัญชีนี้จำนวน 10,000.00 บาท

ในวันที่ 25 พฤศจิกายน 2538 ได้กำหนดให้ข้อมูลทดสอบเช็คเคลียริ่ง 2 ฉบับที่กล่าวข้างต้นเป็นเช็คคืน โปรแกรมได้ทำการปรับยอดดอกเบี้ยเป็นจำนวน 400.00 บาท ซึ่งสูงกว่ายอดที่ถูกต้องจำนวน 16.00 บาท เพราะโปรแกรมได้คำนวณดอกเบี้ยของยอดดอกเบี้ยที่ผ่านรายการในวันที่ 22 พฤศจิกายน 2538 ด้วย ซึ่งอาจเป็นการปฏิบัติไม่ชอบด้วยกฎข้อบังคับของทางการได้

(๕๓) **การล้างข้อมูลซึ่งใช้ในการควบคุมการผ่านบัญชีที่เกี่ยวกับเลขที่เช็คของลูกค้าเงินฝาก ที่ต้องจ่ายคืนเมื่อทวงถามและเงินเบิกเกินบัญชีโปรแกรมทำงานไม่ถูกต้อง**

จากการทดสอบให้มีการล้างข้อมูลเกี่ยวกับเลขที่เช็ค (Purge Log Cheque) ที่องค์กรได้ผ่านรายการตามคำสั่งของลูกค้าหมดทั้งช่วงจำนวน 20 ฉบับ ของบัญชีที่ใช้ในการทดสอบบัญชีหนึ่ง ปรากฏว่าโปรแกรมดังกล่าวได้ทำการล้างเลขที่เช็คที่อยู่ในแฟ้มข้อมูลทั้งหมด นอกจากนี้โปรแกรมระบบงานไม่ได้พิมพ์รายละเอียดข้อมูลของเลขที่เช็คที่ถูกล้างทิ้งทั้งหมดออกมา แต่มีการพิมพ์ในลักษณะของยอดรวม

(๕๔) **โปรแกรมระบบงานป้องกันการผ่านรหัสรายการ (Transaction Code) การแก้ไขไม่สมบูรณ์**

จากการทดสอบการผ่านรายการด้วยรหัสรายการแก้ไขรายเช็คเคลียริ่ง (ECL) โดยไม่ต้องผ่านรายการเช็คเคลียริ่งก่อน ปรากฏว่าโปรแกรมระบบงานไม่ตรวจสอบให้ ทำให้รายการแก้ไขดังกล่าวผ่านเข้าระบบได้

(๕๕) **เช็คใบเดียวสามารถผ่านบัญชีของลูกค้าได้ ๒ ครั้ง**

จากการทดสอบการปิดบัญชีโดยใช้บัญชีทดสอบ ผ่านรายการปิดบัญชีด้วยเช็คเลขที่ 55500 ต่อมาทำการเปิดบัญชีใหม่ด้วยการ Maintenance Naste File แล้วใช้เช็คเลขที่ 55500 ผ่านรายการเพื่อถอนปิดบัญชีอีกครั้งหนึ่ง ปรากฏว่าสามารถผ่านรายการได้ โปรแกรมระบบงานไม่ทำการตรวจสอบให้

หมายเหตุ : ข้อใดที่ไม่มีข้อแนะนำ ขอให้เข้าใจด้วยว่าข้อมูลชัดเจนพอสมควรและธนาคารยอมรับข้อบกพร่องดังกล่าวและได้มีการแก้ไขตามคำแนะนำของผู้ตรวจสอบแล้ว

(56) โปรแกรมผ่านรายการเงินเบิกเกินบัญชีชั่วคราวทำงานไม่ถูกต้อง

จากการทดสอบรายการการให้บัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามเบิกเงินเกินบัญชีชั่วคราวตามอำนาจพนักงานระดับบริหารของสาขา ปรากฏว่าไม่สามารถผ่านรายการได้ เนื่องจาก flag 'y' และพนักงานด้านคอมพิวเตอร์ชี้แจงว่า มีการแก้ไขโปรแกรมนี้บางส่วน ซึ่งไม่ทราบมาก่อนว่าจะมีปัญหาเมื่อนำโปรแกรมที่แก้ไขใหม่มาใช้งาน

(57) วงเงินเบิกเกินบัญชีที่ครบกำหนดสัญญายังสามารถถอนได้

จากการทดสอบพบว่า โปรแกรมระบบงานไม่ป้องกันการใช้วงเงินเบิกเกินบัญชีที่ครบกำหนดสัญญาให้ เป็นผลให้ผู้บริหารสาขาสามารถให้สินเชื่อต่อไปได้โดยไม่ต้องขออนุมัติจากสำนักงานใหญ่

ข้อแนะนำ

องค์กรควรกำหนดระเบียบในการต่ออายุสัญญาก่อนสัญญาครบกำหนดหรือให้มีการออกรายงานบัญชีที่มีวงเงินครบกำหนดให้

(58) การยกเลิกวงเงินเบิกเกินบัญชีจากสาขาที่ไม่ใช่เจ้าของบัญชี

จากการทดสอบพบว่า สามารถทำรายการเพื่อยกเลิกรายการอนุมัติวงเงินเบิกเกินบัญชี และยกเลิกรายการอนุมัติเงินเบิกเกินบัญชีชั่วคราวต่างสาขาได้ ซึ่งการปฏิบัติดังกล่าวอาจเกิดปัญหากรณีที่ทำรายการผิดพลาดและจะมีผลเปลี่ยนแปลงสถานะทางบัญชีของลูกค้าสาขาเจ้าของบัญชี

ข้อแนะนำ

องค์กรไม่ควรให้ทำรหัสรายการ เพื่อยกเลิกรายการอนุมัติวงเงินเบิกเกินบัญชีและรายการอนุมัติเงินเบิกเกินบัญชีชั่วคราวต่างสาขาได้ หรือหากจำเป็นต้องทำก็ควรให้มีหลักฐานการทำรายการดังกล่าวปรากฏในรายงาน

(59) การป้อนวงเงินเบิกเกินบัญชีของกลุ่มลูกค้า เกินวงเงินที่ได้รับอนุมัติ

องค์กรอนุมัติวงเงินเบิกเกินบัญชีให้กับกลุ่มลูกค้า 4 ราย ในวงเงินรวม 50.0 ล้านบาท แต่จากวิธีการปฏิบัติงานองค์กรได้ทำรายการป้อนวงเงินให้กับกลุ่มลูกค้าทั้ง 4 รายเป็นรายละ 50.0 ล้านบาท รวมเป็นวงเงิน รวมทั้งสิ้น 200.0 ล้านบาท

(60) การควบคุมติดตามการต่ออายุวงเงินเบิกเกินบัญชี

องค์กรยังคงควบคุมติดตามการต่ออายุวงเงินเบิกเกินบัญชี โดยใช้การ์ดคุมรายตัวในระบบเดิมไม่ได้ใช้ประโยชน์จากคอมพิวเตอร์ช่วย เนื่องจากองค์กรไม่ได้กำหนดให้มีการป้อนวันที่ครบกำหนดวงเงินเบิกเกินบัญชี (Expiry date) เข้าสู่ระบบคอมพิวเตอร์ด้วย ซึ่งในบางครั้งการควบคุมติดตามการต่ออายุวงเงินเบิกเกินบัญชีทำได้ไม่ทันเวลา

ข้อแนะนำ

ควรกำหนดให้มีการป้อนวันครบกำหนด (Expiry date) ของเงินเบิกเกินบัญชีทุกวงเงิน เพื่อให้คอมพิวเตอร์ออกรายงานวงเงินเบิกเกินบัญชีที่ใกล้จะครบกำหนดสัญญา เพื่อประโยชน์ในการควบคุมติดตามต่อสัญญาเงินเบิกเกินบัญชี

(61) ส่วนบริหารสินเชื่อไม่มีการสอบทานความถูกต้องในการป้อนวงเงินเบิกเกินบัญชี

ส่วนบริหารสินเชื่อที่เป็นผู้อนุมัติวงเงินตั้งแต่เริ่มแรก ไม่ได้รับรายงาน OD limit amendment เพื่อการสอบทานความถูกต้องในการบันทึกวงเงินเบิกเกินบัญชีไว้ในระบบคอมพิวเตอร์อีกครั้งหนึ่ง ซึ่งอาจทำให้เกิดข้อผิดพลาดและเสียหายได้

ข้อแนะนำ

องค์กรควรจัดส่งรายงานดังกล่าวให้ส่วนบริหารสินเชื่อเพื่อตรวจสอบความถูกต้องอีกครั้งหนึ่ง

(62) การควบคุมใบรับฝากเช็คที่ลูกค้าฝากไม่ทันส่งไปเรียกเก็บไม่รัดกุม

เมื่อลูกค้าฝากเงินเข้าบัญชีด้วยเช็คที่ส่งไม่ทันเรียกเก็บในวันนั้น ส่วนเงินฝากกระแสรายวันจะจัดส่ง Pay-in slip พร้อมด้วยเช็คไปเก็บไว้ที่ส่วนหักบัญชี เพื่อรอส่งไปเรียกเก็บในวันทำการถัดไป และจะรับ Pay-in slip กลับมาที่ส่วนเงินฝากกระแสรายวันเพื่อบันทึกรายการเข้าเครื่องในวันรุ่งขึ้น การปฏิบัติดังกล่าวอาจเป็นจุดอ่อน เนื่องจากกรณี Pay-in slip และเช็คหายไปทางส่วนเงินฝากกระแสรายวันจะไม่สามารถควบคุมและมีหลักฐานตรวจสอบได้

ข้อแนะนำ

องค์กรควรมีมาตรการควบคุม โดยอาจแยกเก็บ Pay-in slip กับเช็คที่ส่งไม่ทันเรียกเก็บในวันนั้นออกจากกัน

(63) การปรับปรุงดอกเบี้ยเงินเบิกเกินบัญชีก่อนปิดบัญชียังไม่รัดกุม

การยินยอมให้ผู้ปฏิบัติงานสามารถข้ามขั้นตอนการตรวจสอบยอดดอกเบี้ยค้างรับ (Accrued Interest) เพื่อปรับปรุงดอกเบี้ยที่ต้องเรียกเก็บจากลูกค้าให้ถูกต้องและครบถ้วนได้ ก่อนปิดบัญชีเงินฝากกระแสรายวันหรือเงินเบิกเกินบัญชี อาจมีผลให้ธนาคารเรียกเก็บดอกเบี้ยค้างชำระจากลูกค้าไม่ครบถ้วน

ข้อแนะนำ

องค์กรควรกำหนดระเบียบปฏิบัติ และมีมาตรการควบคุมไม่ให้มีการปิดบัญชีเงินฝากกระแสรายวันหรือเงินเบิกเกินบัญชีได้ ก่อนมีการตรวจสอบยอดดอกเบี้ยค้างรับ

(64) **การควบคุมการทำรายการโอนเงินด้วยเช็คไม่รัดกุม**

การถอนเงินจากบัญชีด้วยรายการเงินโอน ซึ่งต้องป้อนข้อมูลเกี่ยวกับเลขที่เช็ค รหัสการโอน และจำนวนเงินโอนตามข้อกำหนดของรหัสรายการนั้น สามารถป้อนเลขที่เช็คเป็นศูนย์จำนวนหกตัวได้ ซึ่งการปฏิบัติดังกล่าวองค์กรจะใช้ในการโอนเงินระหว่างบัญชีที่องค์กรเป็นผู้ทำรายการเอง ดังนั้น อาจเป็นจุดอ่อนในการควบคุมเช็คผ่านบัญชีโดยเปิดโอกาสให้มีการหลีกเลี่ยงไม่ป้อนเลขที่เช็คในการทำรายการโอนเงินด้วยเช็คได้

ข้อแนะนำ

องค์กรควรกำหนดให้การทำรายการโอนเงินจากบัญชีโดยใช้เช็ค ต้องป้อนข้อมูลเลขที่เช็คทุกครั้ง เพื่อความรัดกุมในการทำรายการโอนเงินด้วยเช็ค และควรแยกรหัสรายการของการโอนเงินด้วยเช็คออกจากรหัสรายการของการโอนเงินระหว่างบัญชีที่องค์กรเป็นผู้ทำรายการเอง

(65) **กำหนดรหัสเงื่อนไขที่ไม่ใช้ไว้ในระบบ**

Misc. Code 39 (Verify Book No.) สำหรับบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและบัญชีเงินเบิกเกินบัญชี เป็นการกำหนดรหัสไว้เกินความจำเป็น และอาจทำให้ผู้ปฏิบัติงานเกิดความสับสนได้

ข้อแนะนำ

องค์กรควรพิจารณายกเลิก Misc. Code 39 ซึ่งไม่เกี่ยวข้องกับการทำรายการบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและบัญชีเงินเบิกเกินบัญชี เพื่อไม่ให้เกิดความสับสน เนื่องจากบัญชีประเภทนี้ไม่ต้องใช้สมุดคู่ฝากในการฝากถอน

(66) **คู่มือปฏิบัติงานสำหรับเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามไม่เป็นปัจจุบัน**

ข้อแนะนำ

คู่มือปฏิบัติงานเป็นเอกสารอ้างอิงที่สำคัญในการดำเนินงานขององค์กร จึงควรจัดทำให้ถูกต้อง ชัดเจน และเป็นปัจจุบัน เพื่อให้สามารถใช้ประโยชน์ได้อย่างแท้จริง

(67) **ไม่มีการลบล้างเลขที่เช็คที่ลูกค้าใช้หมดแล้วเป็นครั้งคราว**

องค์กรไม่มีการลบล้างเลขที่เช็คที่ลูกค้าใช้หมดแล้วเป็นครั้งคราว ทำให้สิ้นเปลืองเนื้อที่ในการจัดเก็บข้อมูลที่ไม่มีความจำเป็นเหล่านี้ไว้ ซึ่งอาจมีผลให้องค์กรต้องเพิ่มเนื้อที่ในการจัดเก็บข้อมูลในอนาคตได้

ข้อแนะนำ

ควรกำหนดให้มีการลบล้างเลขที่เช็ค (Log cheque) ที่ลูกค้าใช้หมดแล้วออกจากแฟ้มข้อมูลเป็นครั้งคราว เพื่อลดความสิ้นเปลืองเนื้อที่ในแฟ้มข้อมูล

(68) หลักฐานการเปิดบัญชีไม่ครบถ้วน

จากการตรวจสอบแฟ้มใบคำขอเปิดบัญชีพบว่า บางบัญชีมีหลักฐานในการเปิดบัญชีไม่ครบถ้วน

ข้อแนะนำ

องค์กรควรติดตามดูแลเอกสารหลักฐานที่ต้องใช้ในการเปิดบัญชีให้ครบถ้วน

(69) ไม่มีการเก็บแบบฟอร์มบันทึกข้อมูลที่ได้จากระบบคอมพิวเตอร์ (Cut form) ไว้เป็นหลักฐานการปฏิบัติงาน

ข้อแนะนำ

องค์กรควรกำหนดให้มีการเก็บเอกสารหลักฐานต่าง ๆ อย่างครบถ้วนเพื่อประโยชน์ในการปฏิบัติงานและการตรวจสอบต่อไป

2.2.2 เงินฝากออมทรัพย์

(1) การปรับปรุงวันที่คำนวณดอกเบี้ยได้เกินกว่างวดหกเดือน

องค์กรไม่มีการป้องกันข้อผิดพลาดในการเปลี่ยนแปลงวันที่คำนวณดอกเบี้ยครั้งหลังสุดซึ่งระบบงานเปิดโอกาสให้พนักงานแก้ไขย้อนหลังได้เกินกว่าหกเดือน ซึ่งเกินกว่างวดการผ่านดอกเบี้ยครั้งหลังสุดขององค์กร ซึ่งไม่สอดคล้องกับความเป็นจริงที่องค์กรจ่ายดอกเบี้ยทุกระยะเวลาหกเดือนอันอาจเกิดความเสียหายแก่องค์กรได้

ข้อแนะนำ

ควรเพิ่มจุดตรวจสอบในระบบงาน ให้มีการตรวจสอบการปรับปรุงวันที่คำนวณดอกเบี้ยครั้งหลังสุดควรอยู่ในช่วงที่เหมาะสม

(2) การบันทึกชื่อลูกค้าในแฟ้มข้อมูลยังไม่ครบถ้วน

องค์กรไม่ได้บันทึกชื่อลูกค้าไว้ในแฟ้มข้อมูลให้ครบถ้วนทุกราย ซึ่งจะมีผลทำให้การนำเงินฝากเข้าบัญชีให้ลูกค้าโดยไม่มีสมุดคู่ฝากผิดบัญชีได้ หากลูกค้าแจ้งเลขที่บัญชีไม่ถูกต้อง และไม่มีชื่อบัญชีลูกค้าให้ตรวจสอบความถูกต้องก่อนทำรายการรับฝาก

ข้อแนะนำ

องค์กรควรจะดำเนินการกำชับให้พนักงานทำการป้อนชื่อลูกค้าในแฟ้มข้อมูลให้ครบถ้วน

(3) การทำรายการปลดวงเงินค้ำประกันไม่รัดกุม

การทำรายการปลดวงเงินค้ำประกัน มีผลทำให้วงเงินที่ถูกอายัดปลอดภาระ ในกรณีที่ผู้ปฏิบัติงานใส่รหัสการค้ำประกันผิด ก็จะมีผลทำให้ข้อมูลเกี่ยวกับรหัสการค้ำประกันยังคงค้างอยู่ในบัญชีทั้ง ๆ ที่ได้ปลดภาระค้ำประกันหมดแล้ว ซึ่งไม่ถูกต้อง อาจทำให้ผู้ใช้ข้อมูลเข้าใจผิดได้เนื่องจากบัญชีนี้ไม่ได้มีภาระของหนี้สินอยู่แล้ว

ข้อแนะนำ

ควรแก้ไขระบบงานให้ตรวจสอบรหัสการค้ำประกัน ตอนปลดภาระค้ำประกันให้ตรงกับรหัสตอนทำรายการกันวงเงินค้ำประกัน

(4) การถอนเงินต่างสาขาไม่บันทึกหมายเลขสมุดคู่ฝากไว้ในใบถอน

การถอนเงินต่างสาขาไม่มีการบันทึกหมายเลขสมุดคู่ฝากไว้ในสลิปสำหรับลูกค้าบางรายไว้เป็นหลักฐาน ทำให้ขาดร่องรอยในการติดตามตรวจสอบภายหลัง

ข้อแนะนำ

องค์กรควรจะรีบดำเนินการติดตามให้มีการบันทึกหมายเลขสมุดคู่ฝากในสลิปถอนเงินต่างสาขาให้ครบถ้วนต่อไป

(5) ระบบงานไม่สอดคล้องกับระเบียบปฏิบัติ

การอนุมัติผ่านเซ็คอเรียกเก็บ ตามระเบียบกำหนดให้ระดับผู้จัดการส่วนขึ้นไป ซึ่งเป็นผู้ถือบัตรอนุมัติรายการระดับ 7 ขึ้นไปเป็นผู้อนุมัติรายการ แต่จากการทดสอบข้อมูลปรากฏว่า ระบบงานต้องการบัตรอนุมัติรายการระดับ 2 เท่านั้น

การเรียกดูข้อมูลลูกค้า ตามระเบียบกำหนดให้ระดับหัวหน้าหน่วยขึ้นไป ซึ่งเป็นผู้ถือบัตรอนุมัติรายการระดับ 5 ขึ้นไปเป็นผู้อนุมัติรายการ แต่จากการทดสอบข้อมูลปรากฏว่าระบบงานต้องการบัตรอนุมัติรายการระดับ 3 เท่านั้น

การแก้ไขรายการกรณีบันทึกรายการผิด ตามระเบียบกำหนดให้ระดับผู้จัดการส่วนขึ้นไป ซึ่งเป็นผู้ถือบัตรอนุมัติรายการระดับ 7 ขึ้นไปเป็นผู้อนุมัติรายการ แต่จากการทดสอบข้อมูลปรากฏว่าระบบงานต้องการบัตรอนุมัติรายการระดับ 5 เท่านั้น

นอกจากนี้ ระดับผู้อนุมัติรายการในการปฏิบัติงานจริง ไม่มีเจ้าหน้าที่ผู้อนุมัติรายการระดับ 2 แต่ตามระบบงานการทำรายการบางประเภทยังคงต้องการบัตรอนุมัติรายการระดับ 2

ข้อแนะนำ

ควรแก้ไขให้ระดับการอนุมัติรายการตามระบบงานและระเบียบปฏิบัติสอดคล้องกัน

(6) ไม่ได้กำหนดวงเงินสูงสุดในการทำรายการโอนฝากเงิน

พนักงาน Teller สามารถทำรายการโอนฝากเงินเข้าบัญชีได้โดยไม่จำกัดจำนวนเงิน และไม่มีพนักงานชั้นบริหารดูแลการปฏิบัติดังกล่าวโดยใกล้ชิด อาจก่อให้เกิดความเสียหายได้ เนื่องจากจำนวนเงินที่โอนเข้าบัญชีสามารถถอนต่างสาขาได้ทันที

ข้อแนะนำ

องค์กรควรกำหนดให้มีการควบคุมรายการโอนฝากเงินเข้าบัญชีจำนวนสูง ๆ เป็นพิเศษ เช่น กำหนดให้เครื่องคอมพิวเตอร์ตรวจสอบรายการฝากเงินจำนวนสูง และกำหนดให้พนักงานผู้ถือบัตร Supervisor เป็นผู้อนุมัติรายการ เป็นต้น

(7) **ไม่มีการปรับปรุงดอกเบี้ยเงินฝากย้อนหลัง**

องค์กรกำหนดให้โปรแกรมระบบงานเงินฝากออมทรัพย์คำนวณดอกเบี้ยสะสมไว้ทุกสิ้นวันและเมื่อมีการแก้ไขรายการย้อนหลังจากวันที่พบข้อผิดพลาด ซึ่งอาจเกิดจากการบันทึกบัญชีเงินฝากของลูกค้าผิดรายหรือคอมพิวเตอร์ขัดข้อง หรือกรณีอื่นใดก็ตาม จะไม่มีการปรับปรุงแก้ไขดอกเบี้ยที่โปรแกรมคำนวณสะสมจากรายการที่ผิดพลาดย้อนหลังด้วย ทำให้การคำนวณดอกเบี้ยเงินฝากออมทรัพย์ไม่ถูกต้องตามความเป็นจริง โดยลูกค้ารายใดรายหนึ่งอาจได้รับและเสียประโยชน์จากดอกเบี้ยเงินฝากนั้นได้

ข้อแนะนำ

ควรปรับปรุงแก้ไขดอกเบี้ยเงินฝากย้อนหลังทุกครั้งที่มีการแก้ไขรายการฝากและถอนเงินข้ามวัน

(8) **ไม่มีการควบคุมการปรับปรุงดอกเบี้ยด้วยมือ**

พนักงาน Teller สามารถปรับปรุงดอกเบี้ยค้างจ่ายด้วยมือได้ถึง 999 ล้านบาท หากมีข้อผิดพลาดในการปรับปรุงดอกเบี้ยดังกล่าว จะทำให้องค์กรได้รับความเสียหาย

ข้อแนะนำ

องค์กรควรกำหนดวงเงินสูงสุดในการทำรายการปรับปรุงดอกเบี้ย เพื่อสามารถติดตามรายการได้และกำหนดมาตรการในการดูแลการทำรายการดังกล่าวโดยใกล้ชิด เพื่อลดความเสียหายจากการปฏิบัติงานผิดพลาด

(9) **การแก้ไขเปลี่ยนแปลงอัตราดอกเบี้ยไม่รัดกุม**

โปรแกรมระบบงานมิได้ตรวจสอบข้อมูลเกี่ยวกับวันที่ที่มีผลบังคับใช้ (Effective Date) ในกรณีที่มีการเปลี่ยนแปลงอัตราดอกเบี้ยใหม่ โดยป้อนวันที่ที่มีผลบังคับใช้ย้อนหลังได้ ทำให้การคำนวณดอกเบี้ยค้างจ่ายของทุกบัญชีมากไป อาจก่อให้เกิดความเสียหายต่อองค์กรได้

ข้อแนะนำ

องค์กรควรป้องกันไม่ให้มีการป้อนวันที่ที่มีผลบังคับใช้ (Effective Date) ย้อนหลังได้ ในกรณีที่มีการเปลี่ยนแปลงอัตราดอกเบี้ยใหม่ เพื่อให้การคำนวณดอกเบี้ยถูกต้อง

(10) **การควบคุมการทำรายการถอนย้อนวันที่เกินวันที่เปิดบัญชี**

ไม่มีการป้องกันข้อผิดพลาดในกรณีที่ผู้ปฏิบัติงานทำรายการถอนย้อนวันที่ก่อนวันเปิดบัญชีทำให้ดอกเบี้ยค้างจ่ายมีค่าเป็นลบ และอาจทำให้ลูกค้าเสียหายได้ เพราะได้รับดอกเบี้ยน้อยกว่าที่ควรจะเป็น

ข้อแนะนำ

องค์กรควรแก้ไขโปรแกรมระบบงานให้มีการตรวจสอบการทำรายการถอนย้อนวันที่มิให้กำหนด Value Date ย้อนหลังเกินกว่าวันที่เปิดบัญชีได้ เพื่อให้การคำนวณดอกเบี้ยจ่ายถูกต้อง

(11) การยกเลิกการเปิดบัญชีที่มีรายการเคลื่อนไหวแล้ว

พนักงาน Teller สามารถยกเลิก (Correct) รายการเปิดบัญชีหลังจากที่มีการเคลื่อนไหวบัญชีแล้วในวันเปิดบัญชี ทำให้รายการที่เกิดขึ้นทั้งหมดในวันนั้นไม่ปรากฏในรายงาน Daily Transaction of Saving A/C ซึ่งเป็นจุดอ่อนในการควบคุมภายใน เนื่องจากรายการที่กล่าวไม่ปรากฏร่องรอยให้ติดตามตรวจสอบได้

ข้อแนะนำ

องค์กรควรป้องกันไม่ให้มีการทำรายการแก้ไขรายการเปิดบัญชีหากมีรายการเคลื่อนไหวในวันนั้นแล้ว เพราะจะทำให้รายการทั้งหมดหายไป ซึ่งยากแก่การติดตามการทำรายการ

(12) การพิมพ์ทับรายการเดิมซึ่งเคยพิมพ์แล้วในสมุดคู่ฝาก

องค์กรเปิดโอกาสให้ผู้ปฏิบัติงานเปลี่ยนบรรทัดที่ใช้พิมพ์รายการฝากถอนของลูกค้าได้ตามความเหมาะสม หากผู้ปฏิบัติงานเปลี่ยนบรรทัดที่ใช้พิมพ์เป็นบรรทัดที่เคยพิมพ์รายการฝากถอนไปแล้วมีผลทำให้เครื่องพิมพ์สมุดคู่ฝาก พิมพ์ข้อมูลใหม่ทับรายการฝากถอนเดิม ซึ่งทำให้ถูกเข้าใจผิดได้

ข้อแนะนำ

การทำรายการเปลี่ยนแปลงบรรทัดที่พิมพ์ในสมุดคู่ฝาก ไม่ควรให้มีการเปลี่ยนแปลงเป็นบรรทัดที่เคยพิมพ์ไปแล้วได้

(13) การกำหนดรหัสรายการตัดบัญชีด้วยเช็คเคลียริ่ง

มีการกำหนดรหัสรายการ Sav CG no book ไว้ในระบบงาน เพื่อใช้ตัดบัญชีเงินฝากของลูกค้าด้วยเช็คเคลียริ่งโดยไม่ต้องใช้สมุดคู่ฝาก เป็นการกำหนดรหัสรายการที่ไม่สอดคล้องกับลักษณะบัญชีเงินฝากออมทรัพย์และไม่มีคำอธิบายรายการดังกล่าวใน User Manual ให้ชัดเจน ซึ่งรหัสรายการนี้จะใช้ในกรณีที่ลูกค้ามีหนังสือยินยอมให้องค์กรสามารถหักบัญชีเงินฝากออมทรัพย์ของลูกค้าได้ ถ้าเช็คมาตัดบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม โดยระบุชัดเจนถึงจำนวนเงินที่โอนจากบัญชีออมทรัพย์เข้าบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม และเมื่อหักบัญชีแล้วจะมีใบแจ้งให้ลูกค้าทราบทุกวัน

(14) โปรแกรมระบบงานไม่ตรวจสอบความถูกต้องในการทำรายการ

1) โปรแกรมไม่ตรวจสอบความสมเหตุสมผลของการทำรหัสรายการ Sav. Set Misc. Code จากการทดสอบการทำรายการปรากฏว่า สามารถกำหนด Misc. Code หมายเลข 38 (Inactive Account for a Period) ให้กับบัญชีที่เปิดใหม่และมีรายการเคลื่อนไหวในวันนั้นมีผลให้บัญชีที่เปิดใหม่นี้กลายเป็นบัญชีที่ไม่เคลื่อนไหวเกิน 6 เดือน หรือ 1 ปี ซึ่งไม่ถูกต้อง

2) จากคู่มือการปฏิบัติงาน ไม่มี Misc. Code 35 และ 36 แต่ในระบบงานสามารถกำหนดรหัสนี้ในการทำรายการได้ และมีผลให้เปลี่ยนสถานะเป็นบัญชีที่ไม่เคลื่อนไหว

3) การทำรายการ Departmental Hold เพื่ออายัดเงินฝาก โปรแกรมไม่ตรวจสอบเลขที่บัญชีที่นำเงินฝากไปค้ำประกัน (H-Acct.) ว่าเป็นบัญชีประเภทใด จากการทดสอบสามารถอายัดเงินฝากเพื่อค้ำประกันบัญชีออมทรัพย์หรือบัญชีฝากประจำได้ และเมื่อทำรายการ 2570 (Release Departmental Hold) เพื่อถอนการอายัด พบว่าโปรแกรมไม่ตรวจสอบเลขที่บัญชีที่นำเงินฝากไปค้ำประกัน (H-Acct.) ว่าเป็นบัญชีเดียวกับที่ป้อนเข้าไปครั้งแรกเมื่อทำการอายัด

(15) ไม่มีการควบคุมการผ่านรายการ

พนักงาน Teller สามารถทำรหัสรายการต่อไปนี้ได้โดยไม่ต้องใช้บัตรอนุมัติรายการ และลูกค้ามีสิทธิถอนเงินได้ทันที ซึ่งหากมีข้อผิดพลาดในการทำรายการ องค์กรอาจได้รับความเสียหายได้ รหัสรายการดังกล่าวได้แก่

2820	BB		(Bill Bought)
2822	BB	NB	(Bill Bought No Book)
2830	CC		(Collection Cheque)
2832	CC	NB	(Collection Cheque No Book)
2850	DD		(Demand Draft)
2852	DD	NB	(Demand Draft No Book)
2862	HC	NB	(Housing Cheque No Book)
2870	IND		(Interest Deposit)
2872	IND	NB	(Interest Deposit No Book)
2900	TRD		(Transfer Deposit)
2902	TRD	NB	(Transfer Deposit No Book)
2910	TT		(Telegram Transfer)
2912	TT	NB	(Telegram Transfer No Book)

ข้อแนะนำ

การทำรายการรับ-จ่ายเกินอำนาจของพนักงาน Teller ควรจะต้องมอบให้พนักงานผู้รับมอบอำนาจตั้งแต่ผู้ช่วยสมุหบัญชีขึ้นไป รับผิดชอบเซ็นชื่อในสลิปและทำรายการตรวจสอบสลิปทุกฉบับเมื่อสิ้นวัน ตามคำสั่งของสำนักงานใหญ่

(16) การปิดบัญชีโดยไม่พิมพ์รายการใน Journal Tape

จากการทดสอบการปิดบัญชีเงินฝากออมทรัพย์ด้วยการทำรายการ Cash Withdrawal และรายการ Sav. Closed A/C เท่านั้น โดยไม่ทำรายการ Int. Deposit ปรากฏว่าใน Journal Tape ไม่มีหลักฐานการทำรายการ Cash Withdrawal และ Sav. Closed A/C ซึ่งทำให้ขาดหลักฐานในการตรวจสอบการทำรายการภายหลัง

ข้อแนะนำ

(1) ควรอธิบายรหัสรายการดังกล่าวในคู่มือการปฏิบัติงาน (User Manual) ให้ชัดเจนเพื่อป้องกันการเข้าใจผิดหรือนำไปใช้ผิดวัตถุประสงค์

(2) ควรมีการตรวจสอบความเป็นไปได้และความสมเหตุสมผลของข้อมูลในการทำรายการแต่ละประเภท เพื่อป้องกันข้อผิดพลาดที่อาจเกิดขึ้น

(3) ควรให้ใช้บัตรอนุมัติรายการในการทำรหัสรายการดังกล่าว โดยเฉพาะรายการที่มีจำนวนเงินสูง ๆ

(4) ใน Journal Tape ควรมีหลักฐานการทำรายการทุกรายการ เพื่อให้สามารถติดตามและตรวจสอบการทำรายการได้

(17) การควบคุมการทำรายการเช็คคืนไม่รัดกุม

การทำรายการเช็คคืน ไม่มีการจัดทำเอกสารหลักฐานที่แสดงว่าทำรายการเช็คคืนถูกต้องและครบถ้วนเพียงใด

ข้อแนะนำ

องค์กรควรชี้แจงให้ผู้ปฏิบัติงานทราบ และได้จัดทำรายละเอียดใน User Manual แล้ว

(18) ไม่มีการป้องกันข้อผิดพลาดในการทำรายการรับฝาก Late Check

รหัสรายการ 180 ที่ใช้ในกรณีลูกค้าฝากเช็คเคลียริ่งไม่ทันเวลาส่งเช็คไปเรียกเก็บเงิน ฝ่ายสำนักหักบัญชี (Late Check) ซึ่งเปิดโอกาสให้ใช้รหัสรายการนี้ได้ตลอดเวลานั้น หากพนักงานเทลเลอร์เกิดความสับสนใช้รหัสรายการดังกล่าวในตอนเช้าก่อนเวลา 11.00 น. จะมีผลทำให้เช็คฉบับนั้นมีสถานะเหมือนเช็คเคลียริ่งที่ลูกค้านำมาฝากในตอนบ่าย (Unclear Check) ซึ่งไม่ถูกต้อง และลูกค้าจะมีปัญหาในการถอนเงินในวันรุ่งขึ้น เพราะในเวลา 11.00 น. ของวันรุ่งขึ้น โปรแกรม Clearing Check 11 AM Process จะไม่เพิกถอนการอายัดเงินฝากตามเช็คฉบับนี้ แม้จะเรียกเก็บเงินตามเช็คได้แล้วก็ตาม

ข้อแนะนำ

องค์กรควรดำเนินการแก้ไขให้ถูกต้อง

(19) **มีจุดอ่อนในการอายัดเงินฝาก (Blocking) เป็นประกัน**

ระบบเปิดโอกาสให้ผู้ปฏิบัติงานสามารถอายัดเงินฝากได้มากกว่ายอดเงินฝากคงเหลืออยู่ในบัญชี ซึ่งเป็นการยินยอมให้อายัดเงินฝากได้ล่วงหน้านั้น อาจทำให้องค์กรได้รับความเสียหายได้ หากผู้ปฏิบัติงานหลีกเลี่ยงการควบคุมโดยทำรายการอายัดเงินฝากหลังจากที่ได้ทำรายการลดยอดเงินฝากให้ลูกค้าแล้ว ซึ่งจะมีผลทำให้จำนวนเงินที่อายัดลดน้อยลง ซึ่งอาจไม่เพียงพอที่จะรองรับความเสียหายหรือคุ้มภัยในส่วนที่ใช้เงินฝากเป็นประกันได้

(20) **การยินยอมให้ถอนเงินก่อนที่จะทราบผลการเรียกเก็บเงินตามเช็ค**

ข้อแนะนำ

องค์กรควรดำเนินการแก้ไขระเบียบปฏิบัติให้สอดคล้องกับการปฏิบัติงาน โดยไม่ก่อให้เกิดปัญหากับองค์กร

(21) **การหักภาษีดอกเบี้ยเงินฝาก ณ ที่จ่าย ไม่ถูกต้อง**

การหักภาษีดอกเบี้ยเงินฝาก ณ ที่จ่าย ของบัญชีเงินฝากออมทรัพย์ ลูกค้าประเภทสถาบันที่ไม่มีวัตถุประสงค์เพื่อหากำไรไม่ได้คำนวณภาษีหัก ณ ที่จ่ายไว้

ข้อแนะนำ

องค์กรควรดำเนินการแก้ไขให้ถูกต้อง

(22) **การแสดงข้อความเตือนเมื่อมีการป้อนรายการผิดพลาด ไม่สอดคล้องกับความเป็นจริง**

ข้อความเตือนที่ปรากฏหน้าจอเทอร์มินอลเมื่อมีการป้อนรายการผิดพลาด ให้ความหมายไม่ตรงกับประเภทของข้อผิดพลาดที่แท้จริง เช่น กรณีพนักงานป้อน CHECK DIGIT ผิดหรือ BRANCH CODE ไม่ถูกต้อง เมื่อเปิดบัญชีใหม่ (OPEN NEW A/C) จะมีข้อความ "A/C NO. NOT FOUND" เหมือนกัน ทั้งสองกรณี เป็นต้น

ข้อแนะนำ

องค์กรควรดำเนินการแก้ไขข้อความเตือนให้สอดคล้องกับสถานการณ์ในแต่ละกรณี

(23) **การโอนบัญชีไม่เคลื่อนไหว (INACTIVE) เข้าบัญชีกำไรขาดทุน ไม่ครบถ้วน**

เมื่อโปรแกรมงานได้โอนบัญชีที่ไม่เคลื่อนไหว (INACTIVE) เข้าบัญชีกำไรขาดทุน ปรากฏว่าในรายงานการปิดบัญชีแสดงจำนวนบัญชีปัจจุบันในตอนท้ายรายงานไม่ถูกต้อง คือ ไม่ได้นำบัญชีที่โอนออกไปหักออกจากจำนวนบัญชีที่มีอยู่ในปัจจุบัน

ข้อแนะนำ

องค์กรควรแก้ไขโปรแกรมงานในเรื่องที่กล่าวให้ถูกต้อง

(24) **การกำหนดขั้นตอนในการออกรายงานไม่รัดกุม**

การกำหนดขั้นตอนการออกรายงาน ณ สิ้นวัน ยังไม่เหมาะสมเท่าที่ควร ทำให้ข้อมูลสำหรับการออกรายการขาดหายไปโดยไม่เจตนาได้

ข้อแนะนำ

องค์กรควรดำเนินการแก้ไขให้ถูกต้อง

(25) **ไม่มีการป้องกันข้อผิดพลาดในการ Set up ข้อมูลจากระบบเดิมเข้าสู่ระบบคอมพิวเตอร์เท่าที่ควร**

1) โปรแกรม NAME & CUSTOMER HISTORY SET UP

โปรแกรมนี้สามารถป้อน ACTIVE CODE ด้วยค่า C (A/C CLOSED) ได้ และบัญชีที่มี ACTIVE CODE "C" จะถูกนับรวมอยู่ในจำนวนบัญชีทั้งหมด (จำนวนบัญชียกมา) ในตอนท้ายของรายงานการปิดบัญชีด้วย ทำให้จำนวนบัญชีที่มีอยู่ ณ สิ้นวัน ไม่ถูกต้อง

2) โปรแกรม BALANCE & INTEREST SET UP

2.1) สามารถป้อน ACTIVE DATE โดยใช้ปี พ.ศ. แทนปี ค.ศ. ได้ ซึ่ง ACTIVE DATE นี้คือวันที่เคลื่อนไหวครั้งสุดท้าย ใช้ในการเช็คสอบเพื่อโอนเป็นบัญชีไม่เคลื่อนไหว (INACTIVE) อาจทำให้การโอนบัญชีเงินฝากออมทรัพย์เป็นบัญชีไม่เคลื่อนไหว (INACTIVE) ผิดพลาดได้

2.2) การใส่วันที่ LAST INT DATE ในโปรแกรม BALANCE & INTEREST SET UP สามารถป้อนย้อนวันที่ได้ อาจทำให้ดอกเบี้ยสะสมของบัญชีเคลื่อนไหวหลังจากการ Set up มากเกินความเป็นจริง และไม่มีการพิมพ์ LAST CAL INT DATE ในรายงานยอดคงเหลือและดอกเบี้ยสะสม (CALLO) ทำให้ไม่สามารถเช็คสอบได้ว่ามีการป้อน LAST CAL INT DATE

2.3) การออกรายงานยอดคงเหลือและดอกเบี้ยสะสม (Callo) หลังจากได้ป้อนข้อมูลผ่านโปรแกรม BALANCE & INTEREST SET UP เสร็จแล้ว สามารถกลับไปเรียกใช้โปรแกรม BALANCE & INTERST SET UP ได้อีกเพื่อแก้ไขรายการต่าง ๆ ที่ป้อนเข้าไปครั้งแรก โดยไม่ต้องออกรายงานยอดคงเหลือและดอกเบี้ยสะสมใหม่ ทำให้ข้อมูลจริงใน Master File ของบัญชีเงินฝากออมทรัพย์ที่ Set up ไม่ถูกต้อง การยินยอมให้ผู้ปฏิบัติงานสามารถเลือกไม่ออกรายงานหลังจากป้อนหรือแก้ไขข้อมูลที่ Set up จะทำให้องค์กรไม่มี Audit Trail สำหรับตรวจสอบความถูกต้องของข้อมูล

3) รายงานที่ออกครั้งแรกหลังวันที่การ Set up ข้อมูลจากระบบเก่าเข้าสู่ระบบคอมพิวเตอร์

- รายงานสรุปยอดคงเหลือเรียงตามรหัส Segment

จากข้อมูลทดสอบ (Test Data) ในวันทำการแรกหลังจากการ Set up "ยอดคงเหลือเดิม" ในรายงานแสดงยอดเป็น 0.00 ไม่ได้ยกยอดบัญชีที่ทำการ Set up เข้าไปมาแสดงไว้

- รายงาน MONEY POSITION

จากข้อมูลทดสอบ (Test Data) รายงานดังกล่าวแสดงยอดสำรองดอกเบี้ยจ่าย สะสม เป็น 0.00 แทนที่จะมียอดเท่ากับผลรวมดอกเบี้ยสะสมของบัญชีที่ Set up โดยผ่านโปรแกรม BALANCE & INTEREST SET UP

ข้อแนะนำ

องค์กรควรจะกำชับให้พนักงานเพิ่มความระมัดระวังในการปฏิบัติงาน โดยใส่วันที่ที่ Set up ให้สอดคล้องกับโปรแกรมการทำงานของระบบงานต่อไป

(26) รายงานเงินฝากออมทรัพย์ที่ออกโดยคอมพิวเตอร์ไม่ถูกต้อง

1) STATEMENT

รายงาน STATEMENT ซึ่งพิมพ์โดยโปรแกรม SAVING MONTHLY STATEMENT มีข้อผิดพลาด ดังนี้

1.1) จากการทดสอบพบว่า STATEMENT ของบัญชีที่ไม่มีรายการเคลื่อนไหวในวันที่พิมพ์ STATEMENT จะมีเลขที่บัญชีและชื่อบัญชีไม่ถูกต้อง คือจะนำเอาเลขที่บัญชีและชื่อบัญชีของบัญชีถัดไป (ที่เคลื่อนไหวในวันนั้น) มาพิมพ์ไว้แทน แต่ข้อมูลที่ปรากฏใน STATEMENT (ซึ่งแสดงเฉพาะยอดยกมาและยอดยกไป เนื่องจากบัญชีไม่เคลื่อนไหว) ถูกต้อง

1.2) โปรแกรม SAVING MONTHLY STATEMENT ไม่พิมพ์ STATEMENT รายการเคลื่อนไหวที่มีอยู่ก่อนปิดบัญชีของบัญชีที่ปิดแล้ว

2) รายงานบัญชีที่จะโอนเข้าบัญชีไม่เคลื่อนไหว

ในรายงานดังกล่าวมีรายละเอียดของเลขที่บัญชี ชื่อบัญชี ยอดคงเหลือ ดอกเบี้ยสะสม และวันที่เคลื่อนไหวครั้งสุดท้าย เท่านั้น แต่ไม่มีรายละเอียดของ HOLD CODE และ BLOCKING AMOUNT ซึ่งมีความสำคัญต่อผู้อ่านรายงานที่จะใช้ประกอบการพิจารณาว่าสมควรจะโอนเป็นบัญชีไม่เคลื่อนไหวหรือไม่

3) รายงานการเปิดบัญชี

การที่องค์กรยินยอมให้มีการเปิดบัญชีไว้ก่อนโดยยังไม่มีเงินนำฝากในวันที่ขอเปิดบัญชีได้ โดยเฉพาะลูกค้าที่เป็นพนักงานลูกจ้างของบริษัทที่รับเงินเดือนโดยผ่านองค์กรนั้น ในรายงานการเปิดบัญชีซึ่งเป็นรายงานที่แสดงเฉพาะบัญชีเปิดใหม่ที่มีรายการฝากจริง จะไม่แสดงบัญชีที่เปิดใหม่โดยไม่มีการฝากเงินในวันเปิดบัญชี แต่จำนวนบัญชีที่เปิดไว้ก่อนโดยยังไม่มีเงินนำฝาก ได้นับรวมไว้ตอนท้ายรายงานการเปิดบัญชีในวันที่เปิดบัญชีแล้ว และนำรายการเปิดบัญชีที่ยังไม่มีการฝากเงินไปแสดงไว้ในรายงานบัญชีเปิดใหม่ แต่ยังไม่ได้ผ่านบัญชี ต่อมาเมื่อมีการโอนเงินเดือนเข้าบัญชีที่เปิดไว้โดยยังไม่มีการฝากเงินดังกล่าว ในรายงานการเปิดบัญชีจะแสดงรายการโอนเงินเดือนเข้าบัญชีไว้เสมือนเป็นรายการเปิดบัญชีใหม่ทำให้จำนวนบัญชีที่เปิดในวันนั้นในรายงานการเปิดบัญชีมีมากกว่าจำนวนบัญชีที่เปิดใหม่ท้ายรายงานการเปิดบัญชีซึ่งถูกต้อง ทำให้ผู้อ่านรายงานเกิดความสับสนได้ ถ้าเป็นกรณีเปิดบัญชีไว้ก่อนโดยไม่มีเงินนำฝากและไม่ใช่บัญชีที่โอนเงินเดือนเข้า เมื่อนำเงินมาเข้าบัญชีครั้งแรกในวันอื่น จะไม่ปรากฏรายการนำเงินเข้าบัญชีในรายงานการเปิดบัญชี

4) รายงานการปิดบัญชี

จากการทดสอบบัญชีที่ปิดแล้วเปิดใหม่ในวันเดียวกัน จะมีรายการปรากฏในรายงานการปิดบัญชี และมีรายการแก้ไขการปิดบัญชีนั้นปรากฏในรายงานการปิดบัญชี ซึ่งจะมีรายการแก้ไขการบันทึกดอกเบี้ยเกินมา ทำให้จำนวนยอดเงินปิดบัญชีในรายงานไม่ถูกต้อง แต่ในตอนท้ายรายงานการปิดบัญชีสรุปจำนวนบัญชีที่ปิดแล้วถูกต้อง โดยไม่นับบัญชีที่ปิดแล้วเปิดใหม่รวมอยู่ในจำนวนบัญชีที่ถูกปิดด้วย

5) รายงานยอดคงเหลือเฉลี่ย

จากการทดสอบพบว่า โปรแกรมนำชื่อบัญชีของบัญชีสุดท้ายไปพิมพ์เป็นชื่อบัญชีให้กับบัญชีอื่น ๆ ทำให้ชื่อบัญชีที่ปรากฏในรายงานไม่ถูกต้อง ยกเว้นบัญชีสุดท้ายที่มีชื่อบัญชีถูกต้อง

(27) ไม่มีการใช้กระดาษ Journal Roll ใน Passbook Printer

Passbook Printer ที่องค์กรใช้อยู่สามารถใส่กระดาษ Journal Roll ซึ่งจะบันทึกรายการต่าง ๆ ที่พนักงาน Teller ป้อนข้อมูลผ่านจอ Terminal ไว้สำหรับตรวจสอบได้ภายหลังเมื่อมีปัญหา แต่องค์กรมิได้กำหนดให้ใช้กระดาษ Journal Roll ดังกล่าวให้เป็นประโยชน์อย่างเต็มที่ และทำให้องค์กรขาดหลักฐานที่ใช้ติดตาม (Audit Trail) เมื่อมีปัญหาได้ในภายหลัง

ข้อแนะนำ

(1) ควรปรับปรุงแก้ไขระบบงานและวิธีปฏิบัติงานในส่วนที่เกี่ยวกับการอายัดเงินฝากออมทรัพย์ไว้เป็นประกัน โดยจัดให้มีการควบคุมที่รัดกุม และมี Message เตือนผู้ปฏิบัติงานให้ทราบถึงปัญหาที่อาจเกิดขึ้น

(2) ข้อความเตือนพนักงานทางจอภาพเมื่อมีการป้อนรายการผิดพลาด ควรบอกสาเหตุของข้อผิดพลาดอย่างชัดเจนไม่คลาดเคลื่อนไปจากความเป็นจริง

(3) ควรปรับปรุงแก้ไขโปรแกรมที่ใช้ในการ Set up ข้อมูล ให้มีการป้องกันข้อผิดพลาด ในการปฏิบัติงานของพนักงานในกรณีต่าง ๆ ตามความเหมาะสม และจัดพิมพ์รายงานตาม SET UP MAIN MENU ให้ครบถ้วน เพื่อใช้เป็น Audit Trail ซึ่งสามารถเก็บไว้ใช้ประโยชน์ในการตรวจสอบความถูกต้องของข้อมูลที่ Set up ได้

(4) ควรปรับปรุงแก้ไขโปรแกรมที่ใช้ออกรายงาน ซึ่งแสดงข้อมูลไม่ครบถ้วนหรือคลาดเคลื่อนไปจากความเป็นจริงให้ถูกต้อง

(5) ควรใช้กระดาษ Journal Roll ใน Passbook Printer เพื่อเป็นหลักฐาน (Audit Trail) การทำรายการของพนักงาน Teller แต่ละคนไว้ตรวจสอบได้ในภายหลัง

(28) การบันทึกและการแก้ไขรายการเงินฝากออมทรัพย์ในสมุดคู่ฝากไม่รัดกุม

โปรแกรมระบบงานในส่วนที่เกี่ยวกับเงินฝากออกทรัพย์ มิได้กำหนดให้พิมพ์รายการเคลื่อนไหวลงในสมุดคู่ฝากด้วยเครื่องพิมพ์ (Printer) ดังนั้น พนักงานจึงต้องเขียนรายการในสมุดคู่ฝากดังกล่าว เป็นผู้ให้การบันทึกรายการฝากเงินของลูกค้าซึ่งมีการฝากแบบไม่ใช้สมุดคู่ฝาก (no book) ไม่เป็นไปตามลำดับรายการที่เกิดขึ้น เนื่องจากพนักงานผู้ทำรายการจะบันทึกรายการฝากทันทีโดยไม่มีการตรวจสอบรายการฝากแบบไม่ใช้สมุดคู่ฝากที่ยังค้างอยู่ก่อน เป็นผลให้ยอดคงเหลือในสมุดคู่ฝากไม่ถูกต้อง นอกจากนี้ ยังมีการแก้ไขรายการในสมุดคู่ฝากออมทรัพย์ด้วยการใช้ยาลบหมึกสีขาวลบข้อมูลที่ผิดพลาด ซึ่งเป็นการปฏิบัติที่ไม่เหมาะสมและรัดกุม

ข้อแนะนำ

องค์กรควรตรวจสอบรายการฝากแบบไม่ใช้สมุดคู่ฝากที่ค้างอยู่จากเครื่อง Terminal ที่ใช้ในการดูข้อมูลของลูกค้าก่อนบันทึกรายการฝากครั้งต่อไป สำหรับรายการที่ผิดพลาด ควรขีดฆ่าและลงนามกำกับไว้เพื่อเป็นแนวทางในการติดตามปัญหาได้ในภายหลัง

(29) การควบคุมสมุดคู่ฝากของบัญชีเงินฝากออมทรัพย์ไม่รัดกุม

1) ไม่มีการควบคุมการเบิกจ่ายสมุดคู่ฝาก

องค์กรไม่มีการควบคุมการเบิก-จ่ายสมุดคู่ฝาก ซึ่งเป็นเอกสารสำคัญที่ลูกค้าสามารถใช้เป็นหลักฐานขอถอนเงินได้ การจ่ายสมุดคู่ฝากโดยไม่ได้จัดทำทะเบียนควบคุมการจ่ายสมุดคู่ฝากให้ลูกค้า สมุดคู่ฝากอาจสูญหายโดยไม่มีผู้ใดทราบ และเป็นจุดอ่อนในการนำสมุดคู่ฝากไปปลอมแปลงเพื่อทำการทุจริตได้

2) การควบคุมการออกสมุดคู่ฝากเล่มใหม่ให้ลูกค้าไม่เหมาะสม

องค์กรออกสมุดคู่ฝากเล่มใหม่ให้แก่ลูกค้าโดยมิได้ให้ลูกค้าลงตัวอย่างลายมือชื่อที่ด้านหลังสมุดคู่ฝาก เนื่องจากลูกค้าไม่มาติดต่อด้วยตนเอง ในกรณีที่พนักงานตรวจลายมือชื่อเจ้าของบัญชีจากตัวอย่างลายมือชื่อด้านหลังสมุดคู่ฝาก อาจเป็นจุดอ่อนในระบบการควบคุมภายในขององค์กร หากมีผู้เก็บสมุดคู่ฝากและลงลายมือชื่อด้านหลังสมุดคู่ฝาก แล้วนำสมุดคู่ฝากมาขอถอนเงินในบัญชีของลูกค้า

ข้อแนะนำ

องค์กรควรกำหนดให้มีเลขที่สมุดคู่ฝากเพื่อใช้ในการควบคุมการเบิกจ่ายสมุดคู่ฝาก และควรกำหนดระเบียบในการออกสมุดคู่ฝากเล่มใหม่ โดยให้ลูกค้ามาติดต่อด้วยตนเอง พร้อมทั้งให้ลูกค้าลงลายมือชื่อที่ด้านหลังสมุดคู่ฝากให้ถูกต้องตรงกับตัวอย่างลายมือชื่อที่ให้ไว้กับองค์กรตอนเปิดบัญชี

(30) การควบคุมเลขที่สมุดคู่ฝากไม่รัดกุม

การควบคุมเลขที่สมุดคู่ฝากกับเลขที่บัญชีขององค์กรจะใช้วิธีป้อนเลขที่สมุดคู่ฝากไว้ต่อท้าย Short name และป้อนเป็น Message ให้เครื่องแสดงทุกครั้งที่ทำรายการกับบัญชีนั้น เพื่อให้ผู้ทำรายการใช้ตรวจสอบกับเลขที่สมุดคู่ฝากว่าถูกต้องหรือไม่ แต่จากการตรวจสอบพบว่ามีหลายบัญชีที่ไม่ได้ป้อนข้อมูลเลขที่สมุดคู่ฝากเข้าเครื่อง

ข้อแนะนำ

ควรเร่งดำเนินการป้อนเลขที่สมุดคู่ฝากไว้ในระบบให้ครบถ้วนทุกบัญชี เพื่อใช้ตรวจสอบความถูกต้องกับสมุดคู่ฝากที่ลูกค้ามาทำรายการ

(31) การควบคุมสมุดคู่ฝากและการทำรายการปิดบัญชียังไม่รัดกุม

1) บัญชีที่ปิดแล้ว สาขาไม่ได้ควบคุมให้มีการปรุสมุดคู่ฝากที่ปิดบัญชีแล้วทุกบัญชี และไม่ได้เก็บสมุดคู่ฝากที่ปิดบัญชีแล้ว เรียงตามเลขที่บัญชี เพื่อความสะดวกในการค้นหาและการควบคุม

ข้อแนะนำ

ควรกำชับให้ปรุสมุดคู่ฝากที่ลูกค้าปิดบัญชีแล้ว และจัดเรียงให้เรียบร้อย

2) จากการตรวจสอบสมุดคู่ฝากของบัญชีที่ปิดไปแล้ว พบว่ามีหลายบัญชีที่ลูกค้าถอนจนยอดคงเหลือเป็นศูนย์ และประทับตรา "A/C CLOSED" แล้ว แต่ยังไม่ได้บันทึกรายการปิดบัญชีในระบบคอมพิวเตอร์ ซึ่งจะมีผลทำให้บัญชีนั้นยังคงสภาพเป็นบัญชีที่เปิดอยู่ โดยมียอดคงเหลือเป็นศูนย์ในระบบคอมพิวเตอร์ อันอาจจะมีผลเสียหายเกิดขึ้นได้หากมีการนำบัญชีนั้นไปเดินรายการต่อ

ข้อแนะนำ

ควรกำชับให้ทำรายการปิดบัญชีสำหรับบัญชีที่ลูกค้ามาขอปิดบัญชีหลังจากถอนจนยอดคงเหลือเป็นศูนย์

(32) การควบคุมการผ่านรายการไม่รัดกุม

พนักงาน Teller สามารถทำรหัสรายการ Interest Deposit ตลอดจนรหัสรายการ Interest Deposit No-Book เพื่อบันทึกรายการดอกเบี้ยเมื่อลูกค้าขอปิดบัญชีได้เอง โดยไม่ต้องใช้บัตรอนุมัติรายการ หากมีข้อผิดพลาดในการบันทึกดอกเบี้ยมากกว่าความเป็นจริงอาจส่งผลเสียหายต่อองค์กรได้

ข้อแนะนำ

ควรกำหนดให้มีระบบการตรวจสอบความถูกต้องของข้อมูล และอนุมัติการทำรายการอย่างเหมาะสม เพื่อป้องกันข้อผิดพลาดจากการทำรายการบันทึกรายการดอกเบี้ยเมื่อลูกค้าขอปิดบัญชี

(33) รายการตัดบัญชีเงินฝากออมทรัพย์ด้วยเช็ค

คู่มือการปฏิบัติงานไม่ได้ระบุให้ชัดเจนว่า ให้ใช้รหัสรายการพิเศษในการผ่านบัญชีสำหรับกรณีสำนักงานสาขาที่ไม่ได้ On-line ได้จ่ายเงินให้ลูกค้าของสำนักงานสาขาเจ้าของบัญชีซึ่งอยู่ในเครือข่าย On-line ไปก่อนแล้วส่งใบเบิกมาขอตัดบัญชีจากสาขาเจ้าของบัญชีในภายหลัง ซึ่งอาจทำให้พนักงานเข้าใจว่า รหัสรายการที่กล่าวสามารถใช้ตัดบัญชีเงินฝากออมทรัพย์ของลูกค้าด้วยเช็คได้โดยไม่ต้องใช้สมุดคู่ฝาก ซึ่งไม่สอดคล้องกับลักษณะบัญชีเงินฝากออมทรัพย์ซึ่งไม่ใช้เช็คในการถอนเงิน

ข้อแนะนำ

ควรปรับปรุงแก้ไขคู่มือปฏิบัติงาน และอธิบายวัตถุประสงค์ในการใช้รหัสรายการต่าง ๆ ให้ชัดเจน เพื่อป้องกันการเข้าใจผิดหรือนำไปใช้ผิดวัตถุประสงค์

(34) การควบคุมการทำรายการโอน

การอนุญาตให้พนักงาน Teller ทำรายการ Transfer deposit และรายการ Telegram transfer เพื่อเครดิตบัญชีเงินฝากออมทรัพย์ของลูกค้าโดยไม่ต้องใช้บัตรอนุมัติรายการควบคุมการทำรายการ และลูกค้ามีสิทธิถอนเงินฝากที่เกิดจากรายการดังกล่าวผ่านเครือข่ายระบบ On-line ได้ทันทีนั้น หากมีข้อผิดพลาดในการทำรายการองค์กรอาจได้รับความเสียหาย

ข้อแนะนำ

ควรจัดให้มีการใช้บัตรอนุมัติรายการ ควบคุมการทำรายการ Transfer deposit และรายการ telegram transfer เพื่อป้องกันข้อผิดพลาดในการทำรายการรับฝากเงิน โดยเฉพาะในกรณี Transfer deposit ซึ่งลูกค้ามีสิทธิถอนเงินฝากที่เกิดจากรายการดังกล่าวผ่านเครือข่ายระบบ On-line ได้ทันที

(35) การพิมพ์ข้อมูลไม่ครบถ้วน

ในรายงาน S/A outstanding report จำนวนเงินฝากออมทรัพย์ที่ถูกอายัด (TOT-Hold) ของลูกค้าแต่ละราย จะถูกพิมพ์ทับด้วยข้อความ ********* ZERO BALANCE ********* ไม่สามารถแสดงข้อมูลการอายัดเงินฝากได้ครบถ้วนตามความเป็นจริง

ข้อแนะนำ

ควรปรับปรุงแก้ไขรายการ S/A outstanding report ไม่ให้พิมพ์ข้อความ ********* ZERO BALANCE ********* ทับพื้นที่ที่ใช้พิมพ์จำนวนเงินฝากออมทรัพย์ที่ถูกอายัด (TOT-Hold) เพื่อให้สามารถแสดงข้อมูลการอายัดเงินฝากออมทรัพย์ได้ครบถ้วนตามความเป็นจริง

(36) โปรแกรมระบบงานบางส่วนทำงานไม่ได้

จากการทดสอบพบว่า โปรแกรม INTPRS ซึ่งใช้ในการพิมพ์ดอกเบี้ยเงินฝากพิเศษลงการ์ดรายตัวผู้ฝากประเภทเงินฝากพิเศษ ยังมีข้อผิดพลาดไม่สามารถสั่งให้เครื่องพิมพ์พิมพ์รายการดอกเบี้ยลงในการ์ดได้ จึงให้ Operator ข้ามขั้นตอนนี้ไป เป็นผลให้ไม่สามารถผ่านดอกเบี้ยลงสมุดคู่ฝากของลูกค้าได้

ข้อแนะนำ

องค์กรควรจะจัดเตรียมโปรแกรมและเครื่องสำหรับใช้ในการทดสอบให้เหมือนกับที่ใช้งานอยู่จริง ทั้งนี้เพื่อให้ข้อมูลที่ได้รับจากการทดสอบถูกต้องตามที่ควรจะเป็น

(37) โปรแกรมที่ใช้ในการประมวลผลข้อมูลและพิมพ์เป็นรายงานบางส่วนทำงานไม่ถูกต้อง

จากการทดสอบโปรแกรมระบบงานเงินฝากพิเศษด้วยข้อมูลทดสอบ ปรากฏว่า "รายงานยอดคงเหลือเฉพาะบัญชีที่เคลื่อนไหวประจำวัน" ซึ่งจะแสดงยอดคงเหลือเฉพาะบัญชีที่มีการเคลื่อนไหวในแต่ละวันเท่านั้น ได้รวมยอดของบัญชีที่มีการเคลื่อนไหวในวันอื่นเข้าไปด้วย เป็นผลให้การรวมยอดคงเหลือของบัญชีที่มีการเคลื่อนไหวในวันนั้นทั้งหมดใน "รายงานยอดคงเหลือเฉพาะบัญชีที่เคลื่อนไหวประจำวัน" สูงกว่ายอดรวมของยอดคงเหลือทุกฉบับที่มีการเคลื่อนไหวในวันเดียวกันจาก "รายงานการเคลื่อนไหวสลิปทุกประเภท (เรียงตามลำดับเลขที่บัญชี)"

(38) ตำแหน่งบรรทัดพิมพ์ข้อมูลในสมุดคู่ฝากไม่ถูกต้อง

การใช้ตำแหน่งบรรทัดพิมพ์ข้อมูลในสมุดคู่ฝากให้เป็นประโยชน์ในการป้องกันข้อผิดพลาดที่อาจเกิดขึ้น ยังมีจุดอ่อนบางประการ ดังนี้

1) จากการทดสอบระบบโดยการฝากเงินสดจำนวน 1,000.00 บาท กรณีลูกค้าไม่ได้นำสมุดคู่ฝากมาแสดงด้วยรายการ Cash deposit nobook และทำรายการ Delete unposted line โดยทันที เมื่อทดสอบนำสมุดคู่ฝากมาบันทึกรายการที่ไม่ใช้สมุดคู่ฝากเป็นหลักฐานในการทำรายการให้ครบถ้วน (Update) ในภายหลังพบว่าระบบคอมพิวเตอร์จะเว้นว่างไว้ 1 บรรทัด ไม่พิมพ์รายการฝากที่กล่าวข้างต้น และไม่นำเงินฝากจำนวน 1,000.00 บาท มาแสดงรวมเป็นยอดเงินฝากคงเหลือในบัญชี แต่ใน Statement ขององค์กรแสดงรายการฝากที่กล่าวและยอดเงินฝากคงเหลือในบัญชีถูกต้อง

2) การยกยอดคงเหลือของบัญชีมาขึ้นหน้าใหม่ ระบบคอมพิวเตอร์จะไม่ตรวจสอบตำแหน่งบรรทัดของสมุดคู่ฝากที่พิมพ์อยู่เดิมว่าครบ 22 บรรทัดแล้วหรือไม่ ก่อนที่จะยินยอมให้ยกยอดเงินฝากคงเหลือไปพิมพ์รายการในบรรทัดที่ 1 ของหน้าถัดไป เปิดโอกาสให้ผู้ปฏิบัติงานสามารถใช้รายการ Modify passbook line บันทึกรายการที่อาจทำให้เกิดความเสียหายได้ เนื่องจากลูกค้าบางรายมีการฝาก-ถอนผ่านเครื่อง ATM ระบบจึงยินยอมให้ปฏิบัติดังกล่าวได้ แต่ก็ได้มีระเบียบปฏิบัติกำหนดไว้ในคู่มือว่า ให้ใช้สมุดเล่มเก่าจนหมดเสียก่อนแล้วจึงจะสามารถขึ้นเล่มใหม่ได้

(39) การควบคุมการทำรายการต่างสาขาไม่รัดกุมเท่าที่ควร

มีจุดอ่อนบางประการดังนี้

1) ระบบบัญชีเงินฝากออมทรัพย์เปิดโอกาสให้ผู้ปฏิบัติงานสามารถใช้รายการ Transfer withdrawal nobook และใช้บัตรอนุมัติรายการระดับ 4 ถอนเงินฝากจากบัญชีลูกค้าเพื่อโอนเงินไปฝากเข้าบัญชีอื่นในลักษณะรายการต่างสาขาได้ โดยลูกค้าไม่จำเป็นต้องนำสมุดคู่ฝากมาแสดงเป็นหลักฐาน นับว่าองค์กรได้ยอมเสี่ยงภัยค่อนข้างสูงในการกำหนดให้มีรายการที่กล่าวไว้ในระบบงานเพราะหากมีข้อผิดพลาดในการปฏิบัติงาน องค์กรอาจได้รับความเสียหายไม่น้อยกว่าการยินยอมให้ลูกค้าถอนเงินสดโดยไม่มีสมุดคู่ฝากเป็นหลักฐานในการถอนเงิน

2) ตามที่คณะทำงาน Saving Online กำหนดหลักเกณฑ์ในการถอนเงินและโอนเงินให้การถอนหรือโอนเงินต่างสาขาต้องถอนโดยผ่านรายการทางบัญชีหรือเป็นรายการเงินสดเสมอ จากการทดสอบปรากฏว่าผู้ปฏิบัติงานยังสามารถใช้รายการ Transfer withdrawal และรายการ transfer withdrawal-magtripe ทำรายการโอนเงินฝากระหว่างบัญชีในลักษณะต่างสาขาได้

3) การอนุญาตให้ใช้รายการอายัดเงินฝากเพื่อค้ำประกันสินเชื่อ และถอนอายัดเงินฝากที่ค้ำประกันสินเชื่อ ซึ่งกระทำต่างสาขาได้โดยใช้บัตรอนุมัติรายการควบคุมการทำรายการที่กล่าวเช่นเดียวกับการทำรายการอื่นบางประเภทโดยไม่มีมาตรการควบคุมอื่น ๆ มาเสริมหรือสนับสนุนอย่างเพียงพอนั้นอาจทำให้องค์กรได้รับความเสียหายได้

(40) **หลังจากบันทึกดอกเบี้ยเงินฝากออมทรัพย์เข้าบัญชีให้ลูกค้าแล้ว** รายงาน Savings Account Listing - High Accrued-Int. ยังคงแสดงยอด Accrued Intrerest ที่คำนวณไว้ในวันสุดท้าย และมีการบันทึกดอกเบี้ยเงินฝากออมทรัพย์เข้าบัญชีให้ลูกค้า ซึ่งไม่ถูกต้อง เพราะไม่ควรมียอด Accrued Interest คงค้าง

นอกจากนี้การแสดงยอด Grand Total ในการรวมยอดข้อมูล Accured Int. ไม่เป็นไปตามคำอธิบายในตัวอย่างรายงาน ซึ่งอาจทำให้ผู้ใช้ข้อมูลเกิดความสับสนได้

ข้อแนะนำ

(1) ควรปรับปรุงวิธีการทำรายการต่างสาขาที่เกี่ยวกับการโอนเงินฝากระหว่างบัญชีและการอายัดเงินฝาก ให้มีการควบคุมที่รัดกุมและเหมาะสม

(2) ควรปรับปรุงแก้ไขวิธีการคำนวณดอกเบี้ยเงินฝากออมทรัพย์ในกรณีที่มีการบันทึกรายการลงวันที่ย้อนหลัง ให้ถูกต้องตามความเป็นจริง

(3) ควรมีข้อความปรากฏทางจอภาพเตือนผู้ปฏิบัติงานให้ทำการบันทึกดอกเบี้ยและหักภาษีดอกเบี้ยเงินฝาก ณ ที่จ่ายทุกครั้ง ก่อนทำรายการปิดบัญชี

(4) ควรปรับปรุงแก้ไขข้อผิดพลาดในรายงานต่าง ๆ ให้ถูกต้องตามความเป็นจริง

(41) **ระบบงานไม่ได้จัดให้มีการออกรายงานพิเศษ** (Exception report) เกี่ยวกับรายการปรับปรุงข้อมูลของลูกค้า และรายการอื่น ๆ ที่สำคัญ เช่น ดอกเบี้ยสะสม แยกออกจากรายงาน Daily transaction report ซึ่งการรวมรายการปรับปรุงดังกล่าวอยู่ในรายงาน อาจทำให้ข้ามหรือผ่านการเช็คสอบไปได้

(42) **ไม่มีการกำหนดรหัสลับ (Password) ให้แก่พนักงาน**

เพื่อควบคุมการใช้คอมพิวเตอร์

ส่วนเงินฝากประจำและออมทรัพย์ ไม่ได้กำหนดรหัสลับ (Password) ให้แก่พนักงาน Teller แต่ใช้เลขศูนย์แทนรหัสลับในการควบคุมการเปิด-ปิดเครื่องคอมพิวเตอร์ ซึ่งอาจเป็นสาเหตุให้ผู้ที่ไม่มีหน้าที่เกี่ยวข้องสามารถเข้าถึงและเปลี่ยนแปลงแก้ไขแฟ้มข้อมูลขององค์กร

ข้อแนะนำ

องค์กรควรกำหนด Password ให้แก่พนักงาน Teller ในการเปิด-ปิดเครื่องคอมพิวเตอร์

2.2.3 เงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา

(1) การควบคุมการใช้วันที่ฝากย้อนหลัง (Value date) ไม่รัดกุม

องค์กรยินยอมให้พนักงานเทลเลอร์ทำรายการฝากเพื่อต่ออายุการฝากเงินให้ลูกค้าที่ครบกำหนดระยะเวลาการฝาก โดยย้อนวันที่รับฝากได้ทั้งกรณีที่ต้องใช้สมุดคู่ฝากและไม่ใช้สมุดคู่ฝากเป็นหลักฐานประกอบการรับฝากเงิน โดยไม่มีพนักงานอื่นควบคุมการทำรายการดังกล่าว ถ้าจำนวนเงินไม่เกินวงเงินของพนักงานเทลเลอร์ นอกจากนี้ ยังสามารถใช้วันที่ฝากย้อนหลังได้เกิน 1 ปี ซึ่งเกินรอบระยะเวลาที่องค์กรใช้บันทึกดอกเบี้ยให้ลูกค้าตามปกติ อาจทำให้องค์กรได้รับความเสียหายที่ต้องจ่ายดอกเบี้ยเกินความเป็นจริงได้

ข้อแนะนำ

ควรเพิ่มจุดตรวจสอบในโปรแกรมให้การใช้วันที่ฝากย้อนหลัง (Value date) ควรอยู่ในช่วงที่เหมาะสม และกำชับพนักงานให้เพิ่มความระมัดระวังในการใช้วันที่ฝากย้อนหลัง

(2) การควบคุมการกำหนดประเภทผู้ฝาก ไม่รัดกุม

ระบบงานอนุญาตให้ผู้ปฏิบัติงานกำหนดประเภทผู้ฝากได้มากกว่าที่องค์กรกำหนดไว้ในตอนทำรายการเปิดบัญชี ซึ่งอาจทำให้ลูกค้าประเภทที่ต้องเสียภาษี เช่น บุคคลธรรมดาหรือนิติบุคคล ไม่ถูกหักภาษี ณ ที่จ่ายไว้

(3) การกำหนดระยะเวลาการฝาก (Subtype) ไม่เหมาะสม

การบันทึกระยะเวลาการฝากโดยใช้รหัสแทนระยะเวลาการฝากตามที่ใช้ปฏิบัติงานในปัจจุบันเป็นดังนี้

ประเภทการฝาก	ระยะเวลาการฝาก
3 เดือน	01
6 เดือน	02
12 เดือน	03
24 เดือน	04
60 เดือน	05

การกำหนดรหัสดังกล่าวอาจก่อให้เกิดปัญหาในการปฏิบัติงาน เนื่องจากพนักงานอาจจำระยะเวลาการฝากผิดพลาด เช่น ประเภทการฝาก 12 เดือน แต่บันทึกระยะเวลาการฝากเป็น 01 เป็นต้น ซึ่งหากผู้ตรวจสอบภายในไม่พบข้อผิดพลาดและแก้ไขให้ถูกต้อง จะทำให้การคำนวณดอกเบี้ยจ่ายผิดพลาดได้

ข้อแนะนำ

ควรกำชับพนักงานให้ตรวจสอบรหัสระยะเวลาการฝาก (Subtype) ของบัญชีที่เปิดใหม่ในรายงานประจำวันโดยสม่ำเสมอ

(4) การทำรายการเช็คคืนไม่รัดกุม

การยกเลิกรายการฝากด้วยเช็คเนื่องจากเช็คคืน อาจมีข้อผิดพลาดได้ เนื่องจากระบบงานไม่มีการตรวจสอบลำดับที่ของรายการฝาก (Deposit number) ว่าเป็นรายการฝากด้วยเช็คหรือไม่ หากผู้ปฏิบัติงานใช้ลำดับที่ของรายการฝากผิดพลาด เป็นลำดับที่ของรายการที่ไม่ได้ฝากด้วยเช็คจะทำให้ทำรายการเช็คคืนผิดลำดับที่ของรายการฝาก และข้อมูลเกี่ยวกับรายการฝากลำดับดังกล่าวจะไม่ถูกต้อง ซึ่งจะทำให้การคำนวณดอกเบี้ยผิดพลาดด้วย

ข้อแนะนำ

ควรเพิ่มจุดตรวจสอบในโปรแกรมให้ทำรายการเช็คคืนได้เฉพาะยอดที่นำฝากด้วยเช็คเท่านั้น

(5) การทำรายการกำหนดอัตราดอกเบี้ยพิเศษ

ระบบงานไม่มีการป้องกันการกำหนดอัตราดอกเบี้ยพิเศษเฉพาะราย พนักงานสามารถใช้อัตราดอกเบี้ยเกินกว่าอัตราดอกเบี้ยที่กำหนดตามกฎหมายได้ และองค์กรอาจได้รับความเสียหายหากไม่มีการตรวจสอบอัตราดอกเบี้ยที่กำหนดกับรายงานประจำวัน

ข้อแนะนำ

ควรเพิ่มจุดตรวจสอบในระบบงานให้ตรวจสอบอัตราดอกเบี้ยสูงสุด ไม่ให้เกินกว่าอัตราที่กำหนดตามกฎหมาย ก่อนที่คอมพิวเตอร์จะยอมรับอัตราดอกเบี้ยพิเศษเข้าไปเก็บไว้ในระบบเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา

(6) การกำหนดจำนวนวันซึ่งใช้เป็นฐานในการคำนวณดอกเบี้ย

การคิดดอกเบี้ยเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาในกรณีที่เป็นอธิกมาสมี 366 วันนั้น ระบบงานคำนวณดอกเบี้ยโดยใช้ฐาน 365 วัน ทำให้องค์กรจ่ายดอกเบี้ยเงินฝากที่ฝากในช่วงปีอธิกมาสเกินไป 1 วัน และอาจจ่ายดอกเบี้ยเกินอัตราที่กฎหมายกำหนดได้หากองค์กรใช้อัตราดอกเบี้ยสูงสุดที่พึงจ่ายได้

(7) ระบบงานยินยอมให้ป้อนอัตราดอกเบี้ยได้สูงสุดกว่าอัตราที่ทางการกำหนด

จากการทดสอบพบว่า การใช้รหัสรายการ (FIX CHANGE FLOAT RATE) ระบบงานยินยอมให้ป้อนอัตราดอกเบี้ยได้สูงกว่าอัตราที่ทางการกำหนด และระบบงานจะคำนวณดอกเบี้ยด้วยอัตราดอกเบี้ยที่ป้อนเข้าไป ซึ่งไม่ถูกต้อง นอกจากนี้ การใช้รหัสรายการ (FIX CHANGE CONTRACT) ระบบงานยินยอมให้ป้อนอัตราดอกเบี้ยได้สูงกว่าอัตราที่ทางการกำหนด แต่ระบบงานจะคำนวณดอกเบี้ยโดยอาศัยข้อมูลจากตารางดอกเบี้ย ซึ่งไม่เกินอัตราที่ทางการกำหนด

โดยปกติเมื่อมีการเปลี่ยนแปลงอัตราดอกเบี้ย องค์กรจะเปลี่ยนแปลงตารางดอกเบี้ย ในระบบคอมพิวเตอร์ เพื่อป้องกันมิให้มีการคำนวณดอกเบี้ยสูงกว่าอัตราที่กำหนด ยกเว้นการใช้รหัสรายการ (FIX CHANGE FLOAT RATE) ซึ่งคำนวณดอกเบี้ยด้วยอัตราดอกเบี้ยที่รับจากข้อมูลนำเข้า ซึ่งไม่ถูกต้อง

ข้อแนะนำ

ควรแก้ไขระบบงานมิให้มีการป้อนอัตราดอกเบี้ย ตลอดจนควบคุมมิให้มีการคำนวณดอกเบี้ยด้วยอัตราที่สูงกว่าอัตราที่องค์กรกำหนด

(8) การคำนวณดอกเบี้ยไม่ถูกต้องเมื่อมีการฝากเพิ่มเข้าใน Sub Account ที่มีอยู่เดิม

จากการทดสอบพบว่า ระบบงานยินยอมให้ผู้ปฏิบัติงานทำรายการฝากเพิ่มเข้าใน Sub Account ที่มีอยู่เดิม และส่งผลให้การคำนวณดอกเบี้ยไม่ถูกต้อง โดยระบบงานจะคำนวณดอกเบี้ยเงินฝากนับจากวันที่ฝากครั้งแรกโดยไม่คำนึงถึงวันฝากเพิ่มเข้าใน Sub Account ในภายหลัง

ข้อแนะนำ

ควรแก้ไขระบบงานมิให้มีการฝากเงินเพิ่มเข้าใน Sub Account ที่มีอยู่เดิม

(9) การคำนวณภาษีหัก ณ ที่จ่ายไม่ถูกต้อง

จากการทดสอบพบว่า ระบบงานคำนวณภาษีหัก ณ ที่จ่ายไม่ถูกต้องสำหรับลูกค้าเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาประเภทนิติบุคคล ซึ่งมีรหัสประเภทการเสียภาษีในอัตราร้อยละ 1 (รหัสภาษี = 2) เมื่อทำรายการโดยใช้รหัสรายการ FIX CHANGE CONTRACT เพื่อฝากย้อนวันที่ โดยให้วันครบกำหนดเป็นวันที่ทำรายการ และทำรายการถอนโดยใช้รหัสรายการ FIX CASH WITHDRAWAL INTEREST ระบบงานจะคำนวณดอกเบี้ยให้โดยถูกต้องแต่คำนวณภาษีหัก ณ ที่จ่ายในอัตราร้อยละ 15 ซึ่งเป็นอัตราภาษีสำหรับบุคคลธรรมดา

ข้อแนะนำ

ควรแก้ไขระบบงานเพื่อป้องกันมิให้เกิดข้อผิดพลาดในการคำนวณภาษีหัก ณ ที่จ่ายสำหรับลูกค้าเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาประเภทนิติบุคคลตามกรณีที่กล่าว

(10) การนำเงินฝากเข้าผิดบัญชี

การรับฝากเงินที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาในกรณีที่ไม่ได้ใช้สมุดคู่ฝาก (No Book) ระบบงานมิได้จัดพิมพ์รายละเอียดชื่อลูกค้าในแบบฟอร์มใบรับฝากเงินสำหรับให้ลูกค้าตรวจสอบความถูกต้อง หากลูกค้าแจ้งเลขที่บัญชีไม่ถูกต้องหรือมีข้อผิดพลาดในการป้อนเลขที่บัญชี อาจทำให้ลูกค้าได้รับความเสียหายจากการนำเงินฝากเข้าผิดบัญชี

ข้อแนะนำ

ควรพิจารณาทบทวนความจำเป็นในการทำรายการโดยไม่ใช้สมุดคู่ฝาก ในกรณีที่จำเป็นบางกรณีและควรแก้ไขระบบงานให้สามารถตรวจสอบความถูกต้อง เพื่อป้องกันการนำเงินฝากเข้าผิดบัญชี

(11) ไม่มีการสอบยันข้อมูล

1) จำนวนเงินที่รับฝากจริงไม่ตรงตามจำนวนเงินตามเงื่อนไขระบบคอมพิวเตอร์มิได้เตือนผู้ปฏิบัติงานให้ทราบ ในกรณีที่ทำรายการรับฝากจริงด้วยจำนวนเงินที่ต่างไปจากจำนวนเงินฝากตามเงื่อนไขที่ได้แจ้งไว้ตามข้อกำหนด

