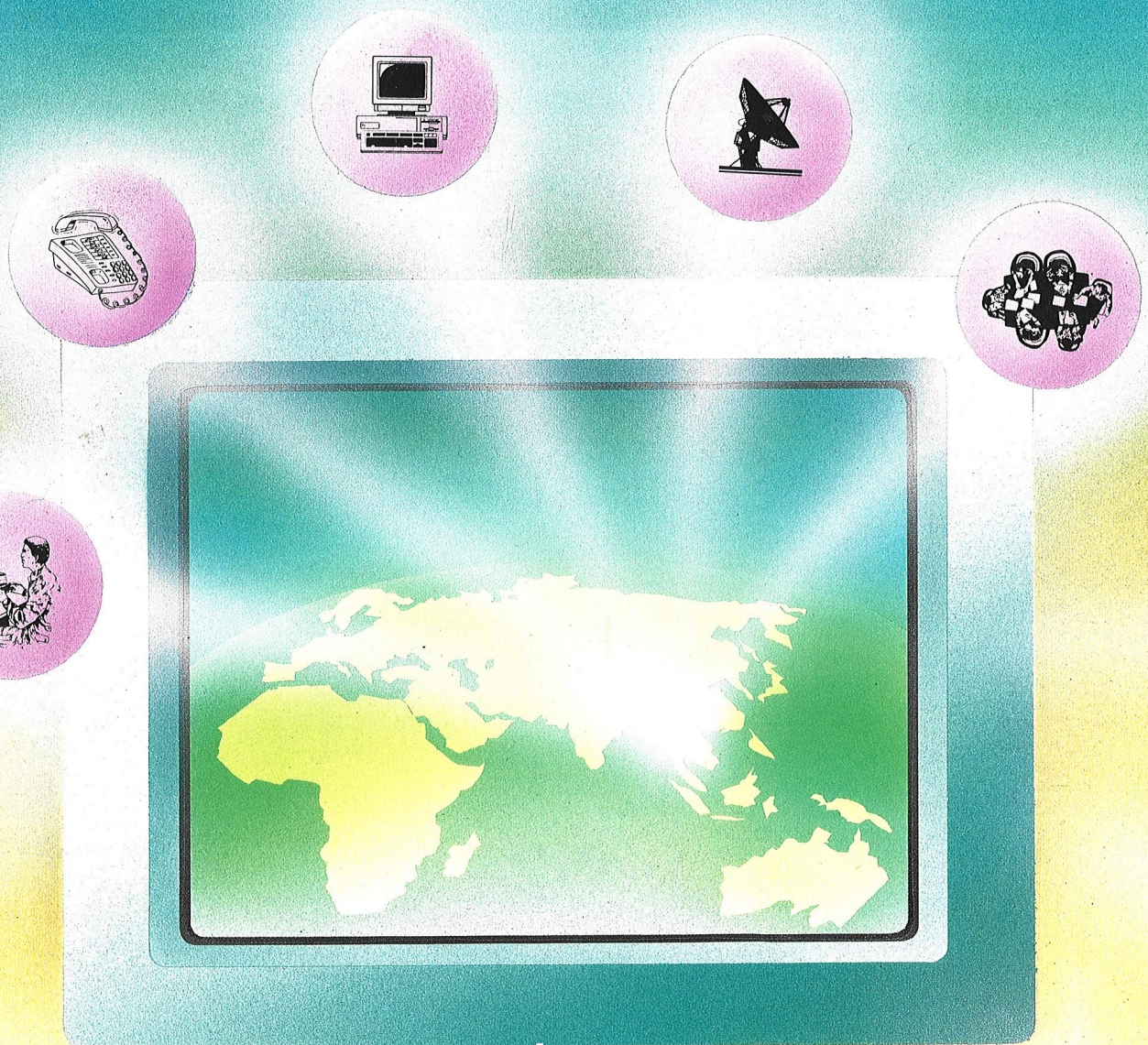


การดำเนินงาน และ การตรวจสอบสถาบันการเงิน ด้านคอมพิวเตอร์



เล่มที่ 1

**การดำเนินงาน
และ
การตรวจสอบสถาบันการเงิน
ด้านคอมพิวเตอร์
เล่ม 1**

เมธา สุวรรณสาร

ISBN 974-89647-9-5

คำนำ

1. การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ เล่มนี้และเล่มต่อ ๆ ไป เป็นการรวบรวมจากเอกสารประกอบการบรรยายเรื่องดังกล่าว โดยมีชื่อเรียกต่าง ๆ กันไปของผมในช่วงเวลาตั้งแต่ปี พ.ศ. 2524-2536 ให้แก่สถาบันหลายแห่ง เช่น การบรรยายให้นักศึกษาปริญญาโท มหาวิทยาลัยธรรมศาสตร์ AIT (Asian Institute of Technology) กลุ่มธนาคารกลางต่าง ๆ ในประเทศเอเชีย (SEACEN-South East Asian Central Banks) มหาวิทยาลัย ธนาคาร พาณิชย์ สถาบันการเงินหลายแห่ง ธนาคารออมสิน สมาคมนักบัญชี และผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย สมาคมธนาคารไทย ชมรมผู้สอบบัญชีภายใน หน่วยงานของรัฐ สมาคมตรวจสอบคอมพิวเตอร์ภาคพื้นกรุงเทพฯ (EDPAA) และสถาบันการฝึกอบรมต่าง ๆ โดยเฉพาะอย่างยิ่งงานบรรยายประจำในช่วงดังกล่าวก็คือ การบรรยายให้ผู้ตรวจสอบของฝ่ายกำกับและตรวจสอบสถาบันการเงิน และฝ่ายกำกับและตรวจสอบธนาคารพาณิชย์ ธนาคารแห่งประเทศไทยในช่วงนั้น

การที่ผมนำเอกสารบรรยายในอดีตหลายครั้งมาจัดทำเป็นรูปเล่มใหม่นี้ การเรียบเรียงและลำดับเรื่องอาจมีข้อมูลบางตอนที่คล้ายกันบ้าง และบางตอนก็อาจนำเรื่องที่เคยกล่าวแล้วไปไว้ในเรื่องที่เกี่ยวข้องอีกเพื่อทำความเข้าใจให้ต่อเนื่องกันไป ทั้งนี้เพราะผมมีแนวการบรรยายและการดำเนินเรื่องที่แตกต่างกันไปในแต่ละครั้ง ซึ่งขึ้นกับความเหมาะสมของผู้ฟังแต่ละองค์กรเป็นหลัก

2. จากหน้าที่หลักที่ผมทำหน้าที่ผู้ตรวจการธนาคารพาณิชย์และสถาบันการเงินต่าง ๆ มานานปี และได้รับมอบหมายจากธนาคารแห่งประเทศไทย ให้ดูแลและรับผิดชอบทางด้านการพัฒนาและการตรวจสอบด้านคอมพิวเตอร์ของสถาบันการเงินในปี 2524 หลังจากทีกลับจากการศึกษา อบรมดูงาน และฝึกงานด้านนี้ครั้งแรกประมาณ 5 เดือน ที่ประเทศสหรัฐอเมริกาและประเทศญี่ปุ่น และต่อมามีโอกาสไปดูงานที่ประเทศอังกฤษทางด้าน Electronic Banking หลังจากนั้นผมและเพื่อนร่วมงานได้ศึกษางานตรวจสอบด้านคอมพิวเตอร์เพิ่มเติมอีกมากเพื่อกำหนดและวางแนวทางการตรวจสอบงานด้านคอมพิวเตอร์ต่อสถาบันการเงินในประเทศไทย

3. จากการที่ผมทำงานทางด้านกำกับและตรวจสอบธนาคารพาณิชย์ รวมทั้งได้ทำงานทางด้านกำกับและตรวจสอบสถาบันการเงินในช่วงเวลาอันยาวนาน ตลอดเวลาที่ทำงานที่ธนาคารแห่งประเทศไทย เป็นเวลาเกือบ 30 ปี ติดต่อกัน ทำให้พอจะมองเห็นภาพและปัญหาการดำเนินงานของธนาคารพาณิชย์และสถาบันการเงินทั้งทางด้าน Financial และด้าน Computer ได้พอสมควร จึงได้รับเชิญให้เป็นผู้บรรยายงานทั้ง 2 ด้าน โดยเฉพาะในช่วงหลังที่ธนาคารให้ผมมารับผิดชอบงานด้านการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ด้วย ผมจึงมีโอกาสดำเนินการบรรยายในรูปแบบความสัมพันธ์และความเกี่ยวข้องซึ่งกันและกันของงานทางด้าน Financial และ Computer ซึ่งอย่างหลังนี้มักจะเรียกกันในปัจจุบันว่า IT (Information Technologies) หรือ IS (Information Systems) เพราะมีความหมายกว้างขวางและเหมาะสมกว่า Computer หรือ EDP (Electronic Data Processing) มาก ดังนั้น ถ้าพูดคำว่า IT Audit หรือ IS Audit แล้วละก็ คำ ๆ นี้ก็คือ Computer หรือ EDP Audit นั่นเอง

4. ความหมายของ Computer Audit ในสายงานของผู้กำกับและผู้ดูแลสถาบันการเงินในความหมายกว้างก็คือ การตรวจสอบการดำเนินงานด้านคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงและความสามารถในการดำเนินงานอย่างต่อเนื่องโดยมีประสิทธิภาพในองค์กรที่ใช้คอมพิวเตอร์ และในความหมายแคบก็คือ การตรวจสอบเพื่อประเมินการควบคุมความเสี่ยงต่าง ๆ จากการดำเนินงานและการบริหารงานด้านคอมพิวเตอร์ที่มีผลเกี่ยวข้องกับความถูกต้องความน่าเชื่อถือได้ของข้อมูลทางการเงินและการควบคุมภายใน เพื่อให้คำแนะนำในแนวทางป้องกันปัญหาล่วงหน้าก่อนที่ปัญหาจริงจะเกิดขึ้น อย่างไรก็ตาม ขอบเขตของการตรวจสอบด้านคอมพิวเตอร์จะขึ้นอยู่กับเป้าหมายของการตรวจสอบเป็นสำคัญ

5. ความเสี่ยง (Risks) ทางด้านคอมพิวเตอร์เป็นความเสี่ยงในรูปแบบใหม่เพิ่มเติมจากความเสี่ยงในการดำเนินงานตามปกติ ที่อาจมีผลเสียหายต่อฐานะและความมั่นคงของสถาบันการเงินที่สำคัญคือ

1) การหยุดชะงักการให้บริการ ซึ่งเกิดจาก Hardware failure, Software failure หรือปัญหาทางบุคลากรที่ใช้คอมพิวเตอร์อย่างไม่ถูกต้อง ซึ่งเรื่องนี้สถาบันการเงินอาจต้องหยุดการให้บริการ ทั้ง ๆ ที่ไม่มีปัญหาด้านสภาพคล่องได้

2) ความผิดพลาดของข้อมูลทางการเงิน

3) การตัดสินใจที่ผิดพลาดของผู้บริหารอันเกิดจากความผิดพลาดของข้อมูล

4) ข้อมูลทางการเงินและการบัญชีไม่อาจยอมรับได้

5) การทุจริตหรือความเสียหาย ซึ่งบางกรณีเป็นเงินจำนวนมาก

6) ค่าใช้จ่ายส่วนเกินที่เกิดจากการใช้คอมพิวเตอร์อย่างไม่มีประสิทธิภาพ หรือเกิดจากความล้มเหลวของ Hardware หรือ Software หรือบุคลากร ซึ่งบางกรณีกระทบกับความมั่นคงโดยตรงของสถาบันการเงิน

7) เสียเปรียบทางการแข่งขันและการบริการ ซึ่งมีผลต่อชื่อเสียงของสถาบันและส่วนแบ่งด้านการตลาด

ความเสี่ยงในแต่ละเรื่องข้างต้น เคยมีตัวอย่างที่ก่อให้เกิดความเสียหายในต่างประเทศและในประเทศเองทุกกรณี และบางกรณีเป็นเรื่องร้ายแรงมาก กรณีของในประเทศมักจะเป็นความลับไม่ได้รับการเปิดเผยทั่วไปส่วนใหญ่ ความเสี่ยงและความเสียหายบางประเภท เช่น การหยุดชะงักการให้บริการเป็นเวลานานกว่า 1 วันทำการ เป็นสิ่งที่ทางการจะยอมให้เกิดขึ้นไม่ได้ การตรวจสอบในลักษณะ After the fact สำหรับ Computer Audit จึงไม่ได้ผล การตรวจสอบที่มีประสิทธิภาพ คือการตรวจสอบในลักษณะ Before the fact และให้คำแนะนำที่มีประสิทธิภาพล่วงหน้า ก่อนที่ปัญหาจริง ๆ จะเกิดขึ้น นั่นเอง

การดูแลความมั่นคงของสถาบันการเงินของธนาคารแห่งประเทศไทย จึงต้องดูแลในทุกเรื่องที่เกี่ยวข้องกับเสถียรภาพและประสิทธิภาพในการบริหารงานเพื่อให้สถาบันการเงินนั้นสามารถดำเนินการได้อย่างต่อเนื่องและมั่นคงตลอดไป

6. จากการบรรยาย เรื่อง การตรวจสอบงานด้านคอมพิวเตอร์ ให้ผู้บริหารระดับสูงของธนาคารออมสิน สำนักงานใหญ่ และหน่วยงานต่าง ๆ ของรัฐ ในช่วงท้าย ๆ ก่อนที่ผมจะเดินทางมารับงานในตำแหน่งผู้อำนวยการสาขา

ที่ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือจังหวัดขอนแก่น ในปลายปี 2536 ซึ่งผมได้รวบรวมเอกสารเท่าที่รวบรวมได้ในเวลาจำกัดจากการบรรยายที่ผ่านมาให้ผู้เข้ารับฟังการบรรยายนั้น ธนาคารอมลสิน สำนักงานใหญ่ได้รวบรวมและเย็บเข้าเล่มจนเป็นที่สนใจของผู้พบเห็นในโอกาสต่อมา และมีการขอร้องให้รวบรวมจัดทำเป็นเล่มขึ้นใหม่เพื่อเป็นวิทยาทานต่อไปด้วย

ผมได้มีโอกาสพิจารณาเรื่องนี้อีกครั้ง เมื่อผู้ตรวจสอบงานด้านคอมพิวเตอร์จากธนาคารอาคารสงเคราะห์ สำนักงานใหญ่ ได้นำเอกสารที่ผมใช้ประกอบการบรรยายบางส่วนมาจัดพิมพ์เข้าแผ่น diskette ทำให้ได้ตัวพิมพ์ที่ชัดเจนขึ้นมาก ส่งผลให้การรวบรวมงานพิมพ์เอกสารประกอบการบรรยายงานด้านคอมพิวเตอร์ของผมในโอกาสต่อมาทำได้สะดวกขึ้น

7. เมื่อผมได้ทำหน้าที่ผู้อำนวยการ ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือที่จังหวัดขอนแก่น เมื่อวันที่ 1 ตุลาคม 2536 เป็นต้นมา ผมก็ยังคงมีหน้าที่หลักประการหนึ่งที่สาขาภาคฯ เช่นเดียวกับที่กรุงเทพฯ นั้นคือการกำกับดูแลฐานะดำเนินงานและความมั่นคงของสถาบันการเงินต่าง ๆ ในภาคตะวันออกเฉียงเหนือ ทั้ง 19 จังหวัดอยู่ด้วย ประกอบกับผมมีความเชื่อมั่นว่า การกำกับสถาบันการเงินที่ได้ผลจะต้องมาจากการป้องกันปัญหาก่อนที่จะเกิดปัญหากับสถาบันการเงินเหล่านั้นวิธีการหนึ่งที่จะบรรลุเป้าหมายนี้ก็คือการให้ผู้บริหารสถาบันการเงินต่าง ๆ มีจรรยาบรรณที่ดี มีความรู้ ความสามารถ รู้จักวิเคราะห์และเข้าใจถึงความเสี่ยงและการป้องกันความเสี่ยงในการบริหารงานของสถาบันการเงินนั้นๆ ผมจึงได้เผยแพร่แจกจ่ายหนังสือเล่มแรก เรื่อง "การจัดระบบควบคุมภายในของสถาบันการเงิน" ให้กับธนาคารพาณิชย์ และสถาบันการเงินทั่วทั้งภาคอีสาน เมื่อปี 2537-2538 และหนังสือเล่มนี้ได้ใช้ในการบรรยายเรื่องดังกล่าวในโอกาสต่าง ๆ ด้วย

8. จากการพบปะกับผู้บริหารสถาบันการเงินต่าง ๆ ในภาคอีสาน ผมได้ปรารภและได้พูดถึงบทบาทของคอมพิวเตอร์ในวงการสถาบันการเงินหลายครั้ง เนื่องจากปรากฏว่า มีสาขาธนาคารพาณิชย์บางแห่ง ในภาคตะวันออกเฉียงเหนือประสบความเสียหายจากการทุจริตที่ใช้คอมพิวเตอร์เป็นเครื่องมือด้วย จึงมีผู้สนใจใคร่จะติดตามเรื่องดังกล่าวมากขึ้น ประกอบกับธนาคารพาณิชย์หลายแห่งได้ให้พนักงานศึกษาเรื่องนี้มากขึ้นเรื่อย ๆ ผมจึงเห็นเป็นโอกาสดีที่จะเผยแพร่หนังสือ เรื่อง "การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์" ซึ่งเป็นการรวบรวมเรื่องที่นำเสนอใจด้านคอมพิวเตอร์ในแง่มุมหลายประการจากเอกสารต่าง ๆ ที่ผมเคยแจกจ่ายให้กับผู้เข้าฟังการสัมมนาและการบรรยายของผมในอดีตที่ผ่านมาในช่วงปี 2524-2536 โดยรวบรวมเรื่องใหม่ จัดเรื่องและเนื้อหาในบางส่วนเพิ่มเติมจากที่มีการรวบรวมไว้แล้วใหม่ โดยเฉพาะอย่างยิ่ง เรื่อง การดำเนินงานด้านคอมพิวเตอร์ ซึ่งได้จัดพิมพ์ใหม่และอาจจะใช้เป็นแนวทางในการปฏิบัติงานด้านคอมพิวเตอร์ในสถาบันการเงินและองค์กรต่าง ๆ ได้ตามสมควร นอกจากนั้นผมยังได้ค้นหาเอกสารที่ได้จัดทำไว้จำนวนมากที่ยังกระจัดกระจายตามหีบห่อเก็บสัณนิษฐานของผมก่อนย้ายมาประจำที่จังหวัดขอนแก่น ก็ปรากฏว่ามีเรื่องที่น่าสนใจที่ไม่เคยเผยแพร่หลายเรื่องด้วยกัน หากผมต้องรวบรวมจัดพิมพ์ในครั้งเดียวกัน ก็จะต้องใช้เวลานานมากขึ้นและเอกสารก็จะหนาเกินไป ผมจึงแยกจัดทำเป็นเล่ม 1 เล่ม 2 และอาจมีถึงเล่ม 3

9. สำหรับเล่ม 1 จะเป็นการบรรยายเน้นหนักในเรื่องที่เกี่ยวข้องกับการดำเนินงานด้านคอมพิวเตอร์ และ ข้อคิดเห็น รวมทั้งข้อสังเกตในการบริหารงานรวมทั้งหลักการการตรวจสอบในบางเรื่อง เล่ม 2 จะเป็นรายละเอียดและ เน้นด้านการควบคุมภายในและการตรวจสอบด้านคอมพิวเตอร์ รวมทั้งการจัดทำแผนฉุกเฉินเป็นหลัก สำหรับเล่ม 3 จะแสดงตัวอย่างของจุดอ่อนทางคอมพิวเตอร์ต่าง ๆ ที่พบในประเทศไทยและต่างประเทศ โดยเฉพาะอย่างยิ่งการกล่าว ถึงการทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือและแนวทางการตรวจสอบการทุจริตทางด้านคอมพิวเตอร์ที่น่าสนใจ โดย ผมได้ดัดแปลง เรียบเรียงเพิ่มเติมจากหลักการตรวจสอบงานด้านคอมพิวเตอร์ตามปกติ ให้ไปสู่แนวทางการตรวจสอบ การทุจริตด้านคอมพิวเตอร์หรือโดยใช้คอมพิวเตอร์ รวมทั้งตัวอย่างการตรวจสอบการทุจริตด้านคอมพิวเตอร์ และ ความร่วมมือระหว่างผู้ตรวจสอบด้านการเงินกับผู้ตรวจสอบด้านคอมพิวเตอร์ เมื่อมีการทุจริตเกิดขึ้น

10. เอกสารประกอบการบรรยายของผมในหนังสือเล่มนี้ รวมทั้งอีก 2 เล่มที่จะพิมพ์ขึ้นนั้น มีหลายบทที่ ใช้คำว่าธนาคารมากกว่าคำว่าสถาบันการเงิน ทั้งนี้เพราะผมได้บรรยายให้กับบุคคลในวงการธนาคารพาณิชย์และธนาคาร อื่น ๆ มากกว่าสถาบันการเงินโดยทั่วไป อย่างไรก็ตามก็ตีความหมายของคำว่าธนาคารนี้ก็ใช้ได้กับสถาบันการเงินโดยทั่วไป และอาจประยุกต์ใช้กับองค์กรอื่น ๆ ที่ใช้คอมพิวเตอร์ในการประมวลผลข้อมูลได้ด้วย อย่างไรก็ตามได้แก้ไขถ้อยคำ ส่วนใหญ่ที่ใช้คำว่า ธนาคารเป็นสถาบันการเงินแล้ว แต่ผมไม่ได้แก้ไขรายการตัวอย่างที่ระบุวันที่ไว้ ทั้งนี้เพื่อให้ ท่านผู้อ่านได้ทราบว่าเป็นการบรรยายในอดีตที่ผ่านมา

11. เนื่องจากผมไม่มีเวลาแก้ไขเพิ่มเติมข้อมูลจากการบรรยายเรื่องต่าง ๆ ของเอกสารเล่มนี้ ซึ่งส่วนใหญ่ เป็นการบรรยายในอดีตตามที่กล่าวถึงข้างต้นแล้ว จึงอาจมีข้อมูลบางส่วนที่อาจไม่ทันสมัยเหมาะกับยุคอยู่บ้าง อย่างไร ก็ดี ข้อมูลหรือเนื้อความมากกว่าร้อยละ 95 ยังคงใช้ได้ดียิ่งจนถึงปัจจุบัน

12. เอกสารเล่มนี้และเล่มต่อ ๆ ไป ได้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อแจกจ่ายและเผยแพร่ให้กับพนักงาน ในส่วนกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทยและสถาบันการเงินต่าง ๆ ในภาคตะวันออกเฉียงเหนือ เพื่อเป็น ส่วนหนึ่งของการทำความเข้าใจในการบริหารงานและการดำเนินงานด้านคอมพิวเตอร์ รวมทั้งเรื่องการตรวจสอบ ซึ่งนับ วันจะมีบทบาทมากขึ้นในแทบจะทุกธุรกรรมของทุกองค์กรโดยเฉพาะอย่างยิ่งในสถาบันการเงิน และเป็นส่วนหนึ่งของการ ป้องกันปัญหาก่อนที่จะเกิดปัญหากับสถาบันการเงินในลักษณะที่เรียกว่า Point to the problem before it points to us. นอกจากนี้จะได้เผยแพร่ในวงการศึกษาซึ่งการเรียนการสอนการดำเนินงานด้านคอมพิวเตอร์และการตรวจสอบ ในปัจจุบันยังอยู่ในวงจำกัดค่อนข้างมาก ทั้ง ๆ ที่คอมพิวเตอร์ได้รับการยอมรับและมีใช้กันโดยทั่วไปในองค์กรต่าง ๆ แล้ว

13. เอกสารทั้ง 3 เล่ม ไม่มีการจำหน่าย แต่มีไว้เพื่อแจกจ่ายตามวัตถุประสงค์ที่กล่าวในข้อ 12. ข้างต้น การเผยแพร่ข้อมูลจากหนังสือเล่มนี้ต่อไปในรูปอื่นใด ควรจะได้อ้างอิงถึงที่มาของข้อมูลด้วย หนังสือเล่มนี้ไม่ได้กล่าว หรืออธิบายถึงการทำงานของระบบคอมพิวเตอร์โดยทั่วไป ทั้งนี้ผมได้ตั้งแนวทางไว้ว่าผู้อ่านได้ทราบเรื่องดังกล่าวพอ สมควรแล้ว

14. ขอขอบคุณบรรดาเพื่อนร่วมงานในอดีตทุกท่าน โดยเฉพาะในรุ่นบุกเบิกการตรวจสอบงานด้านคอมพิวเตอร์ ที่มีส่วนทำให้งานตรวจสอบด้านคอมพิวเตอร์แพร่หลายมากขึ้นในปัจจุบัน และขอขอบคุณอีกครั้งสำหรับการมีส่วนร่วมใด ๆ ที่ผ่านมากในกิจกรรมเผยแพร่เอกสาร การดำเนินงาน และการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ และขอขอบคุณเพื่อนร่วมงานในส่วนกำกับสถาบันการเงินธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ ในปัจจุบันที่ช่วยตรวจทานความถูกต้องในการพิมพ์ครั้งนี้ด้วย

เมธา สุวรรณสาร

ผู้อำนวยการ

ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ

25 มีนาคม 2539

สารบัญ

หน้า

1. ลำดับการพัฒนางานด้านคอมพิวเตอร์ในวงราชการของไทย	1
2. ส่วนงานของคอมพิวเตอร์ในระบบงานขององค์กร	5
3. เทคโนโลยีทางคอมพิวเตอร์	9
☐ Terminal	11
☐ Offline, Input/Output devices	11
☐ Communications	11
☐ Storage media	11
☐ Programming	11
☐ Database	11
☐ System Documentation	11
☐ ผลกระทบจากการที่รูปแบบของหลักฐานที่ใช้ในการตรวจสอบได้เปลี่ยนแปลงไป	13
☐ สภาวะแวดล้อมของธุรกิจที่ใช้คอมพิวเตอร์กับ Audit and Control	20
4. คอมพิวเตอร์กับบทบาทของธนาคารแห่งประเทศไทย	21
☐ คอมพิวเตอร์กับธนาคารพาณิชย์ในประเทศไทย	23
☐ ผลกระทบของคอมพิวเตอร์หรือธนาคารอิเล็กทรอนิกส์ต่อการกำกับและตรวจสอบธนาคารพาณิชย์	23
☐ ความเสี่ยง (Risk) ของธนาคารอิเล็กทรอนิกส์บางประการ	24
☐ การกำกับและตรวจสอบธนาคารอิเล็กทรอนิกส์ในปัจจุบัน	25
☐ การตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์	26
☐ ความเสี่ยงในการดำเนินงานด้านคอมพิวเตอร์อันอาจมีผลกระทบต่อฐานะของธนาคารพาณิชย์	26
☐ เป้าหมายหลักของธนาคารแห่งประเทศไทย	26
☐ มาตรการของ ธปท. ทางด้านคอมพิวเตอร์ที่เกี่ยวข้องกับธนาคารพาณิชย์บางประการ	28
☐ สรุป	31

5. มาตรฐานการดำเนินงานด้านคอมพิวเตอร์	33
□ การตรวจสอบของผู้ตรวจสอบภายในและผู้สอบบัญชี	35
– การคัดเลือกคณะผู้ตรวจสอบ	35
– หน้าที่และความรับผิดชอบของผู้ตรวจสอบภายใน	35
– ความรู้ความสามารถของผู้ตรวจสอบภายในด้านคอมพิวเตอร์	36
– ความเป็นอิสระของผู้ตรวจสอบ	36
– คู่มือการตรวจสอบภายใน	37
– การวางแผน การจัดคณะผู้ตรวจสอบ และการกำกับการตรวจสอบด้านคอมพิวเตอร์	37
– วิธีการตรวจสอบ	38
– เทคนิคการตรวจสอบคอมพิวเตอร์ในระบบที่ทันสมัย	40
– การเข้าร่วมพัฒนาและทดสอบงานที่นำเข้าคอมพิวเตอร์	42
– การจัดทำเอกสารและรายงานการตรวจสอบ	42
– การติดตามผลการตรวจสอบ	43
– ความรู้ความสามารถและความเป็นอิสระของผู้สอบบัญชี	43
– ความรับผิดชอบของผู้สอบบัญชี	44
– การตรวจสอบกิจการที่รับจ้างประมวลผล	45
– การประเมินงานตรวจสอบของผู้ตรวจสอบภายในและผู้สอบบัญชี	45
□ การจัดองค์การของหน่วยงานด้านคอมพิวเตอร์	46
– มาตรฐานขั้นต่ำของการจัดองค์การของศูนย์คอมพิวเตอร์	46
– การตรวจสอบการจัดองค์การของหน่วยงานด้านคอมพิวเตอร์	50
□ มาตรฐานของระบบงาน	50
– การควบคุมโครงการ	51
– มาตรฐานการพัฒนาระบบงานโดยทั่วไป	51
– กระบวนการพัฒนาระบบงาน	51
– การจัดหาหรือจัดซื้อโปรแกรมสำเร็จรูป	52
– มาตรฐานการเขียนโปรแกรม	52
– มาตรฐานการทดสอบระบบงานและโปรแกรม	52
– มาตรฐานการนำระบบงานใหม่ออกใช้งาน	52
– การตรวจสอบผลการนำระบบงานใหม่ออกใช้งาน	53
– การรักษาความปลอดภัยเกี่ยวกับ Operating Systems	53
– การควบคุมการปฏิบัติงานของ Application Programmer	54
– การรักษาความปลอดภัยเกี่ยวกับโปรแกรมที่ใช้ประมวลผล	54
– การควบคุมการปรับปรุงแก้ไขโปรแกรม	55

– การควบคุมการปรับปรุงแก้ไขโปรแกรมในกรณีเร่งด่วนเป็นการชั่วคราว	55
– การตรวจสอบมาตรฐานของระบบงาน	56
□ เอกสารสนับสนุนการปฏิบัติงาน	56
– มาตรฐานการจัดทำเอกสารสนับสนุนการปฏิบัติงาน	57
– คู่มือที่ใช้เป็นมาตรฐานในการปฏิบัติงานด้านคอมพิวเตอร์โดยทั่วไป	57
– เอกสารสนับสนุนการปฏิบัติงานด้าน Software	58
– การควบคุมดูแลและการบำรุงรักษาเอกสาร	60
– คู่มือสำหรับผู้ใช้อุปกรณ์	60
– เอกสารสนับสนุนการปฏิบัติงานที่ประกอบมากับ Software สำเร็จรูป ที่สถาบันการเงินจัดหาหรือซื้อมาใช้งาน	60
– การตรวจสอบเอกสารสนับสนุนการปฏิบัติงาน	61
□ การปฏิบัติงานคอมพิวเตอร์	61
– การรักษาความสะอาดในห้องคอมพิวเตอร์	61
– การบำรุงรักษาเครื่องคอมพิวเตอร์	61
– การแบ่งแยกและสับเปลี่ยนหน้าที่	62
– การใช้เครื่องคอมพิวเตอร์ในการประมวลผล	62
– การจัดทำตารางการใช้เครื่องคอมพิวเตอร์	62
– การควบคุมการใช้เครื่องคอมพิวเตอร์	62
– การควบคุมการปฏิบัติงานของเจ้าหน้าที่ปฏิบัติการในห้องคอมพิวเตอร์	62
– การควบคุม Library	62
– การตรวจสอบการปฏิบัติงานคอมพิวเตอร์	63
□ การจัดทำข้อมูลที่น่าเชื่อถือได้ โดยผู้ตรวจการธนาคารพาณิชย์	63
– งานขั้นต้นในการจัดทำและการจัดส่งข้อมูลเพื่อประมวลผล	64
– การป้อนข้อมูลโดยใช้เครื่อง Terminal	66
– การพิสูจน์ยอด Batch และการควบคุมข้อมูล	67
– การควบคุมการจัดทำข้อมูล	68
– การควบคุมอุปกรณ์ที่ใช้บันทึกข้อมูล	69
– การจัดส่งรายงานให้ผู้ใช้อุปกรณ์และการควบคุม	72
– การสอบทานและการกระหายยอดรายงาน	72
– การจัดเก็บข้อมูลในระบบ data base	74
– การรักษาความปลอดภัยในระบบ data base	76
– การตรวจสอบการจัดทำข้อมูลที่น่าเชื่อถือได้	81

□ การรักษาความปลอดภัย	82
– แผนการรักษาความปลอดภัย	82
– การรักษาความปลอดภัยอาคารสถานที่	83
– การรักษาความปลอดภัยตู้เงินและห้องมั่นคง	83
– การป้องกันความเสียหายเนื่องจากภัยต่าง ๆ โดยทั่วไป	83
– การรักษาความปลอดภัยแฟ้มข้อมูล	83
– การจัดระบบสำรอง	83
– การประกันภัย	84
– การตรวจสอบ การรักษาความปลอดภัย	84
□ การประมวลผลโดยอาศัยระบบสื่อสาร	85
– การประมวลผลในระบบ On-Line	85
– การควบคุมการประมวลผลที่ใช้ระบบสื่อสาร	85
– การเตรียมอุปกรณ์และวิธีการปฏิบัติงานกรณีระบบสื่อสารขัดข้อง	88
– การตรวจสอบ การประมวลผลโดยอาศัยระบบสื่อสาร	89
□ การใช้บริการด้านคอมพิวเตอร์ภายนอกสถาบันการเงิน	89
– การคัดเลือกศูนย์บริการคอมพิวเตอร์	89
– การทำสัญญาระหว่างสถาบันการเงินกับศูนย์บริการคอมพิวเตอร์	90
– การควบคุมการปฏิบัติงาน	90
– การป้องกันและเก็บรักษาข้อมูลของสถาบันการเงิน	92
– การพิจารณาฐานะการเงินของศูนย์บริการคอมพิวเตอร์	92
– การตรวจสอบ การใช้บริการด้านคอมพิวเตอร์ภายนอกสถาบันการเงิน	93

6. มาตรฐานการสอบบัญชีของไทย ในส่วนที่เกี่ยวข้องกับคอมพิวเตอร์

ฉบับที่ 28 ฉบับที่ 29 ฉบับที่ 36	95
----------------------------------	----

□ มาตรฐานการสอบบัญชี ฉบับที่ 28 สมาคมนักบัญชีและผู้สอบบัญชี รับอนุญาตแห่งประเทศไทย เรื่อง การสอบบัญชี ในกรณีที่ธุรกิจใช้คอมพิวเตอร์	97
– ความรู้ความชำนาญ	97
– การใช้บุคคลอื่นช่วยตรวจสอบ	97
– การวางแผนงาน	98
– หลักฐานการสอบบัญชี	98
– ระบบบัญชีและการควบคุมภายใน	99
– วันถือปฏิบัติ	99

❑ มาตรฐานการสอบบัญชี ฉบับที่ 29 สมาคมนักบัญชีและผู้สอบบัญชี รับอนุญาตแห่งประเทศไทย เรื่อง การประเมินประสิทธิภาพการควบคุมภายใน กรณีกิจการใช้คอมพิวเตอร์ – ลักษณะที่สำคัญของกิจการใช้คอมพิวเตอร์ – การจัดโครงสร้างขององค์กร – วิธีการประมวลผล – การออกแบบและวิธีปฏิบัติงาน – การควบคุมภายในของระบบงานคอมพิวเตอร์ – การควบคุมทั่วไป – การควบคุมเฉพาะระบบ – การสอบทานการควบคุมภายในและการประเมินประสิทธิภาพขั้นต้น – การสอบทานการควบคุมทั่วไป – การสอบทานการควบคุมเฉพาะระบบงาน – การประเมินประสิทธิภาพการควบคุมภายในขั้นต้น – การทดสอบการปฏิบัติตามระบบและการประเมินประสิทธิภาพขั้นสุดท้าย – การรายงานถึงจุดอ่อนของการควบคุมภายใน – วันถือปฏิบัติ	100 100 101 101 102 104 104 105 106 106 106 107 108 108 109
❑ มาตรฐานการสอบบัญชี ฉบับที่ 36 สมาคมนักบัญชีและผู้สอบบัญชี รับอนุญาตแห่งประเทศไทย เรื่อง การใช้คอมพิวเตอร์ช่วยในการสอบบัญชี – การใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี – การใช้ข้อมูลทดสอบ – ลักษณะงานที่สามารถใช้คอมพิวเตอร์ช่วยในการสอบบัญชี – ข้อควรพิจารณาเมื่อใช้คอมพิวเตอร์ช่วยในการสอบบัญชี – ความรู้ ความสามารถ ความชำนาญงาน ตลอดจนประสบการณ์ ทางด้านคอมพิวเตอร์ของผู้สอบบัญชี – ความเหมาะสมและสอดคล้องกันระหว่างโปรแกรมคอมพิวเตอร์ ที่ใช้เพื่อการตรวจสอบกับอุปกรณ์คอมพิวเตอร์ของกิจการ – สถานการณ์ที่จำเป็นต้องใช้คอมพิวเตอร์ช่วยในการสอบบัญชี – ลักษณะการจัดเก็บและขนาดของแฟ้มข้อมูลที่จะทำการทดสอบ – ประสิทธิภาพและประสิทธิผลในการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี – ช่วงเวลาในการตรวจสอบ – ลำดับขั้นตอนของการนำคอมพิวเตอร์ช่วยในการสอบบัญชี – การควบคุมการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี	110 111 111 112 113 113 114 114 115 115 116 116 117

- กระดาษทำการ	118
- ข้อควรพิจารณาอื่นในการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี	119
- วันถือปฏิบัติ	120
- ภาคผนวก คำอธิบายศัพท์เทคนิคที่ใช้ในแถลงการณ์มาตรฐานการสอบบัญชีฉบับนี้	121
7. ข้อคิดและแนวทางบางประการในการบริหารงานตรวจสอบองค์กรที่ใช้คอมพิวเตอร์	123
❑ ผู้ตรวจสอบกับการเปลี่ยนแปลงทางเทคโนโลยีที่เกี่ยวกับการบันทึกข้อมูล	125
❑ สภาพการตรวจสอบด้าน EDP ในปัจจุบัน	125
❑ สรุปปัญหาที่เกิดขึ้นแล้ว	126
❑ แนวโน้มการเปลี่ยนแปลงของการตรวจสอบในอนาคต	126
- การเปลี่ยนแปลงในตัวผู้ตรวจสอบ	126
- การเปลี่ยนแปลงกระบวนการตัดสินใจเกี่ยวกับเรื่องที่จะตรวจ	126
- การเปลี่ยนแปลงความคิดเห็นเกี่ยวกับการควบคุมภายใน	127
- การเปลี่ยนแปลงวิธีการประเมินผลการควบคุมของผู้ตรวจสอบ	127
❑ แนวความคิดในการพัฒนาการตรวจสอบ	127
❑ การเปลี่ยนแปลงที่เกิดขึ้นในระบบงานยุคใหม่ที่ใช้คอมพิวเตอร์	128
- วัตถุประสงค์ในการตรวจสอบ	129
- สาเหตุที่ใช้คอมพิวเตอร์ทำให้ผู้ตรวจสอบต้องเปลี่ยนแปลงวิธีและเทคนิคในการตรวจสอบ	129
- ร่องรอยสำหรับการตรวจสอบในระบบคอมพิวเตอร์	130
- การกำหนดขอบเขตและวางแผนตรวจสอบและกระบวนการวางแผนโดยแผนภูมิ	131
❑ ความคิดบางประการของการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์	136
- คอมพิวเตอร์กับผลของการประเมินการควบคุมภายใน	136
- ความรับผิดชอบของผู้บริหารต่อการควบคุมและการตรวจสอบ	136
- บทบาทของคณะกรรมการบริหาร	136
- บทบาทของฝ่ายจัดการหรือผู้ดำเนินงาน	136
- หน้าที่ของ Board of Directors หรือ Audit Committee	136
- บทบาทของผู้ตรวจสอบบัญชีภายใน	137
- บทบาทของผู้สอบบัญชีภายนอก	137
- ความรับผิดชอบของการตรวจสอบทางด้าน Computer หรือ IS	137
- วิธีการตรวจสอบระหว่างระบบงานด้านคอมพิวเตอร์	138

8. ขั้นตอนและกระบวนการตรวจสอบโดยย่อ	139
□ ขั้นตอนการตรวจสอบ	141
– ขั้นตอนที่ 1 การวิเคราะห์ความเสี่ยงพอของการควบคุมภายใน	141
– ขั้นตอนที่ 2 ทดสอบการปฏิบัติงานตามระเบียบที่ได้กำหนดไว้ (Compliance Tests)	141
– ขั้นตอนที่ 3 ทดสอบข้อมูลทางการเงิน (Substantive tests)	141
□ การตรวจสอบ	141
– การตรวจสอบแบบ Around/through the computer	141
– มาตรฐานการตรวจสอบ	142
□ การจัดประเภทการตรวจสอบด้านคอมพิวเตอร์	144
– การตรวจสอบการดำเนินงานของหน่วยงานคอมพิวเตอร์	144
– การตรวจสอบระบบงานที่ใช้คอมพิวเตอร์ประมวลผล	145
□ กระบวนการตรวจสอบ	147
□ หลักการสอบทานการควบคุมภายในที่สำคัญ	150
– การควบคุมภายในทั่วไป	150
– การควบคุมภายในเฉพาะงาน	154
– โครงสร้างการควบคุมภายใน	156
□ การจัดทำรายงานการตรวจสอบ	170
– ความถูกต้อง	170
– ความชัดเจน	170
– ความกระชับรัด	171
– ข้อเสนอแนะ	171
– ความทันกาล	171
9. ความจำเป็นต้องมีหน่วยงานตรวจสอบด้านคอมพิวเตอร์กับความเสี่ยง	173
□ สภาพแวดล้อมที่เปลี่ยนไปเมื่อองค์กรนำคอมพิวเตอร์มาใช้ในการประมวลข้อมูล	175
□ ความเสี่ยงของระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์	176
– การจัดการกับความเสี่ยง	177
– การประกันภัยทางด้านคอมพิวเตอร์	177
– การพิจารณาวิธีการควบคุมความเสี่ยงและความเสียหาย	178
– สิ่งที่ต้องพิจารณาเกี่ยวกับการควบคุม	178
– การวางแผนการตรวจสอบ	180
– การวางแผนสอบบัญชีกับการวิเคราะห์ความเสี่ยง เพื่อให้เข้าถึงจุดควบคุมต่าง ๆ	182

- การประเมินประสิทธิภาพของการควบคุม	192
- การควบคุมภายในระบบงานที่ใช้คอมพิวเตอร์	192
- สรุป	194
❑ การควบคุมงานตรวจสอบองค์กรที่ใช้คอมพิวเตอร์	195
- การขยายขอบเขตความรับผิดชอบการควบคุมภายในใหม่ของผู้สอบบัญชี	195
- ความเข้าใจอย่างเพียงพอต่อความรับผิดชอบของผู้สอบบัญชี	195
- ความรู้และความชำนาญ	195
- ความรับผิดชอบและการควบคุมภายในของผู้สอบบัญชี	196
- โครงสร้างของการตรวจสอบกับการควบคุม	196
- การวางแผนงานสอบบัญชี	196
10. การวางแผนกับวิธีการตรวจสอบ	199
❑ การวางแผน การจัดคณะผู้ตรวจสอบ และการกำกับการตรวจสอบด้านคอมพิวเตอร์	201
- การวางแผนการตรวจสอบ	201
- การจัดคณะผู้ตรวจสอบ	202
- การกำกับการตรวจสอบ	202
❑ วิธีการตรวจสอบ	202
- การตรวจสอบโดยไม่ใช้คอมพิวเตอร์	202
- การตรวจสอบโดยใช้คอมพิวเตอร์	203
- สรุป	204
11. การตรวจสอบของผู้ตรวจสอบภายในและผู้สอบบัญชี	207
❑ การคัดเลือกคณะผู้ตรวจสอบ	209
❑ หน้าที่และความรับผิดชอบของผู้ตรวจสอบภายใน	209
❑ ความรู้ความสามารถของผู้ตรวจสอบภายในด้านคอมพิวเตอร์	210
❑ ความเป็นอิสระของผู้ตรวจสอบ	210
❑ คู่มือการตรวจสอบภายใน	211
❑ การจัดทำเอกสารและรายงานการตรวจสอบ	211
❑ การติดตามผลการตรวจสอบ	212
❑ ความรับผิดชอบของผู้สอบบัญชี	213
❑ การตรวจสอบกิจการที่รับจ้างประมวลผล	214

12. เทคนิคการตรวจสอบคอมพิวเตอร์ในระบบที่ทันสมัย	215
☐ Integrated test facility	217
☐ Simulation	217
☐ Audit logging	217
☐ Parallel operations	217
☐ Base case system operation	218
☐ Embedded audit data collecting	218
☐ Transaction tagging	218
☐ Extended records	218
☐ การเข้าร่วมพัฒนาและทดสอบงานที่นำเข้าคอมพิวเตอร์	218
13. ความรู้ด้านคอมพิวเตอร์กับผู้ตรวจสอบ	219
☐ การตรวจสอบโดยผู้ตรวจสอบภายใน	221
☐ การจัดองค์การด้านคอมพิวเตอร์	221
☐ มาตรฐานของระบบงานและการจัดทำเอกสารสนับสนุน	1222
☐ การปฏิบัติงานคอมพิวเตอร์	222
☐ ความถูกต้องและสมบูรณ์ของข้อมูล	223
☐ เทคนิคที่เกี่ยวกับคอมพิวเตอร์	224
☐ การรักษาความปลอดภัยเครื่องและอุปกรณ์คอมพิวเตอร์	224
☐ การใช้บริการด้านคอมพิวเตอร์จากบุคคลภายนอก	225
14. ผู้บริหารกับคอมพิวเตอร์	227
☐ ปัญหาของสถาบันการเงินและองค์กรต่าง ๆ ที่ใช้คอมพิวเตอร์	229
– องค์กรไม่ให้ความสนใจเท่าที่ควร	229
– วางโครงการไม่ดีและขาดความรัดกุมและการมองการณ์ไกลตั้งแต่เริ่มแรก	229
– พนักงานมีคุณสมบัติไม่เพียงพอ	229
– ขาดบุคลากรในระดับผู้อำนวยการให้เป็นไปตามแผนงาน	229
– ขาดบุคลากรผู้มีความสามารถในการตรวจสอบงานด้านคอมพิวเตอร์	229
– เกิดความไม่เข้าใจในความต้องการใช้ข้อมูลของฝ่ายบริหาร	229
– ขาดการวางแผนงานที่เหมาะสม	230
– ขาดผู้รับผิดชอบต่อโครงการ	230
– ไม่ยอมยกเลิกโครงการ	230
– การควบคุมโครงการไม่ดีพอ	230

- องค์กรขาดแผนงานด้านการฝึกอบรมพนักงาน	230
- เลือก Hardware และรูปแบบ software ที่นำมาใช้งานไม่เหมาะสม	230
❑ บทบาทของฝ่ายบริหารที่มีต่อคอมพิวเตอร์	231
- บทบาทของฝ่ายบริหารที่มีต่อคอมพิวเตอร์	231
- สาเหตุที่ผู้บริหารไม่ให้ความสำคัญต่อผู้ตรวจสอบด้านคอมพิวเตอร์	231
15. อุปสรรคเกี่ยวกับการใช้คอมพิวเตอร์	233
- การดำเนินงานของสถาบันการเงินมีผลกระทบต่อการนำเอาคอมพิวเตอร์มาใช้	235
- ความเชื่อที่ไม่ถูกต้องเกี่ยวกับคอมพิวเตอร์	236
- ข้อกังวลของสถาบันการเงินเกี่ยวกับการใช้คอมพิวเตอร์	236
- ปัญหาที่บรรดาศูนย์คอมพิวเตอร์ต่าง ๆ ส่วนใหญ่ประสบ	237
16. อาชญากรรมทางเทคโนโลยี	239
❑ พัฒนาการทางคอมพิวเตอร์ 3 ประการที่ทำให้อาชญากรรมทางเทคโนโลยีเพิ่มขึ้น	241
❑ คนฉลาดกว่าคอมพิวเตอร์	241
❑ การควบคุมภายในขาดประสิทธิภาพ	241
❑ การทุจริตทางคอมพิวเตอร์	241
- สาเหตุการทุจริต	242
- จุดที่สามารถทุจริตได้	243
- ประเภทของการทุจริตด้านคอมพิวเตอร์ในวงการสถาบันการเงิน	243
- การป้องกันภัยจากการทุจริต	243
- แนวทางในการตรวจสอบการทุจริตด้านคอมพิวเตอร์	243
- สิ่งที่จะตามมาในอนาคต	244
- สิ่งที่ต้องดำเนินการ	244
17. ประเภทการตรวจสอบ	245
❑ การตรวจสอบทางการเงิน	247
❑ การตรวจสอบการปฏิบัติตามการควบคุมภายใน	247
❑ การตรวจสอบการปฏิบัติงาน	247
❑ การตรวจสอบการจัดการ	247
❑ การตรวจสอบการทุจริต	248
❑ การตรวจสอบด้านคอมพิวเตอร์	248