2) ยกเลิกภาระค้ำประกันด้วยข้อมูลที่แตกต่างจากข้อมูลเมื่อทำการค้ำประกันระบบคอมพิวเตอร์มิได้เตือนผู้ปฏิบัติงานให้ทราบในกรณีที่มีการยกเลิกภาระการค้ำประกัน โดยการป้อนวันที่ต่างจากวันที่ติดภาระการค้ำประกันที่เก็บไว้ในระบบคอมพิวเตอร์ นอกจากนี้ยังสามารถป้อนเลขที่บัญชีที่ต้องการค้ำประกัน และรหัสค้ำประกันต่างจากข้อมูลเมื่อทำการค้ำประกันได้ ซึ่งอาจทำให้เข้าใจผิดว่าบัญชีเงินเบิกเกินบัญชีนั้นยังมีหลักประกันอยู่ ทั้งที่ไม่มีหลักประกันแล้ว

(12) การทำรายการลดวงเงินค้ำประกัน

ในกรณีที่ต้องการลดวงเงินค้ำประกัน ตามระเบียบขององค์กรกำหนดว่าให้ทำการล้างวงเงินค้ำประกันเก่าเสียก่อน แล้วจึงกันวงเงินค้ำประกันยอดใหม่ แต่ในทางปฏิบัติพนักงานทำการลดวงเงินค้ำประกันด้วยผลต่างระหว่างวงเงินค้ำประกันยอดเก่ากับยอดใหม่ เพื่อให้วงเงินค้ำประกันคงเหลือตามต้องการ ซึ่งทำให้รหัสการค้ำประกัน (Hold code) ถูกลบไป ดังนั้น จึงไม่สามารถให้รายละเอียดได้ว่ากันวงเงินไว้เป็นหลักประกันสินเชื่อชนิดใด ซึ่งหากปฏิบัติงานตามระเบียบที่วางไว้จะไม่เกิดปัญหาดังกล่าว

(13) ในการทำรายการ Fix Interest Inquiry ซึ่งต้องป้อนข้อมูลเกี่ยวกับ Acct. #, Sub #Amount และ Date พบว่า จำนวนเ งิน (Amount) ที่ต้องแจ้งให้ระบบคอมพิวเตอร์ทราบตามข้อกำหนดของรายการเพื่อสอบถามดอกเบี้ยเป็นจำนวนเงินที่แตกต่างไปจากยอดเงินฝากคงเหลือตามบัญชี และระบบงานไม่ได้เตือนผู้ปฏิบัติงานให้รับทราบเพื่อแก้ไข

ข้อแนะนำ

ระบบงานควรมีข้อความเตือนให้ผู้ปฏิบัติงานทราบ เพื่อป้องกันความผิดพลาดในการประมวลผลข้อมูล

(14) ข้อผิดพลาดงาน Batch Terminal Input

กรณีเงินฝากประจำระยะเวลาฝาก 3 เดือนและ 6 เดือน ครบกำหนดระยะเวลาฝากระบบคอมพิวเตอร์จะคำนวณดอกเบี้ยให้โดยอัตโนมัติ และทบดอกเบี้ยเข้ากับยอดเงินต้นรวมเป็นรายการฝากต่อในวันครบกำหนดนั้น แต่จากการปฏิบัติงานปรากฏว่ามีข้อผิดพลาดเกิดขึ้นเป็นบางวัน โดยไม่ได้ทบดอกเบี้ยเข้าบัญชีให้ลูกค้า แต่จะผ่านรายการดอกเบี้ยเข้าระบบบัญชี (B/L)

(15) **การคำนวณดอกเบี้ยเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา ไม่สอดคล้องกับโปรแกรมระบบงาน**

วิธีปฏิบัติการคำนวณดอกเบี้ยจ่ายเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา ไม่สอดคล้องกับโปรแกรมระบบงาน กล่าวคือ มีการคำนวณดอกเบี้ยโดยใช้เกณฑ์ตามระยะเวลาที่ฝากเป็นจำนวนเดือน แต่โปรแกรมระบบงานมีการคำนวณดอกเบี้ยโดยใช้เกณฑ์ตามระยะเวลาที่ฝากเป็นจำนวนวัน ซึ่งทำให้องค์กรไม่ได้ใช้ประโยชน์จากข้อมูลที่ประมวลผลด้วยคอมพิวเตอร์ที่มีความถูกต้องอยู่แล้ว

(16) **รายการอายัดเงินฝาก** ในการกันเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาหรือการกันเงินฝากประเภทอื่นโดยใช้รหัสรายการที่ทำหน้าที่คล้ายกันเพื่อประกันหนี้ องค์กรไม่ได้กำหนดให้มีการตรวจสอบยอดคงเหลือในบัญชีเงินฝากของลูกค้าว่ามีเช็คที่อยู่ในระหว่างการเรียกเก็บรวมอยู่ในยอดเงินฝากที่จะกันไว้เป็นประกันหนี้หรือไม่

ข้อแนะนำ

องค์กรควรกำหนดให้พนักงานตรวจสอบเลือกก่อนว่ารายการฝากด้วยเช็คที่จะทำการอายัดนั้นจะต้องเป็นรายการที่ทราบผลการเรียกเก็บแล้ว

(17) **องค์กรไม่ได้กำหนดระเบียบปฏิบัติเกี่ยวกับการถอนอายัดเงินฝากบางส่วนที่กันไว้เป็นประกันหนี้ให้แน่ชัด** หากมีผู้ปฏิบัติงานที่ไม่ทราบว่าการถอนอายัดเงินฝากเพียงบางส่วนจะมีผลเท่ากับการถอนอายัดเงินฝากทั้งจำนวน อาจทำให้องค์กรได้รับความเสียหายได้ กล่าวคือ ในกรณีที่เป็นเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและเงินฝากออมทรัพย์ องค์กรสามารถทำการถอนอายัดเงินฝากเพียงบางส่วนได้ โดยส่วนที่เหลือยังคงถูกอายัดอยู่ เครื่องคอมพิวเตอร์ไม่ยอมให้ถอนเงินส่วนที่เหลือนั้น แต่ในกรณีเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลานั้น การถอนอายัดบางส่วนมีผลเท่ากับการถอนอายัดเงินฝากทั้งหมด ซึ่งผู้ฝากจะสามารถถอนเงินฝากจำนวนนี้ทั้งจำนวนจากสาขาใดก็ได้ โดยเครื่องคอมพิวเตอร์จะไม่ทำการตรวจสอบการอายัดให้ ธนาคารชี้แจงว่าในกรณีถอนอายัดเงินฝากประเภทที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลานั้นในทางปฏิบัติจะต้องทำการถอนอายัดทั้งจำนวนเสียก่อนแล้วจึงทำการอายัดจำนวนที่ต้องการใหม่ และปัจจุบันธนาคารได้กำหนดให้พนักงานทำทะเบียนเพื่อตรวจสอบในกรณีมีการทำรายการถอนอายัดเงินฝาก นอกจากนี้ธนาคารจะพิจารณาว่าจะสามารถแก้ไขปัญหาได้โดยวิธีใด

(18) **รหัสรายการที่ใช้แก้ไขหรือยกเลิกรายการถอนโดยโอนไปเข้าบัญชีอื่นนั้น** ไม่มีการตรวจสอบความถูกต้องของเลขที่รายการฝากที่ถูกถอนก่อนที่จะดำเนินการแก้ไขหรือยกเลิกรายการ หากลูกค้าถอนเงินฝากหลายรายการและผู้ปฏิบัติงานป้อนเลขที่รายการฝากที่จะยกเลิกรายการถอนผิดพลาด จะทำให้การแก้ไขหรือการยกเลิกรายการถอนผิดพลาดด้วย

(19) **องค์กรไม่ได้จัดให้มีการตรวจสอบ** Overflow และไม่ได้จัดให้มีการเตือนผู้ปฏิบัติงานให้ทราบว่ายอดเงินฝากของลูกค้ามีจำนวนสูงเกินจำนวนหลักที่พิมพ์ได้

(20) การสอบยันข้อมูลภายในระบบงาน

ระบบคอมพิวเตอร์ไม่ได้เตือนผู้ปฏิบัติงานให้รับทราบสิ่งผิดปกติในบางกรณีเท่าที่ควร คือ

- กรณีที่มีการทำรายการรับฝากจริงด้วยจำนวนเงินที่แตกต่างไป จากจำนวนเงินฝากตามเงื่อนไขที่ได้แจ้งไว้ตามข้อกำหนดของรหัสรายการ FIX change contract เนื่องจากลูกค้าสามารถฝากด้วยเงินสดและเช็คต่าง ๆ ซึ่งต้องทำรายการรับฝาก 2 ครั้ง

- กรณีเงินต้นที่ต้องแจ้งให้ระบบคอมพิวเตอร์ทราบตามข้อกำหนดของรหัสรายการ FIX Interest Inquiry เพื่อสอบถามดอกเบี้ย มีจำนวนเงินที่แตกต่างไปจากยอดเงินฝากคงเหลือตามบัญชี เนื่องจากลูกค้าสามารถถอนเงินฝากน้อยกว่ายอดคงเหลือตามบัญชี สาขาจึงป้อนจำนวนเงินน้อยกว่าได้

- กรณีวันที่ติดภาระค้ำประกัน ที่ต้องแจ้งให้ระบบคอมพิวเตอร์ทราบตามข้อกำหนดของรหัสรายการ FIX release departmental hold เพื่อยกเลิกภาระค้ำประกัน เป็นวันที่แตกต่างไปจากวันที่ติดภาระค้ำประกันที่เก็บไว้ในระบบคอมพิวเตอร์

ข้อแนะนำ

ควรปรับปรุงระบบงานให้สามารถเตือนผู้ปฏิบัติงานหรือผู้ใช้ข้อมูลให้รับทราบสิ่งผิดปกติหรือข้อแตกต่างของข้อมูลที่ป้อนเข้าสู่ระบบคอมพิวเตอร์ตามข้อกำหนดในการทำรายการกับข้อมูลเดิมที่เก็บไว้ในระบบคอมพิวเตอร์

(21) คู่มือปฏิบัติงานไม่เป็นปัจจุบัน

คู่มือปฏิบัติงานระบบเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาในส่วนที่เกี่ยวกับการใช้บัตรอนุมัติรายการระดับ 2 ในการทำรายการดังต่อไปนี้ยังไม่ถูกต้อง เนื่องจากการทำรายการจริงต้องใช้ระดับ 3

Adjust withdraw no book
Cash withdraw no book
Transfer withdraw no book
Cash withdraw interest no book
Transfer withdraw interest no book
Bill bought no book
Pay-in cash no book
Transfer deposit no book

ข้อแนะนำ

ควรปรับปรุงแก้ไขคู่มือปฏิบัติงานระบบเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาในส่วนที่เกี่ยวกับการใช้บัตรอนุมัติรายการระดับ 2 เป็นระดับ 3 ในการทำรายการให้ถูกต้อง

(22) ข้อผิดพลาดในการใช้ Effective Date และ Due Date

ในระบบเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา ซึ่งผู้ปฏิบัติงานสามารถป้อนวันครบกำหนดระยะเวลาการฝากเงินตามสัญญา (Due Date) ย้อนหลังไปก่อนหน้าวันที่องค์กรเริ่มคิดดอกเบี้ยให้ลูกค้าเป็นวันแรก (Effective Date) ได้โดยไม่มีโปรแกรมตรวจสอบความเป็นไปได้ของข้อมูลเกี่ยวกับวันที่ที่นำไปใช้ในการคำนวณดอกเบี้ย หากมีข้อผิดพลาดเกิดขึ้นองค์กรอาจได้รับความเสียหาย เช่น มีการคิดดอกเบี้ยจาก Effective Date วันที่ 6 กรกฎาคม 2538 ย้อนกลับไปวัน Due Date คือวันที่ 6 มกราคม 2538

ข้อผิดพลาดที่กล่าวข้างต้นเกิดขึ้นเนื่องจากวันที่ 8 กรกฎาคม 2538 มีการแก้ไขระยะเวลาการฝาก ซึ่งเดิมมี Effective Date เป็นวันที่ 6 กรกฎาคม 2538 และ Due Date ที่ถูกต้องควรเป็นวันที่ 6 ตุลาคม 2538 (6/10/38) แต่ผู้ปฏิบัติงานเปลี่ยน Due Date ผิดเป็นวันที่ 6 มกราคม 2538 (6/01/38) เมื่อนำรายการนี้ไปประมวลผลหลังเวลาทำการในระบบ Batch จะมีผลทำให้บัญชีเงินฝากของลูกค้าเป็นบัญชีที่ครบกำหนดระยะเวลาการฝาก ซึ่งระบบจะคำนวณดอกเบี้ยเตรียมไว้จ่ายให้ลูกค้าในวันรุ่งขึ้นคือวันที่ 9 กรกฎาคม 2538 หลังจากวันที่มีการแก้ไขทันที ซึ่งไม่ถูกต้องเพราะบัญชีเงินฝากของลูกค้ารายนี้มีระยะเวลาการฝากเพียง 3 วันเท่านั้น

ข้อแนะนำ

ควรมีโปรแกรมตรวจสอบความเป็นไปได้ของข้อมูลเกี่ยวกับวันที่เริ่มคำนวณดอกเบี้ยเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาให้ลูกค้า และวันที่ครบกำหนดระยะเวลาการฝากเงินตามสัญญาก่อนที่จะยอมรับข้อมูลดังกล่าวไปเก็บไว้ในระบบเงินฝาก

(23) การกำหนดอัตราดอกเบี้ย Special Rate

การยินยอมให้พนักงาน Authorized ใช้ Special Rate ในการกำหนดอัตราดอกเบี้ยให้แก่ลูกค้าได้โดยไม่มีโปรแกรมควบคุมอัตราดอกเบี้ยสูงสุดไว้ในระบบ อาจมีข้อผิดพลาดในการกำหนดอัตราดอกเบี้ยเกินกว่าอัตราที่กำหนดตามกฎหมายได้

ข้อแนะนำ

ควรจัดให้มีโปรแกรมตรวจสอบอัตราดอกเบี้ยสูงสุดไม่ให้เกินกว่าอัตราที่กำหนดตามกฎหมาย ก่อนที่คอมพิวเตอร์จะยอมรับอัตราดอกเบี้ยซึ่งเป็น Special Rate เข้าไปเก็บไว้ในระบบเงินฝาก

(24) โปรแกรมคำนวณดอกเบี้ยเงินฝากประจำประเภท 2 ปี ไม่ถูกต้อง

จากการทดสอบโปรแกรมระบบงานเงินฝากประจำตัวโดยใช้ข้อมูลทดสอบ ปรากฏว่าโปรแกรมที่ใช้ในการคำนวณดอกเบี้ยเงินฝากประจำไม่ถูกต้อง กล่าวคือ ได้ทำรายการฝากประเภทใบรับฝากประจำจำนวน 300,000.00 บาท ระยะเวลาฝาก 2 ปี อัตราดอกเบี้ยร้อยละ 11.50 ต่อปี เริ่มฝากวันที่ 22 พฤศจิกายน 2536 ครบกำหนดวันที่ 22 พฤศจิกายน 2538 และได้ทำการถอนเพื่อฝากต่อเมื่อเงินฝากที่กล่าวครบกำหนด ปรากฏว่าดอกเบี้ยจ่ายที่ได้จากการคำนวณของโปรแกรมเท่ากับ 82,225.51 บาท แต่จากการคำนวณด้วยวิธี Manual ได้เท่ากับ 69,000.00 บาท ซึ่งเป็นจำนวนที่ถูกต้อง

ข้อแนะนำ

องค์กรควรดำเนินการปรับปรุงแก้ไขโปรแกรมให้คำนวณดอกเบี้ยถูกต้อง

(25) โปรแกรมที่ใช้ในการประมวลผลข้อมูลและพิมพ์เป็นรายงาน

บางส่วนทำงานไม่ถูกต้อง

- โปรแกรมที่ใช้ในการประมวลผลข้อมูลและพิมพ์รายงานยอดคงเหลือเฉพาะบัญชีที่เคลื่อนไหวประจำวันของเงินฝากประจำ ไม่ได้แสดงบัญชีที่เคลื่อนไหวในวันที่ทดสอบ 1 บัญชี จำนวนเงิน 300,000.00 บาท ซึ่งบัญชีนี้ไม่มีแสดงในรายงานการเคลื่อนไหวสลิปทุกประเภท ทำให้รายงานความคลาดเคลื่อนจากความเป็นจริง

- โปรแกรมที่ใช้ในการประมวลผลข้อมูลและพิมพ์รายงานรายละเอียดเงินฝากประจำและรายงานเงินฝากแยกตามประเภทผู้ฝากของเงินฝากประจำ ทำงานไม่ถูกต้อง กล่าวคือ รายงานทั้ง 2 แสดงยอดรวมเงินฝากประจำไม่ถูกต้อง

ข้อแนะนำ

องค์กรควรได้ดำเนินการปรับปรุงแก้ไขปัญหาดังกล่าวให้ถูกต้อง

(26) การป้อนชื่อบัญชีลูกค้า

จากการตรวจสอบพบว่ามีบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา บางบัญชียังมิได้บันทึกชื่อลูกค้าทำให้ไม่สามารถตรวจสอบควบคุมและยืนยันชื่อลูกค้าได้

ข้อแนะนำ

ควรกำหนดให้ผู้ปฏิบัติงาน ENTER NEW ACCT. NAME ในวันที่ทำรายการเปิดบัญชีและมีการตรวจสอบรายงาน Daily New Account กับรายงาน List Master ทุกสิ้นเดือน เพื่อป้องกันการหลงลืมใส่ชื่อลูกค้าเป็นเวลานาน และกำหนดให้มีการตรวจสอบชื่อบัญชีลูกค้าก่อนทำรายการ

(27) การควบคุมการประมวลผลข้อมูล

การทำรายการบางรายการ เช่น การถอนเงินบางส่วน (PARTIAL WITHDRAW) จากบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลาที่เป็นใบรับฝาก และการทำรายการถอนเงินโดยไม่ใช้สมุดคู่ฝาก (CASH WITHDRAW NO BOOK) ระบบยอมให้ผ่านได้โดยการอนุมัติด้วยบัตรของผู้ช่วยผู้ควบคุม (ASC. SUP. CARD) ซึ่งปกติองค์กรจะไม่ยอมให้ลูกค้าถอนเงินโดยไม่ใช้สมุดคู่ฝาก

ข้อแนะนำ

ควรมีมาตรการที่เหมาะสมเพื่อควบคุมหรือป้องกันการถอนเงินบางส่วนจากบัญชีเงินฝากประจำที่เป็นใบรับฝาก เพื่อให้สอดคล้องกับระเบียบปฏิบัติขององค์กร

(28) **รายงานแสดงข้อมูลคลาดเคลื่อน**

รายงาน Daily Transaction - Miscellaneous แสดง CODE ADJUST ไม่ตรงกับที่ทำรายการจริง รายงานดังกล่าวจะแสดง CODE ADJUST เป็นศูนย์เสมอ ไม่ว่า CODE ADJUST ที่ใช้จริงจะเป็น 1 หรือ 2 ทำให้ผู้ใช้รายงานไม่สามารถควบคุมและเช็คสอบได้ว่าเป็นการทำรายการปรับปรุงเพิ่มหรือลดจำนวนดอกเบี้ย

CODE ADJUST นี้ มีผลต่อการคำนวณดอกเบี้ยคงเหลือคือ 1 จะเป็นการเพิ่มยอดดอกเบี้ยที่เคยจ่ายให้ลูกค้า ทำให้ยอดดอกเบี้ยคงเหลือลดลง และถ้าใส่ 2 จะเป็นการลดยอดดอกเบี้ยที่เคยจ่ายให้ลูกค้า ทำให้ยอดดอกเบี้ยคงเหลือเพิ่มขึ้น

ข้อแนะนำ

ควรแก้ไขให้รายงานดังกล่าวแสดง CODE ADJUST ของรายการ ADJUST INTEREST ให้ตรงกับ CODE ADJUST ที่ทำรายการจริง เพื่อให้รายงานมีความถูกต้องและสามารถใช้ควบคุมและเช็คสอบได้

(29) **รายงานเกี่ยวกับการทำรายการต่างสาขา (INTER-BRANCH REPORT) ของระบบงานเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา**

การทำรายการ เพื่อถอนเงินจากยอดฝากเพียงบางส่วน (PARTIAL WITHDRAW) และรายการเพื่อทำรายการฝากย้อนหลังโดยการโอนและไม่ใช้สมุดคู่ฝาก (BACK DATE TRANSFER DEPOSIT NO BOOK) ไม่แสดงยอดการทำรายการในรายงานการทำรายการต่างสาขา ต่อไปนี้

- Daily Inter-Branch Transactions Summary For Branch ที่สั่งให้สาขาเจ้าของบัญชี
- Daily Inter-Branch Summary For Accounting ที่ส่งให้ฝ่ายบัญชี
- Daily Inter-Branch Transactions For Other Branch ที่สั่งให้สาขาที่ทำรายการแทนสาขาเจ้าของบัญชี และ
- Daily Inter-Branch Transaction By Other Branches ที่ส่งให้สาขาเจ้าของบัญชี

ทำให้การกระทบยอดการทำรายการโดยสาขาอื่นที่ไม่ใช้เจ้าของบัญชีไม่ถูกต้อง และการบันทึกระหว่างสาขาผิดพลาดได้

ข้อแนะนำ

หากองค์กรจะให้บริการฝาก-ถอนต่างสาขา (INTER-BRANCH) ระบบงานเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา องค์กรควรแก้ไขรายงาน

- Daily Inter-Branch Transactions Summary For Branch
- Daily Inter-Branch Summary For Accounting
- Daily Inter-Branch Transactions For Other Branch
- Daily Inter-Branch Transactions By Other Branch

ให้แสดงยอดการทำรายการเพื่อถอนเงินจากยอดฝากเพียงบางส่วน และการทำรายการฝากย้อนหลังโดยการโอนและไม่ใช้สมุดคู่ฝากและรายงาน Daily Fixed Deposit Transactions ที่ส่งให้สาขาเจ้าของบัญชีควรแก้ไขให้แสดงยอดรวมของรายการที่สาขาเจ้าของบัญชีทำเอง และยอดรวมของรายการที่สาขาอื่นทำแทนเพื่อการสอบยันยอดจำนวนรายการและจำนวนเงินระหว่างสาขาผู้ทำรายการแทนและสาขาเจ้าของบัญชี

(30) การควบคุมการเปลี่ยนแปลงที่อยู่ผู้ฝากเงินไม่เหมาะสม

เมื่อลูกค้าเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา แจ้งการเปลี่ยนแปลงแก้ไขที่อยู่ (Address) ให้ทางองค์กรทราบ องค์กรจะบันทึกการเปลี่ยนแปลงแก้ไขที่อยู่ในสมุดจดบันทึก โดยมิได้ทำการเปลี่ยนแปลงที่อยู่ซึ่งเก็บในระบบงานคอมพิวเตอร์

ข้อแนะนำ

องค์กรควรกำหนดระเบียบให้พนักงานต้องทำการแก้ไขเปลี่ยนแปลงที่อยู่ของลูกค้าให้ถูกต้องตรงกันและควรกำหนดให้มีการออกรายงานที่แสดงรายละเอียดการแก้ไขเปลี่ยนแปลงที่อยู่ของลูกค้าเพื่อให้ผู้ที่เกี่ยวข้องทราบ

2.3 ระบบเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน (ATM)

(1) ไม่ทำรายการ Balance inquiry ประกอบการอนุมัติขอมีบัตร ATM

หน่วยเงินฝากออมทรัพย์ สำนักงานใหญ่ ไม่ทำรายการ Balance inquiry แนบมาพร้อมกับแบบฟอร์มคำขอใช้บริการ ATM ของลูกค้าให้ส่วนเอทีเอ็ม เพื่อตรวจสอบชื่อและเลขที่บัญชีให้แน่ใจอีกครั้งหนึ่งว่าเป็นชื่อเดียวกับเจ้าของบัญชีที่จะใช้บริการ ATM

ข้อแนะนำ

ควรกำชับให้พนักงานหน่วยเงินฝากออมทรัพย์ สำนักงานใหญ่ทำรายการ Balance inquiry ข้อมูลบัญชีลูกค้าแนบพร้อมกับแบบฟอร์มคำขอใช้บริการ ATM ของลูกค้าให้ส่วนเอทีเอ็มเพื่อตรวจสอบชื่อ และเลขที่บัญชีให้แน่ใจอีกครั้งว่า เป็นชื่อเดียวกับเจ้าของบัญชีที่จะใช้บริการ ATM

(2) ไม่ลงลายมือชื่อผู้อนุมัติในสมุดทะเบียน ATM

ผู้จ่ายรหัสประจำตัวลูกค้าไม่ลงนามอนุมัติในช่อง "ผู้อนุมัติ" ในสมุดทะเบียน ATM แต่ลงลายมือชื่อในรายงานการออกบัตรและรายงานการออกรหัสแทน ทำให้การใช้ประโยชน์จากสมุดทะเบียน ATM น้อยลงและอาจก่อให้เกิดปัญหาในภายหลังได้

ข้อแนะนำ

องค์กรควรพิจารณาปรับปรุงว่าควรใช้สมุดทะเบียน ATM หรือรายงานที่ได้จากเครื่องคอมพิวเตอร์อย่างใดอย่างหนึ่ง เป็นทะเบียนควบคุมการจ่ายรหัสประจำตัวลูกค้าเท่านั้น

(3) ไม่จัดทำทะเบียนคุมเทปข้อมูลออกบัตรและเทปข้อมูลออกรหัสประจำตัว

ส่วนเอทีเอ็มมิได้จัดทำทะเบียนคุมเทปข้อมูลออกบัตรและเทปข้อมูลออกรหัสประจำตัวผู้ใช้บริการ ATM ทำให้ไม่ทราบจำนวนม้วนเทปที่มีอยู่ จำนวนที่ใช้งานอยู่จริงในแต่ละวัน หรือจำนวนม้วนเทปที่รอเพื่อการใช้งานต่อไป

ข้อแนะนำ

องค์กรควรจัดทำทะเบียนคุมเทปข้อมูลที่ใช้งานอยู่ในระบบ ATM

(4) ไม่มีส่วนงานอื่นร่วมกับส่วนเอทีเอ็มในการจัดทำบัตร ATM

การควบคุมการจัดทำบัตร ATM ยังไม่สอดคล้องกับหลักการควบคุมภายในที่ดีโดยยินยอมให้ส่วนเอทีเอ็มเพียงลำพังเท่านั้น ดำเนินการนำเทปข้อมูลเพื่อออกบัตร และบัตรเปล่า ไปพิมพ์ชื่อและใส่รหัสบนแถบแม่เหล็ก โดยไม่มีพนักงานจากหน่วยงานอื่นร่วมเป็นกรรมการควบคุมดูแลด้วย

ข้อแนะนำ

ควรมีพนักงานของหน่วยงานอื่นนอกจากพนักงานของส่วนเอทีเอ็ม ร่วมเป็นกรรมการควบคุมดูแลการจัดทำบัตร ATM

(5) การจัดทำรหัสประจำตัวลูกค้า (PIN Code)

ธนาคารไม่ได้เก็บรักษาโปรแกรมและตัวเลขลับสำหรับการคำนวณสร้าง PIN Code ให้แก่ลูกค้าเพื่อเป็นรหัสประกอบการใช้บัตร ATM ในการถอนเงินอย่างรัดกุม โดยเก็บไว้ในเครื่องคอมพิวเตอร์ตลอดเวลา และมีผู้รู้รหัสลับ (Password) สำหรับการเรียกโปรแกรมมาใช้งาน 2 คน อาจเป็นจุดอ่อนต่อการควบคุม และก่อให้เกิดความเสียหายต่อลูกค้าขององค์กรได้ หากมีบุคคลอื่นรู้รหัสลับและเรียกโปรแกรมดังกล่าวมาคำนวณสร้าง PIN Code ของลูกค้าโดยมิได้รับอนุญาตจากองค์กร

ข้อแนะนำ

1) องค์กรควรแยกเก็บโปรแกรมและตัวเลขลับสำหรับคำนวณสร้าง PIN Code ไว้นอกเครื่องคอมพิวเตอร์ โดยมอบหมายให้พนักงานระดับบริหารเป็นผู้รับผิดชอบในการเก็บรักษา และจัดทำทะเบียนบันทึกเวลาที่นำออกใช้งานและเวลาที่เสร็จสิ้นในการปฏิบัติงาน

2) องค์กรควรล้างโปรแกรมและตัวเลขลับสำหรับการคำนวณสร้าง PIN code ออกจากระบบคอมพิวพ์เตอร์ทุกครั้งที่เลิกใช้งาน ตลอดจนควบคุมในเรื่องเอกสารหลักฐานอื่นที่ใช้ประกอบการจัดทำ PIN Code เช่น กระดาษพิมพ์ และกระดาษคาร์บอน เป็นต้น

(6) การควบคุมด้านหลังของตัวเครื่อง CD

องค์กรไม่ได้ควบคุมการเข้าถึงด้านหลังของเครื่อง ATM ที่ติดตั้งอยู่ในห้องโดยรัดกุม ระหว่างเวลาทำการ ประตูหลังของห้องเครื่องเปิดทิ้งไว้ตลอดเวลาโดยไม่มีคนดูแล อาจก่อให้เกิดความเสียหายต่อองค์กรหากมีบุคคลอื่นเข้าถึงตัวเครื่องได้ เนื่องจากเครื่อง ATM มีขนาดเล็กและง่ายต่อการใช้วิธีการทำลายเพื่อชิงเงินสดที่เก็บอยู่ในเครื่อง

ข้อแนะนำ

องค์กรควรออกระเบียบปฏิบัติสำหรับการเข้าห้องที่ติดตั้งเครื่อง ATM ในการเปลี่ยนกล่องเงินหรือกระดาษพิมพ์ และกำชับให้พนักงานผู้รับผิดชอบควบคุมดูแลให้ปฏิบัติตามระเบียบโดยเคร่งครัด โดยประตูทางเข้าควรปิดกุญแจไว้ตลอดเวลา เพื่อป้องกันความเสียหายที่อาจเกิดจากบุคคลที่ไม่ได้รับอนุญาตเข้าถึงตัวเครื่องได้ง่าย

(7) ไม่มีหลักฐานแสดงการรับรองความถูกต้องของข้อมูล

หลังจากที่ศูนย์บริหาร ATM ดำเนินการตรวจสอบความถูกต้องของข้อมูลใน Edit Report ที่ฝ่ายคอมพิวเตอร์ให้แล้ว ศูนย์บริหาร ATM จะแจ้งผลการตรวจสอบความถูกต้องของข้อมูลให้ฝ่ายคอมพิวเตอร์ทราบทางโทรศัพท์ ไม่ได้จัดทำเอกสารรับรองความถูกต้องของข้อมูลไว้เป็นหลักฐาน

ข้อแนะนำ

เมื่อศูนย์บริหาร ATM ตรวจสอบความถูกต้องของข้อมูลใน Edit Repot ที่ฝ่ายคอมพิวเตอร์พิมพ์ให้เสร็จเรียบร้อยแล้ว ควรจัดทำเอกสารรับรองความถูกต้องของข้อมูลแจ้งให้ฝ่ายคอมพิวเตอร์ทราบทุกครั้ง

(8) ไม่มีรายงานการเปลี่ยนแปลงแก้ไขข้อมูลลูกค้า

ศูนย์บริหาร ATM ไม่ได้บันทึกการทำรายการเปลี่ยนแปลงแก้ไขข้อมูลของลูกค้า เพื่อใช้เป็นหลักฐานในการตรวจสอบและติดตามรายการแก้ไขต่าง ๆ คงมีแต่รายงาน ATM Card – Holder Maintenance Report ซึ่งเป็นรายงานที่แสดงรายละเอียดเฉพาะข้อมูลที่ได้แก้ไขใหม่แล้วเท่านั้น ไม่มีข้อมูลเก่าก่อนถูกแก้ไขแสดงไว้โดยละเอียด

ข้อแนะนำ

ควรกำหนดให้มีรายงานที่แสดงข้อมูลก่อนและหลังการแก้ไขข้อมูลในระบบงาน ATM

(9) ไม่มีการจดบันทึกรหัสของคณะกรรมการ PIN เก็บไว้ที่อื่นต่างหาก

รหัสของคณะกรรมการ PIN เป็นตัวเลขสำคัญที่ใช้ในการคำนวณรหัสประจำตัวถือบัตร ATM ซึ่งในปัจจุบันเก็บในแผ่น Diskette 2 ชุด โดยสำรองเป็น Back up ไว้ 1 ชุด หากแผ่น Diskette ชุดจริงและชุดสำรองเสียหรือชำรุดไปทั้งคู่ จะก่อให้เกิดความเสียหายไม่สามารถออกรหัสประจำตัวผู้ถือบัตร ATM ให้ลูกค้าได้ เพราะคณะกรรมการ PIN อาจจำรหัสไม่ได้และไม่มีการจดบันทึกไว้ที่อื่น

ข้อแนะนำ

เพื่อป้องกันปัญหาในการออกรหัสประจำตัวผู้ถือบัตร ATM ควรกำหนดให้กรรมการจดบันทึกตัวเลขที่ใช้ในการคำนวณรหัสประจำตัวผู้ถือบัตร ATM ลงในเอกสารลับและเก็บไว้ในที่ปลอดภัย

(10) การเก็บรักษาบัตรเปล่าและการจัดทำบัตร ATM ไม่รัดกุมเท่าที่ควร

การเก็บรักษาบัตรเปล่าและการควบคุมการจัดทำบัตร ATM ยังไม่สอดคล้องกับหลักการควบคุมภายในที่ดี โดยยินยอมให้ศูนย์บริหาร ATM เป็นผู้เก็บรักษาบัตรเปล่า ดำเนินการจัดทำบัตร ATM และแก้ไขข้อผิดพลาดในการผลิต ด้วยการทำบัตร ATM ซ้ำทดแทนบัตร ATM ชำรุดเสียหายได้โดยลำพังไม่มีหน่วยงานอื่นร่วมเป็นกรรมการควบคุมดูแลการเก็บรักษาบัตรเปล่าและการจัดทำบัตร ATM โดยใกล้ชิด

(11) มีการออกบัตร ATM ให้ลูกค้าผิดบัญชี

วิธีการควบคุมเพื่อป้องกันการออกบัตร ATM ให้ลูกค้าผิดบัญชียังไม่ได้ผลเท่าที่ควร จึงมีการออกบัตร ATM ให้ลูกค้าผิดบัญชี

(12) การบรรจุธนบัตรลงกล่องจ่ายเงินไม่รัดกุมเท่าที่ควร

ระบบป้องกันข้อผิดพลาดในการบรรจุธนบัตรลงกล่องจ่ายเงิน และระบบป้องกันการใส่กล่องจ่ายเงินแต่ละชนิดสลับตำแหน่งในเครื่อง ATM ยังมีจุดอ่อนบางประการ ผู้ปฏิบัติงานสามารถบรรจุธนบัตรชนิด 500.00 บาท และชนิด 100.00 บาท สลับกล่องกันได้ นอกจากนี้ การบรรจุกล่องจ่ายเงินเข้าเครื่อง ATM ก็สามารถสลับตำแหน่งระหว่างกล่องธนบัตรชนิด 500.00 บาท และชนิด 100.00 บาทได้

ข้อแนะนำ

1) ควรมีพนักงานชั้นบริหารของหน่วยงานอื่นนอกเหนือจากพนักงานของศูนย์บริหาร ATM ร่วมเป็นกรรมการควบคุมดูแลการเก็บรักษาบัตรเปล่าและการจัดทำบัตร ATM โดยใกล้ชิด

2) ควรกำหนดให้มีการตรวจนับบัตรเปล่า บัตร ATM ที่ลูกค้ายังไม่มารับ และซองเอกสารรหัสประจำตัวผู้ถือบัตร ATM เพื่อตรวจสอบความถูกต้องและครบถ้วนเป็นครั้งคราว

(13) มีการหยุดให้บริการ ATM ในเวลาทำการ

ในระหว่างวันหยุดทำการ เช่น วันเสาร์และวันอาทิตย์ เครื่อง ATM จะจ่ายเงินจนหมดกล่องที่ใช้บรรจุ แล้วก็จะปิดเครื่องเองโดยอัตโนมัติ ซึ่งองค์กรจะไม่บรรจุเงินหรือเพิ่มเงินเข้าไปอีกจนกว่าจะถึงวันเปิดทำการตามปกติทำให้ลูกค้าไม่สามารถจะใช้บริการของเครื่อง ATM ต่อไปได้

ข้อแนะนำ

ควรปรับปรุงแก้ไขปัญหาหรืออุปสรรคที่มีผลกระทบต่อการให้บริการ ATM อย่างจริงจังเพื่อให้การบริการ ATM เป็นไปอย่างต่อเนื่อง

(14) การใช้เครื่อง ATM ผิดประเภท

เครื่อง ATM ชนิดที่ผู้ผลิตออกแบบมาให้ติดตั้งภายในอาคารสำนักงาน (ชนิด Lobby) ซึ่งองค์กรนำไปติดตั้งตามสำนักงานสาขาต่าง ๆ แทนแบบ Through the wall นั้น ค่อนข้างบอบบางไม่มั่นคงแข็งแรงเท่าที่ควร อาจมีปัญหาในการรักษาความปลอดภัย

ข้อแนะนำ

ควรเพิ่มมาตรการรักษาความปลอดภัยในบริเวณที่ตั้งเครื่อง ATM ชนิด Lobby ซึ่งองค์กรนำไปติดตั้งที่สาขาแบบ Through the wall ให้สามารถชดเชยจุดอ่อนในการรักษาความปลอดภัยได้ตามควรแก่กรณี

(15) การพิมพ์เลขที่บัตร ATM จริงลงในบัตรบันทึกรายการ (Transaction Record) เป็นวิธีที่ไม่ปลอดภัยต่อลูกค้า

ในการทำรายการฝากถอนเงินผ่านเครื่อง ATM ลูกค้าจะได้รับบัตรบันทึกรายการ ซึ่งได้พิมพ์เลขที่บัตร ATM จริง ไว้เป็นหลักฐาน แต่ลูกค้าส่วนใหญ่มักทิ้งไว้ในบริเวณที่ตั้งเครื่องประกอบกับอุปกรณ์ที่เป็นแป้นกดข้อมูลของเครื่อง ATM ในเครือข่าย ไม่มีผนังหรือฝาครอบป้องกันผู้อื่น มองเห็นรหัสลับประจำตัวลูกค้า (PIN) อาจทำให้ผู้ที่มีความรู้และอุปกรณ์ในการทำบัตรสามารถจดจำ PIN ที่มองเห็นจากด้านหลังของลูกค้า และนำเลขที่บัตร ATM ในบัตรบันทึกรายการไปทำบัตร ATM ปลอมแล้วใช้ถอนเงินจากบัญชีลูกค้าได้ ซึ่งนอกจากจะเกิดผลเสียหายต่อลูกค้าแล้ว ยังกระทบต่อความเชื่อถือที่ลูกค้ามีต่อองค์กรด้วย

ข้อแนะนำ

ควรพิจารณาจัดพิมพ์รหัสอ้างอิงอื่นแทนเลขที่บัตร ATM จริง ลงในบัตรบันทึกรายการ (Transaction Record) ที่ลูกค้าได้รับจากการทำรายการผ่านเครื่อง ATM

(16) ฝ่ายตรวจสอบภายในเข้าร่วมกระบวนการจัดทำรหัสลับประจำตัวลูกค้า (PIN) ในขอบเขตที่จำกัด

ฝ่ายตรวจสอบภายในมีส่วนร่วมในการจัดทำ PIN ซึ่งจะจัดเตรียมไว้ครั้งละเป็นจำนวนมาก โดยการลงลายมือชื่อรับรองลงในซองเก็บแผ่น Diskette ที่เป็น Master Key ก่อนนำไป load เข้าระบบเท่านั้น โดยมิได้อยู่ร่วมสังเกตการณ์การทำลายใบปะหน้าใบแจ้งรหัสความปลอดภัย และความเหมาะสมในการจัดเก็บใบแจ้งรหัสจนครบกระบวนการ

ข้อแนะนำ

หลังจากตัวแทนฝ่ายตรวจสอบภายใน ตรวจสอบและสังเกตการณ์การจัดทำใบแจ้งรหัสประจำตัวลูกค้าทุกขั้นตอนแล้ว ควรให้ลงลายมือชื่อกำกับในเอกสารแสดงรายละเอียดการจัดทำใบแจ้งรหัสที่ส่วนบริการอิเล็กทรอนิกส์จัดทำไว้ด้วยทุกครั้ง

(17) **ไม่มีหลักฐานแสดงการรับรองความถูกต้องของข้อมูลการขอมีบัตร ATM ที่บันทึกในแผ่น Diskette**

เมื่อหน่วยบริหารบัตรได้ดำเนินการตรวจสอบความถูกต้องของข้อมูลการขอมีบัตร ATM ที่บันทึกใน Diskette จากรายงาน New Customer ATM Report แล้ว ไม่ได้ส่งหลักฐานรับรองความถูกต้องของข้อมูลเป็นลายลักษณ์อักษรให้ส่วนปฏิบัติการคอมพิวเตอร์ เพื่อให้นำข้อมูลใน Diskette ไปดำเนินการในขั้นตอนต่อไปได้

ข้อแนะนำ

หลังจากหน่วยบริหารบัตร ตรวจสอบความถูกต้องของการบันทึกข้อมูลแล้ว ควรจัดทำเอกสารรับรองความถูกต้องของข้อมูลให้ส่วนงานที่เกี่ยวข้อง

(18) **ไม่มีการควบคุมการจ่ายบัตร ATM และรหัสลับประจำตัวลูกค้าเท่าที่ควร**

จากการตรวจสอบทะเบียนการจ่ายบัตร ATM ประกอบการสอบถามพนักงาน ปรากฏว่าการควบคุมการจ่ายบัตร ATM และใบแจ้งรหัสลับประจำตัวลูกค้าของฝ่ายการธนาคารยังไม่รัดกุมเท่าที่ควรกล่าวคือ

1) ไม่มีการกำหนดตัวบุคคลผู้รับผิดชอบในการจ่ายบัตร ATM เช่นเดียวกับรหัสลับประจำตัวลูกค้า ซึ่งมอบหมายให้ผู้อำนวยการฝ่ายการธนาคารเป็นผู้จ่ายแล้ว

2) พนักงานที่จ่ายบัตร ATM และใบแจ้งรหัสลับประจำตัวลูกค้า ไม่ได้กรอกข้อมูลเกี่ยวกับหลักฐานผู้รับบัตร เช่น เลขที่บัตรประจำตัวประชาชน ในทะเบียนการจ่ายบัตร ATM หรือทะเบียนการจ่ายรหัสประจำตัวลูกค้า ซึ่งอาจจะเป็นการจ่ายบัตรโดยขาดการตรวจสอบหลักฐานของผู้รับ

3) ผู้ที่รับผิดชอบและผู้ที่ทำหน้าที่แทนในการจ่ายบัตรหรือรหัสดังกล่าว ลงลายมือชื่อผู้จ่ายในทะเบียนไม่ครบถ้วน

การละเลยการควบคุมในเรื่องดังกล่าว อาจทำให้เกิดความผิดพลาดในการจ่ายบัตรและรหัสประจำตัวลูกค้า โดยไม่สามารถระบุด้วยบุคคลที่รับผิดชอบได้

ข้อแนะนำ

ควรกำชับให้สำนักงานต่าง ๆ จำกัดจำนวนพนักงานที่ทำหน้าที่จ่ายบัตร ATM และให้พนักงานกรอกข้อมูลและลงลายมือชื่อในทะเบียน เพื่อเป็นหลักฐานในการปฏิบัติงานทุกครั้ง

(19) **การทำรายการอนุญาตให้บัตร ATM ใช้กับบัญชีเงินฝากได้ก่อนที่ลูกค้ามารับบัตร เป็นวิธีปฏิบัติที่ไม่เหมาะสม**

การที่องค์กรทำรายการอนุญาตให้บัญชีลูกค้าที่ขอมีบัตรทุกบัญชีใช้บัตร ATM ได้ทันทีโดยการป้อน Message เฉพาะหลังจากได้รับรายงาน ATM New Customer Reference Account ซึ่งเป็นเวลาก่อนที่ลูกค้าจะได้รับบัตรจริง อาจก่อให้เกิดความเสียหายต่อลูกค้าและองค์กรได้

ข้อแนะนำ

ควรกำหนดให้ทำรายการอนุญาตให้บัญชีลูกค้าใช้บริการ ATM ได้ หลังจากลูกค้ามารับบัตรแล้ว

(20) การจัดเก็บบัตร ATM และรหัสประจำตัวลูกค้า ไม่ปลอดภัยเท่าที่ควร

การที่ฝ่ายการธนาคารจัดเก็บใบแจ้งรหัสประจำตัวลูกค้าไว้ในตู้เก็บเอกสารห้องผู้อำนวยการฝ่าย ฯ และใช้ตู้เก็บเอกสารอื่น ๆ ในการเก็บบัตร ATM โดยไม่ได้ปิดกุญแจตู้ในระหว่างวันเป็นการเปิดโอกาสให้พนักงานอื่นที่ไม่มีหน้าที่เกี่ยวข้องสามารถเข้าถึงบัตร ATM หรือใบแจ้งรหัสลับประจำตัวลูกค้าได้ ซึ่งอาจก่อให้เกิดความเสียหายต่อลูกค้าและองค์กรได้

ข้อแนะนำ

ควรจัดเก็บบัตร ATM แยกต่างหากจากเอกสารอื่น และปิดกุญแจตู้ที่เก็บบัตรตลอดเวลาโดยมอบหมายให้พนักงานชั้นบริหารเป็นผู้ถือกุญแจดังกล่าว

(21) วิธีการจัดทำทะเบียนคุมบัตร ATM ที่เครื่องยึดไว้ไม่ได้ประโยชน์เท่าที่ควร

ฝ่ายการธนาคารไม่ได้บันทึกรายละเอียดบัตรที่ถูกยึดทุกรายที่ได้รับจากส่วนบริการอิเล็กทรอนิกส์และตู้ ATM โดยบันทึกรายละเอียดบัตรที่ถูกยึดเฉพาะรายที่ลูกค้ามารับบัตรคืนไปแล้วเท่านั้นทำให้ทะเบียนดังกล่าวใช้เป็นหลักฐานแสดงการรับบัตรของลูกค้าเท่านั้น ไม่สามารถใช้ประโยชน์ในการควบคุมและตรวจสอบความถูกต้องและจำนวนบัตรยึดที่ยังไม่มีลูกค้ามารับได้ ทั้งนี้เนื่องจากองค์กรไม่ได้กำหนดรูปแบบทะเบียนและวิธีปฏิบัติเกี่ยวกับการควบคุมบัตร ATM ที่เครื่องยึดไว้จากลูกค้าในบางกรณีทำให้การปฏิบัติในแต่ละสำนักงานไม่เป็นมาตรฐานเดียวกัน และอาจไม่รัดกุม

ข้อแนะนำ

ควรกำหนดรูปแบบและวิธีปฏิบัติในการจัดทำทะเบียนต่าง ๆ ให้สามารถใช้ควบคุมจำนวนบัตรยึดที่ลูกค้ายังไม่ได้มารับ เพื่อให้การปฏิบัติงานเกี่ยวกับบัตรที่ถูกยึดเป็นไปอย่างรัดกุมและเป็นมาตรฐานเดียวกันทุกสำนักงาน

(22) ไม่มีหลักฐานแสดงว่าได้ตรวจสอบและกระทบยอดความถูกต้องของรายงานทางการเงิน

พนักงานส่วนเงินฝาก ฝ่ายการธนาคาร ที่ทำหน้าที่ตรวจสอบและกระทบยอดรายงานทางการเงินที่ได้รับจากสำนักคอมพิวเตอร์ ไม่ได้ลงลายมือชื่อกำกับไว้ในรายงาน ทำให้ขาดหลักฐานที่แสดงว่ารายงานเหล่านั้นได้ผ่านการตรวจสอบแล้ว

ข้อแนะนำ

ควรกำหนดให้พนักงานที่ทำหน้าที่ตรวจสอบรายงานต่าง ๆ ลงลายมือชื่อกำกับไว้ในตอนท้ายของรายงานเหล่านั้น หลังจากได้ตรวจสอบและกระทบยอดรายงานแล้ว

(23) **ไม่มีการตรวจสอบความถูกต้องของค่าธรรมเนียมที่บริษัทกลางเรียกเก็บและค่าธรรมเนียม (สุทธิ) ที่รับจ่ายระหว่างองค์กร**

ฝ่ายการธนาคารใช้ข้อมูลจากรายงานประจำเดือนของบริษัทกลาง ในการจ่ายหรือรับค่าธรรมเนียมการใช้บริการรับส่งข้อมูลในระบบ ATM แก่บริษัทกลาง และองค์กรอื่นในเครือข่าย โดยมิได้ตรวจสอบความถูกต้องก่อน เนื่องจากไม่สามารถใช้ประโยชน์จากรายงานประจำเดือนขององค์กรที่ได้รับจากสำนักคอมพิวเตอร์ในการกระทบยอดได้ และไม่ได้มีการรวบรวมจำนวนการทำรายการระหว่างกันไว้ซึ่งจากการทดสอบโดยรวบรวมจำนวนรายการจากรายงานที่ยืนยันยอดที่ถูกต้อง กระทบยอดกับรายงานของบริษัทกลางแล้ว ปรากฏว่ามีจำนวนคลาดเคลื่อนกันบ้างเล็กน้อย

ข้อแนะนำ

ควรจัดให้มีการรวบรวมจำนวนรายการที่ทำผ่านบริษัทกลาง และรายการระหว่างองค์กรในเครือข่ายจากรายงานประจำวันที่ได้มีการพิสูจน์ยอดแล้ว กระทบยอดกับจำนวนรายการที่บริษัทกลาง และองค์กรอื่นในเครือข่ายใช้เรียกเก็บค่าธรรมเนียม

(24) **ขอบเขตการตรวจสอบงานที่เกี่ยวข้องกับระบบ ATM ยังไม่เพียงพอ**

ฝ่ายตรวจสอบภายในยังไม่ได้ตรวจสอบงานที่เกี่ยวข้องกับระบบเงินโอนทางอิเล็กทรอนิกส์ ในบางด้านเป็นครั้งคราว ไม่เป็นไปตามเงื่อนไขการอนุญาตเปิดบริการ ATM นอกเวลาทำการ เช่น ความครบถ้วนและเป็นปัจจุบันของเอกสารประกอบระบบงานและคู่มือปฏิบัติงาน การตรวจนับบัตรเปล่าที่ยังไม่ได้บันทึกข้อมูล การควบคุมการเตรียมข้อมูลการขอมีบัตร ATM เป็นต้น

ข้อแนะนำ

ควรเพิ่มขอบเขตการตรวจสอบภายในให้ครอบคลุมงานด้านคอมพิวเตอร์ เพื่อให้เป็นไปตามเงื่อนไขในการอนุญาตให้เปิดบริการเครื่อง ATM

(25) **การแบ่งแยกหน้าที่ไม่เหมาะสม**

องค์กรได้มอบหมายให้พนักงานกลุ่มเดียวกันปฏิบัติหน้าที่และรับผิดชอบในการจัดทำรหัสลับประจำตัวลูกค้า (PIN) การจัดทำบัตรประจำตัวลูกค้า (ATM Card) และการควบคุมข่ายงานผ่านทาง ATM Console ทำให้ขาดการแบ่งแยกหน้าที่ดังกล่าว

ข้อแนะนำ

องค์กรควรแบ่งงานที่มีความสำคัญออกจากกัน เช่น งานที่เปิดโอกาสให้เจ้าหน้าที่เข้าถึง PIN และบัตรได้ โดยมอบหมายให้พนักงานแต่ละคนรับผิดชอบ และสำหรับงานที่มีความสำคัญรองลงมาอาจมอบหมายให้บุคคลหนึ่ง ๆ รับผิดชอบได้หลายงาน แต่ผู้บริหารจำเป็นต้องสอบทานงานดังกล่าวโดยรัดกุม และควรมีการสับเปลี่ยนหน้าที่ของพนักงานเป็นครั้งคราว ทั้งนี้ เพื่อควบคุมการปฏิบัติงานดังกล่าวให้ถูกต้องรัดกุมต่อไป

(26) **การควบคุมการใช้โปรแกรมและแฟ้มข้อมูลไม่รัดกุม**

ปัจจุบันโปรแกรมเมอร์ของระบบงาน ATM ทั้ง 2 คน ทราบทั้ง A-KEY และ E-PIN KEY ซึ่ง E-PIN KEY นี้สามารถที่จะถอดรหัสด้วย A-KEY ได้ โดยผ่านสูตรการคำนวณชื่อ DES ออกมาเป็น PIN ของผู้บริหารที่ใช้ในการทำ PIN ให้ลูกค้า ขณะเดียวกันโปรแกรมเมอร์สามารถเข้าถึงสูตรการคำนวณ DES แฟ้มข้อมูลผู้ถือบัตร (CARD HOLDER FILE) และโปรแกรมการสร้าง PIN ได้ ทำให้สามารถคำนวณ PIN ของลูกค้ารายที่ต้องการทราบได้

ข้อแนะนำ

องค์กรควรกำหนดให้ผู้มีสิทธิทราบ A-KEY และ E-PIN KEY เป็นคนละคนกันและให้เก็บรักษาให้รัดกุม ขณะเดียวกันควรมีการควบคุมการเรียกใช้โปรแกรมการสร้าง PIN และสูตรการคำนวณ DES และแฟ้มข้อมูลของลูกค้า เพื่อป้องกันการนำไปใช้งานโดยไม่ได้รับอนุญาต

(27) **การควบคุมการจ่ายบัตรและ PIN**

ในการจ่ายบัตรและ PIN ให้แก่ลูกค้าขององค์กรยังมีข้อสังเกตดังนี้คือ

1) การนำบัตรและ PIN ไปจ่ายให้แก่ลูกค้านอกองค์กร โดยให้พนักงานเพียงคนเดียวเป็นผู้รับผิดชอบ บางครั้งลูกค้าเป็นพนักงานบริษัทที่นำเงินเดือนเข้าบัญชี ปรากฏว่า สมุหบัญชีของบริษัทดังกล่าวลงลายมือชื่อรับ PIN และบัตรแทนพนักงานทั้งหมด

2) การจ่ายบัตรและ PIN ให้แก่ลูกค้าซึ่งเป็นพนักงานขององค์กร ไม่มีการลงลายมือชื่อของผู้รับในทะเบียนควบคุมการจ่ายบัตรและ PIN เช่นเดียวกับลูกค้าทั่วไป

3) การจ่ายบัตรและ PIN ให้แก่ผู้รับมอบฉันทะจากลูกค้า มีการตรวจสอบความถูกต้องจากบัตรประชาชนของผู้รับมอบฉันทะ ไม่ได้ทำการตรวจสอบความถูกต้องของบัตรประชาชนและลายมือชื่อลูกค้าเพิ่มเติม

4) การเก็บรักษาบัตรและ PIN เพื่อรอจ่ายให้ลูกค้า เจ้าหน้าที่ได้นำบัตรและใส่ในซองจัดไว้เป็นชุด ๆ ตามรายลูกค้า และให้พนักงานคนเดียวควบคุมการจ่ายการเก็บรักษาด้วย

วิธีปฏิบัติทั้ง 4 ข้อที่กล่าว ยังไม่รัดกุมและปลอดภัยเพียงพอ อาจทำให้ลูกค้าและองค์กรเกิดความเสียหายได้

ข้อแนะนำ

ในการจ่ายบัตรและ PIN ควรแยกเจ้าหน้าที่ควบคุมการเก็บรักษาและจ่ายบัตร และเจ้าหน้าที่ควบคุมการเก็บรักษาและการจ่าย PIN ออกจากกัน และควรมีการตรวจสอบบัตรประจำตัวประชาชน และพิสูจน์ลายมือชื่อลูกค้าที่มารับบัตรและ PIN เอง หรือที่มอบฉันทะให้ผู้อื่นมารับแทนด้วย เพื่อป้องกันบุคคลอื่นที่ไม่ใช่เจ้าของบัตรนำไปใช้เองได้ซึ่งจะเกิดความเสียหายทั้งกับลูกค้าและองค์กรได้

(28) การคืนบัตร ATM ที่ถูกเครื่องยึดให้แก่ลูกค้าไม่รัดกุม

เมื่อมีการคืนบัตร ATM ของลูกค้าที่ถูกเครื่องยึดไว้มีเพียงแต่การพิสูจน์ตัวลูกค้าโดยพิจารณาหลักฐานจากบัตรประชาชนนั้น ไม่ได้มีการพิสูจน์ลายมือชื่อลูกค้า ซึ่งยังไม่รัดกุมเพียงพอ

ข้อแนะนำ

ควรมีการพิสูจน์ตัวลูกค้า ทั้งโดยการพิจารณาหลักฐานจากบัตรประชาชนและพิสูจน์ลายมือชื่อลูกค้าด้วยเพื่อความรัดกุมปลอดภัย

(29) การปฏิบัติงานของเจ้าหน้าที่ศูนย์ ATM ไม่รัดกุม

การทำรายการควบคุมระบบงาน ATM ที่สำคัญของพนักงาน ATM Operator ผ่านทาง Console เช่น การอายัดและการถอนอายัด แม้องค์กรจะมีการควบคุมโดยมีการจัดทำทะเบียนและเอกสารประกอบและระบุให้พนักงานคนเดียวมีสิทธิที่จะทำการถอนอายัดก็ตาม แต่ในระบบงานไม่สามารถป้องกันบุคคลอื่นที่รู้วิธีการมาทำการถอนอายัดได้ ซึ่งในจุดนี้อาจก่อให้เกิดความเสียหายแก่องค์กรได้

ข้อแนะนำ

องค์กรควรกำหนดให้มีการใช้ Password หรือการควบคุมอื่นเพื่อป้องกันมิให้ผู้ไม่มีอำนาจสามารถทำรายการที่สำคัญได้ นอกจากนี้ เจ้าหน้าที่ชั้นบริหารควรสอบทาน ATM Log รายงานการอายัดและการถอนอายัด การใช้บัตร เพื่อความปลอดภัยของระบบงาน

(30) การรักษาความปลอดภัยของสถานที่ติดตั้งเครื่อง ATM

การปิดเครื่อง ATM เพื่อเปลี่ยนกล่องเงินที่ตู้ ATM ของสำนักงานใหญ่ เวลา 15.30 น. นั้น ลูกค้าสามารถเข้าไปในห้องหน้าตู้ ATM เหมือนกับเปิดบริการปกติ และมีโอกาสเข้าถึงห้องหลังตู้ ATM อาจไม่ปลอดภัยในขณะเปลี่ยนกล่องเงินได้

ข้อแนะนำ

องค์กรควรหามาตรการที่รัดกุมในการป้องกันความเสี่ยงดังกล่าว โดยอาจจะปิดประตูกระจกทางเข้าห้องหน้าเครื่อง ATM เพื่อป้องกันลูกค้าเข้ามาใช้บริการจนกว่าการเปลี่ยนกล่องเงินจะทำเสร็จจึงเปิดบริการตามปกติ

(31) สถานที่ติดตั้งเครื่อง ATM ของสาขา ไม่ปลอดภัยเพียงพอ

องค์กรติดตั้งเครื่อง ATM ในบริเวณบริการลูกค้าโดยมิได้จัดแยกเป็นสัดส่วนเพื่อความปลอดภัยในการปฏิบัติงานเกี่ยวกับตัวเครื่อง ATM นอกจากนี้ การเปลี่ยนกล่องเงินขณะที่ยังมีลูกค้าอยู่ด้วยอาจเป็นการเปิดโอกาสให้พนักงานหรือบุคคลภายนอกสามารถล่วงรู้รหัสที่ใช้ในการเปิดเครื่อง ATM และอาจเป็นการจูงใจให้เกิดการโจรกรรมเงินสดในเครื่อง ATM และสร้างความเสียหายแก่องค์กรได้

อนึ่ง ขณะทำการเปลี่ยนกล่องเงิน ได้มีการปิดประตูทางเข้าออก และเปิดให้ลูกค้าออกไปได้หลังจากที่ทำการเปลี่ยนกล่องเงินเรียบร้อยแล้ว ผู้จัดการสาขาชี้แจ้งว่า จะเข้มงวดมิให้มีการเปลี่ยนกล่องเงินขณะที่มีลูกค้าอยู่ในบริเวณบริการลูกค้า และรับจะหารือกับสำนักงานใหญ่ในการจัดการให้มีการรักษาความปลอดภัยเกี่ยวกับสถานที่ติดตั้งเครื่อง ATM ต่อไป

(32) **การติดตั้งอุปกรณ์คอมพิวเตอร์ที่ใช้หรือเกี่ยวเนื่องกับการปฏิบัติงานในระบบ ATM ไม่เหมาะสม**

จากการที่องค์กรติดตั้งอุปกรณ์คอมพิวเตอร์ที่ใช้ในระบบงาน ATM ในบริเวณห้อง I/O ซึ่งเป็นเขตหวงห้าม และควรจำกัดเฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องโดยตรงเท่านั้น อาจส่งผลกระทบต่อความปลอดภัยในการปฏิบัติงานในระบบ ATM ดังนี้คือ

1) อุปกรณ์ที่ใช้ในการควบคุมข่ายงาน ATM (ATM Network) อาจไม่เหมาะสมและไม่เกิดความคล่องตัวในการปฏิบัติงาน เนื่องจากเป็นการปฏิบัติงานในส่วนที่เกี่ยวข้องกับการควบคุมทางด้านผู้ใช้ (User) โดยเฉพาะ นอกจากนี้ ยังอาจเป็นอุปสรรคในการแก้ไขปัญหาได้อย่างฉับพลันและต่อเนื่อง และอาจเป็นจุดอ่อนในการรักษาความปลอดภัยเกี่ยวกับการอายัดบัตรและการควบคุมข่ายงานอื่น ๆ เช่น การสั่งเปิด - ปิดเครื่อง ATM โดยไม่ถูกต้อง เป็นต้น

2) อุปกรณ์ที่ใช้สำหรับแก้ไขรายการทางการเงินที่กระทำผ่านระบบงาน ATM โดยเจ้าหน้าที่ของศูนย์ประสานเขต อาจเป็นการเปิดโอกาสให้มีการปลอมแปลงบัตร Supervisor Card เพื่อทำรายการทางการเงินอันกระทบต่อข้อมูลของลูกค้าที่จัดเก็บในระบบคอมพิวเตอร์

ข้อแนะนำ

เนื่องจากในปัจจุบันการปลอมแปลงบัตรประเภทต่าง ๆ สามารถกระทำได้โดยง่าย ดังนั้น หากมิได้มีการแบ่งแยกหน้าที่อย่างเหมาะสมแล้ว ก็อาจส่งผลกระทบต่อองค์กรได้ในที่สุด จึงควรแยกอุปกรณ์คอมพิวเตอร์ที่ใช้ในการควบคุมข่ายงานตลอดจนชุดอุปกรณ์ ซึ่งใช้ในการแก้ไขรายการทางการเงินผ่านระบบงาน ATM ให้อยู่ในความควบคุมดูแลของศูนย์ประสานงานเขตโดยตรง หรือเคลื่อนย้ายมิให้ติดตั้งภายในเขตหวงห้ามของศูนย์คอมพิวเตอร์ เพื่อความปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบงาน ATM

(33) **การควบคุมการแจกจ่ายบัตร-รหัสประจำตัวลูกค้าไม่รัดกุม**

สาขารวมหน้าที่การจัดเก็บและแจกจ่ายบัตร-รหัสประจำตัวลูกค้าในบุคคลเดียวกัน ซึ่งไม่เหมาะสมตามหลักการแบ่งแยกหน้าที่ และอาจเกิดความเสียหายได้โดยง่าย นอกจากนี้ ในกรณีที่ลูกค้าประสงค์จะขอรับบัตร ATM ณ สำนักงานขององค์กร มิได้ให้ลูกค้าลงลายมือชื่อรับบัตร ATM ไว้เป็นหลักฐานตลอดจนมิได้มีการทบทวนและตรวจนับบัตร ATM ตลอดจนรหัสประจำตัวลูกค้าเป็นประจำ อันอาจเป็นช่องทางให้เกิดการสูญหายได้โดยง่าย และอาจเกิดความเสียหายในกรณีที่มีผู้นำบัตร ATM และรหัสประจำตัวลูกค้าดังกล่าวถอนเงินในบัญชีของลูกค้า

(34) ไม่มีการตรวจสอบหลักฐานผู้มารับบัตร ATM อย่างเพียงพอ

การตรวจสอบหลักฐานผู้มารับบัตร ATM และซองเอกสารรหัสประจำตัวผู้ถือบัตร ATM ยังไม่รัดกุมเท่าที่ควร ลูกค้าบางรายแสดงใบนัดรับบัตร ATM เพียงอย่างเดียว โดยไม่ต้องแสดงบัตรประจำตัวประชาชนหรือเอกสารหลักฐานอื่นที่เชื่อถือได้ ประกอบการขอรับบัตร ATM ก็สามารถรับบัตร ATM และซองเอกสารรหัสประจำตัวผู้ถือบัตร ATM ได้

(35) การทดสอบระบบจ่ายเงินของเครื่อง ATM ไม่สมบูรณ์

ตามที่องค์กรได้กำหนดให้เจ้าหน้าที่ของสาขาที่ทำหน้าที่เปลี่ยนกล่องเงินของเครื่องฝากถอนเงินอัตโนมัติ ต้องทำการทดสอบทุกครั้งหลังจากเปลี่ยนกล่องเงินเรียบร้อยแล้ว เพื่อเป็นการทดสอบการจ่ายเงินของเครื่องฝากถอนเงินอัตโนมัติ โดยไม่มีการตรวจนับธนบัตรที่เครื่องจ่ายออกมาเพื่อตรวจสอบความถูกต้องของการทำงานเครื่องอย่างจริงจัง ดังนั้น ถ้าการทำงานของเครื่องบกพร่องจ่ายเงินไม่ถูกต้ององค์กรจะไม่สามารถทราบได้ทันที ซึ่งอาจเกิดผลเสียหายต่อองค์กรได้

ข้อแนะนำ

ควรกำหนดให้มีการตรวจนับธนบัตรที่จ่ายจากเครื่อง ATM เพื่อตรวจสอบความถูกต้องของการทำงานของเครื่อง

(36) ไม่มีการกำหนดระเบียบปฏิบัติเกี่ยวกับ

1) การลบข้อมูลของลูกค้าที่ถูกอายัดบัตรออกจากแฟ้มข้อมูล โดยเฉพาะในกรณีที่มีการอายัดบัตรเนื่องจากบัตรหาย และลูกค้าได้ทำการขอบัตรใหม่แล้ว

2) กรณีลูกค้านำเงินสดฝากผ่านเครื่องฝากถอนเงินอัตโนมัติโดยไม่ใส่ซอง

3) กรณีเจ้าของบัญชีที่ถูกอายัดเงินฝากเนื่องจากนำเงินสดฝากผ่านเครื่องฝากถอนเงินอัตโนมัติโดยไม่ใส่ซอง มาติดต่อองค์กรให้ปรับปรุงบัญชีเงินฝาก

ข้อแนะนำ

องค์กรควรกำหนดระเบียบปฏิบัติในเรื่องที่กล่าวเพื่อเป็นมาตรฐานในการปฏิบัติงานเดียวกันสำหรับ ATM ทุกเครื่อง

(37) ธนาคารไม่มีทะเบียนควบคุมซองรหัสประจำตัวผู้มีบัตร ATM ยังไม่มารับ

ข้อแนะนำ

ควรกำหนดระเบียบการปฏิบัติงานในเรื่องที่กล่าวข้างต้นโดยละเอียด และจัดทำทะเบียนซองรหัสประจำตัวผู้ถือบัตร ATM ที่ลูกค้ายังไม่มารับ เพื่อประโยชน์ในการควบคุมและตรวจสอบ

(38) **เครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินจ่ายเงินผิดพลาด**

การจ่ายเงินของเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินยังมีข้อผิดพลาดในบางกรณี เช่น มีผู้มาถอนเงินที่เครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินสำนักงานใหญ่ แต่ไม่ได้รับเงิน ทำให้ลูกค้ารายต่อมาซึ่งทำรายการสอบถามยอดได้รับเงินจำนวนดังกล่าวไป

ข้อแนะนำ

ควรค้นหาสาเหตุและหาวิธีการป้องกันกรณีเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงินจ่ายเงินให้ลูกค้าผิดพลาด

(39) **เครื่อง ATM จ่ายเงินผิดพลาด**

การจ่ายเงินของเครื่อง ATM ยังมีข้อผิดพลาดในบางกรณี เช่น เครื่อง ATM ที่ติดตั้งอยู่ที่สาขาแห่งหนึ่ง ได้จ่ายเงินให้ลูกค้าขององค์กรอื่นที่อยู่ใน Pool เดียวกัน น้อยกว่าจำนวนที่ต้องการถอน

ข้อแนะนำ

ควรค้นหาสาเหตุและหาวิธีการป้องกันข้อผิดพลาดกรณีเครื่อง ATM จ่ายเงินให้ลูกค้าคลาดเคลื่อนไปจากจำนวนที่ลูกค้าต้องการถอน

(40) **การเก็บรักษาบัตร ATM ที่ถูกเครื่องยึด (Retained Card) ไม่ปลอดภัยเท่าที่ควร**

พนักงานธนาคารเก็บบัตร ATM ที่ถูกเครื่องยึด สอดไว้ในสมุดทะเบียนคุมบัตรที่ถูกยึด (Retained Card Register) และวางอยู่ในที่เปิดเผย อาจทำให้บัตรสูญหายได้

ข้อแนะนำ

เพื่อป้องกันมิให้บัตร ATM สูญหาย หรือเสียหาย หรือมีการนำบัตรไปใช้โดยมิชอบควรกำหนดระเบียบการเก็บรักษาให้รัดกุม โดยมีพนักงานรับผิดชอบเป็นการเฉพาะด้าน

(41) **ข้อมูลเกี่ยวกับบัตรที่แจ้งหายไม่ถูกต้อง**

จำนวนบัตรที่ลูกค้าแจ้งหาย (Hot Card) ในแฟ้มข้อมูล Hot Card และแฟ้มข้อมูลผู้ถือบัตร ATM (Card Holder File) มียอดไม่ตรงกัน เนื่องจากองค์กรได้เปลี่ยนแปลงวิธีการและโปรแกรม Update ข้อมูลโดยปรับปรุงยอดบัตรที่ลูกค้าแจ้งหายเฉพาะในแฟ้ม Hot Card เท่านั้น

ข้อแนะนำ

องค์กรควรกำหนดให้มีการเปรียบเทียบข้อมูลเกี่ยวกับบัตรที่ลูกค้าแจ้งหาย (Hot Card) ในแฟ้มข้อมูลที่เกี่ยวข้องกัน เป็นครั้งคราวตามความเหมาะสม หากพบว่ามีข้อผิดพลาด ก็ควรดำเนินการแก้ไขให้ถูกต้อง

(42) **การคำนวณดอกเบี้ยให้แก่ลูกค้าบัตร ATM คลาดเคลื่อนไปจากความเป็นจริง**

องค์กรนำแฟ้มรายการเคลื่อนไหวในบัญชีของลูกค้าที่ใช้บริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน หลังเวลาทำการของแต่ละวันไปปรับปรุงยอด (Update) ใน Master File เพื่อให้ยอดคงเหลือเป็นปัจจุบันก่อนเปิดบริการในวันทำการถัดไป ซึ่งปกติจะทำการปรับปรุงเวลาประมาณ 8.30 น. สำหรับรายการที่เกิดขึ้นตั้งแต่เวลา 7.00 น. ของแต่ละวันทำการ จะถือเป็นรายการของวันนั้น ๆ ขั้นตอนดังกล่าวเป็นผลให้ไม่มีการหักจำนวนเงินส่วนที่ลูกค้าถอนออกจากบัญชีเงินฝากออมทรัพย์ตั้งแต่หลังเวลาทำการของทุกวันและวันสุดสัปดาห์ หรือวันก่อนวันหยุดทำการอื่น ๆ จนถึงวันเปิดทำการถัดไปจาก Master File ของลูกค้า และโปรแกรมคำนวณดอกเบี้ยก็ยังคงคิดดอกเบี้ยให้แก่จำนวนเงินดังกล่าวโดยไม่มีการปรับปรุงย้อนหลัง ทำให้มีการจ่ายดอกเบี้ยให้แก่จำนวนเงินที่ถูกถอนออกไปแล้ว

ข้อแนะนำ

องค์กรควรแก้ไขโปรแกรมการคำนวณดอกเบี้ยให้ถูกต้อง

(43) **สถานที่ตั้งเครื่องถอนเงินอัตโนมัติของสาขา** ในปัจจุบันไม่เหมาะสม เนื่องจากด้านหลังของตัวเครื่องเป็นที่นั่งทำงานของพนักงานสาขา ทำให้พนักงานที่นั่งในบริเวณด้านหลังเครื่องถอนเงินอัตโนมัติอาจสังเกตเห็นรหัสที่ใช้ในการเปิดประตูเครื่องเปลี่ยนกล่องเงินหรือ Journal Tape ได้ง่ายมีผลให้การควบคุมภายในไม่รัดกุมเพียงพอที่จะป้องกันไม่ให้บุคคลอื่นที่ไม่มีหน้าที่และส่วนเกี่ยวข้องล่วงรู้ขั้นตอนดังกล่าว นอกจากนี้ แป้นกดข้อมูลตัวเลขที่ใช้ป้อนรหัสลับประจำตัวลูกค้า (PIN) ของเครื่องถอนเงินอัตโนมัติมีลักษณะที่ผู้อื่นสามารถสังเกตและมองเห็นการป้อนรหัสลับได้ง่าย และมีลูกค้าบางรายทิ้งบัตรบันทึกรายการไว้ หรืออาจลืมหยิบบัตร ATM ในบางครั้ง อาจทำให้ทั้งลูกค้าและองค์กรได้รับความเสียหายได้

ข้อแนะนำ

ควรให้ความรู้หรือมีคำเตือนกับลูกค้าหรือผู้ใช้บริการ ให้ระมัดระวังในการป้อนรหัสลับประจำตัว (PIN) เพื่อป้องกันไม่ให้ผู้อื่นมองเห็นรหัสลับที่ลูกค้าป้อนบนแป้นกดข้อมูล และปิดประกาศคำเตือนให้ลูกค้าไม่ลืมหยิบบัตร ATM บัตรบันทึกรายการ และเงินสด ทุกครั้งหลังจากทำรายการเสร็จแล้ว

(44) **สาขาไม่ได้ให้ลูกค้าที่มารับบัตร ATM และรหัสลับประจำตัวลูกค้าบางราย ลงลายมือชื่อในช่องผู้รับ** ในทะเบียนการจ่ายบัตร ATM และทะเบียนจ่ายรหัสลับประจำตัวลูกค้า นอกจากนี้ ยังมีการยินยอมให้พนักงานผู้จ่ายบัตร ATM และรหัสลับประจำตัวลูกค้า ซึ่งมิใช่เจ้าของบัญชี ลงลายมือชื่อรับแทนอีกด้วย อาจทำให้เกิดปัญหาได้ในกรณีที่ลูกค้าซึ่งได้รับบัตร ATM และรหัสลับประจำตัวไปใช้ถอนเงินแล้วไม่ยอมรับว่าตนเองได้ทำรายการนั้น เนื่องจากไม่มีหลักฐานเป็นลายลักษณ์อักษรว่าลูกค้าได้รับบัตรและรหัสลับประจำตัวไปแล้วจริง

ข้อแนะนำ

ควรให้พนักงานที่ทำหน้าที่จ่ายบัตร และพนักงานที่ทำหน้าที่จ่ายใบแจ้งรหัสลับประจำตัวลูกค้าดูแลให้ลูกค้าลงลายมือชื่อในช่องผู้รับ ของทะเบียนจ่ายบัตรและทะเบียนจ่ายรหัสประจำตัวลูกค้าให้ครบถ้วนทุกราย และไม่ควรยินยอมให้บุคคลอื่นซึ่งมิใช่เจ้าของบัญชี รับบัตรและใบแจ้งรหัสลับประจำตัวลูกค้าแทนเว้นแต่จะมีหนังสือมอบฉันทะให้ทำการแทนเท่านั้น

(45) **จากทะเบียนจ่ายบัตร ATM** และทะเบียนจ่ายรหัสลับประจำตัวลูกค้า ปรากฏว่า ในการจ่ายบัตร ATM และรหัสลับให้ลูกค้าบางราย ลายมือชื่อผู้จ่ายบัตร ATM และผู้จ่ายใบแจ้งรหัสลับประจำตัวลูกค้า เป็นบุคคลเดียวกัน ซึ่งแสดงว่าสาขาไม่ได้แบ่งแยกหน้าที่ในการจ่ายบัตร ATM และใบแจ้งรหัสลับประจำตัวให้แก่ลูกค้าออกจากกัน ไม่สอดคล้องกับหลักการควบคุมภายในที่ดี เพราะเป็นการเปิดโอกาสให้พนักงานสาขาเข้าถึงบัตร ATM และรหัสลับประจำตัวลูกค้าพร้อมกันได้ในเวลาเดียวกัน

ข้อแนะนำ

ควรแบ่งแยกหน้าที่ในการจ่ายบัตร ATM และใบแจ้งรหัสลับประจำตัวลูกค้าออกจากกันโดยเด็ดขาด และในกรณีที่พนักงานผู้หนึ่งไม่สามารถปฏิบัติงานได้ ควรมอบหมายให้พนักงานอื่นที่เหมาะสมซึ่งมิใช่พนักงานที่ทำอีกหน้าที่หนึ่งใน 2 หน้าที่นั้นปฏิบัติงานแทน เพื่อป้องกันพนักงานคนใดคนหนึ่งสามารถเข้าถึงทั้งบัตร ATM และรหัสลับประจำตัวลูกค้าได้

(46) **สาขาตรวจสอบความครบถ้วนถูกต้องของบัตร** และรหัสประจำตัวลูกค้าที่ยังไม่ได้จ่ายไปโดยใช้วิธีนับว่าบัตรมีจำนวนเท่ากับใบแจ้งรหัสลับประจำตัวลูกค้า แต่ไม่ได้สอบยันกับยอดคงเหลือจากทะเบียนจ่ายบัตร ATM และทะเบียนจ่ายใบแจ้งรหัสลับประจำตัวลูกค้า ซึ่งอาจทำให้ไม่ทราบจำนวนที่แท้จริงของบัตรและใบแจ้งรหัสลับประจำตัวลูกค้า ถ้าเกิดการสูญหายทั้งบัตร ATM และใบแจ้งรหัสลับประจำตัวลูกค้าพร้อมกัน

ข้อแนะนำ

ควรจัดให้มีการตรวจนับบัตร ATM และใบแจ้งรหัสลับประจำตัวลูกค้า ที่ยังไม่จ่ายให้ลูกค้าและสอบยันยอดคงเหลือในทะเบียนคุมเป็นครั้งคราวตามความเหมาะสม เพื่อควบคุมว่าบัตรและใบแจ้งรหัสดังกล่าวมีอยู่ครบถ้วนไม่สูญหาย

(47) **สาขาแต่งตั้งพนักงานที่ทำหน้าที่ด้านการประมวลผลที่ควบคุมเครื่อง ATM** (เครื่องที่ใช้ในการควบคุมระบบงานถอนเงินอัตโนมัติ) เป็นกรรมการในคณะกรรมการบรรจุและควบคุมเงินในเครื่อง ATM หรือเป็นกรรมการในคณะกรรมการตรวจสอบนับเงินในเครื่อง ATM และเมื่อหัวหน้าคณะกรรมการบรรจุ และควบคุมเงินในเครื่อง ATM ลาหยุดงาน ก็ให้หัวหน้าคณะกรรมการตรวจนับเงินในเครื่อง ATM ปฏิบัติหน้าที่แทน ซึ่งเป็นบุคคลเดียวกัน อันมีผลให้ไม่มีการควบคุมภายในโดยการแบ่งแยกหน้าที่ความรับผิดชอบที่เหมาะสม

ข้อแนะนำ

ในการแต่งตั้งให้พนักงานคนใดเข้าร่วมในคณะกรรมการปฏิบัติงานระบบงาน ATM ควรคำนึงถึงอุปสรรคหรือความขัดแย้งในการควบคุมภายในกระบวนการปฏิบัติงานเรื่องการแบ่งแยกหน้าที่ด้วย

(48) **รหัสเปิดประตูด้านหลังเครื่อง ATM** ไม่ได้ถูกจำกัดให้รู้เฉพาะบุคคลที่รับผิดชอบในการใช้รหัสเปิดประตูเครื่องเท่านั้น เนื่องจากพนักงานที่เป็นกรรมการในคณะกรรมการบรรจุและควบคุมเงินในเครื่อง ATM และคณะกรรมการตรวจนับเงินในเครื่อง ATM ส่วนใหญ่ทราบรหัสในการเปิดประตูเครื่อง ATM ทำให้ขาดการควบคุมภายในเรื่องดังกล่าว

ข้อแนะนำ

ควรกำหนดให้เฉพาะพนักงานในคณะกรรมการปฏิบัติงานระบบงาน ATM ที่รับผิดชอบในการใช้รหัสเปิดประตูเครื่อง ATM เท่านั้น ที่รู้รหัสในการเปิดประตูเครื่อง ATM

(49) **สาขาไม่ได้จัดทำทะเบียนการเบิกจ่ายกุญแจในระบบงานเครื่องถอนเงินอัตโนมัติ** ได้แก่ กุญแจเครื่อง ATMC กุญแจเครื่อง ATM กุญแจกล่องเงินในเครื่อง ATM กุญแจตู้เก็บบัตร ATM และกุญแจตู้เก็บใบแจ้งรหัสลับประจำตัวลูกค้า เพื่อบันทึกและควบคุม วัน เวลา และผู้นำกุญแจไปใช้งาน

ข้อแนะนำ

ควรกำหนดระเบียบปฏิบัติเกี่ยวกับตัวพนักงานผู้มีสิทธิใช้กุญแจแต่ละประเภท และจัดทำทะเบียนการเบิกจ่ายกุญแจในระบบงานเครื่องถอนเงินอัตโนมัติ ได้แก่ กุญแจเครื่อง ATMC กุญแจเครื่อง ATM กุญแจกล่องเงินในเครื่อง ATM กุญแจตู้เก็บบัตร ATM และกุญแจตู้เก็บใบแจ้งรหัสลับประจำตัวลูกค้า

(50) **บัตรประจำตัวลูกค้า (Plastic Card)**

1) ในการตรวจนับบัตรพาสติกซึ่งเป็นบัตรเปล่าที่ซื้อมาจากต่างประเทศเพื่อตรวจสอบคุณภาพและความครบถ้วนของจำนวนบัตรที่ได้รับจากผู้ขาย พนักงานที่ตรวจนับบัตรดังกล่าวไม่ได้ลงนามกำกับหีบห่อที่ตรวจแล้ว ทำให้ขาดหลักฐานในการปฏิบัติงาน และไม่สามารถสอบสวนสาเหตุที่บัตรขาดหายไปซึ่งเคยมีกรณีดังกล่าวเกิดขึ้นมาแล้ว

2) ในการนำบัตรเปล่าไปบันทึกชื่อลูกค้าเป็นอักษรตัวนูนบนบัตรและบันทึกข้อมูลลงในแถบแม่เหล็กด้านหลังบัตรในแต่ละครั้ง ไม่มีการกระทบยอดจำนวนบัตรเปล่าที่เบิกใช้กับจำนวนบัตรที่ผ่านเครื่องทำบัตรให้ลูกค้าและจำนวนบัตรเปล่าคงเหลือ ทำให้การควบคุมการใช้เครื่องทำบัตรไม่รัดกุมเท่าที่ควร อาจมีการนำบัตรอื่นมาผ่านกระบวนการผลิตซึ่งสามารถนำไปใช้บริการได้เช่นเดียวกัน

3) เลขที่บัตรประจำตัวลูกค้า (Card No.) เป็นข้อมูลสำคัญที่บันทึกไว้ในแถบแม่เหล็กด้านหลังบัตรประจำตัวลูกค้า ควรเป็นความลับ แต่ในบัตรบันทึกรายการ (Transaction record) ที่เครื่องฝากถอนเงินอัตโนมัติออกให้ลูกค้าเก็บไว้เป็นหลักฐานการฝากเงินหรือถอนเงิน มีเลขที่บัตรประจำตัวลูกค้าพิมพ์แสดงไว้ทุกใบ และ

ลูกค้าส่วนใหญ่ไม่เห็นความสำคัญในการเก็บบัตรบันทึกรายการไว้เป็นหลักฐานจะทิ้งบัตรดังกล่าวไว้ในบริเวณใกล้ ๆ กับที่ตั้งเครื่องฝากถอนเงินอัตโนมัติ ผู้ที่มีความรู้ความสามารถในการทำบัตรประจำตัวลูกค้าอาจนำข้อมูลเกี่ยวกับเลขที่บัตรประจำตัวลูกค้าไปใช้ประโยชน์ในการทำบัตรปลอมได้

(51) รหัสลับประจำตัวลูกค้า (PIN)

องค์กรไม่ได้กำหนดตัวบุคคลที่อนุญาตให้เข้าถึง (Access) ตู้เก็บรหัสลับประจำตัวลูกค้า ซึ่งพิมพ์เสร็จเรียบร้อยแล้วเตรียมจัดส่งสาขาเพื่อแจกลูกค้า และไม่ได้ปิดกุญแจตู้เก็บรหัสลับดังกล่าวไว้ตลอดเวลาอาจทำให้ความลับรั่วไหลได้

(52) การกำหนดวิธีการเขียนรายละเอียดลงในแบบฟอร์มใบขอปรับปรุงรายการ ATM Pool

พนักงานสาขาขององค์กรเขียนรายละเอียดลงในแบบฟอร์มใบขอปรับปรุงรายการ ATM Pool ไม่ถูกต้อง เนื่องจากไม่เข้าใจปัญหาที่เกิดขึ้น หรือไม่เข้าใจวิธีตรวจสอบหาข้อมูลเพื่อตอบคำถามที่สำนักแห่งหนึ่งให้ติดตามรายการที่มีปัญหาให้ ปัญหาที่กล่าวข้างต้นเกิดขึ้นเพราะองค์กรไม่ได้กำหนดวิธีหาข้อมูล และจัดทำตัวอย่างในการเขียนข้อมูลลงในแบบฟอร์มที่กำหนดให้พนักงานยึดถือเป็นแนวทางในการปฏิบัติงาน

ข้อแนะนำ

องค์กรควรจัดทำคู่มือการเขียนรายละเอียดลงในแบบฟอร์มใบขอปรับปรุงรายการ ATM Pool และการจัดหาข้อมูลประกอบรายการปรับปรุงที่ถูกต้อง เพื่อป้องกันข้อผิดพลาดที่อาจก่อให้เกิดความเสียหายต่อลูกค้าและองค์กรได้

(53) การชำระบัญชีระหว่างองค์กร (Inter Office) ตามข้อตกลงใน ATM Pool

จากการประชุมระหว่างองค์กรในกลุ่ม ATM Pool ได้มีข้อตกลงให้แต่ละองค์กรผ่านบัญชีรายการเดบิตและเครดิตในบัญชีระหว่างองค์กร ซึ่งเปิดเป็นบัญชีเงินฝากกระแสรายวันไว้ และหน่วยงานที่รับผิดชอบในเรื่องดังกล่าวของแต่ละองค์กรจะตัดยอดเงินและรายการทุกวันพุธ ตรวจสอบยอดเงินคงเหลือสุทธิระหว่างกันในวันพฤหัสบดีและจะมีการชำระเงินในวันศุกร์ เวลา 10.00 น. โดยการออกแคชเชียร์เช็ค ซึ่งได้กำหนดให้บันทึกบัญชีเงินฝากระหว่างกันด้วยยอดเงินที่ปรากฏในรายงาน "Daily Transaction Report" ที่ได้จากองค์กรผู้จ่ายเงิน แต่จากการตรวจสอบพบว่า ไม่มีการปฏิบัติตามข้อตกลงดังกล่าว

ข้อแนะนำ

องค์กรควรติดตามรายการด้านเงินฝากด้วย เพราะการบันทึกบัญชีโดยใช้ยอดจำนวนเงินจากรายงาน "Daily Transaction Report" ขององค์กรผู้จ่ายเงินนั้น เป็นเพียงยอดเงินที่เกิดจากรายการถอนเท่านั้น ยังไม่รวมยอดจำนวนเงินที่เกิดจากรายการฝาก ซึ่งยังมีข้อผิดพลาดเนื่องจากการปฏิบัติงานของพนักงานที่เกี่ยวข้องด้วย ดังนั้นการชำระเงินจะถูกต้องเมื่อมีการบันทึกบัญชีเงินฝากระหว่างกันถูกต้องด้วย

(54) การตรวจสอบใบคำขอใช้บริการเอทีเอ็ม

องค์กรไม่ได้จัดทำระเบียบปฏิบัติงานเป็นลายลักษณ์อักษรเกี่ยวกับการตรวจสอบแบบฟอร์มใบคำขอใช้บัตรเอทีเอ็ม ได้แก่ การกำหนดวิธีการตรวจสอบ เอกสารที่ใช้ในการตรวจสอบหน้าที่และความรับผิดชอบของพนักงานที่เกี่ยวข้องกับการตรวจสอบ เพราะการควบคุมด้วยโปรแกรมจัดทำบัตรนั้น ควบคุมได้เฉพาะบัญชีที่ได้ทำบัตรไปแล้วเท่านั้น สำหรับบัญชีที่ยังไม่เคยทำบัตรเลยจะเช็คสอบไม่ได้และหากการตรวจสอบใบคำขอใช้บริการเอทีเอ็มไม่รัดกุมแล้ว อาจก่อให้เกิดความเสียหายต่อองค์กรหรือลูกค้าได้ เนื่องจากการกรอกเลขที่บัญชีผิดพลาดได้

ข้อแนะนำ

องค์กรควรจัดทำระเบียบปฏิบัติงานเกี่ยวกับการตรวจสอบแบบฟอร์มใบคำขอใช้บัตรเอทีเอ็ม และควบคุมให้มีการปฏิบัติตามระเบียบโดยเคร่งครัด

(55) การกำหนดรหัส Master Key และจัดทำชุดรหัสเก็บไว้ใน Diskette ซึ่งใช้ในการคำนวณ PIN

ในปัจจุบันองค์กรได้แต่งตั้งพนักงานจำนวน 4 คน เป็นคณะกรรมการควบคุมการจัดทำ PIN และเก็บ Master Key ซึ่งประกอบด้วย หัวหน้าส่วนกลาง ฝ่ายการธนาคารในประเทศ หัวหน้าส่วนตรวจสอบคอมพิวเตอร์ ฝ่ายตรวจสอบ หัวหน้าศูนย์คอมพิวเตอร์ และผู้จัดการสำนักงานสาขา โดยให้แต่ละคนกำหนดรหัส Master Key ขึ้นเองคนละ 1 ชุด และป้อนรหัส Master Key เก็บไว้ใน Diskette คนละแผ่นและเก็บไว้เป็นความลับ เมื่อจะจัดทำ PIN ก็นำออกมาใช้งาน จากวิธีปฏิบัติงานดังกล่าวอาจก่อให้เกิดปัญหาต่อองค์กรได้ ถ้าหากพนักงานคนหนึ่งคนใดในคณะกรรมการที่กล่าวลืมรหัส Master Key และแผ่น Diskette ที่เก็บรหัสเสียหาย ซึ่งเป็นผลให้การจัดทำ PIN ที่ออกให้แก่ลูกค้ารายใหม่ไม่สามารถจัดทำได้

ข้อแนะนำ

องค์กรควรให้คณะกรรมการควบคุมการจัดทำ PIN จัดทำรหัส Master Key เก็บไว้ใน Diskette เพิ่มขึ้นอีกคนละหนึ่งแผ่น และรวบรวมเก็บไว้ที่ผู้บริหารระดับสูง สำหรับนำมาใช้ทดแทนเมื่อกรรมการควบคุมการจัดทำ PIN คนใดคนหนึ่งไม่อยู่ เพื่อให้การปฏิบัติงานด้านการออก PIN ให้ลูกค้ากระทำได้อย่างต่อเนื่อง

(56) การแก้ไขโปรแกรมระบบงาน ATM โดยบริษัทผู้ให้เช่าเครื่อง ATM

เนื่องจากองค์กรเช่าโปรแกรมระบบงาน ATM จากบริษัทผู้ให้เช่าเครื่อง ATM และมีข้อตกลง ว่าองค์กรจะแก้ไขโปรแกรมที่เช่าได้เฉพาะส่วนที่ปรากฏที่หน้าจอ ATM เท่านั้น โปรแกรมส่วนที่เหลือบริษัทผู้ให้เช่าจะเป็นผู้แก้ไขให้ตามความต้องการขององค์กร จากการตรวจสอบพบว่าองค์กรได้ให้บริษัทแก้ไขโปรแกรมบางโปรแกรมและได้นำมาใช้งานตามปกติแล้ว ปรากฏว่าได้ผลตามที่องค์กรต้องการ แต่ได้เกิดปัญหาในกรณีอื่นซึ่งเป็นผลจากการแก้ไขโปรแกรมของบริษัทผู้ให้เช่า เช่น องค์กรให้บริษัทผู้ให้เช่าแก้ไขโปรแกรม ATM ตัดบัญชีลูกค้าทุกรายการที่มีปัญหาที่ช่องจ่ายเงิน ไม่ว่าเครื่อง ATM จะจ่ายเงินหรือให้หรือไม่ ซึ่งโปรแกรมทำถูกต้อง แต่ก่อนการแก้ไขโปรแกรมจะมีรหัสที่ทำไม่สำเร็จ ภายหลังการแก้ไขโปรแกรมแล้วปรากฏว่ามีรหัสที่ทำไม่สำเร็จออกมาเป็น 2 แบบ โดยไม่ทราบสาเหตุ และมีผลต่อการทำงานของเครื่อง ATM

ข้อแนะนำ

องค์กรควรทำข้อตกลงกับบริษัทผู้ให้เช่าโปรแกรมระบบงาน ATM ให้เพิ่มการฝึกอบรมพนักงานด้านโปรแกรมขององค์กรให้มีความรู้เกี่ยวกับโปรแกรมระบบงานมากยิ่งขึ้น และควรกำหนดระยะเวลาที่แน่นอนให้บริษัททำการแก้ไขโปรแกรมระบบงานในส่วนที่มีปัญหาเสร็จสมบูรณ์พร้อมที่จะใช้งานได้โดยเร็ว

(57) การทำลายใบปะหน้าแบบฟอร์มใบแจ้งรหัส

เมื่อเสร็จกระบวนการจัดทำรหัสประจำตัวลูกค้าที่ใช้บริการ ATM แล้ว องค์กรไม่ได้กำหนดให้ผู้ปฏิบัติงานทำลายกระดาษสีดำซึ่งเป็นกระดาษแผ่นแรกของแบบฟอร์มใบแจ้งรหัสที่จะส่งให้ลูกค้าก่อนนำแบบฟอร์มใบแจ้งรหัสออกจากห้องคอมพิวเตอร์ เป็นการเปิดโอกาสให้ผู้ที่ไม่มีส่วนเกี่ยวข้องกับการจัดทำรหัสรู้เห็นรหัสประจำตัวลูกค้าจากรอยพิมพ์รหัสซึ่งปรากฏอยู่ที่ด้านหลังของกระดาษสีดำที่กล่าวได้

ข้อแนะนำ

ควรทำลายกระดาษสีดำซึ่งเป็นกระดาษแผ่นแรกของแบบฟอร์มใบแจ้งรหัสที่จะส่งให้ลูกค้าก่อนนำแบบฟอร์มใบแจ้งรหัสออกจากห้องคอมพิวเตอร์ที่จัดทำรหัส เพื่อป้องกันผู้อื่นรู้เห็นรอยพิมพ์รหัสซึ่งปรากฏอยู่ที่ด้านหลังของกระดาษสีดำ

(58) การควบคุมการจัดเก็บอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องในระบบงาน ATM

การนำเครื่องจักรและอุปกรณ์ทำบัตร ATM รวมทั้งเครื่องจักรและอุปกรณ์คอมพิวเตอร์ชุดอื่น ๆ ที่แก้ไขข้อผิดพลาดที่กระทำผ่านเครื่อง ATM และอุปกรณ์คอมพิวเตอร์ที่ใช้ควบคุมการทำงานของเครื่อง ATM เป็นต้น ติดตั้งปะปนไว้ในห้องเดียวกัน จะทำให้การแบ่งแยกหน้าที่และการควบคุมภายในเกี่ยวกับการจัดทำบัตร ATM และการควบคุมภายในระบบ ATM ไม่ได้ผลเท่าที่ควร

(59) การแจ้งการเปลี่ยนแปลงเงื่อนไขการให้บริการ

การเปลี่ยนเงื่อนไขการให้บริการ ATM ที่มีผลกระทบต่อผลประโยชน์หรือความเสียหายของลูกค้า โดยไม่มีการประชาสัมพันธ์หรือแจ้งให้ลูกค้าทราบล่วงหน้า อาจทำให้ลูกค้าเกิดความสับสนและขาดความเชื่อถือในการให้บริการขององค์กร

ข้อแนะนำ

การเปลี่ยนเงื่อนไขการให้บริการ ATM ที่มีผลกระทบต่อผลประโยชน์หรือความเสียหายของลูกค้าควรมีการประชาสัมพันธ์หรือแจ้งให้ลูกค้าทราบล่วงหน้า เพื่อป้องกันลูกค้าสับสนและขาดความเชื่อถือในการใช้บริการ ATM ขององค์กร

(60) **ไม่มีระบบสัญญาณเตือนภัยที่เครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน**

องค์กรไม่ได้ติดตั้งระบบสัญญาณเตือนภัย (Alarm) ที่เครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน เพื่อป้องกันโจรภัย โดยเฉพาะในช่วงเวลาหลังปิดบริการแล้ว ทำให้สินทรัพย์ขององค์กรล่อแหลมต่อการถูกทำลาย หากมีเหตุร้ายเกิดขึ้นอาจแก้ไขสถานการณ์ได้ไม่ทันท่วงที อีกทั้งไม่เป็นการปฏิบัติตามเงื่อนไขการอนุญาตให้ใช้เครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน เรื่ององค์กรต้องจัดให้มีระบบรักษาความปลอดภัยที่เครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน

ข้อแนะนำ

เพื่อประโยชน์ในการรักษาความปลอดภัย ควรติดตั้งระบบสัญญาณแจ้งภัย (Alarm) ในบริเวณที่ตั้งเครื่อง ATM

(61) **การรักษาความปลอดภัยทางกายภาพของเครื่อง ATM ไม่รัดกุมเพียงพอ**

ที่ตู้ ATM ไม่มีการติดตั้งสัญญาณเตือนภัยกรณีถูกโจรกรรมและงัดแงะ คงมีแต่ยามที่เฝ้าอาคารสำนักงานใหญ่ตรวจตราบริเวณรอบ ๆ องค์กรซึ่งอาจไม่ปลอดภัยหากมีการโจรกรรมเกิดขึ้น

ข้อแนะนำ

องค์กรควรจัดให้มีการติดตั้งสัญญาณเตือนภัยกรณีที่มีการโจรกรรมที่เครื่อง ATM เพื่อความปลอดภัย

(62) **มิได้ติดตั้งสัญญาณเตือนภัยที่เครื่อง ATM**

สาขามิได้ติดตั้งสัญญาณเตือนภัยเพื่อป้องกันการโจรกรรมกล่องเงินในเครื่อง ATM อันอาจเกิดขึ้นและสร้างความเสียหายต่อองค์กร แม้ว่าจะได้มีการประกันภัยเงินสดในเครื่อง ATM ไว้แล้วก็ตาม เนื่องจากเครื่อง ATM อาจได้รับความเสียหาย และไม่สามารถให้บริการได้อย่างต่อเนื่อง อันอาจเป็นการปฏิบัติไม่ชอบตามเงื่อนไขการอนุญาตให้เปิดบริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน

ข้อแนะนำ

เพื่อให้การป้องกันและให้ความคุ้มครองต่อทรัพย์สินขององค์กรอย่างเพียงพอ ควรเร่งดำเนินการติดตั้งระบบสัญญาณเตือนภัยในรูปแบบที่สามารถแจ้งต่อผู้มีหน้าที่รับผิดชอบโดยตรงได้ทันที

(63) **สาขาไม่สามารถรับทราบสัญญาณเตือนภัยได้ตลอด 24 ชั่วโมง** ว่ามีบุคคลอื่นบุกรุกหรือทำลายตัวเครื่องถอนเงินอัตโนมัติที่ติดตั้งใน Booth ภายนอกอาคารที่ทำการสาขาซึ่งบรรจุกล่องเงินไว้ภายในเครื่อง เนื่องจากไม่มีพนักงานปฏิบัติงานที่สาขาตลอดเวลา

ข้อแนะนำ

ควรพิจารณาติดตั้งระบบสัญญาณเตือนภัย สำหรับเครื่องถอนเงินอัตโนมัติที่ติดตั้งใน Booth ภายนอกอาคารที่ทำการสาขาขององค์กรตามที่เห็นควร เพื่อให้มีสัญญาณเตือนภัยหากมีการบุกรุกหรือทำลายตัวเครื่องได้ตลอดเวลา

(64) ไม่มีการรักษาความปลอดภัยการสื่อสารข้อมูลระหว่างองค์กรกับบริษัทกลาง

ปัจจุบันองค์กรมีการใช้ Software Encryption ที่เครื่อง Modem เท่านั้น ยังไม่มีการใช้ Black Box ในองค์กร การเข้ารหัสข้อมูล (Encryption) เพื่อประกอบการทุจริตหรือก่อความเสียหายต่อองค์กรได้

(65) ไม่มีการรักษาความปลอดภัยการสื่อสารข้อมูลในระบบ ATM ระหว่างธนาคารกับบริษัทเครือข่าย

จากรายงานการประชุมคณะทำงานด้าน Auditor ระหว่างองค์กรกับบริษัทเครือข่ายระบุว่าในขณะนี้ไม่มี Security ของระบบการโอนเงินทางอิเล็กทรอนิกส์ โดย Link ที่เชื่อมกับ Host ขององค์กร ไม่มีการป้องกันใด ๆ ทั้งสิ้น แต่จะดำเนินการใช้ Data Encryption ให้แต่ละ Line ในอนาคต

(66) ไม่มีการจัดทำทะเบียนรับแจ้งการอายัดบัตร ATM

การรับแจ้งอายัดบัตร ATM ทางโทรศัพท์ โดยไม่มีการบันทึกเป็นลายลักษณ์อักษรในทะเบียนรับแจ้งการอายัดบัตร ATM หรือเอกสารอื่นไว้เป็นหลักฐาน หากมีปัญหาเกี่ยวกับการอายัดบัตร ATM ในภายหลังจะติดตามค้นหาสาเหตุและตรวจสอบไม่ได้

(67) ไม่มีหลักฐานในการอายัดและการถอนอายัดบัตร ATM

1) การอายัดบัตร ATM

ใบรับแจ้งการอายัดบัตร ATM บางฉบับ ไม่มีลายมือชื่อผู้ทำการอายัด และไม่บันทึกวันที่และเวลาที่ทำการอายัด

2) รายงานการอายัดและการถอนอายัดบัตร ATM

ศูนย์ประสานงานเขตจะทำการถอนอายัดบัตรตามที่รับแจ้งจากสาขา และทำลายใบรับแจ้งการอายัดบัตรที่ศูนย์ประสานงานเขตจัดทำขึ้นเมื่อครั้งที่สาขาแจ้งให้อายัดบัตรของลูกค้า โดยไม่มีการจัดทำรายงานเกี่ยวกับการทำรายการอายัดบัตรและถอนอายัดบัตรของแต่ละครั้งเพื่อให้ศูนย์ประสานงานตรวจสอบความถูกต้องและครบถ้วนของการทำรายการ

ข้อแนะนำ

กำหนดระเบียบปฏิบัติเกี่ยวกับการอายัดบัตร ATM และการถอนอายัดบัตร ATM ให้ชัดเจน โดยมีรายละเอียดอย่างน้อยในเรื่องต่าง ๆ ดังนี้

1) สาขาควรแจ้งการอายัดบัตร ATM ให้ศูนย์ประสานงานเป็นลายลักษณ์อักษร หลังจากที่แจ้งการอายัดบัตรทางโทรศัพท์แล้ว

2) ให้ผู้ทำการอายัดบัตร ATM ลงลายมือชื่อ วันที่ และเวลา ทุกครั้งที่ทำการอายัดบัตร ATM เพื่อเป็นหลักฐานการทำรายการ และเป็นการป้องกันข้อผิดพลาดจากการลืมทำการอายัดบัตร ATM

3) การถอนอายัดบัตร ATM ศูนย์ประสานงานเขตควรรับแจ้งจากสาขาเป็นลายลักษณ์อักษรทุกครั้ง

4) ใบรับแจ้งการอายัดบัตร ATM ควรเก็บไว้เป็นหลักฐานในการตรวจสอบ ไม่ควรทำลายทันทีที่ทำการถอนอายัดบัตร ATM

(68) **ไม่มีการบันทึกหลักฐานในการมอบบัตร ATM ที่ถูกอายัดคืนให้ลูกค้า**

เมื่อลูกค้ามาขอรับบัตร ATM ที่เครื่อง ATM ยึดไว้ คืนจากสาขา สาขาจะตรวจสอบ ชื่อ-นามสกุลของลูกค้ากับบัตรประจำตัวประชาชนหรือบัตรอื่น ๆ ที่ทางราชการเป็นผู้ออกให้ซึ่งมีรูปเจ้าของบัตรปรากฏอยู่ ถ้าถูกต้องตรงกันก็จะคืนบัตร ATM แก่ผู้มาขอรับบัตร โดยไม่มีการบันทึกการคืนบัตรแก่ลูกค้าและไม่มีการเซ็นรับบัตร ATM คืนไว้เป็นหลักฐาน

ข้อแนะนำ

1) ใบรับแจ้งการอายัดบัตร ATM ควรมีลำดับที่กำกับเพื่อสามารถตรวจสอบความครบถ้วนของการทำรายการ

2) ควรมีรายงานแสดงรายละเอียดการทำรายการอายัดบัตร ATM และการถอนอายัดบัตร ATM ที่ถูกเครื่องยึด ซึ่งอยู่ในความรับผิดชอบของสาขา สาขาควรจัดทำทะเบียนบันทึกรายละเอียดบัตร ATM ที่ได้รับจากศูนย์ประสานงานเขต และที่จ่ายให้ลูกค้า พร้อมทั้งบันทึกเลขที่บัตรประจำตัวลูกค้าและให้ลูกค้าลงลายมือชื่อในทะเบียนไว้เป็นหลักฐาน

(69) **สาขาไม่ได้จัดทำรายงานพิเศษสำหรับรายการที่ได้ทำการอายัดหรือยกเลิกการอายัดบัตร ATM แล้ว** เพื่อส่งให้สาขาเจ้าของบัญชีลูกค้าใช้เป็นหลักฐานในการตรวจสอบว่า ผู้ควบคุมเครื่อง ATMC ได้ทำการอายัดและยกเลิกการอายัดบัตร ATM ครบถ้วนตามที่สาขาเจ้าของบัญชีได้แจ้งไว้ นอกจากนี้พนักงานทำรายการอายัดบัตรยกเลิกการอายัดบัตร ATM ไม่ได้ลงลายมือชื่อในใบคำขอเปลี่ยนแปลงข้อมูลและบัตรเอทีเอ็ม ด้วย ทำให้ไม่ทราบว่าใครเป็นผู้ทำรายการดังกล่าว

ข้อแนะนำ

ควรให้พนักงานเทลเลอร์ซุปเปอร์ไวเซอร์ 1 ที่ทำหน้าที่ด้านการประมวลผล จัดทำรายงานการอายัดหรือยกเลิกการอายัดบัตร ATM ให้เป็นไปตามระเบียบปฏิบัติ แล้วส่งให้สาขาเจ้าของบัญชีตรวจสอบว่าได้ทำการอายัดและยกเลิกการอายัดบัตร ATM ตามที่ได้แจ้งมาแล้ว นอกจากนี้ ควรให้พนักงานที่ทำรายการอายัดหรือยกเลิกการอายัดบัตร ATM ลงลายมือชื่อและเวลาในใบคำขอเปลี่ยนแปลงข้อมูลและบัตรเอทีเอ็มด้วย

(70) **ใบคำขอเปลี่ยนแปลงข้อมูลและบัตรเอทีเอ็ม ที่ใช้บันทึกข้อมูลและลงลายมือชื่อบุคคลที่เกี่ยวข้องในกระบวนการทำลายอายัดและยกเลิกการอายัดบัตรนั้น** ปรากฏว่าสาขาบันทึกชื่อพนักงานสาขาอื่น ผู้ที่รับแจ้งให้อายัดบัตรทางโทรศัพท์ไม่ครบถ้วนทุกฉบับ ทำให้ขาดหลักฐานอ้างอิงผู้ทำรายการอายัด

ข้อแนะนำ

หลังจากที่สาขาผู้ใช้ระบบงาน ATM โทรศัพท์แจ้งให้หน่วยงานด้านการประมวลผลทำรายการอายัดบัตร ATM แล้ว ควรบันทึกชื่อพนักงานของสาขาที่รับโทรศัพท์ ไว้ในคำขอเปลี่ยนแปลงข้อมูลและบัตรเอทีเอ็มไว้ด้วย

(71) **หน่วยงานด้านการประมวลผลจะทำรายการยกเลิกหรือถอนอายัดบัตร ATM** หลังจากที่ได้รับแจ้งทางโทรศัพท์ และให้สาขาเจ้าของบัญชีส่งใบคำขอเปลี่ยนแปลงข้อมูลและบัตรเอทีเอ็มมาให้ภายหลัง โดยไม่ได้กำหนดผู้มีอำนาจในการแจ้งยกเลิกหรือถอนอายัดบัตรทางโทรศัพท์และขั้นตอนการปฏิบัติงาน เพื่อใช้ยืนยันได้ว่ามีการแจ้งยกเลิกหรือถอนอายัดบัตร ATM อย่างถูกต้อง

ข้อแนะนำ

ควรกำหนดให้พนักงานทำรายการยกเลิกหรือถอนอายัดบัตร ATM เมื่อได้รับใบคำขอเปลี่ยนแปลงข้อมูลและบัตรเอทีเอ็ม จากสาขาเจ้าของบัญชีแล้ว หากจำเป็นต้องทำรายการดังกล่าวทันทีเมื่อได้รับแจ้งทางโทรศัพท์ ก็ควรกำหนดให้พนักงานบริหารสาขาที่ควบคุมบัญชีนั้นมีอำนาจแจ้งให้ทำรายการยกเลิกหรือถอนอายัดบัตร ATM ทางโทรศัพท์ ทั้งนี้ เพื่อเป็นการยืนยันได้ว่าสาขาเจ้าของบัญชีเป็นผู้แจ้งให้ทำรายการยกเลิกหรือถอนอายัดบัตร ATM ทางโทรศัพท์ ทั้งนี้ เพื่อเป็นการยืนยันได้ว่าสาขาเจ้าของบัญชีเป็นผู้แจ้งให้ทำรายการดังกล่าว

(72) **การเก็บรักษาแผ่นโปรแกรมออกรหัส (PIN CODE LISTING) ไม่ปลอดภัยเท่าที่ควร**

ผู้มีหน้าที่จัดทำซองรหัส ได้เก็บรักษาแผ่นโปรแกรมการออกรหัส (PIN CODE LISTING) ไว้ในตู้เหล็กเก็บเอกสารภายในห้องมั่นคงชั้น 3 ปะปนกับเอกสารอื่นภายในตู้นั้น ซึ่งบางครั้งได้มอบกุญแจเปิดตู้เหล็กดังกล่าวให้พนักงานอื่นมาหยิบเอกสารภายในตู้ได้ และมิได้จัดทำทะเบียนควบคุมการนำเข้า/ออกแผ่นโปรแกรมทำซองรหัส การเก็บรักษาแผ่นโปรแกรมในลักษณะดังกล่าวยังไม่มีความปลอดภัยและรัดกุมเท่าที่ควร

(73) **ไม่มีการควบคุมบัตรเสีย**

บัตรเสียจากการทำบัตรถือเป็นสินทรัพย์ที่สำคัญอย่างหนึ่งขององค์กร ซึ่งต้องมีการควบคุมภายในที่ดีส่วนเอทีเอ็มเพียงแต่เจาะรูที่แถบแม่เหล็ก ไม่มีทะเบียนควบคุม และไม่มีการตรวจนับเป็นครั้งคราว ทำให้บัตรเสียดังกล่าวล่อแหลมต่อการนำออกไปดัดแปลงใหม่ เพื่อนำมาใช้ประกอบการทุจริตได้โดยง่าย

ข้อแนะนำ

ควรจัดทำทะเบียนควบคุมบัตรเสียจากการทำบัตร และควรมีการตรวจนับเป็นครั้งคราว

(74) ไม่มีระเบียบปฏิบัติเกี่ยวกับการทำลายบัตร ATM

องค์กรไม่ได้กำหนดระเบียบการทำลายบัตร ATM ไว้เป็นแนวทาง อาจทำให้มีการปฏิบัติที่ไม่เหมาะสม หรือไม่มีการควบคุมการทำลายบัตร ATM เท่าที่ควร

(75) การทำลายบัตร ATM ที่เลิกใช้แล้ว

การทำลายบัตร ATM ที่เลิกใช้แล้วโดยไม่มีคณะกรรมการทำลายบัตร หรือไม่มีพนักงานที่เป็นตัวแทนจากฝ่ายต่าง ๆ ร่วมสังเกตการตรวจนับบัตร ATM และเป็นพยานในการทำลายบัตร ATM โดยใกล้ชิด เป็นวิธีปฏิบัติที่ยังไม่รัดกุมเท่าที่ควร

ข้อแนะนำ

ควรมีคณะกรรมการทำลายบัตร ATM หรือมีตัวแทนจากฝ่ายต่าง ๆ ร่วมสังเกตการตรวจนับบัตร ATM และเป็นพยานในการทำลายบัตร ATM ที่เลิกใช้ทุกครั้ง เพื่อให้การควบคุมดูแลการจัดทำบัตร ATM มีความรัดกุมยิ่งขึ้น ควรติดตั้งเครื่องจักรและอุปกรณ์ทำบัตร ATM แยกเป็นสัดส่วน ไม่ปะปนกับเครื่องจักรและอุปกรณ์คอมพิวเตอร์ชุดอื่น ๆ

(76) ไม่มีการกระทบยอดตรวจนับบัตร ATM กับทะเบียนคุมเป็นครั้งคราว

การกำหนดให้ศูนย์บริหาร ATM จัดทำทะเบียนคุมบัตร ATM แยกประเภทเป็นบัตรที่ทำเสร็จสมบูรณ์ และบัตรเสีย โดยไม่มีการตรวจนับบัตรเปล่ากระทบยอดกับทะเบียนคุมเป็นครั้งคราวนั้น อาจมีบัตรเปล่าสูญหายโดยไม่ทราบสาเหตุได้

นอกจากนี้ บัตร ATM และซองเอกสารรหัสประจำตัวผู้ถือบัตร ATM ที่ลูกค้ายังไม่มารับซึ่งเก็บไว้ที่สาขาต่าง ๆ ก็มิได้มีการกำหนดให้มีการตรวจนับเป็นครั้งคราวเช่นเดียวกัน

(77) มีการส่งมอบบัตร ATM ของลูกค้าให้ผู้อื่น

จากการที่องค์กรได้มีการรณรงค์ให้ลูกค้ามาใช้บัตร ATM นั้น ปรากฏว่ามีพนักงานขององค์กรที่เป็นผู้แนะนำลูกค้า ได้รับมอบบัตร ATM และซองเอกสารรหัสประจำตัวผู้ถือบัตร ATM แทนลูกค้าไปแล้ว แต่ในภายหลังพบว่าลูกค้ายังไม่ได้รับบัตร องค์กรจึงได้อายัดบัตรของลูกค้า

(78) มีการให้บริการ ATM นอกเวลาทำการโดยไม่ได้รับอนุญาต

องค์กรได้เปิดให้บริการ ATM แก่ลูกค้าโดยถอนเงินจากบัญชีเงินฝากออมทรัพย์ที่ติดตั้งอยู่ ณ สำนักงานใหญ่ หลังเวลาทำการปกติ (8.30 น. -15.30 น.) ตามเงื่อนไขและหลักเกณฑ์การอนุญาตให้ใช้เครื่อง ATM โดยไม่ได้รับอนุญาตหลายรายการ

(79) การควบคุมการเปิดบริการ ATM ในเวลาที่ได้รับอนุญาต

สาขาได้รับอนุญาตให้เปิดบริการ ATM ที่ใช้ในการฝากและถอนเงินนอกเวลาทำการได้เพียง 1 เครื่อง แต่ในระหว่างการตรวจสอบพบว่า องค์กรได้เปิดเครื่อง ATM Lobby type ที่ตั้งอยู่ภายในอาคารสำนักงานสาขาอีก 2 เครื่อง ให้บริการฝากและถอนเงินนอกเวลาทำการในวันที่สาขาเปิดดำเนินงาน ซึ่งไม่เป็นไปตามหนังสืออนุญาตที่องค์กรได้รับ

(80) รายงานการทำรายการประจำวัน (Transaction Journal) ขาดข้อมูลที่จำเป็นเพื่อการตรวจสอบ (Audit Trail)

รายงานการทำรายการประจำวันขาดข้อมูลเกี่ยวกับวันที่ของรายการ (Value Date) สำหรับรายการที่ต้องการให้ผลก่อนหรือหลังวันที่ทำรายการ (Back / Forward Date) และไม่แสดงชื่อย่อหรือรหัสของผู้ทำรายการ ทำให้ไม่สามารถตรวจสอบวันที่ของรายการที่ระบบรับไว้ และไม่สามารถระบุตัวพนักงานผู้ทำรายการได้ เนื่องจากระบบคอมพิวเตอร์มิได้จำกัดการเข้าถึงและใช้เครื่องเทอร์มินัลเฉพาะพนักงานป้อนข้อมูลเท่านั้น ซึ่งจะส่งผลกระทบต่อการคำนวณดอกเบี้ยเงินเบิกเกินบัญชีขององค์กรได้

ข้อแนะนำ

องค์กรควรให้เจ้าหน้าที่ผู้รับผิดชอบทำการสอบถามความสมบูรณ์และถูกต้องของรายการที่มีผลย้อนหลังทุกรายการ และกำหนดให้มีข้อมูลสำหรับใช้เป็นหลักฐานในการติดตามและตรวจสอบรายการอย่างเพียงพอ

(81) ความเสียหายที่เกิดขึ้นเนื่องจากการให้บริการ ATM

ลูกค้าองค์กร ก. มีเจตนากระทำการทุจริต โดยอาศัยจุดอ่อนของระบบงาน ATM และเครื่อง ATM ขององค์กร ข. โดยพยายามทำการทุจริตที่เครื่อง ATM ทั้งหมด 15 แห่ง ได้เงินสดจากเครื่อง ATM 8 แห่ง ซึ่งองค์กร ข. ต้องเป็นผู้รับผิดชอบความเสียหายที่เกิดขึ้นตามข้อตกลงระหว่างองค์กร ใน ATM Pool นี้ที่กำหนดไว้ว่าในกรณีที่มีปัญหาที่เครื่อง ATM และมีการจ่ายเงินผิดพลาดองค์กรเจ้าของเครื่อง ATM เป็นผู้รับผิดชอบ และองค์กรเจ้าของบัญชีจะเป็นผู้ติดตามตัวลูกค้าให้

จากการตรวจสอบระบบงานและวิธีปฏิบัติงานเกี่ยวกับระบบงาน ATM ขององค์กรพอสรุปจุดอ่อนที่เปิดโอกาสให้ทำการทุจริตในกรณีที่เกิดขึ้นได้ ดังนี้

1) ระบบงาน ATM ขององค์กรมีจุดอ่อนในการบันทึกรายการถอนเงินสดเพื่อตัดบัญชีลูกค้า เนื่องจากองค์กรกำหนดให้มีการล้างรายการถอนเงินสด (Reverse Entry) เมื่อมีปัญหาขัดข้องที่ช่องจ่ายเงินแต่ในบางกรณีการล้างรายการดังกล่าวได้กระทำในช่วงที่เครื่อง ATM รุ่นที่องค์กรนำ Software และ Hardware ดังกล่าวให้เป็นประโยชน์ในการทุจริต

2) ระบบงาน ATM ของทุกองค์กรใน ATM Pool ไม่ได้กำหนดจำนวนครั้งของการถอนเงินของแต่ละบัญชีในหนึ่งวันตามที่ได้มีการตกลงกันไว้ ซึ่งเป็นการเปิดโอกาสให้ผู้ทุจริตกระทำการได้หลายครั้ง และก่อให้เกิดความเสียหายได้มากขึ้น ซึ่งองค์กรอาจเสียหายน้อยลงหากมีการกำหนดจำนวนครั้งการถอนเงินสดของแต่ละบัญชีในหนึ่งวัน เช่น ถ้ากำหนดไว้ 4 ครั้งต่อวัน

3) องค์กรไม่จัดให้มีพนักงานปฏิบัติงานเกี่ยวกับเครื่อง ATM ขององค์กรที่ให้บริการนอกเวลาทำการตามสาขาต่าง ๆ ในระหว่างวันหยุดทำการเป็นผลให้การติดตามปัญหาที่เกิดขึ้นที่เครื่อง ATM ของธนาคารในระยะเวลาที่กล่าวบางกรณีไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้ทันท่วงทีเป็นผลให้เกิดความเสียหายมากขึ้น แม้ศูนย์คอมพิวเตอร์สามารถแก้ไขปัญหาได้ เพราะจะต้องมีการแก้ไขปัญหาที่เครื่อง ATM ซึ่งติดตั้งอยู่ที่สาขาขององค์กรควบคู่กับเครื่อง ATMC ที่ศูนย์คอมพิวเตอร์ขององค์กรที่ใช้ในการควบคุมการทำงานของเครื่อง ATM

4) ก่อนเกิดการทุจริต ได้มีการทำรายการในลักษณะเดียวกัน โดยทำผ่านเครื่อง ATM ที่สาขาต่าง ๆ มาแล้ว 5 ครั้ง ทางฝ่ายตรวจสอบขององค์กรได้รับแจ้งจากสาขาเพียง 2 ครั้งเท่านั้นและทางส่วนตรวจสอบคอมพิวเตอร์ขององค์กรไม่ได้ตรวจสอบสาเหตุของข้อผิดพลาดที่เกิดขึ้นอย่างต่อเนื่อง เพื่อจะได้แก้ไขปัญหาที่เกิดขึ้นอย่างรวดเร็ว

ข้อแนะนำ

1) องค์กรควรกำหนดจำนวนครั้งในการถอนเงินผ่านเครื่อง ATM ต่อวัน เพราะในปัจจุบันลูกค้าสามารถถอนเงินได้ถึง 100 ครั้งต่อวัน ภายในวงเงิน 10,000 บาท ตามที่องค์กรกำหนดให้ลูกค้าถอนได้ต่อวัน ซึ่งเกินความจำเป็นและทำให้สิ้นเปลืองค่าใช้จ่าย เวลา ในการใช้เครื่องคอมพิวเตอร์ประมวลผลและพิมพ์รายงานต่าง ๆ ที่เกี่ยวข้อง นอกจากนี้ จำนวนผู้ใช้บริการ ATM ขององค์กรเพิ่มขึ้นเรื่อย ๆ ดังนั้น การลดจำนวนครั้งในการถอนเงินของลูกค้าแต่ละราย จะช่วยเพิ่มการให้บริการแก่ผู้ใช้บริการได้มากขึ้น

2) องค์กรควรจัดให้มีพนักงานปฏิบัติงานนอกเวลาทำการ เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้นกับเครื่อง ATM ได้ทันท่วงที และเปิดบริการลูกค้าได้อย่างต่อเนื่อง ซึ่งเป็นการปฏิบัติตามเงื่อนไขที่ได้รับอนุญาตเกี่ยวกับวันและเวลาทำการของเครื่อง ATM ด้วย

3) องค์กรควรให้ความสำคัญต่อปัญหาที่เกิดขึ้นเนื่องจากการให้บริการ ATM ทุกกรณี และดำเนินการตรวจสอบหาสาเหตุของข้อผิดพลาดอย่างจริงจัง เพื่อแก้ไขปัญหาที่เกิดขึ้นและหามาตรการป้องกันไม่ให้มีปัญหาในกรณีเดียวกันเกิดขึ้นอีก นอกจากนี้องค์กรควรให้ฝ่ายตรวจสอบและศูนย์คอมพิวเตอร์ร่วมกันศึกษา และกำหนดปัญหาที่เกิดขึ้นที่เครื่อง ATM เรื่องใดบ้างที่พนักงานสาขาต้องแจ้งให้ฝ่ายตรวจสอบและศูนย์คอมพิวเตอร์ทราบโดยเคร่งครัด

(82) ข้อบกพร่องที่เกิดขึ้นจากการร่วมใช้ระบบงาน ATM

จากการที่องค์กรได้ร่วมให้บริการ ATM Pool กับองค์กร ก. และองค์กร ค. จากการตรวจสอบระบบงาน ATM ขององค์กร และจากเอกสารขององค์กรใน Pool แล้ว พบว่า การทำงานของโปรแกรม ระบบสื่อสาร และการปฏิบัติงานของพนักงานที่เกี่ยวข้อง ยังมีจุดบกพร่อง ซึ่งมีผลกระทบต่อความถูกต้องของข้อมูลทางการเงิน การควบคุมภายใน การบันทึกบัญชีทั้งขององค์กรเองและองค์กรใน Pool และอาจก่อให้เกิดความเสียหายต่อองค์กรและลูกค้าได้ ดังนี้

1) การบันทึกรายการในระบบ ATM มีข้อผิดพลาดทั้งในกรณีลูกค้าองค์กรไปทำรายการที่เครื่อง ATM ขององค์กรอื่นใน Pool และลูกค้าองค์กรอื่นใน Pool มาทำรายการที่เครื่อง ATM ขององค์กรดังนี้

1.1) กรณีลูกค้าขององค์กรถอนเงินจากเครื่อง ATM ขององค์กรอื่นใน Pool โดยเครื่อง ATM ไม่จ่ายเงิน แต่ตัดบัญชีลูกค้า และมีรายการปรากฏในรายงาน "Daily Transaction Report" ที่บันทึกรายการในบัญชีเงินฝากกระแสรายวันระหว่างกัน และบัญชีเงินฝากขององค์กร เกิดข้อผิดพลาด ดังนี้

ก. มีรายการในรายงานจากเครื่อง Tandem ของทั้ง 2 องค์กร เป็นผลให้บัญชีเงินฝากขององค์กรแสดงยอดรวมต่ำกว่าความเป็นจริง และการบันทึกบัญชีเงินฝากกระแสรายวันแสดงยอดมากกว่าความเป็นจริง

ข. มีรายการในรายงานเฉพาะเครื่อง Tandem ขององค์กรเท่านั้น ของรายวันระหว่างกันไม่ถูกต้องตรงกัน และบัญชีเงินฝากขององค์กรแสดงยอดรวมต่ำกว่าความเป็นจริง

ค. มีรายการในรายงานของเครื่อง Tendem องค์กรอื่น แต่ไม่ปรากฏในรายงานขององค์กรเป็นผลให้การบันทึกบัญชีเงินฝากกระแสรายวันระหว่างกันไม่ถูกต้องตรงกัน และบัญชีเงินฝากขององค์กรแสดงยอดรวมต่ำกว่าความเป็นจริง

ง. ไม่มีรายการในรายงาน "Daily Transaction Report" ของทั้ง 2 องค์กร เป็นผลให้บัญชีเงินฝากขององค์กรแสดงยอดรวมต่ำกว่าความเป็นจริง

1.2) ลูกค้าขององค์กรถอนเงินจากเครื่อง ATM ขององค์กรอื่นใน Pool แต่ทำรายการไม่สำเร็จ และมีการแก้ไขรายการถอนเงินในรายงาน "Daily Transaction Report" ขององค์กรอื่น ปรากฏการแก้ไขรายการ 1 ครั้งถูกต้อง แต่ในรายงานขององค์กรได้แสดงรายการแก้ไขถึง 2 ครั้งซึ่งไม่ถูกต้อง และมีการเพิ่มยอดเงินฝากให้ลูกค้า เป็นผลให้ยอดรวมเงินฝากขององค์กรสูงกว่าความเป็นจริง

1.3) ลูกค้าขององค์กรถอนเงินจากเครื่อง ATM ขององค์กรอื่นใน Pool ทำรายการสำเร็จและเครื่อง ATM จ่ายเงินถูกต้อง แต่ไม่ตัดบัญชีลูกค้าเพราะมีการแก้ไขรายการถอนเงินในรายงาน "Daily Transaction Report" ของทั้ง 2 องค์กร เป็นผลให้ยอดรวมเงินฝากขององค์กรสูงกว่าความเป็นจริง

1.4) ลูกค้าองค์กรอื่นใน Pool ทำรายการถอนเงินจำนวน 7,600 บาท ที่เครื่อง ATM ขององค์กรนั้น แต่เครื่องจ่ายเงินให้เพียง 7,500 บาท ซึ่งน้อยกว่าจำนวนเงินที่ถอน 100 บาท และลูกค้าขององค์กรได้ทำรายการถอนเงินจำนวน 1,000 บาท ที่เครื่องเดียวกันในลำดับต่อมา แต่เครื่อง ATM จ่ายเงินให้ 1,100 บาท มากกว่าจำนวนเงินที่ถอน 100 บาท เป็นผลให้การบันทึกบัญชีเงินฝากกระแสรายวันระหว่างกันไม่ถูกต้องตรงกัน

1.5) ลูกค้าองค์กรอื่นใน Pool มาทำรายการถอนเงินจากเครื่อง ATM ขององค์กร 2 รายการ จำนวน 7,000 บาท และ 500 บาท ตามลำดับ เครื่องจ่ายเงินให้ครบถ้วน 7,500 บาท ใน Journal Tape แสดงยอดถูกต้องทั้ง 2 รายการและตัดบัญชีลูกค้าถูกต้อง แต่ในรายงานการเคลื่อนไหวประจำวัน แสดงรายการถอนเงิน

เพียง 6,500 บาท เนื่องจากมีการ Reverse รายการ 2 ครั้ง ๆ ละ 500 บาท โดยทำการ Reverse รายการถอน 7,000 บาท เพียงบางส่วน และ Reverse รายการถอน 500 บาททั้งจำนวน เป็นผลให้การบันทึกบัญชีเงินฝากกระแสรายวันระหว่างกันไม่ถูกต้องจำนวน 1,000 บาท

1.6) ลูกค้าองค์กรอื่นใน Pool มาทำรายการถอนเงินจากเครื่อง ATM ขององค์กร โดยมีรายการทุกอย่างถูกต้องทั้งหมด ยกเว้นรายงานคอมพิวเตอร์ที่สาขาได้รับจากศูนย์คอมพิวเตอร์สำนักงานใหญ่มีข้อมูลไม่ครบถ้วนและไม่ถูกต้อง เช่น รายการถอน 1,000 บาท ในรายงานคอมพิวเตอร์แสดงจำนวนเงินเพียง 200 บาท หรือไม่ปรากฏรายการถอนในรายงานคอมพิวเตอร์ เป็นต้น เป็นผลให้การบันทึกบัญชีระหว่างกันของสาขากับสำนักงานใหญ่ไม่ถูกต้องตรงกัน

1.7) ลูกค้าองค์กรอื่นใน Pool มาทำรายการถอนเงินจากเครื่อง ATM ขององค์กร เครื่อง ATM ไม่จ่ายเงิน แต่ตัดบัญชีลูกค้า และในรายงานที่ได้จากเครื่อง Tandem แสดงรายการตัดบัญชีส่วนข้อมูลที่ปรากฏใน Journal Tape แสดงจำนวนเงินที่ถอนเป็น 0.00 บาท เป็นผลให้การบันทึกรายการใน Journal Tape ซึ่งใช้ในการตรวจสอบการทำรายการของเครื่อง ATM และสลิปรายการที่ให้ลูกค้าไม่ถูกต้อง

1.8) ลูกค้าองค์กรอื่นใน Pool มาทำรายการถอนเงินจากเครื่อง ATM ขององค์กร 1 รายการ เครื่อง ATM จ่ายเงินถูกต้อง แต่มีการตัดบัญชีลูกค้า 2 ครั้ง สำหรับรายงานที่ได้จาก Tandem แสดงรายการตัดบัญชี 1 ครั้งถูกต้อง

2) **ข้อผิดพลาดที่เกิดจากพนักงานขององค์กรและองค์กรอื่นใน Pool ที่มีหน้าที่เกี่ยวข้องกับ ATM ปฏิบัติงานไม่ถูกต้อง**

2.1) พนักงานขององค์กรได้จัดส่งซองเงินฝากของลูกค้าองค์กรซึ่งฝากผ่านเครื่อง ATM ขององค์กร ไปให้องค์กรอื่นใน Pool เพื่อนำเข้าบัญชี การปฏิบัติผิดพลาดดังกล่าวอาจก่อให้เกิดความเสียหายต่อลูกค้าและองค์กรได้ และมีผลให้การบันทึกบัญชีเงินฝากกระแสรายวันระหว่างกันไม่ถูกต้องตรงกัน

2.2) พนักงานขององค์กรกรอกเลขที่บัญชีลงในรายละเอียดการรับฝากต่างองค์กรและจัดส่งไปให้องค์กรเจ้าของบัญชีใน Pool เป็นผลให้องค์กรนั้นป้อนรายการเข้าบัญชีลูกค้าผิดบัญชี

2.3) ลูกค้าขององค์กรได้นำเช็คไปฝากเข้าบัญชีผ่านเครื่อง ATM ขององค์กรอื่นใน Pool แต่พนักงานขององค์กรเจ้าของเครื่อง ATM ได้ประทับตราขีดคร่อมผิดเป็นอีกองค์กรหนึ่งใน Pool ไม่ใช่ชื่อขององค์กรเป็นผลให้องค์กรที่มีชื่อระบุจากการประทับตราขีดคร่อมในเช็คเป็นผู้เรียกเก็บเงินตามเช็คแทน จากความผิดพลาดดังกล่าวข้างต้นอาจก่อให้เกิดความเสียหายต่อองค์กรและลูกค้าได้

2.4) ลูกค้าขององค์กรใน Pool นำเงินสดฝากผ่านเครื่อง ATM ต่างองค์กรปรากฏว่าพนักงานขององค์กรเจ้าของเครื่อง ATM กรอกแบบฟอร์มใบปะหน้าซองเงินฝากเกี่ยวกับจำนวนเงินฝากไม่ถูกต้องแล้วจัดส่งให้องค์กรเจ้าของบัญชีเพื่อป้อนข้อมูลรายการฝากเข้าบัญชีให้ลูกค้า จากข้อผิดพลาดดังกล่าวข้างต้นเป็นผลให้การบันทึกบัญชีเงินฝากกระแสรายวันระหว่างกันไม่ถูกต้อง องค์กรเจ้าของบัญชีอาจเสียหายได้หากยอดเงินฝากที่ผิดสูงกว่าความเป็นจริงและลูกค้าอาจเสียหายได้ถ้าหากยอดเงินฝากที่ผิดต่ำกว่าความเป็นจริง

3) ข้อผิดพลาดที่เกิดจากลูกค้าผู้ใช้บริการ ATM ขององค์กรเอง และองค์กรอื่นใน Pool

3.1) ลูกค้าขององค์กรไปทำรายการถอนผ่านเครื่อง ATM ขององค์กรอื่นใน Pool เครื่อง ATM จ่ายเงินให้ ตัดบัญชีลูกค้า และมีรายการปรากฏในรายงาน "Daily Transaction Report" จากเครื่อง Tandem ของทั้ง 2 องค์กร แต่ลูกค้าไม่ได้นำเงินออกไปจากช่องจ่ายเงิน และองค์กรเจ้าของเครื่อง ATM ได้เก็บเงินสดไว้ เป็นผลให้การบันทึกเงินฝากกระแสรายวันระหว่างกันไม่ถูกต้องตรงกัน และบัญชีเงินฝากขององค์กรแสดงยอดรวมต่ำกว่าความเป็นจริง

3.2) ลูกค้าองค์กรอื่นใน Pool ได้ทำรายการฝากเงินสดผ่านเครื่อง ATM ขององค์กร แต่ทำรายการไม่สำเร็จเนื่องจากลูกค้าไม่ปฏิบัติตามขั้นตอนที่กำหนดไว้ในระบบงาน กล่าวคือ ลูกค้าใส่ซองเงินฝากในช่องรับฝากช้ากว่าเวลาที่กำหนดไว้ เป็นผลให้ซองเงินฝากดังกล่าวค้างอยู่ระหว่างประตูด้านนอกกับกล่องรับเงินฝากในช่องรับฝากเงิน และลูกค้าไม่ได้เขียนชื่อ เลขที่บัญชี และจำนวนเงินไว้บนซองเงินฝาก

ข้อแนะนำ

ข้อผิดพลาดที่เกิดขึ้นจะมีผลกระทบต่อความถูกต้องของข้อมูลทางการเงิน เป็นผลให้การบันทึกบัญชีไม่ถูกต้องทั้งสองขององค์กรเองและองค์กรอื่นใน Pool และยังกระทบต่อการควบคุมภายในขององค์กร ซึ่งอาจก่อให้เกิดความเสียหายต่อองค์กรและลูกค้าขององค์กรได้ ดังนั้นองค์กรควรดำเนินการในเรื่องต่อไปนี้

1) เมื่อเกิดข้อผิดพลาดเนื่องจากโปรแกรมระบบงาน ระบบสื่อสาร หรืออุปกรณ์ที่ใช้ในระบบ ATM และมีผลต่อความถูกต้องของข้อมูลทางการเงินแล้ว ฝ่ายตรวจสอบและศูนย์คอมพิวเตอร์ขององค์กรควรร่วมหาสาเหตุและดำเนินการแก้ไขปัญหาและกำหนดมาตรการป้องกันปัญหาไม่ให้เกิดขึ้นอีก พร้อมทั้งกำหนดขั้นตอนในการปฏิบัติงานให้พนักงานที่มีหน้าที่เกี่ยวข้องในการตรวจสอบเอกสารและการบันทึกบัญชีไว้เป็นลายลักษณ์อักษร และให้มีการปฏิบัติตามโดยเคร่งครัด เพราะการใช้ระบบงานและการปฏิบัติงานที่ถูกต้อง จะช่วยให้องค์กรประหยัดค่าใช้จ่ายในการติดตามแก้ไขรายการที่เกิดขึ้นจากการให้บริการ ATM และป้องกันความเสียหายที่อาจเกิดขึ้นด้วย

2) ควรจัดให้มีการอบรมพนักงานที่มีหน้าที่เกี่ยวข้องกับระบบงาน ATM ให้มีความเข้าใจระเบียบปฏิบัติงานอย่างเพียงพอ และให้มีจำนวนมากพอที่จะทำงานทดแทนกันได้ในแต่ละหน่วยงาน เพื่อให้การปฏิบัติงานและข้อมูลที่ได้รับถูกต้องเชื่อถือได้

2.4 สินเชื่อ

2.4.1 ระบบงานเงินให้สินเชื่อ

(1) ไม่มีหลักฐานการลบข้อมูล

องค์กรมิได้จัดให้มีรายงานพิเศษแสดงรายละเอียดการเปลี่ยนแปลงแก้ไขข้อมูลโดยใช้โปรแกรมงาน Maintenance Master File และมิได้กำหนดให้มีการอนุญาตหรือแจ้งแก่ผู้บริหารทราบและควบคุมดูแลการลบข้อมูลโดยใกล้ชิด

ข้อแนะนำ

ควรมีเอกสารหลักฐานแสดงการลบข้อมูลออกจากแฟ้มข้อมูลหลักของระบบเงินให้กู้ยืมโดยละเอียด

(2) ข้อผิดพลาดในการแก้ไขข้อมูล

รายงาน Ledger Report และ Accrued Interest & Outstanding Report แสดงยอดคงเหลือสำหรับลูกค้า ณ วันที่ 31 กรกฎาคม 2538 ไว้ไม่ตรงกัน

ผลการตรวจสอบพบว่า ยอดคงเหลือตามรายงานแสดงไว้ไม่ถูกต้อง เนื่องจากผู้ปฏิบัติงานป้อนข้อมูลการรับชำระดอกเบี้ยผิดตัวลูกค้า และได้แก้ไขสำหรับลูกค้ารายอื่นแล้ว แต่ยังมิได้แก้ไขข้อมูลของลูกหนี้รายนี้ให้ถูกต้อง

ข้อแนะนำ

ควรจัดระเบียบการแก้ไขข้อผิดพลาดในการป้อนข้อมูล ให้สามารถป้องกันข้อผิดพลาดที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

(3) วันที่ใช้คำนวณดอกเบี้ยของเงินให้กู้ยืมแต่ละประเภทแตกต่างกัน

วันที่ใช้คำนวณดอกเบี้ยของ Housing Loan และ Local Bill Discounted มีข้อแตกต่างจากเงินกู้ประเภทอื่น ดังนี้

- Housing Loan และ Local Bill Discounted จะเริ่มคิดดอกเบี้ยตั้งแต่วันแรกที่สัญญากู้เงินมีผลบังคับใช้ และไม่คิดดอกเบี้ยวันสุดท้ายที่ชำระหนี้ครบ
- เงินกู้ประเภทอื่น จะเริ่มคิดดอกเบี้ยตั้งแต่วันที่ 2 หลังจากวันที่สัญญากู้เงินมีผลบังคับใช้ และคิดจนกระทั่งถึงวันสุดท้ายที่ชำระหนี้ครบ

ในกรณีที่มีการเปลี่ยนแปลงอัตราดอกเบี้ยในระหว่างที่ยังมียอดหนี้คงค้างอยู่ ก็ย่อมมีผลให้ยอดคงเหลือของดอกเบี้ยแสดงไว้ไม่ตรงกัน

ข้อแนะนำ

ควรปรับปรุงแก้ไขระบบงานในส่วนที่เกี่ยวกับการตั้งดอกเบี้ยคงค้างให้ถูกต้องตามจำนวนเงินต้นและสัญญาเงินให้กู้ยืมแต่ละฉบับ เท่ากับเป็นการเรียกเก็บดอกเบี้ยส่วนหนึ่งล่วงหน้า และตัดทอนเงินชำระบางส่วนที่ลูกค้าควรมีสิทธินำไปหักต้นเงินกู้ อันจะมีผลให้ดอกเบี้ยในเดือนถัดไปลดลง เมื่อคำนวณดอกเบี้ยที่องค์กรควรเรียกเก็บจากลูกค้าเทียบกับจำนวนดอกเบี้ยที่รับจริงแล้ว ปรากฏว่าองค์กรเรียกเก็บดอกเบี้ยมากกว่าที่พึงจะเรียกเก็บจากลูกค้าได้ และอาจเกินกว่าอัตราสูงสุดที่กฎหมายกำหนดได้

(8) ข้อมูลสินเชื่อไม่เป็นปัจจุบันและไม่ถูกต้อง

รายงาน CIF Departmenta Account แสดงยอดเงินกู้ของลูกหนี้รายหนึ่ง คงค้าง 13.0 ล้านบาท แต่มีวงเงินกู้ (Limit) เพียง 6.5 ล้านบาท เนื่องจากลูกค้ารายนี้ได้รับวงเงินกู้ชั่วคราว โดยกันวงเงินจากวงเงินทรัสต์รีซีทชั่วคราวมาเพิ่มอีก 6.5 ล้านบาท รวมเป็นวงเงินกู้ 13.0 ล้านบาท เมื่อหมดความจำเป็นก็จะยกเลิกการกันวงเงินชั่วคราว

ข้อแนะนำ

องค์กรควรปรับปรุงระบบงานให้แสดงข้อมูลในรายงานโดยถูกต้องตรงกับข้อเท็จจริง

(9) ไม่มีการควบคุมการทำรายการโอน (Transfer)

พนักงานบันทึกข้อมูล (Terminal Operator) ของฝ่ายตั๋วสินค้าเข้าและสินค้าออก (Bills Department) สามารถสอบถามยอดคงเหลือ รวมทั้งรายการโอนออกจากบัญชีกระแสรายวันหนึ่งไปเข้าอีกบัญชีหนึ่งได้ ประกอบกับกุญแจที่ใช้อนุมัติการผ่านรายการ (Supervisor Key) มิได้อยู่ในการควบคุมดูแลของพนักงานที่รับผิดชอบ ทำให้เสี่ยงต่อการที่จะเกิดข้อผิดพลาดหรือความเสียหายอื่น

ข้อแนะนำ

เพื่อป้องกันข้อผิดพลาดหรือความเสียหายที่อาจเกิดขึ้น องค์กรควรจำกัดมิให้พนักงานบันทึกข้อมูลของฝ่ายอื่นนอกจากฝ่ายเงินฝากกระแสรายวัน สอบถามและเปลี่ยนแปลงยอดในบัญชีกระแสรายวันได้

(10) มีข้อผิดพลาดในการประมวลผลและการควบคุมภายในของการทำรายการ Loan (Partial) Settlement เพื่อป้อนข้อมูลหรือรายการชำระหนี้เงินให้กู้ยืม (Loan Settlement) ด้วยการหักบัญชีเงินฝากกระแสรายวันหรือเงินเบิกเกินบัญชีของลูกค้าโดยอัตโนมัติ (Auto Account) โดยโปรแกรมระบบงาน ไม่สามารถป้องกันการป้อนรายการหักบัญชีเกินกว่ายอดคงเหลือในบัญชีลูกค้าซึ่งพนักงาน Operator สามารถผ่านรายการได้โดยไม่ผ่านการอนุมัติรายการจากพนักงานชั้นบริหาร

ข้อแนะนำ

นอกจากการปรับปรุงแก้ไขโปรแกรมระบบงาน เพื่อให้สามารถควบคุมและป้องกันไม่ให้เกิดข้อผิดพลาดดังกล่าวแล้ว องค์กรควรจัดให้มีการตรวจสอบความถูกต้องของรายการเมื่อพนักงาน Operator ได้ป้อนข้อมูล ตามการทำรายการข้างต้นด้วย

(11) ไม่มีการควบคุมการตรวจสอบวงเงินให้สินเชื่อ ก่อนบันทึกรายการเงินให้สินเชื่อ

ระบบงานเงินให้สินเชื่อไม่ได้ให้เครื่องคอมพิวเตอร์ตรวจสอบการทำ Hold Fund ของพนักงานแผนก Loan Operation และการอนุมัติรายการ Hold Fund จากแผนก Exposure Control ถึงแม้ว่าระบบงานปัจจุบันมีการตรวจสอบการทำ Hold Fund และควบคุมการบันทึกรายการให้สินเชื่อที่เกินวงเงินอยู่แล้วโดยพนักงาน

ที่เกี่ยวข้อง ความผิดพลาดอันเกิดจากการบันทึกรายการให้สินเชื่อเกินวงเงินจะเกิดขึ้นไม่ได้ เพราะรายการดังกล่าวจะต้องมีการอนุมัติพิเศษก่อนการบันทึกอยู่แล้ว และหากรายการใดไม่มีการทำ Hold Fund ระบบงานในปัจจุบันก็จะตรวจสอบและออกรายงานพิเศษสำหรับรายการที่ไม่ได้ทำ Hold Fund ดังกล่าวในวันรุ่งขึ้นด้วย

ข้อแนะนำ

เพื่อให้ระบบคอมพิวเตอร์ของธนาคารอำนวยประโยชน์ทางด้านการควบคุมยิ่งขึ้น องค์กรควรปรับปรุง ระบบงานเงินให้สินเชื่อ ให้เครื่องคอมพิวเตอร์ตรวจสอบการทำ Hold Fund และการอนุมัติการทำ Hold Fund ก่อนการบันทึกรายการบัญชีเงินให้สินเชื่อเข้าระบบคอมพิวเตอร์

(12) ไม่มีการควบคุมวงเงินสินเชื่อด้วยคอมพิวเตอร์ในระหว่างวัน

แม้องค์กรจะได้บันทึก (Registration) รายละเอียดเกี่ยวกับประเภทสินเชื่อและวงเงินของลูกหนี้ตามโปรแกรมในการกำหนดวงเงินเชื่อ (Credit Line) ไว้ในแฟ้มข้อมูล (File) ก็ตามหากในระหว่างวันมีการบันทึกบัญชีการใช้สินเชื่อเกินกว่าวงเงินที่อนุมัติและบันทึกไว้แล้ว เครื่องคอมพิวเตอร์ก็จะผ่านรายการที่ป้อนให้โดยไม่มีการเช็คสอบวงเงินของลูกหนี้และไม่ต้องขอ Override จากเจ้าหน้าที่ชั้นบริหาร ซึ่งอาจก่อให้เกิดการปฏิบัติงานผิดพลาดในระหว่างวันได้ แม้จะมีรายงานประจำวัน Daily Utilized Balance of Credit Line แจ้งให้ทราบว่ามีลูกหนี้ใช้เกินวงเงินที่มีอยู่เมื่อสิ้นวันก็ตาม

ข้อแนะนำ

ควรกำหนดให้มีการเช็คสอบจำนวนเงินที่ป้อนเข้าเครื่องคอมพิวเตอร์ในการผ่านรายการต่าง ๆ ไม่ให้เกินวงเงินของลูกค้า หากจะยินยอมให้ลูกค้าใช้สินเชื่อเกินวงเงิน ก็ควรผ่านรหัสอนุมัติ (Override) จากเจ้าหน้าที่ชั้นบริหารก่อน

2.4.2 ระบบงาน Customer Facility System (CFS)

(1) การควบคุมการอนุมัติเงินให้สินเชื่อเกินวงเงินแก่ลูกค้าไม่รัดกุม

วิธีการจัดทำรายงานการอนุมัติเงินให้สินเชื่อเกินวงเงินแก่ลูกค้าที่เป็นการชั่วคราว เพื่อเสนอให้พนักงานชั้นบริหารระดับสูงรับทราบ ด้วยการใช้เครื่องไมโครคอมพิวเตอร์พิมพ์รายละเอียดโดยมิได้ใช้ระบบคอมพิวเตอร์หลักซึ่งมีข้อมูลที่เป็นปัจจุบันครบถ้วนอยู่แล้ว

ข้อแนะนำ

องค์กรควรยกเลิกรายงานที่จัดทำด้วยไมโครคอมพิวเตอร์และใช้รายงานซึ่งจัดทำโดยระบบคอม-พิวเตอร์หลักแทน

(2) มีจุดอ่อนในการสอบทานความถูกต้องของข้อมูล

การสอบทานข้อมูลลูกหนี้ที่นำเข้าระบบคอมพิวเตอร์ของแผนก Exposure Control ด้วยการนำรายงานคอมพิวเตอร์ชุด Customer Facility Transaction List ซึ่งแสดงว่า แผนก Credit Service ได้นำข้อมูลของลูกหนี้รายใดบ้างเข้าระบบคอมพิวเตอร์ มาเปรียบเทียบความถูกต้องกับรายงาน Customer Facility Report ที่แผนก Credit Service จัดทำขึ้น และส่งมาให้แผนก Exposure Control เก็บไว้ โดยไม่เรียกดูข้อมูลจริงที่เก็บไว้ในระบบคอมพิวเตอร์ผ่านทางจอภาพมาตรวจสอบความถูกต้องนั้น เป็นจุดอ่อนในการปฏิบัติงาน ทั้งนี้เพราะหากมีการแก้ไขข้อมูลที่กล่าวข้างต้นภายหลังการพิมพ์รายงานชุด Customer Facility Transaction List ผู้สอบทานความถูกต้องของข้อมูลในแผนก Exposure Control จะไม่ทราบว่าข้อมูลที่อยู่ในระบบคอมพิวเตอร์มีความถูกต้องหรือคลาดเคลื่อนไปจากความเป็นจริงเพียงใด ซึ่งอาจเกิดข้อผิดพลาดหรือการทุจริตได้

ข้อแนะนำ

ควรเรียกดูข้อมูลในระบบงาน Customer Facility System ผ่านทางจอภาพ มาสอบทานความถูกต้องและความครบถ้วนของข้อมูลนำเข้าทุกรายการ

(3) ไม่ใช้ข้อมูลปัจจุบันที่เก็บอยู่ในระบบคอมพิวเตอร์ประกอบการพิจารณาอนุมัติเงินให้สินเชื่อเกินวงเงิน

ในการพิจารณาอนุมัติเงินให้สินเชื่อเกินวงเงินแก่ลูกค้าที่เป็นการชั่วคราว ไม่เรียกใช้ข้อมูลปัจจุบันที่เก็บไว้ในระบบคอมพิวเตอร์ โดยเจ้าหน้าที่ยังคงใช้รายงานฉบับที่ไม่เป็นปัจจุบัน จะมีผลทำให้การพิจารณาอนุมัติดังกล่าวผิดพลาดได้

ข้อแนะนำ

องค์กรควรกำหนดระเบียบปฏิบัติในการใช้ข้อมูลที่ถูกต้องและเป็นปัจจุบันในการปฏิบัติงาน

2.4.3 ระบบบัตรเครดิต

(1) ไม่มีคู่มือปฏิบัติงาน (User manual) และคู่มือการใช้รายงาน

องค์กรมิได้จัดทำเอกสารประกอบระบบบัตรเครดิต คู่มือปฏิบัติงานและคู่มือการใช้รายงาน

ข้อแนะนำ

องค์กรควรเร่งพัฒนาระบบบัตรเครดิตให้เสร็จสิ้นโดยเร็ว และจัดทำคู่มือปฏิบัติงานและคู่มือการเข้ารายงานในระบบงานนี้ให้เพียงพอที่จะให้พนักงานอื่นศึกษาเพื่อให้สามารถปฏิบัติงานทดแทนกันได้เมื่อถึงคราวจำเป็น

(2) การป้องกันการบันทึกรหัสข้อมูลบนแถบแม่เหล็ก

เครื่องจักรสำหรับการบันทึกรหัสข้อมูล (Encode) บนแถบแม่เหล็กของบัตรเครดิตรุ่นเก่าที่ตั้งทิ้งไว้ที่ส่วนงานบัตรเครดิตต่างประเทศ ซึ่งไม่ได้ใช้งานแล้ว ยังไม่ได้ส่งคืนเครื่องจักรดังกล่าวให้กับส่วนงานที่รับผิดชอบเพื่อป้องกันการใช้เครื่องจักรบันทึกรหัสข้อมูลบนแถบแม่เหล็กของบัตรประเภทต่าง ๆ โดยไม่ได้รับอนุญาต

ข้อแนะนำ

เครื่องบันทึกรหัสข้อมูลลงบนแถบแม่เหล็กของบัตรเครดิตที่ตั้งทิ้งไว้ที่ส่วนงานบัตรเครดิตต่างประเทศซึ่งไม่ใช้งานแล้ว ควรส่งคืนให้กับส่วนงานที่รับผิดชอบเก็บรักษาไว้ในสถานที่ปลอดภัย เพื่อป้องกันการใช้เครื่องจักรที่กล่าวโดยไม่ได้รับอนุญาต

2.5 ต่างประเทศ

2.5.1 ระบบบัญชีต่างประเทศ (Foreign Accounting)

(1) ไม่มีการควบคุมการแก้ไขข้อมูล

องค์กรยินยอมให้พนักงานป้อนข้อมูลสามารถแก้ไขข้อมูลใน Master File ได้โดยตรงโดยไม่ต้องผ่านการอนุมัติรายการจากผู้บังคับบัญชา อันอาจมีผลกระทบต่อความถูกต้อง ครบถ้วน และเชื่อถือได้ของข้อมูล

ข้อแนะนำ

ควรปรับปรุงมาตรการป้องกันการเข้าถึง Master File และการควบคุมการแก้ไขข้อมูลใน Master File ให้รัดกุมยิ่งขึ้น

(2) ระบบธุรกิจต่างประเทศ

องค์กรไม่ได้จัดทำทะเบียนควบคุมการรับส่งเอกสารข้อมูลผลลัพธ์ของงานด้านธุรกิจต่างประเทศระหว่างสำนักงานใหญ่กับสำนักงานสาขา หากเอกสารที่กล่าวสูญหาย จะไม่มีหลักฐานเพียงพอที่จะติดตามค้นหาเอกสาร

ข้อแนะนำ

ควรจัดทำทะเบียนควบคุมการรับส่งเอกสารข้อมูลผลลัพธ์ของงานด้านธุรกิจต่างประเทศ ระหว่างสำนักงานใหญ่กับสำนักงานสาขา เพื่อประโยชน์ในการติดตามค้นหาเอกสาร

(3) ไม่มีหลักฐานการหักบัญชีเมื่อขอโอนเงินไปต่างประเทศ

จากการตรวจสอบการปฏิบัติงานด้านเงินโอนต่างประเทศ พบว่า การหักบัญชีเงินฝากของลูกค้าในบางกรณี เช่น กรณีที่ลูกค้าให้หักบัญชีจากเงินฝากประเภทออมทรัพย์ (Saving) โดยนำสมุดบัญชีเงินฝากมาให้องค์กรบันทึกบัญชีด้วยนั้น องค์กรจะให้ลูกค้านำ Slip ไปบันทึกบัญชีเงินฝากที่แผนกเงินฝากซึ่งอยู่ชั้นล่าง และนำ

สมุดขึ้นมาแสดง อาจทำให้หักบัญชีไม่ครบถ้วนหากลูกค้ามีการทำรายการโดยจะต้องหักบัญชีเงินฝากด้วยจำนวนเงินที่เท่ากันมากกว่า 1 รายการในวันดังกล่าว และอาจเป็นเหตุให้องค์กรเสียหายได้

ข้อแนะนำ

แผนกงานอื่นที่ต้องการให้แผนกเงินฝากหักบัญชีลูกค้าซึ่งมาใช้บริการในแผนกของตนควรทำหลักฐานให้แผนกเงินฝากลงนามยืนยันว่าได้มีการตัดบัญชีเพื่อรายการนั้น ๆ แล้ว และเก็บเอกสารหลักฐานนั้นเพื่อยืนยันรายการหักบัญชีต่อไปด้วย

2.5.2 ระบบงาน L/C

(1) การควบคุมการแก้ไขข้อมูล

กรณีพบข้อผิดพลาดอันเกิดจาก Key จำนวนเงินผิด และผิดตัวลูกค้า Operator แก้ไขโดยไม่ต้องได้รับอนุญาตหรือแจ้งแก่ผู้บริหารระดับสูง และไม่มีการออกรายงานแสดงการแก้ไขด้วย

การปฏิบัติดังกล่าวอาจจะก่อให้เกิดการแก้ไขข้อมูลที่เก็บอยู่ในแฟ้มข้อมูลหลัก (Master File) ได้โดยไม่ถูกต้อง และไม่มีข้อมูลที่เหลือไว้สำหรับการตรวจสอบ (Audit Trail) ประกอบกับองค์กรมิได้มีการแบ่งแยกหน้าที่เพื่อประโยชน์ในการควบคุมภายในเท่าที่ควร ซึ่งอาจก่อให้เกิดความเสียหายต่อองค์กรได้

ข้อแนะนำ

ควรกำหนดระเบียบปฏิบัติในส่วนที่เกี่ยวกับการแก้ไขข้อมูลในแฟ้มข้อมูลหลัก (Master File) ให้รัดกุมยิ่งขึ้น เพื่อเป็นการป้องกันและควบคุมหรือจำกัดขอบเขตในการทำรายการของผู้ปฏิบัติการ

(2) การ Reverse รายการ L/C ผิดตัวลูกค้า

ผู้ปฏิบัติงานสามารถ Key L/C No. ที่ต่างไปจากแฟ้มข้อมูล หรือนำ L/C No. ของลูกค้ารายอื่นมา Reverse รายการได้ ซึ่งเป็นผลให้มีข้อผิดพลาดในการ Reverse รายการ

การ Reverse รายการ L/C ผิดตัวลูกค้า เกิดจากโปรแกรมตรวจเช็ค L/C No. ของ Customer No. เฉพาะรายการที่ Converse เท่านั้น ไม่มีการเช็ค Loan No. ของ Customer อื่น

ข้อแนะนำ

ไม่ควรให้ระบบคอมพิวเตอร์ยินยอมผ่านรายการ Reverse L/C ในกรณีที่ L/C No. ที่ต้องการ Reverse ไม่ตรงกับ L/C No. ที่มีอยู่ในแฟ้มข้อมูล เพื่อป้องกันข้อผิดพลาดในการ Reverse รายการ

(3) ข้อผิดพลาดในการ Convert ข้อมูล

การ Convert ข้อมูลมาใช้เครื่องคอมพิวเตอร์ ยังมีข้อผิดพลาด

ข้อแนะนำ

ควรค้นหาสาเหตุในการ Convert ข้อมูล และตรวจสอบการบันทึกบัญชีและการประมวลผลข้อมูลด้วยคอมพิวเตอร์ ทั้งนี้เพื่อให้รายงานที่ได้จากการประมวลผลถูกต้องเชื่อถือได้

(4) **ข้อผิดพลาดในการ Update ข้อมูล**

รายงาน SUMMARY OF BALANCE ณ วันที่ 19 กรกฎาคม 2538 ซึ่งมีข้อผิดพลาดเนื่องจากพนักงาน Operator ทำการ Update ข้อมูลซ้ำ 2 ครั้ง

ข้อแนะนำ

ในการ Update ข้อมูล

1) ควรมีระเบียบห้ามแก้ไขเปลี่ยนแปลงข้อมูลหลังจากที่ได้ทำการ Update เรียบร้อยแล้ว ถ้าพบข้อผิดพลาดหลังจากนี้ ก็ให้ทำรายการ Adjust ปรับปรุง โดยมีรายงานแสดงรายการปรับปรุงไว้เป็นหลักฐานสำหรับการตรวจสอบ

2) ควรมีมาตรการที่สามารถป้องกันการ Update ข้อมูลผิดพลาด และกำชับพนักงานให้ปฏิบัติตามระเบียบโดยเคร่งครัด

3) การใช้ Utility Program ที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลได้ ควรจะกำหนดให้เจ้าหน้าที่ที่มีอำนาจมากกว่า Operator เป็นผู้ใช้โปรแกรม และควรมีระเบียบมิให้ Programmer มีส่วนเข้าไปเกี่ยวข้องกับการทำงานของคอมพิวเตอร์

2.5.3 ระบบงาน T/R (TRUST RECEIPT)

(1) **การควบคุมการแก้ไขข้อมูล**

กรณีที่ผู้ใช้ข้อมูลตรวจสอบข้อมูลที่ผิดพลาดอันเนื่องมาจากการป้อนจำนวนเงินผิดหรือผิดตัว Operator ก็จะทำการแก้ไขโดยมิต้องรับอนุญาตหรือแจ้งแก่ผู้บริหาร นอกจากนี้ยังไม่มีการออกรายงานที่แสดงการแก้ไขเหล่านี้ด้วย ซึ่งองค์กรได้ปรับปรุงแก้ไขปัญหาที่กล่าว โดยให้ User ทำบันทึกรายการแก้ไข และมี Authorize ลงนามกำกับการผ่าน I/O control ให้หัวหน้างานคอมพิวเตอร์ทราบ

ข้อแนะนำ

ควรกำหนดระเบียบปฏิบัติในส่วนที่เกี่ยวกับการแก้ไขข้อมูลในแฟ้มข้อมูลหลัก (Master File) ให้รัดกุมยิ่งขึ้น และควรมีการออกรายงานแสดงการแก้ไขทุกครั้งที่มีการแก้ไขข้อมูล

(2) การปฏิบัติงานประมวลผลข้อมูลผิดพลาด

องค์กรได้กำหนด มาตรการป้องกันการปฏิบัติงานประมวลผลข้อมูลผิดพลาดไว้ดังนี้

1) ป้องกันการ Update ซ้อน โดยมีการลงวันที่ใน Update file เพื่อใช้ตรวจเช็คเมื่อมีการเรียกโปรแกรม Update อีกครั้งหนึ่ง และให้มีการ Update ได้ 1 ครั้งต่อ 1 วันทำงานเท่านั้น

2) ป้องกันการ Double payment โดยเพิ่มการตรวจเช็คในโปรแกรม Update หากมีข้อผิดพลาดจะมี Message และยกเลิกการ Update เมื่อได้ตรวจแก้ไขข้อมูลเรียบร้อยแล้วจะใช้ Back up มาทำการ Update ใหม่

3) ใช้ Job Stream Control ป้องกันการข้ามขั้นตอนในการ Update

ข้อแนะนำ

ควรควบคุมดูแลพนักงาน Operator ให้ทำงานตามระเบียบวิธีปฏิบัติโดยครบถ้วนไม่ข้ามขั้นตอน และจัดให้มีการตรวจสอบเปรียบเทียบยอดคงเหลือที่ได้จากรายงานต่าง ๆ โดยมีการติดตามหาสาเหตุของความแตกต่างและทำการแก้ไขปรับปรุงภายในระยะเวลาที่เหมาะสม

(3) การปฏิบัติงานไม่สอดคล้องกัน

การปฏิบัติงานของระบบงาน T/R แต่ละหน่วยงานที่สัมพันธ์กันมีวิธีปฏิบัติงานต่างกันประสานงานกับหน่วย Trust receipt ฝ่ายคอมพิวเตอร์ และฝ่ายตรวจสอบ ร่วมกันดำเนินการ