18. หลักฐานการตรวจสอบด้านคอมพิวเตอร์	249
❑ รูปแบบของหลักฐานที่ผู้ตรวจสอบมักใช้ในการตรวจสอบระบบที่ทำด้วยมือ	251
❑ การเปลี่ยนแปลงลักษณะของหลักฐานเมื่อมีการนำเครื่องคอมพิวเตอร์มาใช้	251
– รายการที่ทำโดยคน	251
– ข้อมูลนำเข้าที่บันทึกในกระดาษ	251
– การอนุมัติรายการ	252
– การจัดส่งข้อมูล	252
– การประมวลผลในรูปแบบที่มองเห็นได้	252
– ข้อมูลหลัก	252
– รายงานข้อมูลผลลัพธ์	252
– การจัดแฟ้มเอกสาร	252
– ร่องรอยการตรวจสอบ	253
– คู่มือการปฏิบัติงาน	253
– การติดตามรายการ	253
– การแบ่งแยกหน้าที่	253
– การประมวลผลรายการจำนวนมาก	253
19. บทบาทและขั้นตอนบางประการที่ผู้ตรวจสอบภายในด้านคอมพิวเตอร์	
ควรเข้าไปมีส่วนเกี่ยวข้อง	255
❑ ขั้นตอนการทำสัญญาซื้อหรือเช่า	258
❑ ขั้นตอนการตรวจรับและการปฏิบัติตามสัญญา	259
❑ การร่วมพัฒนาและทดสอบงานที่นำเข้าประมวลผลด้วยคอมพิวเตอร์	
และเอกสารประกอบระบบงาน	261
❑ ขั้นตอนการนำระบบงานใหม่เข้ามาใช้งาน	262
❑ ขั้นตอนการรักษาความปลอดภัยและลดความเสี่ยงภัยด้านคอมพิวเตอร์	
ด้วยการประกันภัย	263
❑ การทำสัญญาในการใช้บริการหรือให้บริการบุคคลภายนอก	263
20. การทดสอบข้อมูลโดยวิธี Test Data	265
❑ เหตุผลและความจำเป็น	267
❑ การนำ Test Data มาใช้ในการตรวจสอบ	268
– ขั้นตอนการตรวจสอบงานด้านคอมพิวเตอร์	268
– การใช้ Test Data ตรวจสอบความถูกต้องของโปรแกรม	269
– Test Data คืออะไร	270

❑	ขั้นตอนการจัดทำ Test Data และตัวอย่าง	271
–	ขั้นตอนการจัดทำ Test Data	271
–	ตัวอย่างขั้นตอนการจัดทำ Test Data ในระบบ On-line	271
❑	ข้อควรพิจารณาในการจัดทำ Test Data	274
❑	ข้อดี ข้อเสีย ของการ Test Data มาใช้งาน	275
❑	ตัวอย่างการจัดทำ Test Data อย่างง่าย ๆ	276
–	Test Data 1 Cycle	276
–	การทำ Test Data 2 Cycles	281
21.	การป้องกันดีกว่าการแก้ไข	285
–	สัญญาณการทุจริตหรือจุดอ่อนบางประการในองค์กรที่ใช้คอมพิวเตอร์	287
22.	ความสูญเสียของสถาบันการเงินที่มีเหตุมาจากโปรแกรมคอมพิวเตอร์ผิดพลาด	289
❑	เหตุมาจากโปรแกรมคอมพิวเตอร์ผิดพลาด ทำให้ธนาคารตกเป็นลูกหนี้	
32	พันล้านเหรียญสหรัฐอเมริกา	291
–	ประวัติการทำงานของธนาคารโดยย่อ	291
–	ตัวอย่างการดำเนินธุรกิจการซื้อขายหลักทรัพย์รัฐบาล	291
–	สาเหตุของข้อผิดพลาด	292
–	ภายหลังเหตุการณ์	293
–	ข้อคิดเห็น	293
23.	ภาคผนวก	299
❑	ประกาศอธิบดีกรมสรรพากรเกี่ยวกับภาษีมูลค่าเพิ่ม (ที่เกี่ยวข้องกับงานด้านคอมพิวเตอร์)	301
❑	EDP Supervision of Financial Institutions	305
24.	บรรณานุกรม	368

1

ลำดับการพัฒนางาน
ด้านคอมพิวเตอร์
ในวงการธนาคารของไทย

The Historical Development of Electronic Banking In Thailand

Year	Services	Leader
1970-1974	- In-house Deposit Application	Bangkok Bank Limited
1975-1979	- On-line Deposit Application in Bangkok	Bangkok Bank Limited
1980-1984	- On-line Deposit Application in Provinces	Bangkok Bank Limited
	- ATM	Siam Commercial Bank Limited (1983)
	- SWIFT	Bangkok Bank Limited (1984)
	- Tele-Banking	Siam Commercial Bank Limited (1984)
1985	- POS Pool	Bangkok Bank Limited
	- ATM Pool	4 Pools
	- BCR (Badge card reader) / Pin Pad	Bangkok Bank Limited
	- Office Banking / Video Banking / Info Banking / Cash Authorization	Bangkok Bank Limited
	- Credit Card Authorization	Thai Farmers Bank Limited
1987	- Mobile ATM	Thai Farmers Bank Limited
	- Computer branch or Self-service electronic banking corner	Siam Commercial Bank Limited
1988	- Electronic mail	Bank of Ayudthaya Limited
	- Disaster recovery services	Bank of Ayudthaya Limited
	- Second site back up services	
	- Data Depository Services	
	- Security Exchange Information Services	Bangkok Bank Limited
	- Computer back up center	Bangkok Bank Limited and Thai Farmers Bank Limited
1989	- Clearing cheques	Some local commercial banks
1991	- Credit card information service bureau	Medium-sized local commercial bank
1993	- National ATM Poll	All local commercial banks
	- Worldwide ATM Service	Bangkok Bank Limited
	- Electronic cheque Clearing System (ECS)	
	- Off-line Retail Funds Transfer System	During implemented by Bank of Thailand
	- Inter-bank Funds Transfer System (Large value)	

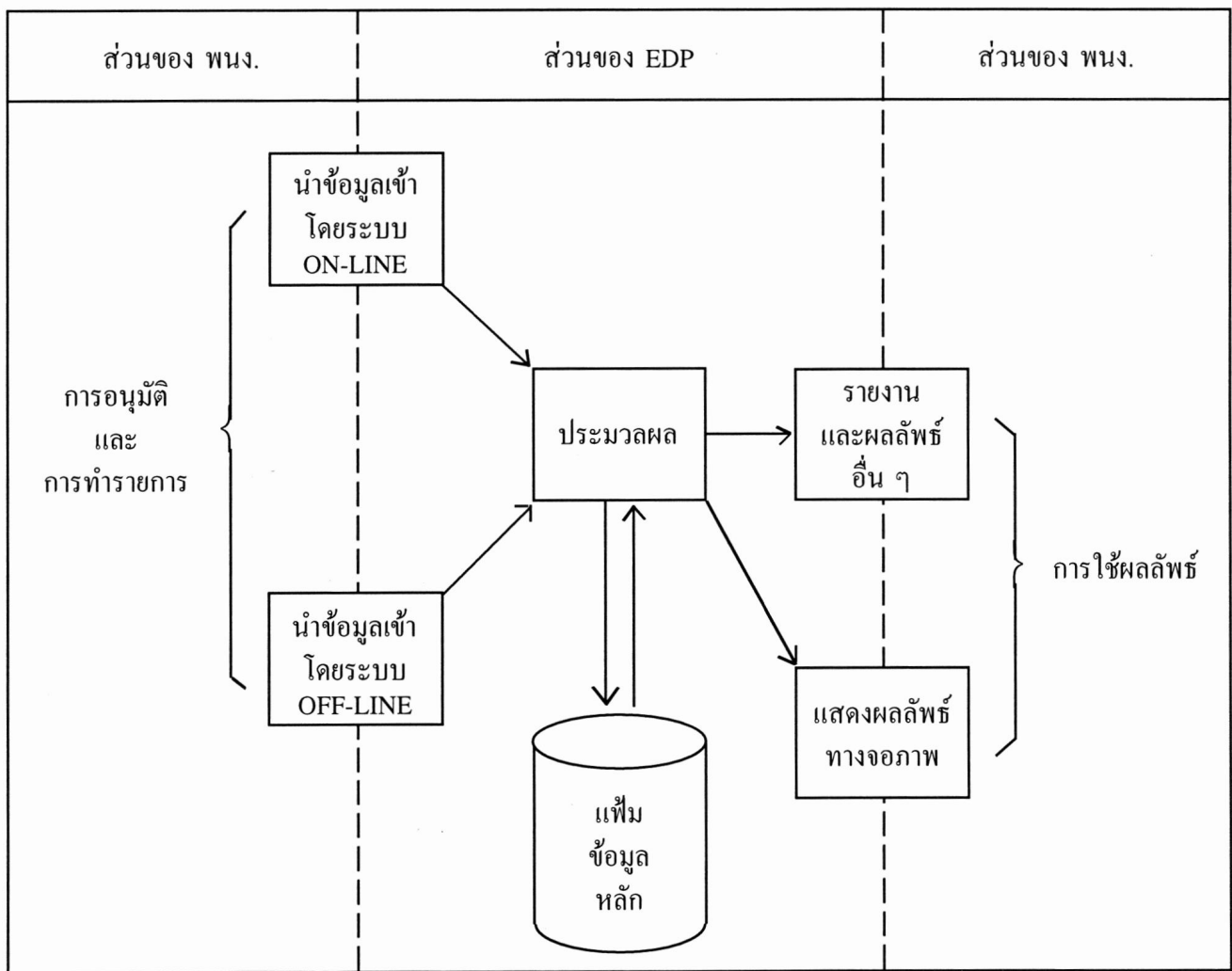
2

ส่วนงานของคอมพิวเตอร์
ในระบบงานขององค์กร

ส่วนงานของ EDP ในระบบงานโดยทั่วไป ขององค์กรที่ใช้คอมพิวเตอร์

ภาพนี้จะทำให้ทราบถึงสิ่งที่จะเกี่ยวข้องกับการตรวจสอบงานทั้งทางด้าน Financial และ Computer ซึ่งจะขึ้นอยู่กับเป้าหมายและขอบเขตการตรวจสอบเป็นเรื่อง ๆ ไป

ภาพของส่วนงานของ EDP ที่เกี่ยวข้องกับส่วนของพนักงานแบ่งได้เป็น 3 ส่วนดังนี้



ส่วนของ EDP ในระบบงาน

- ก. ส่วนของพนักงาน
- ข. ส่วนของพนักงานร่วมกับส่วนของ EDP
- ค. ส่วนของ EDP ล้วน ๆ

ภาพข้างต้นจะอธิบายความสัมพันธ์ของงาน EDP กับงานทางด้าน Manual ได้ในตัวเอง

3

เทคโนโลยีทางคอมพิวเตอร์

เทคโนโลยีทางคอมพิวเตอร์ (Computer Technology)

การใช้ Computer Technology ในรูปแบบและลักษณะต่าง ๆ กันนั้นมีผลกระทบต่อการตรวจสอบ ตัว Technology เองสามารถกำหนดได้ชัดเจนว่าวิธีการใช้งาน Computer Technology แบ่งเป็นประเภทใหญ่ ๆ ได้ดังนี้

1. **Terminal** เครื่องมืออุปกรณ์ที่สามารถรับ - ส่งข้อมูลกับคอมพิวเตอร์ได้โดยตรง เช่น แป้นคีย์ข้อมูลพร้อมจอภาพ (typewrite keyboards with CRTs), อุปกรณ์รวบรวมข้อมูล (data collection equipment), ATMs (Automatic teller machines), เครื่องจ่ายเงินอัตโนมัติ (cash dispensing terminals) และอุปกรณ์ที่ใช้ในการติดตามและตรวจสอบ (monitoring devices)
2. **Offline, Input/Output devices** คืออุปกรณ์ที่ใช้แปลงข้อมูลที่อยู่ในรูปเอกสารให้เป็นข้อมูลที่อยู่ในสื่อที่คอมพิวเตอร์อ่านได้ เช่น keypunch, key-to-disk, printer, optical scanners และอุปกรณ์ computer
3. **Communications** การส่งผ่านข้อมูลกระทำผ่านสายสื่อสาร
4. **Storage media** อุปกรณ์ที่เก็บข้อมูลที่ถูกละเปลี่ยนเป็นรหัสอยู่ในรูปของข้อมูลทางอิเล็กทรอนิกส์ เช่น tapes, drum, disks หรือ cards
5. **Programming** คือการปฏิบัติตามกฎการประมวลผลโดยใช้คอมพิวเตอร์
6. **Database** การใช้ database management system ช่วยให้มีความสะดวกและคล่องตัวในการปรับปรุงข้อมูลได้อย่างมีประสิทธิภาพ เพราะนำข้อมูลมารวมไว้ในแหล่งเดียว ซึ่งสะดวกต่อผู้ใช้ที่ต้องใช้ข้อมูลร่วมกันอีกด้วย
7. **System Documentation** เป็นรายละเอียดคำอธิบายขั้นตอนของระบบงานตั้งแต่การจัดทำ การบำรุงรักษา และการใช้งาน

จากตารางที่ 1 จะแสดงความสัมพันธ์ระหว่างรูปแบบของหลักฐานกับเทคโนโลยี โดยจะชี้ให้เห็นว่าลักษณะของเทคโนโลยีทางคอมพิวเตอร์ สามารถเปลี่ยนแปลงรูปแบบของหลักฐานได้ดังปรากฏอยู่ในตาราง

ตารางที่ 1 Audit Impact Matrix

หลักฐานการตรวจสอบ	เทคโนโลยีทางคอมพิวเตอร์						
	Input/Output devices		Commu- nication	Storage Media	Program- ming	Data base	Systems Documen- tation
	off- line	on- line					
การกำหนดรายการ ข้อมูลนำเข้า	/	/			/		
การอนุมัติ		/			/	/	
การนำส่งข้อมูล			/				
การประมวลผล		(/)	(/)		(/)	/	(/)
ข้อมูลหลัก				/			
ข้อมูลผลลัพธ์	/	/		/			
การจัดแฟ้มเอกสาร				/			
ร่องรอยการตรวจสอบ			/	/		/	
คู่มือปฏิบัติงาน							
การเช็คสอบข้อมูล					/		
การแบ่งแยกหน้าที่		/	/		/	/	
การประมวลผล							
รายการจำนวนมาก		/	/	/	/	/	

8. ผลกระทบจากการที่รูปแบบของหลักฐานที่ใช้ในการตรวจสอบได้เปลี่ยนแปลงไป

(Impact of Changing Evidence on the Audit)

เมื่อรูปแบบของหลักฐานที่ใช้ในการตรวจสอบได้เปลี่ยนแปลงไป จะมีผลให้วิธีการตรวจสอบที่ใช้ต้องเปลี่ยนแปลงไปด้วย ซึ่งจะได้ยกตัวอย่างในสองกรณี คือ

8.1 กรณีตัวอย่าง ก.

องค์กร ก. ได้ใช้ระบบงานคอมพิวเตอร์ในการจ่ายเงินเดือนพนักงานแต่ละคนจะกรอกรายละเอียด ชั่วโมงในใบลงเวลา แล้วให้ผู้ควบคุม (Supervisor) ลงลายมือชื่ออนุมัติหลังจากนั้นจะรวบรวมข้อมูลไปป้อน (Key) ข้อมูลลง (disk) โดยใช้เครื่อง key-to-disk machine ซึ่งจะมีสำเนาข้อมูลส่งกลับมาให้ผู้ควบคุมตรวจสอบความถูกต้องอีกครั้งหนึ่ง และเมื่อเริ่มต้นงวดรอบระยะเวลาการจ่ายเงินเดือนแต่ละครั้ง จะมีการปรับปรุงข้อมูลที่มีการเปลี่ยนแปลง เช่นอัตราค่าจ้างและรายการหักค่าลดหย่อนต่าง ๆ และมีการพิมพ์รายงานแสดงรายละเอียดการจ่ายค่าจ้างของพนักงานแต่ละคนส่งให้แผนกงานต่าง ๆ เพื่อใช้เป็นข้อมูลในการจัดเตรียมการจ่ายค่าจ้าง และในขั้นสุดท้ายก็จะมีการจัดพิมพ์เช็คและส่งให้ผู้ควบคุมแต่ละคนเพื่อจ่ายให้แก่พนักงาน และจะมีการกระทบยอดเช็คสลับหลังโดยฝ่ายบุคคลที่อยู่แยกต่างหากจากแผนกที่ทำหน้าที่เกี่ยวกับการจ่ายเงินเดือน

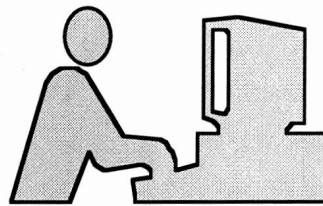
จากระบบงานในลักษณะที่กล่าวข้างต้นนั้น รูปแบบของหลักฐานจะไม่ถูกระทบกระเทือนหรือเปลี่ยนแปลงไปมากนัก ยังคงสามารถใช้วิธีการตรวจสอบเช่นที่ทำในระบบเดิมได้ แต่ถ้าผู้ตรวจสอบจะต้องการปรับปรุงประสิทธิภาพและความประหยัดในการตรวจสอบโดยนำเอาเทคโนโลยีทางด้านคอมพิวเตอร์เข้ามาช่วยในการตรวจสอบได้ เช่นการใช้ audit software เป็นต้น

8.2 กรณีตัวอย่าง ข.

องค์กร ข. ได้ใช้ระบบงานคอมพิวเตอร์ในการจ่ายเงินเดือน ซึ่งระบบนี้จะรวบรวมและบันทึกข้อมูลผ่านเครื่องเทอร์มินอล โดยพนักงานแต่ละคนจะใช้บัตรที่มีแถบแม่เหล็กบันทึกรายการรูดผ่านเครื่องเทอร์มินอลเพื่อบันทึกเวลาที่เข้าทำงานประจำวันและเวลาเลิกงาน เครื่องก็จะบันทึกข้อมูลชั่วโมงการทำงานของพนักงานคนนั้น ๆ ไว้ เมื่อมีการเปลี่ยนแปลงข้อมูลหลักเช่นอัตราค่าจ้าง ฝ่ายบุคคลก็จะป้อนรายการเปลี่ยนแปลง พร้อมวันที่มีผลบังคับใช้ผ่านทางเครื่องเทอร์มินอลเพื่อปรับปรุงข้อมูลใน database โดยตรง ข้อมูลเกี่ยวกับค่าจ้างที่ต้องจ่ายที่ได้จากการประมวลผล จะถูกส่งไปยังธนาคารเพื่อโอนเงินเข้าบัญชีให้พนักงานในลักษณะที่เป็นการโอนเงินทางอิเล็กทรอนิกส์ และจะส่ง statement แสดงรายละเอียดการโอนเงินเข้าบัญชีให้แก่พนักงานถึงบ้าน

ในระบบดังกล่าว จะเห็นว่ารูปแบบของหลักฐานได้เปลี่ยนแปลงไปอย่างมาก จึงจำเป็นต้องอาศัยวิธีการตรวจสอบแบบใหม่ ซึ่งต่างจากการนำคอมพิวเตอร์เข้ามาใช้ในกรณี ก. ซึ่งไม่ได้ทำให้รูปแบบของหลักฐานเปลี่ยนแปลงไป จึงสามารถใช้วิธีการตรวจสอบแบบเดิมได้ ดังนั้น อาจกล่าวได้ว่า ตัวคอมพิวเตอร์เองนั้นไม่ได้มีผลต่อผู้ตรวจสอบโดยตรงแต่ผลกระทบจากระบบงานคอมพิวเตอร์ที่มีต่อรูปแบบของหลักฐานที่ใช้ในการตรวจสอบต่างหากที่มีความสำคัญและทำให้ผู้ตรวจสอบต้องกำหนดวิธีการตรวจสอบให้เหมาะสมและสอดคล้องกับรูปแบบของหลักฐานที่ได้เปลี่ยนแปลงไป

อย่างไรก็ดี ก่อนที่จะมีการตรวจสอบระบบคอมพิวเตอร์นั้น ผู้ตรวจสอบควรทราบถึงลักษณะของเทคโนโลยีที่ธนาคารใช้เสียก่อน โดยอาจจะใช้ Audit Impact Matrix (ตารางที่ 1) เพื่อระบุถึงผลกระทบที่มีต่อรูปแบบของหลักฐาน หากเทคโนโลยีนั้นมีผลให้รูปแบบของหลักฐานเปลี่ยนแปลงไป ผู้ตรวจสอบก็ต้องพิจารณาว่าจะมีผลให้ต้องนำวิธีการตรวจสอบแบบใหม่มาใช้หรือไม่ ในกรณีที่รูปแบบของหลักฐานได้เปลี่ยนแปลงไปโดยสิ้นเชิงผู้ตรวจสอบอาจจำเป็นต้องมีทักษะหรือความเชี่ยวชาญในการตรวจสอบ EDP โดยเฉพาะจึงจะสามารถตรวจสอบได้อย่างเหมาะสม จากตารางที่ 2 จะเป็นแนวทางที่ชี้ให้เห็นถึงวิธีการตรวจสอบที่ควรนำมาใช้เมื่อรูปแบบของหลักฐานได้เปลี่ยนแปลงไปในลักษณะต่าง ๆ โดยสังเขป



ตารางที่ 2
การเปรียบเทียบระหว่างรูปแบบของหลักฐานแบบเดิมและแบบใหม่
(Comarison of Old New Forms of Evidence)

รูปแบบของหลักฐาน แบบเดิม	รูปแบบของหลักฐาน แบบใหม่	วิธีการตรวจสอบเพื่อให้ได้มาซึ่งหลักฐาน ในรูปแบบใหม่
เอกสารต้นกำเนิดจัดทำ ขึ้นโดยพนักงาน	เอกสารต้นกำเนิดจัดทำ โดยคอมพิวเตอร์อัตโนมัติ	ผู้ตรวจสอบต้องตรวจสอบเอกสารระบบงานและโปรแกรม การทำงาน เพื่อสอบถามว่าคอมพิวเตอร์มีขั้นตอนใน การประมวลผลรายการ 1) ใช้วิธีการ test data เพื่อดูว่ารายการต่างๆ ที่เกิดขึ้น นั้นถูกต้องและได้รับการจัดทำขึ้นในเวลาที่เหมาะสม 2) ใช้ audit software ดึงรายละเอียดข้อมูลที่บรรจุ อยู่ในโปรแกรมที่ให้เครื่องคอมพิวเตอร์ใช้ในการให้ กำหนดรายการเพื่อยืนยันว่ารายการดังกล่าวได้จัดทำขึ้น อย่างเหมาะสม
ข้อมูลนำเข้าซึ่งอยู่ในรูป ของเอกสาร	ข้อมูลนำเข้าที่ป้อนโดย ตรงที่เครื่องเทอร์มินอล	ผู้ตรวจสอบสามารถใช้ audit software สุ่มตัวอย่าง รายการขึ้นมาจำนวนหนึ่งและตรวจสอบกับผู้รับผิดชอบ ในการป้อนข้อมูลว่ารายการดังกล่าวได้เกิดขึ้นโดยผู้รับ ผิดชอบในการป้อนข้อมูลได้ป้อนเข้าไปในระบบจริง
การอนุมัติด้วยมือ	การอนุมัติด้วยระบบ อิเล็กทรอนิกส์อัตโนมัติ	ผู้ตรวจสอบอาจใช้ audit software ในการจัดทำ หนังสือที่ขอให้ผู้ที่มีหน้าที่รับผิดชอบในการอนุมัติยืนยัน ว่ารายการต่างๆ เหล่านั้น ได้ผ่านการอนุมัติอย่างแท้จริง
การนำส่งเอกสาร	การนำส่งข้อมูลในรูปของ ข้อมูลทางอิเล็กทรอนิกส์ (Telecommunications)	ผู้ตรวจสอบดึงข้อมูลรายการที่จัดส่งจากสถานที่หนึ่ง ออกมาเปรียบกับข้อมูลรายการที่ดึงมาจากสถานที่ ปลายทางที่เป็นผู้รับเพื่อตรวจสอบความครบถ้วนสมบูรณ์และ ความถูกต้อง

รูปแบบของหลักฐาน แบบเดิม	รูปแบบของหลักฐาน แบบใหม่	วิธีการตรวจสอบเพื่อให้ได้มาซึ่งหลักฐาน ในรูปแบบใหม่
การประมวลผลข้อมูลที่อยู่ในลักษณะของเอกสาร ซึ่งเป็นการประมวลผลที่ทำด้วยมือ	การประมวลผลที่ทำโดยคอมพิวเตอร์	มีวิธีการหลายวิธีที่สามารถในการตรวจสอบการประมวลผลด้วยคอมพิวเตอร์ เช่น 1) การ test data ซึ่งสมมติข้อมูลขึ้นมาแล้วนำไปประมวลผลใช้โปรแกรมการประมวลผลของธนาคารเมื่อได้ผลลัพธ์ก็นำไปเปรียบเทียบกับผลลัพธ์ที่คำนวณด้วยมือไว้ล่วงหน้าแล้ว 2) ใช้วิธีเขียนโปรแกรมขึ้นมา (โดยเขียนจากการพิจารณาว่าถ้าจะได้ output ในลักษณะดังกล่าวจะต้องผ่านขั้นตอนการประมวลผลเช่นไรซึ่งอย่างน้อยระบบงานคอมพิวเตอร์ของธนาคารก็ควรมีขั้นตอนเช่นที่กล่าวแต่โปรแกรมที่ผู้ตรวจสอบเขียนขึ้นจะอยู่ในลักษณะที่ง่ายกว่าไม่สลับซับซ้อนและเช็คการทำงานเป็นจุดเท่านั้น) แล้วใช้ข้อมูลจริงของธนาคารมาประมวลผลโดยผ่านโปรแกรมที่ผู้ตรวจสอบเขียนขึ้นหลังจากนั้นก็เปรียบเทียบผลลัพธ์ว่าถูกต้องตรงกันหรือไม่ 3) ใช้วิธีวาด flowchart ของโปรแกรมออกมาโดยใช้ automatic flow-charting routine และใช้ "paper – debug" ในกระบวนการประมวลผลดังกล่าว เพื่อพิจารณาตัดสินใจว่าการประมวลผลดังกล่าวมีความถูกต้อง
ข้อมูลหลักซึ่งอยู่ในรูปของเอกสาร	ข้อมูลหลักอยู่ในแฟ้มข้อมูลของระบบงานคอมพิวเตอร์	ผู้ตรวจสอบสามารถใช้ audit software สุ่มถึงรายละเอียดข้อมูลหลักเช่น ข้อมูลราคาสินค้าและเปรียบเทียบดูว่ามีเอกสารแสดงการอนุมัติให้มีการป้อนข้อมูลหลักเข้าไปเก็บไว้ในแฟ้มข้อมูลของระบบงานคอมพิวเตอร์หรือไม่
การจัดเก็บข้อมูลในรูปของแฟ้มเอกสาร	การจัดเก็บข้อมูลในระบบแฟ้มข้อมูลทางคอมพิวเตอร์	ผู้ตรวจสอบอาจใช้ audit software เพื่อดึงข้อมูลที่ต้องการจากแฟ้มข้อมูลทางคอมพิวเตอร์แล้วพิมพ์ลงในกระดาษต่อเนื่องเพื่อใช้ตรวจสอบได้