ข้อแนะนำ

ควรมีการพิจารณาปรับปรุงแก้ไขระเบียบวิธีปฏิบัติในหน่วยงานต่าง ๆ ให้สอดคล้องกัน เพื่อให้สามารถตรวจสอบการปฏิบัติงานระหว่างหน่วยงานได้

(4) ข้อมูลทางการบัญชีไม่ถูกต้อง

ยอดคงเหลือตามการ์ดบัญชีรายตัวของบัญชี แตกต่างกับยอดคงเหลือที่แสดงไว้ในงบทดลอง

ข้อแนะนำ

ควรจะจัดให้มีการสอบทานบัญชีรายตัวและบัญชีคุมเป็นระยะ ๆ และควรค้นหาสาเหตุของข้อผิดพลาด และทำรายการปรับปรุงให้ถูกต้อง

2.5.4 ระบบงาน SWIFT

(1) **การบันทึกปัญหาที่เกิดขึ้นและวิธีการปรับปรุงแก้ไข**

เมื่อเกิดปัญหาในการปฏิบัติงานขึ้น ผู้ปฏิบัติงานจะติดต่อกับศูนย์บริการ (Support) ของ SWIFT โดยผ่านเครื่อง Terminal เพื่อสอบถามวิธีการแก้ไขเป็นคราว ๆ ไป โดยมิได้จดบันทึกปัญหาและวิธีการแก้ไขไว้เพื่อประโยชน์ในการแก้ปัญหากรณีเกิดปัญหาเดียวกันในครั้งต่อ ๆ ไป ซึ่งถ้าหากเป็นกรณีเร่งด่วน และไม่สามารถติดต่อกับศูนย์บริการให้ช่วยแก้ไขปัญหาได้ทันต่อเวลา ก็อาจเกิดความเสียหายต่อการดำเนินงานขององค์กรได้ รวมทั้งขาดหลักฐานไว้สำหรับตรวจสอบเพื่อปรับปรุงการปฏิบัติงานให้ดีขึ้นอีกด้วย

ข้อแนะนำ

ผู้ปฏิบัติงานควรจดบันทึกปัญหาและวิธีการปรับปรุงแก้ไข เพื่อใช้เป็นแนวทางในการควบคุมและตรวจสอบติดตามการปฏิบัติงานและการแก้ไขปัญหาของเจ้าหน้าที่ที่รับผิดชอบ

(2) **การควบคุมเอกสารการโอนเงินไม่รัดกุม**

การส่งเอกสารคำสั่งการโอนเงินผ่านระบบงาน SWIFT จากแผนก Foreign Exchange Operation ไปแผนก General Service โดยไม่ได้จัดทำทะเบียนสำหรับควบคุมการรับส่งเอกสาร และไม่มีสำเนาเอกสารดังกล่าวเก็บไว้เป็นหลักฐาน เป็นวิธีปฏิบัติที่ไม่เหมาะสม หากเอกสารสูญหายในระหว่างการส่งเอกสาร จะทำให้ไม่มีการโอนเงิน ซึ่งจะก่อให้เกิดความเสียหายได้

ข้อแนะนำ

ควรมีวิธีป้องกันเอกสารการโอนเงินสูญหายในระหว่างการส่งมอบเอกสารระหว่างแผนก โดยจัดทำทะเบียนการรับส่งเอกสารการโอนเงินระหว่างแผนก เพื่อให้สามารถตรวจสอบความถูกต้องและทราบข้อผิดพลาดได้ทันที หรือส่งเอกสารคู่ฉบับ (สำเนา) ไปให้แผนก General Service ลงลายมือชื่อ แล้วส่งคืนไปยังแผนกที่สั่งโอนเงินในวันนั้นหรือวันรุ่งขึ้น

(3) **การควบคุมการเข้าออกห้องที่ตั้งเครื่อง SWIFT ไม่รัดกุม**

องค์กรมิได้ควบคุมการเข้าออกห้องที่ตั้งเครื่อง SWIFT เท่าที่ควร บุคคลที่ไม่มีหน้าที่เกี่ยวข้องสามารถเข้าถึงเครื่อง SWIFT ได้โดยง่าย และมิได้มีการลงนามในทะเบียนทุกครั้งที่มีการเข้าออกห้องที่ตั้งเครื่อง SWIFT ตามที่องค์กรกำหนดไว้โดยเคร่งครัด นอกจากพนักงานแผนก General Service แล้ว องค์กรอนุญาตให้พนักงานแผนกอื่น ๆ ซึ่งมีหน้าที่ต้องติดต่องานกัน สามารถเข้าห้องเครื่อง SWIFT ได้โดยไม่ต้องลงทะเบียนดังกล่าว เช่น แผนก Treasury

ข้อแนะนำ

สำหรับผู้ที่มิได้รับอนุญาต หากมีธุรกิจที่จะต้องเข้าในห้อง SWIFT จะต้องได้รับอนุญาตจากหัวหน้าแผนก Telex และต้องลงชื่อและเหตุผลในทะเบียน เพื่อควบคุมการเข้าออกห้อง SWIFT

(4) การควบคุมรหัสที่ใช้ในการเปิดเครื่อง (Log-in table) ไม่รัดกุม

องค์กรมิได้ควบคุมรหัสที่ใช้ในการเปิดเครื่อง (Log-in table) อาจเป็นสาเหตุให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องสามารถเปิดเครื่อง SWIFT และทำให้เข้าถึงระบบงาน SWIFT ได้

ข้อแนะนำ

ควรเปิดเครื่อง (Log-in table) โดยมี Authorized Officer 2 คน เป็นผู้ถือรหัสที่ใช้ในการเปิดเครื่อง ซึ่งมีอยู่ 2 ชุด (ชุด A และชุด B) แยกออกจากกันคนละชุด เพื่อให้การป้องกันการเข้าถึงระบบงาน SWIFT รัดกุมยิ่งขึ้น

(5) ไม่มีการบันทึกปัญหาที่เกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ของระบบงาน SWIFT

การติดต่อกับบริษัทผู้ขายให้มาแก้ไขปัญหาในการปฏิบัติงาน โดยมิได้จดบันทึกปัญหาที่เกิดขึ้นและวิธีการแก้ไข และไม่ได้แจ้งให้ผู้ตรวจสอบภายในทราบถึงปัญหาที่เกิดขึ้น เป็นวิธีปฏิบัติที่ไม่เหมาะสม และมีผลทำให้องค์กรไม่มีข้อมูลที่เป็นประโยชน์ในการวิเคราะห์ปัญหาที่เกิดขึ้น และขาดหลักฐานไว้สำหรับตรวจสอบเพื่อปรับปรุงการปฏิบัติงานให้ดีขึ้นอีกด้วย

ข้อแนะนำ

ควรจดบันทึกปัญหาการใช้เครื่องคอมพิวเตอร์และวิธีการปรับปรุงแก้ไข เพื่อให้มีข้อมูลเพียงพอต่อการวิเคราะห์ปัญหา และใช้เป็นแนวทางในการควบคุมและตรวจสอบติดตามการปฏิบัติงานและการแก้ไขปัญหาของเจ้าหน้าที่ที่รับผิดชอบ รวมทั้งควรจัดทำรายงานแจ้งให้ผู้ตรวจสอบภายในทราบด้วย

2.6 บัญชี

2.6.1 ระบบงานบัญชี

(1) การควบคุมข้อมูลนำเข้า

ฝ่ายบริหารการเงินมีหน้าที่จัดทำสลิป ตรวจสอบความถูกต้อง และลงลายมือชื่ออนุมัติรายการพร้อมกับรวบรวมสลิปไว้ในตะแกรงลวด เฉพาะในส่วนของบริหารการเงิน หลังจากนั้นในระหว่างเวลา 15.30 -16.00 น. เจ้าหน้าที่ฝ่ายบัญชีจะมารับตะแกรงลวดที่ใส่สลิปนำไปจัดแยกประเภท เพื่อส่งป้อนข้อมูลสำหรับประมวลผลต่อไป โดยไม่มีการตรวจนับจำนวนสลิปที่รับจากฝ่ายบริหารการเงินว่ามีจำนวนถูกต้องครบถ้วนหรือไม่ การปฏิบัติดังกล่าวยังไม่เป็นการควบคุมที่รัดกุมเพียงพอ เนื่องจากสลิปรายการบัญชีต่าง ๆ อาจเกิดการสูญหายไประหว่างทาง โดยไม่สามารถสอบยันได้ว่าเกิดขึ้น ณ ฝ่ายใด

ข้อแนะนำ

1) ส่วนงานที่จัดทำสลิปควรควบคุมจำนวนสลิปและจำนวนเงิน โดยการตรวจนับและบวกเลขผลรวมจำนวนเงิน และสรุปยอดในใบปะหน้าสลิปก่อนส่งมอบให้หน่วยงานอื่น พร้อมลงทะเบียนบันทึกการส่งมอบเอกสารเพื่อเป็นหลักฐาน และสอบยันความถูกต้องของหน่วยงานต่าง ๆ หากสลิปเกิดสูญหายระหว่างทาง

2) สลิปที่ผ่านการป้อนข้อมูลเพื่อนำเข้าประมวลผลแล้ว ควรเย็บรวมเป็นชุด ตามวันที่ออกสลิป และให้เลขลำดับ (Serial Number) ไว้ในแต่ละชุด เพื่อประโยชน์ในการควบคุมความครบถ้วนและใช้สอบยันกับการบันทึกรายการบัญชีในแต่ละวัน

(2) ไม่มีการเก็บรักษารายงานไว้ตรวจสอบ

องค์กรไม่มีการจัดเก็บรักษารายงานซึ่งเป็นรายงานยืนยันความถูกต้องขั้นต้นของข้อมูลจาก Slip ที่ป้อนเข้าสู่ระบบงาน ซึ่งสามารถนำไปใช้ประโยชน์สำหรับการตรวจสอบในภายหลังได้

ข้อแนะนำ

ควรเก็บรักษารายงาน Edit and Validate G/L Transaction List เพื่อประโยชน์ในการตรวจสอบความถูกต้องและครบถ้วนของข้อมูล

2.6.2 ระบบงาน Financial Control

การประมวลผลข้อมูลล่าช้าไม่ทันเวลา

การประมวลผลข้อมูลของระบบงาน Financial Control ล่าช้าค่อนข้างมาก เช่น ณ วันที่เข้าตรวจสอบ (5 ก.พ. 2539) องค์กรประมวลผลข้อมูลของระบบได้เพียงเดือนตุลาคม 2538 ซึ่งอาจมีผลทำให้องค์กรนำข้อมูลจากระบบงานไปใช้ประโยชน์ได้น้อยและไม่ทันเวลา

ข้อแนะนำ

ควรประมวลผลข้อมูลระบบงาน Financial Control ให้ทันเวลา เพื่อให้สามารถนำไปใช้ในการตัดสินใจได้อย่างรวดเร็ว

2.6.3 ระบบงาน L/G (LETTER OF GUARANTEE)

(1) การควบคุมการแก้ไขข้อมูล

กรณีที่ผู้ใช้ข้อมูลตรวจสอบพบข้อมูลที่ผิดพลาดอันเนื่องมาจากการป้อนจำนวนเงินผิดหรือตัดผิด Operator จะทำการแก้ไขโดยมิต้องรับอนุญาตหรือแจ้งแก่ผู้บริหารระดับสูง และไม่มีการออกรายงานแสดงการแก้ไขด้วย นอกจากนี้ โปรแกรมที่กล่าวยังเป็นโปรแกรมที่ไม่ได้แสดงไว้ในเอกสารระบบงาน หากมีการสับเปลี่ยนโยกย้ายพนักงานที่เกี่ยวข้องไปทำหน้าที่อื่น อาจมีปัญหาในการปฏิบัติงานได้เพราะการแก้ไขข้อมูลที่เก็บอยู่ในแฟ้มข้อมูลหลัก (Master File) อาจไม่ถูกต้องและไม่มีข้อมูลที่เหลือไว้สำหรับการตรวจสอบ (Audit Trail) อันอาจจะก่อให้เกิดความเสียหายต่อองค์กรได้

ข้อแนะนำ

ควรกำหนดระเบียบปฏิบัติในส่วนที่เกี่ยวกับการแก้ไขข้อมูลในแฟ้มข้อมูลหลัก (Master File) ให้รัดกุมยิ่งขึ้น กล่าวคือ ควรจะมีหลักฐานเป็นหนังสือจากผู้ใช้ข้อมูล (User) แจ้งมายังฝ่ายคอมพิวเตอร์ และควรปรับปรุงแก้ไขโปรแกรมงานให้สามารถออกรายงานแสดงการแก้ไขไว้เป็นหลักฐานด้วย

(2) **ไม่มีหลักฐานการลบข้อมูล**

การลบข้อมูลออกจากแฟ้มข้อมูลหลักโดยไม่มีการออกรายงานเก็บไว้เป็นหลักฐานเนื่องจากข้อจำกัดของโปรแกรม

นอกจากนี้ องค์กรมิได้กำหนดให้มีการขออนุมัติลบข้อมูลออกจากแฟ้มข้อมูล การยินยอมให้ผู้ปฏิบัติงาน (Operator) ใช้โปรแกรมงานสำหรับการลบข้อมูลโดยไม่ต้องได้รับอนุญาตจากผู้บริหารระดับสูงอาจทำให้องค์กรได้รับความเสียหาย

ข้อแนะนำ

ควรกำหนดระเบียบปฏิบัติในการลบข้อมูลออกจากแฟ้มข้อมูลให้รัดกุมยิ่งขึ้น และควรจะพัฒนาโปรแกรมงานให้สามารถออกรายงานแสดงข้อมูลที่ลบออกจากแฟ้มข้อมูลด้วย

2.6.4 อื่น ๆ

ระบบ Cashier's Order

การตรวจสอบการอายัด Cashier's order ก่อนที่จะล้างรายการ Cashier's order ออกจากแฟ้มข้อมูลด้วยระบบ Manual อาจไม่ได้ผลเท่าที่ควร หากพนักงานที่ได้รับมอบหมายให้ตรวจสอบการอายัด Cashier's order หลงลืมหรือละเลยไม่ตรวจสอบ Cashier's order ฉบับที่ต้องการล้างรายการกับใบแจ้งการอายัด Cashier's order ของฝ่ายจัดองค์งาน

อย่างไรก็ดีองค์กรได้นำเครื่องไมโครคอมพิวเตอร์มาใช้กับงาน Cashier's order ของฝ่ายการธนาคารสำนักงานใหญ่แทนแล้ว และในระบบงานนี้มีการใช้ Factor หลายตัวในการตรวจสอบข้อมูล (Edit) ต่าง ๆ พร้อมทั้งให้พนักงาน Officer ตรวจสอบการทำงานด้วย สำหรับการตรวจสอบการอายัด Cashier 's order เป็นหน้าที่ของฝ่ายการบัญชีและฝ่ายการธนาคาร ซึ่งต้องมีการออกหนังสือเวียนให้สาขาต่าง ๆ ได้ทราบด้วย

ข้อแนะนำ

ควรปรับปรุงระบบ Cashier's order ให้สามารถตรวจสอบการอายัด Cashier's order ก่อนล้างรายการออกจากแฟ้มข้อมูลของระบบ Cashier's order ได้โดยอัตโนมัติ

บทที่ 16

ตัวอย่าง
จุดอ่อนของระบบงาน (Application)
ด้านคอมพิวเตอร์ที่อาจก่อให้เกิดการทุจริตได้

บทนำ

การตรวจสอบการดำเนินงานหรือการบริการด้านคอมพิวเตอร์เป็นหลักการของ EDP Examiner หรือ IS Examiner และเป็นส่วนหนึ่งของการปฏิบัติงานของผู้สอบบัญชีรับอนุญาต (Certified Public Accounts – CPA) และ Internal Auditor นอกเหนือการปฏิบัติงานตรวจสอบด้านอื่นตามที่ได้กล่าวมาแล้วในเล่มที่ 2

การตรวจสอบด้าน Data Center หรือ General Controls นั้น เป็นส่วนหนึ่งที่สำคัญเพราะจุดอ่อนหรือสิ่งที่อาจก่อให้เกิดความเสียหาย (Exposures) ได้ การดำเนินงานด้าน Data Center จะส่งผลกระทบถึงการควบคุมภายในที่อาจมีต่อจุดอ่อนหรือก่อให้เกิดความเสียหายทางด้าน "งาน" หรือApplication ไม่มากก็น้อยเสมอ

ดังนั้น ผู้ตรวจสอบที่มีทักษะย่อมจะต้องคำนึงถึงประเด็นข้างต้นด้วย เพื่อจะได้กำหนดขอบเขตการตรวจสอบงานของตนได้เหมาะสมยิ่งขึ้นและมีประสิทธิภาพ ประสบการณ์ต่อไปนี้เป็นเรื่องที่ได้ดัดแปลงให้เหมาะสมต่อการศึกษาแล้วขอย้ำว่า "จุดอ่อน" ดังกล่าวเป็นเรื่องของอดีตที่ได้เกิดขึ้นในองค์กรต่าง ๆ และไม่มีปัญหาในปัจจุบัน วัตถุประสงค์ของการเผยแพร่ประสบการณ์ในการดำเนินงานด้านคอมพิวเตอร์ของประเทศต่าง ๆ ก็เพื่อเป็นอุทาหรณ์และเป็นตัวอย่างในการศึกษามิให้ปัญหาดังกล่าวเกิดขึ้นอีกทั้งในปัจจุบันและในอนาคต เพราะ "จุดอ่อน" ในการบริหารงานและดำเนินการจะมีปัจจัยหนึ่งของการนำไปสู่การทุจริตโดยผู้ไม่หวังดีซึ่งส่วนใหญ่มักจะเป็นงานภายในองค์กรนั่นเอง เพื่อให้ประสบการณ์ในการดำเนินงานด้านคอมพิวเตอร์ของประเทศต่างมีประโยชน์ต่อผู้อ่านอย่างแท้จริง ผมใคร่แนะนำว่าการอ่านในแต่ละประเด็นที่กล่าวถึงจุดอ่อนและอาจรวมคำแนะนำโดยสรุปด้วยนั้น ถ้าท่านผู้อ่านพิจารณาพร้อม ๆ กันไปกับเรื่องต่อไปนี้ก็น่าจะได้รับประโยชน์เพิ่มขึ้นด้วย

1. ผู้ตรวจสอบตรวจทานเรื่องได้อย่างไร
2. ระบบงานภายในองค์กรของเรามีจุดอ่อนอย่างนั้นจริงหรือ
3. องค์กรของเรามีนโยบาย ระเบียบปฏิบัติ คำสั่ง ฯลฯ ที่เกี่ยวข้องในเชิงป้องกันจุดอ่อนนั้นแล้วหรือไม่ และ
4. มีการป้องกันหรือการควบคุมอื่น ๆ ที่จะชดเชยจุดอ่อนนั้น ๆ อย่างไรบ้าง
5. เราหรือคณะของเราเข้าใจประเด็น "จุดอ่อน" และผลกระทบต่อ "องค์กร" เราเพียงพอหรือไม่ในประเด็นที่ผู้ตรวจสอบสรุป
6. ถ้าองค์กรต้องปฏิบัติตามคำแนะนำของผู้ตรวจสอบจะกระทบต่อระบบงาน ระบบการปฏิบัติงานและค่าใช้จ่ายเพียงใด

หมายเหตุ : หลาย ๆ กรณีผู้บริหารขององค์กรมักปฏิเสธว่าองค์กรของตนมีจุดอ่อน เพราะตรวจงานด้านคอมพิวเตอร์มักจะระบุจุดอ่อนขององค์กร ทั้ง ๆ ที่ปัญหาขององค์กรยังไม่เกิดขึ้นเลย ผู้ตรวจสอบจึงต้องสรุปปัญหาและอธิบายต่อผู้บริหารอย่างชัดเจนทีละขั้นตอน จนกว่าจะเห็นพ้องกันในปัญหาดังกล่าว

7. เราใจกว้างพอที่จะ "ยอมรับ" หรืออย่างน้อย "รับพิจารณา" แก้ไขในสิ่งที่อาจจะก่อให้เกิดความเสียหายในองค์กรหรือไม่
8. เราอยากจะ "รับฟัง" และ "พยายามเข้าใจ" ผู้ตรวจสอบโดยพิจารณาว่าจะเป็นประโยชน์ต่อองค์กรอย่างแท้จริง
9. องค์กรของเราน่าจะมีบุคลากรที่มีความสามารถที่จะชี้ "จุดอ่อน" ขององค์กรได้และดูแลตนเองได้หรือไม่

จุดอ่อนในระบบงานต่าง ๆ ขององค์กร อันอาจเป็นช่องทางในการกระทำทุจริตได้

องค์กรแห่งหนึ่งได้นำเครื่องคอมพิวเตอร์มาใช้กับงานขององค์กร ได้แก่ ระบบงานเงินฝาก ระบบงานสินเชื่อ และระบบงานบัญชี และมีโครงการที่จะใช้กับระบบงานอื่น ๆ จนครบทุกระบบ เพื่อเป็น Full Computerized System ในอนาคต

ในการปฏิบัติงานป้อนข้อมูลและ Update ข้อมูลประจำวัน จะให้พนักงาน Operator เป็นผู้ทำ (อยู่ที่แผนกเงินฝากและแผนก EDP)

ระบบงานเงินฝากกระแสรายวัน Operator มีอำนาจและขอบเขตในการทำงานอย่างกว้างขวาง ยกเว้นรายการบางอย่างที่จะต้องให้พนักงานชั้นบริหารอนุมัติรายการเสียก่อน โดยการ key รหัสประจำตัวเข้าเครื่องคอมพิวเตอร์ผ่านเครื่อง Terminal ซึ่งเป็นเครื่องรับส่งข้อมูล ทั้งนี้หลักการปฏิบัติงานอยู่ภายใต้ข้อสมมติฐานที่ว่า พนักงานทุกคนมีความซื่อสัตย์สุจริตและไว้วางใจซึ่งกันและกัน

ดังนั้น หากมีจุดอ่อนเกิดขึ้นในระบบงานดังกล่าว ประกอบกับพนักงานมีเจตนาจะทุจริต ก็อาจจะนำความเสียหายมาสู่ธนาคารได้

กรณีตัวอย่างต่อไปนี้สรุปจากประสบการณ์ที่ได้เกิดขึ้น และนำมาเป็นข้อสังเกตหรือข้อเตือนใจว่า จุดอ่อนต่าง ๆ ที่มีอยู่นั้นสามารถนำมาใช้เป็นเครื่องมือในการกระทำทุจริตได้ อย่างไรก็ดีการควบคุมโดยเคร่งครัดมากเกินไป ก็อาจทำให้การปฏิบัติงานไม่คล่องตัว ดังนั้น ผู้บริหารจึงต้องชั่งน้ำหนักหรือพิจารณาผลดีผลเสียก่อนที่จะดำเนินการมาตรการควบคุมต่าง ๆ ตลอดจนค่าใช้จ่ายต่าง ๆ ที่จะเกิดขึ้นว่าคุ้มค่าหรือไม่ด้วย



ตัวอย่าง

จุดอ่อนในระบบงาน (Application) ที่อาจได้รับความเสียหายจากการทุจริต

จุดอ่อนของระบบงาน	ผลกระทบ/โอกาสที่ก่อให้เกิดการทุจริตได้
1. ระบบงานเงินฝากและเงินเบิกเกินบัญชี	
1) **การควบคุมเลขที่สมุดเช็คที่จ่ายให้ลูกค้า** การทำรายการ Issue Check Book เพื่อป้อนเลขที่เช็คเข้าระบบคอมพิวเตอร์ พนักงาน Teller ทำได้ โดยไม่ต้องใช้บัตรอนุมัติรายการ (Authorized Card) และไม่มีพนักงานอื่นสอบทานการป้อนข้อมูล	ผู้ที่ทราบจุดอ่อนนี้สามารถทำรายการ Issue Check Book เพื่อให้ระบบคอมพิวเตอร์ยอมผ่านเช็คฉบับที่ต้องการตัดบัญชีของลูกค้าได้ทุกบัญชี
2) **การคิดดอกเบี้ยนอกเหนือจากอัตราดอกเบี้ยที่แจ้ง** อัตราดอกเบี้ยสูงสุดของบัญชีเงินเบิกเกินบัญชีที่ระบบคอมพิวเตอร์แจ้งให้ทราบเมื่อทำรายการ Contract inquiry จะเป็นข้อมูลครั้งหลังสุดที่มีการเปลี่ยนแปลงอัตราดอกเบี้ยสูงสุดของบัญชีลูกหนี้เงินเบิกเกินบัญชีแต่ละราย ซึ่งอาจไม่ใช่ดอกเบี้ยสูงสุดที่แท้จริงที่ใช้คำนวณดอกเบี้ยในวันนั้น หาก Effective date ซึ่งเป็นวันที่มีผลบังคับใช้อัตราดอกเบี้ยสูงสุดที่เปลี่ยน-แปลงครั้งหลังสุดเป็นวันก่อนหน้า Effective date ของการเปลี่ยนแปลงอัตราดอกเบี้ยสูงสุดในครั้งก่อน เช่น ร้อยละ 5 ต่อปี **วันทำรายการ จากร้อยละ เป็นร้อยละ Effective date** 1 ต.ค. 30 17.00 15.00 1 ต.ค. 30 1 ต.ค. 30 15.00 16.00 30 ก.ย. 30	เมื่อทำรายการ Contract inquiry ระบบคอมพิวเตอร์จะแจ้งให้ทราบว่าอัตราดอกเบี้ยสูงสุดที่ธนาคารเรียกเก็บจากลูกหนี้รายนี้เท่ากับร้อยละ 16 ต่อปี ซึ่งคลาดเคลื่อนไปจากความเป็นจริง เพราะอัตราดอกเบี้ย สูงสุดที่ระบบคอมพิวเตอร์ใช้คำนวณดอกเบี้ยนับตั้งแต่วันที่ 1 ตุลาคม 2528 เป็นต้นไป ที่แท้จริงคือ อัตราร้อยละ 15 ต่อปี จุดอ่อนที่กล่าวสามารถซ่อนเร้นข้อผิดพลาดที่อาจเกิดขึ้นโดยเจตนาหรือไม่เจตนาได้ และมีผลกระทบต่อความน่าเชื่อถือของข้อมูลดอกเบี้ยเงินเบิกเกินบัญชีที่เรียกเก็บจากลูกค้าแต่ละราย

จุดอ่อนของระบบงาน	ผลกระทบ/โอกาสที่ก่อให้เกิดการทุจริตได้
ระบบงานเงินฝากกระแสรายวันและเงินเบิกเกินบัญชี	
1) การป้อนข้อมูลเพื่อปรับปรุงหรือเปลี่ยน-แปลง แก้ไขรายการ หรือข้อมูลที่สำคัญของลูกค้าเงินเบิกเกินบัญชีมีจุดอ่อน คือ	
- ไม่มีการป้องกันและควบคุมหรือจำกัดขอบเขตในการทำรายการของพนักงานที่มีอำนาจในการใช้เครื่อง Terminal เพราะพนักงานสามารถแก้ไขรหัสการอนุมัติวงเงิน วันครบกำหนดสัญญา วงเงินเบิกเกินบัญชี และอัตราดอกเบี้ยของลูกค้าได้	ทำให้พนักงานสามารถข้ามขั้นตอนการควบคุมเพื่อผ่านรายการถอนเงินเบิกเกินบัญชีโดยไม่ต้องขออนุมัติจากพนักงานชั้นบริหาร
2) ไม่มีการป้องกันและควบคุมการทำรายการสำคัญในการสร้าง ปรับปรุงแก้ไข และล้างรายการข้อมูล เช่น ชื่อ ที่อยู่	การเปลี่ยนแปลงแก้ไขชื่อและที่อยู่ของลูกค้ามีส่วนสำคัญต่อการยืนยันยอดคงเหลือเงินฝาก หรือการติดต่อระหว่างธนาคารและลูกค้า หากไม่มีการควบคุมพนักงานอาจแก้ไขรายการเพื่อสนับสนุนในการทุจริตบัญชีเงินฝากของลูกค้าได้
3) จุดอ่อนในการทำรายการบันทึกการจ่ายเช็คให้ลูกค้า และตัดเลขที่เช็คออกจาก File ของลูกค้าเพื่อให้เนื้อที่ว่างสำหรับบันทึกเลขที่เช็คใหม่ คือ	
- ไม่ได้ควบคุมและป้องกันการบันทึกรายการ Cheque Collected Type "O" เพื่อยกเลิกหรือล้างหมวดเลขที่เช็คทั้งหมดออกจากบัญชีของลูกค้าในแฟ้มข้อมูล ซึ่งทำให้มีเนื้อที่ว่างพอที่จะบันทึกเลขที่เช็คหมวดใหม่เข้าไปได้ (แต่จะต้องมีการบันทึกเลขที่เช็คที่ต้องการมาเบิกเงินโดยทุจริตเข้าไปใหม่อีกครั้งหนึ่ง)	มีผลให้เลขที่เช็คที่เคยเบิกถอนเงินไปแล้วแสดงสถานะในแฟ้มข้อมูลว่ายังไม่เคยเบิกถอนเงินออกไป และถ้ามีเช็คที่เคยหักบัญชีไปแล้วนำมาเบิกถอนเงินอีก โปรแกรมจะไม่สามารถตรวจสอบได้ว่าเลขที่เช็คฉบับนั้นเคยเบิกถอนเงินแล้ว จึงทำให้สามารถเบิกถอนเงินจากบัญชีลูกค้าได้อีกครั้งหนึ่งโดยมิชอบ ดังที่เคยเกิดกรณีเช่นนี้มาแล้วในอดีต ซึ่งทำความเสียหายมาสู่ธนาคารมาก

จุดอ่อนของระบบงาน	ผลกระทบ/โอกาสที่ก่อให้เกิดการทุจริตได้
- ไม่ได้กำหนดให้มีการอนุมัติจากพนักงานชั้นบริหารในการควบคุมหรือจำกัดขอบเขตการป้อนข้อมูลเพื่อบันทึกรายการ Cheque Issue ของลูกค้า	พนักงานสามารถใช้เช็คของผู้อื่นหรือเช็คที่เคยหักบัญชีไปแล้วมาเบิกถอนจากบัญชีลูกค้าได้ โดยใช้รายการดังกล่าวอันอาจจะก่อให้เกิดความเสียหายต่อธนาคารได้
ระบบงานเงินฝาก	
1. เงินฝากกระแสรายวันและเงินเบิกเกินบัญชี	
- รหัสรายการ (Convert withdraw) ในระบบงานไม่มีการตรวจสอบยอดคงเหลือในบัญชีลูกค้าหรือวงเงินเบิกเกินบัญชีกับจำนวนเงินที่ถอนก่อนยินยอมให้ผ่านรายการ	ผู้ปฏิบัติงานอาจใช้รหัสรายการนี้ผ่านรายการให้ลูกค้า และหลีกเลี่ยงการขออนุมัติวงเงินเบิกเกินบัญชีชั่วคราวได้
- การป้อนเลขที่เช็คซึ่งใช้ในการควบคุมการผ่านรายการถอนด้วยเช็ค	- ป้อนเลขที่เช็คสลับบัญชี
2) การรักษาความปลอดภัย Password ของพนักงานชั้นบริหาร เปิดโอกาสให้ Operator รู้เห็น Password ของพนักงานชั้นบริหาร	ทำให้การควบคุมการใช้ Menu ของพนักงานชั้นบริหาร ซึ่งเป็นเครื่องมือที่ใช้ในการควบคุมการปฏิบัติงานประจำวันไม่ได้ผลเท่าที่ควร Operator สามารถทำรายการทุกอย่างได้จากจอของ Operator เอง
3) การควบคุมการใช้โปรแกรม Maintenance ในการเปิดบัญชี ไม่มีการควบคุม	โปรแกรมอาจถูกนำไปใช้ในการเปิดบัญชีใหม่และใช้ปรับปรุงแก้ไขข้อมูลในบัญชีลูกค้าโดยมิชอบ
2. เงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม และเงินเบิกเกินบัญชี เงินฝากพิเศษ และ CD ของสาขา	
ไม่มีการควบคุมการทำรายการรับฝากเงินจากลูกค้า	Operator ของสาขาสามารถทำรายการฝากเงินเข้าบัญชีลูกค้าได้ทุกบัญชี โดยไม่จำกัดจำนวนเงินฝาก
3. เงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม และเงินเบิกเกินบัญชีของสำนักงานใหญ่	
โปรแกรมระบบงานป้องกันการผ่านรหัสรายการ (Transaction code) การแก้ไขไม่สมบูรณ์	สามารถแก้ไขรายการเช็คเคลียริ่ง (ECL) โดยไม่ต้องมีการผ่านรายการเช็คเคลียริ่งนั้นมาก่อน

จุดอ่อนของระบบงาน	ผลกระทบ/โอกาสที่ก่อให้เกิดการทุจริตได้
4. เงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม และเงินเบิกเกินบัญชีของสาขา ผู้บริหารสาขาสามารถเพิ่มวงเงินเบิกเกินบัญชีได้เองโดยไม่ต้องผ่านการอนุมัติจากสำนักงานใหญ่	อาจทำให้สินทรัพย์เสี่ยงของธนาคารขาดหลักทรัพย์ค้ำประกันที่เพียงพอ
1. ระบบงานเงินฝาก 1) ระบบเงินฝากมีจุดอ่อนเกี่ยวกับการป้อนข้อมูล (key) เลขที่บัญชีลูกค้า เนื่องจาก Check Digit ที่ธนาคารนำมาใช้ไม่สามารถป้องกันการป้อนเลขที่บัญชีลูกค้าผิด เพราะเลขที่บัญชีที่ต่างกันจะมี Check Digit และ Branch Digit เหมือนกันได้	ก่อให้เกิดการบันทึกรายการผิดบัญชีและผิดสำนักงานได้ หากธนาคารแก้ไขรายการที่เกิดขึ้นได้ไม่ทันเวลา บุคคลอื่นซึ่งเป็นเจ้าของบัญชีที่รับโอนเข้าบัญชี (ผิดบัญชี) สามารถถอนเงินได้ทุกขณะ โดยเฉพาะอย่างยิ่งเมื่อธนาคารพัฒนางานไปสู่ระบบ On-line อย่างสมบูรณ์
2) การควบคุมการเปลี่ยนแปลง Password ไม่รัดกุมในกรณีที่พนักงาน Operator ต้องการเปลี่ยน Password แต่ Password ใหม่ที่เปลี่ยนซ้ำกับ Password ของผู้อื่นโดยบังเอิญ ที่จอภาพของพนักงาน Operator จะปรากฏข้อความ ทำให้ทราบว่า Password ที่เปลี่ยนใหม่ซ้ำ แต่ที่จอภาพของพนักงานระดับ Authorized จะไม่ปรากฏข้อความใด ๆ	ทำให้ผู้ปฏิบัติงานอาจทราบ Password ของผู้อื่นได้ ซึ่งมีผลกระทบต่อการควบคุมการใช้ข้อมูลในระบบเงินฝาก
3) ธนาคารไม่ได้จัดทำทะเบียนควบคุมการเบิกจ่ายสมุดคู่ฝากที่ยังไม่ได้ใช้ให้ลูกค้าและธนาคารยังยินยอมให้พนักงาน Operator ซึ่งเก็บสมุดคู่ฝากที่ยังไม่ได้ใช้สามารถทำการบันทึก (Write) ข้อมูลลงในแถบแม่เหล็กของสมุดคู่ฝากลูกค้าได้โดยไม่มีพนักงาน Authorized หรือพนักงานอื่นควบคุมดูแลโดยใกล้ชิด	ทำให้สมุดคู่ฝากอาจสูญหายโดยไม่มีผู้ใดทราบ และพนักงานอาจนำสมุดคู่ฝากนี้ไปใช้ได้ ซึ่งก่อให้เกิดความเสียหายต่อธนาคาร
2. ระบบงานบัตรเงินสด (Cash Deposit) 1) การเก็บรักษาโปรแกรมและตัวเลขลับสำหรับการคำนวณสร้างรหัสประจำตัวลูกค้า (PIN	หากมีผู้อื่นรู้รหัสลับ (Password) และเรียกโปรแกรมดังกล่าวมาคำนวณสร้าง PIN Code ของ

จุดอ่อนของระบบงาน	ผลกระทบ/โอกาสที่ก่อให้เกิดการทุจริตได้
code) ไม่รัดกุม โดยจะเก็บโปรแกรมไว้ในเครื่องคอมพิวเตอร์ตลอดเวลา และมีผู้รู้รหัสลับ (Password) สำหรับการเรียกโปรแกรมมาใช้งาน 2 คน	ลูกค้าโดยมิได้รับอนุญาต อาจก่อให้เกิดความเสียหายต่อลูกค้าของธนาคารได้
2) ธนาคารไม่มีการควบคุมการเข้าถึงด้านหลังของเครื่องบริการบัตรเงินสด (CD) ที่ติดตั้งไว้	ทำให้บุคคลอื่นเข้าถึงตัวเครื่องได้ อาจก่อให้เกิดความเสียหายต่อธนาคาร เนื่องจากเครื่องบริการบัตรเงินสดมีขนาดเล็ก และง่ายต่อการใช้วิธีการทำลายเพื่อดึงเงินสดที่เก็บอยู่ในเครื่อง
ระบบงานเงินฝากออมทรัพย์ 1) ระบบงานเงินฝากออมทรัพย์มีจุดอ่อนในการควบคุมภายในเกี่ยวกับการป้อนข้อมูล (Key) หมายเลขรหัสประจำสาขาที่จะโอนไปเข้าบัญชี ในกรณีที่มีการรับฝากแทนสาขาอื่น เนื่องจากเลขรหัสสาขาสัมพันธ์กัน ทำให้เลขที่บัญชีเงินฝากมี Check digit เท่ากัน และวิธีปฏิบัติงานมีข้อยกเว้นให้พนักงาน Teller เลือกป้อนเลขรหัสสาขาหรือไม่ก็ได้ โดยระบบงานคอมพิวเตอร์จะสร้างรหัสสาขาหรือสำนักงานที่ป้อนข้อมูลให้โดยอัตโนมัติ (Default) จึงมีโอกาสที่จะเกิดการบันทึกรายการผิดบัญชีผิดสาขาได้ นอกจากนั้นยังมีคู่สาขาที่เลข Check digit เท่ากันทุกบัญชี และ มีโอกาสเกิดผิดพลาดในลักษณะเดียวกันอีก	ก่อให้เกิดการบันทึกรายการผิดบัญชีผิดสาขา หากธนาคารแก้ไขรายการที่เกิดขึ้นได้ไม่ทันเวลา บุคคลอื่นซึ่งเป็นเจ้าของบัญชีที่รับโอนเข้าบัญชี (ผิดบัญชี) สามารถถอนเงินได้ทุกขณะ โดยเฉพาะอย่างยิ่งเมื่อธนาคารพัฒนางานไปสู่ระบบ On-line อย่างสมบูรณ์
2) ธนาคารไม่ได้กำหนดระเบียบและวิธีปฏิบัติและความรับผิดชอบที่แน่นอนสำหรับพนักงานที่อนุมัติหรือ Key รายการ Hold Days เป็นศูนย์ ในกรณีที่ธนาคารต้องการผ่านเช็ค เพื่ออำนวยความสะดวกแก่ลูกค้าก่อนเวลาที่จะเคลียริ่งให้ลูกค้าโอนเงินได้ตามปกติ	ทำให้ลูกค้าสามารถถอนเงินจากเช็คเคลียริ่งที่ยังไม่รู้ผลการเรียกเก็บเงินได้ ซึ่งอาจทำให้ธนาคารเกิดความเสียหายได้ หากไม่มีการรายงานหรือติดตามรายการเหล่านี้ในวันต่อไป

จุดอ่อนของระบบงาน	ผลกระทบ/โอกาสที่ก่อให้เกิดการทุจริตได้
ระบบงานเงินฝากออมทรัพย์ - ผู้ปฏิบัติงานสามารถใช้โปรแกรม ซึ่งปกติใช้สำหรับปรับจำนวนดอกเบี้ยค้างจ่ายตอนสิ้นงวดบัญชีคำนวณดอกเบี้ยล่วงหน้าจนถึงวันที่ที่ต้องการได้ และหากมีรายการเคลื่อนไหวต่อมาจะทำให้ดอกเบี้ยค้างจ่ายของบัญชีนั้นเพิ่มขึ้นสูงกว่าที่ควรจะเป็นมาก	หากผู้ปฏิบัติงานนำโปรแกรมดังกล่าวไปใช้ในทางที่มิชอบ ก็อาจก่อให้เกิดความเสียหายแก่ธนาคารได้
2. ระบบ ATM **1) การทำลายใบปะหน้าแบบฟอร์มใบแจ้งรหัส** เมื่อเสร็จกระบวนการจัดรหัสประจำตัวลูกค้าที่ใช้บริการ ATM แล้ว ธนาคารไม่ได้กำหนดให้ผู้ปฏิบัติงานทำลายกระดาษสีดำซึ่งเป็นกระดาษแผ่นแรกของแบบฟอร์มใบแจ้งรหัสที่จะส่งให้ลูกค้า ก่อน นำแบบฟอร์มใบแจ้งรหัสออกจากห้องคอมพิวเตอร์	เป็นการเปิดโอกาสให้ผู้ที่ไม่มีส่วนเกี่ยวข้องกับการจัดทำรหัส รู้เห็นรหัสประจำตัวลูกค้าจากรอยพิมพ์รหัส ซึ่งปรากฏอยู่ที่ด้านหลังของกระดาษสีดำที่กล่าวได้
2) การเข้าถึงข้อมูลของลูกค้าโดยบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง การใช้นักศึกษาฝึกหัดงานจัดเก็บเอกสารเกี่ยวกับการใช้บริการ ATM เช่น ใบคำขอถือบัตร ATM ของลูกค้าเป็นต้น เป็นการยินยอมให้บุคคลภายนอกเข้าถึงข้อมูลที่มีความสำคัญของระบบ ATM ได้โดยง่าย	อาจมีผลกระทบต่อความปลอดภัยของลูกค้าที่ใช้บริการ ATM
2. ระบบเครื่องฝากถอนเงินอัตโนมัติ (ATM) **2.1 บัตรประจำตัวลูกค้า** 1) ในการตรวจนับบัตรพลาสติกซึ่งเป็นบัตรเปล่าที่ซื้อมาจากต่างประเทศ เพื่อตรวจสอบคุณภาพและความครบถ้วนของจำนวนบัตรที่ได้รับจากผู้ขาย พนักงานที่ตรวจนับบัตรดังกล่าวไม่ได้ลงนามกำกับหีบห่อที่ตรวจนับแล้ว	ทำให้ธนาคารไม่สามารถสอบสวนสาเหตุที่บัตรขาดหายไป

จุดอ่อนของระบบงาน	ผลกระทบ/โอกาสที่ก่อให้เกิดการทุจริตได้
2) ในการนำบัตรเปล่าไปบันทึกชื่อลูกค้าเป็นอักษรตัวนูนบนบัตร และบันทึกข้อมูลลงในแถบแม่เหล็กด้านหลังบัตรในแต่ละครั้ง ไม่มีการกระทบยอดจำนวนบัตรเปล่าที่เบิกใช้กับจำนวนบัตรที่ผ่านเครื่องทำบัตรให้ลูกค้า และจำนวนบัตรเปล่าคงเหลือ	ทำให้อาจมีการนำบัตรอื่นมาผ่านกระบวนการผลิต ซึ่งสามารถนำไปใช้บริการได้เช่นเดียวกัน
3) เลขที่บัตรประจำตัวลูกค้าเป็นข้อมูลสำคัญที่บันทึกไว้ในแถบแม่เหล็กด้านหลังบัตรประจำตัวลูกค้าควรเป็นความลับ แต่ในบัตรบันทึกรายการ (Transaction record) ที่เครื่องฝากถอนเงินอัตโนมัติออกให้ลูกค้าเก็บไว้เป็นหลักฐานการฝากหรือถอนเงิน มีเลขที่บัตร ประจำตัวลูกค้าพิมพ์แสดงไว้ทุกใบ และลูกค้าส่วนใหญ่ไม่เห็นความสำคัญในการเก็บบัตรบันทึกรายการไว้เป็น หลักฐาน จะทิ้งบัตรดังกล่าวไว้ในบริเวณใกล้ ๆ กับที่ตั้งเครื่องฝากถอนเงินอัตโนมัติ	ผู้ที่มีความรู้ความสามารถในการทำบัตรประจำตัวลูกค้า อาจนำข้อมูลเกี่ยวกับเลขที่บัตรประจำตัวลูกค้าไปใช้ประโยชน์ในการทำบัตรปลอมได้
2.2 รหัสลับประจำตัวลูกค้า (PIN)	
- ธนาคารไม่ได้กำหนดตัวบุคคลที่อนุญาตให้เข้าถึง (Access) ตู้เก็บรหัสลับประจำตัวลูกค้า ซึ่งพิมพ์เสร็จเรียบร้อยแล้ว เตรียมจัดส่งสาขาเพื่อแจกลูกค้า และไม่ได้ปิดกุญแจตู้เก็บรหัสลับดังกล่าวไว้ตลอดเวลา	อาจทำให้ความลับของรหัสดังกล่าวรั่วไหลได้
2.3 เรื่องอื่นๆ	
1) เครื่องฝากถอนเงินอัตโนมัติที่ตั้งอยู่ภายนอกสถานที่ทำการของธนาคารไม่ได้ติดตั้งระบบสัญญาณแจ้งภัย	หากมีเหตุร้ายเกิดขึ้นอาจแก้ไขสถานการณ์ได้ไม่ทันท่วงที ซึ่งกระทบต่อความเชื่อถือของลูกค้าในด้านการรักษาความปลอดภัยของธนาคาร
2) ธนาคารยินยอมให้ลูกค้าบางรายมอบบัตรและรหัสลับประจำตัวให้บุคคลอื่นมาใช้บริการเครื่องฝากถอนเงินอัตโนมัติแทนตนเอง	เจ้าของบัญชีที่มีการใช้บริการด้วยวิธีดังกล่าวอาจได้รับความเสียหาย หากผู้ที่ได้รับมอบหมายใช้บริการนอกคำสั่งที่ตกลงกันไว้

บทที่ 17

การตรวจสอบการทุจริต และทบทวน การตรวจสอบจุดอ่อนในระบบงานในองค์กร ที่ใช้คอมพิวเตอร์

การตรวจสอบการทุจริตและ จุดอ่อนในระบบงานในองค์กรที่ใช้คอมพิวเตอร์

1. คำนำ

คอมพิวเตอร์มีคุณค่ามหาศาล แต่มีความเสี่ยงใหม่ ๆ ที่อาจมีผลกระทบต่อธุรกิจในด้านต่าง ๆ ได้มากมายและมหาศาลเช่นเดียวกัน ถ้าหากองค์กรและผู้ใช้ไม่เข้าใจเกี่ยวกับระบบคอมพิวเตอร์ตลอดจนรูปแบบแปลก ๆ ที่ไม่เคยพบมาก่อน ก็อาจนำความสูญเสียให้เกิดขึ้นได้อย่างคาดไม่ถึงเอาทีเดียว และในบางกรณีก็อาจทำให้ธุรกิจถึงขั้นหยุดชะงักอย่างเช่นเหตุการณ์ที่เกิดขึ้นที่ Big Bang ตลาดค้าหุ้นในกรุงลอนดอน และในกรณี Bank of New York เมื่อหลายปีก่อนหรือแม้กระทั่งเหตุการณ์ที่เกิดขึ้นในประเทศไทยเรา ในกรณีที่ผู้ฝากไม่อาจถอนเงินได้จากการหยิบแฟ้มข้อมูลผิดพลาดหรือแผ่นดิสก์เสียหายจากการครูดของหัวอ่าน หรือเหตุการณ์ทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือโกงอย่างมีประสิทธิภาพผ่านระบบ On - line ของธนาคารใหญ่แห่งหนึ่งและเสียหายไปหลายล้านบาท หรือแม้กระทั่งการควบคุมในระบบงานมีจุดอ่อน จนเกิดช่องว่างให้มีการโอนเงินผิดพลาดจำนวนมาก เป็นต้น

การที่ได้เห็นความเสียหายที่เกิดขึ้นในอดีต รวมทั้งกรณีการทุจริตหลายแบบที่เกิดขึ้นแล้ว เป็นวิธีการวิเคราะห์ความเสี่ยงง่าย ๆ แบบหนึ่ง ที่นอกจากจะเป็นประโยชน์ในการสร้างระบบการป้องกันและควบคุมแล้ว ยังให้ประโยชน์แก่งานด้านการตรวจสอบอีกด้วย กล่าวคือ การวิเคราะห์ความเสี่ยงจะทำให้ผู้ตรวจสอบมองเห็นจุดที่ควรตรวจสอบ ซึ่งในแง่ความเสี่ยงก็คือจุดที่ก่อให้เกิดความเสียหายได้นั่นเอง การทราบจุดตรวจสอบที่แน่ชัดจะทำให้การใช้ทรัพยากรตรวจสอบเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล เพราะเป้าหมายของการตรวจสอบที่สำคัญคือการค้นหาความผิดพลาดหรือความเสียหายหรือผลกระทบต่อฐานะการเงินและการดำเนินงานอย่างต่อเนื่องขององค์กรให้ได้เร็วที่สุดและเสียค่าใช้จ่ายน้อยที่สุด

การตรวจสอบการทุจริตซึ่งรวมทั้งการตรวจสอบจุดอ่อนและความเสี่ยงในระบบงานต่าง ๆ ขององค์กรไม่ว่าจะเป็นด้าน Financial และด้าน Computer นั้นมีหลักการ และแนวทาง เช่นเดียวกับการตรวจสอบระบบงานหรือ "งาน" (Application) เป็นส่วนใหญ่ ข้อแตกต่างที่สำคัญ คือ วัตถุประสงค์หรือเป้าหมายในการตรวจสอบขอบเขตในการตรวจสอบ การเพ่งเล็งหรือค้นหาความผิดพลาดหรือการทุจริตรวมทั้งวิธีการทุจริต ตลอดจนความเสียหายที่ได้เกิดขึ้นแล้ว หรือที่อาจจะเกิดขึ้นได้ จะเป็นตัวกำหนดขอบเขตรวมทั้งการทำรายงานผลที่แตกต่างกันไป

ประสบการณ์การทุจริตของประเทศต่าง ๆ ตลอดจนจุดอ่อน ของระบบงานและการบริหารงานด้วยคอมพิวเตอร์ตามบทก่อนหน้านี้ จะช่วยให้ท่านที่สนใจติดตามเรื่องการตรวจสอบการทุจริตด้านคอมพิวเตอร์ หรือด้านคอมพิวเตอร์ได้ดีขึ้น เพราะจุดอ่อนต่าง ๆ ที่ผู้ตรวจสอบได้พบและให้คำแนะนำให้องค์กรแก้ไขแล้วนั้น เคยปรากฏว่ามีหลายกรณีที่องค์กรยังไม่ทันได้แก้ไข องค์กรนั้นก็ได้ประสบการณ์การทุจริตที่เกิดจากจุดอ่อนในระบบงานต่อมาในภายหลังหลายกรณี เรื่องเหล่านี้เป็นข้อพิสูจน์ว่าจุดอ่อนในระบบงานขององค์กรเป็นองค์ประกอบอย่างหนึ่งของการทุจริต

2. ขอบเขตและความถี่ในการตรวจสอบด้านคอมพิวเตอร์

ขอบเขตของการปฏิบัติงาน และความถี่สำหรับการตรวจสอบภายในจะต้องมีอย่างเพียงพอที่จะบรรลุวัตถุประสงค์ในการตรวจสอบ โดยต้องครอบคลุมในเรื่องต่อไปนี้

1) การสอบทานการปฏิบัติตามข้อกำหนด

เป็นการสอบทานการปฏิบัติตามนโยบาย มาตรฐาน และวิธีปฏิบัติงานที่ได้กำหนดไว้อย่างเป็นทางการ

2) การสอบทานคุณภาพ

เป็นการสอบทานคุณภาพของนโยบาย มาตรฐาน และวิธีปฏิบัติงานที่ได้กำหนดไว้อย่างเป็นทางการ ทั้งนี้รวมถึงคุณภาพของการบริหาร ประสิทธิภาพของการปฏิบัติงานและความเพียงพอของขั้นตอนการปฏิบัติงานและการควบคุม

3) การสอบทานความถูกต้องเชื่อถือได้

เป็นการสอบทานการติดตามการทุจริต ความถูกต้องของโปรแกรมระบบงานและระบบควบคุมคอมพิวเตอร์ การออกแบบและการนำระบบงานออกใช้ และการตรวจสอบกิจกรรมของพนักงาน

ภายใต้การสอบงานประเภทต่าง ๆ ดังกล่าว ผู้ตรวจสอบจำเป็นต้องสอบทานหน้าที่ในการกระทบยอด การบันทึกและควบคุมข้อมูล การปฏิบัติงานของอุปกรณ์คอมพิวเตอร์ระบบงานและโปรแกรมการสื่อสารข้อมูล และการควบคุมการประมวลผลข้อมูลในแต่ละส่วนงานของผู้ใช้

ความถี่ในการตรวจสอบขึ้นอยู่กับการประเมินความเสี่ยงในเรื่องต่าง ๆ นั่นคือองค์ประกอบที่ควรพิจารณาในการประเมินความเสี่ยง ได้แก่

1) คุณลักษณะของการปฏิบัติงานพิเศษและสินทรัพย์และหนี้สินที่เกี่ยวข้อง
2) มาตรฐานของนโยบายที่เหมาะสมและการควบคุมภายในที่มีอยู่ในกิจการ
3) ประสิทธิผลของการปฏิบัติงานและการควบคุมภายใน
4) โอกาสที่จะเกิดข้อผิดพลาดหรือการฝ่าฝืนกฎหมายอย่างมีนัยสำคัญในส่วนของการปฏิบัติงานเฉพาะอย่าง
5) ผลของการสอบทานงานต่าง ๆ ที่ผ่านมาและจุดที่เป็นปัญหา

วิธีการตรวจสอบ

วิธีการตรวจสอบด้านคอมพิวเตอร์จะแปรเปลี่ยนไปตามปรัชญาและความชำนาญงานด้านเทคนิคของฝ่ายตรวจสอบ อย่างไรก็ตามวิธีการปฏิบัติงานและ / หรือเทคนิคที่เป็นมาตรฐานมักจะใช้ได้กับองค์กรที่ใช้คอมพิวเตอร์เป็นส่วนมาก เทคนิคการตรวจสอบอาจแบ่งเป็นการตรวจสอบโดยใช้และไม่ใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

1) การตรวจสอบโดยไม่ใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

ในการปฏิบัติงานทดสอบข้อมูล ผู้ตรวจสอบภายในอาจเลือกวิธีที่ไม่ต้องใช้คอมพิวเตอร์ช่วยในการปฏิบัติงาน แต่วิธีนี้จะมีประสิทธิผลได้ถ้าจะต้องคำนึงถึงสภาพแวดล้อมของการควบคุมภายในศูนย์ประมวลผลข้อมูลด้วย เมื่อมีการทดสอบข้อมูล record ใด record หนึ่งของระบบงานหนึ่ง ๆ การทดสอบนั้นจะต้องไม่ใช้โปรแกรมระบบงานนั้นมาประมวลผล ซึ่งการทดสอบข้อมูลดังกล่าวรวมถึงการเปรียบเทียบตัวอย่างข้อมูลที่เก็บไว้ในระบบคอมพิวเตอร์กับข้อมูลที่อยู่ในเอกสารต้นกำเนิด และ / หรือ การสอบทานข้อมูลโดยการยืนยันยอดโดยตรง ผลของการตรวจสอบด้วยวิธีนี้ควรมีการกระทบยอดในลักษณะเดียวกับการตรวจสอบข้อมูลที่จัดทำโดย manual ด้วย

ไม่ว่าจะใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบหรือไม่ก็ตามผู้ตรวจสอบภายในด้านคอมพิวเตอร์ควรสอบทานระบบงาน ทดสอบการปฏิบัติตามกฎระเบียบที่วางไว้ทดสอบความถูกต้องของยอดคงเหลือ และประเมินข้อมูลเพื่อตรวจสอบความถูกต้องของการประมวลผลการตรวจสอบแต่ละวิธีมีดังนี้



การเข้าถึงเป้าหมายการตรวจสอบ	วิธีตรวจสอบ
1) การสอบทานระบบงาน	- ใช้แบบสอบถาม - สัมภาษณ์บุคลากรในส่วนงานประมวลผลข้อมูล - จัดทำคำอธิบายระบบโดยทั่ว ๆ ไป - สอบทานการควบคุมที่สำคัญของผู้ใช้และฝ่ายประมวลผลข้อมูล - สอบทานการควบคุมในแต่ละโปรแกรมของทุกระบบงานที่สำคัญ
2) การทดสอบการปฏิบัติตามกฎระเบียบที่กำหนดไว้	- ตรวจสอบหลักฐานที่เกี่ยวข้องกับการควบคุม (เช่น รายการแสดงข้อผิดพลาด รายการบันทึกเพื่อควบคุมกลุ่มข้อมูล - ใช้ผลลัพธ์ที่ได้จากคอมพิวเตอร์ในการติดตามรายการจากผลลัพธ์ไปยังเอกสารต้นกำเนิดจากเอกสารต้นกำเนิดไปยังรายงาน และยอดรวมในรายงานไปยังจุดควบคุมต่าง ๆ - ตรวจสอบตัวอย่างบางรายการว่าประมวลผลถูกต้องหรือไม่ - ประเมินความเพียงพอของข้อมูลทดสอบเพื่อจะตัดสินได้ว่าการทดสอบนั้นมีข้อมูลทดสอบที่เพียงพอ - ทดสอบความถูกต้องของยอดรวมต่าง ๆ - ทดสอบตัวอย่างบางรายการในรายละเอียด โดยการยืนยันคำตอบ ทดสอบความสมเหตุสมผล ฯลฯ
3) การประเมินข้อมูลที่จัดเก็บในรูป record	- กระทบยอดรวมที่ใช้ในการควบคุมผู้ใช้ กับสิ่งที่ได้จากการประมวลผล และยอดรวมที่ได้จากระบบคอมพิวเตอร์ กับตัวเลขในบัญชีแยกประเภททั่วไป - พิจารณาว่าฝ่ายงานของผู้ใช้ ฝ่ายประมวลผลข้อมูล และจุดควบคุมในโปรแกรมได้ทำหน้าที่ของตนตามที่กำหนดไว้เป็นลายลักษณ์อักษร

2) การตรวจสอบโดยใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

ผู้ตรวจสอบควรพยายามอย่างยิ่งที่จะใช้คอมพิวเตอร์ในการปฏิบัติงานตรวจสอบเพราะคอมพิวเตอร์สามารถช่วยลดต้นทุนในการทดสอบและการสุ่มตัวอย่าง ซึ่งมิฉะนั้นแล้วจะต้องทำการ manual นอกจากนี้การใช้คอมพิวเตอร์จะช่วยให้ผู้ตรวจสอบคุ้นเคยกับการทำงานของอุปกรณ์ต่าง ๆ ในศูนย์ประมวลผลด้วย

ตัวอย่าง ผู้ตรวจสอบสามารถใช้คอมพิวเตอร์ในการ :

- ทดสอบยอดรวมย่อยต่าง ๆ และความถูกต้องในการคำนวณเพื่อสอบทานความถูกต้องของผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์
- ทดสอบข้อมูลใน record ต่าง ๆ ในเรื่องของความครบถ้วน ความสม่ำเสมอ ความถูกต้องของเงื่อนไข และความสมเหตุสมผลของจำนวนเงิน
- รวมยอดข้อมูลและวิเคราะห์ผลที่ได้
- คัดเลือกและพิมพ์ข้อมูลโดยใช้เทคนิคการสุ่มตัวอย่างทางสถิติเพื่อรอคำยืนยัน
- จำลองการประมวลผลรายการอย่างอิสระเพื่อตรวจสอบความถูกต้องและความสม่ำเสมอในการทำงานของโปรแกรมคอมพิวเตอร์
- จัดทำงบทดลองเพื่อใช้ในการตรวจสอบและรายงานต่าง ๆ ที่เกี่ยวข้อง

เพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ ผู้ตรวจสอบภายในอาจใช้ :

- โปรแกรมที่เขียนโดยผู้เขียนโปรแกรมที่เป็นบุคลากรภายในหรือภายนอกองค์กรโดยอยู่ภายใต้การกำกับของผู้ตรวจสอบ
- โปรแกรมตรวจสอบสำเร็จรูป (เช่น โปรแกรมสำเร็จรูปของผู้ผลิตอุปกรณ์คอมพิวเตอร์ สำนักงานสอบบัญชี และบริษัทผู้ขายโปรแกรมอิสระ)
- โปรแกรมที่เขียนขึ้นโดยผู้ตรวจสอบด้านคอมพิวเตอร์
- โปรแกรมของผู้ผลิตอุปกรณ์คอมพิวเตอร์และโปรแกรมต่าง ๆ เพื่อวิเคราะห์ประสิทธิภาพการทำงานของเครื่องจักร ผู้เขียนโปรแกรม และการปฏิบัติงาน

ไม่ว่าโปรแกรมตรวจสอบจะมาจากแหล่งใด โปรแกรมที่จะใช้ในการตรวจสอบควรอยู่ภายใต้การควบคุมอย่างเข้มงวดของฝ่ายตรวจสอบ นั่นคือจะต้องมีการควบคุมเอกสารวัสดุที่ใช้ในการทดสอบ โปรแกรมทำงานที่เก็บอยู่ในรูปแบบของภาษาที่มนุษย์เข้าใจได้ และภาษาเครื่อง รวมทั้งการเปลี่ยนแปลงต่าง ๆ ในโปรแกรมอย่างเข้มงวด การติดตั้งที่ใช้ระบบการควบคุมโปรแกรมสำเร็จรูปชั้นสูง จะต้องมีการป้องกันการเข้าถึงโปรแกรมตรวจสอบโดยใช้รหัสลับ ซึ่งข้อปฏิบัตินี้เป็นที่ยอมรับตราบที่ผู้ตรวจสอบยังคงควบคุมเอกสารและคำสั่งควบคุมงานต่าง ๆ ที่ต้องใช้ในการดึงและนำโปรแกรมที่เก็บไว้เป็นภาษาเครื่องออกมาใช้งาน ถ้ากระบวนการควบคุมภายในระบบคอมพิวเตอร์ไม่มีการควบคุมที่เข้มงวดก็ไม่ควรนำโปรแกรมตรวจสอบมาใช้งาน โปรแกรมคอมพิวเตอร์ที่จะนำมาใช้ในการตรวจสอบควรจัดทำเอกสารประกอบระบบงานอย่างรอบคอบ เพื่อระบุวัตถุประสงค์ และเพื่อให้ผู้ใช้แน่ใจว่าจะมีประโยชน์อย่างต่อเนื่อง และมีการทำงานที่ไว้ใจได้

เมื่อนำโปรแกรมตรวจสอบสำเร็จรูปมาใช้งาน ผู้ตรวจสอบต้องเชื่อมั่นว่าการประมวลผลถูกต้อง นั่นคือต้องมีการควบคุมที่เหมาะสม ดังนี้

- กำหนดให้มีการควบคุมโปรแกรมตรวจสอบสำเร็จรูปทางกายภาพ ถ้าโปรแกรมดังกล่าวไม่ได้อยู่ในระบบและมีการป้องกันอย่างเหมาะสม
- สังเกตการประมวลผลของระบบงานตรวจสอบ
- กำหนดจุดควบคุมต่าง ๆ ในโปรแกรมอย่างเป็นอิสระ ซึ่งจะตรวจตราหรือควบคุมการประมวลผลโปรแกรมตรวจสอบสำเร็จรูป
- กำหนดการควบคุมคุณลักษณะของโปรแกรมสำเร็จรูป การจัดการเอกสารประกอบระบบงานและใบควบคุมงาน
- ควบคุมความถูกต้องในการประมวลแฟ้มข้อมูลและการแสดงผลลัพธ์

3. การมีส่วนร่วมในการพัฒนาและทดสอบระบบงานของหน่วยงานตรวจสอบ

การพัฒนาระบบงานอัตโนมัติใด ๆ เป็นกระบวนการที่ใช้เวลายาวนานและซับซ้อน จึงต้องการแหล่งข้อมูลที่สำคัญและการประสานงานระหว่างกลุ่มผู้เขียนโปรแกรมและผู้ใช้ในฝ่ายงานต่าง ๆ เพื่อให้มั่นใจได้ว่าระบบงานที่พัฒนาขึ้นมาได้ตอบสนองความต้องการขององค์กร ซึ่งจะต้องมีขั้นตอนการพัฒนาโดยละเอียด และในระหว่างการพัฒนาแต่ละขั้นตอนนั้นผู้ตรวจสอบควรจะสอบทานการควบคุมภายในและร่องรอยการตรวจสอบของแต่ละระบบงานด้วย เนื่องจากการเปลี่ยนแปลงแก้ไขโปรแกรมระบบงานที่พัฒนาเสร็จเรียบร้อยแล้วเป็นเรื่องยากและต้องใช้ค่าใช้จ่ายสูง ผู้ตรวจสอบจึงต้องมีส่วนร่วมในระหว่างการพัฒนางาน เพื่อให้มั่นใจได้ว่ามีจุดควบคุมที่สำคัญรวมอยู่ในระบบงานด้วยตั้งแต่แรกเริ่ม โดยผู้ตรวจสอบต้องกำหนดแนวทางที่จะใช้ในการสอบทานระบบงานใหม่ในขั้นตอนของการออกแบบระบบงาน เพื่อที่จะสามารถระบุการควบคุมที่จะตรวจสอบได้ตั้งแต่ต้น

อย่างไรก็ตามหน้าที่การตรวจสอบโดยอิสระยังคงเป็นสิ่งจำเป็นสำหรับองค์กร ผู้ตรวจสอบควรมีอิสระในการตัดสินใจและเสนอแนะการควบคุมที่เหมาะสมแก่ฝ่ายบริหารอย่างระมัดระวังว่าจะไม่รับประกันจุดควบคุมของผู้ออกแบบระบบงานโดยไม่มีคุณภาพ นอกจากนี้ผู้ตรวจสอบต้องระวังที่จะไม่ก้าวก่ายหน้าที่ของผู้ใช้หรือผู้ออกแบบระบบงานในเรื่องที่ไม่เกี่ยวข้องกับการตรวจสอบ

คณะผู้ตรวจสอบด้านคอมพิวเตอร์มักจะประสงค์ที่จะมีส่วนร่วมในการสอบทานระบบงานใหม่ ๆ หลังจากที่นำออกใช้งานแล้ว และทบทวนระบบงานที่ใช้อยู่ในปัจจุบันเพื่อจะมั่นใจได้ว่าระบบงานเหล่านั้นได้สนองตอบวัตถุประสงค์ที่ตั้งไว้ภายในงบประมาณและระยะเวลาที่กำหนด

การทดสอบ

เพื่อที่จะมั่นใจได้ว่าระบบงานต่าง ๆ มีจุดควบคุมที่สำคัญโดยครบถ้วนผู้ตรวจสอบควรจัดทำข้อมูลทดสอบและประเมินผลการทดสอบก่อนที่จะนำระบบงานใหม่ออกใช้งาน ในการบรรลุวัตถุประสงค์ดังกล่าว ผู้ตรวจสอบด้านคอมพิวเตอร์ควรจะทำความคุ้นเคยกับแหล่งกำเนิดข้อผิดพลาดต่าง ๆ การทดสอบความถูกต้องของข้อมูล และการควบคุมยอดรวมที่ได้

แหล่งกำเนิดข้อผิดพลาดต่าง ๆ ประกอบด้วย

- การให้รหัสผิดพลาด
- การประมวลผลผิดพลาด
- ตรวจการทำงานของโปรแกรมไม่สมบูรณ์
- การทดสอบเงื่อนไขต่าง ๆ ล้มเหลว
- การเปลี่ยนแปลงโปรแกรมไม่สมบูรณ์หรือเปลี่ยนแปลงโดยไม่ได้รับอนุมัติ

การทดสอบที่ฝังไว้ในโปรแกรม ประกอบด้วย

- ทดสอบที่จะเปิดเผยรายการยกเว้นต่าง ๆ ที่เกิดขึ้นเกินกว่าที่ได้กำหนดไว้ โดยการให้พิมพ์ exceptional report ขึ้นมา
- ทดสอบยอดรวมที่รวมแต่ละรายการโดยอิสระจากกัน และสอบยันกับยอดรวมที่พัฒนาโปรแกรมขึ้นมาคำนวณเอง
- ยอดรวมที่ใช้ในการควบคุมที่พัฒนาขึ้นมาในลักษณะเดียวกับยอดรวมที่ใช้ในการควบคุมข้อมูลนำเข้า
- การควบคุมข้อผิดพลาดของผู้ปฏิบัติงานโดยใช้โปรแกรมควบคุมเพื่อช่วยลดความถี่ในการเกิดข้อผิดพลาด โดยกำหนดให้แสดงข้อมูลให้ผู้ปฏิบัติงานทราบ ทดสอบความเหมาะสมของการติดตั้งอุปกรณ์ และตรวจสอบแฟ้มข้อมูลทุกแฟ้มที่จะนำมาใช้งานว่าเป็นแฟ้มข้อมูลที่ถูกต้อง
- จุดควบคุมที่ผู้แทนจำหน่ายจัดทำไว้ให้ในระบบเครื่องและในโปรแกรมสำเร็จรูป

สถาบันขนาดใหญ่บางแห่งที่มีฝ่ายประมวลผลข้อมูลขนาดใหญ่ด้วยอาจจะมีกลุ่มบุคคลอิสระที่ทำการทดสอบ เช่น กลุ่มรับประกันคุณภาพ ในกรณีนี้กลุ่มตรวจสอบคอมพิวเตอร์อาจไม่จำเป็นต้องเกี่ยวข้องกับการทดสอบระบบงานใหม่ ๆ ทั้งหมด แต่อาจสอบทานคุณภาพของการทดสอบโดยทั่วไปโดยตรวจสอบวิธีการ และผลงานของกลุ่มตรวจสอบในองค์กรอีกครั้งหนึ่ง

การทดสอบความถูกต้องของข้อมูล ประกอบด้วยการทดสอบ

- ความถูกต้องของการให้รหัส
- ความถูกต้องของตัวอักษร
- ขนาดของ field
- เครื่องหมายทางคณิตศาสตร์
- ส่วนประกอบของ field
- ความถูกต้องในการรวมกันของหลาย ๆ field
- ข้อมูลที่ขาดหายไป
- การเรียงลำดับ
- ข้อจำกัด หรือความสมเหตุสมผล
- การคำนวณตัวเลขที่ใช้ในการควบคุม (Check digit)

การคำนวณยอดรวมที่ใช้ในการควบคุมนั้นกระทำเพื่อป้องกันข้อผิดพลาดของข้อมูล และมักเป็นที่สนใจของผู้ตรวจสอบเป็นอย่างมาก กระบวนการใช้ยอดรวมเพื่อการควบคุมนั้นจะต้องมีการคำนวณตัวเลขที่ใช้ในการควบคุมก่อนการประมวลผล (ด้วย manual หรือ auto ก็ได้) และในระหว่างการประมวลผลก็มีการคำนวณอีกครั้งหนึ่ง แล้วนำยอดรวมที่ได้ไปเปรียบเทียบกับยอดรวมที่ได้คำนวณไว้ก่อนแล้ว ทั้งนี้ควรมีข้อความที่ยืนยันการเปรียบเทียบและตัวเลขยอดรวมแสดงให้เห็นด้วย ถึงแม้ว่าการเปรียบเทียบนั้นจะไม่ปรากฏข้อผิดพลาดใด ๆ ก็ตาม

การจัดทำเอกสารและรายงานการตรวจสอบ

ฝ่ายตรวจสอบควรกำหนดมาตรฐานที่เป็นลายลักษณ์อักษรสำหรับกระดาษทำการ และการติดต่อสื่อสารที่เกี่ยวข้องกับงานตรวจสอบไว้ในคู่มือตรวจสอบภายในด้วย เนื่องจากกระดาษทำการเป็นหลักฐานเบื้องต้นของงานตรวจสอบ จึงควรที่จะจัดรูปแบบที่ดี มีข้อความชัดเจนและครอบคลุมเนื้อหาภายในขอบเขตการตรวจสอบ

กระดาษทำการมักประกอบด้วย

- สำเนาวิธีการตรวจสอบ
- คำบรรยายจุดควบคุมการปฏิบัติงาน การบริหารงาน และที่มีอยู่ในโปรแกรมของศูนย์ประมวลผล
- คำบรรยายโดยละเอียดเกี่ยวกับการสอบทานอุปกรณ์เครื่องคอมพิวเตอร์และระบบงานต่าง ๆ
- คำบรรยายวิธีการและขอบเขตของการทำการทดสอบ
- คำอธิบายผลลัพธ์จากการทดสอบ

วิธีการสรุปและนำเสนอสิ่งที่พบจากการตรวจสอบต่อฝ่ายบริหารควรจะทำอย่างเป็นทางการ โดยติดต่อสื่อสารอย่างมีประสิทธิภาพ แนวทางปฏิบัติขั้นพื้นฐานมีดังนี้

- ควรสรุปประเด็นสำคัญที่พบจากการตรวจสอบอย่างชัดเจน ถกปัญหากับฝ่ายบริหาร และรายงานเป็นลายลักษณ์อักษรไปยังผู้บริหารอาวุโส และคณะกรรมการอำนวยการ
- ผู้ตรวจสอบอาวุโสควรแลกเปลี่ยนความคิดเห็นกับคณะกรรมการอำนวยการ ในเรื่องข้อบกพร่องที่ร้ายแรงเกี่ยวกับการควบคุมซึ่งงานตรวจสอบมิได้ครอบคลุมถึง และประเด็นสำคัญต่าง ๆ ที่พบจากการตรวจสอบและยังไม่ได้รับการแก้ไข
- รายงานการตรวจสอบทั้งหมดจะต้องเขียนเป็นอย่างดี เน้นข้อสังเกตที่สำคัญ ความเสียหายร้ายแรง และข้อเสนอแนะในการแก้ไขปัญหาอย่างกระชับ
- รายงานการตรวจสอบทั้งหลายจะต้องแสดงความคิดเห็นต่อหน้าที่ในการตรวจสอบ ระบุว่ามีการปรับปรุงแก้ไข หรือคลี่คลายไปในทางที่ดีขึ้นหรือไม่ นับตั้งแต่การตรวจสอบครั้งสุดท้าย พร้อมทั้งเหตุผลของการเปลี่ยนแปลงโดยละเอียด
- ข้อวิจารณ์ และข้อสังเกตทั้งหลายที่ระบุในรายงานการตรวจสอบจะต้องมีเอกสารสนับสนุนในกระดาษทำการ
- ฝ่ายบริหารควรทำหนังสือตอบรายงานการตรวจสอบภายในระยะเวลาที่เหมาะสม
- ผู้ตรวจสอบภายในต้องติดตามข้อสังเกตต่าง ๆ เพื่อให้แน่ใจว่าได้รับการแก้ไขแล้ว หรือคณะกรรมการอำนวยการได้ยอมรับความเสี่ยงที่เกิดขึ้นแล้ว

การรายงานข้อสรุปจากการตรวจสอบ

วิธีการพิเศษในแผนการตรวจสอบด้านคอมพิวเตอร์คือ ต้องทำให้ผู้ตรวจสอบภายในสามารถบรรลุวัตถุประสงค์การตรวจสอบที่เกี่ยวข้องได้ ข้อสรุปจะต้องมีความเหมาะสมในแง่ของการปฏิบัติงานตรวจสอบ และสอดคล้องกับข้อสังเกตที่บันทึกไว้เป็นลายลักษณ์อักษรผู้ตรวจสอบจะต้องใช้วิจารณญาณที่ดีในการจำแนกข้อสังเกตที่มีนัยสำคัญมิฉะนั้นแล้วผู้ตรวจสอบอาจขาดประสิทธิภาพโดยทำให้รายงานการตรวจมีเรื่องหยุมหยิมอยู่เกลื่อนกลาด ซึ่งไม่มีความหมายต่อคณะกรรมการอำนวยการและผู้บริหารอาวุโส

รายงานการตรวจสอบที่เป็นลายลักษณ์อักษรจะเป็นตัวกลางในการสื่อสารข้อมลูที่เป็นประโยชน์ระหว่างฝ่ายปฏิบัติการและฝ่ายที่รับผิดชอบงาน รายงานดังกล่าวควรมีส่วนช่วยประเมินผลการปฏิบัติงานทั้งสิ้นของฝ่ายประมวลผลหากสามารถบรรลุวัตถุประสงค์ดังกล่าวได้รายงานการตรวจสอบมิได้เพียงแต่ช่วยเน้นจุดที่น่าสนใจที่มีการปฏิบัติงานผิดพลาดหรือวิธีการควบคุมประจำวันหย่อนยาน แต่ยังช่วยแจ้งให้ทราบจุดเสี่ยงภัยที่พบในงานประมวลผลข้อมูลพร้อมทั้งข้อแนะนำในการแก้ไขหรือปรับปรุงอีกด้วย รายงานการตรวจสอบควรจัดทำให้ทันเวลา สรุปข้อเท็จจริงและชี้ให้เห็นถึงสถานะของข้อสังเกตในครั้งก่อน ข้อมูลในรายงานควรมีโครงสร้างที่ดี ถูกต้อง และนำเสนออย่างชัดเจนสมเหตุสมผลเพื่อที่รายงานการตรวจสอบที่มีข้อตำหนิทุกชิ้นจะกระตุ้นให้ผู้บริหารเริ่มตัดสินใจ

อย่างไรก็ดีการสรุปผลการตรวจสอบด้วยวาจามักจะนำมาใช้อยู่เสมอในการนำเสนอสิ่งที่พบจากการตรวจสอบและวิธีการแก้ไขปัญหาที่เป็นไปได้ในระหว่างการปฏิบัติงานตรวจสอบ ดังนั้นผู้ตรวจสอบจะต้องสามารถติดต่อสื่อสารอย่างมีประสิทธิภาพทั้งด้วยวาจาและเป็นลายลักษณ์อักษร ดังนั้นผู้บริหารที่เอาใจใส่และไม่ต้องการให้เกิดปัญหาการทุจริตหรือป้องกันการทุจริตนี้ไม่ให้เกิดขึ้นในองค์กรของตน ควรให้ความสำคัญและดำเนินการแก้ไขตามคำแนะนำของผู้ตรวจสอบโดยเร็วก่อนที่ความเสียหายจะเกิดขึ้น

วิธีการตรวจสอบเพื่อค้นหาจุดอ่อนในระบบงานรวมทั้งการทุจริตที่อาจเกิดขึ้นหรือเกิดขึ้นแล้วก็ตามผู้ตรวจสอบควรได้ทบทวนเรื่องการตรวจสอบระบบงานหรืองาน (Application) ดังได้สรุปไว้ในข้อต่อไป

4. การวิเคราะห์ความเสี่ยง ผลเสียหาย การควบคุม และการตรวจสอบ

จากตัวอย่างของจุดอ่อนต่าง ๆ ในระบบงานและการทุจริตตามที่กล่าวในบทก่อน ๆ เป็นเพียงส่วนน้อยและความเสียหายในแง่มุมต่าง ๆ ที่หยิบยกมาพูดถึง จะทำให้ผู้รับฟังได้เข้าใจและเห็นภาพจริงของความเสี่ยงและความเสียหายเมื่อจะได้วิเคราะห์ถึงจุดควบคุมต่าง ๆ ทั้งในด้านการป้องกัน (Preventive) การค้นให้พบปัญหาและข้อผิดพลาด (Detective) และการแก้ไข (Corrective) เพื่อจะลดความเสี่ยงและความเสียหายให้มีน้อยที่สุด หรือสามารถแก้ไขปัญหาใหญ่ ๆ ที่อาจแก้ไขได้ยากมาเป็นปัญหาที่อาจแก้ไขได้อย่างมีประสิทธิภาพ โดยหยิบยกตัวอย่างที่เป็นจริงมาเป็นอุทาหรณ์ พร้อมทั้งอธิบายเพิ่มเติมในหลักการวิเคราะห์ความเสี่ยง เพื่อหาจุดควบคุมและตรวจสอบที่มีประสิทธิภาพ โดยชี้ให้เห็นถึงเหตุต่าง ๆ ที่อาจนำไปสู่ความเสียหายหรือความสำเร็จของงานอย่างเป็นระบบ ซึ่งประกอบไปด้วย

4.1) การพิจารณามูลเหตุที่นำไปสู่ความเสียหาย

4.2) การประเมินความเสี่ยงและความเสียหาย

4.3) การพิจารณาวิธีการควบคุมความเสี่ยงและความเสียหาย

4.4) การประเมินประสิทธิภาพของการควบคุม

วิธีการดังกล่าว จะเป็นการนำไปสู่การค้นหาจุดอ่อนในระบบงานที่อาจก่อให้เกิดการทุจริตได้ต่อไปหรืออย่างน้อยก็ช่วยให้ผู้บริหารทราบว่าองค์กรควรจะออกกฎเกณฑ์และระเบียบปฏิบัติที่เกี่ยวข้องอย่างไรต่อไป

5. ผลกระทบของคอมพิวเตอร์ต่อการควบคุมทางด้านบัญชี (Accounting Control) บางประการ

5.1 กิจกรรมต่าง ๆ ที่ก่อให้เกิดความเสี่ยง ที่เป็นประเด็นสำคัญในการควบคุมกิจกรรมนั้น ๆ ในระบบ Manual อาจควบคุมโดยการใช้พนักงานหลาย ๆ คน แบ่งแยกกันทำกิจกรรมนั้น ๆ โดยมิให้บุคคลใดบุคคลหนึ่งกระทำรายการตั้งแต่แรกจนจบตามลำพัง

แต่ในระบบงานที่ใช้คอมพิวเตอร์นั้น กิจกรรมต่าง ๆ ตามที่กล่าวข้างต้นอาจถูกประมวลโดยระบบคอมพิวเตอร์ตั้งแต่แรกจนจบกระบวนการในลักษณะเป็น Centralize ที่ประมวลโดยโปรแกรมคอมพิวเตอร์ทำให้การแบ่งแยกหน้าที่กันในระบบ Manual หมดไป

นี่คือความเสี่ยงที่เพิ่มขึ้นมาประการหนึ่ง ที่ผู้บริหารและผู้ตรวจสอบควรตระหนักถึง เพราะความเสี่ยง (Risk) ไม่อาจควบคุมได้ แต่กิจกรรม (Activities) ต่าง ๆ เป็นหัวใจที่ต้องการดูแลและควบคุม

5.2 ขาดเอกสารประกอบระบบงาน หรือมีก็ไม่ค่อยเพียงพอสำหรับผู้บริหารและผู้ตรวจสอบ ดังนั้นแนวทางการบริหารหรือเรียกอีกอย่างหนึ่งว่าร่องรอยการตรวจสอบ (Audit Trail) อาจหายไปหรือไร้ร่องรอยในการติดตาม ความเข้าใจของผู้ตรวจสอบต่อระบบงานที่ตรวจสอบจึงเป็นหัวใจของการตรวจสอบในองค์กรที่ใช้คอมพิวเตอร์ การสุ่มการตรวจสอบอาจใช้ไม่ได้ผล

5.3 การตรวจสอบด้วยตาหรือเอกสารต่าง ๆ เพื่อดูจุดควบคุมต่าง ๆ อาจต้องใช้คอมพิวเตอร์เป็นเครื่องมือเข้าช่วยในการตรวจสอบ

5.4 การเก็บข้อมูลใน Storage และการ Process ด้วย Program คอมพิวเตอร์ และการสร้างข้อมูลหรือ update ข้อมูลได้เองด้วยคอมพิวเตอร์นั้นทำให้ผู้ตรวจสอบต้องประเมินความน่าเชื่อถือของโปรแกรมเหล่านั้นก่อนให้ความเชื่อถือข้อมูลใน Report หรือ Hard Copy ต่าง ๆ

6. ข้อควรคำนึงและพิจารณาในการตรวจสอบ

6.1 ความพอเพียงของระบบการควบคุมภายใน ในทางการบัญชี (Adequacy of Internal Accounting Control)

6.2 การดำเนินการแบบต่อเนื่อง (Going Concern)

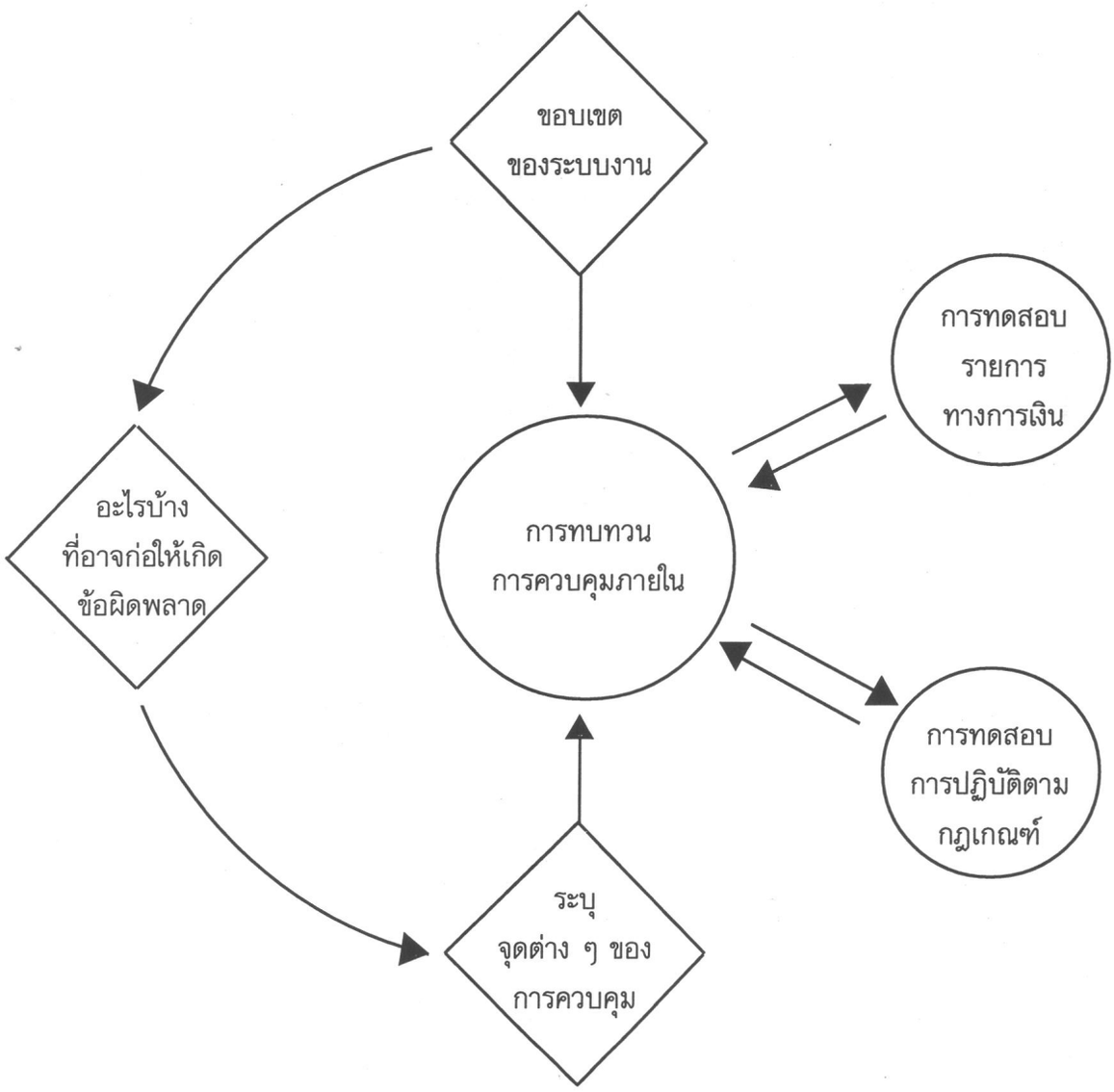
6.3 แนวโน้มของการทุจริต การปฏิบัติในทางที่ไม่ชอบและการกระทำที่ผิดกฎหมาย (Potential of Fraud, Irregularities or Illegal Acts)

6.4 ความพอเพียงของนโยบายและวิธีการปฏิบัติ (Operating Policy and Procedure Adequacy)

หมายเหตุ : วัตถุประสงค์ของการควบคุมหลัก ๆ ที่ใคร่ขอทบทวนก็คือ

1. การควบคุมด้านการเงิน : ซึ่งได้แก่การควบคุม การอนุมัติ และบันทึกรายการอย่างครบถ้วนถูกต้องสมบูรณ์ในเวลาที่กำหนดตามหลักการและวิธีการบัญชีที่ยอมรับอย่างสากล
2. การควบคุมด้านการดำเนินงาน : ได้แก่การควบคุมด้านการปฏิบัติงานอย่างมีประสิทธิผลและมีประสิทธิภาพด้วยความประหยัด
3. แบบของการควบคุม : มี 3 แบบด้วยกันคือ Preventive, Detective และ Corrective

7. การตรวจสอบกับการควบคุมโดยย่อ



ทบทวนองค์ประกอบของการควบคุม

8. วิธีการตรวจสอบแบบ Total System Approach

- Total System หมายถึง ขั้นตอนหรือวิธีการต่าง ๆ ที่ได้จากระบบงานที่ใช้คอมพิวเตอร์จากจุดเริ่มต้นของข้อมูล ถึงจุดที่ได้ผลลัพธ์ออกมา การใช้ผลลัพธ์จากการประมวลผล ตลอดจนถึงการจัดทำเอกสารประกอบระบบงานการตรวจสอบทั้งในส่วนที่ใช้คอมพิวเตอร์ ส่วนที่เป็น Manual และส่วนผสมของคอมพิวเตอร์กับ Manual
- วิธีนี้สามารถใช้กับผู้ตรวจสอบที่มีความรู้คอมพิวเตอร์เพียงเบื้องต้น
- เป็นวิธีการเข้าใจระบบงานอย่างง่าย ๆ โดยวิเคราะห์การควบคุมของระบบงานทีละขั้น
- ช่วยในการวางรูปแบบหรือจัดทำเอกสารประกอบการตรวจสอบ
- ช่วยให้การทำงานด้านตรวจสอบเข้าลักษณะเป็นการตรวจสอบด้านโครงสร้างด้วย (Structure)

9. จุดที่ควรตรวจสอบและข้อควรคำนึงบางประการในภาพรวม ๆ ของการตรวจสอบ

9.1 ขึ้นกับเป้าหมายและขอบเขตการตรวจสอบ

9.2 ทุกกรณีของเป้าหมายการตรวจสอบสิ่งที่ต้องคำนึงก็คือ "จุดที่อาจก่อให้เกิดความเสี่ยงและความเสียหายให้กับองค์กรได้" ข้อสำคัญที่ไม่ควรละเลยก็คือ จุดอ่อนที่อาจก่อให้เกิดการทุจริตได้ด้วย

9.3 การตรวจสอบและประเมินประสิทธิภาพการควบคุมก็คือ การตรวจสอบความพอเพียงในการควบคุมความเสี่ยงต่าง ๆ ดังนั้นการวิเคราะห์ความเสี่ยงด้านต่าง ๆ ขององค์กรเป็นความท้าทายความสามารถของผู้บริหาร และผู้ตรวจสอบเป็นอย่างยิ่ง เพราะมีปัจจัยหลายประการที่ต้องการความเข้าใจอย่างลึกซึ้งของผู้ที่เกี่ยวข้องโดยเฉพาะอย่างยิ่งองค์กรที่ใช้คอมพิวเตอร์ในการประมวลข้อมูล

9.4 จุดที่ควรควบคุมในด้านต่าง ๆ ขององค์กร มีปัจจัยที่ต้องพิจารณาดังนี้

9.4.1 ความเสี่ยง

9.4.2 จุดอ่อนที่อาจก่อให้เกิดความเสียหาย

9.4.3 ต้นทุนของการควบคุมนั้น เช่น ถ้าการควบคุมต้องมีต้นทุนที่สูงเกินไปเมื่อเทียบกับความเสียหายที่จะเกิดขึ้น องค์กรก็อาจเลือกระดับการควบคุมที่พอยอมรับได้ ส่วนต่าง ๆ ที่เป็นความเสียหายที่อาจจะเกิดขึ้นก็บริหารโดยการทำประกันภัยให้ครอบคลุมความเสียหายได้ เป็นต้น

หมายเหตุ : Total System อาจอธิบายเพิ่มเติมว่าเป็นการตรวจสอบงานที่เป็นระบบตามโครงสร้างของการประมวลผลทั้งในแบบ Manual, Automation และแบบผสมของ Input – Processing – Output รวมทั้งการใช้ผลลัพธ์ในรูปแบบต่าง ๆ ให้เป็นประโยชน์ตั้งแต่การจัดทำเอกสารประกอบระบบงานจนถึงการทำรายงาน

9.5 การพิจารณาวิเคราะห์ความเสี่ยงและความพอเพียง การควบคุมในองค์กรที่ใช้คอมพิวเตอร์และ/หรือความเสี่ยงทางด้านคอมพิวเตอร์ มีหลักการโดยสรุปดังนี้

9.5.1 ระบุประเภทรวมทั้งปริมาณความเสี่ยงและความเสียหายที่อาจจะเกิดขึ้น

9.5.2 กำหนดระดับความเสี่ยงที่องค์กรอาจยอมรับได้ (ขึ้นกับต้นทุนการควบคุม)

9.5.3 ออกแบบและกำหนดการควบคุมที่จำเป็นไม่ว่าจะเป็นการกำหนดนโยบายคำสั่ง ระเบียบวิธีการปฏิบัติงานการตรวจสอบให้เพียงพอที่จะควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้เท่านั้น

9.5.4 วิเคราะห์และพิจารณารวมทั้งประเมินประสิทธิภาพของการควบคุมความเสี่ยงเหล่านั้น

หลักการข้างต้น อาจกล่าวได้ว่าเป็นงานของการวิเคราะห์ความเสี่ยงและการควบคุมในองค์กรโดยภาพรวม ๆ ดังนั้น ผู้บริหารและผู้ตรวจสอบควรทราบวงจรนี้ เพราะมีประโยชน์อย่างยิ่งในการบริหารงานและการตรวจสอบ โดยเฉพาะอย่างยิ่งการประเมินและการตรวจสอบการปฏิบัติงานขององค์กร

การวิเคราะห์ความเสี่ยงในปัจจุบันจึงเป็นหัวใจของความสำเร็จในการบริหารงานและการตรวจสอบอย่างแท้จริง และเป็นจุดเริ่มต้นของการตรวจสอบไม่ว่าจะเป็นการตรวจสอบประเภทใด

9.6 ภาพการตรวจสอบด้านคอมพิวเตอร์และ/หรือองค์กรที่ใช้คอมพิวเตอร์โดยสรุปก็คือ

9.6.1 การพิจารณาและวิเคราะห์ความเสี่ยง

9.6.2 ค้นหาจุดอ่อนที่อาจก่อให้เกิดความเสียหายได้

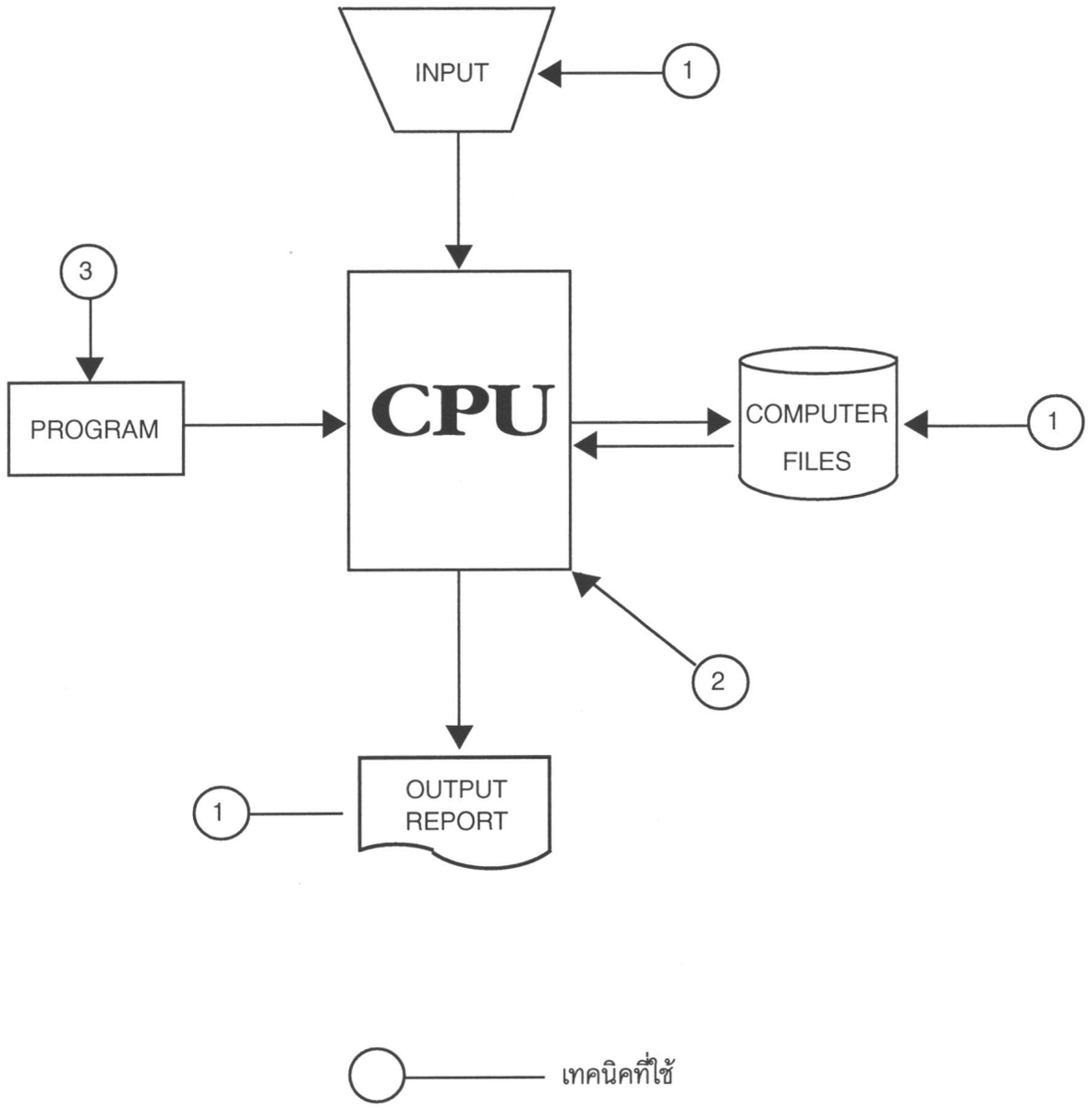
9.6.3 พิจารณาและประเมินประสิทธิภาพตลอดจนความพอเพียงของการควบคุมด้านต่าง ๆ ที่อาจก่อนให้เกิดความเสียหายนั้น และ

9.6.4 ดำเนินการตรวจสอบตามเป้าหมายที่กำหนด

หมายเหตุ : การควบคุม (Controls) คือ การดำเนินการใด ๆ ไม่ว่าด้วยวิธีการอะไรเพื่อลดจุดอ่อนที่อาจก่อให้เกิดความเสียหายกับองค์กรหรือระบบงานโดยรวมหรือลดความเสียหายให้กับฐานะความมั่นคงของระบบการเงิน ซึ่งขึ้นกับเป้าหมายของการกำกับหรือการควบคุมนั้น ๆ

10. เทคนิคที่ใช้ในการสร้างคอมพิวเตอร์โปรแกรมเพื่อการตรวจสอบ

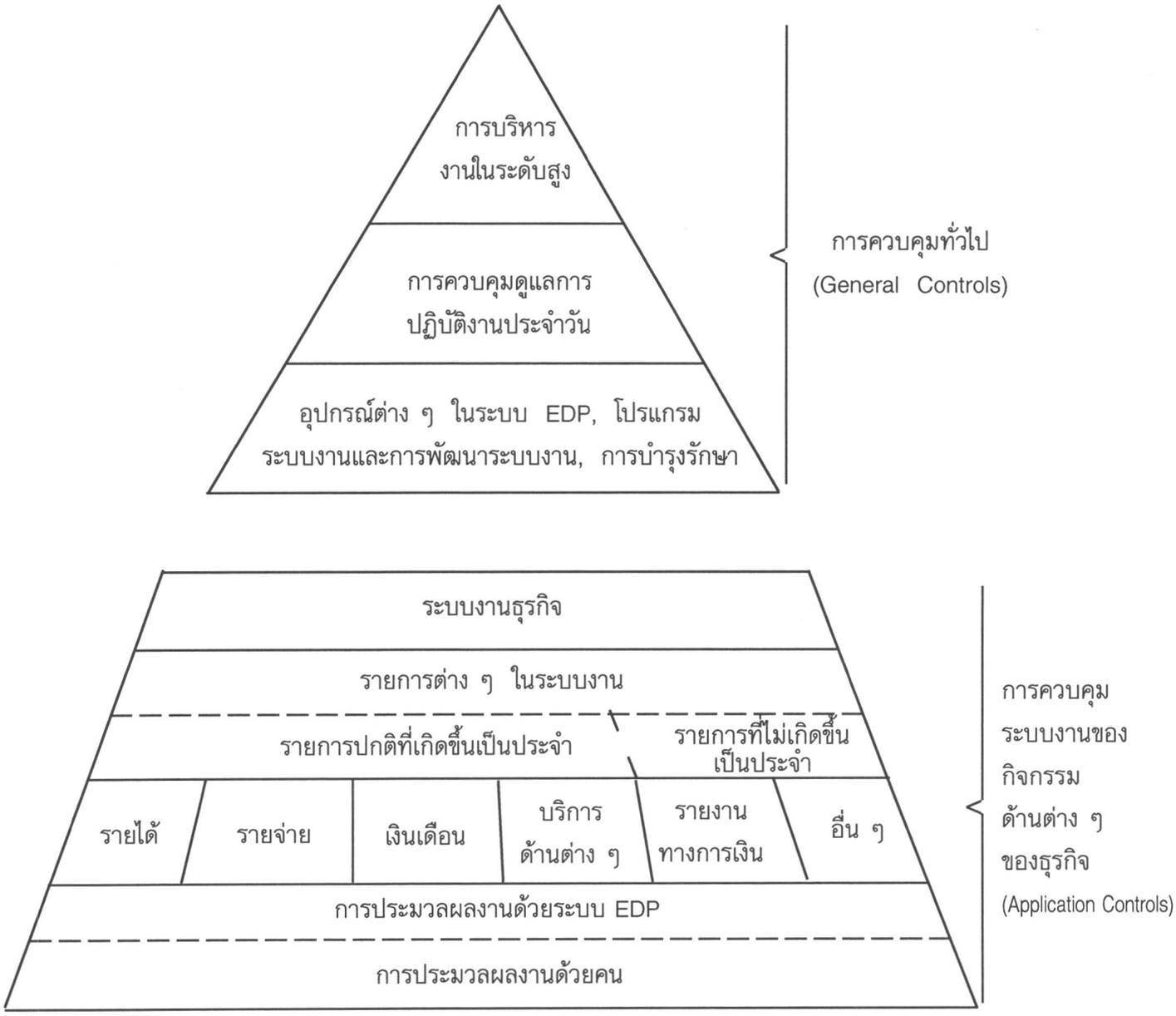
1. HISTORICAL DATA TECHNIQUES
2. CONCURRENT DATA TECHNIQUES
3. PROGRAM ANALYSIS



11. แนวทางการตรวจสอบการควบคุมทางบัญชีของระบบงาน (EDP Accounting Application)

ขั้นตอนของการประมวลข้อมูล	แนวทางหรือร่องรอยการตรวจสอบ
ข้อมูลนำเข้า (Input) - การบันทึกรายการ - การจัดเตรียมการป้อนข้อมูลแบบเป็นชุด (Batch) - การบันทึกข้อมูลแบบเป็นชุด ๆ - การบันทึกข้อมูลแบบ On-line	- เอกสารหลักฐานเบื้องต้นที่เกี่ยวข้องของที่มาของข้อมูล - list ที่แสดงรายการของข้อมูลที่นำเข้าต่าง ๆ - รหัสต่าง ๆ ที่ระบุถึงที่มาของข้อมูลนั้น ๆ - ความถูกต้องสมบูรณ์ของรายการในเทปในแผ่นดิสก์ - บันทึกของข้อมูลเป็นชุดที่สื่อที่เกี่ยวข้อง - เอกสารหรือสลิปประกอบข้อมูลในสื่อนั้น ๆ - บันทึกหรือทะเบียนที่แสดงความผิดพลาดทั้งในระบบ Manual และ Computer file - ข้อมูลทดสอบ (Test Data) - เอกสารต่าง ๆ ประกอบโปรแกรมระบบงานที่เกี่ยวข้อง
การประมวลผล (Processing) - ความถูกต้องสมบูรณ์ทันการของข้อมูล - การคำนวณ - การเปรียบเทียบ - การสรุป - การ update ข้อมูลใน File ต่าง ๆ - การดูแลรักษาแฟ้มข้อมูล (File) ต่าง ๆ - การลำดับข้อมูล - การติดตามตรวจสอบข้อมูล - การแก้ไขข้อผิดพลาด	- ค่าและความหมายในตารางการปฏิบัติงานที่กำหนด (Table Content) ทำให้ข้อมูลผลลัพธ์ผิดไปจากความเป็นจริง - ค่าของความสัมพันธ์ของข้อมูลที่กำหนดไว้แล้ว (Factor Value) - ข้อมูลที่นำเข้าสู่ระบบการประมวลผลโดยผู้ปฏิบัติงาน (Operation) - การเปลี่ยนแปลงค่าหรือทางเลือกที่กำหนดไว้แล้ว (Default Option) ทำให้ข้อมูลผลลัพธ์ผิดไปจากความเป็นจริง - รายการประมวลข้อมูลที่ listings - รายการที่แสดงถึงข้อมูลที่ประมวลหรือเกิดขึ้นอย่างอัตโนมัติ - แฟ้มข้อมูลที่แสดงกิจกรรมการประมวลผล - แฟ้มข้อมูล (File) ที่ใช้บันทึกข้อผิดพลาดเป็นการชั่วคราว - ทะเบียนการบันทึกข้อผิดพลาดทางการประมวลข้อมูล - ข้อมูลทดสอบ (Test Data)
ข้อมูลผลลัพธ์ (Output) - ข้อมูลที่อยู่ใน File - รายงานต่าง ๆ - เอกสารต่าง ๆ	- แฟ้ม (เทป, ดิสก์) ข้อมูลต่าง ๆ - ยอดเงินคงเหลือที่เกี่ยวข้องใน File (แฟ้มข้อมูล) - รายงานทางการบัญชีและการเงินต่าง ๆ - รายงานต่าง ๆ ของฝ่ายบริหาร ที่ได้จากการประมวลข้อมูล - รายงานอ้างอิงที่เกี่ยวข้อง - ทะเบียนการบันทึกข้อผิดพลาดของผลลัพธ์ไม่ว่าจะอยู่ในรูปแบบใด - รายงานข้อผิดพลาดต่าง ๆ - เอกสารแสดงข้อมูลผลลัพธ์ - ข้อมูลทดสอบ (Test Data)

12. โครงสร้างของการควบคุมในกิจการที่ใช้คอมพิวเตอร์



13. ความรับผิดชอบของผู้สอบบัญชีในด้านการตรวจสอบงานที่ประมวลผลด้วยคอมพิวเตอร์

13.1 ต้องเข้าใจขั้นตอนการทำรายการ (Flow of Transaction) เบื้องต้นที่ทำผ่านระบบงาน (Application) ที่มีนัยสำคัญต่อการประมวลผล และความถูกต้องของรายงานทางการเงิน

13.2 ต้องเข้าใจโครงสร้างของการควบคุมขั้นต้น (ทั้งในระบบ Manual และ Computerized)

13.3 ต้องเข้าใจรายละเอียดของข้อมูลที่บันทึกไว้ในแฟ้มข้อมูล (Content of EDP Files) และความเกี่ยวข้องของข้อมูลนั้น ๆ ที่มีต่อรายละเอียดในงบการเงิน

13.4 ถ้าหากองค์กรผู้รับตรวจสอบใช้เทคนิคการตรวจสอบ โดยใช้โปรแกรมการตรวจสอบจะต้องมีการทบทวนและทดสอบก่อนที่จะให้ความเชื่อถือ

13.5 การทบทวนระบบการควบคุมภายในของงานที่ประมวลผลด้วยคอมพิวเตอร์ และการใช้เทคนิคทางด้านการตรวจสอบโดยใช้คอมพิวเตอร์ จะต้องปฏิบัติงานโดยผู้สอบบัญชีที่มีความรู้ทางด้านเทคนิคอย่างเพียงพอ

14. วิธีการตรวจสอบระบบจะช่วยผู้สอบบัญชีได้อย่างไร

การศึกษาถึงขั้นตอนการตรวจสอบระบบในส่วนรวม จะช่วยงานตรวจสอบของผู้สอบบัญชีได้ดังนี้ คือ

14.1 รู้ว่ามีงานอะไรบ้างที่สมควรจะต้องเข้าไปตรวจสอบ และควรจะเริ่มงานอย่างไร

14.2 รู้ว่ามีเอกสารเกี่ยวกับอะไรบ้างที่ควรได้รับการตรวจสอบ

14.3 รู้ขั้นตอนการปฏิบัติงาน และรู้ว่าควรจะทำเมื่อใด

14.4 รู้ว่าเมื่อใดที่ฝ่ายบริหารควรจะเข้ามามีส่วนในการตัดสินใจก่อนที่จะเริ่มงานตรวจสอบต่อไป

15. สิ่งที่ผู้ตรวจสอบควรทราบในการตรวจสอบการทุจริต

15.1 เข้าใจองค์ประกอบในการตรวจสอบแต่ละเรื่อง องค์ประกอบในการตรวจสอบในเรื่องใด ๆ ก็ตาม ควรมีองค์ประกอบในการตรวจสอบดังต่อไปนี้

15.1.1 วัตถุประสงค์ที่ต้องการบรรลุ

15.1.2 กิจกรรมที่มีอยู่ในแต่ละเรื่อง หรือในแต่ละขั้นตอนที่จะตรวจสอบหรือเกิดขึ้นในการประมวลรายการ

15.1.3 ข้อผิดพลาดที่อาจเกิดขึ้นได้ในแต่ละขั้นตอนการประมวลผล สาเหตุของข้อผิดพลาด ความบ่อยและขนาดของข้อผิดพลาดที่อาจจะเกิดขึ้น

15.1.4 การควบคุมที่สามารถกำหนดเพื่อป้องกันสาเหตุของข้อผิดพลาดหรือติดตาม และแก้ไขข้อผิดพลาด และประสิทธิผลของการควบคุมเหล่านั้น

15.1.5 จุดอ่อนที่สามารถเกิดขึ้นได้ถ้าการควบคุมสาเหตุของข้อผิดพลาดและจุดอ่อนนั้น ๆขาดประสิทธิผล

15.1.6 การทดสอบเพื่อตรวจสอบการควบคุมจุดอ่อนอย่างเหมาะสม

16. เข้าใจประเด็นที่ต้องพิจารณาในการเริ่มการตรวจสอบ คือ

16.1 การมองผังทางเดินของกิจกรรมและความสัมพันธ์กับข้อผิดพลาด หรือการควบคุมที่เกี่ยวข้องให้ออก

16.2 การพิจารณาตัดสินใจเลือกเอกสารที่จำเป็นในการทำความเข้าใจกิจกรรมต่าง ๆ และการหาจุดที่อาจเกิดข้อผิดพลาด ระดับและความบ่อยของข้อผิดพลาดที่อาจเกิดขึ้น จุดที่ควรมีการควบคุม และจะประสานทั้งสองสิ่งอย่างไรในลักษณะที่เหมาะสม และเป็นเหตุเป็นผลต่อกัน

16.3 เพื่อเข้าใจว่าการควบคุมบางอันมีประสิทธิภาพและประสิทธิผลเหนือการควบคุมอื่น และในบรรดาการควบคุมอื่น ๆ นั้นอาจมีประสิทธิผลและประสิทธิภาพพอ ๆ กัน

16.4 เพื่อเข้าใจว่าจุดอ่อนบางอันอาจไม่มีความสำคัญต่อวัตถุประสงค์ในการตรวจสอบเลย ในขณะที่จุดอ่อนบางอันกลับมีความสำคัญอย่างยิ่งยวด

17. เข้าใจถึงการพิจารณาผังทางเดินของกิจกรรมและความสัมพันธ์กับข้อผิดพลาดหรือการควบคุมที่เกี่ยวข้อง

ผู้ตรวจสอบควรพยายามมองให้เห็นภาพพจน์ของกิจกรรม ขบวนการ ขั้นตอนต่าง ๆ ในระบบในขณะที่จะเริ่มขบวนการรวบรวมเอกสารข้อมูล และอาจใช้เทคนิคการตั้งคำถามเพื่อหาจุดที่สามารถก่อให้เกิดข้อผิดพลาดขึ้นได้ในแต่ละขบวนการและในแต่ละขั้นตอน คำตอบที่ได้จะชี้ถึงลักษณะของสาเหตุและความเฉพาะของความผิดพลาดที่เกิดขึ้น เช่น สาเหตุหนึ่งที่อาจทำให้เกิดจุดอ่อน คือ การบันทึกบัญชีผิดพลาด ซึ่งเป็นความผิดพลาดจากการทำด้วยมือ ลักษณะของความผิดพลาดก็อาจมีผลมาจากความผิดพลาดของพนักงาน เช่น ไม่บันทึกรายการให้ครบถ้วน หรือบันทึกรายการผิดพลาด หรือจำแนกประเภทรายการผิด เป็นต้น

คำถามที่ผู้ตรวจสอบควรถามต่อไปคือ ความผิดพลาดที่เกิดขึ้นนั้นมีสาระสำคัญหรือไม่ มีการควบคุมอะไรบ้าง ณ จุดนั้น ถ้าจะป้องกันมิให้เกิดจุดอ่อนขึ้นจะต้องมีการควบคุมอย่างไร

18. เข้าใจประเด็นคำถามที่เกี่ยวข้องกับองค์ประกอบในการตรวจสอบ

ประเด็นคำถามที่จะช่วยในการตรวจสอบ

องค์ประกอบในการตรวจสอบ	คำถามโดยทั่วไปของผู้ตรวจสอบ
จุดที่ตรวจสอบ	มีนัยสำคัญต่อการตรวจสอบหรือไม่
↓	↓
วัตถุประสงค์ในการควบคุมจุดนั้นหรือขบวนการนั้น	ทำไมจุดดังกล่าวจึงมีความสำคัญต่อการตรวจสอบ
↓	↓
กิจกรรมและการควบคุมต่าง ๆ ที่มี ณ จุดนั้น	กิจกรรมเหล่านั้นมีความสัมพันธ์กันอย่างไร
↓	↓
ลักษณะข้อผิดพลาดที่อาจเกิดขึ้นได้	ข้อผิดพลาดใดที่อาจเกิดขึ้นและมีนัยสำคัญ และโอกาสที่จะเกิดบ่อยเพียงไร
↓	↓
สาเหตุของข้อผิดพลาด	ทำไมจึงเกิดข้อผิดพลาด (ตั้งใจหรือไม่ได้ตั้งใจ)
↓	↓
สามารถควบคุมข้อผิดพลาดดังกล่าวได้อย่างไร	มีการควบคุมในจุดที่เป็นสาเหตุของข้อผิดพลาดที่ปรากฏหรือไม่ ถ้ามีการควบคุมดังกล่าวได้รับการออกแบบอย่างมีประสิทธิภาพและประสิทธิผลหรือไม่
↓	↓
ผลที่ตามมาถ้าไม่ได้มีการควบคุมข้อผิดพลาดดังกล่าว	ถ้าไม่ได้มีการควบคุมข้อผิดพลาด จุดอ่อนดังกล่าวจะมีผลเช่นไร
↓	↓
การกำหนดจุดควบคุมลงไป	มีวิธีทดสอบอย่างไรเพื่อตรวจสอบว่าการควบคุม สาเหตุข้อผิดพลาด และจุดอ่อนดังกล่าว ทำงานได้อย่างเหมาะสม
↓	↓
การออกระเบียบ กฎเกณฑ์ ข้อบังคับ (ที่มีแล้วหรือควรจะมีต่อไป)	หากไม่มีการปฏิบัติตามกฎเกณฑ์การควบคุมองค์กรจะมีผลกระทบที่เกิดจากความเสียหาย หรือผลกระทบต่อฐานะการเงินอย่างไร
↓	↓
ติดตามตรวจสอบการปฏิบัติตามกฎเกณฑ์ข้อบังคับนี้ หรือให้คำแนะนำที่ป้องกันปัญหาได้	ควรทำรายงานที่ครอบคลุมถึงประเด็นที่สำคัญ ๆ เพื่อให้มีการติดตามแก้ไขโดยฝ่ายบริหารอย่างไร โดยเฉพาะอย่างยิ่งรายงานและข้อแนะนำในลักษณะการป้องกันปัญหาก่อนที่จะเกิดปัญหา

19. วิธีการตรวจสอบระบบงาน (Application Audit)

การตรวจสอบการทุจริตในงานใดงานหนึ่ง มีหลักการขั้นตอนใหญ่ ๆ ในการตรวจสอบเช่นเดียวกับงานทั่วไปคือมี 3 ขั้นตอน

ขั้นตอนที่ 1 สอบทานระบบการควบคุมภายใน

ขั้นตอนที่ 2 ทดสอบการควบคุมภายในด้านที่สำคัญ

ขั้นตอนที่ 3 ตรวจสอบความถูกต้องของรายงานทางการเงิน

ขั้นตอนที่ 1 สอบทานระบบการควบคุมภายใน

วัตถุประสงค์ : เพื่อประเมินความเพียงพอของการควบคุมภายใน ทั้งโดยคนและโดยคอมพิวเตอร์

วิธีการที่ใช้ในการวิเคราะห์และประเมินผล

- กำหนดขอบเขตระบบงาน
- พิจารณาว่าอะไรบ้างที่สามารถเกิดข้อผิดพลาดได้
- ชี้จุดที่ต้องการควบคุม

ขั้นตอนที่ 2 ทดสอบการควบคุมภายในที่สำคัญ

ผู้ตรวจสอบต้องแน่ใจว่า องค์การมีการดำเนินการควบคุมในจุดที่สำคัญ โดย

- ทำการทดสอบความเหมาะสมของการควบคุมด้วยเครื่องคอมพิวเตอร์
- ทำการทดสอบ การควบคุมในส่วนที่ทำด้วยคน

ขั้นตอนที่ 3 ตรวจสอบความถูกต้องของรายงานทางการเงิน

ผู้ตรวจสอบต้องนำผลการทดสอบการควบคุมภายในมาใช้ในการกำหนดขอบเขตและวิธีการปฏิบัติในการตรวจสอบความถูกต้องของรายงานทางการเงินให้เหมาะสม ถ้าหากว่าองค์กรมีการควบคุมภายในอย่างเพียงพอและสามารถใช้ได้ผลแล้ว ขอบเขตในการตรวจสอบขั้นตอนที่ 3 ก็จะน้อยลงในสัดส่วนเดียวกัน

ในการตรวจสอบระบบงานใด ๆ ผู้ตรวจสอบต้องตรวจสอบทั้งในส่วนที่ประมวลผลด้วยคนและด้วยเครื่องคอมพิวเตอร์ ตลอดจนระบบงานอื่น ๆ ที่เกี่ยวข้อง เช่น การตรวจสอบบัญชีเงินฝากกระแสรายวัน ผู้ตรวจสอบต้องพิจารณาทั้งในส่วนคนและเครื่องคอมพิวเตอร์ และระบบการบัญชี การเรียกเก็บเงินตามเช็ค และเงินฝากประเภทอื่นที่เกี่ยวข้องกัน

20. การทำความเข้าใจในการตรวจสอบทั่วไป

วิธีการตรวจสอบ
ระบบงานที่ใช้
คอมพิวเตอร์

วัตถุประสงค์	ขั้นตอน	วิธีการ
- เพื่อประเมินความเพียงพอของการควบคุมภายในทั้งในส่วนที่เป็น Manual และ Automated (เพื่อหาจุดอ่อนที่อาจก่อให้เกิด ความเสียหายรวมทั้งการทุจริตได้)	สอบทานระบบการควบคุมภายใน	1. กำหนดวัตถุประสงค์ในการตรวจสอบทั้งหมดตั้งแต่เริ่มแรก 2. ทำความเข้าใจเบื้องต้นเกี่ยวกับธุรกิจของผู้รับตรวจ และลักษณะการปฏิบัติงาน 3. ทำความเข้าใจในวัตถุประสงค์ของธุรกิจนั้น 4. ทำความเข้าใจเกี่ยวกับอันตรายที่อาจจะเกิดขึ้นกับองค์กรนั้นหากไม่ปฏิบัติตามวัตถุประสงค์ที่ตั้งไว้ 5. ศึกษาความเสี่ยงที่สำคัญที่อาจเกิดขึ้นได้ 6. ทำความเข้าใจกับกระบวนการและโครงสร้างของการควบคุมที่องค์กรนั้นถือปฏิบัติ 7. พิจารณาว่า มีปัจจัยอะไรบ้างที่อาจจะส่งผลกระทบและเป็นอันตรายต่อระบบงานและข้อมูลขององค์กร 8. กำหนดรายละเอียดของความผิดพลาดและความเสี่ยงที่สามารถเกิดขึ้นในระบบงาน และในรายการที่มีสาระสำคัญ 9. หาวิธีเพื่อให้ได้รับมาซึ่งข้อมูลที่เพียงพอที่จะบอกรายละเอียดเพื่อประเมินจุดอ่อนจุดแข็งในการควบคุมทั้งในด้านประสิทธิ-ภาพและประสิทธิผล 10. กำหนดรายละเอียดการควบคุมหลัก ๆ ที่สามารถป้องกันและแก้ไขข้อผิดพลาดที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพและประสิทธิผล และเชื่อถือได้
- เพื่อให้แน่ใจว่าองค์กรมีการดำเนินการควบคุมในจุดที่สำคัญ ๆ	ทดสอบการควบคุมภายในที่สำคัญ	11. ออกแบบการทดสอบเพื่อทดสอบการควบคุมหลัก ๆ 12. ทดสอบความเหมาะสมของการควบคุมหลักในส่วนที่เป็น Manual และ Automated 13. ประเมินผลและรายงานผลการตรวจสอบ (ตามเป้าหมายขอบเขตการตรวจสอบ)
- เพื่อรวบรวมหลักฐานและข้อมูลที่จะเสนอในรายงานการตรวจสอบ เพื่อพิสูจน์ยอดคงเหลือตามบัญชีและข้อมูลอื่นในงบการเงิน (รวมทั้งชี้ประเด็นที่เป็นปัญหาด้วย)	ตรวจสอบความถูกต้องของรายการทางการเงิน	14. การสอบยัน การสำรวจหรือตรวจนับ วิธีการคำนวณ การตรวจสอบเอกสารประกอบการลงบัญชีการกระทบยอด 15. การวิเคราะห์ความผิดปกติจากตัวเลขหรืองบประมาณอัตราส่วนทางการเงิน 16. ประเมินผลและรายงานการตรวจสอบ ขึ้นอยู่กับว่าผู้ตรวจสอบตั้งเป้าหมายว่าเป็นการตรวจสอบประเภทใด (โปรดดูข้อ 13 ประกอบ)

สรุป - วิธีการตรวจสอบระบบงาน (Application Audit) รวมทั้งการตรวจสอบการทุจริตที่ใช้คอมพิวเตอร์ในรูปแบบที่เข้าใจได้ง่าย ๆ แบบหนึ่ง

21. สรุปแนวทางในการตรวจสอบจุดอ่อนในระบบงาน และการทุจริตด้านคอมพิวเตอร์

21.1 สร้างเป้าหมายในการตรวจสอบให้ชัดเจน เช่น เป้าหมายอยู่ที่การตรวจสอบการทุจริตที่เกิดขึ้นแล้วหรือจุดอ่อนที่อาจก่อให้เกิดการทุจริตได้ เป็นต้น

21.2 ประเมินระบบงานและวิธีการปฏิบัติงาน ตรวจสอบดูว่ามีจุดใดในแต่ละกิจกรรมของระบบงานนั้นที่มีความเสี่ยงและการก่อให้เกิดความเสียหายต่องค์กรได้บ้าง

21.3 ประเมินถึงความเสียหายที่มีนัยสำคัญ ทั้งทางการเงิน การบัญชีและผลกระทบทุกด้านรวมทั้งด้านกฎหมายต่าง ๆ

21.4 ประเมินการควบคุมที่สำคัญในแต่ละกิจกรรมที่อาจก่อให้เกิดความเสียหายนั้น ๆ

21.5 ประเมินประสิทธิภาพระบบการควบคุมภายในที่มีอยู่ว่าน่าเชื่อถือได้เพียงใด

21.6 เลือกเทคนิคการทดสอบเพื่อประเมินประสิทธิภาพของการควบคุมให้สอดคล้องกับเป้าหมายและแนวความคิดของผู้ตรวจสอบ

21.7 ดำเนินการตรวจสอบตามเทคนิคที่เลือกไว้แล้ว

21.8 วิเคราะห์ผลการตรวจสอบ

21.9 สรุปจุดอ่อน (ถ้ามี) เกี่ยวกับการควบคุมภายในนั้น

21.10 ประเมินผลกระทบและความเสี่ยงของจุดอ่อนที่มีอยู่โดยรวบรวมจุดอ่อนทั้งที่ไม่มีการควบคุมหรือจุดอ่อนที่มีการควบคุมแต่ไม่เพียงพอนั้น

21.11 ประเมินประเภทของการทุจริต โอกาสการทุจริต สถานที่ที่จะเกิดการทุจริต วิธีการทุจริตที่เป็นไปได้ ผู้ที่จะทุจริตได้ ผู้ที่จะเสียหายในแต่ละช่วง ความเสียหายที่เป็นจำนวนเงินและที่ไม่ใช่เป็นตัวเงิน เช่น ชื่อเสียงและการบริการลูกค้า ในแต่ละช่วงหรือในแต่ละขั้นตอนของจุดอ่อนนั้น

21.12 เลือกเทคนิคที่จะทดสอบการทุจริต ตามแนวความคิดของผู้ตรวจสอบที่จะเป็นไปได้มากที่สุดก่อน (ซึ่งเป็นที่แน่นอนว่าผู้ตรวจสอบนั้นต้องเข้าใจระบบงานและวิธีปฏิบัติงานดีแล้วเท่านั้น)

21.13 ปฏิบัติการทดสอบตามเทคนิคที่เลือกไว้แล้ว

21.14 วิเคราะห์ผลการตรวจสอบ

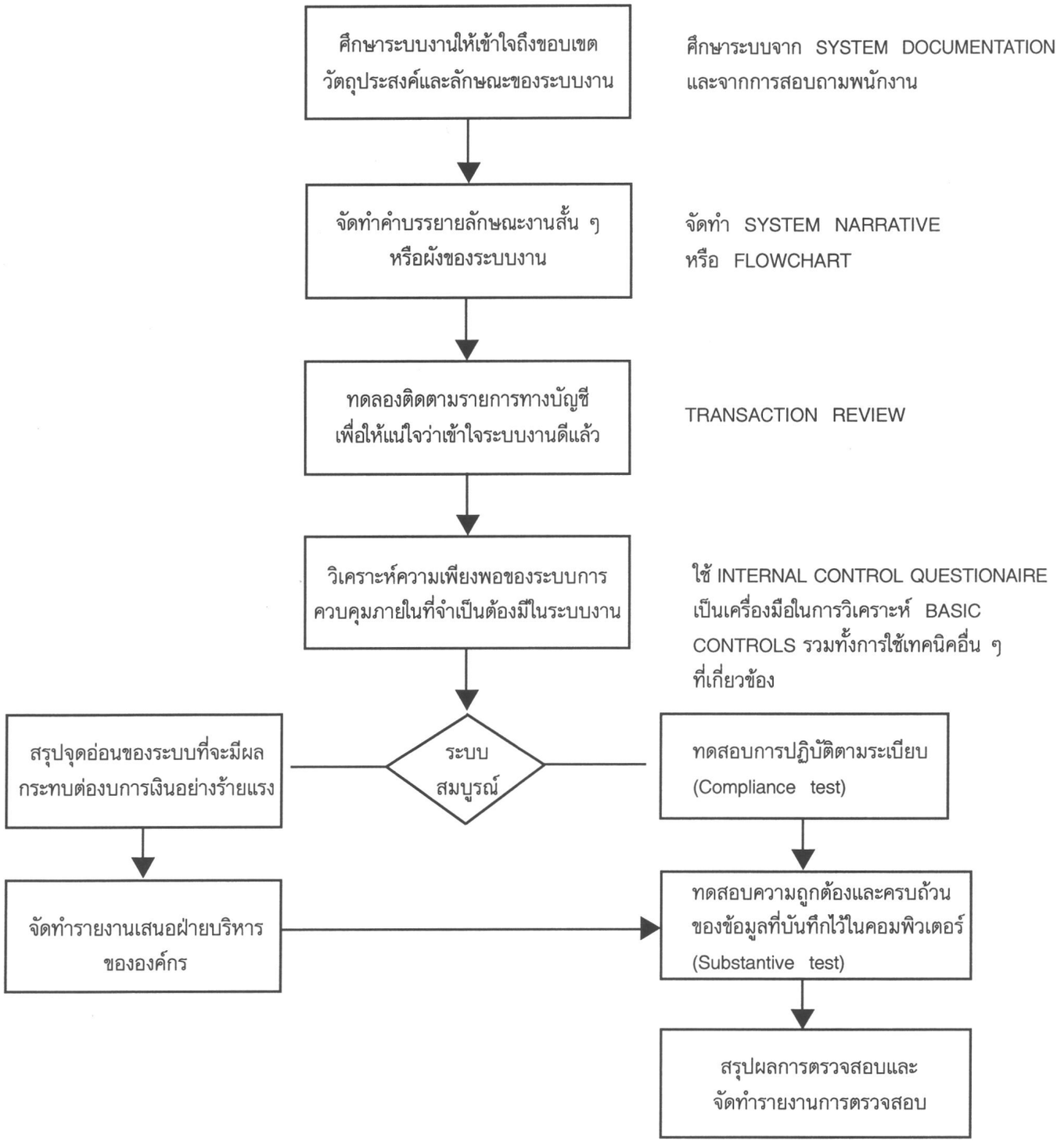
21.15 สรุปผลการตรวจสอบ

21.16 จัดทำรายงานการตรวจสอบ

หมายเหตุ : แนวทางดังกล่าวใช้ได้ดีกับการตรวจสอบระบบงานด้านคอมพิวเตอร์ทั่ว ๆ ไป หัวข้อนี้จึงเป็นการสรุปหรือทบทวนการตรวจสอบด้านคอมพิวเตอร์ที่ได้กล่าวรายละเอียดในเล่มสองแล้ว

22. แนวการตรวจสอบระบบงานในองค์กรที่ใช้คอมพิวเตอร์

EDP AUDIT APPROACH

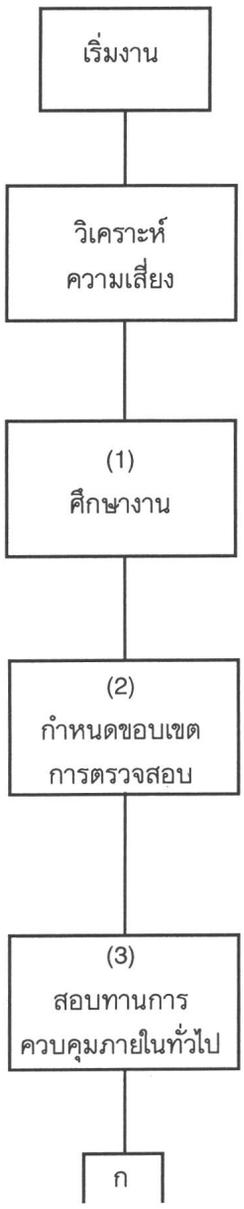


หมายเหตุ 1. เป็นอีกแนวทางหนึ่งจะเป็นการวิเคราะห์ความเสี่ยง (Risk) เพื่อให้เข้าใจถึงจุดควบคุม ระบบงานที่เกี่ยวข้อง

2. รวมทั้งการทุจริตที่อาจเกิดขึ้นหรือเกิดขึ้นแล้ว

3. จัดทำรายงานตามเป้าหมายที่กำหนดรวมทั้งการทุจริตที่ตรวจสอบ

23. แนวการตรวจสอบระบบงานด้านคอมพิวเตอร์ (Application Audit)



(1) ศึกษางานก่อนตรวจสอบ (Preliminary phase of review)

วัตถุประสงค์

เพื่อทำความเข้าใจระบบบัญชีที่ใช้คอมพิวเตอร์ และส่วนที่ไม่ได้ใช้คอมพิวเตอร์โดยศึกษา

- ทางเดินของรายการและรายงานที่มีความสำคัญ
- ขอบเขตการใช้คอมพิวเตอร์ของฝ่ายบริหารและงานบัญชีที่มีความสำคัญ
- โครงสร้างพื้นฐานของการควบคุมทางการบัญชีการควบคุมภายในด้าน คอมพิวเตอร์และการควบคุมผู้ใช้ข้อมูล

วิธีการ

โดยการสอบถาม สังเกตการณ์ ศึกษาจากเอกสารที่พอจะหาได้ ติดตามความเคลื่อนไหวของรายการ ใช้แบบสอบถามการควบคุมภายใน และ Check list

(2) กำหนดขอบเขตการตรวจสอบ (Determine scope of audit)

วัตถุประสงค์

- เพื่อประเมินขอบเขตการควบคุมภายในด้านคอมพิวเตอร์และด้านอื่น ๆ เช่น การทุจริต
- เพื่อกำหนดขอบเขตการตรวจสอบในส่วนที่เกี่ยวข้อง

วิธีการ

ขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบ

(3) สอบทานการควบคุมภายในทั่วไป (Review of general controls)

วัตถุประสงค์

- เพื่อศึกษาการควบคุมภายในทั่วไปและลักษณะการทำงานของการควบคุมภายในทั่วไป
- เพื่อศึกษาความรัดกุมและจุดอ่อนของการควบคุมภายในทั่วไป และผลกระทบที่มีต่อการควบคุมเฉพาะงาน
- พิจารณาถึงความจำเป็นในการทดสอบการควบคุมภายในทั่วไปบางประเภท

วิธีการ

ศึกษาระเบียบ ข้อบังคับ และมาตรฐานการปฏิบัติงานของหน่วยงานคอมพิวเตอร์ สอบถามและสังเกตการณ์

หมายเหตุ : แนวการตรวจสอบการทุจริตด้านคอมพิวเตอร์ไม่ว่าจะเกิดขึ้นแล้ว หรือการตรวจสอบเพื่อค้นหาจุดอ่อนในระบบงานที่อาจเกิดการทุจริตขึ้นได้ ก็อาจใช้แนวการตรวจสอบแบบข้างต้นได้อีกแบบหนึ่งแนวทางนี้ใช้การวิเคราะห์ความเสี่ยงนำในการปฏิบัติการตรวจสอบ เพราะการวิเคราะห์ความเสี่ยงจะทำให้ ผู้ตรวจสอบมองเห็นจุดที่ควรตรวจสอบนั่นคือจุดที่ก่อให้เกิดความเสียหายได้นั่นเอง



(4) สอบทานการควบคุมภายในเฉพาะงาน (Review of application controls)

วัตถุประสงค์

- เพื่อศึกษาการควบคุมภายในเฉพาะงาน และลักษณะการทำงานของการควบคุมภายในเฉพาะงาน โดยเฉพาะจุดที่เป็นเป้าหมายหลัก เช่น จุดที่อาจก่อให้เกิดการทุจริตได้
- พิจารณาถึงความจำเป็นในการทดสอบการควบคุมภายในเฉพาะงานบางประเภท โดยเพ่งเล็งไปถึงความผิดพลาด ความเสียหายที่เป็นผลกระทบต่อเป้าหมายหรือต่อฐานะทางการเงิน

วิธีการ

ศึกษาเอกสารระบบงานและโปรแกรมระเบียบ ข้อบังคับ หรือคู่มือปฏิบัติงานของหน่วยงานผู้ใช้ข้อมูล สอบถาม สังเกตการณ์

(5) ประเมินความรัดกุมของการควบคุมภายในที่สอบทานแล้ว (Assessment of controls)

วัตถุประสงค์

- เพื่อพิจารณาว่าข้อผิดพลาดหรือสิ่งผิดปกติที่จะเกิดขึ้นในแต่ละระบบงานเป็นข้อผิดพลาดชนิดใด
- วิธีการควบคุมที่ใช้สามารถค้นหาข้อผิดพลาดได้เพียงใด
- เพื่อประเมินประสิทธิภาพการควบคุมภายในด้านคอมพิวเตอร์และด้านอื่น ๆ ที่เกี่ยวข้อง

วิธีการ

ขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบ

(6) ทดสอบการปฏิบัติงานตามระเบียบข้อบังคับหรือข้อกำหนดในการประมวลผลข้อมูล (Test of Compliance)

วัตถุประสงค์

- เพื่อพิจารณาว่ามีการปฏิบัติตามระเบียบ ข้อบังคับ หรือข้อกำหนดในการประมวลข้อมูลเพียงใด
- เพื่อหาเหตุผลสนับสนุนก่อนที่จะแน่ใจว่าการควบคุมภายในที่ต้องการทดสอบทำหน้าที่ได้อย่างเหมาะสม
- เพื่อพิจารณาความเหมาะสมของขอบเขตการควบคุมภายในเอกสารหลักฐานผู้รับผิดชอบกำหนดเวลา และวิธีการที่ใช้เพื่อประโยชน์ในการควบคุมภายใน

วิธีการ

ตรวจสอบบันทึกการปฏิบัติงาน ทดสอบวิธีการควบคุมด้วยวิธีการที่เหมาะสม สอบถามและสังเกตการณ์



(7) ประเมินสรุปผลการควบคุมภายใน (Evaluation of controls)

วัตถุประสงค์

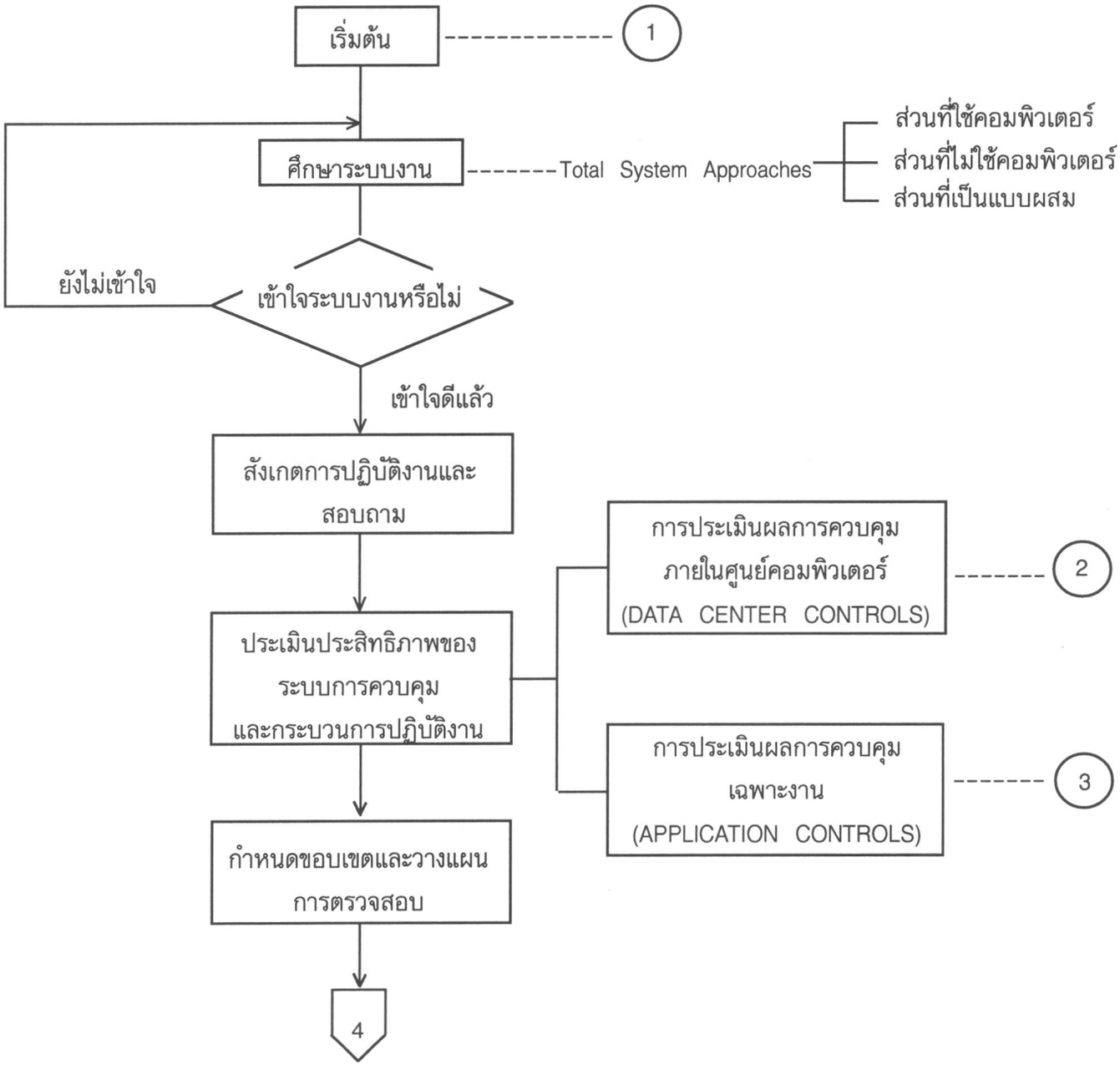
- เพื่อพิจารณาว่าข้อผิดพลาดหรือสิ่งผิดปกติที่อาจเกิดขึ้นในแต่ละระบบงานเป็นข้อผิดพลาดชนิดใด
- วิธีการควบคุมที่ใช้ สามารถป้องกันและค้นหาข้อผิดพลาดได้เพียงใด
- พิจารณาว่าได้จัดให้มีการควบคุมภายในที่สำคัญไว้หรือไม่ และมีการปฏิบัติตามระเบียบการควบคุมภายในดังกล่าวเป็นที่น่าพอใจเพียงใด
- ประเมินจุดอ่อนตลอดจนถึงการทุจริต (หากมี) และผลกระทบที่มีต่อลักษณะ เวลา และขอบเขตการตรวจสอบ

วิธีการ

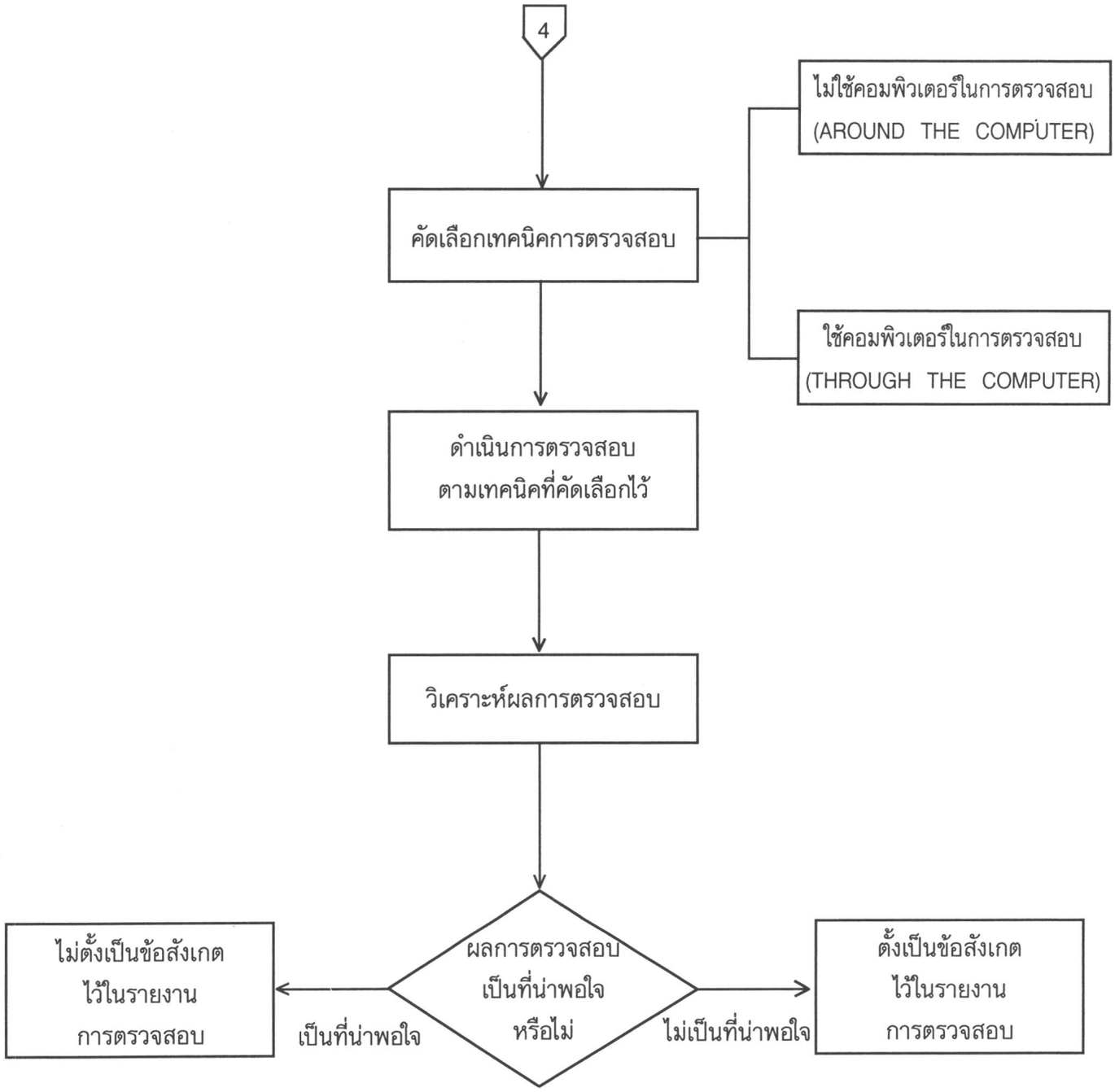
ขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบ

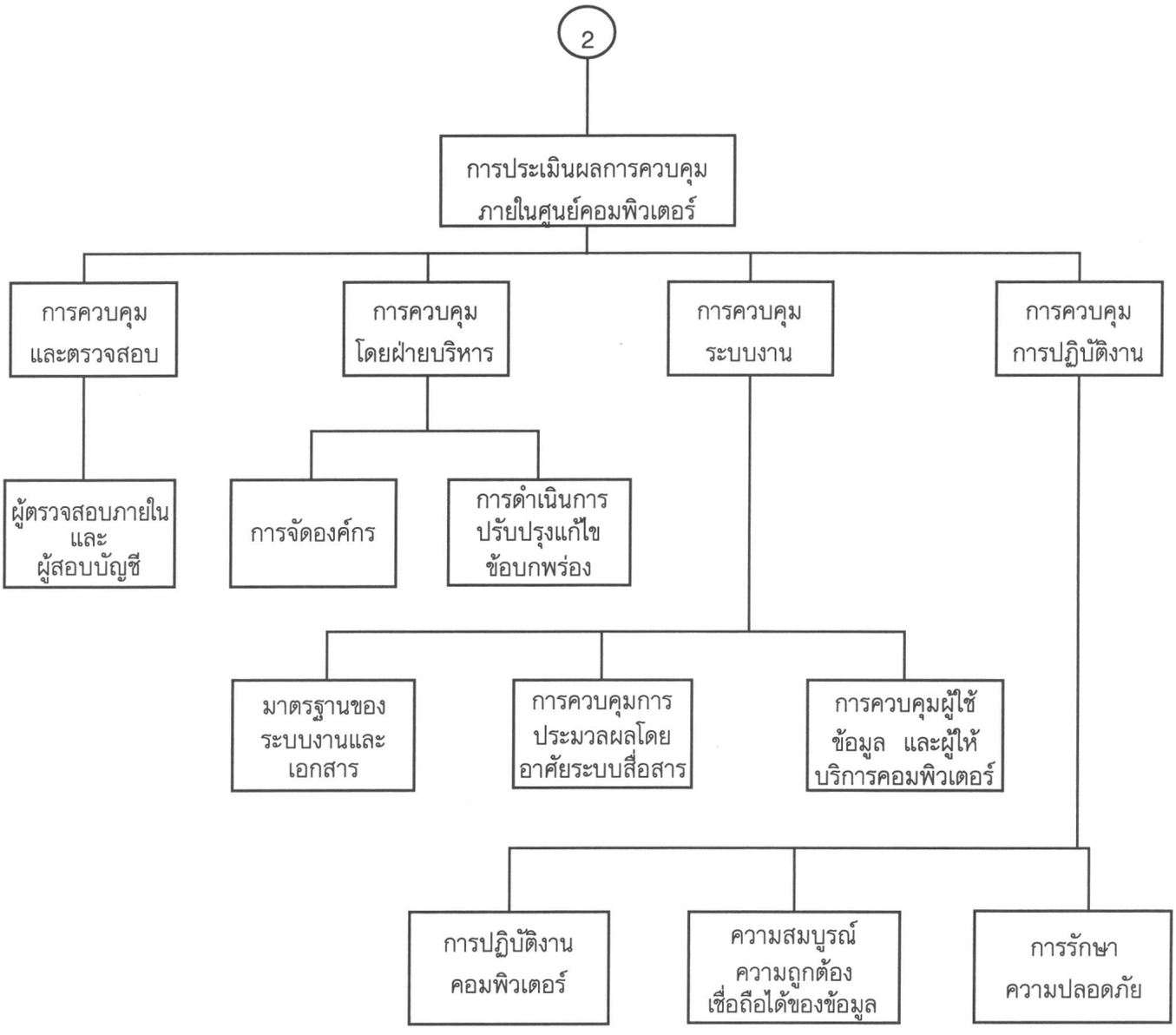


24. อีกรูปแบบหนึ่งของการกำหนดและวางแผนการตรวจสอบโดยทั่วไป ซึ่งอาจนำมาประยุกต์ใช้กับการตรวจสอบการทุจริตในองค์กรที่ใช้คอมพิวเตอร์ได้



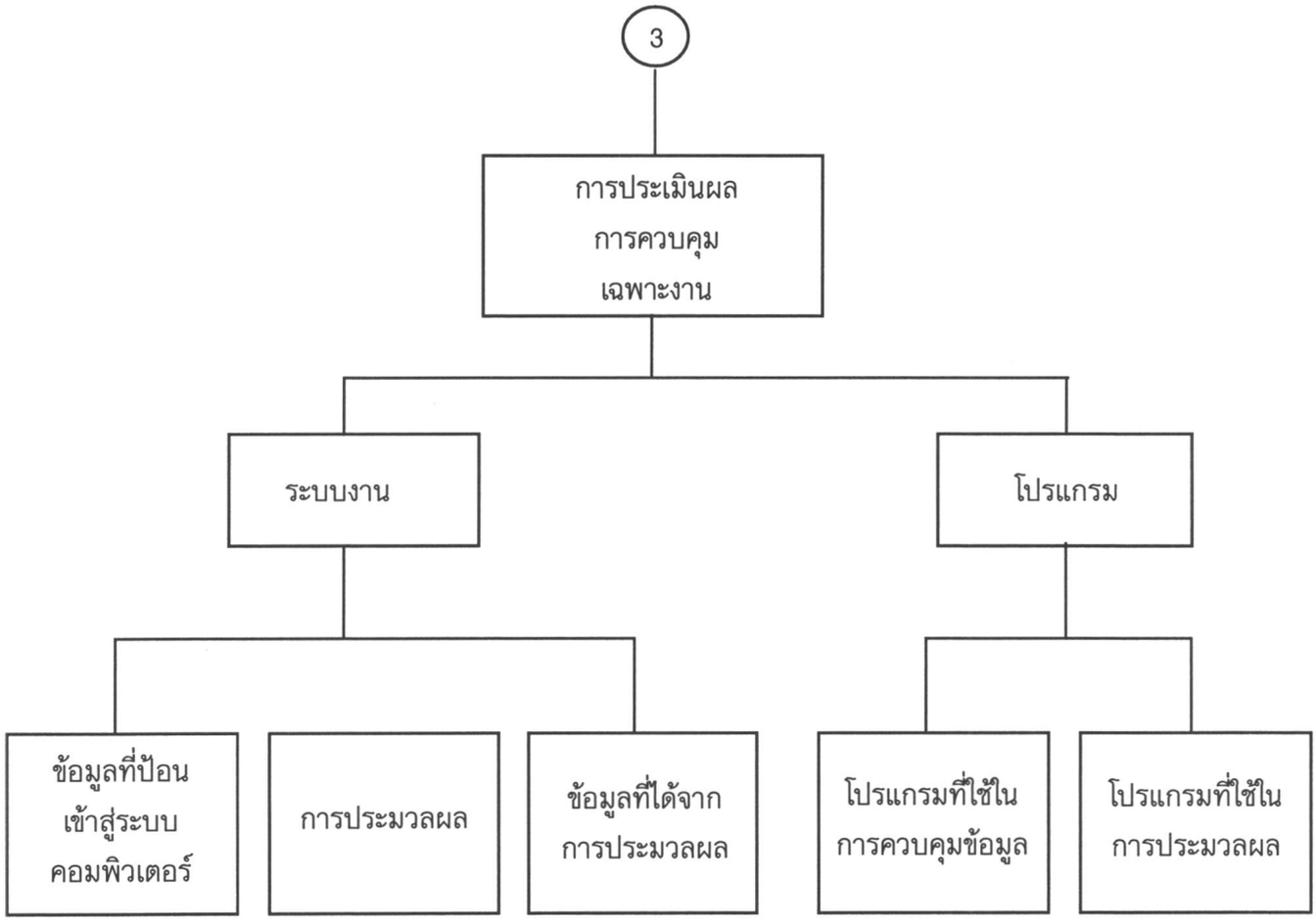
หมายเหตุ : ทั้งนี้ขึ้นอยู่กับเป้าหมายและขอบเขตในการตรวจสอบเป็นสิ่งสำคัญ รายละเอียดมีปรากฏในเล่ม 1 และเล่ม 2 แล้ว สำหรับการตรวจสอบการทุจริตส่วนใหญ่จะเน้นการตรวจสอบด้าน Application อย่างไรก็ดีหากเป็นการตรวจสอบในภาพรวมไม่เฉพาะเจาะจง การตรวจสอบด้าน Data Center เพื่อค้นหาจุดอ่อนด้านบริหารที่อาจกระทบต่อการปฏิบัติงานด้าน Application ก็กระทบได้


4
คัดเลือกเทคนิคการตรวจสอบ
ไม่ใช้คอมพิวเตอร์ในการตรวจสอบ (AROUND THE COMPUTER)
ใช้คอมพิวเตอร์ในการตรวจสอบ (THROUGH THE COMPUTER)
ดำเนินการตรวจสอบ ตามเทคนิคที่คัดเลือกไว้
วิเคราะห์ผลการตรวจสอบ
ผลการตรวจสอบ เป็นที่น่าพอใจ หรือไม่
เป็นที่น่าพอใจ
ไม่ตั้งเป็นข้อสังเกต ไว้ในรายงาน การตรวจสอบ
ไม่เป็นที่น่าพอใจ
ตั้งเป็นข้อสังเกต ไว้ในรายงาน การตรวจสอบ



หมายเหตุ : 1. แผนภาพนี้ใช้ในการทบทวนการตรวจสอบการบริหารงานทั่วไป หรือ เป็นการตรวจสอบด้าน Data Center หรือ General Controls ขององค์กร

2. ก่อนการตรวจสอบหรือประเมินผลการควบคุมภายในเฉพาะงาน (Application Controls) ตามแผนภาพหน้าถัดไปนั้น หากผู้ตรวจสอบได้ทำการประเมินผลการตรวจสอบภายในศูนย์คอมพิวเตอร์ (Data Center) เพื่อพิจารณาว่ามีจุดอ่อนที่จะมีผลกระทบต่อการควบคุมภายในเฉพาะงาน (Application Controls) อย่างไรบ้าง ก็จะได้ภาพที่ชัดเจนยิ่งขึ้น ไม่ว่าจะเป็นการตรวจสอบตามปกติหรือการตรวจสอบการทุจริต หรือการค้นหาจุดอ่อนเพื่อป้องกันการทุจริตหรือเพื่อการกำหนดกฎเกณฑ์การ ควบคุมที่เหมาะสม



หมายเหตุ : 1. การตรวจสอบหรือการประเมินผลการควบคุมเฉพาะงาน (Application Controls) นี้ จะมีความสัมพันธ์กับการตรวจสอบองค์กรหรือ Data Center หรือ General Controls ด้วยเสมอ เพราะจุดอ่อนที่พบใน General controls จะกระทบต่อการควบคุมเฉพาะงาน (Application Controls) ไม่มากก็น้อย

2. การตรวจสอบการทุจริตส่วนใหญ่จะเน้นการตรวจสอบที่ "งาน" (Application) อย่างไรก็ดี ผู้ตรวจต้องไม่ลืมข้อมูลตามที่กล่าวข้อ 1 ด้วย

25. การป้องกันการทุจริต

25.1 ความเอาใจใส่และความเข้าใจระบบงาน การประมวลข้อมูลคอมพิวเตอร์ของผู้บริหารและผู้ที่เกี่ยวข้อง

25.2 การเข้าใจระบบงานขององค์กรอย่างแท้จริงของผู้วิเคราะห์และผู้พัฒนาระบบงาน โดยเฉพาะอย่างยิ่งการใส่หรือจัดระบบการควบคุมและตรวจสอบไว้ในระบบงานอย่างอัตโนมัติ (Automatic) และด้วยมือ (Manual) ให้เหมาะสมกับขั้นตอนการปฏิบัติงาน โดยมีหลักฐานที่สามารถติดตามและตรวจสอบได้ ทั้งนี้ โดยพิจารณาควบคู่กันไปกับสาเหตุการทุจริต โอกาสทุจริต และความล้มเหลวของระบบงานด้านต่าง ๆ อันเกิดจากการทุจริตและไม่ใช่การทุจริต ทั้งนี้ ให้มีลักษณะการควบคุมในแบบ Preventive, detective และ Corrective ตามความเหมาะสม

25.3 การควบคุมและการตรวจสอบที่มีประสิทธิภาพ หากองค์กรไม่สามารถป้องกันความผิดพลาดหรือการทุจริตได้ องค์กรก็ควรทราบสิ่งผิดปกติโดยเร็วที่สุด

25.4 ต้องการผู้ใช้ข้อมูลที่เอาใจใส่ในข้อมูลที่เกี่ยวข้องสม่ำเสมอ

26. สิ่งที่ควรดำเนินการ

26.1 ผู้ตรวจสอบภายในด้านคอมพิวเตอร์ควรจะได้มีบทบาทและพิจารณาตนเองให้มากยิ่งขึ้นในด้านการป้องกันการทุจริตขององค์กรโดยยึดคติ "การป้องกันดีกว่าการแก้ไข" และการป้องกันที่ดีที่สุดก็คือการสร้างระบบการป้องกันขึ้นอย่างอัตโนมัติไว้ในระบบงานขององค์กร

26.2 ผู้บริหารควรจะได้ให้ความสนใจในด้านการตรวจสอบงานและข้อสังเกตของผู้ตรวจสอบงานทางด้านคอมพิวเตอร์มากขึ้น

26.3 องค์กรไม่ควรพึ่งพาบุคลากรภายนอก ผู้ให้บริการทางด้านคอมพิวเตอร์มากจนเกินไป

26.4 องค์กรพึงตระหนักว่าบุคคลภายในองค์กรที่มีความเข้าใจในระบบงานภายในองค์กรดีจะสามารถช่วยการพัฒนางานองค์กรได้มาก หากเขาเหล่านั้นสามารถเข้าใจระบบงานทางด้านคอมพิวเตอร์และสามารถประยุกต์การปฏิบัติงานให้เข้ากับระบบงานคอมพิวเตอร์ได้

26.5 การแลกเปลี่ยนทักษะระหว่างหน่วยงานที่ใช้คอมพิวเตอร์เป็นสิ่งจำเป็น เช่น การจัดตั้งชมรมผู้สอบบัญชีภายในด้านคอมพิวเตอร์ของธนาคารพาณิชย์ หรือระหว่างองค์กรต่าง ๆ ที่ใช้คอมพิวเตอร์ก็จะช่วยลดปัญหาทางด้านเทคนิคได้ดี

26.6 องค์กรที่ใช้เครื่องคอมพิวเตอร์ขนาดเล็ก ควรจะระมัดระวังเป็นพิเศษโดยเฉพาะในด้าน Computer Security และการเข้าถึงข้อมูลทุกประเภท

27. สรุป

27.1 คอมพิวเตอร์สามารถประมวลข้อผิดพลาดได้ทั้งโดยเจตนาและไม่เจตนาและสิ่งที่จะตามมาได้ก็คือความล้มเหลวของระบบงานและหรือการทุจริต

27.2 การป้องกันเป็นภาพที่มองเห็นและพิจารณากันได้ยาก แต่ก็คุ้มค่าที่จะศึกษาและหาทางป้องกันก่อนที่ปัญหาจะเกิด เพราะหากโชคไม่ดีเอามาก ๆ อาจหมายถึงความหายนะขององค์กร เมื่อประสบกับสิ่งที่คาดไม่ถึงของผลกระทบจากเทคโนโลยีสมัยใหม่

27.3 การดำเนินงานด้านคอมพิวเตอร์มีความเสี่ยงและความเสียหายที่แตกต่างรวดเร็วและกว้างขวางอย่างเปรียบกันไม่ได้กับระบบที่ประมวลงานด้วยมือหรือเครื่องจักรตามปกติ บุคลากรที่เกี่ยวข้องที่ใช้คอมพิวเตอร์จึงมีความ “พร้อม” และตระหนักถึงภัยและปัญหา

27.4 สถาบันการเงินหรือบริษัทอาจใช้คอมพิวเตอร์ตกแต่งฐานะทางการเงินได้และยากต่อการตรวจสอบมากขึ้น

27.5 การอภิปรายหรือการสัมมนาเรื่องที่เกี่ยวกับการทุจริตหรือวิธีการทุจริตด้านคอมพิวเตอร์ เป็นดาบสองคมที่มีทั้งประโยชน์และมีทั้งโทษต่อองค์กร จึงขึ้นกับว่าผู้ที่ได้รับความรู้นำสิ่งที่ได้รับไปใช้ประโยชน์ทางด้านใดและใครจะเป็นผู้ “ลงมือ” ก่อนกัน

27.6 หน่วยงานของรัฐที่ทำหน้าที่ควบคุมดูแลสถาบันทางการเงินที่เกี่ยวข้องกับประชาชนทุกประเภท เช่น ธนาคารพาณิชย์ บริษัทเงินทุนต่าง ๆ ตลอดจนถึงบริษัทประกันภัย ควรมีบทบาทด้านกำหนดมาตรฐานขั้นต่ำ (Minimum Standard of Information) และมาตรฐานเกี่ยวกับความปลอดภัยทางด้านคอมพิวเตอร์ (Computer Security) ตลอดจนรายงานการตรวจสอบทางด้านที่เกี่ยวข้องให้กับองค์กรเหล่านี้ เพื่อให้เป็นที่แน่ใจว่าการประมวลข้อมูลด้วยคอมพิวเตอร์ขององค์กรเหล่านั้นมีความน่าเชื่อถือได้และสามารถติดตามการตรวจสอบฐานะและการดำเนินงานที่แท้จริงได้

โดยมีหลักฐานที่พอเพียงและไม่สร้างความเดือดร้อนให้กับประชาชนและหน่วยงานที่เกี่ยวข้องทั้งในปัจจุบันและอนาคต

27.7 การวิเคราะห์ความเสี่ยงที่มีประสิทธิภาพของผู้ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งหากองค์กรใดโชคดีมีผู้บริหารที่รู้จักใช้การวิเคราะห์ความเสี่ยงให้เป็นประโยชน์ก็จะช่วยองค์กรได้มาก เพราะความเสี่ยงจะทำให้ผู้ตรวจสอบมองเห็นจุดที่ควรตรวจสอบ ซึ่งในแง่ความเสี่ยงก็คือจุดที่ก่อให้เกิดความเสียหายได้นั่นเอง เป้าหมายของการตรวจสอบที่สำคัญ คือ การค้นหาความผิดพลาดหรือความเสียหายหรือผลกระทบต่อฐานะการเงินและการดำเนินงานอย่างต่อเนื่องขององค์กรให้ได้เร็วที่สุดและเสียค่าใช้จ่ายน้อยที่สุด

บทที่ 18

ตัวอย่างการตรวจสอบกรณีทุจริต โดยใช้คอมพิวเตอร์เป็นเครื่องมือและความร่วมมือระหว่าง Computer Auditors (IS Auditors) กับ Financial Auditors

(ประสบการณ์ของต่างประเทศ)

ตัวอย่างการตรวจสอบกรณีทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือ และความร่วมมือระหว่าง IS Auditors กับ Financial Auditors (ประสบการณ์ของต่างประเทศ) [1]