รูปแบบของหลักฐาน แบบเดิม	รูปแบบของหลักฐาน แบบใหม่	วิธีการตรวจสอบเพื่อให้ได้มาซึ่งหลักฐาน ในรูปแบบใหม่
คู่มือปฏิบัติงาน	data dictionary	ผู้ตรวจสอบสามารถสังพิมพ์รายงานข้อมูลจาก data dictionary เพื่อตรวจสอบ data attributes
การตรวจสอบข้อมูลเบื้องต้นในลักษณะที่ทำด้วยมือ	การตรวจสอบข้อมูลเบื้องต้นโดยใช้วิธี editing และอื่น ๆ	ผู้ตรวจสอบอาจสมมติข้อมูลที่ผิดพลาดแล้วส่งเข้าประมวลผลเพื่อเช็คสว่าโปรแกรมที่กำหนดเพื่อใช้ในการตรวจสอบความถูกต้องเบื้องต้นของข้อมูลสามารถป้องกันข้อผิดพลาดที่เกิดขึ้นกับข้อมูลได้
การแบ่งแยกหน้าที่	การแบ่งแยกขั้นตอนการประมวลผลโดยอัตโนมัติ	ผู้ตรวจสอบสามารถใช้ Transaction conflict matrix เพื่อตรวจสอบว่ามีการแบ่งแยกขั้นตอนการประมวลผลรายการโดยอัตโนมัติขึ้นเพียงพอหรือไม่



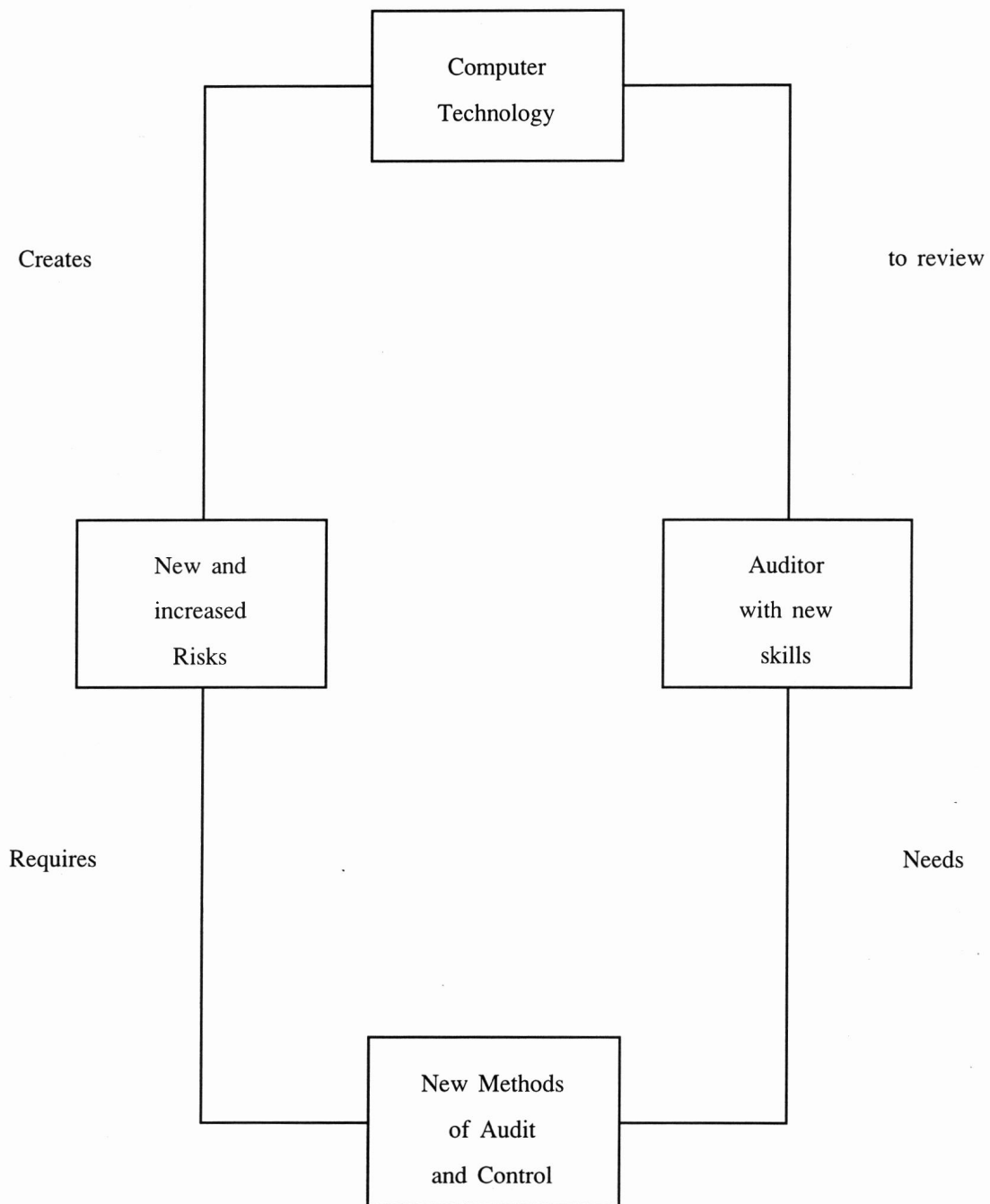
ความเสี่ยงทั่วไปของการประมวลผลด้วยคอมพิวเตอร์ (EDP RISKS)

ความเสียหายที่อาจเกิดขึ้น (EXPOSURES)	สาเหตุ																			
	การบริหารงาน						การปฏิบัติการภายในศูนย์ฯ										การพัฒนากระบวนการ			
	แผนงาน/โครงการ/กิจกรรม	บุคลากร	งบประมาณ	เทคโนโลยี	ข้อมูล	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน	การดำเนินงาน				
ผลตอบแทนไม่คุ้มค่าหรือเสีย ค่าใช้จ่ายมากเกินไป	แผนงาน/โครงการ/กิจกรรม	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	บุคลากร	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	งบประมาณ	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	เทคโนโลยี	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	ข้อมูล	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
การตัดสินใจผิดพลาด	แผนงาน/โครงการ/กิจกรรม	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	บุคลากร	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	งบประมาณ	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	เทคโนโลยี	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	ข้อมูล	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
ทรัพยากรสูญหายหรือเสียหาย เสียประโยชน์ทางด้านการแข่งขัน	แผนงาน/โครงการ/กิจกรรม	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	บุคลากร	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	งบประมาณ	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	เทคโนโลยี	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	ข้อมูล	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
การถูกดำเนินคดีทางกฎหมาย ความล้มเหลวธุรกิจทั่วโลก	แผนงาน/โครงการ/กิจกรรม	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	บุคลากร	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	งบประมาณ	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	เทคโนโลยี	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	ข้อมูล	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
การประมวลผลหยุดชะงัก	แผนงาน/โครงการ/กิจกรรม	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	บุคลากร	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	งบประมาณ	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	เทคโนโลยี	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				
	ข้อมูล	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3				

หมายเหตุ 3 = ค่อนข้างมาก
2 = ปานกลาง
1 = ค่อนข้างน้อย

หมายเหตุ 3 = ค่อนข้างมาก
2 = ปานกลาง
1 = ค่อนข้างน้อย

9. สภาพแวดล้อมของธุรกิจที่ใช้คอมพิวเตอร์กับ Audit and control



Audit and Control in a computerized business environment



**คอมพิวเตอรืกับบทบาทของ
ธนาคารแห่งประเทศไทย**

คอมพิวเตอร์กับบทบาทของธนาคารแห่งประเทศไทย

1. คอมพิวเตอร์กับธนาคารพาณิชย์ในประเทศไทย

ผลของการนำคอมพิวเตอร์มาใช้กับงานต่าง ๆ ของธนาคารพาณิชย์ ก่อให้เกิดการเปลี่ยนแปลงทั้งวิธีการปฏิบัติงานการควบคุมภายใน และการบริหารงาน โดยมีเทคนิคและวิธีการต่าง ๆ ที่ถูกนำมาพัฒนาและปรับปรุงภายในธนาคารพาณิชย์อย่างมากมาย มีการขยายขอบเขตงานเพื่ออำนวยความสะดวกการให้บริการโดยเชื่อมต่อเป็นข่ายงานออนไลน์ระหว่างสำนักงานใหญ่และสาขาทั่วประเทศ เพื่อประมวลผลและแลกเปลี่ยนข้อมูลรายการทางบัญชีต่าง ๆ โดยเฉพาะการรับฝากและโอนเงินของบัญชีเงินฝากลูกค้าต่างสำนักงานหรือต่างสาขานอกจากที่กล่าวคอมพิวเตอร์ยังนำความเสี่ยง (Risk) ในรูปแบบใหม่ ๆ ที่จำเป็นต้องควบคุมและดูแลให้เหมาะสมและสอดคล้องกับวิธปฏิบัติและระบบคอมพิวเตอร์ที่นำมาใช้ เพื่อให้เกิดความปลอดภัยและไม่ทำให้เกิดความเสียหายต่อธนาคารและลูกค้าผู้ให้บริการ

ธนาคารพาณิชย์ในประเทศไทยได้นำระบบคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลและให้บริการต่อลูกค้าตั้งแต่ปี พ.ศ. 2513 และได้มีการขยายขอบเขตและปริมาณการใช้งานและการให้บริการกว้างขวางมากขึ้นเรื่อย ๆ จนกล่าวได้ว่า ในปัจจุบันธนาคารพาณิชย์และสถาบันการเงินทุกแห่งได้นำระบบคอมพิวเตอร์เข้ามาใช้อย่างแพร่หลายแล้ว

2. ผลกระทบของคอมพิวเตอร์หรือธนาคารอิเล็กทรอนิกส์ต่อการกำกับและตรวจสอบธนาคารพาณิชย์

ความเป็นมา

การกำกับธนาคารพาณิชย์นั้น มีแนวทางที่สำคัญแยกได้เป็น 2 ด้าน คือ

2.1 ด้านการวางกฎเกณฑ์

มีการกำหนดระเบียบ กฎเกณฑ์ และเงื่อนไข ข้อบังคับ ในรูปของกฎหมาย ประกาศ หนังสือเวียน และหนังสือขออนุญาตตามที่กฎหมายกำหนดและให้อำนาจไว้ เพื่อให้ธนาคารพาณิชย์สามารถดำเนินธุรกิจอย่างมีมาตรฐานสอดคล้องกับแนวทางและนโยบายของทางการและมีฐานะมั่นคงปลอดภัย และเป็นที่เชื่อถือของลูกค้าประชาชนที่เกี่ยวข้อง

2.2 ด้านการติดตามฐานะของธนาคาร

ใช้วิธีการประเมินฐานะประกอบกับการติดตามดูการปฏิบัติต่างๆ ให้เป็นไปตามกฎหมายและข้อกำหนดต่าง ๆ อันมีวัตถุประสงค์ให้ธนาคารพาณิชย์ดำเนินงานอยู่ในขอบเขตอันสมควรและเหมาะสม งานด้านนี้จะวิเคราะห์สรุปได้จากรายงานต่าง ๆ ที่ทางการกำหนดให้ธนาคารพาณิชย์จัดส่ง ประกอบกับการไปตรวจสอบ ณ สำนักงานของธนาคารพาณิชย์นั้น ๆ

หลักการใหญ่ๆ ที่ใช้ในการประเมินฐานะของธนาคาร คือการประเมินความเพียงพอของเงินกองทุน คุณภาพของสินทรัพย์ การจัดการ ความสามารถในการหารายได้ และการดำรงสภาพคล่อง (CAMEL : Capital, Assets, Management, Earnings และ Liquidity) ซึ่งมักเป็นการประเมินจากข้อมูลตัวเลขที่ปรากฏในงบการเงิน ซึ่งได้แก่ งบดุล และงบกำไรขาดทุน ประกอบกับข้อมูลในรายละเอียดตามรายการต่าง ๆ ที่ปรากฏอยู่ในงบการเงินดังกล่าว

ในปัจจุบันธุรกิจธนาคารได้วิวัฒนาการและเปลี่ยนแปลงวิธีปฏิบัติและการให้บริการไปจากเดิม โดยมี การทำธุรกรรมและนำเอาเทคโนโลยีใหม่ ๆ มาใช้มากขึ้น ก่อให้เกิดความเสี่ยง (Risk) ในรูปแบบที่แตกต่างไปจากเดิม และยากแก่การวัดหรือประเมินผล ได้แก่ รายการนอกงบดุล (Off Balance Sheet Business) เช่น การทำ Syndicated Loan, Letters of Credit, Foreign Exchange, Wire Transfer, Electronic Data Processing (EDP) หรือ Electronic Banking และ อื่น ๆ เป็นต้น ซึ่งผู้ที่ทำหน้าที่ในการกำกับและตรวจสอบธนาคารพาณิชย์ จำเป็นต้องศึกษาให้เข้าใจถึง ความเสี่ยง (Risk) ดังกล่าว และผลกระทบที่อาจมีต่อการประเมินฐานะของสถาบันการเงิน

3. ความเสี่ยง (Risk) ของธนาคารอิเล็กทรอนิกส์บางประการ

ความเสี่ยง (Risk) ในด้านของ Electronic Data Processing หรือ การนำเอา Electronic Banking เข้ามาใช้ในการดำเนินงานของธนาคารพาณิชย์ มีความเสี่ยงที่สำคัญบางประการดังนี้

3.1 ระบบไม่สามารถประมวลผลข้อมูลได้อย่างต่อเนื่องและเกิดการหยุดชะงัก

ในกรณีที่ระบบคอมพิวเตอร์เกิดความล้มเหลว จนธนาคารพาณิชย์ไม่สามารถดำเนินงานและให้ บริการแก่ลูกค้าได้ นับเป็นความเสี่ยงที่สำคัญอย่างยิ่ง การป้องกันความเสี่ยงในจุดนี้โดยการกำหนดสำรองภัยและแผน ฉุกเฉินเมื่อเกิดเหตุการณ์ที่ทำให้ไม่สามารถดำเนินการประมวลผลในระบบที่ใช้อยู่ได้ จึงเป็นสิ่งที่ต้องประเมินถึงว่า ธนาคารได้มีการตระหนักถึงความเสี่ยงในจุดดังกล่าวและมีการประเมินความเสี่ยงพร้อมทั้งการเตรียมพร้อมต่อ สถานการณ์ดังกล่าวอย่างไร ซึ่งจะมีความกระทบต่อฐานะความมั่นคงและการดำเนินงานของธนาคารอย่างมาก

3.2 ข้อมูลได้รับความเสียหายหรือถูกทำลายเนื่องจากขาดความรัดกุมในระบบการควบคุมภายใน และระบบสำรองภัย (Back up)

เมื่อระบบเกิดความล้มเหลวหรือผิดพลาด ขาดระบบการแก้ไขข้อมูลให้กลับคืนดังเดิม (Recovery) หรือขาดร่องรอยของข้อมูลที่จะใช้ติดตาม (Audit Trail) ซึ่งไม่ได้มีการกำหนดหรือออกแบบไว้อย่างเพียงพอ ในระบบ ที่มีการใช้เทคโนโลยีที่ก้าวหน้าและมีความสลับซับซ้อนนั้น จำเป็นต้องมีการออกแบบร่องรอยการตรวจสอบอย่างรัดกุม และรอบคอบมากยิ่งขึ้น

3.3 การใช้เทคโนโลยีโดยปราศจากการวางแผนที่ดี

การเร่งรัดพัฒนาใช้คอมพิวเตอร์โดยไม่ศึกษาผลกระทบที่เกี่ยวข้องทั้งในระยะสั้นและในระยะยาวจะ สร้างปัญหาให้กับองค์กรได้มากโดยเฉพาะอย่างยิ่งทางด้านระบบการควบคุมภายในที่ควรมีการวางแผนและพัฒนาควบคู่ กันไปกับการพัฒนางานต่าง ๆ ขององค์กรตั้งแต่เริ่มแรก ทั้งนี้ อาจสรุปปัญหาได้ดังนี้

- * โปรแกรมที่ไม่สามารถดัดแปลงแก้ไขได้โดยง่ายหรือต้องสิ้นเปลืองมากกว่าจะดัดแปลงให้เข้ากับ ความต้องการในปัจจุบัน
- * บุคลากรทางคอมพิวเตอร์ไม่มีความรู้ความสามารถและประสบการณ์อย่างเพียงพอ หรือมีการเข้า ออกในอัตราสูง
- * ขาดการต่อเนื่องในการพัฒนาโปรแกรม หรือขาดการจัดทำเอกสารประกอบ เพื่ออำนวยความสะดวก โดยบุคคลอื่น

- * บางโปรแกรมอาจมีการกำหนดจุดควบคุมไม่เพียงพอ ทำให้ผลจากการประมวลผลไม่ถูกต้องหรือไม่ครบถ้วน ต้องสิ้นเปลืองเวลาและทรัพยากรในการแก้ไขเปลี่ยนแปลงโดยเปล่าประโยชน์ และบางกรณีอาจจะก่อความสูญเสียให้กับองค์กรได้มากมาย
- * จัดองค์การและการบริหารบุคลากรในแผนกคอมพิวเตอร์ที่ไม่เหมาะสม มีการทำงานซ้ำซ้อนและไม่มีประสิทธิภาพ

3.4 ความเสี่ยงที่เกิดจากระบบการควบคุมภายในไม่เพียงพอ

ทำให้มีการเข้าถึงระบบคอมพิวเตอร์ เช่น อุปกรณ์คอมพิวเตอร์และระบบการสื่อสาร โปรแกรมระบบงาน เพิ่มข้อมูลและเอกสารประกอบระบบ ซึ่งอาจก่อให้เกิดความเสียหายจากการถูกทำลาย ถูกลักขโมย ถูกโจรกรรม ถูกเปลี่ยนแปลงแก้ไข เพิ่มเติม หรือลบข้อมูลโดยเจตนา ทำให้ความน่าเชื่อถือของงบการเงินจำเป็นต้องมีการตรวจสอบอย่างเหมาะสมและมีประสิทธิภาพอย่างสอดคล้องกับสภาวะการณ์ที่ได้เปลี่ยนแปลงด้วย

4. การกำกับและตรวจสอบธนาคารอิเล็กทรอนิกส์ในปัจจุบัน

เหตุผลและความจำเป็นที่ต้องมีการกำกับและตรวจสอบด้านคอมพิวเตอร์ของธนาคารพาณิชย์ก็เพราะเทคโนโลยีทำให้ขั้นตอนและวิธีการปฏิบัติเปลี่ยนไป เกิดความเสี่ยง (Risk) ที่ได้กล่าวไปแล้วติดตามมาในรูปแบบต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อธนาคารพาณิชย์และระบบธนาคารด้วย ซึ่งการประเมินตามหลักการ CAMEL ในแบบเดิมนั้นอาจไม่เพียงพอต่อการประเมินฐานะและการดำเนินงานของธนาคารพาณิชย์ในปัจจุบัน เนื่องจาก

4.1 การกำกับและตรวจสอบในลักษณะเดิมในสมัยที่ธนาคารพาณิชย์ประมวลงานแบบ Manual ส่วนใหญ่เป็นการประเมินจากเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีต หรือ After-the-Fact เช่น การวิเคราะห์และตรวจสอบจากงบการเงิน คุณภาพของสินเชื่อ ความสามารถในการชำระหนี้ การหารายได้ของธนาคาร ผลการบริหารและการดำเนินงานที่ผ่านมา เป็นต้น

4.2 การกำกับและตรวจสอบในลักษณะเดิมส่วนใหญ่ไม่ได้เกี่ยวข้องกับความเสี่ยงที่อาจก่อให้เกิดความเสียหายจากการให้บริการที่มีระบบการควบคุมและรักษาความปลอดภัยไม่เพียงพอ เช่น การสูญหายของข้อมูลทางการเงินในระบบคอมพิวเตอร์ การทุจริตผ่านทางระบบสื่อสารและความเสี่ยงจากระบบงานขัดข้องหรือเสียหาย ซึ่งมีผลกระทบต่อการทำงานอย่างต่อเนื่องของธนาคารพาณิชย์ เป็นต้น

4.3 ขอบเขตการกำกับและตรวจสอบในปัจจุบัน ควรครอบคลุมถึงความสามารถในการหารายได้และกำไรของธนาคาร ซึ่งมีการพัฒนาบริการใหม่ ๆ เนื่องจากแหล่งที่มาของรายได้ที่เป็นดอกเบี้ยเพียงอย่างเดียวไม่เพียงพอต่อการให้บริการ Electronic Banking ที่มีต้นทุนและค่าใช้จ่ายที่ค่อนข้างสูงมาก ธนาคารพาณิชย์ที่พัฒนาด้านนี้จึงควรมีรายได้อื่นมาชดเชย เช่น ค่าบริการต่าง ๆ เป็นต้น จะเป็นผลดีกับ Earnings และ Liquidity ของธนาคารโดยตรง

4.4 การกำกับและตรวจสอบธนาคารพาณิชย์ในปัจจุบัน ควรเน้นการประเมินการบริหารงานในระบบใหม่ที่มีการใช้ Electronic Banking เนื่องจากความจำเป็นในการพัฒนาและปรับปรุงแนวการบริหารให้ทันกับเทคโนโลยีและมีการวางแผนและหาวิธีต่าง ๆ มาใช้ หรือที่เรียกว่า Strategic Planning for Technology and Electronic Banking ซึ่งเป็นวิธีที่ทำให้ผู้บริหารของธนาคารทราบฐานะที่แท้จริงของธนาคาร เพื่อสร้างทิศทางที่เหมาะสมซึ่งส่งผลต่อความอยู่รอดของธนาคารทั้งในปัจจุบันและในอนาคต ซึ่งการประเมินทางด้านการบริหารหรือการจัดการนี้ จะช่วยลดความเสี่ยง ที่จะเกิดขึ้นกับธนาคารพาณิชย์ได้

ดังนั้น เพื่อให้การกำกับและตรวจสอบธนาคารพาณิชย์มีประสิทธิภาพ สามารถประเมินและวิเคราะห์ฐานะความมั่นคงของธนาคารได้อย่างถูกต้อง เหมาะสม ทันกาล และมีคุณค่าเพิ่มขึ้น จึงมีการกำกับและตรวจสอบทางด้านธนาคารอิเล็กทรอนิกส์เพิ่มขึ้นอีกประเภทหนึ่ง นอกเหนือจากการตรวจสอบฐานะและการดำเนินงานตามปกติ เพื่อให้เหมาะสมและสอดคล้องกับการเปลี่ยนแปลงทาง Banking Technology

5. การตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์

วัตถุประสงค์หลักในการตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์ก็คือการประเมินความเสี่ยงในการดำเนินงานด้านคอมพิวเตอร์ของธนาคารพาณิชย์ ซึ่งอาจมีผลกระทบต่อฐานะและความสามารถในการดำเนินงานได้อย่างต่อเนื่อง การตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์มีลักษณะเป็นการป้องกันปัญหาและให้ข้อเสนอแนะในการแก้ไขหรือลดความเสี่ยงในการดำเนินงานด้านคอมพิวเตอร์ก่อนที่จะเกิดความเสียหายแก่ธนาคารพาณิชย์

6. ความเสี่ยงในการดำเนินงานด้านคอมพิวเตอร์อันอาจมีผลกระทบต่อฐานะของธนาคารพาณิชย์

ได้แก่ความเสี่ยงในการดำเนินงานด้านคอมพิวเตอร์ที่มีผลกระทบ CAMEL คือ Capital, Assets, Management, Earnings และ Liquidity ได้

ในกรณีที่ธนาคารพาณิชย์ระดมเงินทุนเพื่อลงทุนในอุปกรณ์คอมพิวเตอร์มากเกินไปเกินฐานะและความจำเป็นของธนาคาร แทนการนำเงินทุนดังกล่าวไปสร้างเป็นสินทรัพย์เพื่อก่อให้เกิดรายได้ อาจจะทำให้เกิดความไม่เหมาะสมในเรื่องแหล่งที่มาและที่ใช้ไปของเงินทุน (Source and use of fund) ซึ่งเกิดจากการใช้ประโยชน์ไม่คุ้มค่าและมีจุดอ่อนที่ก่อให้เกิดความเสี่ยงอย่างมีนัยสำคัญในระบบงานและการควบคุมที่จะมีผลกระทบต่อรายได้ (E) คุณภาพของสินทรัพย์ (A) และเงินกองทุน (C) ของธนาคารและก่อให้เกิดปัญหาซึ่งเกิดจากการบริหารงานและการจัดการ (M) ของธนาคาร และในกรณีที่ธนาคารได้รับผลเสียหายจากระบบงานมีจุดอ่อนอย่างร้ายแรง ในระบบ payment system ก็อาจมีผลกระทบต่อสภาพคล่อง (L) ของธนาคารได้ในที่สุด

7. เป้าหมายหลักของธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทยในฐานะที่เป็นธนาคารกลางของประเทศ เป็นสถาบันการเงินที่มีความสำคัญยิ่ง วัตถุประสงค์หลักเพื่อรักษาเสถียรภาพทางการเงินทั้งภายในประเทศและระหว่างประเทศ เพื่อสร้างเสริมความมั่นคงของสถาบันการเงิน และเพื่อสนับสนุนการเติบโตทางเศรษฐกิจให้อยู่ในระดับที่เหมาะสม

ความก้าวหน้าทางเทคโนโลยีและการสื่อสารทำให้ธุรกิจการเงินของโลกมีความเชื่อมโยงสัมพันธ์ใกล้ชิดจากเครือข่ายในประเทศขยายออกเป็นเครือข่ายระดับโลก (Internationalization) รวมทั้งสถาบันการเงิน ตลาดเงินและตลาดทุนระหว่างประเทศเป็นระบบเดียวกันมากขึ้น (Globalization) ระบบการเงินทั้งธนาคารพาณิชย์และสถาบันการเงินจึงให้ความสำคัญแก่ประสิทธิภาพมากขึ้น แต่ขณะเดียวกันธนาคารแห่งประเทศไทยก็ต้องมีหน้าที่ดูแลการปรับปรุงประสิทธิภาพเหล่านั้น ต้องไม่ทำลายหรือทำให้ความมั่นคงน้อยลง

การกำกับและตรวจสอบธนาคารอิเล็กทรอนิกส์มิได้มีขอบเขตอยู่เพียงการไปตรวจสอบระบบงานและการปฏิบัติงานคอมพิวเตอร์เท่านั้น แต่ยังได้วิเคราะห์และประเมินความเสี่ยง (Risk) ของ Banking technology และธนาคารอิเล็กทรอนิกส์และเป้าหมายเพื่อควบคุมและลดหรือขจัดความเสี่ยงต่าง ๆ ที่จะกระทบกับฐานะและความมั่นคงของธนาคารพาณิชย์และธนาคารทั้งระบบ โดยเน้นในด้านการป้องกันปัญหาที่ความเสียหายจะเกิดขึ้นเป็นสำคัญ

ธนาคารแห่งประเทศไทยได้ให้ความสนใจในการที่ธนาคารพาณิชย์นำเอาธนาคารอิเล็กทรอนิกส์มาให้บริการ และได้ติดตามความก้าวหน้าของธนาคารพาณิชย์มาโดยตลอด จนกระทั่งในช่วงปี พ.ศ. 2524 ได้มีการจัดตั้งหน่วยงานทำหน้าที่ดูแลและตรวจสอบในเรื่องนี้เป็นพิเศษ และได้มีส่วนร่วมพิจารณาวางกฎเกณฑ์ เงื่อนไขในการอนุญาตให้ธนาคารพาณิชย์เปิดบริการ ATM มีการกำหนดระบบการรักษาความปลอดภัยขั้นต่ำ เพื่อเสริมสร้างความมั่นคงปลอดภัย และให้ความคุ้มครองแก่ผู้ใช้บริการ และในช่วงเวลาที่ผ่านมามีหลังจากนั้น ก็ได้ให้หยุดยั้งในการศึกษาการพัฒนาด้านเทคโนโลยีที่ธนาคารพาณิชย์นำมาใช้ในการให้บริการ โดยมีวัตถุประสงค์เพื่อควบคุมดูแลติดตามฐานะของธนาคารพาณิชย์และส่งเสริมพัฒนาการด้านระบบการเงินการธนาคาร และรักษาไว้ซึ่งเสถียรภาพของระบบการเงินและเศรษฐกิจ อันจะเป็นประโยชน์ต่อประเทศชาติโดยรวมและให้ความคุ้มครองแก่ผู้ฝากเงิน

จากภาระหน้าที่ดังกล่าว ธนาคารแห่งประเทศไทยจึงจำเป็นต้องมีเครื่องมือที่ใช้ในการกำกับดูแลและติดตามฐานะความมั่นคงของธนาคารพาณิชย์ ให้มีการปฏิบัติอยู่ในขอบเขตของกฎหมาย ระเบียบ ข้อบังคับ โดยออกไปตรวจสอบ ณ สถานที่ทำการของธนาคารพาณิชย์ หรือการประเมินและวิเคราะห์จากข้อมูลที่ธนาคารพาณิชย์ต้องรายงานให้ทราบตามกฎหมาย

เช่นเดียวกับการตรวจสอบด้านคอมพิวเตอร์และการให้บริการธนาคารอิเล็กทรอนิกส์ก็จำเป็นต้องอาศัยเครื่องมือและปัจจัยเกื้อหนุน เพื่อใช้กำหนดทิศทางการให้บริการธนาคารอิเล็กทรอนิกส์ ให้เป็นไปในทิศทางที่ถูกต้องเหมาะสม และเอื้อประโยชน์ต่อประเทศชาติและส่วนรวม อย่างไรก็ตาม การพัฒนาเติบโตไปข้างหน้าของธนาคารพาณิชย์ในด้านเทคโนโลยีและการดำเนินธุรกิจในรูปแบบใหม่ ๆ บางครั้งอาจเป็นไปอย่างรวดเร็ว และเครื่องมือที่เคยใช้ได้ผลสำเร็จในการกำกับและดูแลติดตามฐานะของธนาคารพาณิชย์ อาจเข้าไปไม่ถึงฐานะและสภาพการดำเนินงานที่แท้จริงของธนาคารพาณิชย์ ทำให้เกิดช่องว่างขึ้นได้ ธนาคารแห่งประเทศไทยจึงจำเป็นต้องเข้าไปมีบทบาทในเรื่องที่เกี่ยวข้องกับคอมพิวเตอร์ด้วย

8. มาตรการของ ธปท. ทางด้านคอมพิวเตอร์ที่เกี่ยวข้องกับธนาคารพาณิชย์บางประการ

8.1 เรื่องที่เกี่ยวข้องกับฐานะความมั่นคงและการควบคุม

ระเบียบ กฎเกณฑ์ และข้อบังคับต่าง ๆ ที่กำหนดขึ้นก็เพื่อมุ่งจะเพิ่มประสิทธิภาพในระบบบัญชี ระบบการเงิน ให้มีความถูกต้องและน่าเชื่อถือได้เป็นสำคัญ ทั้งนี้อาจสรุปได้ดังนี้

ลำดับที่	ปี พ.ศ	เรื่องที่สำคัญโดยย่อ	วัตถุประสงค์
1	2524	ตั้งหน่วยตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์ที่ธนาคารแห่งประเทศไทย	ศึกษา พัฒนา งานการกำกับและตรวจสอบให้คำแนะนำทางด้านการลดความเสี่ยงในการดำเนินงานด้านคอมพิวเตอร์
2	2525	ส่งผู้ตรวจสอบไปซักซ้อมทำความเข้าใจเรื่องการตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์กับผู้บริหารระดับสูงของธนาคารพาณิชย์ทุกแห่ง	เพื่อให้ผู้บริหารระดับสูงของธนาคารพาณิชย์ได้ตระหนักและรับรู้ถึงการบริหาร และการดำเนินงานด้านคอมพิวเตอร์ที่มีประสิทธิภาพที่ได้มาตรฐานโดยทั่วไป พร้อมทั้งให้คำแนะนำเป็นการล่วงหน้าโดยเน้นการควบคุมและการพัฒนาที่จำเป็น ซึ่งธนาคารพาณิชย์อาจใช้เป็นมาตรฐานขั้นต่ำ ในการดำเนินงานที่เกี่ยวข้องกับคอมพิวเตอร์ได้ในระหว่างที่ธนาคารพาณิชย์หลายแห่งยังไม่พร้อมทางด้านนี้
3	2528	กำหนดให้ธนาคารพาณิชย์ต้องจัดให้มีระบบการรักษาความปลอดภัยทางด้านคอมพิวเตอร์ (Computer security) ตามมาตรฐานขั้นต่ำ (Minimum standard requirement) ตามที่ ธปท. กำหนด	เพื่อลดความเสี่ยง (Risk) ที่จะเกิดผลกระทบต่อฐานะความมั่นคงและการดำเนินงานอย่างต่อเนื่องของ ธ.พ. (ใช้ควบคู่กับเงื่อนไขการเปิดบริการ Electronic banking ต่างๆ เช่น ATM, Telebanking etc. ในอดีต)
4	2528	กำหนดให้ธนาคารพาณิชย์ต้องจัดให้มีการตรวจสอบด้านคอมพิวเตอร์ (Computer audit) อย่างน้อยหนึ่งครั้งในรอบ 12 เดือน โดยมีขอบเขตการตรวจสอบอย่างเพียงพอตามที่ ธปท. กำหนด และส่งสำเนารายงานพร้อมคำสั่งและข้อแนะนำให้ ธปท.	เพื่อให้ ธ.พ. จัดให้มีหน่วยตรวจสอบภายในด้านคอมพิวเตอร์ (Internal EDP auditor) โดยเฉพาะในการพัฒนางานตรวจสอบ และสร้างระบบการควบคุมภายในที่เหมาะสมในระหว่างที่กำลังพัฒนาระบบงานใหม่ๆซึ่งเป็นเรื่อง SDLC ให้ทัน กับการพัฒนางานของ ธ.พ. ในส่วนที่เกี่ยวข้องกับ Computer technology

ลำดับที่	ปี พ.ศ.	เรื่องที่สำคัญโดยย่อ	วัตถุประสงค์
5	2531	ให้ ธ.พ. จัดทำแผนฉุกเฉินและมีระบบคอมพิวเตอร์สำรอง (Emergency and Recovery plan) นอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลัก (Host computer) ของ ธ.พ. ให้ใช้งานได้ภายในปี 2532	เพื่อป้องกันมิให้บริการของ ธ.พ. ที่ใช้คอมพิวเตอร์ต้องหยุดชะงักอันเกิดจาก Hardware Software Peopleware ทุกประเภท ทั้งนี้ ตั้งแต่ปี 2533 เป็นต้นไป ธ.พ. จะหยุดการให้บริการอันมีสาเหตุจากคอมพิวเตอร์ขัดข้องหรือเสียหายเกิน 1 วันทำการ ไม่ได้
6	2531	กำหนดหลักเกณฑ์ให้ ธ.พ. ดำเนินการให้ External auditor ของ ธ.พ. จัดส่ง Audit program ทั้งทางด้าน Financial และทางด้าน Computer ให้ ธ.พท. พิจารณา เพื่อให้ความเห็นชอบ ในการเป็นผู้สอบบัญชีของธนาคารพาณิชย์นั้นๆ	เพื่อประเมินประสิทธิภาพและความน่าเชื่อถือของผู้สอบบัญชี ผู้ที่จะเป็นผู้รับรองงบการเงินของธนาคารพาณิชย์ว่าได้จัดให้มีขอบเขตการตรวจสอบที่จำเป็นและเหมาะสมกับธุรกิจธนาคารพาณิชย์ที่ใช้คอมพิวเตอร์ในการประมวลข้อมูลตามสมควร ตั้งแต่งวดการบัญชีประจำปี 2531 เป็นต้นไป
7	2533	กำหนดเงื่อนไขการย้าย Data Center ออกไปตั้งนอกประเทศ และการตรวจสอบศูนย์บริการประมวลผล (Data Center) ของ Third Party ทั้งในประเทศและต่างประเทศ	เพื่อรักษามาตรฐานของการตรวจสอบทั้งทางการเงิน (Financial Examination) และการตรวจสอบด้านคอมพิวเตอร์ (EDP examination) และเพื่อเป้าหมายในการให้ประเทศไทยเป็นศูนย์กลางทางการเงินแห่งหนึ่งในภูมิภาคนี้
8	2533 (อยู่ระหว่าง การ ดำเนิน งาน ในปีนี้)	ศึกษาความเสี่ยงในรูปแบบใหม่ ๆ ที่มาจากพัฒนาการ Computer technology ในวงการธนาคารและสถาบันการเงินใหม่ ๆ	เพื่อลดความเสี่ยงใหม่ๆ จาก Computer technology ที่ธนาคารพาณิชย์และสถาบันการเงินนำมาใช้ โดยเฉพาะอย่างยิ่ง Electronic Fund Transfer และ การหักกลบลบหนี้ (Netting scheme) ทั้งในและระหว่างประเทศที่เกี่ยวข้องกับ Systematic risk, Settlement risk, Receiver risk, Sender risk, Liquidity risk เป็นต้น

ลำดับที่	ปี พ.ศ.	เรื่องที่สำคัญโดยย่อ	วัตถุประสงค์
9	2533 (อยู่ ระหว่าง การ ดำเนิน งาน ในปีนี้)	ศึกษา Minimum Standard of Information (MSI) ที่จำเป็นต่อการตรวจสอบด้านการเงิน (Financial examination)	เพื่อป้องกันปัญหาการตรวจสอบทางการเงินในกรณีที่ธนาคารพาณิชย์พัฒนาระบบไปสู่ยุค Paperless system เพราะ Hard Copy ที่พอจะมีให้ตรวจสอบบางประเภทได้ก็อาจถูกจำกัดโดยระบบงาน ทำให้ผู้ตรวจสอบโดยทั่วไปมีปัญหาในการปฏิบัติงานได้

นอกจากนี้ ก็มีการประสานงานและพัฒนาการตรวจสอบร่วมกันระหว่าง Financial examiner กับ EDP examiner และผู้วิเคราะห์งานที่เกี่ยวข้อง เพื่อปรับปรุงแนวทางการกำกับและตรวจสอบธนาคารพาณิชย์ที่ใช้คอมพิวเตอร์ให้เหมาะสมยิ่งขึ้น

8.2 เรื่องอื่น ๆ

ศึกษาค้นคว้าและพัฒนาปรับปรุงงานที่กระทบต่อการกำกับและตรวจสอบธนาคารพาณิชย์ในขอบเขตต่อไปนี้

- * การพัฒนาทางเทคโนโลยีการสื่อสาร เครื่องมืออุปกรณ์ Hardware และ Storage รวมทั้ง Software
- * การคิดค้นทางเทคโนโลยี (Technology) ที่กระทบต่อการวางแผนและการควบคุมของธนาคารพาณิชย์
- * ความเสี่ยงที่เกิดขึ้นจากการให้บริการธนาคารอิเล็กทรอนิกส์ (Electronic Banking) ทั้ง Wholesale และ Retail รวมทั้งสถานะปัจจุบันของการให้บริการที่สำคัญแต่ละประเภท
- * กำหนดมาตรการและแผนฉุกเฉินเพื่อป้องกันความเสียหายจากการใช้ระบบอิเล็กทรอนิกส์ในการปฏิบัติงานภายใน และส่วนที่ไปใช้บริการคอมพิวเตอร์ภายนอกธนาคาร
- * กำหนดและเพิ่มเติมทางเลือกในการกำกับและควบคุมธนาคารพาณิชย์ที่เหมาะสมรวมทั้งการเข้าไปมีส่วนร่วมในการพัฒนามาตรฐานระบบงานเท่าที่พิจารณาว่าสมควร
- * การปรับปรุงแก้ไขปัญหาด้านกฎหมายและออกกระเบียบคำสั่งที่เกี่ยวข้องกับเทคโนโลยีเพื่อการธนาคาร (Banking Technology)
- * ผลกระทบจากวิวัฒนาการทางด้านเทคโนโลยีที่มีต่อนโยบายการกำกับและตรวจสอบธนาคารพาณิชย์ทั้งในฐานะที่ธนาคารแห่งประเทศไทยรับผิดชอบในการควบคุมและดูแลความมั่นคงปลอดภัยและความมีเสถียรภาพในระบบการเงินของประเทศ ที่มีการแข่งขันกันให้บริการทางการเงินประเภทต่าง ๆ อย่างมากมาย

และกว้างขวาง และการดำเนินงานให้บรรลุผลสำเร็จตามเป้าหมายเพื่อรักษาผลประโยชน์ของประเทศเป็นสำคัญ จึงจำเป็นต้องหาจุดดุลยภาพที่เหมาะสมระหว่าง

1. การให้ความสนับสนุนส่งเสริมและมั่นใจว่า ธนาคารพาณิชย์ซึ่งเป็นส่วนหนึ่งของระบบการเงินมีความมั่นคงและการดำเนินงานที่ดี (Safety and Soundness) และมีการปฏิบัติตามกฎหมาย
2. การให้การสนับสนุนและส่งเสริมการแข่งขันการให้บริการทางการเงินให้เป็นไปอย่างมีประสิทธิภาพ ถูกต้องเชื่อถือได้ และมีเสถียรภาพ

9. สรุป

เนื่องจากการพัฒนาการด้านเทคโนโลยีและการสื่อสารเป็นไปอย่างรวดเร็ว มีผลให้มีการนำบริการธนาคารอิเล็กทรอนิกส์รูปแบบใหม่ ๆ มาใช้ ธนาคารแห่งประเทศไทยในฐานะผู้ดูแลและกำกับธนาคารพาณิชย์ ตลอดจนมีหน้าที่สนับสนุนส่งเสริมการพัฒนาระบบการเงินและรักษาไว้ซึ่งเสถียรภาพทางระบบการเงินและระบบเศรษฐกิจของประเทศ จำเป็นต้องติดตามความเคลื่อนไหวดังกล่าวและประเมินผลกระทบที่จะเกิดขึ้นกับระบบธนาคาร ทั้งนี้ เพื่อรักษาและดำรงไว้ซึ่งความสามารถในการกำหนดแนวทางดูแลและกำกับธนาคารพาณิชย์ในเรื่องดังกล่าวได้โดยเหมาะสม กล่าวคือ

(1) มีการกำหนดและผ่อนคลายกฎเกณฑ์ เงื่อนไข กฎหมาย ข้อบังคับ ที่เหมาะสมและส่งเสริมความเจริญเติบโตของอุตสาหกรรมธนาคาร เพื่อที่จะดำรงไว้ซึ่งความเข้มแข็งทางการเงินของธนาคาร และเพื่อส่งเสริมให้ธนาคารมีความสามารถในการแข่งขันอย่างมีประสิทธิภาพและไม่ก่อให้เกิดความเสียหายแก่ระบบธนาคาร

(2) มีการศึกษาให้ทราบถึงความเสี่ยงใหม่ ๆ ที่ติดตามมาพร้อมกับการใช้เทคโนโลยีธนาคารอิเล็กทรอนิกส์ เพื่อสามารถตรวจสอบและควบคุมธนาคารพาณิชย์มิให้ปฏิบัติขัดต่อกฎหมายให้ความคุ้มครองและสร้างความปลอดภัยแก่ผู้ใช้บริการ

(3) ส่งเสริมให้มีการใช้ทรัพยากรอย่างประหยัด และมีประสิทธิภาพสูงสุด โดยมีการเพิ่มและขยายบริการที่คุ้มกับการลงทุน และเป็นประโยชน์ทั้งสำหรับธนาคารพาณิชย์ ผู้ใช้บริการ ธนาคารแห่งประเทศไทย และสังคมโดยรวมของประเทศ

(4) มีการให้บริการทัดเทียมกันและยุติธรรม โดยให้ธนาคารขนาดเล็กมีช่องทางขยายบริการให้ลูกค้าของตนตามที่ต้องการได้ โดยลงทุนไม่สูงมากจนกระทั่งไม่สามารถดำเนินการได้หรือตกอยู่ในฐานะเสียเปรียบ

(5) หาช่องทางร่วมมือกันในระดับธนาคารพาณิชย์ด้วยกัน และระหว่างธนาคารพาณิชย์กับธนาคารแห่งประเทศไทย หรือส่วนราชการอื่น ๆ เพื่อให้การวางแผนระยะยาวเป็นไปได้และสอดคล้องกับนโยบายหลักของประเทศ

(6) ให้มีการเลือกเครื่องมืออุปกรณ์อิเล็กทรอนิกส์ที่มีความยืดหยุ่นเพียงพอที่จะรองรับและสามารถปรับให้เข้ากับการขยายบริการอิเล็กทรอนิกส์ประเภทอื่น ๆ ที่จะมีในอนาคตได้อย่างเพียงพอ และก่อให้เกิดความประหยัด

(7) สนับสนุนส่งเสริมให้มีการคุ้มครองผู้บริโภคในการใช้บริการธนาคารอิเล็กทรอนิกส์ ซึ่งจะเป็นสิ่งสำคัญในการรองรับและสนับสนุนระบบธนาคารอิเล็กทรอนิกส์ และช่วยทำให้ผู้บริโภคยอมรับในบริการต่าง ๆ เหล่านั้น

การจะให้บรรลุวัตถุประสงค์ดังกล่าว จำเป็นต้องเข้าใจสภาพการณ์ที่เกี่ยวข้องในการนำธนาคารอิเล็กทรอนิกส์มาให้บริการ นั่นคือ ต้องมีการศึกษาผลกระทบอย่างรอบคอบ จึงจะกำหนดแนวทางการกำกับและตรวจสอบธนาคารพาณิชย์ได้โดยถูกต้องเหมาะสม อันจะเป็นประโยชน์โดยรวมแก่ทุกฝ่ายที่เกี่ยวข้อง



มาตรฐานการดำเนินงาน
ด้านคอมพิวเตอร์

1. การตรวจสอบของผู้ตรวจสอบภายในและผู้สอบบัญชี

สถาบันการเงินที่นำคอมพิวเตอร์มาใช้งาน ควรจัดให้มีการควบคุมภายในอย่างเพียงพอ เพื่อให้แน่ใจว่าการปฏิบัติข้อมูลถูกต้องและปลอดภัย ยึดมั่นตามนโยบาย มาตรฐานการบริหารงาน และระเบียบปฏิบัติที่เหมาะสม การควบคุมภายในจะมีประสิทธิภาพได้ก็ต่อเมื่อมีการตรวจสอบที่เป็นอิสระ ดังนั้น ภาระรับผิดชอบเบื้องต้นของคณะกรรมการบริหารของสถาบันการเงินคือ การจัดให้มีการตรวจสอบเพื่อประเมินผลการควบคุมภายใน

ผู้ตรวจสอบควรเสนอรายงานและแจ้งผลการตรวจสอบโดยตรงต่อคณะกรรมการบริหารสถาบันการเงิน เพื่อป้องกันมิให้ผู้ตรวจสอบอยู่ภายใต้การบังคับบัญชาของผู้ที่ถูกตรวจสอบ ซึ่งอาจทำให้ขาดความเป็นอิสระในการตรวจสอบได้

1.1 การคัดเลือกคณะผู้ตรวจสอบ

สถาบันการเงินควรคัดเลือกบุคคลที่มีความรู้ความชำนาญพอที่จะตรวจสอบงานประมวลผลได้มาเป็นผู้ตรวจสอบภายในด้านคอมพิวเตอร์ของสถาบันการเงิน ในกรณีที่ผู้ตรวจสอบภายในของสถาบันการเงินยังไม่มีความรู้ความชำนาญดีพอ ควรขอความช่วยเหลือหรือมอบหมายหน้าที่ให้ผู้อื่น เช่น สำนักงานสอบบัญชี หรือผู้เชี่ยวชาญด้านคอมพิวเตอร์ หรือสถาบันการเงินอื่นที่เคยร่วมมือให้ความช่วยเหลือกัน ทำหน้าที่ตรวจสอบให้ จนกว่าสถาบันการเงินจะพัฒนาผู้ตรวจสอบภายในด้านคอมพิวเตอร์ที่มีคุณสมบัติเหมาะสมได้

สำหรับสถาบันการเงินที่ใช้บริการด้านคอมพิวเตอร์จากภายนอกสถาบันการเงินควรระบุความรับผิดชอบในการตรวจสอบไว้ในสัญญาจ้างให้แน่ชัด ซึ่งอาจเลือกวิธีใดวิธีหนึ่งหรือหลายวิธีรวมกันดังนี้