บทคัดย่อของการทุจริตในระบบ Refund System และการตรวจสอบโดยย่อ

The Virginia Supplemented Retirement System (VSRS) ทำหน้าที่เป็นกองทุนเลี้ยงชีพ พนักงานลูกจ้างของรัฐประมาณ 700 แห่ง ใน The Commonwealth of Virginia มีบัญชีเงินฝากของพนักงานทั้งที่ทำงานอยู่และลาออกแล้วกว่า 235,000 บัญชี มีสินทรัพย์รวม 1,300 ล้านเหรียญ ซึ่งส่วนใหญ่เป็นหุ้นและพันธบัตร มีกรรมการ 7 คน เริ่มใช้คอมพิวเตอร์เมื่อ 1 กรกฎาคม 2515 โดยที่คณะกรรมการไม่มีใครมีความรู้เรื่องคอมพิวเตอร์เลย และ Department of Automated Data Processing (ADP) ซึ่งเป็นผู้วางแผนพัฒนาระบบของรัฐ ได้ตรวจพบว่ามีข้อบกพร่องที่สำคัญ ๆ อีก 26 แห่ง แต่เนื่องจากปริมาณงานมาก VSRS จึงตัดสินใจใช้คอมพิวเตอร์โดยการจ้างพนักงานของ ADP 3 คน ที่รับผิดชอบพัฒนาระบบให้เป็นผู้อำนวยการ ผู้จัดการฝ่าย Operator และผู้จัดการฝ่ายประมวลผล เพื่อให้แก้ไขข้อบกพร่องต่าง ๆ ดังกล่าว

VSRS ไม่มีผู้ตรวจสอบภายใน มีแต่ Auditor of Public Accounts (APA) ซึ่งเป็นหน่วยตรวจสอบฐานะการเงินองค์การของรัฐทำหน้าที่ตรวจสอบ APA ไม่สามารถตรวจสอบได้ทุกปี เพราะมีเจ้าหน้าที่น้อย หลังสุดตรวจสอบถึงปีการเงินสิ้นสุด 30 มิถุนายน 2525

มีนาคม 2520 APA เข้าตรวจและพบการทุจริตโดยใช้คอมพิวเตอร์กว่า 1 แสนเหรียญ มีผู้ทุจริต 16 คน เป็นพนักงาน VSRS 3 คน บุคคลภายนอก 13 คน ถูกศาลพิพากษาจำคุกรวมกัน 50 ปี โดยหัวหน้าแผนก Refund 8 ปี เสมียนแผนก Refund 2 คน ๆ ละ 6 ปี รายละเอียดการทุจริตตามที่ตรวจพบมีดังนี้

การตรวจสอบเบื้องต้น

การตรวจสอบในปี 2520 เป็นการตรวจด้าน Financial ย้อนหลัง 5 ปี และไม่มีการตรวจสอบด้าน EDP หรือใช้ Audit เลยตลอด 5 ปีที่ผ่านมา ผู้ตรวจสอบจึงใช้วิธีประชุมกับฝ่ายบริหาร VSRS ทำให้ทราบว่าระบบงานคอมพิวเตอร์ที่สำคัญ ๆ มีดังนี้

---

[1] จากวารสารชื่อ EDPACS ซึ่งเสนอข่าวสารเกี่ยวกับการตรวจสอบ การควบคุม และรักษาความปลอดภัยคอมพิวเตอร์ ฉบับเดือนสิงหาคม-กันยายน 2524 เขียนโดย Steven F. Blanding ผู้จัดการแผนกตรวจสอบคอมพิวเตอร์ของ Tandy Corporation ในเมือง Fort Worth มลรัฐ Texas ก่อนหน้านี้เขาเป็นผู้ควบคุมการตรวจสอบด้านคอมพิวเตอร์ของ The Commonwealth of Virginia อยู่ 5 ปี

1. Member Contribution Account System (MCA) ใช้บันทึกรายการนำส่งเงินของสมาชิก ซึ่งแต่ละปีจะมีมากกว่า 3 ล้านรายการ เป็นเงินมากกว่า 100 ล้านเหรียญ การส่งเงินของสมาชิก VSRS แต่ละรายทำโดยผ่านนายจ้าง นายจ้างจะหักเงินแล้วนำส่งให้ VSRS พร้อมรายละเอียด โดยแจ้งรายชื่อสมาชิกเฉพาะรายที่มีการเปลี่ยนแปลง รายงานสำคัญที่ได้จากระบบงานนี้ คือ "รายชื่อสมาชิกที่ไม่มีใน MCA Master File" ซึ่งมักเกิดจากนายจ้างไม่กรอกแบบฟอร์ม #1 (VSRS Memberships Form) เพื่อแจ้งรายละเอียดของพนักงานเข้าใหม่ ปกติเมื่อได้รับแบบฟอร์มแล้วจะเพิ่มรายชื่อใน Master File แล้วนำเรื่องเข้าแฟ้มเก็บไว้ในห้องเก็บของ ซึ่งไม่ได้ควบคุมการเข้าออก

2. Refund System ใช้ประมวลผลรายการจ่ายเงินคืนให้แก่สมาชิกรายที่ออกจากงาน และแสดงความจำนงขอถอนเงินที่ฝากไว้คืน แต่ละปีมีประมาณ 20,000 รายเป็นเงินประมาณ 18 ล้านเหรียญ โดยสมาชิกต้องกรอกแบบฟอร์ม # 3 ระบุหมายเลขประกันสังคม ชื่อนายจ้าง ฯลฯ แล้วส่งให้แผนกเงินเดือนของตน เพื่อเพิ่มรายละเอียดว่าหักเงินเดือนครั้งสุดท้ายวันที่เท่าไร พร้อมรหัสนายจ้าง จำนวนเงินนำส่งที่ยังไม่ได้รายงานให้ VSRS ทราบแล้วลงนาม ส่งไปให้ VSRS แผนก Refund Section

เมื่อ Refund Section ได้รับแบบฟอร์ม #3 จะตรวจสอบแล้วส่งให้ฝ่ายประมวลผลบันทึกใน Refund Inventory Tape ซึ่งแสดงรายการขอเงินคืนที่คงค้างอยู่ทั้งหมด เสร็จแล้วจะนำแบบฟอร์ม #1 ที่เก็บอยู่ในห้องเก็บของมาเข้าคู่กับแบบฟอร์ม #3

เมื่อจ่ายเงินคืนแล้วจะบันทึกจำนวนเงินที่ถอนคืนไปใน Control Book ซึ่งเป็นสมุดเล่มเดียวกันกับที่บันทึกจำนวนเงินที่รับจากสมาชิกทั้งสิ้น และใช้ Control Sheet 1 แผ่น ต่อ 1 เดือน สำหรับนายจ้างแต่ละราย เพื่อบันทึกความเคลื่อนไหวของเงินรับเข้าและจ่ายคืนให้แก่ลูกจ้างของนายจ้างแต่ละคน ฉะนั้นยอดตาม Control Book จะต้องตรงกับยอดคงเหลือของบัญชีนายจ้างทุกรายรวมกัน และต้องตรงกับยอดรวมรายตัวลูกจ้างทุกรายใน MCA Master File แต่นายจ้างบางรายส่งแต่เงินไม่ยอมส่งรายชื่อมาให้ จึงทำให้ข้อมูลใน MCA Master File ไม่ตรงกับยอดตาม Control Book และเมื่อสิ้นปีการเงินจะทำ MCA Year End History Tape จาก MCA Master File เก็บไว้ 1 ชุด

จุดอ่อนที่พบเบื้องต้น

จากการตรวจสอบ MCA และ Refund เบื้องต้นเสร็จสิ้นในเดือนกรกฎาคม 2520 ผู้ตรวจสอบได้ขอให้ฝ่ายบริหารของ VSRS ยกเลิกนโยบายการให้ถอนเงินคืน โดยที่นายจ้างยังไม่ได้แจ้งรายชื่อลูกจ้างที่ถูกหักเงินมา เนื่องจากมีจุดอ่อนอย่างร้ายแรง แต่ฝ่ายบริหาร VSRS ไม่ทำตาม ผู้ตรวจสอบ APA จึงขออนุมัติจากผู้อำนวยการ APA เพื่อทดลองทำการทุจริต



ขั้นตอนการทดลองทุจริตและผลการทดลอง

1. เขียนโปรแกรมสร้างบัญชีปลอมใน MCA Master File
2. เขียนโปรแกรมโอนเงินจากบัญชีอื่นเข้าบัญชีปลอม
3. ปลอมแบบฟอร์ม #1 เข้าไปเก็บไว้ในห้องเก็บของเวลาพักเที่ยง
4. ปลอมแบบฟอร์ม #3 ให้สอดคล้องกับแบบฟอร์ม #1 และบัญชีที่ปลอมส่งให้ VSRS ทางไปรษณีย์ 6 สัปดาห์ให้หลังมีเช็ค 3 ฉบับ มูลค่ากว่า 3,000 เหรียญ ส่งมาให้ผู้ตรวจสอบตามที่อยู่ที่ระบุไว้ตอนล่างของแบบฟอร์ม #3 ซึ่งการกระทำนี้แสดงให้เห็นว่าพนักงานของ VSRS ก็สามารถทำทุจริตได้ เมื่อฝ่ายบริหาร VSRS ทราบการทดลองทุจริตก็แสดงอาการไม่พอใจ

จากผลการตรวจสอบ ผู้ตรวจสอบได้สั่งการให้

1. ยุติการคืนเงินรายที่นายจ้างยังไม่ได้ส่งรายงานการหักเงินมาให้
2. จัดทำเอกสารคำอธิบายระบบงานและคู่มือปฏิบัติงาน
3. กระทบยอดข้อมูลในคอมพิวเตอร์กับสมุดบัญชีที่สำคัญ ๆ

การค้นพบทุจริต

23 กุมภาพันธ์ 2521 ผู้ตรวจสอบได้เปรียบเทียบยอดของ VSRS ที่กระทบยอดเสร็จแล้วกับสมุดบัญชีของสำนักงานบัญชีกลางของรัฐ ตามมาตรฐานที่ APA ถือปฏิบัติอยู่ พบว่าจำนวนเงินที่บันทึกในสมุดเงินสดจ่ายของ VSRS ไม่ตรงกับที่สำนักงานกลางบัญชี จึงขอต้นฉบับ Refund Voucher จากสำนักงานกลางบัญชี เปรียบเทียบกับสำเนาที่เก็บไว้ที่ VSRS พบว่า Refund Voucher ต้นฉบับมีการแก้ไขและปรับยอดรวมในใบปะหน้าให้สอดคล้องกันโดยไม่แก้ไขสำเนา และจากการเปรียบเทียบข้อมูลที่ได้จากสำนักงานสรรพากรของรัฐเกี่ยวกับชื่อผู้รับเงิน หมายเลขประกันสังคม ปรากฏว่าเป็นรายการถอนเงินปลอม รายการปลอมเหล่านี้พิมพ์ด้วยเครื่องคอมพิวเตอร์ จึงได้รายงานการทุจริตให้สำนักงานอัยการรัฐ ตำรวจรัฐ และผู้ว่าการรัฐ Virginia ทราบ

การป้องกันรักษาข้อมูลเกี่ยวกับการทุจริต

คัดลอกข้อมูลจากแฟ้มข้อมูลต่าง ๆ และโปรแกรมที่เกี่ยวข้องลงไว้ในเทปแม่เหล็ก

การประสานงานตรวจสอบ

จากการตรวจสอบ Refund Voucher ปี 2520 และ 2521 ได้หลักฐานเพียงพอที่จะจับกุมอดีตพนักงาน Refund Section 2 คน ที่ลาออกไปแล้ว แต่ปรากฏว่าพนักงานบุคคลทั้งสองลาออกแล้ว การทุจริตยังคงดำเนินต่อไป แสดงว่าพนักงานปัจจุบันมีส่วนในการทุจริต จึงให้ VSRS ปิดทำการตั้งแต่วันจันทร์ที่ 27 กุมภาพันธ์ 2521 รวม

2 วัน พบว่าหัวหน้าแผนก Refund Section ทำการทุจริต อย่างไรก็ดีการตรวจสอบที่ผ่านมามีสภาพสับสน ทำงานซ้ำซาก จึงได้ประชุมคณะผู้ตรวจสอบแบ่งงานกันในวันที่ 28 กุมภาพันธ์ 2521 ดังนี้

1. ผู้ตรวจสอบด้านคอมพิวเตอร์รับผิดชอบเรื่องศึกษาระบบงานวางแผนการตรวจสอบ แบ่งแยกงานตรวจ EDP และแนะนำแนวทางการตรวจแก่ Financial Auditors, จัดทำรายงานทางคอมพิวเตอร์เกี่ยวกับ MCA และ Refund ให้ Financial Auditors
2. ผู้ตรวจสอบด้านการเงิน (Financial Auditors) รับผิดชอบงานตรวจเอกสารเบื้องต้น ข้อมูลทางบัญชีและหลักฐานการทุจริตตามรายงานคอมพิวเตอร์
3. ตำรวจสอบสวนของรัฐรับผิดชอบงานสอบสวนที่เกิดเหตุ และออกหมายจับตามเอกสารที่ได้จากผู้ตรวจสอบ

นอกจากนี้ยังมีอัยการรัฐคอยให้คำปรึกษาแก่ตำรวจ คณะกรรมการของสภานิติบัญญัติแห่งรัฐตรวจสอบด้านบริหารงาน VSRS อย่างกว้าง ๆ และสำนักงานบัญชีแห่งหนึ่งจัดวางการควบคุมและวิธีปฏิบัติงานใหม่ให้ VSRS

แบบการตรวจสอบทุจริต

เพื่อให้การตรวจสอบมีประสิทธิภาพยิ่งขึ้น ผู้ตรวจสอบคอมพิวเตอร์ได้ศึกษาระบบและกำหนดรูปแบบทุจริตที่อาจจะเกิดขึ้นได้ ทำให้สามารถแยกลักษณะรายการที่เหมือนกับรายการทุจริตออกมาได้ การตรวจสอบทุจริตจึงแบ่งเป็น 2 แบบ ดังนี้

1. Dynamic เป็นแบบที่ผู้ตรวจสอบคอมพิวเตอร์ดึงข้อมูลที่น่าสงสัย เนื่องจากมีลักษณะเหมือนกับรายการทุจริตที่เกิดค้นพบแล้ว
2. Descriptive เป็นการกำหนดรูปแบบการทุจริตที่อาจจะเกิดขึ้นได้ โดยการศึกษาการควบคุมภายในอย่างกว้าง ๆ และจัดทำเป็นผังการควบคุมภายในเพื่อประเมินข้อดีข้อเสีย แล้วกำหนดรูปแบบที่อาจเกิดการทุจริตได้

รูปแบบการทุจริตที่ตรวจพบ

การทุจริตที่ตรวจพบมี 4 แบบ คือ

1. การแก้ไขสลิปถอนเงิน
2. การสร้างบัญชีสมาชิกปลอม
3. การถอนเงินจากบัญชีที่ไม่เคลื่อนไหว
4. การสร้างรายการถอนเงินปลอม

การแก้ไขสลิปถอนเงิน หลังจากที่ผู้อำนวยการ VSRS ได้ลงลายมือชื่อในสลิปแล้วอดีตพนักงาน Refund Section 2 คน ได้แก้ไขจำนวนเงินให้เพิ่มขึ้น เช่น 1,000 เหรียญ แก้ไขเพิ่มเป็น 7,000 เหรียญ แล้วส่งไปยัง

สำนักงานคลังของรัฐ เพื่อจ่ายเงินให้แก่สมาชิกที่ร่วมทุจริต วิธีนี้ตรวจพบได้โดยการทำสลิปที่สำนักงานคลังของรัฐเปรียบเทียบกับสำเนาสลิปที่ VSRS

การสร้างบัญชีสมาชิกปลอม จากการตรวจสอบผู้ตรวจสอบเชื่อว่าต้องมีการสร้างรายการปลอม ซึ่งผู้จัดการฝ่ายประมวลข้อมูลของ VSRS ได้ให้ความร่วมมือหาบัญชีปลอมให้ MCA Master File และพบว่ามีลักษณะพิเศษ เช่น ช่องจำนวนเงินมียอดเป็นศูนย์ ไม่มีแบบฟอร์ม #1 เป็นต้น ผู้จัดการฝ่ายประมวลข้อมูลชี้แจงว่า ลูกจ้างที่ทำงานกับนายจ้างครบ 1 ปี มีสิทธิกรอกแบบฟอร์ม #3 ได้โดยที่นายจ้างไม่เคยส่งแบบฟอร์ม #1 เลย ปรากฏว่าเสมียนแผนก Refund ใช้วิธีการนี้ปลอมบัญชีโดยใช้ชื่อตนเอง เพื่อน และญาติ ว่าเป็นลูกจ้างของนายจ้างรายหนึ่ง ซึ่งขาดส่งรายชื่อลูกจ้าง 17 ถึง 18 เดือน หลังจากเพิ่มชื่อแล้วก็จะส่งแบบฟอร์ม #3 ให้แผนก Refund แล้วขอรับเช็คตามที่อยู่ที่ระบุ (ผู้ตรวจสอบ APA สงสัยว่าผู้จัดการฝ่ายประมวลผลข้อมูลจะมีส่วนในการทุจริต แต่ไม่มีหลักฐาน)

การถอนเงินจากบัญชีที่ไม่เคลื่อนไหว ผู้ตรวจสอบพบการทุจริตวิธีนี้เนื่องจากชื่อผู้รับเงินรายหนึ่งเป็นชื่อเดียวกันกับบัญชีปลอมที่พบในการทุจริตแบบอื่น ๆ เมื่อตรวจสอบรายละเอียดจึงพบว่าเป็นการถอนเงินจากบัญชีที่ไม่เคลื่อนไหว ซึ่งเป็นบัญชีที่มีอยู่จริง แต่ในสลิปถอนเงินลงชื่ออื่น การทุจริตวิธีนี้เกิดจากเสมียนแผนก Refund เป็นผู้เจาะบัตรป้อนข้อมูลจากแบบฟอร์ม #3 หรือรายงานบัญชีที่ไม่เคลื่อนไหว เมื่อส่งข้อมูลที่เจาะเข้าคอมพิวเตอร์ โปรแกรมจะสั่งให้พิมพ์รายงานตามข้อมูลที่ป้อนโดยไม่เช็คสอบกับ MCA Master File ดังนั้นรายงานที่ได้จึงไม่ใช่ข้อมูลที่ถูกต้องทุกรายการ แต่เนื่องจากบัญชีที่ไม่เคลื่อนไหวมีมากถึง 67,000 บัญชี ผู้ตรวจสอบคอมพิวเตอร์จึงใช้โปรแกรมเปรียบเทียบรายการถอนเงินใน History Tape กับ MCA Master File ดูว่าหมายเลขประกันสังคมตรงกัน แต่ชื่อต่างกันออกมา ได้ 3,000 บัญชี เพื่อส่งให้ผู้ตรวจสอบด้านการเงิน ทั้งนี้เพราะหมายเลขประกันสังคมใน MCA Master File ไม่สามารถเปลี่ยนแปลงแก้ไขอย่างไรก็ตามรายการถอนเงินที่มีหมายเลขประกันสังคม และชื่อบัญชีตรงกันก็อาจมีการส่งเช็คไปให้คนในกลุ่มผู้ทุจริตเอง ฉะนั้นจึงต้องสอบถามไปยังเจ้าของบัญชีว่าได้รับเงินที่ถอนไปหรือไม่ การทุจริตวิธีนี้เกิดขึ้นระหว่างกันยายน 2520 ถึงมกราคม 2521 ซึ่งเป็นระยะที่ผู้ตรวจสอบได้เข้าทำการตรวจสอบ เสมียนและหัวหน้าแผนก Refund เป็นผู้ทุจริต โดยใช้ชื่อตนเอง ญาติ และเพื่อน ๆ

การสร้างรายการถอนเงินปลอม หัวหน้าแผนก Refund เป็นผู้ทุจริต โดยทำสลิปถอนเงินไม่ผ่านคอมพิว-เตอร์ ประทับตรา "ด่วนมาก" ให้ผู้อำนวยการ VSRS อนุมัติส่งให้สำนักงานคลังของรัฐ ผู้ตรวจสอบด้านการเงินค้นพบการทุจริตโดยการเลือกสลิปถอนเงินที่ทำด้วยมือมาตรวจสอบ การทุจริตเกิดขึ้นระหว่างที่ผู้ตรวจสอบเข้าทำการตรวจสอบกล่าวคือ ระหว่างเดือนพฤษภาคมถึงธันวาคม 2520



สรุป

อุปสรรคที่สำคัญในการตรวจสอบคอมพิวเตอร์ของ VSRS มีอุปสรรคที่สำคัญ 2 ประการ คือ

1. ฝ่ายบริหารของ VSRS ไม่ให้ความร่วมมือ เพราะรู้สึกว่าถูกผู้ตรวจสอบแทรกแซงระบบคอมพิวเตอร์
2. คู่มือประกอบระบบงาน (System Document) ไม่ดีพอ ผู้ตรวจสอบต้องสอบถามจากพนักงานผู้ปฏิบัติ ทำให้พนักงานทราบว่าผู้ตรวจสอบยังไม่ทราบเรื่องใด และพยายามไม่เปิดเผยสิ่งที่นอกเหนือคำถาม เป็นเหตุให้ผู้ตรวจสอบไม่สามารถเข้าใจระบบงานอย่างลึกซึ้ง และมองข้ามจุดอ่อนบางอย่างไป

การประสานงาน

การตรวจสอบการทุจริตทั้ง 4 แบบ เป็นงานการตรวจสอบด้านการเงิน แต่เนื่องจากการ Process งานด้านบัญชีทำโดยคอมพิวเตอร์ ฉะนั้น ความร่วมมือและการชี้แนะของผู้ตรวจสอบด้านคอมพิวเตอร์ จึงมีความสำคัญยิ่งต่อความสำเร็จในการปฏิบัติงานครั้งนี้

จุดอ่อนของระบบงานที่ก่อให้เกิดการทุจริต

1. ไม่มีการควบคุมการเข้าออกห้องเก็บแบบฟอร์ม #1 และแบบฟอร์ม #3 เป็นเหตุให้เสมียนแผนก Refund ปลอมแปลงเอกสารดังกล่าวเพื่อทำการทุจริต
2. การยินยอมให้ถอนเงินก่อนที่นายจ้างจะส่งรายชื่อลูกจ้างที่ถูกหักเงินมาให้ เสมียนแผนก Refund จึงแก้ไขจำนวนเงินในสลิป โดยไม่ต้องพะวงว่ายอดในบัญชีจะมียอดคงเหลือพอหรือไม่
3. การให้เสมียนแผนก Refund เจาะบัตรข้อมูลถอนเงินในบัญชีที่ไม่เคลื่อนไหวโดยไม่มีการเช็คสอบรายละเอียดกับ MCA Master File จึงเป็นช่องทางให้เกิดการทุจริต
4. แบ่งแยกหน้าที่ไม่เหมาะสม เช่น ให้ฝ่ายประมวลผลข้อมูลรับผิดชอบเกี่ยวกับความถูกต้องของยอดรวมใน Control Book
5. การยินยอมให้ผู้เขียนโปรแกรมและวิเคราะห์ระบบงาน เช่น ผู้จัดการฝ่ายประมวลผลข้อมูลสามารถเข้าไปใช้แฟ้มข้อมูลและโปรแกรมทั้งหมดโดยไม่จำกัด

การลงโทษผู้ทุจริต

ผู้ทุจริต 16 คน เป็นพนักงาน VSRS 3 คน บุคคลภายนอก 13 คน ถูกศาลพิพากษาจำคุก โดยหัวหน้าแผนก Refund 8 ปี เสมียนแผนก Refund 2 คน ๆ ละ 6 ปี เมื่อรวมโทษจำคุกที่แต่ละคนได้รับคือ 50 ปี

การทุจริตและการตรวจสอบกรณีทุจริตเกี่ยวกับคอมพิวเตอร์ (กรณีการจ่ายคืนเงินฝากในรายละเอียด)

1. ความเป็นมาขององค์กรที่เกิดการทุจริต

The Virginia Supplemental Retirement System คือ องค์กรที่ทำหน้าที่เป็นกองทุนเลี้ยงชีพร่วม (Consolidated pension System) พนักงานลูกจ้างของรัฐใน The Commonwealth of Virginia ส่วนใหญ่เป็นพนักงานลูกจ้างของส่วนราชการท้องถิ่น โรงเรียน รัฐบาล คณะกรรมการศึกษาโรงเรียน และหน่วยงานของรัฐอื่น ๆ ประมาณ 700 แห่ง มีบัญชีเงินฝากของพนักงานทั้งที่ยังทำงานอยู่และออกจากงานแล้วกว่า 235,000 บัญชี มีสินทรัพย์รวม 1,300 ล้านเหรียญสหรัฐ ส่วนใหญ่เป็นหุ้นและพันธบัตร ซึ่งเท่ากับ VSRS เป็นธนาคารที่ใหญ่ที่สุดแห่งหนึ่งใน Virginia

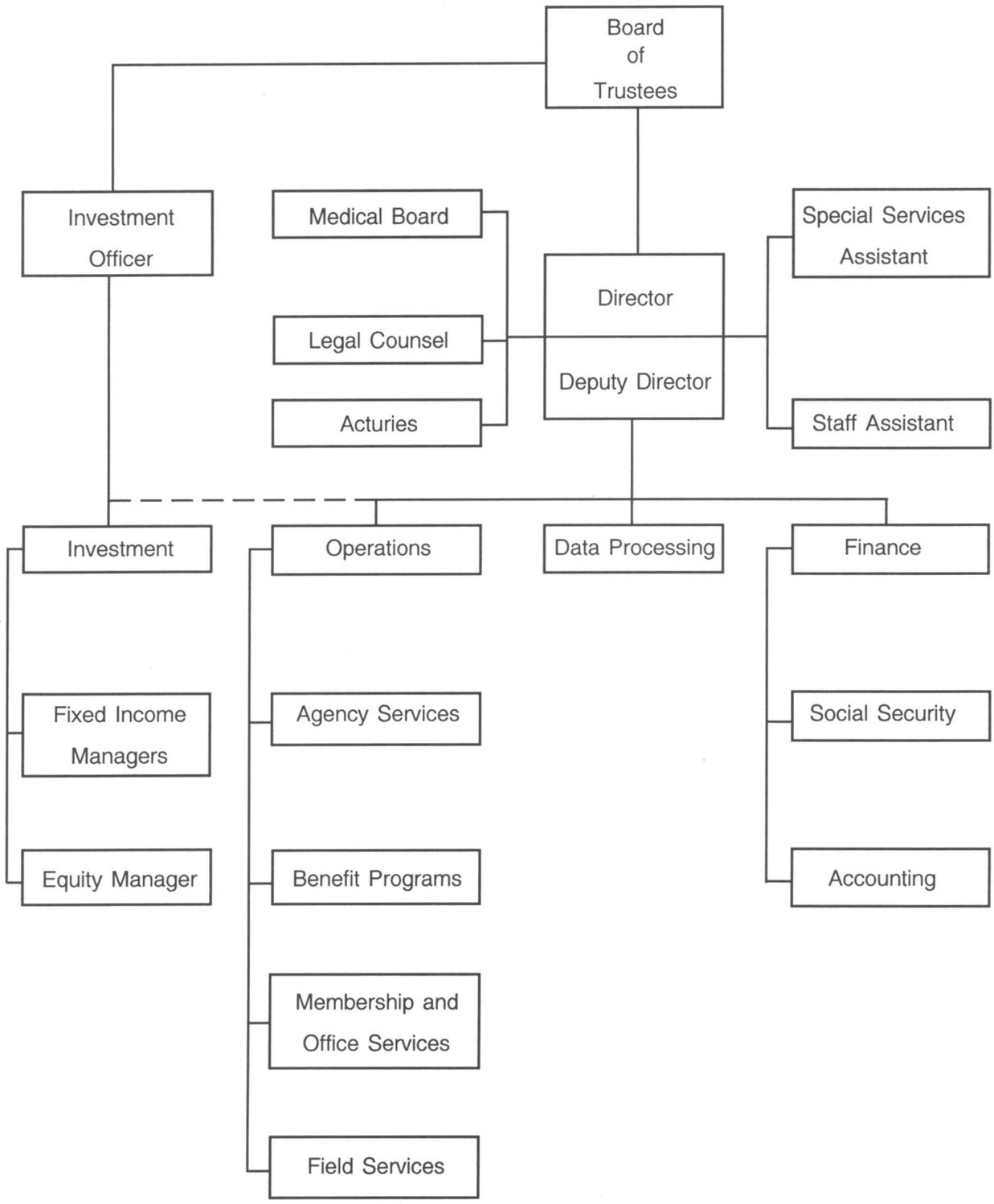
รัฐเป็นผู้ดำเนินการกองทุนร่วมนี้ โดยมอบหมายให้คณะกรรมการ 7 คน เป็นผู้บริหารงาน ประกอบด้วยเจ้าหน้าที่จากส่วนกลาง ตัวแทนจากคณะกรรมการโรงเรียน ส่วนราชการท้องถิ่น และ State executive branch และบุคคลภายนอกอีก 3 คนรวมเป็น 7 คน คณะกรรมการเหล่านี้ไม่มีความรู้เกี่ยวกับการบัญชี หรือการประมวลผลด้วยคอมพิวเตอร์ แต่อย่างไรก็ตามก่อนหน้าปี พ.ศ. 2520 สองคนในคณะกรรมการชุดนี้เป็นผู้สอบบัญชีรับอนุญาต

คณะกรรมการมีหน้าที่รับผิดชอบเกี่ยวกับการบริหารงานประจำวัน ในปี 2520 ซึ่งเป็นปีที่มีการตรวจสอบ VSRS แบ่งองค์กรออกเป็น 4 แผนกใหญ่ ๆ (ตามรูปภาพที่ 1) ดังนี้



VIRGINIA SUPPLEMENTAL RETIREMENT SYSTEM (VSRS)

Organization Chart



รูปภาพที่ 1

1. แผนก Investments มีหน้าที่ซื้อขายหุ้นและพันธบัตร แผนกนี้ไม่มีส่วนเกี่ยวข้องในการทุจริต
2. แผนก Operations มีหน้าที่รับผิดชอบหน่วยงานหลายหน่วย รวมทั้งหน่วยงานที่ให้บริการแก่สมาชิกกองทุน (Member and Offices Services) ซึ่งเป็นหน่วยงานต้นตอของการเกิดทุจริต
3. แผนก Data Processing มีผู้จัดการแผนกซึ่งทำหน้าที่ทั้งวิเคราะห์ระบบงานและเขียนโปรแกรม จนกระทั่งปี พ.ศ.2520 จึงจ้างนักโปรแกรมผู้ช่วยมา 1 คน นอกจากนั้นผู้จัดการแผนกยังต้องบังคับบัญชาพนักงานระดับเสมียนอีก 15 คน ซึ่งทำหน้าที่ Retirement Contribution Reporting, Remote job entry และ Data control
4. แผนก Finance มีหัวหน้าแผนกและพนักงานบัญชีอีก 5 คน รับผิดชอบในการบันทึกรายการในบัญชีย่อยและบัญชีคุมยอดทั่วไป (Subsidiary and General Ledgers)

VSRS ส่งข้อมูลเข้าไปประมวลผลในคอมพิวเตอร์ โดยผ่านทางเครื่องรับส่งที่ตั้งอยู่ในสถานที่ทำงาน (RJE Station) ซึ่งห่างจากศูนย์กลางคอมพิวเตอร์ IBM 370/158 ประมาณ 2 ไมล์ และศูนย์คอมพิวเตอร์แห่งนี้ยังให้บริการแก่องค์การของรัฐอื่นอีก 28 แห่ง

2. เหตุการณ์ที่ก่อให้เกิดการทุจริต

เนื่องจากปริมาณธุรกิจของ VSRS เพิ่มขึ้นมากในช่วงระยะเวลา 10 ปี ทำให้ไม่สามารถบันทึกบัญชีด้วยมือต่อไปได้อีก VSRS จึงตัดสินใจที่จะนำคอมพิวเตอร์มาใช้ โดยมอบหมายให้องค์การของรัฐที่เรียกว่า Department of Automated Data Processing (ADP) เป็นผู้พัฒนาระบบงานประมวลผลด้วยคอมพิวเตอร์ ADP เป็นหน่วยงาน ที่มีหน้าที่พัฒนาระบบงาน เขียนโปรแกรม และประมวลผลให้องค์การของรัฐที่ไม่มีหน่วยงานคอมพิวเตอร์เป็นของตนเอง

ในปี 2515 หลังจากที่พยายามพัฒนาระบบงานมาแล้ว 5 ปี ทั้ง VSRS และ ADP มีความเห็นพ้องตรงกันว่า โครงการที่ทำอยู่นี้ล้มเหลวโดยสิ้นเชิง ทั้งนี้เนื่องมาจากขาดการบริหารโครงการที่ดี และ VSRS มีความเห็นไม่ตรงกันกับ ADP เกี่ยวกับความต้องการของระบบงาน (System requirements) อย่างไรก็ตาม VSRS เริ่มใช้คอมพิวเตอร์เมื่อวันที่ 1 กรกฎาคม 2515 ทั้ง ๆ ที่ตรวจพบว่ายังมีข้อบกพร่องที่สำคัญ ๆ ในระบบอีก 26 แห่ง และเนื่องจาก VSRS ไม่มีพนักงานหรือผู้เชี่ยวชาญที่จะดำเนินงานตามระบบงานใหม่นี้ได้ จึงต้องจ้างพนักงานของ ADP 3 คน ซึ่งรับผิดชอบโครงการนี้มาทำหน้าที่เป็นรองผู้อำนวยการ ผู้จัดการฝ่าย Operation และผู้จัดการฝ่ายประมวลผลของ VSRS โดยมอบหมายให้แต่ละคนรับผิดชอบเกี่ยวกับการแก้ไขข้อบกพร่องและใช้ระบบงานใหม่นี้

3. บทบาทของผู้สอบบัญชี

VSRS ไม่มีหน่วยงานที่ทำหน้าที่ตรวจสอบภายในของตนเอง แต่อย่างไรก็ตามผู้สอบบัญชีรับอนุญาตจากรัฐ (Auditor of Public Accounts – APA) ซึ่งมีหน้าที่ตรวจสอบฐานะการเงินขององค์การของรัฐใน Virginia ทำหน้าที่เป็นผู้ตรวจสอบฐานะการเงินของ VSRS แต่เนื่องจาก APA ขาดกำลังเจ้าหน้าที่ผู้ตรวจสอบ จึงไม่สามารถตรวจสอบ VSRS อย่างสม่ำเสมอได้ ดังนั้นจึงทำการตรวจสอบในปีการเงินสิ้นสุด 30 มิถุนายน 2512 และ 2515 เท่านั้น

คณะผู้ตรวจสอบที่เข้าทำการตรวจสอบ VSRS ในปีการเงินสิ้นสุด 30 มิถุนายน 2520 พบว่า การตรวจสอบของปี 2515 ยังไม่สมบูรณ์ การตรวจสอบเบื้องต้น (Preliminary Work) ซึ่งเริ่มตั้งแต่เดือนมีนาคม 2520 ได้แก่ การตรวจสอบระบบการควบคุมทางด้านการบัญชี และการประมวลผลด้วยคอมพิวเตอร์ (EDP) ผู้ตรวจสอบจะตรวจสอบและจัดทำงบการเงินสำหรับปีสิ้นสุด 30 มิถุนายน 2516, 2517, 2518, 2519 และ 2520 แต่ไม่มีการตรวจสอบด้าน EDP เลยในระยะ 5 ปีที่ผ่านมา และไม่เคยแม้แต่จะตรวจสอบระบบการควบคุมภายในอย่างกว้าง ๆ เกี่ยวกับระบบงานด้านคอมพิวเตอร์ ซึ่งอาจเป็นสาเหตุหนึ่งที่ทำให้การตรวจสอบด้านการเงิน (Financial examination) ได้ผลไม่สมบูรณ์ และไม่อาจตรวจพบกรณีการทุจริตที่เกิดขึ้นได้

4. การตรวจสอบเบื้องต้น (Preliminary Audit Review)

ผู้ตรวจสอบเข้าร่วมประชุมกับฝ่ายบริหารของ VSRS เพื่อชี้แจงเกี่ยวกับวิธีการตรวจสอบโดยทั่ว ๆ ไป และขอบเขตของการตรวจสอบ ผู้ที่ไม่ได้เข้าร่วมประชุม คือรองผู้อำนวยการ VSRS ซึ่งลาออกและย้ายไปอยู่ที่รัฐอื่น เรื่องที่สำคัญ ๆ ได้แก่

1. การสอบถามพนักงานของ VSRS และศึกษาระบบงานจาก System Documentation
2. การจัดทำแผนผังการควบคุมและคำบรรยายเกี่ยวกับลักษณะของระบบงาน (Computer Application Systems)

ระบบงานคอมพิวเตอร์ที่สำคัญ ๆ แบ่งออกเป็น 4 ระบบ คือ

1. Member Contribution Account (MCA) System
2. Refund System
3. Retirement Annuitant Payroll System (RAPS)
4. Investment Portfolio Accounting System

5. Member Contribution Accounts (MCA) System

หมายถึง ระบบงานที่ใช้สำหรับบันทึกและประมวลผลรายการนำส่งเงินของสมาชิก VSRS แต่ละราย ซึ่งมีบัญชีอยู่ในแฟ้มข้อมูลทั้งสิ้น 315,000 บัญชี การค้นหาและเก็บข้อมูลในบัญชีใช้ระบบ ISAM (Indexed Sequential Access Method) ลักษณะของข้อมูลที่บรรจุอยู่ใน MCA master file ปรากฏอยู่ในรูปภาพที่ 2

ในแต่ละปีจะมีรายการ (Transactions) เข้ามาในระบบงาน MCA มากกว่า 3 ล้านรายการ หรือเป็นจำนวนเงินที่รับเข้ามามากกว่า 100 ล้านเหรียญสหรัฐ การส่งเงินของสมาชิกแต่ละรายกระทำโดยผ่านทางนายจ้าง นายจ้างจะหักเงินเดือนพนักงานซึ่งเป็นสมาชิกของ VSRS และนำส่งเช็ค ใบนำส่งเช็ค และรายชื่อสมาชิก และจำนวนเงินแต่ละราย (Contribution Report) ให้ VSRS

เมื่อ VSRS ได้รับเอกสารที่กล่าวเรียบร้อยแล้ว จะส่งเช็คและใบนำส่งเช็คไปให้แผนกบัญชี แผนกบัญชีจะออกใบรับฝากเงิน (Deposit Certificate) ให้ และนำเช็คไปฝากเข้าธนาคาร จากนั้นจะบันทึกรายการในสมุดบัญชีเงินสดรับ (Cash Receipts Ledger) และทำใบนำส่งเช็คไปเก็บเรื่องเข้าแฟ้มไว้เป็นหลักฐาน สำหรับ Contribution Report จะถูกส่งไปยังแผนก Contribution Reporting Section

MCA MASTER FILE
RECORD LAYOUT

Data Item	Source of Data	Definition
Delete Code	-	COBOL ISAM delete field (1 byte)
Account Status	-	Status of Account 1 = actively contributing to VSRS 2 = no longer contribution to VSRS but has chosen to keep money in the account 3 = contribution balance has been refunded 4 = contribution balance has been transferred to a retirement account 5 = contribution balance has been paid to a beneficiary
ISAM Record Key		
Reporting Code	Form VSRS-1 or	Employer reporting code
Social Security Number	Contribution Report	Member's social security number
Member Name	Form VSRS-1 or Contribution Report	First name, middle initial, and last name of the member
Last Contribution Date	Contribution Report	Date of the last contritubution report processed for the account
Contribution Amount	Contribution Report	The amount contributed on the last contribution report processed
Membership Date	Form VSRS-1	Initial membership date
Sex	Form VSRS-1	Member's sex
Birth Date	Form VSRS-1	Member's birth date
Termination Date	Form VSRS-3	Date the member will no longer be contributing to VSRS (date of last contribution report to be processed for the account)
YTD Contribution Amount	Computed	Total contributions in the account during current fiscal year
Prior Contribution Amount	Computed	Total contributions in the account prior to current fiscal year
Prior Interest Amount	Computed	Balance of interest applied to prior contribution balances
Refund Code	Refund Card	A one-byte field. If the field contains an "R", then the balance in the account have already been refunded

รูปภาพที่ 2

รายงาน Contribution Report ที่ส่งมาให้ VSRS โดยปกติจะแสดงเฉพาะสมาชิกรายซึ่งเปลี่ยนแปลงหรือเพิ่มขึ้นใหม่เท่านั้น (exception basis) ส่วนรายที่มิได้รายงานถือว่าคงเดิม ดังนั้นการบันทึกข้อมูลเข้าไปเก็บไว้ใน MCA master file จะยึดถือจำนวนเงินที่นำส่งครั้งก่อนเป็นหลัก แล้วปรับปรุงด้วยส่วนที่เปลี่ยนแปลงหรือเพิ่มเติมตามรายงานที่ฝากนายจ้างส่งมาให้ก่อนที่จะสั่งให้คอมพิวเตอร์ UPDATE บัญชีสมาชิกด้วยจำนวนเงินที่กล่าว VSRS จะให้คอมพิวเตอร์พิมพ์รายงานจำนวนเงินนำส่งรวมของนายจ้างแต่ละรายแล้วส่งไปให้แผนก Contribution Reporting Section เพื่อเปรียบเทียบกับจำนวนเงินในใบนำส่งเช็ค (Check Transmittal Form) เมื่อ UPDATE เรียบร้อยแล้วคอมพิวเตอร์จะออกรายงานส่งให้แผนก Contribution Reporting Section 3 ฉบับคือ Posting Sheet Report, Possible Duplicate Accounts Report และ Missing Membership Data Report

Posting Sheet Report คือ รายงานที่แสดงจำนวนเงินรวมที่ UPDATE ในบัญชีสมาชิก VSRS ของนายจ้างแต่ละราย หลังจากบันทึกจำนวนรวมดังกล่าวไว้ใน Control Book แล้วก็จะทิ้ง Posting Sheet Report ไป

Possible Duplicate Accounts Report คือ รายงานที่แสดงบัญชีสมาชิกที่มีชื่อและหมายเลขประกันสังคม (Social Security Number) เหมือนกัน รายงานนี้เป็นประโยชน์ในการค้นหาหมายเลขประกันสังคมที่นายจ้างรายงานมาผิดพลาด

Missing Membership Data Report คือ รายงานที่แสดงรายชื่อของสมาชิกรายที่ไม่มีบัญชีใน MCA master file ทั้งนี้เนื่องจากนายจ้างไม่กรอกและส่งแบบฟอร์ม VSRS Membership Form (VSRS-1) มาให้ จึงทำให้ VSRS ไม่ได้เพิ่มบัญชีสมาชิกให้ตามปกติในสัปดาห์แรกที่พนักงานใหม่เข้าทำงาน นายจ้างต้องกรอกแบบฟอร์ม VSRS-1 ระบุชื่อ อายุ เพศ วันที่เป็นสมาชิก และผู้รับผลประโยชน์ ส่งไปให้ VSRS เพื่อเปิดบัญชีสมาชิกใหม่ให้ VSRS จะเก็บ VSRS-1 เรียงเข้าแฟ้มไว้ในห้องเก็บของ (Storeroom) ซึ่งมิได้ควบคุมการเข้าและออกในแผนก Membership and Office Services Section

สมาชิกที่ยังคงดำรงสภาพพนักงานอยู่ (Active Members) จะได้รับใบแจ้งยอดคงเหลือในบัญชี (Account Statements) ปีละครั้ง โดย VSRS จะส่งตรงไปให้นายจ้างเพื่อแจกจ่ายให้พนักงานซึ่งเป็นสมาชิกต่อไป

6. Refund System

หมายถึง ระบบงานที่ใช้สำหรับบันทึกและประมวลผลรายการจ่ายคืนเงินให้แก่สมาชิกรายซึ่งออกจากงาน และยื่นหนังสือแสดงความจำนงขอถอนเงินที่ฝากไว้คืน ในกรณีที่สมาชิก (Active Member) ถึงแก่กรรม VSRS จะคืนเงินที่รับฝากให้แก่กองมรดกหรือผู้รับประโยชน์ และปรับปรุงยอดคงเหลือในบัญชีของสมาชิกรายที่รับเงินคืนไป

ในแต่ละปี VSRS จะคืนเงินให้สมาชิก 18,000 ถึง 22,000 ราย เป็นจำนวนเงินประมาณ 14 ถึง 21 ล้านเหรียญ ส่วนใหญ่จะชุกในช่วงฤดูร้อน เพราะอัตราการเปลี่ยนงานสูง โดยเฉพาะอาชีพครู

เมื่อสมาชิกมีความประสงค์จะขอถอนเงินคืน จะต้องกรอกแบบฟอร์ม VSRS-3 รูปภาพที่ 3 ซึ่งระบุหมายเลขประกันสังคม ชื่อ ที่อยู่ วันเดือนปีเกิด และชื่อของนายจ้าง หลังจากลงลายมือชื่อเรียบร้อยแล้วก็ให้ส่ง VSRS-3 ไปยังแผนกเงินเดือนของตน แผนกเงินเดือนจะกรอกรายละเอียดที่เหลือของแบบฟอร์ม VSRS-3 ท่อนล่าง ซึ่งระบุวันที่ที่หักเงินเดือนครั้งสุดท้าย ชื่อ และรหัสประจำตัวของนายจ้าง และรายละเอียดของเงินนำส่งที่ยังไม่ได้รายงานให้ VSRS ทราบ จากนั้นก็ลงนามแล้วส่งไปให้ VSRS ซึ่งจะมอบหมายให้แผนก Refund Section (สังกัดอยู่ใน Membership and Office Service Department) ตรวจสอบความสมบูรณ์ของเอกสาร จากนั้นจะส่ง VSRS-3 ไปให้ฝ่ายประมวลข้อมูลทำการเจาะบัตรเพื่อบันทึกลงเทปที่เรียกว่า Refund Inventory Computer Tape ซึ่งใช้สำหรับบันทึกรายการขอถอนเงินคืนที่ยังคงค้างอยู่ทั้งหมด และพิมพ์รายละเอียดของรายการขอถอนเงินคืนที่คงค้างในเทป ฝ่ายประมวลข้อมูลจะส่งรายละเอียดนี้พร้อมกับเทปไปให้แผนก Refund Section



MEMBERSHIP WITHDRAWAL

"Request to be Paid Accumulated Contributions"

(Please Print or Type)

Social Security Number _____

Last Name _____ First _____ Middle _____ Date of Birth _____

Street Address _____ City or Town _____ State _____ Zip _____

If you worked for any other employer under the Virginia Supplemental Retirement System and did not receive a refund, insert the following :

_____ Employed From _____ through _____

Name of other Employer

I have read and understand the front and back of this form.

Signature of Employee _____ Date _____

TO BE COMPLETED BY EMPLOYER

THE ABOVE EMPLOYEE HAS TERMINATED HIS EMPLOYMENT AND FINAL

DEDUCTION REPORTED ON PAYROLL FOR PAY PERIOD ENDING _____

(Enter pay period ending date)

Agency Name _____ Agency Code # _____ Activity # _____

LIST CONTRIBUTIONS NOT YET REPORTED TO VSRS (FROM LAST PAYROLL TO TERMINATION) :

Month and Year					
Amount					

Signature of Employer _____

FOR RETIREMENT SYSTEM USE ONLY

(continued on next page)

รูปภาพที่ 3

M.D._____ T_____ F_____ K _____ S.S.No. _____ Dept. _____

D.O.B._____ Date Dropped _____ Termination_____

Pay to_____

Beneficiary of_____

Prior Interest_____

Prior Coutributions_____

Current Interest_____

Current Coutributions._____

Total_____

Voucher No._____Check No._____

Check Mailed_____

รูปภาพที่ ๓ (ต่อ)

แผนก Refund Section จะนำ VSRS-1 ซึ่งเก็บไว้ใน Storeroom มาประกบกับ VSRS-3 รายที่ขอถอนเงินคืน แล้วเก็บรวบรวมกันไว้ในแฟ้ม พนักงานประจำเครื่องรับส่งข้อมูล (RJE Operator) จะเรียกโปรแกรมคอมพิวเตอร์เพื่อมาทำการเปรียบเทียบข้อมูลที่เก็บไว้ใน Refund Inventory Tape กับ MCA master file และพิมพ์รายงานยอดคงเหลือของแต่ละบัญชีสัปดาห์ละครั้ง แล้วส่งรายงานนี้ไปให้แผนก Refund Section ตรวจสอบกับ VSRS-3 ที่เก็บไว้ในแฟ้ม แผนก Refund Section จะคำนวณจำนวนเงินที่ต้องคืนให้แก่สมาชิกจากแบบฟอร์ม VSRS-3 ท่อนล่าง ซึ่งจะเท่ากับจำนวนเงินที่ปรากฏตามรายงานยอดคงเหลือในบัญชี บวกด้วยส่วนที่นายจ้างรับรองว่าได้หักจากเงินเดือนของพนักงานแล้ว แต่ยังไม่ได้รายงานให้ VSRS ทราบ

แผนกบัญชี (Accounting Section) จะออกสลิปปะหน้า (Voucher Cover Sheet) ปิด VSRS-3 ส่งให้ฝ่ายประมวลข้อมูลเจาะรหัสบนบัตร Refund Card รูปภาพที่ 4 แล้วจัดทำรายละเอียดจำนวนเงินที่ขอถอนคืนแต่ละราย และรวมยอดจำนวนเงินที่ขอถอนคืนทั้งสิ้นตาม Refund Card เปรียบเทียบกับจำนวนเงินรวมในสลิปปะหน้า อย่างไรก็ตามการถอนเงินคืนไม่จำเป็นจะต้องถอนจนยอดในบัญชีเหลือเป็นศูนย์ แต่จะกำหนดรหัสพิเศษให้เพื่อแสดงว่าบัญชีนี้มีการถอนเงินคืนไปแล้ว เสร็จแล้วจะโอนรายการถอนเงินคืนจาก Refund Inventory Tape ไปเก็บไว้ใน Refund Transaction History Tape สำหรับ Refund Card ฝ่ายประมวลข้อมูลจะเก็บเข้าแฟ้มไว้เพื่อใช้ในการหักบัญชีสมาชิกต่อไปเมื่อนายจ้างส่งเงินมาให้เพิ่มเติมตามที่ระบุไว้ใน VSRS-3 โดยเรียงลำดับตามหมายเลขรหัสของนายจ้างและวันครบกำหนดในแฟ้มนี้จะมี Refund Card ประมาณ 2,000-3,000 ใบ

ฝ่ายประมวลข้อมูลจะส่งรายงานคอมพิวเตอร์และ VSRS-3 กลับคืนไปให้ Refund Section เพื่อเช็คสอบยอดรวม เสร็จแล้ว Refund Section จะส่งสลิปถอนเงิน (Voucher) ไปให้ผู้อำนวยการ VSRS ลงนาม สั่งจ่าย เมื่อ Refund Section ได้รับสลิปคืนมาก็จะส่งโดยทางไปรษณีย์ไปให้สำนักงานคลังของรัฐ (State Treasurer's Office) พร้อมกับที่อยู่ตามที่ระบุไว้ในท่อนล่างของ VSRS-3 และจะส่งสลิปต้นฉบับไปให้สำนักงานบัญชีกลางของรัฐ (State Comptroller's Office) ส่วนสลิปชุดสำเนาจะถูกส่งไปยังแผนกบัญชีเพื่อบันทึกในสมุดบัญชีเงินสดจ่าย (Cash Disbursements Ledger) แล้วส่งกลับไปเก็บเข้าแฟ้มใน Refund Section

ตามที่กล่าวไว้ตอนต้นแล้วว่า VSRS จะยังไม่คืนเงินให้แก่สมาชิกจนกว่านายจ้างจะส่งรายงานและเงินมาให้จนครบแล้ว ดังนั้นเมื่อนายจ้างส่งรายงานมาครบแล้ว เสมียนในแผนก Contribution Reporting Section จะดึง Refund Card รายที่มีวันครบกำหนดตรงกับวันที่ในรายงาน (Reporting Period Date) จากนั้นก็ส่ง Refund Card ไปให้พนักงานประจำเครื่อง RJE เพื่อลดยอดคงเหลือในบัญชีด้วยจำนวนเงินตามที่ปรากฏใน Refund Card แล้วสั่งให้เครื่องคอมพิวเตอร์พิมพ์รายงานจำนวนเงินที่ถอนคืนไปทั้งหมด (Refund Total Report) โดยแสดงรายละเอียดเฉพาะหมายเลขประจำตัวนายจ้างและจำนวนเงินรวมแต่ละราย จากนั้นก็บันทึกจำนวนเงินที่ถอนคืนไปทั้งสิ้นใน Control Book ซึ่งเป็นสมุดเล่มเดียวกับที่เคยบันทึกจำนวนเงินรับจากสมาชิกทั้งสิ้น เสร็จแล้วก็ทิ้ง Refund Card ไป

REFUND CARD
DATA CONTENT

	Data Item	Definition
1.	Social Security Number	Member's social security number
2.	Payee Name	Initials and last name of member or beneficiary
3.	Voucher Number	Voucher number under which this refund was issued
4.	Reporting Code	Employer reporting code
5.	Termination Date	Date the member will no longer be contributing to VSRS (date of last contribution report to be processed)
6.	Prior Contribution Amount	Amount of prior contributions to be refunded
7.	Prior Interest Amount	Amount of prior interest to be refunded
8.	Current Contribution Amount	Amount of current contributions to be refunded
9.	Current Interest Amount	Amount of current interest to be refunded
10.	Total Refund Amount	Amount of the total to be refunded (sum of items 6-9)

รูปภาพที่ 4

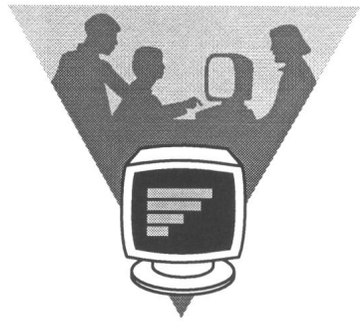
ในกรณีที่ยังมียอดคงเหลืออยู่ในบัญชีหลังจากที่คืนเงินให้สมาชิกแล้ว ทั้งนี้อาจจะเนื่องมาจากการคำนวณผิดพลาด แผนก Refund Section จะต้องตรวจสอบดูว่าควรจะคืนเงินที่เหลือให้แก่สมาชิกหรือไม่ ในบางกรณีก็จะส่งใบยืนยันยอดไปให้สมาชิกหรือนายจ้าง เมื่อได้รับใบยืนยันยอดคืนมาจะส่งไปให้ฝ่ายประมวลข้อมูลพร้อมกับ Refund Worksheets เพื่อเจาะรหัสลงบัตร แต่โดยปกติเสมียนในแผนก Refund Section จะเป็นผู้เจาะบัตรด้วยตนเอง จากนั้นก็ดำเนินการเหมือนกับกรรมวิธีข้างต้น ยกเว้นว่าไม่ต้องบันทึกรายการขอ Refund ไว้ใน Refund Inventory Tape

การคืนเงินให้แก่ผู้รับประโยชน์หรือกองมรดก ก็คงดำเนินวิธีการเช่นเดียวกับการคืนเงินตามปกติ

7. การควบคุมภายในระบบ MCA (MCA Control Process)

เนื่องจากเอกสารคำอธิบายเกี่ยวกับระบบ MCA และ Refund System ที่มีอยู่ไม่เพียงพอ เพราะฉะนั้นผู้ตรวจสอบต้องอาศัยการสอบถามเรื่องการควบคุมจากพนักงานของ VSRS

VSRS ใช้ Control Book ควบคุมยอดคงเหลือของ MCA รายการบัญชีใด ๆ ก็ตามที่มีผลกระทบต่อยอดเงินรับฝากคงเหลือ (Contribution Balances) จะต้องบันทึกลงใน Control Book ซึ่งมีลักษณะเป็นแผ่น ๆ (Control Sheet) แผ่นหนึ่งใช้สำหรับบันทึกรายการของนายจ้าง 1 ราย ในเวลา 1 เดือน รูปภาพที่ 5 เป็นตัวอย่าง Control Sheet ของนายจ้างรหัสเลขที่ 5234 เดือนพฤศจิกายน 2518 บรรทัดแรกเป็นยอดยกมาของเดือนก่อน บรรทัดต่อมาเป็นจำนวนเงินรวมที่ส่งในเดือนพฤศจิกายน US $2,805.20 ในระหว่างเดือนมีรายการขอถอนเงินคืนจากสมาชิก 2 ราย US $4,527.64 และ $179.64 ดอกเบี้ย US $2,275.68 และ $51.00 ตามลำดับ ยอดคงเหลือสิ้นเดือนพฤศจิกายนจะเป็นยอดที่ยกไปต้นเดือนธันวาคม



CONTROL SHEET

CODE 5234

MONTH NOV. '75

	Prior Contributions	Prior Interest	Current Contributions
Balance Forward	5,044,554.94	714,061.77	9,593.70
Contribution Report(s)			2,805.20
Transfers			
Refunds	24,527.64 179.64	2,275.68 51.00	- -
Retirements	2,092.68	273.22	-
Deaths			
Journal Vouchers	468.59 +	96.57 +	
Type 3S			
Life Adjustment			
TOTAL	5,018,223.57	711,558.44	12,398.90

รูปภาพที่ 5

Control Book ของแต่ละเดือนจะรวม Control Sheet ของนายจ้างแต่ละใบ ฉะนั้นในขณะใดขณะหนึ่งก็ตามยอดคงเหลือใน Control Book จะต้องตรงกับยอดคงเหลือในบัญชีของนายจ้างแต่ละรายเช่นเดียวกัน รายการฝากและถอนเงินที่บันทึกไว้ MCA master file และ Control Book ก็จะต้องตรงกับรายการในสมุดบัญชีเงินสดรับ และเงินสดจ่ายตามระบบการบัญชีรวม (Central Accounting System)

เมื่อสิ้นสุดปีการเงินแต่ละปี ฝ่ายประมวลข้อมูลจะคัดลอก (Copy) ข้อมูลใน MCA master file ไปลงในเทปแม่เหล็ก (Magnetic Tape) ซึ่งเรียกว่า MCA Year End History Tape เทปนี้จะมีข้อมูลสมบูรณ์ก็ต่อเมื่อนายจ้างรายสุดท้ายได้ส่งรายงาน Contribution Report ของเดือนมิถุนายน สิ้นสุดวันที่ 30 มาให้เรียบร้อยแล้ว เทปม้วนนี้มีความสำคัญต่อการตรวจสอบ (Audit Trail) เพราะมียอดคงเหลือในบัญชีของสมาชิกแต่ละราย ณ วันที่ 30 มิถุนายน ซึ่งเมื่อรวมกันแล้วควรจะเท่ากันกับยอดรวมในสมุดบัญชีคุมยอดทั่วไป (General Ledger)

8. สิ่งที่ค้นพบจากการตรวจสอบเบื้องต้น (Preliminary Review Findings)

การตรวจสอบระบบ MCA และ Refund เบื้องต้นเสร็จสิ้นในเดือนกรกฎาคม 2520 ผู้ตรวจสอบ พบว่าระบบการควบคุมภายในมีจุดอ่อนที่ร้ายแรง (Serious Weaknesses) จึงแจ้งให้ฝ่ายบริหารของ VSRS ยุตินโยบายการให้ถอนเงินคืนไปโดยที่ยังไม่ได้รับรายงาน Contribution จากฝ่ายนายจ้าง (Policy of Refunding Unreported Contributions) แต่ฝ่ายบริหารของ VSRS ไม่มีทีท่าว่าจะทำตามคำแนะนำดังกล่าว ดังนั้นผู้ตรวจสอบจึงตัดสินใจที่จะทดลองทำการทุจริตโดยอาศัยคอมพิวเตอร์ (Computer Fraud) เพื่อพิสูจน์ให้เห็นว่า Refund System นี้ง่ายต่อการฉ้อฉลโดยบุคคลใดบุคคลหนึ่ง (Manipulation)

ผู้ตรวจสอบวางแผนจะดำเนินการตรวจสอบเพื่อหาร่องรอยของการทุจริตที่อาจเป็นไปได้ เพื่อแสดงให้เห็นว่าพนักงานของ VSRS คนใดคนหนึ่งที่มีความชำนาญด้านโปรแกรมคอมพิวเตอร์มีความรู้เกี่ยวกับระบบ MCA และ Refund และเรียกใช้ MCA master file ได้ ก็สามารถทำการทุจริตได้ตามลำพังโดยไม่ต้องรับรู้ร่วมคิดกับผู้อื่น ทั้งนี้ก่อนที่จะดำเนินการตรวจสอบวิธีการทุจริตโดยใช้คอมพิวเตอร์ ผู้ตรวจสอบได้ขออนุมัติจากผู้อำนวยการของ APA ก่อนแล้ว

ในเดือนกรกฎาคม 2520 ผู้ตรวจสอบเริ่มดำเนินการตามแผนงานตรวจสอบการยักยอกเงินจาก VSRS โดยการเขียนโปรแกรมเพื่อสร้างบัญชีปลอมใน MCA master file จากนั้นก็ใช้โปรแกรมที่สองโอนเงินจากบัญชีอื่นมาใส่ไว้ในบัญชีปลอม เสร็จแล้วก็ปลอมแปลงเอกสาร VSRS-1 นำไปเก็บไว้ในแฟ้มภายในห้องเก็บ VSRS-1 ในระหว่างเวลาอาหารกลางวัน จากนั้นก็ปลอมแปลงเอกสาร VSRS-3 ให้สอดคล้องกับบัญชี และ VSRS-1 ปลอม ส่ง VSRS-3 ไปให้ VSRS โดยทางไปรษณีย์ 6 สัปดาห์ หลังจากนั้นจะมีเช็ค 3 ใบ มูลค่ามากกว่า US $3,000 เหรียญส่งโดยทางไปรษณีย์มาตามที่อยู่ในท่อนล่างของ VSRS-3 การทดลองทำการทุจริตครั้งนี้ผู้ตรวจสอบอาศัยเพียงแต่ความรู้ด้านการตรวจสอบเท่านั้น ไม่ได้ใช้อำนาจหน้าที่อื่นใดในฐานะผู้ตรวจสอบ ซึ่งพนักงานของ VSRS ไม่สามารถกระทำได้

เมื่อฝ่ายบริหารทราบผลของการทดลองทำการทุจริต ก็แสดงอาการไม่พอใจที่ผู้ตรวจสอบเข้าไปแทรกแซงระบบคอมพิวเตอร์ของ VSRS และชี้ให้เห็นว่าผู้ตรวจสอบสามารถยักยอกได้แต่เพียงจำนวนเงินน้อย ๆ เท่านั้น หากเป็นรายการใหญ่ ๆ จะต้องถูกจับได้อย่างแน่นอน

ผู้ตรวจสอบดำเนินการตรวจสอบเบื้องต้นต่อไปตามจุดอื่น ๆ ของ VSRS และหลังจากเสร็จสิ้นการตรวจสอบเบื้องต้นแล้ว ได้สรุปสิ่งสำคัญ ๆ ที่พบจากการตรวจสอบส่งให้กับผู้บริหาร ของ VSRS ดังนี้

1. ใน MCA master file ไม่แสดงรายการเคลื่อนไหวของบัญชี คงมีเฉพาะยอดคงเหลือปัจจุบันและดอกเบี้ยเท่านั้น

2. ในระหว่างปีการเงิน 2516 และ 2517 บัญชีสมาชิกทั้งหมดของนายจ้าง 470 ราย สูญหายและถูกทำลาย ปี 2518 เทปที่ใช้เก็บข้อมูลการคืนเงินในอดีต (Refund Transaction History Tape) มีรอยขูดขีด และไม่มีเทปชุดสำรอง

3. VSRS มีปัญหาที่สำคัญยิ่งในด้านการควบคุมความถูกต้องของข้อมูลทางบัญชี เนื่องจากการที่บรรดานายจ้างไม่ส่ง Contribution Reports มาให้ เพียงแต่ส่งเช็คและใบนำส่งเช็คให้ภายใน 30 วันนับจากวันสิ้นเดือน (Reporting Period) ตัวอย่างเช่น งวด 30 มิถุนายน 2517 มีองค์การของรัฐ 94 แห่งที่ไม่ส่งรายงานดังกล่าวให้ VSRS จนกระทั่งเลยกำหนดไปแล้ว 5 เดือนหรือมากกว่านั้น ในจำนวนนี้มี 6 แห่งที่ไม่ได้รายงานเป็นเวลา 1 หรือ 2 ปี ทำให้ VSRS ไม่สามารถจัดทำงบแสดงฐานะการเงินได้

4. ฝ่ายบริหารยินยอมให้คืนเงินแก่สมาชิกรายซึ่งออกจากงานในระหว่างนายจ้างยังส่ง Contribution Report มาให้ไม่ครบถ้วน ทั้งนี้เป็นผลมาจากการที่นายจ้างไม่ยอมส่งรายงานให้ทันเวลา

5. นับตั้งแต่ปี 2516 ไม่มีการกระทบยอด (Reconciliation) ข้อมูลใน MCA master file กับรายการบัญชีในสมุดบัญชีเงินสดรับและเงินสดจ่าย ในปีแรกที่เริ่มใช้ระบบ MCA การกระทบยอดข้อมูลทำได้ไม่ยุ่งยากนักต่อมาเมื่อมีการยินยอมให้คืนเงินได้โดยไม่ต้องรอรายงานจากนายจ้าง ประกอบกับเอกสารที่ใช้ในการบันทึกรายการใน MCA master file และสมุดบัญชีไม่สามารถใช้ยันกันได้ จึงทำให้ไม่สามารถกระทบยอดได้โดยสิ้นเชิง ในขณะที่ตรวจสอบพบว่ามีผลต่างระหว่างจำนวนเงินในบัญชีกับ Control Book อยู่ US $10 ล้านเหรียญ

6. การแบ่งแยกหน้าที่ในฝ่ายประมวลข้อมูลยังไม่ดีพอ แผนก Contribution Reporting Section ซึ่งมีหน้าที่จัดทำรายการนำฝาก (Contribution Transactions) และคืนเงิน (Refund Cards) อยู่ภายใต้การบังคับบัญชาของผู้จัดการฝ่ายประมวลข้อมูล และยิ่งไปกว่านั้นผู้จัดการฝ่าย ฯ ยังรับผิดชอบในการดูแลความถูกต้องของยอดรวมใน Control Books อีกด้วย

7. ผู้จัดการฝ่ายประมวลข้อมูลในฐานะที่เป็นผู้วิเคราะห์ระบบงานและเขียนโปรแกรม สามารถเข้าไปใช้แฟ้มข้อมูลและโปรแกรมได้โดยไม่จำกัด

จากผลของการตรวจสอบ ผู้ตรวจสอบได้สั่งการอีกครั้งหนึ่ง

- ให้ VSRS ยุติการยินยอมคืนเงินโดยที่ยังไม่ได้รับรายงาน Contribution ทันที
- ให้ VSRS จัดทำเอกสารคำอธิบายระบบงาน คู่มือปฏิบัติงาน

- ให้กระทำการกระทบยอดข้อมูลในคอมพิวเตอร์กับรายการในสมุดบัญชีที่สำคัญ ๆ และจะต้องทำให้เสร็จก่อนที่ APA จะเริ่มงานตรวจสอบต่อไป ดังนั้น VSRS จึงจ้างบริษัทสอบบัญชีมาดำเนินการกระทบยอดข้อมูลตามคำสั่งของผู้สอบบัญชี แต่การทำงานของบริษัทสอบบัญชีล่าช้า กลุ่มผู้ตรวจสอบของ APA จึงตัดสินใจทำงานชิ้นนี้ให้เสร็จเอง เพื่อประหยัดเงินที่จ่ายให้กับบริษัทสอบบัญชี

9. การค้นพบการทุจริต (The Discovery of Fraud)

ผู้ตรวจสอบกะว่าจะทำการกระทบยอดข้อมูลให้เสร็จสิ้นภายในเดือนธันวาคม 2520 จากนั้นก็จะกระทบยอดรายการในสมุดบัญชีของ VSRS กับรายการในสมุดบัญชีของสำนักงานบัญชีกลางของรัฐ ซึ่งเป็นมาตรฐานการตรวจสอบที่ APA ใช้เป็นประจำในการตรวจสอบองค์การของรัฐ

เช้าวันที่ 23 กุมภาพันธ์ 2521 ผู้ตรวจสอบค้นพบว่าจำนวนเงินที่บันทึกในสมุดบัญชีเงินสดจ่ายของ VSRS ไม่ตรงกับที่บันทึกในสมุดบัญชีของสำนักงานบัญชีกลาง ผู้ตรวจสอบจึงขอสลิป (Refund Voucher) ต้นฉบับจากสำนักงานบัญชีกลางมาเปรียบเทียบกับสลิปชุดสำเนาที่เก็บไว้ในแฟ้มของแผนก Refund Section ผู้ตรวจสอบพบว่ามีการแก้ไขสลิปต้นฉบับ และแก้ไขยอดเงินรวมในใบปะหน้าสลิปให้สอดคล้องกัน แต่มิได้แก้ไขเอกสารชุดสำเนา

ผู้ตรวจสอบได้นำสลิปที่ได้รับการแก้ไขไปให้หัวหน้าผู้ตรวจสอบที่รับผิดชอบในการ ตรวจสอบ VSRS และผู้อำนวยการของ APA พิจารณา ขอข้อมูลเพิ่มเติมจากสำนักงานสรรพากรของรัฐ (State Department of Taxation) เพื่อพิสูจน์ว่าชื่อผู้รับเงินและหมายเลขประกันสังคมนั้นเป็นของจริงหรือของปลอม ผลการพิสูจน์ปรากฏว่าเป็นรายงานถอนเงินปลอม

ประมาณ 2 โมงเช้า เจ้าหน้าที่ของ APA ที่ควบคุมการตรวจสอบ EDP ได้รับแจ้งว่ามีการทุจริตเกิดขึ้น และขอให้ตรวจสอบรายละเอียดของเอกสารที่เกี่ยวข้องใหม่ เนื่องจากรายการถอนเงินปลอมที่ปรากฏอยู่ในสลิปพิมพ์ด้วยเครื่องคอมพิวเตอร์ ดังนั้นผู้ควบคุมการตรวจสอบ EDP จึงสรุปว่าได้มีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำทุจริตโดยทางใดทางหนึ่ง

4 โมงเช้าผู้ตรวจสอบได้ยื่นหลักฐานการทุจริตให้แก่ผู้อำนวยการและรองผู้อำนวยการของ VSRS และได้รายงานการทุจริตให้สำนักงานอัยการประจำรัฐ ตำรวจประจำรัฐ และผู้ว่าการรัฐ Virginia ทราบเช่นเดียวกัน

10. สิ่งที่ต้องทำในการตรวจสอบ (Audit Functions)

เหตุการณ์ครั้งนี้เป็นการทุจริตครั้งใหญ่ที่เกี่ยวข้องกับคอมพิวเตอร์เป็นครั้งแรกในมลรัฐ Virginia ถึงแม้ว่าผู้ตรวจสอบไม่ได้ทำการทดสอบความถูกต้องของข้อมูลในคอมพิวเตอร์ทั้งหมดเมื่อพบว่ามีการทุจริตเกิดขึ้น ความรู้เกี่ยวกับระบบ Member Contribution Accounts (MCA) และระบบ Refund ที่ได้จากการตรวจสอบเบื้องต้นจะเป็นพื้นฐานช่วยให้ตรวจสอบการทุจริตนี้สำเร็จลงได้จากขั้นพื้นฐานที่จะต้องทำในการตรวจสอบ ได้แก่

10.1 การป้องกันรักษาข้อมูลการบัญชีที่เกี่ยวข้องกับการทุจริต รวมทั้งแฟ้มข้อมูลและโปรแกรมคอมพิวเตอร์ คัดลอกข้อมูลจาก History Tape, Current MCA master file และ Program Libraries ไปลงไว้ในเทปแม่เหล็ก

เมื่อทำการค้นหาต่อไป ผู้ตรวจสอบพบว่ามีการทุจริตเพิ่มขึ้นอีก สำหรับ Refund Vouchers ที่ออกในปี 2520 และ 2521 และขณะนี้มีหลักฐานเพียงพอที่จะออกหมายจับกุมอดีตพนักงานในแผนก Refund Section 2 คน แต่อย่างไรก็ตามหลังจากที่บุคคลทั้งสองลาออกไปแล้ว การทุจริตก็ยังคงดำเนินต่อไป ผู้ตรวจสอบสงสัยว่าพนักงานปัจจุบันมีส่วนในการทุจริต ดังนั้นจึงสั่งให้ VSRS ปิดสถานที่ประกอบการ 2 วัน เริ่มตั้งแต่วันจันทร์ที่ 27 กุมภาพันธ์ ในระหว่างเวลานั้นก็ทำการตรวจสอบรายการคืนเงินทุกรายที่อยู่ในระหว่างดำเนินการ และส่งเรื่องให้ตำรวจออกหมายจับกุมหัวหน้าแผนก Refund Section เมื่อพบหลักฐานว่ากระทำการทุจริตจริง

10.2 การวางแผนและประสานงานตรวจสอบ (Planning and Coordinating the Audit)

การค้นหาการทุจริตใน 4 วันแรก มีสภาพค่อนข้างสับสนวุ่นวาย ทั้งนี้เพราะ

1) ขาดการติดต่อระหว่างกัน
2) ทำงานซ้ำซ้อนกัน
3) ใช้วิธีการตรวจสอบที่ไม่มีประสิทธิผล
4) ไม่เข้าใจระบบ MCA และระบบ Refund อย่างลึกซึ้ง

จนกระทั่งถึงวันที่ 28 กุมภาพันธ์ คณะผู้ตรวจสอบได้จัดให้มีการประชุมเพื่อพิจารณาผลงานของวันก่อน ๆ วิธีการบริหารงาน และการตรวจสอบที่จะทำในอนาคต ที่ประชุมตกลงมอบหมายหน้าที่และความรับผิดชอบให้แก่ผู้ที่เกี่ยวข้องในการตรวจสอบการทุจริต ดังนี้

1) ผู้ตรวจสอบด้านคอมพิวเตอร์ (EDP Audit Group) รับผิดชอบในการศึกษาระบบ งานวางแผนการตรวจสอบ และมอบหมายงาน แบ่งแยกงานการตรวจ EDP และแนะนำแนวทางการตรวจแก่ Financial Auditors และจัดทำรายงานทางคอมพิวเตอร์เกี่ยวกับข้อมูลใน MCA และ Refund file ส่งให้ผู้ตรวจสอบด้านการเงิน
2) ผู้ตรวจสอบด้านการเงิน (Financial Audit Staff) รับผิดชอบในการตรวจสอบเอกสารเบื้องต้น ข้อมูลการบัญชี และหลักฐานการทุจริตตามรายงานคอมพิวเตอร์
3) ตำรวจสอบสวนของรัฐ (State Police Investigators) รับผิดชอบในการสอบสวนสถานที่เกิดเหตุ และออกหมายจับกุมตามเอกสารสำคัญที่ได้จากผู้ตรวจสอบ
4) สำนักงานอัยการประจำรัฐ (Commonwealth Attorney's Office) มีหน้าที่ให้คำปรึกษาแก่ตำรวจสอบสวนของรัฐ

กลุ่มบุคคลอื่นที่ไม่มีหน้าที่โดยตรงในการค้นหาการทุจริต แต่มีส่วนช่วยในการตรวจสอบ

1) The Joint Legislative Audit and Review Committee (JLARC) ซึ่งเป็นคณะกรรมการคณะหนึ่งของสภานิติบัญญัติแห่งรัฐ Virginia ได้มอบหมายให้ผู้วิเคราะห์กลุ่มหนึ่งทำการเช็คสอบการบริหารงานของ VSRS อย่างกว้าง ๆ
2) สำนักงานสอบบัญชีซึ่งเดิมเคยรับจ้างกระทบยอดข้อมูลให้ VSRS ทำสัญญาที่จะออกแบบและพัฒนาระบบงานให้ดีขึ้น รวมทั้งจัดวางการควบคุมและวิธีปฏิบัติงานใหม่

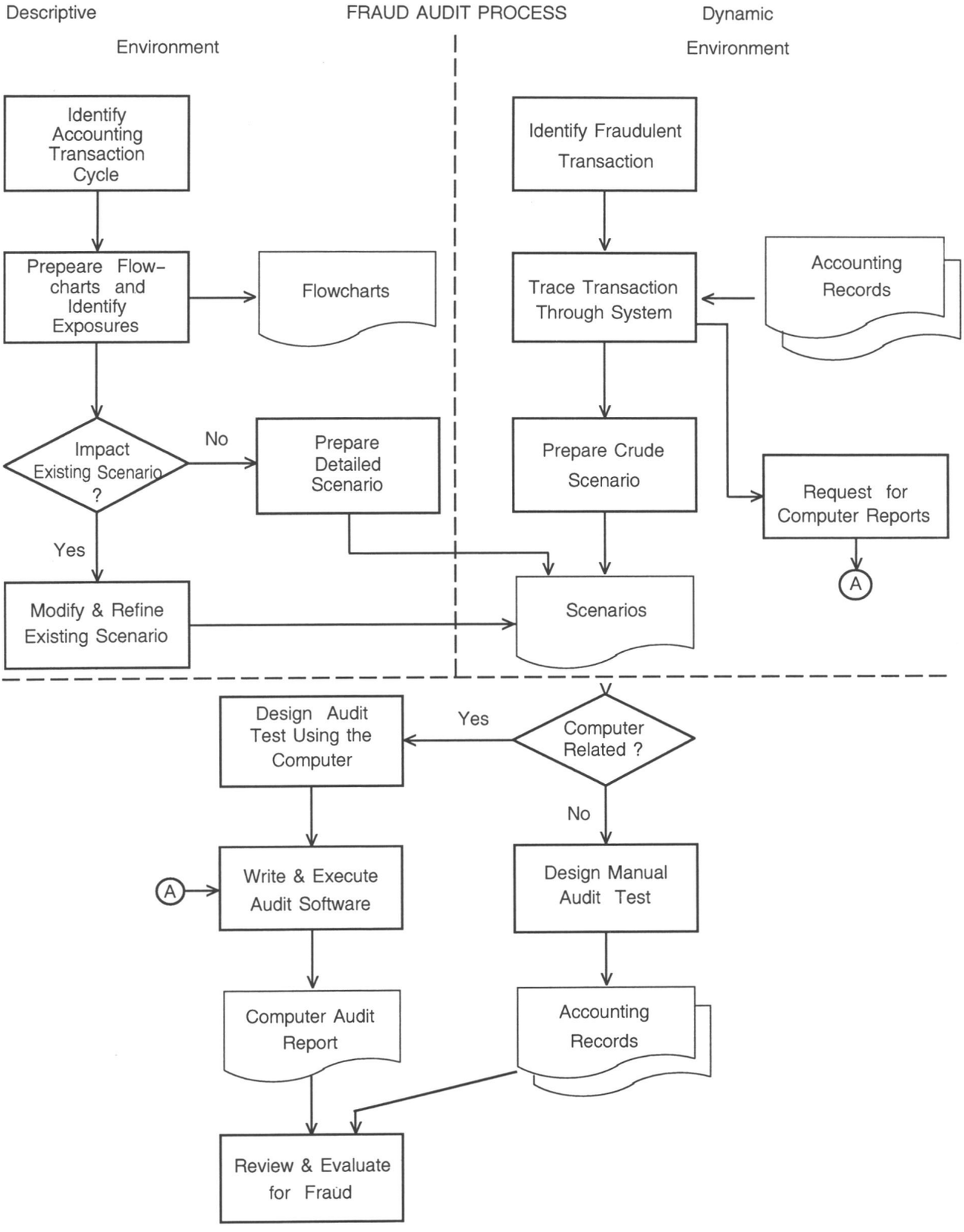
10.3 การเขียนเค้าโครงเรื่องของการทุจริต (Developing Fraud Scenarios) และการปฏิบัติงานของ EDP examiners และ Financial examiners

ในขั้นแรกที่พบว่ามีการทุจริตเกิดขึ้น ผู้ตรวจสอบก็ได้เขียนโครงเรื่องหยาบ ๆ ไว้แล้ว แต่ไม่มีเวลาที่จะเขียนรายละเอียดเพิ่มขึ้น เพราะจะต้องค้นหารายการทุจริตเพิ่มเติม ผู้ตรวจสอบด้านการเงินซึ่งทำหน้าที่ค้นหารายการทุจริตไม่มีพื้นความรู้เกี่ยวกับระบบคอมพิวเตอร์ จึงไม่สามารถเข้าใจระบบการบัญชีและการควบคุมภายในด้านคอมพิวเตอร์ จึงไม่อาจกำหนดรูปแบบและวิธีการตรวจสอบการทุจริตได้ ดังนั้นผู้ตรวจสอบด้านคอมพิวเตอร์ จึงต้องเข้ามาช่วยศึกษาระบบ และกำหนดรูปแบบของการทุจริตที่อาจจะเกิดขึ้นได้ และเป็นผู้แนะนำวิธีการตรวจสอบและแนวการตรวจสอบแต่ละขั้นตอนในเรื่องที่เกี่ยวข้องให้แก่ Financial examiner เพื่อการปฏิบัติงานการตรวจสอบร่วมกันด้วย และเพื่อให้เห็นภาพที่แท้จริง ผู้ตรวจสอบด้านคอมพิวเตอร์จะติดตามรายการข้อมูลแต่ละรายการของระบบงานตั้งแต่ต้นจนจบ และจะบันทึกวิธีปฏิบัติด้วยมือและเครื่องคอมพิวเตอร์ที่เกี่ยวข้อง พร้อมทั้งเอกสารหลักฐานที่จะใช้ตรวจสอบ (Audit Trail Documentation) จากข้อมูลอันนี้ผู้ตรวจสอบสามารถทราบได้ว่าใครคือผู้อนุมัติรายการทุจริตที่เกิดขึ้น และที่สำคัญมากไปกว่านี้คือ ผู้ตรวจสอบด้านคอมพิวเตอร์สามารถแยกรายการที่มีลักษณะเหมือนกับรายการทุจริตออกมาต่างหากได้

ลักษณะการตรวจสอบทุจริตแยกได้ออกเป็น 2 แบบ คือ

1) Dynamic คือ การให้ผู้ตรวจสอบคอมพิวเตอร์เป็นผู้ดึงรายการข้อมูลที่น่าสงสัย โดยพิจารณาจากลักษณะของรายการทุจริตที่เกิดมาแล้ว ส่งให้ผู้ตรวจสอบด้านการเงินตรวจสอบเอกสารหลักฐานเพิ่มเติม ในกรณีที่เป็นการทุจริตอันเกิดมาจากการแก้ไขข้อมูลที่บันทึกในคอมพิวเตอร์ ผู้ตรวจสอบด้านคอมพิวเตอร์จะต้องพิจารณาดูว่าเค้าโครงเรื่องของการทุจริตเหมือนกับที่เกิดมาแล้วหรือเป็นเรื่องใหม่