- (1) ให้ผู้ตรวจสอบภายในของบริษัทที่รับจ้างสถาบันการเงินประมวลผลช่วยตรวจสอบ วิธีนี้จะใช้ได้ผล หากสถาบันการเงินแน่ใจในความเป็นอิสระของผู้ตรวจสอบ
- (2) ใช้ผู้ตรวจสอบภายในและ/หรือผู้สอบบัญชีของสถาบันการเงินดำเนินการตรวจสอบ
- (3) ใช้บุคคลที่สาม (Third-party) ที่มีคุณสมบัติเหมาะสมมาดำเนินการตรวจสอบโดยอิสระไม่ขึ้นกับใครทั้งสองฝ่าย
- (4) ตรวจสอบร่วมกันหลายสถาบันการเงิน ในกรณีที่สถาบันการเงินหลายแห่งใช้บริการด้านคอมพิวเตอร์จากบริษัทที่รับจ้างประมวลผลแห่งเดียวกัน โดยอาจตกลงร่วมกันตรวจสอบงานประมวลผล

1.2 หน้าที่และความรับผิดชอบของผู้ตรวจสอบภายใน

สถาบันการเงินควรกำหนดหน้าที่และความรับผิดชอบของผู้ตรวจสอบภายในเป็นลายลักษณ์อักษร ให้ชัดเจน งานของผู้ตรวจสอบภายใน ได้แก่

- (1) ตรวจสอบ ประเมินผล และรายงานเกี่ยวกับการบัญชี การเงิน และการควบคุมภายใน มี การปฏิบัติที่ถูกต้องและน่าพอใจเพียงใด
- (2) ช่วยให้การควบคุมภายในมีประสิทธิภาพ
- (3) ควบคุมให้มีการปฏิบัติตามนโยบาย แผนงาน วิธีการและระเบียบที่วางไว้
- (4) ควบคุมการใช้ทรัพย์สินและป้องกันมิให้สูญหาย

- (5) ควบคุมการบริหารงานข้อมูลที่นำมาใช้งาน
- (6) ประเมินประสิทธิภาพการทำงานของหน่วยงานต่าง ๆ
- (7) เสนอแนะแนวทางการแก้ไขข้อบกพร่องของการควบคุมภายใน

ผู้ตรวจสอบภายในจะต้องศึกษาเจาะลึกเข้าไปในเรื่องการบันทึกบัญชี การควบคุมงานทุกขั้นตอน เพื่อทำความเข้าใจเกี่ยวกับงานที่ตรวจสอบอย่างเต็มที่ และจะต้องวิเคราะห์ ประเมินผลให้คำแนะนำ ตั้งข้อสังเกตเกี่ยวกับงานที่ตรวจสอบ เสนอต่อฝ่ายบริหาร

1.3 ความรู้ความสามารถของผู้ตรวจสอบภายในด้านคอมพิวเตอร์

ผู้ตรวจสอบภายในด้านคอมพิวเตอร์ควรมีความรู้ความชำนาญ ดังนี้

- (1) มีความรู้ความเข้าใจในระบบการบัญชีและการจัดเก็บข้อมูลเป็นอย่างดี
- (2) มีความเข้าใจในหลักการควบคุมภายในอย่างลึกซึ้ง
- (3) มีความสามารถในการตรวจสอบและจัดทำรายงานการตรวจสอบ
- (4) มีความสามารถในการติดต่อกับผู้ที่ถูกตรวจสอบและฝ่ายบริหารระดับสูง
- (5) มีความสามารถในการตรวจสอบสาเหตุ ข้อสรุป และเขียนรายงานวิจารณ์ในทางสร้างสรรค์
- (6) มีความเข้าใจในการปฏิบัติงานด้านคอมพิวเตอร์และการควบคุมภายในของระบบคอมพิวเตอร์
- (7) มีความรู้ความเชี่ยวชาญเกี่ยวกับการตรวจสอบ ตลอดจนเทคนิคในการตรวจสอบ
- (8) มีความรู้ทางวิชาการ (Technology) ด้านการปฏิบัติข้อมูล

สถาบันการเงินควรมีแผนฝึกอบรมแก่ผู้ตรวจสอบอย่างเพียงพอ เพื่อให้ทันกับความเจริญทางด้านคอมพิวเตอร์ ดังนี้

- (1) มีการฝึกอบรมตามหลักสูตรของผู้ผลิตคอมพิวเตอร์ ผู้จำหน่ายโปรแกรมสำเร็จรูปที่ใช้ในการตรวจสอบและในมหาวิทยาลัย
- (2) ให้ศึกษาค้นคว้าด้วยตนเอง
- (3) ฝึกปฏิบัติงานจริง
- (4) ร่วมกิจกรรมที่สมาคมวิชาชีพจัดขึ้น

1.4 ความเป็นอิสระของผู้ตรวจสอบ

ผู้ตรวจสอบภายในควรมีสายการบังคับบัญชาขึ้นตรงต่อคณะกรรมการบริหารสถาบันการเงิน หรือ คณะกรรมการตรวจสอบ คณะกรรมการบริหารสถาบันการเงินจะต้องมอบอำนาจให้ผู้ตรวจสอบอย่างเพียงพอ เพื่อให้สามารถตรวจสอบข้อมูลและการปฏิบัติงานได้ทุกชนิดรวมทั้งการแก้ไขข้อบกพร่องที่ตรวจพบได้ตามความเหมาะสม การรายงานผลการตรวจสอบให้คณะกรรมการบริหารสถาบันการเงินโดยตรงจะช่วยให้คณะกรรมการบริหารรับผิดชอบดูแลการตรวจสอบได้สมบูรณ์ยิ่งขึ้น

1.5 คู่มือการตรวจสอบภายใน

ฝ่ายตรวจสอบภายในของสถาบันการเงินควรจัดทำคู่มือการตรวจสอบเสนอให้คณะกรรมการบริหารหรือผู้รับผิดชอบของสถาบันการเงินพิจารณาเกี่ยวกับมาตรฐานและวิธีการตรวจสอบ ก่อนที่จะนำมาใช้เป็นมาตรฐานในการตรวจสอบและฝึกอบรมผู้ตรวจสอบต่อไป คู่มือการตรวจสอบควรระบุนโยบาย มาตรฐาน และวิธีการตรวจสอบอย่างน้อยในเรื่องต่อไปนี้.-

- (1) งานหรือหน้าที่ในการตรวจสอบ
- (2) ความถี่หรือระยะเวลาที่เข้าตรวจสอบ
- (3) วิธีการตรวจสอบงานประมวลผลที่สำคัญโดยละเอียด
- (4) วิธีการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ
- (5) มาตรฐานของกระดาษทำการ
- (6) มาตรฐานการรายงานและติดตามผลการตรวจสอบ
- (7) มาตรฐานของ Audit software (ได้แก่ เอกสารเกี่ยวกับ Software ที่นำมาใช้ การใช้ Software และการจัดซื้อ Software)
- (8) แนวการตรวจสอบระบบงานที่จะนำคอมพิวเตอร์ ซึ่งอยู่ระหว่างการพัฒนา

คู่มือดังกล่าวควรมีการปรับปรุงแก้ไข เพื่อให้สอดคล้องกับวิธีการตรวจสอบที่เปลี่ยนแปลงไป เนื่องจากการเปลี่ยนแปลงขอบเขตการตรวจสอบหรือระบบการปฏิบัติข้อมูลที่เปลี่ยนแปลงไปจากเดิม

1.6 การวางแผน การจัดคณะผู้ตรวจสอบ และการกำกับการตรวจสอบด้านคอมพิวเตอร์

1.6.1 การวางแผนการตรวจสอบ (Planning) หมายถึง การกำหนดวัตถุประสงค์ และวิธีการตรวจสอบโดยละเอียด เพื่อใช้เป็นแนวทางในการตรวจสอบ ลักษณะการตรวจสอบโดยทั่วไปแบ่งวิธีการตรวจสอบออกเป็นหลายขั้นตอน โดยทุกขั้นตอนจะมีจุดมุ่งหมายในการตรวจสอบ ดังนี้.-

วิธีการตรวจสอบโดยย่อ

(1) การตรวจสอบขั้นต้น (Preliminary review) มีจุดมุ่งหมายเพื่อทำความเข้าใจระบบบัญชีทั้งส่วนที่ใช้คอมพิวเตอร์ และส่วนที่ไม่ใช้คอมพิวเตอร์ ทั้งนี้ควรศึกษาขั้นตอนในการบันทึกบัญชี ขอบเขตการใช้ข้อมูล โครงสร้างพื้นฐานของการควบคุมทางบัญชีในศูนย์ประมวลผลและผู้ใช้ข้อมูล โดยอาจจะใช้วิธีการสอบถาม สังเกตการณ์ตรวจสอบเอกสารสำคัญ (Documentation) ติดตามการจัดทำข้อมูล และใช้แบบสอบถามเกี่ยวกับการควบคุมภายใน หรือ Check Lists

(2) การกำหนดขอบเขตของการตรวจสอบ เพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ (Determine Scope of Audit Necessary to Accomplish Audit Objectives) มีจุดมุ่งหมายเพื่อประเมินผลการควบคุมภายในที่สำคัญ เช่น การควบคุมทางบัญชีโปรแกรมและการปฏิบัติงาน เป็นต้น วิธีการและขอบเขตของการตรวจสอบขึ้นอยู่กับความคิดเห็นของผู้ตรวจสอบ

(3) **สอบทานระบบควบคุมทั่วไป** (Review of General Controls) มีจุดมุ่งหมายเพื่อศึกษาระบบควบคุมทั่วไปภายในศูนย์คอมพิวเตอร์และหน่วยงานที่ใช้ข้อมูล พิจารณาข้อดีและข้อเสีย และทดสอบการควบคุมที่จำเป็น การสอบทานทำได้โดยการศึกษาเอกสารสำคัญ (Documentation) อย่างละเอียด สอบถามพนักงานในศูนย์คอมพิวเตอร์และหน่วยงานที่ใช้ข้อมูลและการสังเกตการณ์

(4) **สอบทานระบบควบคุมสำหรับงานใดงานหนึ่งโดยเฉพาะ** (Review of Application Controls) มีจุดมุ่งหมายเพื่อศึกษาระบบควบคุม และพิจารณาทดสอบการควบคุมที่จำเป็น วิธีสอบทานเป็นทำนองเดียวกับข้อ (3)

(5) **การประเมินผลขั้นต้นเกี่ยวกับการควบคุมภายใน** (Assessment of Controls) มีจุดมุ่งหมายเพื่อประเมินผลการควบคุมภายในที่สำคัญ เป็นการพิจารณาชนิดของข้อผิดพลาด วิธีควบคุม วิธีค้นหาวิธีการตรวจสอบขึ้นอยู่กับความคิดเห็นของผู้ตรวจสอบ

(6) **การทดสอบการปฏิบัติงานตามระเบียบที่ได้กำหนดไว้** (Test of Compliance) มีจุดมุ่งหมายเพื่อพิจารณาว่า มีวิธีการควบคุมภายในที่จำเป็นและผลของการควบคุมน่าพอใจเพียงใด วิธีการที่ใช้ คือ การตรวจสอบบันทึกการทำงาน ทดสอบวิธีควบคุม สอบถามและสังเกตการณ์

(7) **การประเมินผลขั้นสุดท้ายเกี่ยวกับการควบคุมภายใน** (Evaluation of Controls) มีจุดมุ่งหมายเพื่อพิจารณาชนิดของข้อผิดพลาด และวิธีป้องกันหรือค้นหาข้อผิดพลาด ผลที่กระทบต่อลักษณะเวลาและขอบเขตของการตรวจสอบ วิธีการที่ใช้ขึ้นอยู่กับความคิดเห็นของผู้ตรวจสอบ

1.6.2 การจัดคณะผู้ตรวจสอบ (Organizing) หมายถึง การจัดผู้ตรวจสอบและเครื่องมือที่จะใช้ในการตรวจสอบ กำหนดหน้าที่ความรับผิดชอบแต่ละบุคคลตามแผนงานที่วางไว้ และประเมินประสิทธิภาพของโครงสร้างและแผนงานที่กำหนดไว้

1.6.3 การกำกับการตรวจสอบ (Supervising) หมายถึง การกำหนดขอบเขต ความถี่ และมาตรฐานการตรวจสอบ ดูแลให้มีการปฏิบัติตามมาตรฐานการตรวจสอบ ติดตาม ควบคุม และปรับปรุงมาตรฐานการตรวจสอบที่กำหนดไว้ให้สอดคล้องกับสถานการณ์อย่างใกล้ชิด เพื่อนำผลการตรวจสอบมาปรับปรุงแก้ไขตามควรแก่กรณี

1.7 วิธีการตรวจสอบ (Audit Procedures) การตรวจสอบด้านคอมพิวเตอร์มีอยู่หลายวิธี สุดแล้วแต่ความรู้ความชำนาญของฝ่ายตรวจสอบและสภาพของสถาบันการเงินแต่ละแห่ง แต่พอสรุปวิธีการตรวจสอบที่เป็นมาตรฐานได้ 2 วิธี คือ วิธีที่ไม่ใช้คอมพิวเตอร์ช่วยในการตรวจสอบ และวิธีที่ใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

1.7.1 การตรวจสอบโดยไม่ใช้คอมพิวเตอร์

การตรวจสอบตามวิธีนี้อาศัยการพิจารณาสภาพการดำเนินงานประมวลผลเป็นหลักในการทดสอบข้อมูล โดยการสุ่มตัวอย่างข้อมูลมาทำการทดสอบ ซึ่งไม่จำเป็นต้องใช้โปรแกรมและคอมพิวเตอร์เข้าช่วย ผู้ตรวจสอบภายในจะนำข้อมูลที่คัดเลือกมาทดสอบนี้เปรียบเทียบกับเอกสารขั้นต้นที่เป็นแหล่งกำเนิดข้อมูล และ/หรือสอบทานยืนยันยอดข้อมูลแต่ละรายการกับเอกสารต้นฉบับโดยตรงเป็นการกระหายอดข้อมูล ซึ่งจะได้ผลเช่นเดียวกับการตรวจสอบสมุดบัญชีตามแบบเก่าที่ใช้พนักงานบันทึกบัญชี

นอกจากนี้ ผู้ตรวจสอบภายในควรตรวจสอบการปฏิบัติงาน ทดสอบการปฏิบัติตามระเบียบและทำการทดสอบในเรื่องอื่น ๆ ที่มีความสำคัญ รวมทั้งประเมินคุณภาพของข้อมูลด้วย แม้ว่าการตรวจสอบดังกล่าวไม่ได้ระบุไว้ในโปรแกรมการตรวจสอบด้านคอมพิวเตอร์ก็ตาม ทั้งนี้ เพื่อสอบทานความถูกต้องในการประมวลผล โดยดำเนินการดังนี้

- (1) ตรวจสอบการปฏิบัติงาน (Application Review)
 - (1.1) ใช้แบบสอบถาม
 - (1.2) สอบถามพนักงานของศูนย์ประมวลผล
 - (1.3) ศึกษากระบวนการทั่วไปโดยละเอียด
 - (1.4) ตรวจสอบวิธีการควบคุมที่สำคัญในส่วนที่เกี่ยวข้องกับหน่วยงานที่ใช้ข้อมูลและศูนย์ประมวลผล
 - (1.5) ตรวจสอบวิธีการใช้โปรแกรมงานควบคุมข้อมูลที่นำมาประมวลผล เพื่อประโยชน์ในการตรวจสอบที่สำคัญ
- (2) ทำการทดสอบการปฏิบัติตามระเบียบที่ได้กำหนดไว้ (Compliance Test)
 - (2.1) ตรวจสอบเอกสารหลักฐานที่ใช้ในการควบคุมภายใน เช่น รายละเอียดเกี่ยวกับข้อผิดพลาด ยอดรวม batch ต่าง ๆ เป็นต้น
 - (2.2) ตรวจสอบรายงานที่ได้จากการประมวลผลย้อนกลับไปยังเอกสารขั้นต้นหรือในทางกลับกันอาจตรวจจากเอกสารขั้นต้นมายังรายงาน และตรวจสอบยอดรวมข้อมูลที่ปรากฏตามรายงานกับยอดรวมขั้นต้นด้วย
 - (2.3) สุ่มตัวอย่างข้อมูลมาตรวจสอบความถูกต้องในการประมวลผล
 - (2.4) ประเมินคุณภาพการทดสอบข้อมูล
 - (2.5) ตรวจสอบความถูกต้องในการสรุปยอดบัญชี(ยอดรวมย่อยกับยอดรวมทั้งสิ้น)
 - (2.6) สุ่มตัวอย่างข้อมูลมาทำการทดสอบ โดยการยืนยันยอด (confirmation) ทดสอบความสมจริง (reasonableness test) ฯลฯ
- (3) การประเมินข้อมูล
 - (3.1) กระทบยอดคุมของหน่วยงานที่ใช้ข้อมูลกับยอดคุมข้อมูลที่ได้ในระหว่างการประมวลผลและกระทบยอดตามรายงานที่ได้จากการประมวลผลกับตัวเลขในบัญชีแยกประเภททั่วไป
 - (3.2) พิจารณาการควบคุมภายในของหน่วยงานที่ใช้ข้อมูลศูนย์ประมวลผล และวิธีการควบคุมในโปรแกรมเป็นไปตามระเบียบที่วางไว้หรือไม่

1.7.2 การตรวจสอบโดยใช้คอมพิวเตอร์

การใช้คอมพิวเตอร์ช่วยตรวจสอบจะสามารถลดค่าใช้จ่ายในการทดสอบและสุ่มตัวอย่างลงได้ นอกจากนี้ ยังช่วยให้ผู้ตรวจสอบคุ้นเคยกับการใช้อุปกรณ์ในศูนย์ประมวลผลด้วย

ตัวอย่างการใช้คอมพิวเตอร์ช่วยตรวจสอบ

- (1) ทดสอบยอดรวมและการคำนวณ เพื่อสอบทานความถูกต้อง ในการประมวลผล
- (2) ทดสอบความสมบูรณ์ (completeness) ความมีเหตุผล สอดคล้องกันอย่างสม่ำเสมอ (logical consistency) ความถูกต้องในเงื่อนไข (validity of conditions) และความสมจริง (reasonableness) ของข้อมูล
- (3) สรุปยอดข้อมูลและวิเคราะห์การปฏิบัติงาน
- (4) ใช้เทคนิคการสุ่มตัวอย่างทางสถิติคัดเลือกข้อมูลมาใช้ในการยืนยันยอด
- (5) ดำเนินการประมวลผลโดยอิสระเลียนแบบของจริงเพื่อสอบทานความถูกต้อง (correctness) และความสม่ำเสมอ (consistency) ในการประมวลผลของโปรแกรมที่ใช้
- (6) ออกงบทดลองและรายงานสำหรับการตรวจสอบ

โปรแกรมที่ใช้ในการตรวจสอบ มีดังนี้

- (1) โปรแกรมที่เขียนขึ้นโดยคณะผู้ตรวจสอบภายในด้านคอมพิวเตอร์
- (2) โปรแกรมตรวจสอบทั่วไป (เช่น software audit package ของผู้ผลิตคอมพิวเตอร์ หรือสำนักงานสอบบัญชี)
- (3) โปรแกรมที่จ้างให้บุคคลภายนอกเขียนขึ้น

โปรแกรมที่ใช้ในการตรวจสอบเหล่านี้ ควรมีการควบคุมอย่างเข้มงวด ดังนั้นจะต้องควบคุมเอกสารที่เกี่ยวข้องกับโปรแกรม ข้อมูลที่ใช้ในการทดสอบ รายละเอียดเกี่ยวกับข้อมูลที่ทดสอบ (source listings) รวมทั้ง source และ object โปรแกรมที่ใช้ตรวจสอบ นอกจากนี้ จะต้องควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรมด้วย ในศูนย์ประมวลผลที่มีการควบคุม software library ที่ทันสมัย object audit program จะถูก catalogue เก็บไว้และใช้รหัสลับ (password) ป้องกัน ในกรณีนี้ ผู้ตรวจสอบจะต้องควบคุมเอกสารที่เก็บไว้ใน library หากวิธีการดังกล่าวขัดต่อระเบียบควบคุมภายในก็ไม่ควรจะ catalogue โปรแกรมที่ใช้ในการตรวจสอบเก็บไว้ใน library โปรแกรมต่าง ๆ ที่ใช้ในการตรวจสอบควรจัดทำเอกสารประกอบโดยละเอียดเพื่อทราบจุดมุ่งหมายและวิธีใช้โปรแกรมอย่างถูกต้อง

การนำเอา audit software ไปใช้ในการตรวจสอบควรดำเนินการดังนี้

- (1) จัดให้มีการควบคุมอุปกรณ์ (physical control) audit เว้นแต่ audit software ดังกล่าวจะถูก catalogue เก็บไว้ในระบบและมีการป้องกันเป็นอย่างดี
- (2) สังเกตการประมวลผลงานตรวจสอบ
- (3) ใช้โปรแกรมอิสระควบคุมหรือติดตามการประมวลผลด้วย audit software
- (4) ควบคุมแฟ้มข้อมูลที่จะใช้ในการประมวลผลและจัดทำรายงานให้สมบูรณ์และถูกต้อง

1.8 เทคนิคการตรวจสอบคอมพิวเตอร์ในระบบที่ทันสมัย (Advanced EDP Audit Techniques)

ในระบบคอมพิวเตอร์ที่ทันสมัย เช่น on-line realtime ระบบ data base และ distributive processing เป็นต้น การประเมินระบบงานจำเป็นต้องใช้ผู้ตรวจสอบที่มีความรู้ความชำนาญสูง และเคยผ่านงานตรวจสอบด้านคอมพิวเตอร์มาพอสมควร นอกจากนี้ ยังสิ้นเปลืองค่าใช้จ่ายสูงและใช้เวลาตรวจสอบมาก แต่จำเป็นต้องใช้

เทคนิคต่าง ๆ เข้าช่วยตรวจสอบ เนื่องจากการประมวลผลในระบบใหม่นี้จะทำให้ข้อมูลเปลี่ยนแปลงอยู่ตลอดเวลาการตรวจสอบแบบเก่าที่ใช้วิธี snapshot โดยการ dump ข้อมูลออกมาตรวจสอบทีละครั้งในระหว่างการประมวลผลย่อมไร้ผล สำหรับวิธีการตรวจสอบแนวใหม่ที่จะกล่าวต่อไปนี้เป็นเพียงหลักการย่อ ๆ ที่นิยมใช้กันดังนี้

(1) **Integrated test facility** เป็นการทดสอบข้อมูลในระหว่างการประมวลผลจริง ผู้ตรวจสอบจะสร้างข้อมูลสำหรับการตรวจสอบ ซึ่งมีลักษณะเหมือนข้อมูลจริงของหน่วยงานที่ใช้ข้อมูล แล้วป้อนเข้าคอมพิวเตอร์ให้ประมวลผลคละไปกับข้อมูลจริง ต่อจากนั้นจึงนำผลลัพธ์ที่ได้จากการประมวลผลเปรียบเทียบกับผลลัพธ์ที่ผู้ตรวจสอบคำนวณได้ล่วงหน้า แต่การใช้วิธีนี้จะต้องระมัดระวังในการแยกบัญชีและยอดรวมของข้อมูลที่ถูกทดสอบเป็นพิเศษ เพื่อหลีกเลี่ยงความสับสนที่อาจทำให้ผู้รายงานเข้าใจผิดคิดว่า มีการบันทึกสินทรัพย์สูงกว่าความเป็นจริง นอกจากนี้สถาบันการเงินบางแห่งยังไม่ยอมรับวิธีการนี้

(2) **Simulation** เป็นการพิสูจน์ความถูกต้องของข้อมูลโดยอิสระแยกต่างหากจากการประมวลผลจริง โดยใช้โปรแกรมอีกชุดหนึ่งของผู้ตรวจสอบ ซึ่งมีลักษณะการประมวลผลเหมือนกับโปรแกรมใช้งาน เพื่อเลียนแบบการประมวลผลและใช้ข้อมูลจริง แล้วนำผลลัพธ์เปรียบเทียบกับผลการประมวลผลจริง

(3) **Audit logging** คือ การบันทึกการปฏิบัติงานของพนักงานที่เกี่ยวข้องกับการประมวลผลเพื่อใช้เป็นข้อมูลสำหรับตรวจสอบในเรื่องที่เกี่ยวกับการใช้แฟ้มข้อมูล รวมทั้งการป้อนข้อมูลผ่านทางเครื่อง terminal และข้อมูลอ้างอิงเกี่ยวกับตัวผู้ใช้เครื่อง Terminal

(4) **Parallel operations** เป็นการสอบทานความถูกต้องของโปรแกรมใหม่ ๆ ที่จะนำมาใช้งานหรือโปรแกรมที่ถูกปรับปรุงแก้ไขใหม่ โดยนำโปรแกรมใหม่นี้ไปประมวลผลด้วยข้อมูลจริง ในขณะเดียวกันก็ให้ปฏิบัติงานที่จะใช้โปรแกรมใหม่ทำแทนไปตามเดิมควบคู่กันไปก่อนหากเป็นการแก้ไขโปรแกรมใหม่ก็ให้ใช้โปรแกรมเก่าประมวลผลด้วย เพื่อนำผลงานมาเปรียบเทียบหาข้อแตกต่างที่เป็นจุดบกพร่องของโปรแกรมใหม่ โดยปกติผู้เขียนโปรแกรมและผู้วิเคราะห์ระบบงานจะใช้วิธีดังกล่าว ทดสอบความถูกต้องของโปรแกรมอยู่แล้ว แต่ผู้ตรวจสอบจำเป็นต้องทดสอบให้แน่ใจอีกครั้ง

(5) **Base case system operation** คือ การใช้ข้อมูลที่ทำขึ้นสำหรับทดสอบโปรแกรมใหม่ที่จะนำมาใช้งาน เพื่อศึกษาการทำงานของโปรแกรมทุกขั้นตอนโดยละเอียดและเป็นการสอบทานความถูกต้องในการประมวลผล โดยนำผลการประมวลผลทุกขั้นตอนเปรียบเทียบกับผลลัพธ์ที่คำนวณไว้ล่วงหน้า

(6) **Embedded audit data collecting** คือ การใช้โปรแกรมน้อยที่ทำหน้าที่ตรวจสอบ (audit subroutine) เก็บไว้ใน software ร่วมกับโปรแกรมงานอยู่ตลอดเวลา เพื่อคัดเลือกข้อมูลที่ป้อนเข้าคอมพิวเตอร์และข้อมูลที่ได้รับการประมวลผลที่ควรนำมาตรวจสอบ

(7) **Transaction tagging** เป็นวิธีการตรวจสอบโดยการเติมรหัสพิเศษ (special code) ลงในท้าย record ที่บันทึกข้อมูลที่ป้อนเข้าสู่ระบบคอมพิวเตอร์เพื่อให้ทำหน้าที่ตรวจสอบการประมวลผลในจุดที่สำคัญ

(8) **Extended records** คือ การขยาย record ที่บันทึกข้อมูลเพื่อเพิ่ม control field สำหรับใส่ข้อมูลที่ใช้ในการควบคุมการประมวลผลเรียกว่า special field หรือ trailer record สามารถใช้ร่วมกับข้อมูลอื่นที่ป้อนเข้าคอมพิวเตอร์ได้ทุกงาน เพื่อประโยชน์ในการตรวจสอบ เช่น

(8.1) ทำ hash totals ซึ่งเป็นการรวมยอดข้อมูลเพื่อตรวจสอบความถูกต้องของข้อมูลที่ได้รับการประมวลผลโดยโปรแกรมที่สำคัญ และมีผลกระทบต่องานทั้งระบบ

- (8.2) คัดเลือกข้อมูลบางชนิด เพื่อประโยชน์ในการวิเคราะห์ประวัติแฟ้มข้อมูล
- (8.3) หาผลลัพธ์เพื่อนำไปคำนวณเปรียบเทียบกับข้อมูลที่ได้จากการประมวลผลในภายหลัง

1.9 การเข้าร่วมพัฒนาและทดสอบงานที่นำเข้าคอมพิวเตอร์ (Audit Participation in Application Development and Testing)

ผู้ตรวจสอบควรเข้าร่วมพัฒนาระบบงาน เพื่อให้การควบคุมภายในระบบงานมีประสิทธิภาพตั้งแต่เริ่มแรก โดยศึกษาความเหมาะสมของการควบคุมภายในและข้อมูลที่ควรเหลือไว้สำหรับการตรวจสอบ (Audit Trails) ในแต่ละงาน เพื่อเสนอแนะวิธีการควบคุมที่ดีต่อฝ่ายบริหาร และเมื่อผู้ออกแบบระบบงานออกแบบเสร็จเรียบร้อยแล้ว ผู้ตรวจสอบควรเข้าร่วมจัดทำข้อมูลที่ใช้ในการทดสอบ และประเมินผลของการทดสอบก่อนนำระบบงานใหม่ไปใช้ โดยผู้ตรวจสอบด้านคอมพิวเตอร์ควรทราบเกี่ยวกับสาเหตุของข้อผิดพลาด (Sources of Error) วิธีการทดสอบความถูกต้องของข้อมูล (Tests for valid data) และองค์ประกอบของยอดรวม (Control total composition)

1.10 การจัดทำเอกสารและรายงานการตรวจสอบ (Documenting and Reporting Audit Work)

ในคู่มือการตรวจสอบ ควรกำหนดมาตรฐานในการจัดทำกระดาษทำการและรายงานการตรวจสอบ มาตรฐานในการจัดทำกระดาษทำการ ควรประกอบด้วย

- (1) วิธีการปฏิบัติงานตรวจสอบ
- (2) วิธีการปฏิบัติงาน การบริหารงาน และควบคุมโปรแกรมของศูนย์คอมพิวเตอร์
- (3) รายละเอียดเกี่ยวกับ Hardware และระบบงานที่ตรวจสอบ
- (4) ลักษณะและขอบเขตของการทดสอบ
- (5) ผลการทดสอบ

การสรุปสิ่งที่ตรวจพบให้ฝ่ายบริหารทราบ ควรทำเป็นทางการโดยมีแนวปฏิบัติดังนี้

- (1) สรุปประเด็นสำคัญที่ตรวจพบเพื่อแจ้งให้ผู้บริหารตามสายงานทราบก่อนแล้วเขียนรายงานเสนอฝ่ายบริหารระดับสูงและคณะกรรมการบริหารสถาบันการเงินต่อไป
- (2) ขอบกพร่องในการควบคุมที่สำคัญที่ตรวจพบและปัญหาสำคัญที่ยังไม่มีข้อยุติ ควรให้ผู้ตรวจสอบอาวุโสยกขึ้นปรึกษาคณะกรรมการบริหารสถาบันการเงิน
- (3) การเขียนรายงาน ควรใช้สำนวนที่สละสลวย ข้อสังเกตที่สำคัญควรเขียนให้รวบรัด มีข้อเท็จจริงและข้อเสนอแนะแก้ไข
- (4) ในรายงานการตรวจสอบ ควรแสดงเหตุผลในการเปลี่ยนแปลงวิธีการตรวจสอบที่ต่างไปจากการตรวจสอบครั้งก่อน
- (5) ข้อวิจารณ์ (criticisms) และข้อสังเกตต่าง ๆ (observations) ที่ระบุในรายงานการตรวจสอบ ควรมีเอกสารกระดาษทำการสนับสนุนอย่างเพียงพอ
- (6) ควรให้เจ้าหน้าที่บริหารตามสายงานตอบชี้แจงข้อสังเกตต่าง ๆ ตามรายงานมาในเวลาอันควร

- (7) ผู้ตรวจสอบภายในต้องติดตามผลตามข้อสังเกตที่ระบุไว้ดังกล่าวเพื่อให้แน่ใจว่า ได้มีการแก้ไขให้ถูกต้องแล้ว หรือคณะกรรมการบริหารสถาบันการเงินได้ยอมรับความเสี่ยงภัยที่อาจเกิดขึ้น โดยไม่ทำการแก้ไขตามข้อสังเกตในรายงาน

รายงานสรุปผลการตรวจสอบ (Reporting Conclusions) เมื่อการตรวจสอบเสร็จสิ้นลง ผู้ตรวจสอบควรสรุปผลการตรวจสอบตามข้อเท็จจริงและเอกสารต่าง ๆ ที่ตรวจพบแยกตามความสำคัญ เพื่อมิให้รายงานการตรวจสอบสับสนไร้สาระ ซึ่งอาจทำให้คณะกรรมการบริหารธนาคารและฝ่ายบริหารระดับสูงมองไม่เห็นคุณค่าของรายงานดังกล่าวได้

รายงานการตรวจสอบจะแสดงข้อมูลที่เป็นประโยชน์ต่อฝ่ายที่ถูกตรวจสอบ ซึ่งมีหน้าที่รับผิดชอบช่วยให้สามารถประเมินผลการปฏิบัติงานของคุณยประมวลผลได้ ในรายงานการตรวจสอบไม่ควรระบุเพียงเรื่องที่ชี้ให้เห็นถึงการปฏิบัติงานที่ไม่ถูกต้องหรือความหละหลวมในการควบคุมงานประจำวันเท่านั้น แต่ควรรายงานให้ทราบถึงสภาพอันไม่เหมาะสมต่าง ๆ ที่ตรวจพบ พร้อมทั้งแนะนำวิธีการเพื่อแก้ไขหรือปรับปรุงให้ถูกต้องด้วย การจัดทำรายงานการตรวจสอบควรรวดเร็วและทันเวลา โดยสรุปข้อเท็จจริงและชี้ให้เห็นถึงสภาพการปฏิบัติงานที่น่าสังเกต เนื้อหาของรายงานควรเขียนเป็นแนวสร้างสรรค์ ถูกต้องและชัดเจน มีเหตุผลเพื่อให้ฝ่ายบริหารใช้เป็นแนวทางตัดสินใจ

นอกจากนี้ ผู้ตรวจสอบควรมีความสามารถในการติดต่อสนทนา เช่นเดียวกับการเขียนรายงาน เพื่อชี้แจงข้อเท็จจริงที่ตรวจพบ และเข้าใจปัญหาในระหว่างที่ทำการตรวจสอบ

1.11 การติดตามผลการตรวจสอบ (Audit Follow-up)

การติดตามผลการตรวจสอบว่า ฝ่ายบริหารได้ปฏิบัติตามข้อแนะนำต่าง ๆ ตามรายงานการตรวจสอบได้รวดเร็วและได้ผลเพียงใดนั้น ย่อมเป็นเครื่องชี้ให้เห็นถึงประสิทธิภาพในการตรวจสอบได้ประการหนึ่ง ฝ่ายตรวจสอบควรกำหนดรายละเอียดวิธีการในการติดตามผล ไว้ในคู่มือตรวจสอบเพื่อเป็นแนวทางในการติดตามผลตามข้อแนะนำต่อไป การติดตามผลการตรวจสอบสามารถทำได้ โดย

- (1) ให้เจ้าหน้าที่ตรวจสอบไปตรวจสอบติดตามผลในภายหลัง
- (2) กำหนดให้ทำหนังสือรายงาน เมื่อได้ทำการแก้ไขตามข้อแนะนำ
- (3) พิจารณารายงานการแก้ไข แล้วนำเสนอคณะกรรมการบริหารสถาบันการเงิน

ส่วนข้อบกพร่องสำคัญ ๆ ที่พบระหว่างตรวจสอบ ผู้ตรวจสอบควรติดตามผลในขณะนั้นได้เลย เพื่อให้แน่ใจว่าได้มีการแก้ไขเป็นที่น่าพอใจแล้ว หากไม่มีการปฏิบัติตามข้อแนะนำและข้อบกพร่องนั้นยังคงมีอยู่ ควรแจ้งไว้ในรายงานการติดตามผล แล้วเสนอให้คณะกรรมการบริหารสถาบันการเงินทราบต่อไป

การติดตามผลการตรวจสอบจะช่วยให้การตรวจสอบได้ผลดี แต่ไม่ควรจะเร่งรัดดำเนินการให้เร็วจนเกินไปจนกว่าจะแน่ใจว่า เทคนิคการติดตามผลที่ใช้ันได้ผล

1.12 ความรู้ความสามารถและความเป็นอิสระของผู้สอบบัญชี

ความรู้ความสามารถและความเป็นอิสระของผู้สอบบัญชี ควรเป็นไปตามมาตรฐานการตรวจสอบ

ดังนี้

- (1) มีแผนงานตรวจสอบ
 - (2) ควบคุมดูแลผู้ช่วย (ถ้ามี) ในการตรวจสอบ
 - (3) ศึกษาและประเมินผลการควบคุมภายใน เพื่อพิจารณากำหนดขอบเขตและวิธีการตรวจสอบ รวมทั้งการขยายขอบเขตการทดสอบ
 - (4) มีเอกสารหลักฐานสนับสนุนความเห็นที่ปรากฏในงบการเงินที่ตรวจสอบอย่างเพียงพอ
- สำนักงานสอบบัญชีบางแห่งอาจใช้บริการจากผู้เชี่ยวชาญภายนอกมาช่วยให้ความรู้ความชำนาญ การตรวจสอบด้านคอมพิวเตอร์เมื่อต้องการ

1.13 ความรับผิดชอบของผู้สอบบัญชี

หน้าที่ความรับผิดชอบของผู้สอบบัญชี ควรจะกำหนดให้ชัดเจน โดยทำเป็นหนังสือเสนอคณะกรรมการบริหารสถาบันการเงินและฝ่ายจัดการระดับสูงให้ทราบก่อนที่ผู้สอบบัญชีจะเริ่มปฏิบัติงานตรวจสอบ โดยระบุขอบเขตในการตรวจสอบ ระยะเวลาที่ใช้ในการตรวจสอบ และเวลาที่คาดว่าจะส่งรายงานได้ ควรสรุปเรื่องสำคัญ ๆ พร้อมทั้งแนบรายละเอียดในการตรวจสอบไว้ทุกเรื่องประวัติของผู้ตรวจสอบที่เกี่ยวข้อง และการเปิดเผยข้อมูลในรายงานการตรวจสอบ นอกจากนี้อาจจะระบุวิธีการตรวจสอบที่ไม่นำมาใช้ เช่น การยืนยันยอดลูกหนี้หรือเงินฝาก และอาจจะบ่งชี้ได้ว่าผู้สอบบัญชีจะแสดงความเห็นต่องบการเงินของสถาบันการเงินหรือไม่

ผู้สอบบัญชีควรสอบทานวิธีการควบคุมภายในด้านคอมพิวเตอร์ โดยถือเป็นส่วนหนึ่งของการประเมินผลระบบการควบคุมภายในทางการบัญชีทั้งหมด ดังนี้

(1) ผู้สอบบัญชีต้องสรุปความเห็นเกี่ยวกับวิธีการควบคุมด้านบัญชีที่ใช้คอมพิวเตอร์ในการประมวลผล และกำหนดขอบเขตการทดสอบที่จำเป็น

(2) เมื่อผู้สอบบัญชีเห็นว่า การควบคุมด้านบัญชีที่ใช้คอมพิวเตอร์ในการประมวลผลมีจุดอ่อน โดยปราศจากข้อสงสัย ผู้สอบบัญชีจะต้องประเมินผลกระทบของจุดอ่อนดังกล่าวที่มีต่องบการเงินที่ตรวจสอบและใช้วิธีการตรวจสอบอื่น เพื่อให้บรรลุวัตถุประสงค์ของการตรวจสอบด้วย

โดยปกติผู้สอบบัญชีต้องตรวจสอบการควบคุมภายในทั้งในด้าน General Controls และในด้าน Application Controls ซึ่งมีผลกระทบต่อการบันทึกและการป้องกันดูแลรักษาทรัพย์สิน ตลอดจนความถูกต้องของงบการเงิน General Controls ได้แก่ การควบคุมเกี่ยวกับการจัดองค์การ การปฏิบัติงาน วิธีการจัดทำเอกสาร การใช้อุปกรณ์และแฟ้มข้อมูล รวมทั้งการควบคุมอื่น ๆ ที่มีผลกระทบต่อการปฏิบัติงานด้านคอมพิวเตอร์ Application Controls ได้แก่ วิธีการควบคุมที่ใช้กับงานใดงานหนึ่งโดยเฉพาะ เพื่อให้แน่ใจว่าการบันทึกข้อมูล การประมวลผล และการรายงาน ได้กระทำโดยถูกต้อง

ในระหว่างที่ผู้สอบบัญชีตรวจสอบระบบการควบคุมภายในทางการบัญชีควรพิจารณาถึงขอบเขตการนำเอาคอมพิวเตอร์ไปใช้ปฏิบัติงานด้านการบัญชีที่สำคัญ ๆ ทุกงานเพื่อกำหนดขอบเขตในการตรวจสอบการควบคุมภายในด้านคอมพิวเตอร์ที่จำเป็น

ผู้สอบบัญชีแต่ละคนจะมีวิธีการศึกษาและประเมินผลการควบคุมด้านคอมพิวเตอร์แตกต่างกัน ส่วนใหญ่จะใช้แบบสอบถาม (Questionnaire) หรือ Work Program เป็นเอกสารหลักฐานในการสอบทานวิธีการควบคุมด้านคอมพิวเตอร์ทั้งแบบ General และ Application Controls ในเรื่องต่อไปนี้

- (1) การจัดรูปองค์การ (organization) เกี่ยวกับอุปกรณ์ที่ใช้ร่วมกับคอมพิวเตอร์ (equipment) และ software ที่ใช้ในการประมวลผล
- (2) การควบคุมข้อมูลที่ได้จากการประมวลผลของหน่วยงานที่ใช้ข้อมูล
- (3) เอกสารแสดงรายละเอียดเกี่ยวกับโปรแกรมและคู่มือปฏิบัติงาน
- (4) การควบคุมการประมวลผล
- (5) การรักษาความปลอดภัย
- (6) การตรวจสอบภายใน

1.14 การตรวจสอบกิจการที่รับจ้างประมวลผล

ผู้ตรวจสอบและผู้ตรวจสอบภายในของสถาบันการเงินจำเป็นต้องตรวจสอบการปฏิบัติงานของกิจการที่สถาบันการเงินว่าจ้างประมวลผลด้วย ผู้ตรวจสอบดังกล่าวทำการตรวจสอบในเรื่องคล้ายกันเป็นส่วนใหญ่ อย่างไรก็ตาม วัตถุประสงค์ ขอบเขตและวิธีการตรวจสอบของผู้ตรวจสอบทั้ง 2 ประเภท จะแตกต่างกัน

การตรวจสอบกิจการที่รับจ้างประมวลผลควรกระทำทุกด้าน เช่นเดียวกับการตรวจสอบศูนย์ประมวลผลของสถาบันการเงินเอง โดยพิจารณาความเพียงพอของการควบคุมในทุก ๆ ด้าน รวมทั้งการปฏิบัติงานในห้องคอมพิวเตอร์ ระบบงาน และโปรแกรม ตลอดจนการควบคุมข้อมูลที่ป้อนเข้าคอมพิวเตอร์และข้อมูลที่ได้จากการประมวลผลที่จะนำไปใช้

1.15 การประเมินงาน ตรวจสอบของผู้ตรวจสอบภายในและผู้สอบบัญชี

วัตถุประสงค์

1. เพื่อให้แน่ใจว่าผู้ตรวจสอบภายในหรือผู้สอบบัญชีได้ดำเนินการตรวจสอบและประเมินผลการควบคุมภายในของระบบการผลิตข้อมูลด้านคอมพิวเตอร์ ตลอดจนทำการทดสอบรายการต่าง ๆ ที่เกี่ยวข้องอย่างมีประสิทธิภาพ

2. เพื่อตรวจสอบรายงานของผู้ตรวจสอบภายในหรือผู้สอบบัญชี เพื่อพิจารณาว่าจะเชื่อถือตามรายงานนั้นได้มากน้อยเพียงใด ทั้งนี้ เพื่อกำหนดขอบเขตการตรวจสอบและการปฏิบัติงานของผู้ตรวจสอบได้ตามความเหมาะสม

แผนงานการตรวจสอบโดยย่อ

1. โครงสร้างของงานการตรวจสอบภายในที่มีอยู่
2. รายงานการตรวจสอบตั้งแต่การตรวจสอบครั้งก่อนจนถึงรายงานฉบับล่าสุดถ้าจำเป็นจะขอตรวจดูกระดาษทำการ เพื่อให้ทราบถึงขอบเขตและวิธีการตรวจสอบที่ใช้ (ผู้ตรวจสอบ อาจดเว้นการตรวจสอบในบางเรื่องได้ หากเชื่อถือการตรวจสอบของ Internal auditor ของสถาบันการเงิน)
3. รายงานการประชุมคณะกรรมการ เพื่อประเมินถึงบทบาทและการบริหารงานของฝ่ายบริหาร และการพิจารณาแก้ไขปัญหาต่าง ๆ

4. ประวัติย่อของพนักงานตำแหน่งสำคัญ ๆ ของฝ่ายตรวจสอบ และประวัติของเจ้าหน้าที่ตรวจสอบคอมพิวเตอร์แต่ละคน (เพื่อวัดประสิทธิภาพของผู้ตรวจสอบ อย่างไรก็ดี ผู้ตรวจสอบจะตระหนักไว้เสมอว่า ความชำนาญงานอาจได้มาโดยวิธีอื่น โดยไม่จำเป็นต้องเป็นผู้ที่มีคุณวุฒิทางการศึกษาเสมอไป)

5. คู่มือในการตรวจสอบระบบคอมพิวเตอร์ (EDP Audit Manual) เพื่อประเมินขอบเขตของงานการตรวจสอบ

6. Documentation ของงานบางประเภทที่ใช้โปรแกรมในการตรวจสอบ (Audit software programme) เพื่อพิจารณาถึงขอบเขตการทำงานของโปรแกรมที่ใช้ในการตรวจสอบ

2. การจัดองค์การของหน่วยงานด้านคอมพิวเตอร์

การจัดองค์การ เป็นการรวบรวมและจัดรูปร่างทางด้านคอมพิวเตอร์ให้เป็นสัดส่วนพร้อมทั้งกำหนดระเบียบการปฏิบัติภายในศูนย์คอมพิวเตอร์ เพื่อให้มีการแบ่งความรับผิดชอบมีบุคคลที่มีคุณภาพเหมาะสมกับตำแหน่งงาน และมีการทำงานที่เป็นระเบียบและเป็นขั้นตอน ซึ่งอำนวยความสะดวกในการควบคุมและตรวจสอบ ตลอดจนการดูแลรักษาข้อมูล

2.1 มาตรฐานขั้นต่ำของการจัดองค์การของศูนย์คอมพิวเตอร์

2.1.1 ศูนย์คอมพิวเตอร์ ควรเป็นอิสระขึ้นตรงต่อผู้บริหารระดับสูงของสถาบันการเงินและสามารถปฏิบัติงานร่วมกับแผนกอื่นได้ ภายใต้ระเบียบปฏิบัติที่ตกลงร่วมกัน หรือที่กำหนดโดยสถาบันการเงินเป็นลายลักษณ์อักษร

2.1.2 ส่วนงานและความรับผิดชอบในการปฏิบัติงานภายในศูนย์คอมพิวเตอร์ควรแบ่งขอบเขตโดยเด็ดขาดจากกันอย่างน้อย 3 ขอบเขต ดังนี้

- (1) งานด้านการบริหารทั่วไป ได้แก่ งานด้านการวางแผนและการควบคุมการปฏิบัติงานภายในศูนย์คอมพิวเตอร์
- (2) งานด้านการพัฒนาระบบงาน การจัดทำโปรแกรม ได้แก่ งานด้านวิเคราะห์และออกแบบระบบงาน การปรับปรุงวิธีการปฏิบัติงาน การออกแบบและจัดทำโปรแกรมสั่งงาน การพัฒนา ทดสอบ และบำรุงรักษาโปรแกรม และการจัดทำเอกสารประกอบระบบงาน โปรแกรมและการปฏิบัติการ
- (3) งานด้านการปฏิบัติการ ได้แก่ งานด้านการปฏิบัติงานประจำวันเกี่ยวกับระบบคอมพิวเตอร์ ดูแลการปฏิบัติงาน ผลิตข้อมูลประจำวันให้เป็นไปตามตารางที่กำหนดไว้ ควบคุมการทำงานของคอมพิวเตอร์ตามคู่มือการปฏิบัติงานที่ฝ่ายพัฒนาระบบงานกำหนดไว้ รับผิดชอบในการเก็บรักษาและควบคุมแฟ้มข้อมูลและโปรแกรม รับข้อมูลจากแผนกต่าง ๆ เพื่อทำการประมวลผลและจัดส่งข้อมูลที่ประมวลผลเรียบร้อยแล้วไปยังผู้ใช้

2.1.3 จัดให้มีคณะกรรมการดำเนินงานด้านคอมพิวเตอร์ ประกอบด้วย ตัวแทนจากหน่วยงานสำคัญของสถาบันการเงินและผู้บริหารระดับสูงเพื่อทำหน้าที่วางแผน แนะนำ ควบคุม และกำหนดทิศทางการดำเนิน

งานด้านคอมพิวเตอร์ของสถาบันการเงินโดยเน้นหนักไปในทางที่สนองตอบความต้องการของผู้ใช้ข้อมูล และความต้องการด้านการตรวจสอบ

ผู้แทนของแต่ละหน่วยงานจะต้องเป็นผู้ที่เข้าใจนโยบาย ระเบียบปฏิบัติ และวิธีการของแต่ละหน่วยงานเป็นอย่างดี รวมทั้งเป็นผู้ที่มีอำนาจในการตัดสินใจแทนหน่วยงานที่ตนสังกัดอยู่ได้ด้วย

การประชุมคณะกรรมการแต่ละครั้งจะต้องบันทึกรายงานการประชุมไว้โดยละเอียด

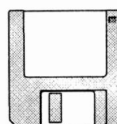
โดยทั่วไปคณะกรรมการดำเนินงานด้านคอมพิวเตอร์จะร่วมกันพิจารณาทบทวนและอนุมัติในเรื่องต่อไปนี้