2) Descriptive คือ การให้ผู้ตรวจสอบด้านคอมพิวเตอร์เป็นผู้ศึกษาการควบคุมภายในระบบงานที่ใช้คอมพิวเตอร์อย่างกว้าง ๆ เพื่อปรับปรุงเค้าโครงเรื่องการทุจริตที่มีอยู่แล้วให้ดีขึ้น หรือกำหนดรูปแบบของการทุจริตอื่นที่อาจจะเกิดขึ้นได้ เครื่องมือที่จะช่วยให้ผู้ตรวจสอบบรรลุเป้าหมายคือ การทำผังการควบคุมภายใน (Control Flowcharting)


Descriptive
Environment
FRAUD AUDIT PROCESS
Dynamic
Environment
Identify Accounting Transaction Cycle
Prepeare Flow-charts and Identify Exposures
Flowcharts
Impact Existing Scenario ?
No
Prepare Detailed Scenario
Yes
Modify & Refine Existing Scenario
Identify Fraudulent Transaction
Trace Transaction Through System
Accounting Records
Prepare Crude Scenario
Request for Computer Reports
A
Scenarios
Computer Related ?
Yes
Design Audit Test Using the Computer
No
Design Manual Audit Test
A
Write & Execute Audit Software
Computer Audit Report
Accounting Records
Review & Evaluate for Fraud

10.4 การจัดทำผังการควบคุมภายในระบบงาน (Preparing Control Flowcharts)

เพื่อจะให้เข้าใจการควบคุมภายในระบบงานที่ใช้คอมพิวเตอร์เป็นอย่างดี จำเป็นต้องจัดทำผังแสดงรายละเอียดของการควบคุมของแต่ละระบบงาน ผังการควบคุมนี้จะแสดงวิธีการปฏิบัติงานทั้งหมดของระบบงานที่ใช้คอมพิวเตอร์ เมื่อประเมินจุดอ่อนและจุดแข็งของระบบเรียบร้อยแล้ว ผู้ตรวจสอบจะสามารถกำหนดรูปแบบของการทุจริตที่จะเกิดขึ้นได้

10.5 การใช้โปรแกรมตรวจสอบ (Using Audit Software)

ในการตรวจสอบการทุจริตเกี่ยวกับคอมพิวเตอร์ การวิเคราะห์และดึงข้อมูลออกมาจากเครื่องคอมพิวเตอร์ได้อย่างรวดเร็วและมีประสิทธิภาพเป็นสิ่งสำคัญ ดังนั้นถ้าหากไม่ใช้โปรแกรมตรวจสอบช่วยแล้ว ก็ไม่อาจตรวจสอบการทุจริตได้อย่างมีประสิทธิผล ผู้ตรวจสอบด้านคอมพิวเตอร์ที่ VSRS มีประสบการณ์ในการใช้โปรแกรมตรวจสอบมาแล้วมากกว่า 1 ปี ดังนั้นภายในเวลา 2 สัปดาห์ก็สามารถใช้โปรแกรมตรวจสอบออกรายงานต่าง ๆ ได้ประมาณ 150 ชนิด

10.6 การเข้าไปร่วมในการพัฒนาระบบงานใหม่ (Participating in New System Development)

จากผลของการทุจริตที่เกิดขึ้น VSRS จำเป็นต้องวางวิธีการควบคุมใหม่ภายในระบบ Refund โดยเร็วที่สุด ก่อนที่จะดำเนินการปรับปรุงแก้ไข ได้สั่งย้ายพนักงานของแผนก Refund Section ไปทำหน้าที่อื่น โดยให้ผู้ตรวจสอบด้านการเงินทำหน้าที่แทน สำนักงานสอบบัญชีดำเนินการวางระบบการควบคุมและวิธีปฏิบัติงานใหม่เสร็จภายใน 2 สัปดาห์ ผู้ตรวจสอบด้านคอมพิวเตอร์เป็นผู้ตรวจสอบและรับรองการเปลี่ยนแปลงนี้ และยังมีส่วนในการออกแบบและพัฒนาระบบงานร่วมกับบริษัทสอบบัญชีด้วย

11. ผลที่ได้จากการตรวจค้นการทุจริต (Results of the Fraud Investigation)

ผู้ตรวจสอบพบว่ามีการทุจริต 4 แบบ และจำนวนเงินที่ถูกยักยอกไปเท่ากับ US $111,149.92 เหรียญ ดังนี้

1. การแก้ไขรายการในสลิปถอนเงิน (The Alteration of Refund Vouchers)
2. การสร้างบัญชีสมาชิกปลอม (Creation of Fictitious Member Contribution Accounts)
3. การยักยอกเงินจากบัญชีที่ไม่เคลื่อนไหว (Looting Inactive Member Contribution Accounts)
4. การสร้างรายการถอนเงินปลอม (Creation of Fictitious Refund Voucher Transactions)

11.1 การแก้ไขรายการในสลิปถอนเงิน (The Alteration of Refund Vouchers)

การทุจริตวิธีนี้เกิดจากการที่เสมียนเพิ่มจำนวนในสลิปถอนเงินที่ส่งไปยัง สำนักงานคลังของ รัฐ เพื่อจ่ายเงินให้แก่สมาชิก ฝ่ายบริหารของ VSRS ไม่สามารถตรวจพบการทุจริตวิธีนี้ได้ เพราะการแก้ไขรายการในสลิปเกิดขึ้นหลังจากที่ผู้อำนวยการของ VSRS ได้ตรวจสอบและลงลายมือชื่อในสลิปเหล่านี้เรียบร้อยแล้ว ตัวอย่างเช่น แก้ไขจำนวนเงินในสลิปถอนเงินจาก US $1,444.49 เหรียญ เป็น US $ 7,444.49 เหรียญ เพิ่มขึ้น US $6,000 เหรียญ ผู้ตรวจสอบพบรายการทุจริตโดยเพียงแต่ตรวจสอบสลิปถอนเงินของ VSRS ทั้งหมดที่ส่งไปยังสำนักงานคลังของรัฐกับใบปะหน้า และรายชื่อของสมาชิกผู้รับเงินและจำนวนเงินที่ได้รับในรายงานคอมพิวเตอร์ ผู้ตรวจสอบยังค้นพบว่าอดีตพนักงานในแผนก Refund Section สองคนเป็นผู้กระทำการทุจริต และสามารถยักยอกเงินไปได้ US $62,797.72 เหรียญ ตั้งแต่วันที่ 1 มีนาคม ถึง 17 พฤษภาคม 2520

11.2 การสร้างบัญชีสมาชิกปลอม (Creation of Fictitious Member Contribution Accounts - MCA)

การตรวจพบว่ามีการแก้ไขจำนวนเงินในสลิป ทำให้ผู้ตรวจสอบเชื่อว่าต้องมีการทุจริตแบบอื่นอีกที่ใช้วิธีสร้างรายการแปลกปลอมเข้าไปเก็บไว้ใน Refund Systems ดังนั้นผู้ที่จะช่วยเหลือในการตรวจค้นการทุจริตวิธีนี้ก็คือผู้จัดการฝ่ายประมวลข้อมูล ซึ่งมีความรู้ความชำนาญทางด้านเทคนิคเกี่ยวกับระบบคอมพิวเตอร์ของ VSRS เป็นอย่างดี

จากคำบอกเล่าเกี่ยวกับลักษณะของรายการทุจริต ประกอบกับความรู้ความชำนาญด้านเทคนิค ทำให้ผู้จัดการฝ่ายประมวลข้อมูลสามารถดึงรายการทุจริตออกมาได้เพิ่มขึ้นอีก ซึ่งเป็นผลทำให้ผู้อำนวยการฝ่ายตรวจสอบและเจ้าหน้าที่ตำรวจเริ่มสงสัยผู้จัดการฝ่ายประมวลข้อมูล เนื่องจากสามารถค้นหารายการทุจริตได้รวดเร็วมาก และเท่ากับย้ำความคิดที่ว่าผู้ทุจริตต้องเป็นผู้ที่มีความเชี่ยวชาญด้านคอมพิวเตอร์ แต่ก็ไม่พบหลักฐานใดที่แสดงว่าผู้จัดการฝ่ายประมวลข้อมูลเป็นผู้ที่กระทำการทุจริตเอง

ลักษณะทั่ว ๆ ไปของบัญชีปลอมใน MCA master file มีดังนี้

1) บัญชีที่มี Status Code เป็น 3
2) ช่องที่ใช้สำหรับบันทึกจำนวนเงิน (Contribution Update File) มียอดเป็นศูนย์
3) ไม่มีแบบฟอร์มใบสมัครเป็นสมาชิก (VSRS-1)

จากลักษณะที่กล่าวนี้สรุปได้ว่า มีการจัดทำ VSRS-3 และคืนเงินให้แก่เจ้าของบัญชีรายซึ่งไม่เคยกรอกแบบฟอร์ม VSRS-1 และส่งรายงาน Contribution มาให้เลย ผู้จัดการฝ่ายประมวลข้อมูลชี้แจงให้ผู้ตรวจสอบทราบว่า การปฏิบัติเช่นนี้ไม่เป็นสิ่งผิดปกติแต่ประการใดในระบบการ Refund เพราะเพียงแต่ VSRS-3 อย่างเดียวก็สามารถใช้เป็นเอกสารหลักฐานสำหรับเปิดบัญชีได้ พนักงานซึ่งทำงานกับนายจ้างเป็นเวลา 1 ปี มีสิทธิที่จะกรอกแบบฟอร์ม VSRS-3 ได้ โดยที่ไม่เคยส่ง VSRS-1 หรือรายการ Contribution มาให้ VSRS แต่ก็ทำเป็นครั้งคราวเท่านั้น ผู้ตรวจสอบไม่ทราบวิธีปฏิบัติเช่นนี้เพราะในเอกสารประกอบระบบงานมิได้ระบุไว้ และไม่มีร่องรอยพอที่จะตรวจสอบได้

เสมียนในแผนก Refund ใช้วิธีการนี้ปลอมแปลงบัญชีขึ้นมา โดยการปลอม VSRS-3 ของนายจ้างราย Fairfax Country School Board ใช้ชื่อตนเอง เพื่อน และญาติ เป็นผู้รับเงิน ขณะที่ปลอม VSRS-3 ปรากฏว่านายจ้างรายที่กล่าวขาดส่งรายงาน Contributions ให้ VSRS เป็นเวลา 17 ถึง 18 เดือน เสมียนแผนก Refund เป็นผู้ที่นำ VSRS-3 มาเจาะลงบัตร แล้วส่งบัตรที่เจาะแล้วไปให้เจ้าหน้าที่ RJE ซึ่งจะเป็นผู้เรียกโปรแกรมคอมพิวเตอร์มาใช้ในการเพิ่มบัญชีเข้าไปใน MCA master file พร้อมกับออกรายงานรายการที่นำเข้าไปในคอมพิวเตอร์ เมื่อตรวจสอบความถูกต้องทางข้อมูลในรายงานเรียบร้อยแล้ว ก็จะทิ้งรายงานไปพร้อมกับบัตรเจาะ แล้วส่ง VSRS-3 คืนกลับไปยังแผนก Refund เพื่อดำเนินการตามปกติต่อไป หลังจากนั้นจะมีเช็คส่งไปยังที่อยู่ตามแบบฟอร์ม VSRS-3 ท่อนล่าง

วิธีตรวจค้นบัญชีปลอมที่ดีที่สุดคือ การใช้โปรแกรมดึงบัญชีที่มีลักษณะตามที่กล่าวข้างต้นออกมา ดังนั้น ผู้ตรวจสอบจึงตัดสินใจดึงบัญชีรายที่ไม่ได้ส่งรายงาน Contribution มาให้ VSRS ผู้ตรวจสอบไม่เลือกบัญชีซึ่งไม่มีใบ VSRS-1 เพราะเกรงว่าเสมียนแผนก Refund อาจจะปลอมแปลง VSRS-1 ขึ้นมาคู่กับบัญชีปลอมได้ แต่จะไม่สามารถแก้ไขข้อมูลในช่องที่ใช้บันทึกจำนวนเงินของแต่ละบัญชีในคอมพิวเตอร์ได้ หากไม่มีความรู้ด้านโปรแกรม ผู้ตรวจสอบใช้โปรแกรมเลือกดึงข้อมูลมาจาก MCA History Tape และ Current MCA master file จำนวนทั้งหมด 836 บัญชี ซึ่งไม่เคยมีรายการนำฝากเงินเลย (Contribution Transaction) จากการตรวจสอบบัญชีเหล่านี้พบว่ามีบัญชีปลอม 29 บัญชี ซึ่งใช้ในการยักยอกเงินได้ US $33,425.16 เหรียญ การทุจริตครั้งแรกเริ่มเมื่อเดือนพฤศจิกายน 2519 และครั้งสุดท้ายเมื่อเดือนพฤษภาคม 2520 ในกลุ่มแรกของบัญชีปลอมมีอยู่ 2 บัญชีที่มีชื่อและหมายเลขประกันสังคมเหมือนกัน และปรากฏอยู่ในรายงาน Possible Duplicate Accounts Report ที่ส่งให้แก่ Contribution Reporting Section แต่เนื่องจากแผนกนี้ไม่เคยส่งใบสอบถามไปยังนายจ้าง (Fairfax Country) เลย จึงไม่พบบัญชีปลอม 2 บัญชีนี้

11.3 การยักยอกเงินจากบัญชีที่ไม่เคลื่อนไหว (Looting Inactive Member Contribution Accounts)

ผู้ทุจริตได้หยุดการยักยอกเงินตามวิธีที่ 2 ในเดือนมิถุนายน 2520 เพราะนายจ้างที่เคยส่งรายงานล่าช้า รวมทั้ง Fairfax Country ได้ปรับปรุงการส่งรายงานให้เร็วขึ้นแล้ว จึงคิดว่าไม่มีทางยักยอกเงินได้อีก แต่ถ้าหากทราบว่าไม่มีการควบคุมภายในระบบ Refund เพียงพอที่จะค้นพบบัญชีปลอมได้ ก็คงจะยังทำเช่นนี้ต่อไป เวลาต่อมาเสมียนในแผนกคนหนึ่งได้ลาออกไป

ในระหว่างเดือนพฤษภาคมและมิถุนายน 2520 เจ้าหน้าที่ผู้ควบคุมการตรวจสอบ EDP ได้ทำการตรวจสอบเบื้องต้นเกี่ยวกับระบบงานที่ใช้คอมพิวเตอร์ ซึ่งรวมการสอบถามพนักงานในแผนก Refund ด้วย เมื่อผู้จัดการฝ่าย Operation ทราบว่าผู้ตรวจสอบกำลังให้ความสนใจเกี่ยวกับความอ่อนแอของการควบคุม ก็ได้ลาออกไปตอนปลายเดือนมิถุนายน 2520

ในเดือนกันยายน 2520 ก็มีรายการทุจริตแบบใหม่เกิดขึ้นอีก คราวนี้เป็นการลักลอบถอนเงินจากบัญชีสมาชิกรายที่ไม่มีรายการเคลื่อนไหวในแผนก MCA master file ผู้ตรวจสอบค้นพบการทุจริตวิธีนี้ได้โดยการคัดเลือกสลิปคืนเงินที่มีชื่อ L.A. Tanner ซึ่งเป็นชื่อบัญชีปลอมที่พบในการทุจริตกรณีอื่น ๆ ปรากฏว่ามีสลิปใบ

หนึ่งลงวันที่ 17 ตุลาคม 2520 ลงนาม L.A. Tanner และเมื่อสอบรายละเอียดในสลิปย้อนกลับไป แทนที่จะพบว่าเป็นรายการถอนเงินจากบัญชีปลอม กลับกลายเป็นรายการถอนเงินจากบัญชีที่ไม่เคลื่อนไหว ซึ่งยังคงมียอดคงเหลืออยู่และชื่อบัญชีในคอมพิวเตอร์ก็เป็นชื่อจริง แต่ในสลิปถอนเงินลงชื่อ L.A. Tanner

เมื่อผู้ตรวจสอบด้านคอมพิวเตอร์ทำการวิเคราะห์เพิ่มเติม ก็ทราบว่าการทุจริตเกิดขึ้นได้เพราะเสมียนในแผนก Refund เป็นผู้เจาะบัตรถอนเงินบางรายจากเอกสารเบื้องต้น (เช่น VSRS-3 หรือรายงานบัญชีที่ไม่เคลื่อนไหว) ซึ่งรวมถึงการเจาะรายชื่อลงบัตรด้วย เมื่อส่งบัตรที่เจาะแล้วไปเข้าเครื่องคอมพิวเตอร์โปรแกรมคอมพิวเตอร์จะพิมพ์รายงาน ชื่อ และจำนวนเงินที่ถอนคืน ตามข้อมูลในบัตรเจาะโดยที่ไม่ได้เช็คสอบกับชื่อและยอดคงเหลือในบัญชีที่แท้จริงในคอมพิวเตอร์ และถ้าหากจะมีผลต่างเกิดขึ้นก็ไม่มีใครตรวจพบ เพราะเสมียนเป็นผู้ควบคุมงานตั้งแต่ต้นจนจบ บัญชีที่ไม่เคลื่อนไหวเป็นบัญชีซึ่งไม่มีรายการฝากถอนมานานแล้ว และเจ้าของบัญชีบางรายสิ้นชีวิตไปแล้ว ผู้ที่มีสิทธิรับเงินจึงไม่ทราบยอดเงินคงเหลือในบัญชี ดังนั้นเสมียน Refund เพียงแต่เจาะชื่อปลอมลงในบัตรถอนเงินคืน (Refund Card) เท่านั้นก็ยักยอกเงินมาใช้ได้ นอกจากนี้ระบบคอมพิวเตอร์ของ VSRS ไม่มีโปรแกรมที่จะป้องกันการถอนเงินจากบัญชีที่มียอดคงเหลือเป็นศูนย์ ฉะนั้นเสมียนจึงสามารถถอนเงินออกไปจำนวนเท่าใดก็ได้ ไม่ว่าในบัญชีจะมียอดคงเหลือหรือไม่ก็ตาม

ผู้ตรวจสอบได้ดำเนินการค้นหารายการที่ทุจริตโดยยึดถือรายงานบัญชีไม่เคลื่อนไหวฉบับก่อนเป็นหลัก เพราะเชื่อว่าเสมียน Refund ใช้รายงานนี้เป็นแหล่งข้อมูลที่จะใช้ในการทุจริต ณ สิ้นเดือนมิถุนายน 2520 VSRS มีบัญชีไม่เคลื่อนไหวรหัส (Status) 3, 4 และ 5 ประมาณ 5,000 บัญชี ยอดคงเหลือในบัญชีเป็นบวกและลบทั้งสิ้นมากกว่า US $+200,000 เหรียญ และ US $-125,000 เหรียญ ตามลำดับ นอกจากนั้นยังมีบัญชีไม่เคลื่อนไหวรหัส 2 กว่า 62,000 บัญชี ยอดคงเหลือรวมมากกว่า US $100 ล้านเหรียญ เนื่องจากจำนวนบัญชีไม่เคลื่อนไหวมีมาก ดังนั้นผู้ตรวจสอบจึงใช้คอมพิวเตอร์ช่วยในการตรวจสอบและวิเคราะห์ ผู้ตรวจสอบ คอมพิวเตอร์ใช้โปรแกรมเปรียบเทียบรายการถอนเงิน (Refund Transactions) ใน History Tape กับบัญชีใน MCA master file ของปีปัจจุบันและปีก่อนที่มีหมายเลขประกันสังคมตรงกัน เสมียน Refund ไม่สามารถเปลี่ยนแปลงแก้ไขหมายเลขประกันสังคมได้เมื่อเจาะบัตรถอนเงินคืน เพราะหมายเลขประกันสังคมเป็นข้อบังคับส่วนหนึ่งของการนำข้อมูลเข้า MCA master file ตามระบบ ISAM ซึ่งไม่ยินยอมให้รายการที่ไม่มีหมายเลขประกันสังคมใน MCA master file เข้าไปในคอมพิวเตอร์

คอมพิวเตอร์จะดึงรายการถอนเงินใน History Tape ที่มีหมายเลขประกันสังคมเหมือนกับบัญชีใน MCA master file แต่มีชื่อสมาชิกเจ้าของบัญชีต่างกันออกมาประมาณ 3,000 รายการ และพิมพ์เป็นรายงานส่งให้ผู้ตรวจสอบด้านการเงิน (Financial Auditors) ทำการตรวจสอบความถูกต้องของรายการเหล่านี้ต่อไป อย่างไรก็ตามรายการถอนเงินซึ่งมีหมายเลขประกันสังคมและชื่อบัญชีเหมือนกันใน MCA master file ก็อาจจะเป็นรายการที่ทุจริตได้ เพราะอาจจะมีการส่งเช็คไปให้แก๊งของผู้ทุจริต ฉะนั้นวิธีที่จะค้นพบรายการทุจริตเช่นนี้ คือ สอบถามไปยังเจ้าของบัญชีว่าได้รับเงินที่ถอนไปหรือไม่ นับตั้งแต่เดือนกันยายน 2520 จนถึงมกราคม 2521 เสมียนและหัวหน้าแผนก Refund ยักยอกเงินไปได้เพียง US $10,670.40 เหรียญ ในนามของตนเอง ญาติและเพื่อน ๆ

11.4 การสร้างรายการถอนเงินปลอม (Creation of Fictitious Refund Voucher Transactions)

การทุจริตแบบที่สี่นี้ง่ายมาก หัวหน้าแผนก Refund เป็นผู้ที่ปลอมแปลงสลิปถอนเงินเอง โดยไม่ผ่านคอมพิวเตอร์ ประทับตรา "ด่วนมาก" (RUSH) ลงในสลิป แล้วส่งให้ผู้อำนวยการของ VSRS ลงนามอนุมัติ เพื่อส่งต่อไปให้สำนักงานคลังของรัฐและสำนักบัญชีกลางของรัฐ ต่อมาสำนักงานคลังของรัฐก็จะส่งเช็คมาให้ผู้ทุจริต หัวหน้าแผนก Refund กล้าทำวิธีนี้เพราะทราบจากการที่ได้พูดคุยกับผู้ตรวจสอบด้านการเงินระหว่างที่ทำการตรวจสอบเบื้องต้นเกี่ยวกับระบบ Refund ว่า ผู้ตรวจสอบไม่ทราบมาก่อนว่าการจัดทำสลิปถอนเงินด้วยมือสามารถกระทำได้

ผู้ตรวจสอบด้านการเงินเป็นผู้ค้นพบรายการทุจริตนี้ เพราะเป็นรายการที่ไม่เกี่ยวข้องกับคอมพิวเตอร์ โดยเลือกสลิปถอนเงินที่จัดทำด้วยมือมาตรวจสอบความถูกต้อง ผลปรากฏว่าหัวหน้าแผนก Refund ใช้วิธีนี้ขโมยเงินไป US $4,074.64 เหรียญ ตั้งแต่เดือนพฤษภาคมถึงธันวาคม 2520

12. สรุป

12.1 การตรวจสอบเพื่อค้นหารายการทุจริตทั้งหมดได้เสร็จสิ้นลงในเดือนพฤษภาคม 2521 สรุปได้ว่ามีผู้ทุจริตทั้งสิ้น 16 คน เป็นพนักงานของ VSRS 3 คน และบุคคลภายนอก 13 คน ถูกส่งฟ้องในข้อหาโจรกรรมและมีส่วนร่วมในการโจรกรรม ศาลพิพากษาให้จำคุกรวมทั้งสิ้น 50 ปี ผู้ที่ได้รับโทษหนักที่สุดคือ หัวหน้าแผนก Refund 8 ปี เสมียนแผนก Refund 2 คน คนละ 6 ปี จนถึงเดือนมิถุนายน 2521 ผู้ตรวจสอบก็กลับไปตรวจสอบด้านการเงินตามปกติต่อไปจนเสร็จสิ้นในเดือนพฤศจิกายน 2521 แล้วส่งรายงานงบแสดงฐานะการเงินของ VSRS พร้อมทั้งความเห็นของผู้สอบบัญชีให้แก่ฝ่ายบริหารของ VSRS

12.2 ในการตรวจสอบระบบคอมพิวเตอร์ของ VSRS ครั้งนี้ ผู้ตรวจสอบด้านคอมพิวเตอร์ได้พบอุปสรรคในการตรวจสอบที่สำคัญ 2 ประการ คือ

1. ฝ่ายบริหารของ VSRS ไม่ให้ความร่วมมือและแสดงอาการไม่พอใจที่ผู้ตรวจสอบเข้าไปแทรกแซงระบบคอมพิวเตอร์
2. เนื่องจาก VSRS จัดทำคู่มือประกอบระบบงาน (System Document) ไม่ดีพอ ดังนั้นความรู้เกี่ยวกับระบบงานส่วนใหญ่ได้มาจากการสอบถามพนักงานของ VSRS โดยตรง ผลเสียของการใช้วิธีการสอบถามก็คือ พนักงานของ VSRS จะทราบในระหว่างที่สอบถามว่าผู้ตรวจสอบยังไม่ทราบเรื่องใดบ้าง และจะพยายามไม่ตอบหรือเปิดเผยสิ่งที่นอกเหนือคำถาม ฉะนั้นจึงทำให้ผู้ตรวจสอบไม่สามารถเข้าใจระบบงานนั้นได้อย่างลึกซึ้งและมองข้ามจุดอ่อนบางอย่างไปได้

12.3 ความร่วมมือและการชี้แนะของ EDP examiner ต่อ Financial examiner เพื่อการตรวจสอบการทุจริตทางการเงิน มีความสำคัญยิ่งต่อความสำเร็จในการปฏิบัติงานครั้งนี้ ทั้งนี้เพราะการตรวจพบการทุจริตทั้ง 4 แบบ เป็นงานการตรวจสอบด้าน Financial แต่การ process งานด้านบัญชีกระทำโดยระบบคอมพิวเตอร์ ดังนั้นความร่วมมือและการประสานงานของผู้ตรวจสอบในแต่ละด้าน จึงเป็นสิ่งจำเป็นจะต้องดำเนินการควบคู่กันไปเสมอ

12.4 จุดอ่อนของระบบงานที่เป็นช่องทางให้เกิดการทุจริต

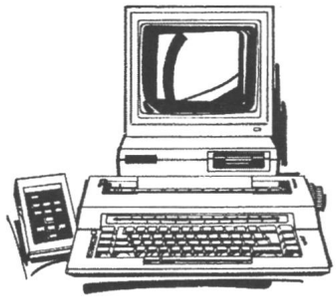
1. ไม่มีการควบคุมการเข้าและออก Storeroom ซึ่งเป็นห้องที่ใช้เก็บ VSRS-1 และ VSRS-3 ทำให้พนักงาน VSRS สามารถปลอมแปลงเอกสารดังกล่าวไปเก็บไว้ในห้อง หรือนำเอกสารออกมาใช้โดยไม่ได้รับอนุญาตหรือมีส่วนเกี่ยวข้อง เสมียนในแผนก Refund อาศัยจุดอ่อนนี้ปลอมแปลง VSRS-3 เพื่อสร้างบัญชีสมาชิกปลอมขึ้นตามข้อ 11.2

2. การยินยอมให้ถอนเงินก่อน และจะบันทึกหักบัญชีภายหลังเมื่อนายจ้างส่งรายงาน Contribution Report มาให้ครบถ้วนแล้ว เสมียนในแผนก Refund อาศัยจุดอ่อนนี้แก้ไขจำนวนเงินในสลิปถอนเงินโดยไม่ต้องพะวงว่ายอดในบัญชีจะมียอดคงเหลือพอหรือไม่ ตามข้อ 11.1

3. การยินยอมให้เสมียนในแผนก Refund เป็นผู้มีอำนาจเจาะบัตรถอนเงินในบัญชีที่ไม่เคลื่อนไหว และรายการถอนเงินนี้จะไม่ปรากฏใน Refund Inventory Tape เสมียนในแผนก Refund อาศัยจุดอ่อนนี้ยักยอกเงินจากบัญชีที่ไม่เคลื่อนไหวตามข้อ 11.3

4. การแบ่งแยกหน้าที่ในฝ่ายประมวลข้อมูลไม่เหมาะสม แผนก Contribution Reporting Section ซึ่งมีหน้าที่เกี่ยวกับการรับเงินฝากและถอนเงินฝากอยู่ภายใต้การบังคับบัญชาของผู้จัดการฝ่ายประมวลข้อมูล และฝ่ายประมวลข้อมูลยังมีหน้าที่รับผิดชอบเกี่ยวกับความถูกต้องของยอดรวมใน Control Book ด้วย

5. ผู้จัดการฝ่ายประมวลข้อมูลซึ่งเป็นผู้ที่เขียนโปรแกรม และวิเคราะห์ระบบงานสามารถเข้าไปใช้แฟ้มข้อมูลและโปรแกรมทั้งหมดโดยไม่จำกัด



บทที่ 19

คำแนะนำในการตรวจสอบ : การควบคุมภายในระบบบัญชีที่ใช้คอมพิวเตอร์

คำแนะนำในการตรวจสอบ : การควบคุมภายในระบบบัญชีที่ใช้คอมพิวเตอร์

คำนำ

มาตรฐานการสอบบัญชีได้กล่าวถึงหลักการขั้นพื้นฐานและวิธีการตรวจสอบ มาตรฐานว่าด้วยการปฏิบัติงานของผู้สอบบัญชีและคำแนะนำในการปฏิบัติงานของผู้สอบบัญชีสามารถนำไปใช้ได้ไม่ว่าระบบการบันทึกและการประมวลผลจะเป็นเช่นใด อย่างไรก็ตามในการตรวจสอบระบบที่ใช้คอมพิวเตอร์แม้ว่าคำแนะนำเกี่ยวกับการตรวจสอบโดยทั่ว ๆ ไปจะยังคงใช้ได้อยู่ แต่ก็เป็นการสมควรที่จะมีคำแนะนำบางอย่างเพิ่มเติม

จะถือว่าการตรวจสอบเป็นการตรวจระบบที่ใช้คอมพิวเตอร์ไม่ว่าการใช้คอมพิวเตอร์จะกระทำโดยกิจการนั้นเอง หรือจัดทำโดยสถานบริการ หลักการขั้นพื้นฐานในการสอบบัญชีมิได้เปลี่ยนไป แต่วิธีการตรวจสอบอาจจะเปลี่ยนไปบ้าง และผู้สอบบัญชีอาจจะต้องการความเชี่ยวชาญบางประการเพิ่มเติม

การนำคอมพิวเตอร์มาใช้ก่อให้เกิดการเปลี่ยนแปลงในวิธีการทางการบัญชี การเปลี่ยนแปลงนี้กระทบถึงวิธีการควบคุมภายในและหลักฐานที่จะใช้ในการตรวจสอบซึ่งจะผิดแปลกไปจากระบบเดิม ดังนี้

ก. ผลกระทบต่อการควบคุมภายใน

(1) การควบคุมภายในทั่วไปจะควบคุมการทำงานของคอมพิวเตอร์ เช่น การควบคุมการเปลี่ยนแปลงโปรแกรมคำสั่ง เพื่อให้มั่นใจว่าการประมวลผลเป็นไปอย่างถูกต้อง

(2) มีความเสี่ยงบางประการเกิดขึ้นจากการใช้คอมพิวเตอร์ประมวลผล เช่น การละเว้นรายการบางรายการจากการประมวลผล และการมีข้อผิดพลาดเกิดขึ้นซ้ำ ๆ กันอันเกิดจากระบบ

ข. ผลกระทบที่มีต่อหลักฐานในการตรวจสอบ

(1) อาจจะไม่มีหลักฐานให้มองเห็นที่แสดงว่าการประมวลผลได้ดำเนินไปอย่างถูกต้อง รวมทั้งการปฏิบัติการอื่น ๆ เช่น การวิเคราะห์ข้อมูล

(2) หลักฐานอาจจะปรากฏในแฟ้มคอมพิวเตอร์ชั่วระยะเวลาจำกัด

มาตรฐานในการปฏิบัติงานของผู้สอบบัญชีกำหนดว่า "หากผู้สอบบัญชีจะให้ความเชื่อถือในการควบคุมภายในแล้ว ผู้สอบบัญชีจะต้องสำรวจและประเมินการควบคุมภายในนั้นพร้อมทั้งทดสอบการปฏิบัติตามระบบ"

คำแนะนำในการสำรวจและประเมินการควบคุมภายในได้กล่าวไว้ในคำแนะนำว่าด้วยการควบคุมภายใน แต่เนื่องจากการควบคุมภายในสำหรับระบบบัญชีที่ใช้คอมพิวเตอร์แตกต่างจากการควบคุมภายในสำหรับระบบบัญชีที่ทำด้วยมือ ในคำแนะนำนี้จึงจะให้รายละเอียดเพิ่มเติมเกี่ยวกับการสำรวจประเมิน และทดสอบการควบคุมภายในสำหรับระบบบัญชีที่ใช้คอมพิวเตอร์

คำแนะนำนี้ใช้กับระบบบัญชีที่ใช้คอมพิวเตอร์ ไม่ว่าจะใช้เครื่องขนาดเล็กหรือใหญ่ ประมวลผลภายในกิจการนั้นเอง หรือใช้บริการประมวลผล ณ สถานบริการ วิธีการในการตรวจสอบจะแตกต่างกันออกไปตามลักษณะและความซับซ้อนของการประมวลผล แต่หลักการทั่วไปไม่เปลี่ยนแปลง

การควบคุมภายในระบบบัญชีที่ใช้คอมพิวเตอร์

การควบคุมภายในระบบบัญชีที่ใช้คอมพิวเตอร์มักจะพิจารณาภายใต้ 2 หัวข้อ คือ

ก. การควบคุมภายในเฉพาะระบบงาน (Application Controls)

ข. การควบคุมภายในทั่วไป (General Controls)

การควบคุมภายในเฉพาะระบบงานครอบคลุมเกี่ยวกับรายการและข้อมูลถาวรที่นำมาใช้ในการประมวลผลแต่ละครั้ง จึงเป็นการควบคุมเฉพาะเรื่อง วัตถุประสงค์ของการควบคุมภายในเฉพาะระบบงานนี้ก็เพื่อให้เกิดความมั่นใจเกี่ยวกับความสมบูรณ์และความถูกต้องของการบันทึกรายการทางการบัญชี และความถูกต้องของรายการอันเป็นผลของการประมวลผลทั้งด้วยมือและคอมพิวเตอร์ การควบคุมเฉพาะระบบงานอาจจะทำด้วยมือ เช่นการกระทบยอดรวมของข้อมูลนำเข้า หรืออาจทำโดยเครื่อง เช่น การตรวจทานความเหมาะสมของข้อมูลนำเข้าโดยโปรแกรมคำสั่ง

การควบคุมภายในทั่วไปครอบคลุมถึงสภาวะแวดล้อมในการพัฒนา รักษา และนำระบบงานมาใช้ และสภาวะแวดล้อมในการประมวลผล วัตถุประสงค์ของการควบคุมทั่วไปก็เพื่อก่อให้เกิดความมั่นใจในความถูกต้องของการพัฒนาระบบและการนำไปใช้ ความถูกต้องของโปรแกรมคำสั่งและแฟ้มข้อมูล และการประมวลผลการควบคุมภายในทั่วไปนี้อาจทำด้วยมือ เช่น การห้ามมิให้ผู้ไม่มีหน้าที่เข้าไปเกี่ยวข้องกับแฟ้มข้อมูล หรือทำโดยเครื่อง เช่น การใช้ password ในการใช้โปรแกรมคำสั่ง

แม้ว่าการควบคุมภายในทั่วไปจะครอบคลุมถึงระบบงานประมวลผลทั้งหมด แต่ระบบงานประมวลผลบางระบบอาจจะจำเป็นต้องมีมาตรการการควบคุมทั่วไปเพิ่มเติม เช่น การใช้ Password ในการใช้โปรแกรมคำสั่งและแฟ้มข้อมูลอาจจะจำเป็นเฉพาะการประมวลข้อมูลเกี่ยวกับค่าแรงเท่านั้นเป็นต้น

ความเชื่อมั่นของผู้สอบบัญชีที่มีต่อการควบคุมภายใน

วัตถุประสงค์ของผู้สอบบัญชีในการประเมินและทดสอบการควบคุมภายในก็เพื่อดูว่าตนจะสามารถเชื่อถือข้อมูลทางการบัญชีที่ได้จดบันทึกไว้นั้นได้มากน้อยเพียงใด ถ้าจากผลของการทดสอบการปฏิบัติตามระบบแสดงว่าการควบคุมภายในมีประสิทธิภาพเพียงพอที่จะให้ความมั่นใจในความถูกต้องและสมบูรณ์ของการบันทึกทางการบัญชีและความถูกต้องของรายการ ผู้สอบบัญชีก็จะจำกัดขอบเขตในการทดสอบความถูกต้องของรายการบัญชี

ในการพิจารณาความมีประสิทธิภาพของการควบคุมภายใน ผู้สอบบัญชีต้องคำนึงถึงทั้งการควบคุมภายในทั่วไปและการควบคุมภายในเฉพาะระบบงาน การจะเกิดความมั่นใจมากน้อยเพียงใดนั้นย่อมขึ้นอยู่กับการควบคุมภายในที่มีอยู่และค่าใช้จ่ายในการประเมินและทดสอบ หากสามารถเลือกได้ ผู้สอบบัญชีมักเลือกที่จะให้ตนได้รับความมั่นใจจากการควบคุมภายในเฉพาะระบบงานมากกว่าการควบคุมภายในทั่วไป ทั้งนี้เพราะการประเมินและทดสอบการ

ควบคุมภายในเฉพาะระบบงานมักจะได้ผลดีกว่าเมื่อมองในแง่ค่าใช้จ่ายที่ต้องเสียไป อย่างไรก็ตามในกรณีที่การควบคุมภายในเฉพาะระบบงานครอบคลุมถึงวิธีการใช้โปรแกรมคำสั่ง ผู้สอบบัญชีจำเป็นต้องพิจารณาถึงผลของการควบคุมภายในทั่วไปที่มีต่อวิธีการดังกล่าวด้วย

ในการประมวลผลบางระบบงาน การปฏิบัติงานบางอย่างอาจจะไม่อยู่ภายใต้การควบคุมภายในเฉพาะระบบงาน ตัวอย่างเช่น การคำนวณคูณราคาสินค้าในใบกำกับสินค้าอาจจะไม่มีการควบคุมที่จะให้มั่นใจว่าการคำนวณนั้นถูกต้อง หรือข้อมูลที่นำเข้าทาง terminal อาจจะไม่มีการรวมยอดก่อนนำเข้าเพื่อให้แน่ใจว่าได้มีการนำเข้าครบถ้วน เพื่อให้มั่นใจว่าการประมวลผลได้กระทำอย่างถูกต้อง ผู้สอบบัญชีอาจจะต้องให้ความสนใจกับการควบคุมภายในทั่วไปเกี่ยวกับความถูกต้องของการบันทึก ถ้าหากผู้สอบบัญชีประสงค์จะจำกัดขอบเขตการตรวจสอบความถูกต้องของรายการบัญชี

ในระบบที่ทำด้วยมือ ความผิดพลาดอาจเกิดขึ้นอย่างไม่สม่ำเสมอ อันเกิดจากความผิดพลาดของพนักงาน แต่ในระบบบัญชีที่ใช้คอมพิวเตอร์ โอกาสที่ความผิดพลาดจะเกิดขึ้นซ้ำแล้วซ้ำอีกอันเป็นผลจากการผิดพลาดในโปรแกรมคำสั่งหรือจากการทำงานที่ผิดปกติของเครื่องนั้นมีอยู่ เนื่องจากความผิดพลาดในลักษณะเช่นนี้อาจจะป้องกันหรือค้นหาได้โดยการควบคุมทั่วไปเกี่ยวกับการพัฒนาระบบและการนำระบบไปใช้ การควบคุมเกี่ยวกับโปรแกรมคำสั่งและแฟ้มข้อมูลและการประมวลผล ผู้สอบบัญชีจึงควรแสวงหาความมั่นใจเกี่ยวกับการควบคุมเหล่านี้

ความมั่นใจที่ผู้สอบบัญชีจะได้รับจากการควบคุมภายในทั่วไปเกี่ยวกับสภาวะแวดล้อมที่ระบบบัญชีที่ใช้คอมพิวเตอร์ปฏิบัติการอยู่ อาจจะอยู่ในขอบเขตจำกัด โดยเฉพาะในระบบที่ใช้เครื่องขนาดเล็ก การควบคุมภายในทั่วไปจะมีน้อยกว่าในระบบที่ใช้เครื่องขนาดใหญ่ ในสถานะการณ์เช่นนี้ผู้สอบบัญชีอาจจะสามารถจำกัดขอบเขตการทดสอบความถูกต้องของรายการบัญชีได้ด้วยการให้ความสนใจกับการควบคุมการประมวลผลในส่วนที่ทำด้วยมือ

การควบคุมบางประการ ไม่ว่าจะเป็นการควบคุมภายในเฉพาะระบบงานหรือการควบคุมภายในทั่วไป อาจจะอยู่ในมือของบุคคลที่สาม เช่น สถานบริการประมวลผล ในกรณีเช่นนี้ผู้สอบบัญชีอาจจะต้องสำรวจวิธีการปฏิบัติ ของกิจการที่ตนตรวจสอบเพื่อสำรวจการควบคุมภายใน หรือในบางกรณีที่เหมาะสม อาจจะประเมินและทดสอบ การควบคุม ณ สถานบริการ

วิธีการตรวจสอบที่เกี่ยวเนื่องกับการควบคุมภายใน

การสำรวจและการประเมินขั้นต้น

ก่อนที่จะทำการประเมินการควบคุมภายใน ผู้สอบบัญชีควรจะต้องทำการสำรวจเพื่อศึกษาถึงสภาวะการณ์การควบคุม ถ้าผลของการสำรวจนี้ชี้ให้เห็นว่ามีการควบคุมที่ผู้สอบบัญชีคิดว่าอาจให้ความเชื่อถือได้ ผู้สอบบัญชีก็จะทำการประเมินขั้นต้นเพื่อดูว่าการควบคุมนั้นมีอยู่และตนจะได้ทำการทดสอบการปฏิบัติตามต่อไป ในกรณีที่การสำรวจหรือการประเมินขั้นต้นแสดงให้เห็นว่าการควบคุมภายในบกพร่องหรือมีจุดอ่อน ผู้สอบบัญชีก็จะไม่ทดสอบการปฏิบัติตามระบบ แต่จะทำการทดสอบความถูกต้องของรายการทันที

ในการสำรวจผู้สอบบัญชีเพียงแต่ต้องการทราบและเข้าใจเรื่องราวโดยทั่ว ๆ ไป และไม่ต้องการทราบรายละเอียดเกี่ยวกับระบบการควบคุม เช่น อยากจะทราบแต่เพียงว่าการตรวจทานความถูกต้องของข้อมูลโดยโปรแกรมคำสั่งมีอยู่สำหรับข้อมูลนำเข้าที่สำคัญ แต่ไม่จำเป็นต้องทราบวิธีการตรวจทานข้อมูลแต่ละอย่างโดยละเอียด และวิธีการในการรายงานและติดตามรายการผิดปกติต่าง ๆ

ขั้นแรกในการประเมินการควบคุมภายในขั้นต้น คือ การสำรวจการควบคุมภายในเฉพาะระบบงาน ถ้าการควบคุมภายในด้านนี้ดี ผู้สอบบัญชีอาจคิดว่าตนอาจจะให้ความเชื่อถือในการควบคุมภายในนี้ได้ หากการควบคุมเฉพาะระบบงานครอบคลุมไปถึงการประมวลผลโดยคอมพิวเตอร์ผู้สอบบัญชีจำเป็นต้องประเมินผลของการควบคุมภายในทั่วไปที่มีต่อการประมวลผลนั้นด้วย เช่น ในการควบคุมเกี่ยวกับราคาสินค้าที่ส่งให้ลูกค้า เพื่อนำไปใช้ทำใบกำกับสินค้าอาจจะต้องมีการเปรียบเทียบรายการสินค้าและแฟ้มข้อมูลลูกค้า ผู้สอบบัญชีจึงต้องพิจารณาถึงการควบคุมภายในทั่วไปเกี่ยวกับการเปลี่ยนแปลงโปรแกรมคำสั่งและแฟ้มข้อมูลที่เกี่ยวข้อง ในบางกรณีการควบคุมภายในเฉพาะระบบงานเป็นการควบคุมวิธีการที่ทำด้วยมือ ในกรณีเช่นนี้ผู้สอบบัญชีอาจตัดสินใจว่าตนไม่ต้องให้ความสนใจในการควบคุมภายในทั่วไปมากนัก

ในกรณีที่ผู้สอบบัญชีสรุปว่าตนไม่สามารถเชื่อถือการควบคุมภายในเฉพาะระบบงานไม่ว่าในการประมวลผลทั้งหมดหรือเพียงบางส่วน ผู้สอบบัญชีอาจจะตัดสินใจว่าตนจะแสดงความเชื่อมั่นจากการทดสอบความถูกต้องของรายการบัญชีเท่านั้น หรือในทางตรงข้าม ผู้สอบบัญชีอาจคิดว่าตนจะสามารถให้ความเชื่อถือในระบบการควบคุมภายในทั่วไปและจำกัดขอบเขตการทดสอบความถูกต้องของรายการให้ลดน้อยลงได้ ถ้าหากว่าการควบคุมภายในทั่วไปดูน่าจะเชื่อถือได้ ในกรณีเช่นนี้ผู้สอบบัญชีจะประเมินและทดสอบการควบคุมภายในทั่วไปที่นำมาใช้ในการประมวลผล

การทำเอกสารเกี่ยวกับการตรวจสอบ

ทั้งในการสำรวจและประเมินการควบคุมในขั้นต้น การจัดทำเอกสาร ซึ่งจะช่วยชี้ให้เห็นว่าการควบคุมภายในรายการใดที่ผู้สอบบัญชีอาจจะให้ความเชื่อถือได้ จะช่วยผู้สอบบัญชีได้มาก การจัดทำเอกสารดังกล่าวอาจจะจัดทำได้หลายรูปแบบ เช่น อาจจะประกอบด้วยคำถามที่ถามว่ามีการควบคุมใดบ้างในระบบ ซึ่งจะช่วยให้วัตถุประสงค์ในการควบคุมเป็นผลสำเร็จ หรือที่อาจจะป้องกันหรือค้นพบข้อผิดพลาดบางประการตามที่ระบุไว้ หรือป้องกันมิให้มีการละเลยบางรายการไปเสียได้

สำหรับการควบคุมภายในเฉพาะระบบงาน คำถามเกี่ยวกับการควบคุมภายในอาจจะครอบคลุมทั้งการประมวลผลด้วยมือและด้วยคอมพิวเตอร์



การทดสอบ

ในระบบบัญชีใดก็ตาม ผู้สอบบัญชีทดสอบการปฏิบัติงานระบบเพื่อให้มั่นใจว่าการควบคุมภายในที่ตนคิดว่าจะให้ความเชื่อถือนั้นได้มีการปฏิบัติตามอย่างถูกต้องและสม่ำเสมอตลอดระยะเวลาที่ตนต้องให้คำรับรอง ในการทดสอบการปฏิบัติตามระบบผู้สอบบัญชีควรจะพยายามหาหลักฐานที่ตรงกับจุดที่ตนต้องการทดสอบการควบคุม ดังนั้นการทดสอบนี้จึงมักจะคลุมถึงการสังเกตการปฏิบัติงานเกี่ยวกับการควบคุมและ/หรือการตรวจเอกสารหลักฐานเกี่ยวกับการปฏิบัติงาน

เนื่องจากระบบคอมพิวเตอร์อาจจะมีหลักฐานการปฏิบัติงานอยู่ไม่มากนัก ผู้สอบบัญชีอาจพบว่าหลักฐานที่มีอยู่ไม่เพียงพอที่จะให้ความมั่นใจตามที่ต้องการ ในกรณีเช่นนี้ผู้สอบบัญชีอาจจะต้องการหลักฐานเพิ่มเติมจากวิธีการอื่น เช่น ลองปฏิบัติการเกี่ยวกับการควบคุมนั้นด้วยตนเอง การขาดหลักฐานที่เป็นเอกสารนี้อาจจะกระทบกระเทือนการควบคุมภายในเฉพาะระบบงาน แต่มักจะพบมากเกี่ยวกับการควบคุมภายในทั่วไป

การทดสอบการปฏิบัติตามระบบที่ให้หลักฐานเกี่ยวกับการควบคุมภายในเฉพาะระบบงานในส่วนที่ทำด้วยมืออาจจะกระทำในลักษณะเดียวกับการทดสอบการควบคุมในระบบบัญชีที่ทำด้วยมือ และอาจจะคลุมถึงวิธีการทดสอบการกระทบยอดรวมของข้อมูลนำเข้า เป็นต้น ในกรณีของการควบคุมภายในเฉพาะระบบงานที่ควบคุมด้วยโปรแกรมคำสั่ง เช่น การตรวจทานความถูกต้องของข้อมูลนำเข้า (edit check) ผู้สอบบัญชีอาจจะหาหลักฐานในการปฏิบัติหน้าที่เช่นนี้ไม่เพียงแต่โดยการตรวจดูรายงานการประมวลผลที่พิมพ์ออกมา แต่อาจจะใช้การตรวจสอบโดยใช้คอมพิวเตอร์เพื่อให้ได้หลักฐานของการปฏิบัติหน้าที่ในการควบคุม

ลักษณะของการทดสอบการปฏิบัติตามระบบการควบคุมภายในทั่วไปย่อมขึ้นอยู่กับระดับความเชื่อถือที่ผู้สอบบัญชีคิดว่าตนอาจจะมีต่อการควบคุมภายในทั่วไปนี้ ดังนั้นเมื่อผลของการประเมินการควบคุมมีว่าผู้สอบบัญชีจะให้ความเชื่อถือในการควบคุมภายในทั่วไปนี้ในขอบเขตจำกัด การสอบถามและการสังเกตการณ์เกี่ยวกับการควบคุมภายในทั่วไปในการสำรวจขั้นแรก หรือในระหว่างการทดสอบการปฏิบัติตามระบบการควบคุมภายในเฉพาะระบบงานก็นับว่าเพียงพอแล้ว

สรุปได้ว่าการทดสอบการปฏิบัติตามระบบและการทดสอบความถูกต้องของรายการจะทำมากน้อยเพียงใด และการทดสอบการควบคุมภายในทั่วไปและการควบคุมภายในเฉพาะระบบงานจะทำมากน้อยเพียงใดย่อมขึ้นอยู่กับความสัมพันธ์ระหว่างการควบคุมภายในทั่วไปและการควบคุมภายในเฉพาะระบบงาน ความลำบากในการทดสอบการควบคุมภายในทั่วไป และเทคนิคการตรวจสอบโดยคอมพิวเตอร์นี้จะสามารถนำมาใช้ได้

เรียบเรียงจาก Auditing Guidelines : Internal Controls in computer based accounting systems. – Exposure draft. January 1982. The Institute of Chartered Accountant in England and Wales

บทที่ 20

การป้องกันอาชญากรรมคอมพิวเตอร์ และสิ่งที่ผู้บริหารควรพิจารณาดำเนินการ

การป้องกันอาชญากรรมคอมพิวเตอร์ และสิ่งที่ผู้บริหารควรพิจารณาดำเนินการ

1. การป้องกันอาชญากรรมคอมพิวเตอร์

1.1 การใช้คอมพิวเตอร์ทำให้ข้อมูลมารวมกันอยู่ที่จุดเดียวหมด
- ควรป้องกัน File Library ให้รัดกุม

1.2 การใช้คอมพิวเตอร์ช่วยให้ซุกซ่อนความผิดได้ง่าย
- ข้อมูลอยู่ในจานแม่เหล็กมองไม่เห็นด้วยตาเปล่า จึงต้องมีโปรแกรมตรวจสอบอย่างดี

1.3 การใช้คอมพิวเตอร์ช่วยให้สามารถแก้ไขโปรแกรมและข้อมูลโดยไม่ทิ้งร่องรอยไว้มาก
- จะต้องจัดให้มีรหัสลับสำหรับผู้ที่จะมีสิทธิแก้ไขข้อมูลและโปรแกรม
- จัดให้คอมพิวเตอร์บันทึกการแก้ไขเอาไว้เป็น Exception Report

1.4 การใช้คอมพิวเตอร์ช่วยให้สามารถทำลายหลักฐานได้ง่ายดาย
- แก้ไขได้โดยการจัดทำ Back up Copy และมีการตรวจสอบ Back up Copy เป็นระยะ ๆ

1.5 การใช้คอมพิวเตอร์ในระบบ On-Line มักจะมีการตรวจสอบข้อมูลน้อยกว่าระบบธรรมดา
- ใช้บุคคลควบคุมในการส่งข้อมูลเข้า
- ใช้ program ควบคุมในการส่งข้อมูลเข้า
- ใช้ password ควบคุม

1.6 การใช้คอมพิวเตอร์ทำให้ชาวบ้านเชื่อถือมากเกินไป
- แก้ไขโดยการประชาสัมพันธ์ให้ผู้ใช้ทั่วไปทราบว่า คอมพิวเตอร์ก็ผิดได้ ถ้ามีคนสั่งทำให้ผิด

1.7 การใช้คอมพิวเตอร์ทำให้ควบคุมข้อมูลลำบาก
- ข้อมูลที่เก็บเป็นจานแม่เหล็กบางชุดอาจต้องอยู่ในสถานที่คอมพิวเตอร์เรียกใช้ตลอดเวลา (On-Line) ผู้ที่มี Terminal อาจติดต่อหรือคัดลอกข้อมูลได้ แก้ไขได้โดยการแปลข้อความเป็นรหัส

1.8 การใช้คอมพิวเตอร์บางแห่งทำให้ไม่มีการแยกความรับผิดชอบ
- แก้ได้โดยการจัดแบ่งหน้าที่พนักงานเตรียมข้อมูล ไม่ให้คนเดียวมีสิทธิทำได้ทุกอย่าง

1.9 การออกแบบระบบคอมพิวเตอร์มักจะไม่คำนึงถึงการตรวจสอบ
- จัดให้มีผู้ตรวจสอบร่วมพัฒนาระบบงานด้วย

2. สิ่งที่ผู้บริหารควรพิจารณาดำเนินการ

- ผู้ตรวจสอบภายในด้านคอมพิวเตอร์ควรจะได้มีบทบาทมากขึ้นในด้านการป้องกันการทุจริต และควรจะได้มีจำนวนเพิ่มขึ้นอย่างเร่งด่วนตามปริมาณการใช้คอมพิวเตอร์
- ผู้บริหารควรจะได้ให้ความสนใจในด้านการตรวจสอบงาน และข้อสังเกตของผู้ตรวจสอบทางด้านคอมพิวเตอร์มากขึ้น โปรดอย่าได้เร่งรัดพัฒนางานจนลืมนึกถึงผลกระทบต่อองค์กรที่เกิดขึ้นจากจุดอ่อนในการพัฒนาระบบงานตั้งแต่ต้น
- องค์กรไม่ควรพึ่งพาบุคลากรภายนอก หรือผู้ให้บริการทางด้านคอมพิวเตอร์จนเกินควร องค์กรพึงตระหนักว่าผู้ที่มีความเชี่ยวชาญทางด้านคอมพิวเตอร์หรือผู้สันทัดกรณีทางด้านขายอุปกรณ์เทคนิคคอมพิวเตอร์ ไม่สามารถจะช่วยงานด้านพัฒนาขององค์กรได้มากนัก หากผู้ให้บริการไม่มีความรู้ความชำนาญงานในระบบงานขององค์กรดีพอโดยเฉพาะอย่างยิ่งระบบงานทางด้านธนาคารพาณิชย์และสถานบันการเงิน
- องค์กรพึงตระหนักว่า บุคลากรภายในองค์กรจะมีความเข้าใจในระบบงานภายในขององค์กรได้มาก หากเขาเหล่านั้นสามารถจะเข้าใจระบบงานทางด้านคอมพิวเตอร์และสามารถประยุกต์การปฏิบัติงานให้เข้ากับระบบงานด้านคอมพิวเตอร์ได้
- การแลกเปลี่ยนทักษะระหว่างหน่วยงานที่ใช้คอมพิวเตอร์เป็นสิ่งจำเป็น
- องค์กรที่ใช้เครื่องคอมพิวเตอร์ขนาดเล็ก ควรจะระมัดระวังเป็นพิเศษ



บทที่ 21

องค์ประกอบสำคัญในการประมวลข้อมูลโดยระบบคอมพิวเตอร์

องค์ประกอบสำคัญในการประมวลข้อมูลโดยระบบคอมพิวเตอร์

ประกอบด้วย Hardware, Software และ Firmware

Hardware หมายถึงส่วนประกอบของระบบคอมพิวเตอร์ที่ทำงานเฉพาะอย่าง เช่น หน่วยประมวลผลข้อมูลกลาง หน่วยบันทึกความจำ เครื่องขับจานแม่เหล็ก และเครื่องพิมพ์ เป็นต้น

Software คือโปรแกรมควบคุมระบบงาน และโปรแกรมประยุกต์ที่ทำหน้าที่สั่งงานในการทำงานของ hardware

Firmware ประกอบด้วยโปรแกรมภาษาเครื่องที่ใช้ควบคุมการทำงานของ Hardware และขึ้นกับโปรแกรมควบคุมระบบหรือโปรแกรมใช้งาน ที่บรรจุไว้อย่างถาวรในส่วนความจำของตัวเครื่อง นอกจากนี้ ยังมีอุปกรณ์ที่สำคัญของ hardware คือ หน่วยบันทึกความจำข้อมูล (Storage) ซึ่งสามารถเก็บไว้ได้เป็นเวลานานบนแผ่นจานแม่เหล็กชนิดอ่อน (diskette) หรือบนเทปตลับและเทปแม่เหล็ก เป็นต้น ข้อมูลจะถูกเก็บในหน่วยข้อมูลหลัก (primary storage) จากนั้นจะถ่ายข้อมูลเป็นส่วน ๆ จาก file ซึ่งมีข้อมูลมากเกินส่วนความจำหลัก เข้าและออกในหน่วย real storage เพื่อทำการประมวลผลต่อไป

การตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ ที่มีขอบเขตการตรวจสอบทั้งศูนย์คอมพิวเตอร์ (Data Center) และระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ (Application) ในบางกรณีอาจต้องตรวจสอบให้เข้าถึงระบบการบริหารข้อมูล (Operting System) เช่น MVS/OS (Multiple Vertual Storage Operating System) คือระบบการบริหารข้อมูลที่มีความสามารถสูงในการควบคุมการทำงานของหลายงานในเวลาเดียวกันได้ กล่าวคือ หน่วยบันทึกข้อมูลหลายหน่วยทำงานประสานกันในรูปของ multiprograming คือ โปรแกรมจากผู้ใช้หลายคนป้อนข้อมูลเข้ามาพร้อมกันเพื่อทำการประมวลผลประสานงานกันไป (multiprocessing)

ผู้เป็นต้นคิดการทำงานแบบ MVS คือ IBM สร้างขึ้นสำหรับประมวลผลที่ใช้ปริมาณมากและช่วยประหยัดเวลาในการประมวลผลให้เหลือน้อยลง พร้อมกันนี้ยังมีโปรแกรมสำเร็จรูปที่ทำหน้าที่ควบคุมการบริหารข้อมูล และช่วยให้การประมวลผลเกิดความคล่องตัวขึ้น เช่น การปรับข้อมูลให้ทันต่อเวลา และการจัดคิวลำดับความสำคัญของข้อมูลตามคำสั่งโปรแกรมที่สร้างไว้ เป็นต้น

หลักการทำงานของ MVS สามารถแยกเป็น 5 จุด คือ

1. Supervisor : ทำหน้าที่ควบคุมการทำงานของ multiprogramming ให้งานเป็นไปตามขั้นตอนแต่ละโปรแกรม
2. Master Scheduler : มีหน้าที่รับผิดชอบในการเริ่มทำงาน และติดต่อกับ operator และสั่งงานตามสายงานในหน่วยข้อมูล (Vertual Storage)
3. Job Entry Subsystem : ช่วยให้การทำงานอยู่ในข่ายระบบงานเดียวกัน และส่งผลลัพธ์กลับไปยัง user ได้ โดยมีโปรแกรม System Management Facility ทำหน้าที่เก็บรวบรวมข้อมูลต่าง ๆ มาวิเคราะห์เพื่อส่งต่อให้ user ต่อไป

4. Data management : ควบคุมการจัดการ file และข้อมูล I/O ทั้งหมด โดยมี Utility Programs ช่วยในการจัด Copy files และจัด Catalog โปรแกรมให้ทันต่อเวลา และมี System Support Programs ทำหน้าที่อำนวยความสะดวกในการ load โปรแกรมอื่น ๆ ได้อีก
5. Telecommunication : เป็นสื่อการติดต่อระหว่างเครื่อง terminal จากศูนย์ต่าง ๆ มาที่ Host

ตัวอย่างการตรวจสอบขั้นตอนการปฏิบัติงานคอมพิวเตอร์ (Computer Operation)

การตรวจสอบในขั้นต้นนั้น ผู้ตรวจสอบอาจจะเริ่มตรวจจาก Audit log คือ บันทึกตารางการทำงานประมวลผลของเครื่องว่าเป็นไปตามที่ตารางจัดไว้ โดยเริ่มจากการขอดูการจัดตารางการประมวลผล และงานที่ทำนี้มีการ run งานจริงหรือไม่ เพราะทุกครั้งที่มีการประมวลผลเกิดขึ้น เครื่องจะบันทึก วัน วันที่ เดือน ปี เวลา และชื่องานที่ทำทุกครั้ง ผู้ตรวจสอบอาจจะตรวจได้โดยใช้วิธีสุ่มวันที่ที่ต้องการ หรือใช้วิธีตรวจทานว่าได้มีการทำงานขึ้นจริงในแต่ละวัน

คำอธิบายศัพท์และลักษณะการทำงานในระบบคอมพิวเตอร์ที่สำคัญ

interrupt handlers	:	คือสัญญาณที่ถูกส่งโดยโปรแกรม เพื่อขัดจังหวะการทำงานของเครื่องคอมพิวเตอร์ และขอให้ไปทำงานอื่น เมื่องานที่ทำแทนสำเร็จแล้ว เครื่องคอมพิวเตอร์จะกลับไปทำงานเดิมที่ยังค้างอยู่
External interrupt	:	คือสัญญาณที่เข้าระบบคอมพิวเตอร์และปรากฏบนจอภาพ เพื่อแจ้งให้ทราบว่ามีงานสำคัญกว่าที่ต้องเข้าประมวลผลแทนงานเดิม
Machine Interrupt	:	คือสัญญาณแจ้งที่จอภาพว่า เครื่องคอมพิวเตอร์มีเหตุข้อข้อง ณ จุดใดจุดหนึ่งในระบบเครื่อง
Program Interrupt	:	คือการขัดข้องในระหว่างการประมวลผล (run process) เช่น มีการใช้รหัสผิดคำสั่ง
I/O Interrupt	:	คือการขัดข้องที่เกิดในช่วงระหว่างการป้อนข้อมูลเข้าและส่งผลข้อมูล ณ จุด hardware โดยจะส่งสัญญาณมาที่ตัว CPU
SVC (Supervisor Call) Interrupt	:	คือสัญญาณเตือนเมื่อ User พยายามที่จะใช้คำสั่งของโปรแกรมบริหารข้อมูลโดยไม่มีสิทธิใช้ ตัว Supervisor Call จะทำหน้าที่ควบคุมการทำงานของ User ที่ไม่มีอำนาจเข้าถึงงานบางด้าน
VSAM (Virtual Storage Access Method)	:	คือวิธีการทำงานของ file ใน Virtual Storage ที่ถูกสร้างขึ้นสำหรับการบริหารข้อมูลเฉพาะ IBM/370 เป็นส่วนใหญ่
VTAM (Virtual Tele-communication Access Method)	:	คือระบบสื่อสารที่สร้างขึ้นในส่วนของ host processor ข้อมูลที่เข้ามาอาจจะเก็บอยู่ใน record mode โดยผ่านคำสั่ง SEND หรือ RECEIVE หรือเก็บใน basic mode โดยผ่านคำสั่ง READ และ WRITE

บทที่ 22

เทคนิคในการนำคอมพิวเตอร์มาใช้ในงานตรวจสอบ
(COMPUTER-ASSISTED AUDIT TECHNIQUES)

เทคนิคในการนำคอมพิวเตอร์มาใช้ในงานตรวจสอบ (COMPUTER-ASSISTED AUDIT TECHNIQUES)

เนื่องจากได้มีการนำเอาคอมพิวเตอร์มาใช้มากขึ้นในการประมวลผลทางการบัญชีของลูกค้า ทำให้ผู้สอบบัญชีจำเป็นต้องนำวิธีการตรวจสอบโดยใช้คอมพิวเตอร์มาช่วยในการตรวจสอบด้วย เพื่อเป็นการเพิ่มประสิทธิภาพของการตรวจสอบ

ผู้สอบบัญชีสามารถใช้เทคนิคต่าง ๆ ของการตรวจสอบด้วยคอมพิวเตอร์ในการตรวจสอบการควบคุมภายในเฉพาะระบบงาน โดยมีวัตถุประสงค์ดังต่อไปนี้

1. ใช้ตรวจสอบความถูกต้องของการประมวลผลที่ทำโดยมือและหรือโดยคอมพิวเตอร์
2. เพื่อตรวจสอบผลของการประมวลผล

การเลือกเทคนิคที่จะใช้ตรวจสอบ

ในการที่ผู้สอบบัญชีจะเลือกเทคนิคใดนั้น ผู้สอบบัญชีจะต้องเข้าใจในขั้นตอนของการประมวลผลที่สำคัญ และการควบคุมของระบบที่ต้องการตรวจสอบ การตรวจสอบสิ่งต่าง ๆ เหล่านี้อาจหาได้จากผังระบบงาน และตารางแสดงการควบคุมภายใน

I. เทคนิคในการรวบรวมข้อมูล (TECHNIQUES FOR GATHERING INFORMATION)

1. สำรวจรายละเอียดของโปรแกรมคำสั่ง (Program Listing Review)

การสอบทานจากรายละเอียดของโปรแกรมคำสั่ง (Program listing หรือที่เรียกกันว่า deck checking หรือ program code checking) ให้ข้อมูลเกี่ยวกับการประมวลผลของคอมพิวเตอร์ วิธีนี้ ผู้สอบบัญชีจะอ่านและวิเคราะห์รายละเอียดของรหัสของโปรแกรมคำสั่งที่เขียนโดยโปรแกรมเมอร์ เทคนิคนี้ต้องการคนที่ได้รับการอบรมในหลักการของการตรวจสอบและมีความชำนาญในการเขียนโปรแกรมมาก จะต้องมีความรู้ในรายละเอียดของภาษาที่ใช้ในการเขียนโปรแกรม ระบบการทำงานของเครื่อง และตัวเครื่องคอมพิวเตอร์ที่ใช้



สรุปวัตถุประสงค์ เทคนิค และเครื่องมือของการตรวจสอบ

วัตถุประสงค์	เทคนิค	เครื่องมือ
การรวบรวมข้อมูลเพื่ออธิบายถึงการควบคุมภายใน	สำรวจรายละเอียดของโปรแกรมคำสั่ง (Review program listing)	
	สำรวจจากผังโปรแกรมคำสั่ง (Reveiew logic flowchart)	โปรแกรมคำสั่งทำ Flowchart
การทดสอบวิธีการประมวลผล	การตรวจสอบโดยไม่ใช้คอมพิวเตอร์ในการตรวจสอบ (Audit around)	
	การใช้ข้อมูลทดสอบ (Test data)	โปรแกรมคำสั่งเพื่อทดสอบข้อมูล โปรแกรมคำสั่งเพื่อการสอบบัญชี
	การทดสอบข้อมูลจำลองร่วมกับข้อมูลจริง (Integrated test facility (ITF))	
	การใช้โปรแกรมจำลองขนานกับโปร-แกรมที่ใช้อยู่ในการประมวลผล (Parallel simulation)	โปรแกรมคำสั่ง เพื่อการสอบบัญชี โปรแกรมคำสั่งที่ดัดแปลงแล้ว
	การสร้างแฟ้มเพื่อการตรวจสอบสำหรับการควบคุมในระบบ (SCARF)	
	การรายงานในแต่ละขั้นตอนของการประมวลผล (Snapshot)	
การทดสอบผลสัพธ์	การขอคำยืนยันยอด (Confirmation)	โปรแกรมคำสั่งเพื่อการสอบบัญชี โปรแกรมคำสั่งที่ดัดแปลงแล้ว
	การเปรียบเทียบ (Comparison with file or physical)	โปรแกรมคำสั่งเพื่อการสอบบัญชี โปรแกรมคำสั่งที่ดัดแปลงแล้ว
	การทดสอบความสมเหตุสมผลและความถูกต้อง (Edit & reasonableness tests)	โปรมแกรมคำสั่งเพื่อการสอบบัญชี โปรแกรมคำสั่งที่ดัดแปลงแล้ว

ความยุ่งยากของเทคนิคนี้ อยู่ที่ระดับความชำนาญของผู้สอบบัญชี เนื่องจากมีคนไม่มากนักที่มีความรู้ดีเพียงพอที่จะทำได้ นอกจากนี้ ยังมีความลำบากอย่างมากในการตรวจสอบความถูกต้องสมเหตุสมผลของโปรแกรมจากรายละเอียดของโปรแกรมคำสั่ง แม้แต่โปรแกรมเมอร์ซึ่งเป็นผู้เขียนโปรแกรมนั้นเอง ก็ยังพบความยุ่งยากเมื่อย้อนกลับมาอ่านคำสั่งที่ตนเขียนไว้ในภายหลัง ด้วยเหตุนี้เมื่อคำนึงถึงโปรแกรมที่ต้องตรวจสอบในแต่ละระบบงาน ซึ่งมีอยู่มากมาย และเวลาที่ต้องใช้วิธีนี้จึงไม่เหมาะสมในแง่ของความประหยัด

2. สำรวจจากผังโปรแกรมคำสั่ง (Program Flowchart Review)

การรวบรวมรายละเอียดข้อมูล อาจทำได้โดยการตรวจสอบขั้นตอนต่าง ๆ ของผังโปรแกรมคำสั่ง (Program Flowchart) มีโปรแกรมคำสั่ง (Software) บางชนิดที่สามารถสร้างผังโปรแกรม (Flowchart) จากโปรแกรมคำสั่งที่ต้องการได้ ข้อดีของการสอบทานจากผังโปรแกรม คือ ทำความเข้าใจความสมเหตุสมผลของโปรแกรมได้ง่ายกว่าการสอบทานจากรายละเอียดของโปรแกรมคำสั่ง อย่างไรก็ดี การสอบทานผังโปรแกรม ก็ยังคงต้องการผู้มีความชำนาญทั้งการสอบบัญชี และความเข้าใจในการประมวลผล เทคนิคนี้จะมีประสิทธิภาพในการตรวจสอบ ก็ต่อเมื่อผู้สอบบัญชีทราบถึงปัญหาที่จะพิจารณา

II. เทคนิคที่ใช้ในการตรวจสอบการควบคุมภายใน (TECHNIQUES FOR TESTING CONTROLS)

มีวิธีการตรวจสอบอยู่ 2 วิธี ที่จะใช้ทดสอบการควบคุมภายในเฉพาะระบบงาน นั่นก็คือ

1. การทดสอบผลลัพธ์ (Testing the results)
2. การทดสอบวิธีการประมวลผล (Testing the processing)

1. การทดสอบผลลัพธ์

การทดสอบผลลัพธ์ถือหลักเกณฑ์ที่ว่าหากผลลัพธ์ที่ได้ถูกต้องย่อมแสดงถึงการมีการควบคุมภายในที่ใช้ได้ผล เช่น ถ้าส่งคำยืนยันยอดลูกหนี้ในระหว่างปีและคำตอบที่ได้รับไม่ปรากฏข้อผิดพลาดใด ๆ ย่อมหมายถึงว่าการควบคุมการออกใบกำกับสินค้าเพื่อมาลงบัญชีอย่างทันเวลา พร้อมกับมีการควบคุมการรับเงินอย่างเหมาะสมด้วย

มีเทคนิค 3 อย่างที่ถูกนำมาใช้อย่างกว้างขวางมาเป็นเวลาหลายปีในการตรวจสอบที่ไม่ใช้คอมพิวเตอร์ และในชั้นเดิมเป็นการทดสอบแบบทดสอบความถูกต้องของรายการ (Substantive test) ซึ่งสามารถทำได้ทั้งด้วยมือหรือด้วยคอมพิวเตอร์ เทคนิคดังกล่าวได้แก่

1.1 การขอคำยืนยันยอด (Confirmation) โดยการโต้ตอบโดยตรงกับบุคคลที่สามในการหาหลักฐานมาสนับสนุนรายการหรือยอดคงเหลือต่าง ๆ

1.2 การเปรียบเทียบ (Comparison) เป็นการเปรียบเทียบแฟ้มข้อมูลหนึ่งกับแฟ้มข้อมูลที่เก็บไว้ตามแผนกต่าง ๆ ที่ไม่เกี่ยวข้องกัน หรือ เปรียบเทียบกับผลของการตรวจนับ

1.3 การทดสอบความสมเหตุสมผลและความถูกต้อง (Reasonableness and edit tests)

1.1 การขอคำยืนยันยอด

ตัวอย่างที่พบมากที่สุดของการทดสอบผลลัพธ์ก็คือ การยืนยันยอดของรายการที่บันทึกในแฟ้มข้อมูลของบริษัท กับที่บันทึกโดยบุคคลอื่น รายการอาจประกอบด้วย แฟ้มข้อมูลทั้งหมด หรือตัวอย่างที่เลือกขึ้นมาเป็นตัวแทน ตัวอย่างของการทดสอบแฟ้มข้อมูลโดยการขอคำยืนยันยอด ได้แก่ เงินฝาก ธนาคาร ลูกหนี้ สินค้าฝากขาย เจ้าหนี้ และ หนี้สินอื่น ๆ เป็นต้น

รายการที่ได้รับการยืนยันยอดว่าถูกต้อง จะให้ความมั่นใจอย่างมากว่าแฟ้มที่ถูกตรวจนั้นได้มีการลงรายการอย่างครบถ้วนทันต่อเหตุการณ์อย่างถูกต้อง อย่างไรก็ตาม ควรใช้ความระมัดระวังในผลของการขอคำยืนยันยอด ในบางครั้งไม่อาจสรุปได้ว่าการได้รับคำยืนยันยอดว่าถูกต้องจะให้ผลในการทดสอบที่เชื่อถือได้ของมูลค่าทรัพย์สินหรือหนี้สินที่มีอยู่จริง ตัวอย่างเช่น การได้รับคำยืนยันยอดของลูกหนี้นั้นไม่สามารถยืนยันได้ว่า ลูกหนี้จะสามารถชำระหนี้ได้ตามข้อตกลง

1.2 การเปรียบเทียบแฟ้มข้อมูลหนึ่งกับแฟ้มข้อมูลที่เก็บไว้ตามแผนกต่าง ๆ ที่ไม่เกี่ยวข้องกันหรือเปรียบเทียบกับผลของการตรวจนับ

วิธีที่สอง คือ การเปรียบเทียบข้อมูลจากแฟ้มหนึ่งกับอีกแฟ้มหนึ่ง ที่ถูกเก็บไว้ต่างหากแยกจากกันในบริษัทเดียวกัน หรือเปรียบเทียบระหว่างข้อมูลในแฟ้มกับของที่มีอยู่จริงซึ่งได้จากการตรวจนับ ตัวอย่างของการตรวจสอบแบบนี้ซึ่งพบเสมอ คือ การเปรียบเทียบแฟ้มเงินเดือนกับแฟ้มข้อมูลของฝ่ายการพนักงาน หรือเปรียบเทียบตัวเลขตามที่บันทึกกับของที่มีอยู่จริง เช่น สินค้าคงเหลือ สินทรัพย์ถาวร

1.3 การทดสอบความสมเหตุสมผลและความถูกต้อง

การทดสอบความสมเหตุสมผลและความถูกต้องของรายการในแฟ้ม โดยปกติการทดสอบดังกล่าวจะกระทำเพื่อค้นหาสิ่งที่ไม่ควรจะปรากฏปะปนอยู่ในแฟ้มรายการ ถ้าการควบคุมเพื่อป้องกันความผิดพลาดมีประสิทธภาพการตรวจสอบดังกล่าวเป็นการตรวจสอบเพื่อหาจุดบกพร่องของการควบคุมภายในระบบ หากผู้สอบบัญชีพิจารณาเห็นว่าการทดสอบความสมเหตุสมผลและความถูกต้องของรายการอาจนำมาใช้ได้เพื่อประโยชน์ในการตรวจสอบบัญชีตามปกติ ผู้สอบบัญชีอาจขอให้นำการตรวจสอบดังกล่าวใส่ไว้ในระบบงานตามปกติก็ได้

2. การทดสอบวิธีการประมวลผล

2.1 การตรวจสอบโดยไม่ใช้คอมพิวเตอร์ในการตรวจสอบ (Auditing Around the Computer)

ในการตรวจสอบโดยไม่ใช้คอมพิวเตอร์ในการตรวจสอบ ผลจากการประมวลผลของคอมพิวเตอร์จะนำมาทดสอบด้วยมือกับแหล่งข้อมูลที่ป้อนเข้าเครื่อง การตรวจสอบความถูกต้องจะกระทำโดยที่ผู้สอบบัญชีไม่ได้ไปยุ่งเกี่ยวกับการประมวลผลภายในคอมพิวเตอร์

การทดสอบแบบนี้จะกระทำทั้งโดยวิธีการสุ่มตัวอย่าง หรือโดยการเปรียบเทียบจำนวนรวม เทคนิคนี้โดยทั่ว ๆ ไปจะมีประสิทธิภาพตราบเท่าที่เอกสารสำหรับการตรวจสอบนั้นยังคงมีอยู่ หรือสามารถทำขึ้นมาได้อย่างเรียบร้อย

ในการตรวจสอบโดยไม่ใช้คอมพิวเตอร์ในการตรวจสอบสิ่งที่จำเป็น คือ

ก) พิจารณาว่าผลที่ได้จากการประมวลผลและการควบคุมที่มีอยู่ สามารถเอื้ออำนวยต่อการคำนวณด้วยมือ ในขั้นตอนหลักแต่ละขั้นตอนของกระบวนการจะต้องมีการจัดพิมพ์รายการ และมีผลรวมของรายการที่บันทึกในแฟ้มที่ถูกประมวลผลทั้งก่อนและหลังการประมวลผล โดยแท้จริงแล้วรายการก่อนการประมวลผลในขั้นตอน ใดขั้นตอนหนึ่ง ซึ่งถือเป็นข้อมูลนำเข้า คือข้อมูลที่ส่งออกที่ได้จากการประมวลผลครั้งก่อนนั้นนั่นเอง ดังนั้นเพื่อประสิทธิภาพในการตรวจสอบวิธีนี้รายการค้าทั้งหมดที่ได้นำใส่เข้าไปในการประมวลผล จะต้องรวมอยู่ในรายงานที่ออกมาจากคอมพิวเตอร์

ข) หาวิธีที่จะสุ่มตัวอย่างให้ได้ตัวแทนของรายการค้าทั้งหมด การสุ่มตัวอย่างมีความจำเป็น เนื่องจากรายการค้าทั้งหมดมีปริมาณมากเกินกว่าที่จะตรวจสอบทุกรายการด้วยมือ เทคนิคการสุ่มตัวอย่างจะต้องแน่ใจได้ว่า รายการที่เป็นตัวแทนรายการค้าต่าง ๆ และรายการผิดปกติจะต้องถูกนำมาทดสอบด้วย

ค) การตรวจสอบการควบคุมภายในแต่ละประเภทและการประมวลผลแต่ละขั้นตอนที่ผู้สอบบัญชีต้องการให้ความเชื่อถือด้วยมือ

ข้อดี

ข้อดีที่สำคัญประการหนึ่งในการตรวจสอบโดยไม่ใช้คอมพิวเตอร์ คือผู้สอบบัญชีไม่จำเป็นต้องผ่านการอบรมทางด้านคอมพิวเตอร์มากนัก การตรวจสอบส่วนใหญ่เป็นการตรวจสอบความถูกต้องสมเหตุสมผล เมื่อใช้วิธีนี้ผู้สอบบัญชีสามารถพิจารณาถึงความสำคัญของสิ่งที่ตนตรวจพบระหว่างการตรวจสอบได้ดีกว่ากรณีใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

ข้อเสีย

ยิ่งระบบคอมพิวเตอร์ใหญ่มากเท่าใด ผลที่พิมพ์ออกมาก็ยิ่งเข้าใจยากขึ้นเท่านั้น ดังนั้นการตรวจสอบโดยไม่ใช้คอมพิวเตอร์จะทำได้น้อยลง ในการตรวจสอบโดยไม่ใช้คอมพิวเตอร์ในแต่ละขั้นตอนของการประมวลผลต้องการผลของการประมวลผลที่พิมพ์ออกมาอย่างละเอียด นอกจากนี้ ในกรณีที่ปริมาณของรายการค้ามีมากก็อาจทำให้เงื่อนไขที่จะต้องทดสอบเกินความสามารถของการตรวจสอบด้วยมือ แม้ว่าจะได้นำเทคนิคการสุ่มตัวอย่างมาใช้หากเป็นระบบที่สลับซับซ้อนย่อมจะไม่สามารถตรวจพบรายการที่ไม่ปกติได้ โดยเฉพาะเมื่อระบบนั้นมีการควบคุมความสมเหตุสมผลของตัวเลขอยู่แล้ว

ในการตรวจสอบโดยไม่ใช้คอมพิวเตอร์นั้น มีความยุ่งยากในการทดสอบความสมบูรณ์ของการประมวลผล วิธีการปกติที่ใช้กันคือ การตรวจสอบการควบคุมเกี่ยวกับยอดรวมของรายการที่นำเข้าเครื่อง (batch control) แต่วิธีการเช่นนี้เป็นสิ่งที่ยุ่งยากเนื่องจาก (batch control) ส่วนมากจะรวมปริมาณรายการค้าจำนวนมากจนไม่สามารถที่จะทำการคำนวณใหม่อีกครั้งด้วยมือได้

ในการใช้เทคนิคการตรวจสอบโดยไม่ใช้คอมพิวเตอร์นี้ ผู้สอบบัญชีจะต้องทำตามขั้นตอนดังนี้

ก) กำหนดวิธีการประมวลผลและวิธีการควบคุมที่จะทำการทดสอบ เช่นเดียวกับการตรวจสอบในสถานการณ์อื่น ๆ ผู้สอบบัญชีจำเป็นต้องเริ่มการตรวจสอบโดยการกำหนดวัตถุประสงค์ของการตรวจสอบ ตามวิธีนี้ผู้สอบบัญชีมีความยืดหยุ่นมากกว่าการตรวจสอบโดยใช้คอมพิวเตอร์ เนื่องจากผู้สอบบัญชีทราบถึงการควบคุมภายในที่มีอยู่ได้ตลอด จึงสามารถขยายหรือลดขอบเขตของการทดสอบ ทั้งนี้ขึ้นอยู่กับสิ่งที่เขาตรวจพบในตอนกลางปี

ข) เลือกรายการที่จะทดสอบ

ผู้สอบบัญชีควรเริ่มโดยการเลือกผลของการประมวล (output) ที่จะทดสอบแล้วตรวจสอบกับข้อมูลที่เกี่ยวข้องที่ป้อนเข้าเครื่อง (input) ซึ่งจะนำมาใช้ในการพิจารณาความสมเหตุสมผลและความถูกต้องของผลของการประมวลผลที่เลือก ถ้าข้อมูลเป็นจำนวนมากถูกป้อนเข้าไปประมวลผลเพื่อให้ได้ผลรวมออกมายอดเดียว หรือถ้าปริมาณรายการมีมากเกินความสามารถที่จะตรวจสอบได้ด้วยมือก็จำเป็นต้องใช้เทคนิคการสุ่มตัวอย่าง ในการเลือกตัวอย่างจะต้องเลือกจนสิ่งที่ได้จากการประมวลผลทุกประเภทได้ถูกเลือกเพื่อตรวจสอบ รวมทั้งรายการที่มีปรากฏในรายงานข้อมูลที่ไม่ผ่านการตรวจสอบความถูกต้อง

ค) การทดสอบการประมวลผลใหม่ของรายการที่เลือกขึ้นมา

เมื่อผู้สอบบัญชีเลือกผลของการประมวลผล และได้ข้อมูลที่นำไปประมวลที่สอดคล้องกันแล้ว ผู้สอบบัญชีก็พร้อมที่จะทดสอบการคำนวณได้ ในขั้นนี้ต้องอาศัยความเข้าใจอย่างละเอียดในสิ่งที่ควรจะทำ และผลที่ควรจะได้ ผู้สอบบัญชีควรจะตระหนักว่า เทคนิคการคำนวณที่ใช้กับคอมพิวเตอร์ไม่จำเป็นต้องสอดคล้องกับที่ใช้ในการประมวลผลด้วยมือ

ง) การแก้ปัญหาเมื่อมีการค้นพบข้อผิดพลาด

ภายหลังเมื่อการทดสอบเสร็จสิ้นลงแล้ว ถ้ามีข้อผิดพลาดใด ๆ ในการประมวลผล ผู้สอบบัญชีจะต้องพิจารณาถึงสาเหตุของข้อผิดพลาดว่าเป็นเพราะจุดอ่อนของการควบคุมหรือเป็นเพราะข้อผิดพลาดในงานประมวลผล รายงานรายการที่มีข้อผิดพลาดจะแสดงให้เห็นชนิดของข้อผิดพลาดซึ่งจะได้มีการพิจารณาถึงผลของความผิดพลาดนั้นอาจกำหนดให้มีวิธีการตรวจสอบความเหมาะสมเพื่อป้องกันและรายงานข้อผิดพลาดจากการปฏิบัติงานไว้ในโปรแกรมคำสั่งด้วย

2.2 ข้อมูลทดสอบ (Test Data)

ข้อมูลทดสอบโดยทั่ว ๆ ไป เรียกกันว่า test data เป็นกลุ่มข้อมูลนำเข้าที่แทนรายการค้าชนิดต่าง ๆ เพื่อป้อนเข้าคอมพิวเตอร์ในการตรวจสอบ โดยผ่านวิธีการประมวลผลที่ใช้งานอยู่จริง วิธีนี้เป็นวิธีหนึ่งที่จะใช้ตรวจสอบเพื่อดูผลที่ไม่ถูกต้อง ข้อมูลทดสอบที่ดีควรจะรวมเอารายการค้าในสถานการณ์ต่าง ๆ ที่อาจเกิดขึ้นจริงในระหว่างการปฏิบัติงาน ปริมาณของรายการที่จะทดสอบอาจมีจำนวนมากเป็นพันหรือหมื่นรายการก็ได้

ผู้สอบบัญชีจะพบกับปัญหายุ่งยากในการทำความเข้าใจเงื่อนไขต่าง ๆ ในการจัดแฟ้มข้อมูลและรายการเพื่อที่จะทดสอบการประมวลผลที่เป็นไปได้ทั้งหมด ดังนั้น การทดสอบโดยวิธีนี้จะสามารถใช้ได้ผลดีที่สุด ถ้าปริมาณของรายการค้า วิธีการประมวลผล และการควบคุม มีไม่มากนัก และเอกสารอ้างอิงที่เชื่อถือได้ก็จำเป็นต้องมี

เพียงพอ ผู้สอบบัญชีมีความเข้าใจในรูปแบบของรายการที่จะนำไปประมวลผล รูปแบบของแฟ้มข้อมูล วิธีการประมวลผล และควบคุม

สิ่งหนึ่งที่ต้องมีในโครงการพัฒนาระบบ ก็คือ การทดสอบโปรแกรมก่อนที่จะมีการใช้ระบบใหม่ในการประมวลผล ทำให้จำเป็นต้องสร้างข้อมูลทดสอบขึ้นมาเพื่อทำการแก้ไขที่ผิดของโปรแกรมคำสั่งที่เขียนขึ้นมาใหม่ ถ้าข้อมูลทดสอบนั้นยังคงเก็บเอาไว้ ผู้สอบบัญชีอาจจะใช้ข้อมูลของการทดสอบนั้นเป็นจุดเริ่มต้น แต่ถ้าไม่สามารถหาได้แล้วความยากลำบากในการสร้างข้อมูลทดสอบขึ้นมาใหม่จะทำให้โอกาสที่จะนำเทคนิคนี้มาใช้ในการตรวจสอบลดน้อยลง

ข้อดี

ตามปกติ เทคนิคนี้สามารถทำได้โดยคนที่มีพื้นความรู้ทางด้านเทคนิคเพียงเล็กน้อยเท่านั้น อย่างไรก็ตามผู้ที่จะเตรียมข้อมูลทดสอบจะต้องมีความคุ้นเคยกับรายละเอียดในการคำนวณของโปรแกรมคำสั่ง รวมทั้งความสมเหตุสมผลและการควบคุมเฉพาะจุดใดจุดหนึ่งในโปรแกรมคำสั่งนั้น

ข้อเสีย

ในทางปฏิบัตินั้น เป็นไปได้ยากที่จะหวังให้ผู้สอบบัญชีมีความคุ้นเคยอย่างสมบูรณ์ในรายละเอียดทั้งหมดของขั้นตอนโดยละเอียดในการประมวลผลแต่ละเรื่อง ดังนั้น จึงเป็นไปไม่ได้ในทางปฏิบัติที่ผู้ออกแบบข้อมูลทดสอบจะคาดคะเนได้ว่าอะไรอาจเกิดขึ้นได้บ้างในระหว่างการประมวลผลของโปรแกรมนั้น ๆ เพื่อจะได้ออกแบบข้อมูลทดสอบให้สอดคล้องกับสิ่งที่จะเกิดขึ้น

ข้อเสีย ที่สำคัญที่สุดของเทคนิคนี้ คือ เป็นการทดสอบสถานการณ์ที่กำหนดไว้ล่วงหน้า (preconceived situation) ทำให้ข้อมูลทดสอบที่สร้างขึ้นมีโอกาสที่จะรวมข้อผิดพลาดหรือข้ามความสำคัญบางสิ่งบางอย่างไปเช่นเดียวกับที่เกิดในโปรแกรมคำสั่ง

ตัวอย่างเช่น ข้อมูลทดสอบที่ถูกออกแบบเพื่อตรวจสอบโปรแกรมสำหรับลูกหนี้ผ่อนชำระของธนาคารพาณิชย์แห่งหนึ่ง ข้อมูลที่จัดทำขึ้นเพื่อการทดสอบจะสมมุติข้อมูลเพื่อให้โปรแกรมคำสั่งตรวจความสมเหตุสมผลตามเงื่อนไขที่กำหนดในโปรแกรมคำสั่ง ดังนั้นหากในโปรแกรมคำสั่งมิได้คำนึงถึงโอกาสที่บัญชีลูกหนี้จะมียอดติดลบและมิได้สั่งให้พิมพ์รายงานกรณีเกิดข้อผิดพลาดเช่นนี้ การตรวจสอบโดยวิธีใช้ข้อมูลทดสอบย่อมไม่สามารถทราบเหตุการณ์เช่นนี้ได้

อุปสรรคที่สำคัญอื่น ๆ คือ การพิสูจน์ความสำคัญของผลที่เกิดขึ้น ถ้าผู้สอบบัญชีพบข้อบกพร่องบางอย่างในโปรแกรมคำสั่ง เช่น ความไม่สมเหตุสมผลในขั้นตอนการทำงาน ในบางกรณีผู้สอบบัญชีก็มักจะได้รับคำตอบโต้ว่าข้อบกพร่องนั้นไม่เคยเกิดขึ้นเลย ข้อโต้แย้งเช่นนี้อาจเกิดขึ้นเนื่องจากผู้ที่มีหน้าที่รับผิดชอบไม่เคยรับรู้ปัญหานั้นมาก่อน ข้อมูลที่ได้มาโดยการตรวจสอบด้วยการใช้ข้อมูลทดสอบไม่สามารถตอบปัญหาเช่นนี้ได้

ท้ายที่สุด เมื่อได้มีการทดสอบโปรแกรมคำสั่งแล้ว ผู้สอบบัญชีจะต้องพิจารณาว่า โปรแกรมคำสั่งที่ตนทดสอบเป็นโปรแกรมเดียวกับที่ใช้ในการประมวลผลจริง เนื่องจากโปรแกรมคำสั่งที่แตกต่างออกไปอาจถูกนำมาใช้แทนโปรแกรมคำสั่งเดิมที่เคยทดสอบไว้ เพื่อตบแต่งรายงานที่ได้จากการประมวลผลให้เป็นที่น่าพอใจสำหรับผู้สอบบัญชี

ในการประยุกต์ใช้เทคนิค test data ผู้สอบบัญชีต้องทำดังต่อไปนี้

ก) กำหนดวัตถุประสงค์

การตรวจสอบโดยใช้เทคนิคข้อมูลทดสอบ ต้องการคำจำกัดความของวัตถุประสงค์ในการทดสอบอย่างเป็นทางการมากกว่าเทคนิคอย่างอื่น ทั้งนี้เนื่องมาจากลักษณะโดยเฉพาะของเทคนิคนี้ ซึ่งจะทำการตรวจสอบเฉพาะลักษณะหรือการควบคุมที่ผู้สอบบัญชีกำหนดไว้อย่างชัดเจน

ข) การจัดเตรียมข้อมูลทดสอบ

ขั้นที่ 1 ในการใช้เทคนิคนี้ คือการได้มาซึ่ง master file หรือ file ที่มีคุณสมบัติเหมาะสม การจัดเตรียม master file ที่มีเงื่อนไขและลักษณะทั้งหมดที่จะทำการทดสอบอาจเป็นสิ่งที่มีความยุ่งยากมากที่สุดในการใช้เทคนิคข้อมูลทดสอบ

ค) การคำนวณผลล่วงหน้า

ขั้นต่อไป คือ การคำนวณล่วงหน้า ถึงผลที่จะได้จากข้อมูลทดสอบ ซึ่งทำได้โดยการใช้ข้อมูลจริงที่รวมอยู่ใน master records และรายการค้าที่เกี่ยวข้องที่ใช้เป็น test data โดยอาศัยความเข้าใจในเงื่อนไขของระบบงาน วิธีการคำนวณ และลักษณะของการควบคุม ผลการคำนวณข้อมูลทดสอบตามเงื่อนไขต่าง ๆ ด้วยมือจะถูกนำไปเปรียบเทียบกับผลของการประมวลผลโดยคอมพิวเตอร์

ขั้นตอนนี้ก็มีอุปสรรคที่สำคัญเช่นกัน การประมวลผลด้วยมือสำหรับรายการเป็นพันหรือเป็นหมื่นอาจเกินกำลังของผู้สอบบัญชีโดยทั่วไป เพื่อที่จะทำการคำนวณเหล่านี้อาจต้องอาศัยโปรแกรมคำสั่งเพื่อการตรวจสอบอย่างทั่ว ๆ ไป (general purpose audit software)

4. การประมวลผลข้อมูลทดสอบด้วยคอมพิวเตอร์

ขั้นตอนต่อไป คือการนำข้อมูลทดสอบเข้าไปทดสอบโปรแกรมคำสั่งทั้งหมดในแต่ละระบบงาน และเพื่อที่จะให้บรรลุวัตถุประสงค์ในการตรวจสอบโดยใช้ข้อมูลทดสอบ ผู้สอบบัญชีอาจจะต้องใช้รายการมากกว่าหนึ่งกลุ่ม หรือแม้แต่ใช้ master file มากกว่าหนึ่งแฟ้ม ถ้ามีการนำรายการต่างประเภทกันมาประมวลผลในขั้นตอนต่าง ๆ กันในแต่ละระบบงาน

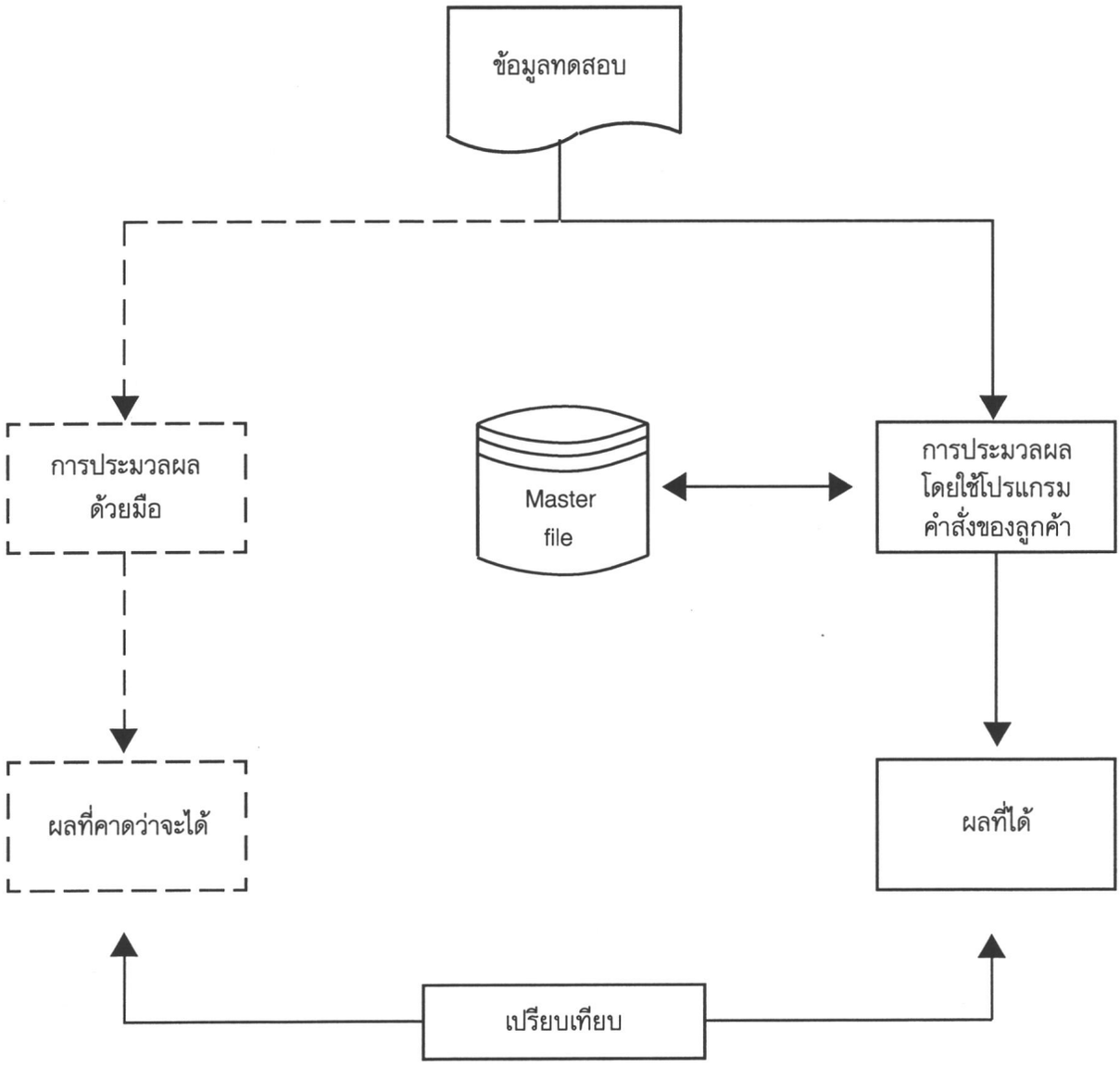
จ) การเปรียบเทียบผลที่ได้จากคอมพิวเตอร์กับที่คำนวณด้วยมือ

หลังจากการประมวลผลแล้ว ผู้สอบบัญชีต้องเปรียบเทียบผลที่ได้รับ กับที่คำนวณไว้ล่วงหน้า หากมีผลต่างเกิดขึ้นจะต้องวิเคราะห์หาสาเหตุ

ฉ) การแก้ปัญหาเมื่อพบข้อผิดพลาด

ถ้าผลของการทดสอบชี้ให้เห็นถึงข้อผิดพลาดที่เกิดขึ้นในการประมวลผลของโปรแกรมคำสั่ง ผู้สอบบัญชีจะต้องพิสูจน์หาสาเหตุที่แท้จริงของแต่ละเรื่อง และพิจารณาหาวิธีการตรวจสอบเพิ่มเติม เพื่อวัดผลของการประมวลผลของโปรแกรมที่ผิดนั้น

เราสามารถสรุปเทคนิคข้อมูลทดสอบได้ตามรูปที่แสดงข้างใต้นี้



2.3 การทดสอบข้อมูลจำลองร่วมกับข้อมูลจริง (Integrated Test Facility Method)

วิธี Integrated test facility (ITF) เป็นเทคนิคที่ได้พัฒนามาจากวิธี test data เป็นวิธีที่นำเอาข้อมูลทดสอบป้อนเข้าไปในคอมพิวเตอร์พร้อม ๆ กับข้อมูลจริงของบริษัทและติดตาม flow ของรายการที่ใช้ทดสอบเหล่านั้น ผ่านการประมวลผลขั้นตอนต่าง ๆ เพื่อจะได้เปรียบเทียบผลที่จะได้รับกับผลที่ได้กำหนดไว้ล่วงหน้า

ITF นั้นเกี่ยวข้องกับการกำหนดรายการที่จำลองจากข้อมูลที่ถูกประมวล เช่น ข้อมูลเกี่ยวกับแผนก พนักงาน เป็นต้น หลังจากที่ได้กำหนดรายการจำลองดังกล่าวขึ้นแล้ว จะนำรายการทั้งหมดนี้เข้าประมวลผลพร้อม ๆ กับรายการจริงของบริษัท ผู้สอบบัญชีต้องกำหนดสิ่งที่ตนเองต้องการตรวจสอบ เช่น รายการที่ค้างเกินกำหนด หรือ สินค้ารับคืน เป็นต้น และเปรียบเทียบผลที่ได้กับผลที่กำหนดไว้ล่วงหน้า

ข้อดี

ข้อดีของ ITF มีดังนี้

- ความจำเป็นทางด้านการอบรมเกี่ยวกับเทคนิคมีน้อย
- ต้นทุนในการประมวลผลต่ำ เนื่องจาก test data ถูกประมวลพร้อม ๆ กับรายการปกติ
- ได้มีการทดสอบระบบที่กิจการใช้งานอยู่จริง
- คนทั่ว ๆ ไปสามารถเข้าใจได้โดยง่าย เนื่องจากผู้สอบบัญชีใช้วิธีการที่บริษัทใช้อยู่ตามปกติ

ข้อเสีย

ข้อเสียของ ITF คือ

- รายการทดสอบจะต้องถูกขจัดออกจากบันทึกของบริษัท (เช่น จากบัญชีแยกประเภท) ทั้งนี้โดยการลงรายการปรับปรุงด้วยมือ หรือการแก้ไขด้วยโปรแกรม
- ต้นทุนจะสูง ถ้าโปรแกรมต้องมีการแก้ไขเพื่อขจัดผลของรายการทดสอบ
- อาจเป็นไปได้ที่แฟ้มข้อมูลอาจจะถูกทำลาย เนื่องจากรายการอาจกระทบต่อข้อมูลที่อยู่ในแฟ้ม
- ปริมาณของข้อมูลทดสอบที่ผู้สอบบัญชีจะใช้ อาจถูกจำกัดโดยความสามารถในการรับข้อมูลจริงของคอมพิวเตอร์

การประยุกต์เทคนิค ITF ผู้สอบบัญชีต้องทำดังต่อไปนี้

ก) กำหนดวัตถุประสงค์

วิธี ITF นั้นไม่ได้ทำให้การกำหนดวัตถุประสงค์เปลี่ยนแปลงไป วิธีการกำหนดวัตถุประสงค์ของเทคนิค test data สามารถนำมาใช้กับเทคนิคนี้ได้

ข) การสร้างข้อมูลจำลองเพิ่มเติมในแฟ้มข้อมูลจริง

ตามปกติ ผู้สอบบัญชีจะต้องสร้างข้อมูลจำลองในแฟ้มข้อมูลต่างหาก เพื่อบันทึกผลที่ได้จากการประมวลข้อมูลทดสอบ ตามวิธี ITF นั้น ข้อมูลเหล่านี้จะถูกสร้างใน file เดียวกับที่ใช้บันทึกข้อมูลจริง (live records) อย่างไรก็ตามจะต้องมีการกำหนด ตัวกำหนด (identification) บางอย่าง เช่น เลขที่บัญชี รหัสแผนก หรือรหัสของสาขา เป็นต้น ที่จะบอกว่าข้อมูลใดเป็นข้อมูลจำลอง วิธีการที่ใช้สร้างคุณสมบัติเหล่านี้จะต้องได้รับการพิจารณาอย่างระมัดระวัง เนื่องจากอาจก่อให้เกิดข้อจำกัดในการประมวลผล

ค) ต้องมีการกำหนดวิธีการที่จะขจัดผลของการประมวลข้อมูลทดสอบออกไปจากผลของการประมวลผล

เนื่องจากข้อมูลทดสอบที่นำไปประมวลผลอยู่รวมกับข้อมูลที่เกิดขึ้นจริงๆ และรายการทดสอบจะถูกใส่เข้าไปในการประมวลผลตามปกติ จึงต้องมีการเตรียมวิธีการบางอย่างเพื่อขจัดผลของรายการทดสอบเหล่านี้ออกจากผลที่เกิดจากการประมวลผลจริง วิธีการเช่นว่านี้มีอยู่หลายวิธี ดังนี้

- ขจัดผลของรายการทดสอบที่มีผลต่อรายงานต่าง ๆ ด้วยมือ
- เขียนโปรแกรมคำสั่งขึ้นมาไม่ให้รวมรายการทดสอบเหล่านี้ในบัญชีคุมยอด
- กำหนดให้รายการทดสอบมีค่าน้อยมาก เพื่อว่าผลของรายการทดสอบจะไม่เป็นสาระสำคัญและสามารถละเลยได้

การขจัดผลของ ITF ด้วยมือนั้น แม้ว่าจะไม่สิ้นเปลือง แต่ก็ไม่น่าเชื่อถือ

การเขียนโปรแกรมขึ้นมาเพื่อให้ขจัดผลจากรายการทดสอบนั้น จะต้องมีการวางแผนล่วงหน้าในตอนเขียนโปรแกรม มิเช่นนั้นอาจจะต้องเสียค่าใช้จ่ายในการปรับปรุงแก้ไขโปรแกรมที่แพงมาก ด้วยเหตุนี้ผู้สอบบัญชีจึงควรเข้าร่วมในการเขียนโปรแกรมใหม่ ๆ ด้วย ข้อเสียอีกประการหนึ่งก็คือ ข้อมูลทดสอบมิได้ถูกประมวลผลในลักษณะเดียวกับข้อมูลจริง ทำให้เกิดปัญหาในความถูกต้องและเชื่อถือได้ของการทดสอบ

ทางเลือกสุดท้าย คือ การใช้ค่าที่ไม่มีความสำคัญ คือน้อยมาก (เช่น 0.01 บาท) เพื่อหลีกเลี่ยงข้อเสียของทางเลือกต่าง ๆ ข้างต้นให้มากที่สุด แต่กลับก่อให้เกิดปัญหาใหม่ คือ ไม่สามารถทดสอบการควบคุมภายในของโปรแกรมคำสั่งสร้างขึ้นเพื่อควบคุมรายการที่มียอดเงินสูง ๆ ได้ ซึ่งสิ่งนี้อาจจะมีหรือไม่มีผลต่อวัตถุประสงค์ในการตรวจสอบก็ได้

ง) การคำนวณผลที่คาดว่าจะได้รับจากการทดสอบ

ขั้นตอนนี้ คล้ายกับที่ใช้ในเทคนิค test data ที่กล่าวไปแล้ว ผู้สอบบัญชีจะต้องกำหนดผลที่ควรจะได้จากการทดสอบ ซึ่งอาจจะทำก่อนหรือหลังการทดสอบก็ได้

จ) การป้อนข้อมูลทดสอบเข้าเครื่องคอมพิวเตอร์

วิธี ITF นั้น ข้อมูลทดสอบจะถูกป้อนเข้าเครื่องไปพร้อม ๆ กับข้อมูลจริงของบริษัทซึ่งไม่ได้หมายความว่าข้อมูลดังกล่าวจะต้องรวมเข้ากับข้อมูลจริง แต่อย่างน้อยจะต้องป้อนเข้าไปโดยผ่านขั้นตอนและถูกประมวลผลในเวลาเดียวกัน

ฉ) การเปรียบเทียบผลที่ประมวลได้กับผลที่คำนวณไว้ล่วงหน้า

ขั้นตอนนี้ก็คล้ายกับเทคนิค test data เช่นกัน ต้องมีการคำนวณล่วงหน้าสำหรับผลที่ควรจะเกิดขึ้น ซึ่งผู้สอบบัญชีจะต้องนำมาเปรียบเทียบกับผลที่เกิดขึ้นจริง และหาสาเหตุของความแตกต่างให้ได้ซึ่งอาจจะต้องใช้เวลาในการวิเคราะห์มาก

ช) ขจัดผลของการทดสอบออกจากผลของการประมวลผล

ขั้นสุดท้ายในวิธีนี้ คือ การขจัดผลของรายการทดสอบออกจากผลของการประมวลผล ถ้าการขจัดรายการนี้ได้นำเข้าไปรวมอยู่ในโปรแกรมการทำงานแล้ว ก็ไม่จำเป็นต้องทำอะไรอีก

2.4 การสร้างแฟ้มเพื่อการตรวจสอบสำหรับการควบคุมในระบบ (System Control Audit Review File หรือ SCARF)

SCARF เป็นวิธีการตรวจสอบที่เกี่ยวกับการรวมเอาการทดสอบความสมเหตุสมผลที่ผู้สอบบัญชีกำหนดเข้าไว้ในโปรแกรมคำสั่งด้วย ผลของการทดสอบนี้จะรายงานต่อผู้สอบบัญชีมากกว่าผู้ใช้ข้อมูล ทั้งนี้เพื่อให้ผู้สอบบัญชีสำรวจข้อมูลต่าง ๆ ที่ควรต้องพิจารณาและสืบหาสาเหตุสำหรับข้อมูลเหล่านั้น

ขั้นตอนต่าง ๆ ที่รวมอยู่ในเทคนิคนี้ ได้แก่

ก) ผู้สอบบัญชีแจ้งสิ่งที่ต้องการต่อเจ้าหน้าที่ที่ทำการพัฒนาระบบงานของหน่วยงานในระหว่างที่มีการพัฒนาระบบงาน

ข) สิ่งต่าง ๆ ที่ผู้สอบบัญชีต้องการจะทดสอบจะถูกรวมเข้าไปในโปรแกรมคำสั่งระหว่างการเขียนโปแกรมคำสั่ง

ค) เมื่อโปรแกรมคำสั่งใหม่ถูกนำไปใช้ การควบคุมเพื่อจะตรวจหาข้อมูลที่ไม่ปรกติซึ่งระบุโดยผู้สอบบัญชีจะถูกรวมอยู่ในขั้นตอนการประมวลผลปกติด้วย และรายการที่ผิดแปลกออกไปซึ่งพบโดยการทดสอบเหล่านี้จะถูกบันทึกในแฟ้มข้อมูล

ง) แฟ้มข้อมูลที่แสดงรายการต่าง ๆ ที่มีลักษณะผิดแปลกออกไป ซึ่งพบจากการตรวจสอบจะได้รับการสอบทานโดยผู้สอบบัญชี โดยใช้มือหรือให้คอมพิวเตอร์เข้ามาช่วยก็ได้

จ) ผู้สอบบัญชีจะทำการตรวจสอบในสิ่งที่ตนเห็นว่าจำเป็น ซึ่งก็ขึ้นอยู่กับรายการผิดแปลกที่ตนตรวจพบ

ถ้าการควบคุมเพื่อทดสอบข้อผิดพลาดที่เสนอโดยผู้สอบบัญชีเป็นสิ่งที่ดี ผู้ใช้ก็น่าที่จะรับเอามาใช้โดยทั่ว ๆ ไป ผู้สอบบัญชีอาจไม่สามารถชักจูงผู้ใช้เกี่ยวกับการควบคุมที่สำคัญ ๆ ได้ ซึ่งผู้สอบบัญชีก็ควรพิจารณาถึงการละเลยในหน้าที่และความรับผิดชอบของผู้ใช้ ซึ่งอาจก่อให้เกิดปัญหาที่สำคัญในการบริหารของหน่วยงานนั้น

2.5 การสร้างแฟ้มข้อมูลตัวอย่างเพื่อการตรวจสอบ (Sample Audit Review File หรือ SARF)

SARF มีความคล้ายคลึงกับ SCARF ยกเว้นข้อมูลที่จะนำมาทำการทดสอบ จะถูกเลือกมาจากการสุ่มตัวอย่างมากกว่าเป็นรายการผิดปกติที่ได้ตรวจคัดออกแล้ว หรือจากการทดสอบความสมเหตุสมผลหรือจากการตรวจสอบความถูกต้องของรายการ วัตถุประสงค์ของเทคนิคนี้ คือให้ได้มาซึ่งแฟ้มข้อมูลซึ่งเป็นตัวอย่างที่ดีของข้อมูลที่นำมาประมวลผลเพื่อวิเคราะห์สำหรับการตรวจสอบ

SARF เป็นวิธีการที่เหมาะสำหรับผู้สอบบัญชี ซึ่งต้องการทดสอบการควบคุม หรือทดสอบรายการที่เกิดขึ้นตลอดปีที่ทำการตรวจสอบ อย่างไรก็ตาม เทคนิคนี้ก็มีความเหมาะสมสำหรับผู้ตรวจสอบภายใน ซึ่งต้องการตัวอย่างรายการที่เป็นตัวแทนของข้อมูล

ขั้นตอนต่าง ๆ ในการนำเทคนิคของ SARF มาใช้

ก) ผู้สอบบัญชีแจ้งสิ่งที่ตนต้องการต่อหน่วยพัฒนาระบบงาน ระหว่างที่มีการพัฒนาระบบอยู่
ข) สิ่งที่ผู้สอบบัญชีต้องการจะนำไปรวมเข้าไว้ในโปรแกรมคำสั่งที่กำลังพัฒนาขึ้นมาด้วย
ค) เมื่อมีการนำระบบการใช้งานไปใช้ จะมีการนำข้อมูลจากการสุ่มตัวอย่างไปบันทึกในแฟ้มข้อมูล
ง) ผู้สอบบัญชีจะทำการตรวจสอบแฟ้มข้อมูลดังกล่าวด้วยมือ หรือโดยการใช้คอมพิวเตอร์
จ) ผู้สอบบัญชีต้องดำเนินการกับสิ่งผิดปกติที่ตรวจพบอย่างเหมาะสม

2.6 การรายงานในแต่ละขั้นตอนของการประมวลผล (SNAPSHOT)

SNAPSHOT เป็นรูปแบบหนึ่งของการพิมพ์รายละเอียดของรายการ (transaction trail) สำหรับรายการที่ป้อนเข้าเครื่องบางรายที่จะเลือกเท่านั้นโดยการให้รหัสพิเศษไว้ วิธีนี้เหมาะสำหรับระบบงานที่มีปริมาณรายการมาก และรายการข้อมูลที่ป้อนเข้าเครื่องเป็นส่วนที่ใช้ในการประมวลผลเพื่อให้ได้ข้อมูลจากการประมวลผลรหัสพิเศษที่ใส่ในรายการที่ป้อนเข้าเครื่องจะสามารถพิมพ์ออกมาเป็นรายละเอียด (transaction trail) ในแต่ละขั้นตอนของการประมวลผล



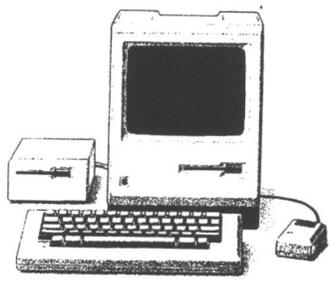
การนำเทคนิค Snapshot มาใช้มีขั้นตอนดังนี้

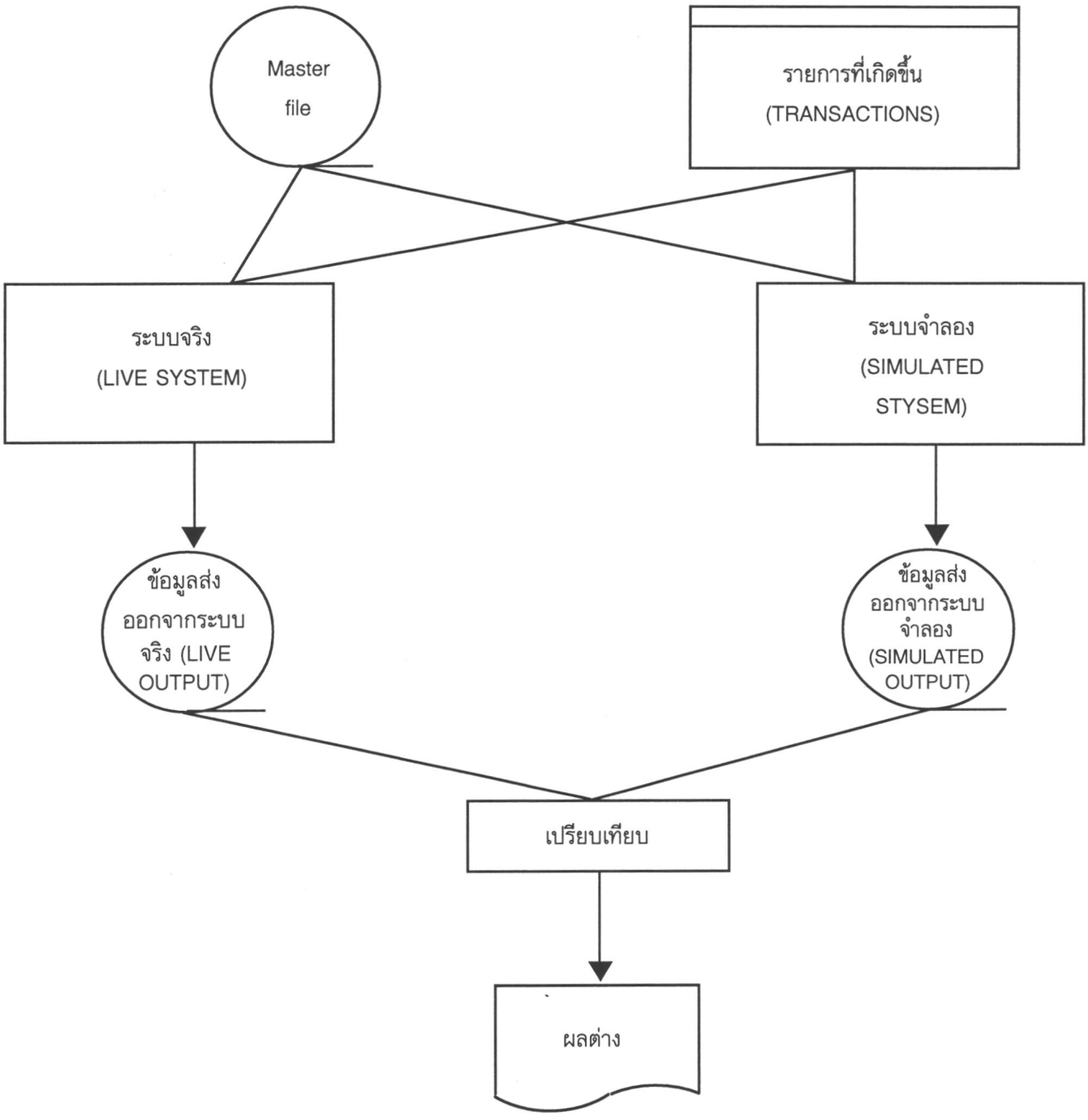
ก) ผู้สอบบัญชีแจ้งสิ่งที่ตนต้องการให้แก่ผู้พัฒนาระบบ ในระหว่างการพัฒนาระบบงาน
ข) ผู้พัฒนาระบบจะกำหนดให้มีการพิมพ์รายการที่เลือกไว้ในทุกขั้นตอนของการประมวลผล
ค) ในระหว่างการใช้งานของระบบใหม่ ผู้สอบบัญชีสามารถใส่รหัสพิเศษเพิ่มเข้าไปในรายการที่เลือกได้ โดยไม่มีผลกระทบต่อการประมวลผลรายการอื่น
ง) เมื่อผ่านการประมวลผลแล้ว จะมีรายงานพิมพ์ออกมา ณ จุดที่กำหนดไว้ล่วงหน้าเพื่อที่จะเปิดเผยผลของการคำนวณรายการที่มีรหัสพิเศษเหล่านั้นในแฟ้มบันทึกข้อมูล
จ) ผู้สอบบัญชีรับรายงานที่เป็นการแสดงผลการประมวลรายการที่มีรหัสพิเศษ
ฉ) ผู้สอบบัญชีทำการวิเคราะห์รายงานที่ได้รับเพื่อให้บรรลุวัตถุประสงค์การตรวจสอบ

การใช้วิธีการให้รหัสพิเศษแก่รายการบางลักษณะตามแต่จะเลือก ไม่เพียงแต่เป็นเครื่องมือที่มีประสิทธิภาพสำหรับผู้สอบบัญชีเท่านั้น แต่ยังมีประโยชน์โดยเฉพาะอย่างยิ่งต่อผู้ที่เกี่ยวข้องกับการพัฒนาระบบ และเขียนโปรแกรมคำสั่งในการขจัดสาเหตุของข้อผิดพลาดในการประมวลผล ยิ่งไปกว่านั้น ผู้บริหารงานอาจมีความสนใจในเรื่องเดียวกับผู้สอบบัญชีได้ ดังนั้นเทคนิคนี้จึงเป็นสิ่งที่ดีที่สุดที่จะใช้เป็นเครื่องมือสำหรับโปรแกรมเมอร์ในการแก้ข้อผิดพลาดที่มีในโปรแกรมการใช้งาน

2.7 การใช้โปรแกรมจำลองขนานกับโปรแกรมที่ใช้อยู่ในการประมวลผล (Parallel Simulation)

Parallel Simulation ประกอบด้วยการใช้โปรแกรมที่สร้างขึ้นต่างหาก แต่จะแสดงหน้าที่เดียวกับโปรแกรมที่ใช้ในการประมวลผลตามปกติของบริษัท โปรแกรมที่จำลองขึ้นจะอ่านข้อมูลที่ป้อนเข้าเครื่อง ซึ่งเป็นชุดเดียวกับข้อมูลที่อ่านโดยโปรแกรมที่ใช้อยู่ตามปกติ ผลที่ได้จากการประมวลด้วยโปรแกรมที่จำลองขึ้นจะถูกนำไปเปรียบเทียบกับผลที่ได้จากโปรแกรมที่ใช้จริง วิธีนี้มีแนวความคิดเหมือนกับการตรวจสอบโดยไม่ใช้คอมพิวเตอร์ (Auditing around the computer) เพียงแต่ไม่ได้ทำด้วยมือ





ภายใต้เทคนิคนี้โปรแกรมจำลองจะประมวลผลรายการต่าง ๆ และสร้างแฟ้มผลการประมวลผลขึ้นมาเอง ซึ่งสามารถนำไปเปรียบเทียบกับแฟ้มที่สร้างขึ้นโดยโปรแกรมที่บริษัทใช้งานอยู่จริง ข้อมูลที่ได้จากการประมวลผลโดยโปรแกรมจำลอง และที่ได้จากโปรแกรมที่บริษัทใช้งานอยู่จริงสามารถนำมาเปรียบเทียบกันโดยใช้คอมพิวเตอร์ โดยไม่จำเป็นต้องทำการเปรียบเทียบด้วยมือ ในกรณีนี้รายงานที่ออกมาจะมีแต่เพียงรายการที่ต่างกันเท่านั้น

โปรแกรมจำลองนี้ อาจเขียนขึ้นด้วยภาษาใด ๆ ก็ได้ อย่างไรก็ตาม ผู้สอบบัญชีควรจะใช้โปรแกรมเพื่อการตรวจสอบบัญชี (general purpose audit sofware) ซึ่งจะช่วยให้ผู้ที่ไม่มีความรู้ทางเทคนิคสามารถสร้างโปรแกรมจำลองขึ้นมาได้ โดยไม่ต้องใช้ความพยายามมากนัก โปรแกรมจำลองนี้เหมาะสำหรับงานตรวจสอบ เนื่องจากโปรแกรมจำลองทำหน้าที่เช่นเดียวกับโปรแกรมใช้งานจริง แต่ผ่านกรรมวิธีการประมวลผลที่ต่างกัน และเนื่องจากโปรแกรมคำสั่งของคอมพิวเตอร์จะทำการประมวลผลอย่างสม่ำเสมอในสถานการณ์ที่เหมือนกัน ดังนั้นผู้สอบบัญชีจึงสามารถให้ความมั่นใจได้มากในผลของการประมวลแต่ละครั้งอันเกิดจากโปรแกรมคำสั่งเดียวกัน

หลังจากที่แฟ้มข้อมูลและรายการเดียวกันได้นำมาประมวลผลโดยระบบทั้งสองแล้ว ผลลัพธ์ที่ได้ควรจะเหมือนกัน และเปรียบเทียบกันได้ในแง่ของการประมวลผลและการควบคุมที่เลือกมาทำการทดสอบ ผู้สอบบัญชีจะทำการเลือกข้อมูลและขั้นตอนการประมวลผล โดยอาศัยความสำคัญในแง่การตรวจสอบบัญชีและใช้เทคนิคนี้ทำการทดสอบเฉพาะในส่วนที่เลือกขึ้นมา

การเตรียมโปรแกรมจำลอง โดยใช้โปรแกรมเพื่อการตรวจสอบบัญชี มีขั้นตอนดังต่อไปนี้

ก) กำหนดวัตถุประสงค์

การประมวลผลที่สำคัญในระบบงานที่ผู้สอบบัญชีควรต้องตรวจสอบให้แน่ใจในความถูกต้อง
- การประมวลผลที่สำคัญ เช่น การคำนวณภาษีเงินเดือน
- รายการที่เกิดขึ้นจากการประมวลผล เช่น การรายงานถึงบัญชีธนาคารที่เบิกเกิน

ข) ทำความเข้าใจกับระบบงาน

ผู้สอบบัญชีต้องทำความเข้าใจในรายละเอียดของระบบงานแต่ไม่จำเป็นที่จะต้องรู้ความถูกต้องทั้งหมดในโปรแกรมคำสั่ง แต่ควรเข้าใจความถูกต้องในส่วนที่ผู้สอบบัญชีเข้าไปเกี่ยวข้อง ผู้สอบบัญชีสามารถละเลยความถูกต้องบางอย่างที่มีในสถานการณ์ที่พบยาก และอาจจะหาผลของความแตกต่างซึ่งเกิดจากสิ่งนี้ด้วยมือ

ผู้สอบบัญชีควรทำความเข้าใจในรายละเอียดของสิ่งต่าง ๆ ดังนี้
- ลักษณะของ records และ transactions
- วิธีการให้รหัสที่ใช้ในแฟ้มคอมพิวเตอร์
- จำนวนของจุดทศนิยมที่จะคำนวณออกมา

ค) เข้าใจในความเหมาะสมของโปรแกรมคำสั่ง

ผู้สอบบัญชีสามารถทำความเข้าใจในความถูกต้องของโปรแกรมคำสั่งโดยใช้ผังโปรแกรม ซึ่งแสดงขั้นตอนและหน้าที่ต่าง ๆ ในการประมวลผล

ง) การให้รหัสคำสั่ง

กำหนดรหัสที่ต้องใช้สำหรับโปรแกรมเพื่อการตรวจสอบบัญชี เทคนิคการลงรหัสนี้จะลดความจำเป็นของผู้สอบบัญชีในการต้องเขียนโปรแกรมคำสั่งด้วยตนเอง ผู้สอบบัญชีจะระบุรายละเอียดของแฟ้มข้อมูลที่จะนำมาประมวลผล และหน้าที่ ๆ จะต้องทำเป็นอักษรย่อ วิธีนี้ต้องการความรู้ในทางเทคนิคเพียงเล็กน้อยการใช้โปรแกรมเพื่อการตรวจสอบช่วยให้ประหยัดเวลากว่าการใช้วิธีอื่น เช่น ภาษา COBOL

จ) การกำหนดแฟ้มที่จะใช้ในการประมวลผล

แฟ้มข้อมูลต่าง ๆ ที่จะใช้ประมวลผล สามารถหาได้จากระบบการทำงานจริงที่มีอยู่ อย่างไรก็ตามจะต้องมีความระมัดระวัง เพื่อที่จะได้แน่ใจว่าได้ข้อมูลของสถานการณ์ทั้งหมด ที่ผู้สอบบัญชีต้องการจะพิสูจน์

ถ้าแฟ้มสำหรับการทดสอบขาดรายการประเภทที่ผู้สอบบัญชีต้องการแล้ว ผู้สอบบัญชีจะมีทางเลือกที่จะทำสองอย่าง คือ ตนอาจจะเพิ่มข้อมูลที่ตนสร้างขึ้นในแฟ้มข้อมูลรับเข้า หรืออาจจะยอมรับแฟ้มข้อมูลที่มีอยู่ในระบบงานจริง

สำหรับรายการที่เกิดขึ้นไม่บ่อยนัก การตรวจสอบในส่วนนี้ก็ไม่เป็นสิ่งจำเป็น เนื่องจากความผิดพลาดที่อาจเกิดขึ้น อาจไม่มีสาระสำคัญมากพอแม้ว่าการประมวลผลจะไม่ถูกต้องก็ตาม แต่การตัดสินใจที่จะละเลยสถานการณ์ดังกล่าวจะต้องทำขึ้นอย่างไตร่ตรองและระมัดระวังและก็เป็นการถูกต้องที่ผู้สอบบัญชีจะเน้นการทดสอบสถานการณ์ที่มีโอกาสเกิดข้อผิดพลาดบ่อยที่สุด

ฉ) การแก้ไขความผิดพลาดในโปรแกรมจำลอง

เช่นเดียวกับเทคนิคในการเขียนโปรแกรมอื่น ๆ คือ ควรจะมีการทดลองการทำงานของโปรแกรมเพื่อการตรวจสอบกับคอมพิวเตอร์ เพื่อที่จะหาข้อติดขัด (bug) เพื่อให้เอกสารการกำหนดแบบเสร็จสมบูรณ์ คอมพิวเตอร์จะพิมพ์ขั้นตอนการประมวลผล และแฟ้มที่ใช้ในลักษณะที่อ่านง่ายและมีรายละเอียดครบถ้วน และถ้าหากมีข้อผิดพลาดในระหว่างการทดสอบ test run ก็จะมีข้อความพิมพ์ออกมาเช่นกัน

ช) การใช้โปรแกรมเพื่อตรวจสอบมาประมวลผล

ในการใช้โปรแกรมเพื่อการตรวจสอบ ผู้สอบบัญชีจะต้องมีการควบคุมการประมวลผลอย่างสมบูรณ์ ผู้สอบบัญชีที่ผ่านการอบรมมาอย่างพอเพียงเกี่ยวกับโปรแกรมก็สามารถที่จะรู้วิธีการในการใช้โปรแกรมจำลอง ซึ่งไม่ได้หมายความว่า ผู้สอบบัญชีจะเป็นผู้ที่มีความเชี่ยวชาญในการดำเนินการเกี่ยวกับคอมพิวเตอร์ แต่ควรจะมีความรู้เพียงพอที่จะทำงานอย่างถูกต้องด้วยตนเอง โดยเป็นอิสระจากพนักงานแผนกคอมพิวเตอร์ของบริษัทถ้ามีความจำเป็น

เรียบเรียงจาก Computer Control and Audit โดย William C. Mair,
Conald R. Wood & Keagle W. Davis. The Institute fo Internal Auditors.

ภาคผนวก ก

กรณีศึกษา : การจัดการ
ความรับผิดชอบของพนักงานชั้นบริหาร

1) เมื่อไม่นานมานี้ที่เมืองนิวยอร์ค บริษัท TIME SHARING ชื่อ ACCUSYSTEMS INC. ได้เป็นผู้ชนะคดี บริษัทผู้ผลิตและจำหน่ายเครื่องคอมพิวเตอร์ HONEYWELL INC. ซึ่งเป็นจำเลยในข้อหาบิดเบือนข้อเท็จจริงเกี่ยวกับประสิทธิภาพของเครื่องคอมพิวเตอร์ HONEYWELL LEVEL 6 SYSTEM ทำให้บริษัท ACCUSYSTEMS ประสบปัญหาในการประกอบธุรกิจจนถึงขั้นต้องเลิกล้มกิจการ

ผู้พิพากษาได้พิจารณาแล้วมีความเห็นว่า การกระทำของบริษัท HONEYWELL เป็นการหลอกลวงลูกค้าโดยให้คำวินิจฉัยว่า "การที่บริษัท HONEYWELL บิดเบือนข้อเท็จจริงเกี่ยวกับคุณภาพของเครื่องคอมพิวเตอร์ก่อนที่จะมีการตกลงทำสัญญาซื้อ เป็นการกระทำผลโดยไม่คำนึงถึงผลที่จะเกิดขึ้นว่าจะทำได้จริงหรือไม่ เพื่อจะให้โจทก์ทำสัญญาซื้อเครื่องเท่านั้น"

ประเด็นที่ถกเถียงกันมากได้แก่เรื่องความเสียหายที่เกิดขึ้น ทางบริษัท ACCUSYSTEMS ได้อ้างว่าความล้มเหลวของเครื่องคอมพิวเตอร์เป็นผลให้บริษัทต้องเลิกล้มกิจการ ในขณะที่บริษัท HONEYWELL ได้กล่าวว่าความเสียหายที่เกิดขึ้นควรจะมีวิธีแก้ไขได้หากผู้บริหารของบริษัทลูกค้ามีความสามารถเพียงพอ

เป็นที่ทราบกันโดยทั่วไปว่า บริษัทผู้จำหน่ายเครื่องคอมพิวเตอร์มักโฆษณาประสิทธิภาพของเครื่องคอมพิวเตอร์เกินความจริง ผู้ขายที่เป็นกิจการขนาดใหญ่หรือบริษัทผู้ผลิตและจำหน่ายชั้นนำอื่น ๆ นั้น ลูกค้าจะมีโอกาสได้รับชดใช้ค่าเสียหายมากกว่ากรณีซื้อจากบริษัทเล็ก ๆ หรือผ่านผู้แทนจำหน่ายซึ่งมีโอกาสเรียกร้องค่าเสียหายได้น้อยมาก

อย่างไรก็ตาม ประเทศสหรัฐอเมริกาและประเทศอังกฤษได้มีการปรับปรุงแก้ไขกฎหมายให้รัดกุมยิ่งขึ้นเพื่อลงโทษตัวบุคคลในบริษัทที่เกี่ยวข้อง ผู้ที่ไม่ซื่อสัตย์หรือขาดความรับผิดชอบในหน้าที่ ซึ่งในขณะนี้ถูกปกป้องอยู่ในรูปแบบที่กลายเป็นความรับผิดชอบของบริษัท นอกจากนี้กฎหมายที่ปรับปรุงใหม่ยังให้การสนับสนุนบุคคลที่สาม โดยเฉพาะอย่างยิ่งบริษัทประกันภัยซึ่งเป็นผู้รับประกันที่ชดใช้ค่าเสียหาย ให้มีสิทธิดำเนินการฟ้องร้องกรรมการบริหารหรือบุคคลที่เกี่ยวข้องนั้น ๆ ด้วย

2) คดีระหว่าง FIRST NATIONAL BANK OF COLUMBUS กับ HANSEN ศาล WISCONSIN วินิจฉัยว่า "บริษัทที่เกี่ยวข้องไม่ได้ฟ้องกรรมการบริหารในประเด็นเกี่ยวกับการมีส่วนร่วมในการปกปิดความไม่ซื่อสัตย์หรือละเลยต่อหน้าที่ของ HANSEN ซึ่งมีผลเท่ากับการทุจริต หากพิสูจน์ได้ว่าผู้บริหารได้รับประโยชน์จากการกระทำผิดในครั้งนี้ด้วย จะต้องให้ความเป็นธรรมกับบุคคลหรือบริษัทที่ชดใช้ค่าเสียหาย โดยจะดำเนินการกับกรรมการบริหารเหล่านี้แทน"

ศาลแห่งรัฐ OREGON ผู้ตัดสินคดีระหว่าง EVARDING กับ FARRELL AND TOFT ได้ให้คำจำกัดความเกี่ยวกับการทุจริตว่า "ความไม่รอบคอบ ละเลยต่อหน้าที่ มีความหมายต่างกับการทุจริตในกรณีที่การเพิกเฉยมีผลทำให้เกิดการกระทำผิด ผู้ต้องสงสัยจะถูกสอบสวนว่ามีเจตนาหรือไม่"

คดีระหว่าง PEOPLE'S NATIONAL BANK กับ GUTER รัฐ KENTUCKEY ได้มีการกล่าวถึงความหมายของการทุจริตว่า "ในการประกอบธุรกิจการค้า การที่ผู้ซื้อมีข้อข้องใจหรือสงสัยในกรณีใด แต่ยังคงเพิกเฉยไม่สอบถาม มีเจตนาละเลยก็ถือว่าเป็นความไม่สุจริตใจ" ในทำนองเดียวกัน คดีระหว่าง TRANSPORT TRUCKING กับ FIRST NATIONAL BANK แห่งรัฐ MISSOURI ศาลมีความเห็นว่า ธนาคารละเลย หรือปฏิเสธที่จะรับรู้ความจริงเมื่อมีโอกาสเพราะเกรงว่าหากสอบถามแล้วจะมีผลทำให้การประกอบธุรกิจรายการนั้นเสียหาย เพราะมีการปฏิบัติที่ไม่ถูกต้อง

MR. ROGER WADE RIZK แห่ง HOWELL LILES BRADDOCK AND MILTON, JACKSONVILLE, FLORIDA ได้ให้ข้อแนะนำในการประเมินความรับผิดชอบของกรรมการบริหารธนาคารไว้ดังนี้

1. ธนาคารมีผู้ตรวจสอบภายในหรือไม่ และผู้ตรวจสอบได้รายงานให้กรรมการบริหารของธนาคารทราบถึงข้อผิดสังเกตอยู่เสมอ แต่กรรมการบริหารของธนาคารยังคงเพิกเฉยไม่ดำเนินการสอบสวนหรือไม่

2. ลูกหนี้ได้ร้องเรียนต่อกรรมการบริหารของธนาคารถึงข้อผิดสังเกตหรือสงสัยในการทำสัญญากู้ และกรรมการบริหารของธนาคารรับทราบแล้วยังเพิกเฉยไม่ดำเนินการใด ๆ หรือไม่

3. ธนาคารได้จ้างผู้ตรวจสอบจากภายนอกมาประเมินการควบคุมภายในของธนาคารหรือไม่ และผู้ตรวจสอบจากภายนอกได้เสนอกรรมการบริหารของธนาคารแล้วว่า การควบคุมภายในไม่เป็นไปตามมาตรการที่กำหนด

4. ผู้ตรวจสอบจากสถาบันประกันเงินฝาก (FEDERAL DEPOSIT INSURANCE CORPORATION-FDIC) หรือจาก STATE DEPARTMENT OF BANKING ได้ให้ข้อสังเกตในการตรวจสอบหรือแจ้งจุดอ่อนการควบคุมภายในเกี่ยวกับการปฏิบัติงานของธนาคาร และกรรมการบริหารของธนาคารมิได้ติดตามดำเนินการ

ความเสียหายที่เกิดขึ้นอันเนื่องจากการทุจริตของพนักงานซึ่งอาจเกิดขึ้นจากการลักลอบใช้ทรัพย์สินหรือข้อมูลของบริษัทเพื่อประโยชน์ส่วนตัวหรือขาดความรอบคอบ เจตนาละเลยต่อหน้าที่ซึ่งเป็นการแสดงถึงความไม่ซื่อสัตย์ควรมีการดำเนินการสืบสวน พิจารณาโทษบุคคลนั้น ๆ ด้วย

เรียบเรียงจากบทความเรื่อง NEGLIGENCE AND THE RESPONSIBILITY OF MANAGERS
วารสาร COMPUTER FRAUD & SECURITY BULLETIN VOL. 6 NO. 10/1984

ภาคผนวก ข

การกำหนดของธนาคารแห่งประเทศไทย
กับระบบรักษาความปลอดภัยของธนาคารพาณิชย์

1. มีการแบ่งแยกหน้าที่และความรับผิดชอบให้ชัดเจนในเรื่องการพัฒนาระบบงาน การบำรุงรักษาระบบงาน การบำรุงรักษาเครื่อง การจัดทำบัตรประจำตัวลูกค้า การจัดทำรหัสประจำตัวลูกค้า การจัดเตรียมเงินสดที่จะบรรจุในกล่องเงิน และการควบคุมข่ายงาน

2. มีเอกสารสนับสนุนการปฏิบัติงาน (Documentation) ให้เพียงพอต่อการควบคุมและปฏิบัติงาน และให้จัดทำสำเนาเพื่อใช้ประกอบการประเมินและตรวจสอบได้ด้วย โดยมีรายละเอียดขั้นต่ำดังนี้

2.1 ต้องมีเอกสารประกอบระบบงาน (System Manual) โดยมีรายละเอียดและคำอธิบายเกี่ยวกับ

2.1.1 ระบบงานทั่วไปและข่ายงาน

2.1.2 เครื่องจักรและอุปกรณ์ประมวลผลและสื่อสาร รวมทั้งระบบสำรอง

2.1.3 การจัดเก็บข้อมูลและระบบสำรองข้อมูล

2.1.4 ลักษณะข้อมูลและการบันทึกรายการในระบบงาน

2.1.5 ระบบงานที่เกี่ยวข้องและการควบคุม

2.1.6 รายงานที่ได้จากระบบงานทุกประเภท

2.2 ต้องมีเอกสารประกอบโปรแกรมคำสั่งงาน (Program Description Manual) โดยมีคำอธิบายเกี่ยวกับ

2.2.1 รายละเอียดแต่ละโปรแกรม ซึ่งประกอบด้วย ชื่อ วัตถุประสงค์ หน้าที่การทำงาน ขั้นตอนการทำงาน และความสัมพันธ์กับตัวระบบงาน

2.2.2 รายละเอียดโปรแกรมใช้งาน (Program Listing)

2.2.3 รายละเอียดโปรแกรมที่ใช้สำหรับการควบคุมและตรวจสอบความถูกต้องของข้อมูล (Edit and Control Program)

2.2.4 รายละเอียดการปรับปรุงแก้ไขระบบงานและโปรแกรมคำสั่งงาน

2.3 ต้องมีเอกสารคู่มือการปฏิบัติงานสำหรับเจ้าหน้าที่ที่เกี่ยวข้องกับระบบงาน (User manual) โดยมีรายละเอียดเกี่ยวกับ

2.3.1 คำอธิบายลักษณะงานและหน้าที่รับผิดชอบ

2.3.2 วิธีการปฏิบัติงานของเจ้าหน้าที่

2.3.3 วิธีการแก้ไขและปรับปรุงรายการเมื่อระบบงานเกิดขัดข้องหรือเกิดข้อผิดพลาด

2.4 ต้องมีเอกสารที่อธิบายองค์ประกอบของระบบงาน ซึ่งประกอบด้วย

2.4.1 ลักษณะทั่วไปและส่วนประกอบของเครื่อง

2.4.2 บัตรประจำตัวลูกค้า

2.4.3 รหัสประจำตัวลูกค้า

2.4.4 ข้อความต่าง ๆ (Message) ที่เกี่ยวข้องทั้งในส่วนของลูกค้าและระบบงาน

2.4.5 การบรรจุกล่องเงิน

2.4.6 การติดต่อสื่อสารกับศูนย์คอมพิวเตอร์พร้อมคำสั่ง (Command Message) ที่ใช้ติดต่อระหว่างกัน

2.4.7 การจัดพิมพ์ใบบันทึกรายการ (Transaction Record)

2.4.8 การทำงานของกลไกในการเบิกจ่ายเงินจากกล่องเงิน

2.4.9 การจัดการเกี่ยวกับการฝากเงินและ/หรือการชำระค่าใช้จ่าย

2.4.10 การบันทึกรายการในทะเบียนต่าง ๆ (Logs)

3. มีการควบคุมระบบสื่อสารข้อมูล โดยมีรายละเอียดขั้นต่ำดังนี้

3.1 ต้องมีการป้องกันไม่ให้บุคคลที่ไม่มีอำนาจเข้าถึงอุปกรณ์และสายสื่อสาร

3.2 ต้องมีการสำรองระบบสื่อสารและแผนการปรับปรุงแก้ไขเมื่อระบบงานหยุดชะงัก

3.3 ต้องมีการบันทึกรายการทุกรายการ และจัดเก็บไว้เป็นหลักฐานเพื่อควบคุมและตรวจสอบ โดยรายการดังกล่าวต้องมีรายละเอียดขั้นต่ำดังนี้

3.3.1 รหัสที่ตั้งเครื่อง

3.3.2 วันที่และเวลาของรายการ

3.3.3 ประเภทของรายการ

3.3.4 เลขที่บัตรและเลขที่บัญชีที่เกี่ยวข้อง

3.3.5 จำนวนเงิน

4. มีการรักษาความปลอดภัยสำหรับผู้ใช้บริการขั้นต่ำ ดังนี้

4.1 ต้องมีเอกสารแจ้งให้ผู้ใช้บริการทราบถึงวิธีการจัดเก็บบัตร รหัสประจำตัว วิธีการแจ้งอายัดบัตร พร้อมทั้งคำเตือนข้อความควรระมัดระวังถึงความเสียหายที่อาจเกิดขึ้นได้

4.2 ต้องมีสัญญาหรือข้อตกลงเป็นลายลักษณ์อักษรกำหนดความรับผิดชอบระหว่างธนาคารพาณิชย์ ผู้ใช้บริการ และผู้ที่เกี่ยวข้องทุกฝ่าย และในกรณีที่มีการเปลี่ยนแปลงข้อกำหนดหรือเงื่อนไขต้องแจ้งให้ผู้ใช้บริการทราบก่อนด้วย

4.3 ต้องมีการป้องกันและรักษาความลับของผู้ใช้บริการมิให้ผู้อื่นได้ทราบและล่วงรู้

4.4 ต้องมีคำเตือนหรืออุปกรณ์ที่ป้องกันมิให้ผู้ใช้บริการลืมหยิบบัตรประจำตัว และใบบันทึกรายการหลังจากทำรายการเสร็จ

5. มีการควบคุมและรักษาความปลอดภัยเกี่ยวกับสถานที่ติดตั้งเครื่องขั้นต่ำดังนี้

5.1 ต้องมีแสงสว่างเพียงพอ และอยู่ในที่เปิดเผยแก่สาธารณชนทั่วไป

5.2 ต้องมีระบบสัญญาณเตือนภัย

6. มีการประกันภัยที่ให้ความคุ้มครองความเสียหายที่เกิดขึ้น

7. มีการควบคุมและรักษาความปลอดภัยอาคารสถานที่ตั้งและเครื่องคอมพิวเตอร์อุปกรณ์เครื่องมือ และระบบงานคอมพิวเตอร์ที่ใช้ประมวลผลข้อมูลและให้บริการของธนาคารพาณิชย์ขั้นต่ำดังนี้

7.1 ต้องมีแผนการรักษาความปลอดภัยและมาตรการป้องกันความเสียหายจากภัยพิบัติต่าง ๆ ที่อาจมีผลให้การดำเนินงานและการให้บริการตามปกติของธนาคารพาณิชย์หยุดชะงัก เช่น อัคคีภัย ภัยธรรมชาติต่าง ๆ ความเสียหายของระบบสื่อสารและระบบงาน ความเสียหายที่เกิดจากบุคคลภายในและภายนอกธนาคารพาณิชย์ และความเสียหายจากภัยพิบัติอื่น ๆ

7.2 ต้องมีแผนการและมาตรการปรับปรุงแก้ไข หรือกำหนดวิธีการอื่นใดที่จะทดแทนการหยุดทำงานของระบบงานด้านคอมพิวเตอร์ เพื่อให้ธนาคารพาณิชย์สามารถดำเนินการและให้บริการได้ตามปกติ

7.3 ต้องมีรายละเอียดขั้นต่ำของแผนการรักษาความปลอดภัยและการปรับปรุงแก้ไขดังนี้

7.3.1 การจัดเตรียมหรือจัดทำระบบสำรองของเครื่องคอมพิวเตอร์อุปกรณ์เครื่องมือและระบบงานคอมพิวเตอร์ เพื่อใช้ทดแทนการทำงานเมื่อเกิดความเสียหาย

7.3.2 ขั้นตอนวิธีการปฏิบัติงาน และอุปกรณ์เครื่องมือที่ใช้ป้องกันหรือเตือนภัย ตามประเภทของภัยที่อาจจะเกิดขึ้น

7.3.3 การบำรุงรักษาและทดสอบการปฏิบัติตามแผนการรักษาความปลอดภัยและแผนการปรับปรุงแก้ไข

7.3.4 การกำหนดอำนาจหน้าที่ความรับผิดชอบของเจ้าหน้าที่และส่วนงานที่เกี่ยวข้องกับแผนการรักษาความปลอดภัยและแผนการปรับปรุงแก้ไข

7.3.5 การจัดลำดับและขั้นตอนของงานที่ต้องปรับปรุงแก้ไข

7.3.6 การประชาสัมพันธ์และสร้างความเข้าใจกับลูกค้าประชาชนที่เกี่ยวข้อง



การกำหนดของธนาคารแห่งประเทศไทย
เรื่อง ขอบเขตการตรวจสอบด้านคอมพิวเตอร์

เพื่อให้เป็นไปตามเงื่อนไขในการเปิดบริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน ซึ่งระบุว่าธนาคารพาณิชย์ต้องจัดให้มีการตรวจสอบด้านคอมพิวเตอร์อย่างน้อยครั้งหนึ่งทุกรอบ 12 เดือน โดยมีขอบเขตการตรวจสอบอย่างเพียงพอตามที่ธนาคารแห่งประเทศไทยกำหนดนั้น ธนาคารแห่งประเทศไทยจึงกำหนดขอบเขตการตรวจสอบด้านคอมพิวเตอร์ขั้นต่ำให้ธนาคารพาณิชย์ต้องปฏิบัติไว้ ดังนี้

1. ต้องมีการตรวจสอบในเรื่องต่าง ๆ ขั้นต่ำ ดังนี้

   1.1 การดำเนินงานการประมวลผลข้อมูลด้วยคอมพิวเตอร์

      1.1.1 การจัดองค์งานด้านคอมพิวเตอร์

      1.1.2 ระบบงานและโปรแกรมคำสั่งงาน

      1.1.3 การควบคุมข้อมูล

      1.1.4 การปฏิบัติงานคอมพิวเตอร์

      1.1.5 การประมวลผลโดยอาศัยระบบสื่อสาร

      1.1.6 การโอนเงินทางอิเล็กทรอนิกส์

      1.1.7 การใช้บริการศูนย์คอมพิวเตอร์ภายนอกธนาคาร (ถ้ามี)

   1.2 ระบบงานที่ประมวลผลข้อมูลด้วยคอมพิวเตอร์ (Application)

      1.2.1 การจัดทำเอกสารสนับสนุนระบบงาน

      1.2.2 การทดสอบระบบงาน

      1.2.3 การปรับปรุงแก้ไขระบบงานและ/หรือโปรแกรมคำสั่งงาน

      1.2.4 การควบคุมการใช้ข้อมูลในระบบงาน

      1.2.5 การควบคุมแฟ้มข้อมูลและโปรแกรมคำสั่งงาน

      1.2.6 การสำรองระบบงาน

   1.3 ความเสียหายทางด้านการเงินที่เกิดจากระบบงานคอมพิวเตอร์หรือจุดอ่อนจากการควบคุมภายในด้านคอมพิวเตอร์ ในกรณีต่าง ๆ ดังต่อไปนี้

      1.3.1 เครื่องคอมพิวเตอร์ อุปกรณ์เครื่องมือ ระบบงานคอมพิวเตอร์ และระบบสื่อสารขัดข้อง หรือหยุดชะงัก หรือเสียหาย

      1.3.2 การทุจริต หรือโจรกรรม หรือความเสียหายอื่น ๆ ที่เกิดจากบุคคลภายในหรือภายนอกธนาคารพาณิชย์

2. ต้องมีข้อมูลเกี่ยวกับการตรวจสอบขั้นต่ำ คือ

2.1 ชื่อ ที่ตั้ง และวันเปิดดำเนินการของศูนย์คอมพิวเตอร์ที่ตรวจสอบ

2.2 วัน เวลาเริ่มต้นและเสร็จสิ้นการตรวจสอบ

2.3 ครั้งที่ของการตรวจสอบ และวันที่ตรวจสอบครั้งก่อน

2.4 รายชื่อผู้ตรวจสอบ

2.5 รายละเอียดในเรื่องต่าง ๆ พร้อมทั้งข้อสังเกตและข้อแนะนำในการตรวจสอบ

2.6 รายละเอียดของความเสียหายทางด้านการเงินที่เกิดจากระบบงานคอมพิวเตอร์หรือจุดอ่อนจากการควบคุมภายในด้านคอมพิวเตอร์ในกรณีต่าง ๆ ประกอบด้วย

2.6.1 สาเหตุและปัญหาที่เกิดความเสียหาย

2.6.2 ข้อบกพร่องหรือจุดอ่อนที่เกิดความเสียหาย

2.6.3 จำนวนเงินที่เสียหาย

2.6.4 มาตรการป้องกันความเสียหายที่ได้ปรับปรุงไปแล้ว

2.7 รายการแนบระบบงาน (Application) ที่ตรวจสอบ

2.7.1 โครงสร้างการจัดองค์งานในส่วนที่ตรวจสอบ

2.7.2 รายละเอียดการปรับปรุงและเปลี่ยนแปลงคอมพิวเตอร์ และโปรแกรมคำสั่งงาน (ถ้ามี)

2.7.3 รายละเอียดระบบงานที่ตรวจสอบ ประกอบด้วย

- ผังการปฏิบัติงาน (Work Flow)
- ผังระบบงาน (System Flowchart)
- ชื่อและวัตถุประสงค์ของโปรแกรมแต่ละโปรแกรมในระบบงาน

2.7.4 เอกสารหลักฐานประกอบพร้อมคำอธิบายความเสียหายที่เกิดขึ้นในแต่ละกรณี

- ร่องรอยหรือรายงานบันทึกรายการที่เสียหายจากคอมพิวเตอร์
- เอกสารหลักฐานอื่น ๆ ที่เกี่ยวข้องกับรายการที่เสียหาย



ภาคผนวก ค

Check Digit

ในระบบงานคอมพิวเตอร์ โดยเฉพาะระบบงานที่ใช้ Data Base เช่น เลขที่บัญชีเงินฝากของธนาคารพาณิชย์ เลขประจำตัวผู้เสียภาษี เลขประจำตัวประชาชน เป็นต้น นิยมใช้ Check Digit ซึ่งเป็นตัวเลข 1 หลักต่อท้ายเลขประจำตัว หรือเลขที่บัญชีต่าง ๆ เพื่อป้องกันการเรียกใช้หรือ Update ข้อมูลผิดบัญชี

1. วิธีการคำนวณหา Check Digit

วิธีการคำนวณหา Check Digit มีหลายวิธี ซึ่งตามตัวอย่างต่อไปนี้ 5 วิธีจะแสดงให้ทราบว่าวิธีการคำนวณหา Check Digit แต่ละวิธี มีขั้นตอนและวิธีการคำนวณอย่างไร โดยทุกตัวอย่างจะใช้ 24757 เป็นเลขที่บัญชีที่ต้องการคำนวณหาค่า Check Digit ตัวอย่าง 5 วิธีดังกล่าว คือ

1.1 Modulus 10 Simple Sum

1.2 Modulus 10 Alternate "2-1-2"

1.3 Modulus 10 Arithmetic

1.4 Modulus 11 Arithmetic

1.5 Modulus 11 Geometric

1.1 Modulus 10 Simple Sum

1) เลขที่บัญชีที่ต้องการหา Check Digit คือ 24757
2) แยกเลขที่บัญชีออกเป็นตัวเลขแต่ละหลัก คือ 2, 4, 7, 5, 7,
3) หาผลบวกของตัวเลขตาม 2) คือ 2 + 4 + 7 + 5 + 7 = 25
4) หารผลบวกตาม 3) ด้วย 10 ซึ่งเป็นค่าของ Modulus ที่ใช้ คือ 25 / 10 = 2 เศษ 5
5) นำเศษ 5 ที่ได้ไปลบออกจากค่าของ Modulus ที่ใช้ คือ 10 - 5 = 5
6) ผลต่างที่ได้คือ Check Digit = 5

1.2 Modulus 10 Alternate "2-1-2"

1) เลขที่บัญชีที่ต้องการหา Check Digit คือ 24757
2) แยกเลขที่บัญชีออกเป็นตัวเลขแต่ละหลัก คือ 2, 4, 7, 5, 7
3) คูณตัวเลขแต่ละหลักตาม 2) ด้วยค่าถ่วงน้ำหนัก (Weighting Factor) 2, 1, 2,...โดยเริ่มจากหลักหน่วยของเลขที่บัญชีไปจนครบทุกหลัก

2	4	7	5	7	
2	1	2	1	2	X
4	4	14	5	14	

4) บวกค่าผลคูณตาม 3) คือ 4 + 4 + 14 + 5 + 14 = 41

5) หารผลบวกตาม 4) ด้วย 10 ซึ่งเป็นค่าของ Modulus ที่ใช้ คือ 41 / 10 = 4 เศษ 1

6) นำเศษ 1 ที่ได้ไปลบออกจากค่าของ Modulus ที่ใช้ คือ 10 - 1 = 9

7) ผลต่างที่ได้คือ Check Digit = 9

1.3 Modulus 10 Arithmetic

1) เลขที่บัญชีที่ต้องการหา Check Digit คือ 24757

2) แยกเลขที่บัญชีออกเป็นตัวเลขแต่ละหลัก คือ 2, 4, 7, 5, 7

3) คูณตัวเลขแต่ละหลักตาม 2) โดยใช้เลขอนุกรมแบบเลขคณิตเป็นค่าถ่วงน้ำหนัก (Weighting Factor) คือ 2, 3, 4, 5, 6, 7, 2, 3, 4, 5, ... โดยเริ่มจากหลักหน่วยของเลขที่บัญชีไปจนครบทุกหลัก

2	4	7	5	7	
6	5	4	3	2	x
12	20	28	15	14	

4) บวกค่าผลคูณตาม 3) คือ 12 + 20 + 28 + 15 + 14 = 89

5) หารผลบวกตาม 4) ด้วย 10 ซึ่งเป็นค่าของ Modulus ที่ใช้ คือ 89 / 10 = 8 เศษ 9

6) นำเศษ 9 ที่ได้ไปลบออกจากค่าของ Modulus ที่ใช้ คือ 10 - 9 = 1

7) ผลต่างที่ได้คือ Check Digit = 1

1.4 Modulus 11 Arithmetic

1) เลขที่บัญชีที่ต้องการหา Check Digit คือ 24757

2) แยกเลขที่บัญชีออกเป็นตัวเลขแต่ละหลัก คือ 2, 4, 7, 5, 7

3) คูณตัวเลขแต่ละหลักตาม 2) โดยใช้เลขอนุกรมแบบเลขคณิตเป็นค่าถ่วงน้ำหนัก (Weighting Factor) คือ 2, 3, 4, 5, 6, 7, 2, 3, 4, 5, ... โดยเริ่มจากหลักหน่วยของเลขที่บัญชีไปจนครบทุกหลัก

2	4	7	5	7	
6	5	4	3	2	x
12	20	28	15	14	

4) บวกค่าผลคูณตาม 3) คือ 12 + 20 + 28 + 15 + 14 = 89

5) หารผลบวกตาม 4) ด้วย 11 ซึ่งเป็นค่าของ Modulus ที่ใช้ คือ 89 / 11 = 8 เศษ 1

6) นำเศษ 1 ที่ได้ไปลบออกจากค่าของ Modulus ที่ใช้ คือ 11 - 1 = 10

7) ผลต่างที่ได้คือ Check Digit = 10

หมายเหตุ ในกรณีที่ใช้ MODULUS 11 หากเลขที่บัญชีใดหาค่า CHECK DIGIT ได้ = 10 จะไม่ใช้เลขที่บัญชีนั้น

1.5 Modulus 11 Geometric

1) เลขที่บัญชีที่ต้องการหา Check Digit คือ 24757
2) แยกเลขที่บัญชีออกเป็นตัวเลขแต่ละหลัก คือ 2, 4, 7, 5, 7
3) คูณตัวเลขแต่ละหลักตาม 2) โดยใช้เลขอนุกรมแบบเรขาคณิตเป็นค่าถ่วงน้ำหนัก (Weighting Factor) คือ 2, 4, 8, 16, ... โดยเริ่มจากหลักหน่วยของเลขที่บัญชีไปจนครบทุกหลัก

2	4	7	5	7	
32	16	8	4	2	X
64	64	56	20	14	

4) บวกค่าผลคูณตาม 3) คือ 64 + 64 + 56 + 20 + 14 = 218.
5) หารผลบวกตาม 4) ด้วย 11 ซึ่งเป็นค่าของ Modulus ที่ใช้ คือ 218 / 11 = 19 เศษ 9
6) นำเศษ 9 ที่ได้ไปลบออกจากค่าของ Modulus ที่ใช้ คือ 11 - 9 = 2
7) ผลต่างที่ได้คือ Check Digit = 2

การคำนวณหา Check Digit ทุกวิธี ถ้าหากผลรวมของผลคูณเมื่อหารด้วยค่า Modulus ที่ใช้ คือ 10 หรือ 11 ได้ลงตัว จะใช้ค่า Check Digit = 0

2. ประโยชน์ของ Check Digit

ตามตัวอย่างที่ 1.3 เลขที่บัญชี 24757 จะต้องมี Check Digit เป็น 1 เท่านั้น จึงใช้ 24757-1 เป็นเลขที่อ้างอิงในระบบงาน หากใช้เลข Check Digit ผิด ระบบงานจะทราบทันทีว่าเลขที่บัญชีนั้นผิด ดังนั้น เลขที่บัญชีที่มี Check Digit ไม่ถูกต้องจะไม่สามารถเข้าสู่ระบบงาน เพื่อประมวลผลต่อไปได้ จึงช่วยลดความผิดพลาดที่อาจเกิดขึ้นให้ลดน้อยลงได้

3. รูปแบบความผิดพลาดที่พบ

ระบบ Check Digit เพียงแต่ช่วยลดความผิดพลาด แต่ไม่สามารถป้องกันหรือตรวจจับความผิดพลาดได้ทั้งหมด โดยเฉพาะในกรณีที่เลขที่บัญชีผิดเป็นเลขที่บัญชีอื่นที่มีเลข Check Digit ถูกต้องตรงกับเลขที่บัญชีในระบบงานพอดี ความผิดพลาดที่เกิดขึ้นมีหลายรูปแบบ ซึ่งวิธีการคำนวณหา Check Digit และค่าถ่วงน้ำหนักที่ใช้แต่ละวิธีสามารถตรวจจับความผิดพลาดแต่ละรูปแบบได้ไม่เท่ากัน

การใช้ Check Digit เพื่อตรวจจับความผิดพลาดของข้อมูลนั้น จะได้ผลมากน้อยเพียงใดขึ้นอยู่กับการเลือกรูปแบบการคำนวณและค่าถ่วงน้ำหนักที่ใช้ ซึ่งจะพบว่าการคำนวณแบบ Modulus 11 ถ่วงน้ำหนักแบบ Arithmetic เป็นแบบที่ดีที่สุด

ในกรณีที่ระบบงานใช้รูปแบบ Check Digit ที่มีจุดอ่อนและไม่สามารถปรับเปลี่ยนเป็นรูปแบบใหม่ได้ อาจใช้วิธีเพิ่มจุดควบคุมและตรวจสอบอื่น ๆ เป็นการชดเชย เช่น การกำหนดให้ระบบงานเงินฝากต้องแสดงชื่อบัญชี ทั้งบนจอภาพและในสลิปใบฝากเงิน เพื่อให้พนักงาน Teller ผู้เกี่ยวข้องและลูกค้าสามารถตรวจสอบได้ว่า ชื่อบัญชีถูกต้องหรือไม่



บรรณานุกรม

1. Auditing EDP Systems โดย Donald A. Watne และ Peter B.B. Turney.
2. Phornar Whiteside, "Computer Capers," New York. The New American Library, Inc., 1979 p.50
3. Bequai, August, Computer Crime.
4. Parker, Donn B., Crime By Computer.
5. Burch, John G. and Joseph L. Sardinas Jr. Computer Control and Audit.
6. Krauss, Leonard I., and Ailleen Macgahen, Computer Fraud and Countermeasure.
7. Allen, Braudt, "The Biggest Computer Fraud : Lessons For CPAs, The Journal of Accountancy.
8. Hemphill, Charles F., Jr. and Hemphill D., Security Safeguards for the Computer.
9. Computer Fraud and Security Bulletin.
10. Manager Guide to Computer Security for Don B. Parker.
11. EDPACS

บันทึก

บันทึก

พิมพ์ที่

หจก. โรงพิมพ์คลังนานาวิทยา

33/17-18 ถนนหน้าเมือง ต.ในเมือง อ.เมือง จ.ขอนแก่น 40000 โทร. (043) 236344, 332152-3 Fax. 333785