- (1) การเปลี่ยนแปลง Hardware และ Software ที่สำคัญ
- (2) การศึกษา วิจัย และพัฒนาโครงการ
- (3) การจัดลำดับความสำคัญของโครงการ
- (4) การวิเคราะห์ต้นทุนเปรียบเทียบผลที่ได้ของโครงการ
- (5) การจัดกำลังและอุปกรณ์ของศูนย์คอมพิวเตอร์
- (6) การดำเนินการควบคุมอย่างมีประสิทธิภาพ
- (7) การปรับปรุงแผนการปฏิบัติงานให้เหมาะสม
- (8) การพิจารณาแผนการรักษาความปลอดภัยของศูนย์คอมพิวเตอร์
- (9) การจัดทำงบประมาณและวางแผนของศูนย์คอมพิวเตอร์

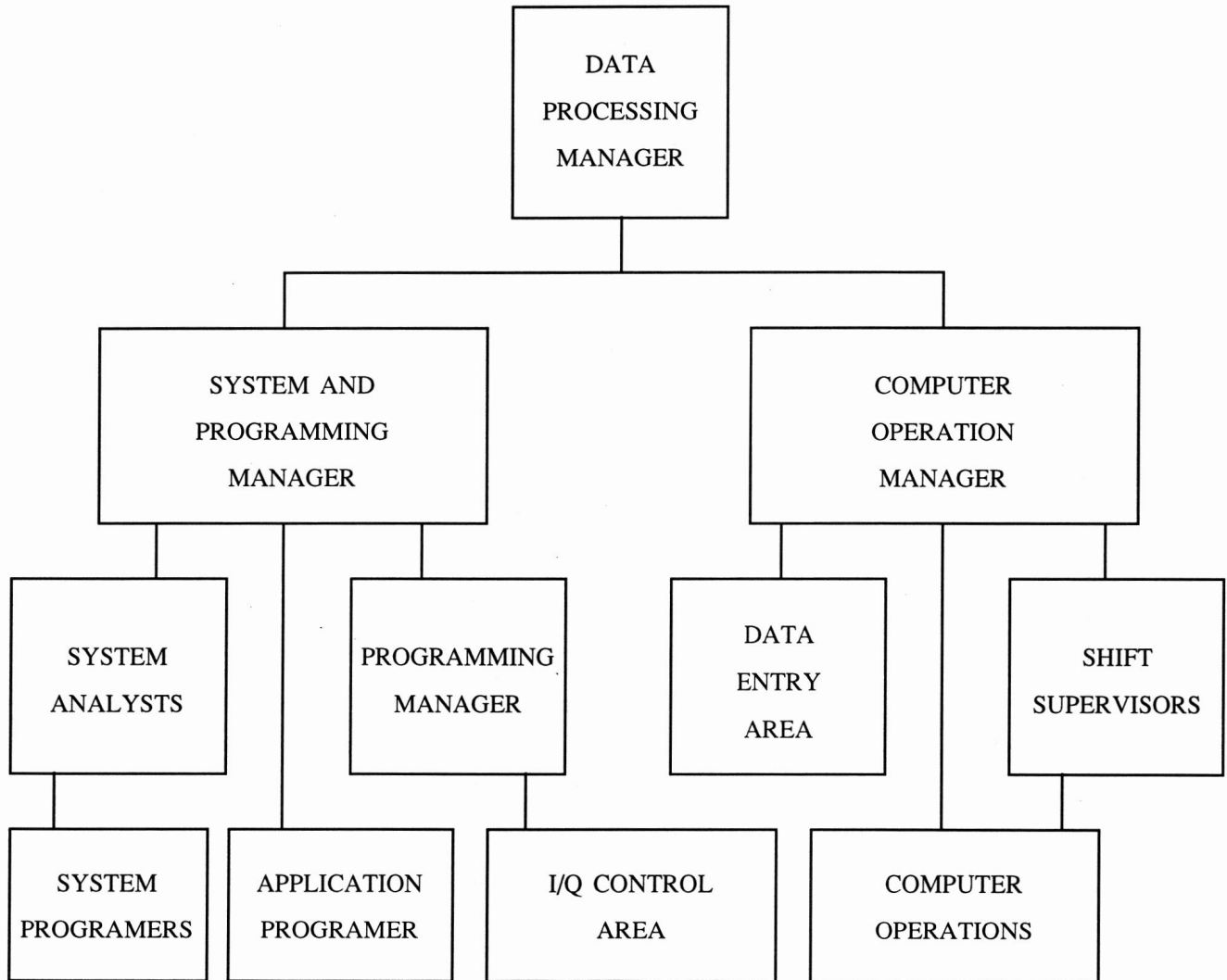
2.1.4 จัดให้มีมาตรฐาน วิธีการปฏิบัติงาน และการควบคุมการดำเนินงานด้านคอมพิวเตอร์อย่างเหมาะสม ซึ่งรวมถึงการวัดผลการปฏิบัติงาน การควบคุมภายใน และการจัดทำรายงานเสนอผู้บริหาร

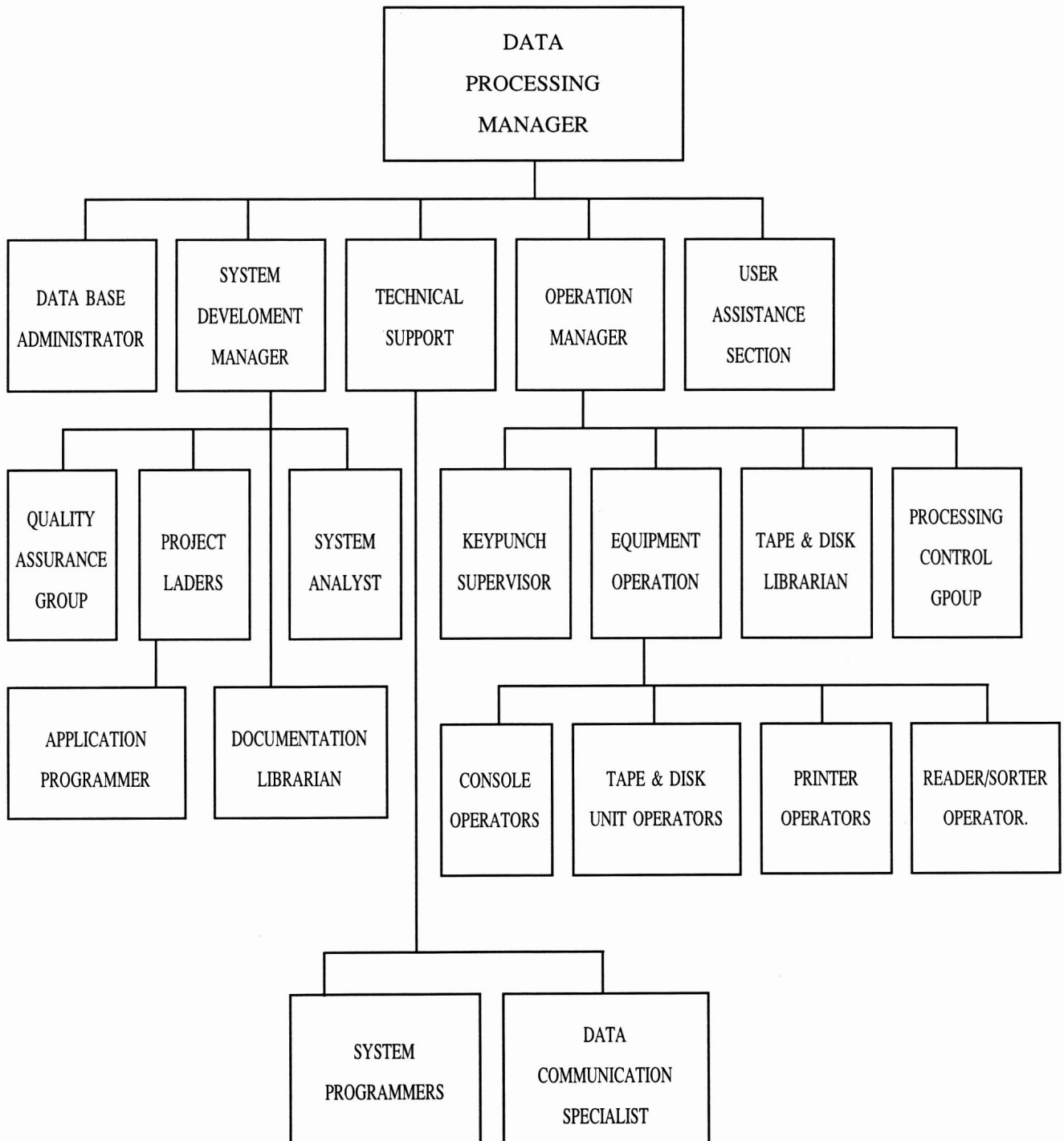
2.1.5 จัดทำคำอธิบายเกี่ยวกับลักษณะงาน (Position Descriptions) โดยระบุหน้าที่และความรับผิดชอบ ของแต่ละตำแหน่งงาน คุณสมบัติพื้นฐานและคุณสมบัติพิเศษของบุคลากรในตำแหน่งงานต่าง ๆ ลักษณะของงานที่ทำและการรายงานต่อผู้บังคับบัญชา

ตัวอย่างการจัดองค์การเฉพาะด้านคอมพิวเตอร์ และตัวอย่างโครงสร้างการจัดองค์การในภาพรวม ซึ่งแสดงถึงหน่วยงานตรวจสอบด้วย ได้ปรากฏตามแนบ



การจัดองค์กรของศูนย์คอมพิวเตอร์ขนาดเล็ก





2.2 การตรวจสอบการจ้างองค์การของหน่วยงานด้านคอมพิวเตอร์

วัตถุประสงค์

1. เพื่อตรวจสอบความเหมาะสมและส่งเสริมสภาพของโครงสร้างการจัดองค์การ และการบริหารงานด้านคอมพิวเตอร์ที่มีประสิทธิภาพสูงสุด ทั้งในด้านการปฏิบัติงานและการควบคุม เพื่อลดช่องทางความผิดพลาดและความเสียหายของการประมวลผลข้อมูล

2. เพื่อการพัฒนาระบบงานที่สอดคล้องกับการประกอบธุรกิจสถาบันการเงินที่ดี

แผนงานการตรวจสอบโดยย่อ

1. โครงสร้างขององค์กร หน้าที่ของหน่วยงาน และหน้าที่ของตำแหน่งงาน
2. ประวัติของพนักงานในศูนย์คอมพิวเตอร์
3. หน้าที่ของคณะกรรมการบริหารงานด้านคอมพิวเตอร์ และการดำเนินงาน โดยตรวจสอบจากรายงานการประชุมคณะกรรมการ
4. แผนการพัฒนาระบบงานใหม่และการปรับปรุงแก้ไขระบบงาน
5. มาตรการในการรักษาความปลอดภัย

3. มาตรฐานของระบบงาน

มาตรฐานของระบบงาน (Systems Standards) จะใช้เป็นแหล่งอ้างอิงหรือแนวทางสำหรับการพัฒนาระบบงานใหม่ การบำรุงรักษาระบบงานหรือการปรับปรุงระบบงานคอมพิวเตอร์ให้ดีขึ้น การตรวจสอบมาตรฐานเหล่านี้จะทำให้ผู้ตรวจสอบเข้าใจถึงระบบและการควบคุมทั่วไปของระบบคอมพิวเตอร์ ซึ่งควรมีการกำหนดวิธีปฏิบัติให้สอดคล้องกับมาตรฐานไว้เป็นลายลักษณ์อักษร และดูแลให้มีการปฏิบัติที่ผิดแผกไปจากมาตรฐานที่กำหนดไว้เสมอ

มาตรฐานของระบบงาน โดยทั่วไปอาจพิจารณาได้จาก

- 3.1 การควบคุมโครงการ
- 3.2 มาตรฐานการพัฒนาระบบงานโดยทั่วไป
- 3.3 กระบวนการพัฒนาระบบงาน
- 3.4 การจัดหาหรือจัดซื้อโปรแกรมสำเร็จรูป
- 3.5 มาตรฐานการเขียนโปรแกรม
- 3.6 มาตรฐานการทดสอบระบบงานและโปรแกรม
- 3.7 มาตรฐานการนำระบบงานใหม่ออกใช้งาน
- 3.8 การตรวจสอบผลการนำระบบงานใหม่ออกใช้
- 3.9 การรักษาความปลอดภัยเกี่ยวกับ Operating Systems
- 3.10 การควบคุมการปฏิบัติงานของ Application Programmer
- 3.11 การรักษาความปลอดภัยเกี่ยวกับโปรแกรมที่ใช้ประมวลผล
- 3.12 การควบคุมการปรับปรุงแก้ไขโปรแกรม
- 3.13 การควบคุมการปรับปรุงแก้ไขโปรแกรมในกรณีเร่งด่วนเป็นการชั่วคราว

3.1 การควบคุมโครงการ

เพื่อให้การบริหารโครงการบรรลุเป้าหมาย มีประสิทธิภาพและสามารถควบคุมค่าใช้จ่ายได้ สถาบันการเงินควรจัดให้มี

- (1) กำหนดระยะเวลาปฏิบัติงานตามโครงการ และวันที่ปฏิบัติงานแล้วเสร็จตามเป้าหมายทุกขั้นตอน เพื่อให้เปรียบเทียบกับผลการปฏิบัติงานจริง
- (2) หากมีการเปลี่ยนแปลงโครงการ ระยะเวลาปฏิบัติงาน และวันที่ที่แล้วเสร็จ ควรพิจารณา ทบทวนค่าใช้จ่ายของโครงการใหม่
- (3) จัดทำรายงานแสดงผลการปฏิบัติงานตามโครงการเสนอผู้บริหารระดับสูงของสถาบันการเงิน ทุกระยะ เพื่อใช้เป็นข้อมูลในการบริหารงาน

3.2 มาตรฐานการพัฒนาระบบงานโดยทั่วไป

การพัฒนาระบบงานที่ใช้ประมวลผลควรมีมาตรฐานและแนวทางปฏิบัติเกี่ยวกับเรื่องต่าง ๆ โดยทั่วไป ดังนี้

- (1) การออกแบบระบบงาน
- (2) การวิเคราะห์และการคัดเลือกโปรแกรมที่จัดหาหรือจัดซื้อมาใช้งาน
- (3) การจัดทำโปรแกรม
- (4) การทดสอบโปรแกรมและระบบงาน
- (5) การนำระบบงานใหม่ออกใช้งาน
- (6) การ Catalog โปรแกรม
- (7) การปรับปรุงแก้ไขโปรแกรม
- (8) การควบคุมและการจัดทำเอกสารสนับสนุนการปฏิบัติ

3.3 กระบวนการพัฒนาระบบงาน

กระบวนการพัฒนาระบบงานที่ละเอียดและชัดเจนทุกขั้นตอนจะช่วยให้ระบบงานที่พัฒนามีคุณภาพ การพัฒนาระบบงานส่วนใหญ่จะมีกระบวนการที่คล้ายคลึงกัน จะแตกต่างกันที่ระยะเวลาและกิจกรรมที่ต้องทำในรายละเอียดบางประการ กระบวนการพัฒนาระบบงานที่สำคัญมีดังนี้

- (1) ศึกษาความเป็นไปได้ของโครงการเพื่อประเมินผลดีผลเสียและหาข้อมูลสนับสนุนในการพิจารณาอนุมัติโครงการ
- (2) กำหนดลักษณะของงานที่ต้องทำในการพัฒนาระบบงาน เรียงตามลำดับก่อนหลัง โดยมีหน่วยงานที่ใช้ข้อมูลและผู้ที่เกี่ยวข้องร่วมพิจารณา และให้ความเห็นชอบนำไปใช้จัดทำโปรแกรม
- (3) การประเมินผลการควบคุมภายในของระบบงานใหม่ และข้อเสนอแนะของผู้ตรวจสอบด้านคอมพิวเตอร์เกี่ยวกับการควบคุมภายใน
- (4) การทดสอบความสมบูรณ์ของระบบงานใหม่ โดย computer operator และผู้ใช้ข้อมูลก่อนใช้งานจริง

- (5) การตรวจสอบผลการนำระบบงานใหม่ออกใช้งาน

3.4 การจัดหาหรือจัดซื้อโปรแกรมสำเร็จรูป

องค์ประกอบที่ใช้วิเคราะห์ในการจัดหาโปรแกรมสำเร็จรูปมีดังนี้

- (1) คุณสมบัติของ software จาก systems specifications
- (2) การวิเคราะห์ต้นทุนและผลตอบแทน (cost/benefit analysis) ของ software ที่เลือกซื้อ
- (3) ฐานะทางการเงินของผู้ผลิตหรือผู้ขาย software
- (4) ระบบเอกสารสนับสนุนการปฏิบัติงาน (documentation system) ของ software ที่จะซื้อ

3.5 มาตรฐานการเขียนโปรแกรม

เพื่อประสิทธิภาพในการพัฒนาโปรแกรมและประโยชน์ในการควบคุมภายในสถาบันการเงินควรจัดทำคู่มือเขียนโปรแกรมไว้เป็นมาตรฐานในการปฏิบัติงาน แม้ว่างานเขียนโปรแกรมส่วนใหญ่จำเป็นต้องอาศัยความคิดสร้างสรรค์มากก็ตาม คู่มือดังกล่าวควรประกอบด้วยวิธีการใช้คู่มือ เทคนิคการเขียนโปรแกรม วิธีการใช้ routine และโปรแกรมใช้งานอื่นทั่ว ๆ ไปที่สามารถนำมาใช้เพื่อช่วยลดงานเขียนโปรแกรมให้น้อยลง ตลอดจนวิธีการควบคุมภายในที่ควรมีในโปรแกรมเป็น built-in controls และวิธีการควบคุมอื่นๆ ที่อาจเป็นประโยชน์ต่อการเขียนโปรแกรมด้วย

3.6 มาตรฐานการทดสอบระบบงานและโปรแกรม

การทดสอบโปรแกรมระบบงานใหม่ที่จะนำไปใช้ประมวผลเป็นขั้นตอนที่สำคัญที่สุดอีกขั้นตอนหนึ่ง เป็นการพิสูจน์ว่าระบบงานที่ออกแบบสามารถทำงานได้ตรงตามวัตถุประสงค์หรือไม่ จึงจำเป็นต้องกำหนดมาตรฐานในการทดสอบมีหลายวิธีซึ่งสามารถเลือกใช้ได้ตามความเหมาะสม เช่นอาจดำเนินการดังนี้

- (1) ทดสอบประมวผลด้วยระบบงานควบคู่กับระบบงานเก่าที่ใช้อยู่เดิม (Parallel test)
- (2) มอบหมายให้ผู้ใช้ข้อมูลและผู้ที่เกี่ยวข้องกับการปฏิบัติงานจริงในระบบใหม่เป็นผู้ตรวจสอบผล

การทดสอบ

(3) ควรใช้ข้อมูลชุดสำรองในการทดสอบ และไม่ควรนำ live data file มาใช้ทดสอบเพื่อป้องกันการแก้ไขเปลี่ยนแปลงหรือถูกทำลาย

- (4) สร้างข้อมูลเลียนแบบของจริงสำหรับการทดสอบ

(5) ทดสอบการแก้ไขโปรแกรมโดยละเอียด เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นกับคำสั่งอื่นภายในโปรแกรมเดียวกัน หรือโปรแกรมอื่นที่สัมพันธ์กัน

3.7 มาตรฐานการนำระบบงานใหม่ออกใช้งาน

เพื่อให้แน่ใจว่าระบบงานใหม่สามารถประมวผลได้จริงตามความต้องการ จึงควรมีมาตรฐานในการนำระบบงานใหม่ออกใช้งานดังนี้

- (1) กำหนดให้ผู้ใช้ข้อมูลลงนามรับรองหรืออนุมัติให้ใช้ระบบงานใหม่ได้หลังจากที่ได้ทดสอบการทำงานจนเป็นที่พอใจแล้ว

(2) กำหนดให้ผู้ใช้อุปกรณ์ computer operator และผู้ที่เกี่ยวข้องกับการปฏิบัติงานในระบบงานใหม่ ทดสอบการใช้คู่มือปฏิบัติงานจนแน่ใจว่าจะใช้งานได้จริง

(3) ฝึกอบรมการปฏิบัติงานของบุคคลที่กล่าวตามข้อ (2) ให้สามารถปฏิบัติงานแก้ปัญหาที่อาจเกิดขึ้นได้

(4) เอกสารสนับสนุนการปฏิบัติงานต้องเสร็จสมบูรณ์ก่อนนำระบบงานออกใช้

3.8 การตรวจสอบผลการนำระบบงานใหม่ออกใช้งาน

หลังจากนำระบบงานใหม่ออกใช้งานไปแล้ว 1-6 เดือน ควรดำเนินการตรวจสอบผลการปฏิบัติงาน เพื่อประเมินผลและวัดความสำเร็จของโครงการ เพื่อจัดรายงานเสนอฝ่ายบริหารในเรื่องต่าง ๆ ดังต่อไปนี้

(1) เปรียบเทียบระยะเวลาและค่าใช้จ่ายตามที่กำหนดไว้ในโครงการกับระยะเวลาและค่าใช้จ่ายที่เกิดขึ้นจริง

(2) ผลการปฏิบัติงานบรรลุวัตถุประสงค์ที่วางไว้หรือไม่

(3) ความประหยัดจากการใช้ระบบงานใหม่

(4) ปัญหาในการปฏิบัติงาน

(5) ผลตอบแทนที่ได้รับจากระบบงานใหม่ที่ไม่เป็นตัวเงิน

3.9 การรักษาความปลอดภัยเกี่ยวกับ Operating Systems

เนื่องจาก operating systems หรือ supervisor programs มีความสำคัญยิ่งต่อการควบคุมการทำงานในระบบคอมพิวเตอร์ จึงควรจัดให้มีการรักษาความปลอดภัยที่รัดกุม เช่น

(1) ห้ามนำชุดคำสั่งพิเศษที่มีไว้สำหรับพนักงานชั้นบริหาร (privileged instructions) มาใช้ในการประมวลผลงานทั่วไป

(2) มีวิธีการป้องกันมิให้ application program รุกล้ำเข้าไปถึงส่วนที่เป็น supervisor เพราะอาจทำให้ควบคุมดูแลรักษาความปลอดภัยไม่ทั่วถึง เว้นแต่ supervisor program จะเรียกไปใช้เองเท่านั้น

(3) มีมาตรการป้องกัน user program มิให้อ่านข้อมูลที่อยู่ในส่วนที่เป็น supervisor เพราะผู้ใช้คอมพิวเตอร์อาจนำข้อมูลที่ทราบในส่วนนี้ให้เป็นประโยชน์ต่อการใช้รหัสลับ (password) หรือหลีกเลี่ยงระบบรักษาความปลอดภัย

(4) ในช่วงเวลาที่ปฏิบัติงานตามปกติ ควรห้ามแก้ไข supervisor program

(5) มีการแบ่งแยกหน้าที่ระหว่าง system programmer และ application programmer อย่างชัดเจน

(6) ควรห้าม system programmer มีส่วนรู้เห็นหรือปฏิบัติงานเกี่ยวกับ

(6.1) application program ส่วนที่จะมีผลกระทบต่อการควบคุมภายใน

(6.2) เอกสารเกี่ยวกับ application program

(7) ควรห้าม application programmer มีส่วนรู้เห็นหรือปฏิบัติงานเกี่ยวกับ

(7.1) operating system ส่วนที่จะมีผลกระทบต่อการควบคุมภายใน

(7.2) เอกสารที่เกี่ยวกับ operating system

(7.3) แฟ้มข้อมูลที่ใช้อยู่ในปัจจุบัน

(8) ควรห้าม system programmer และ application programmer เข้าไปใช้เครื่องในห้องคอมพิวเตอร์และ library file

3.10 การควบคุมการปฏิบัติงานของ Application Programmer

ควรจัดให้มีการควบคุมดูแลการปฏิบัติงานของ application programmer โดยใกล้ชิด ดังนี้

(1) มีการมอบหมายงานพัฒนาหรือแก้ไข application program ให้แก่ผู้เขียนโปรแกรมแต่ละคนรับผิดชอบเป็นส่วน ๆ ไป และห้ามบุคคลอื่นเข้าไปรู้เห็นหรือช่วยปฏิบัติงานในส่วนที่ตนไม่ได้รับมอบหมาย

(2) หากผู้เขียนโปรแกรมได้รับมอบหมายให้ใช้ low level language เช่น Assembler ในการเขียนโปรแกรม ควรห้ามใช้คำสั่งเกี่ยวกับ operating system

(3) ควรห้ามผู้เขียนโปรแกรมใช้คำสั่งเกี่ยวกับ storage dump หากจำเป็นต้องใช้ควรกำหนดตัวผู้รับผิดชอบ ควรทำลาย storage dump listing และ program source listing ทันทีที่เลิกใช้

3.11 การรักษาความปลอดภัยเกี่ยวกับโปรแกรมที่ใช้ประมวลผล

สถาบันการเงินควรมีระเบียบปฏิบัติงานในด้านต่าง ๆ เป็นเครื่องมือในการควบคุมเพื่อประโยชน์ในการรักษาความปลอดภัยเกี่ยวกับโปรแกรมที่ใช้ประมวลผล ดังนี้

(1) ควบคุมการใช้โปรแกรม เครื่องมือ และอุปกรณ์ประมวลผล เช่น

(1.1) Application programs

(1.2) Operating systems programs

(1.3) Utility programs

(1.4) Data files

(1.5) Documentation

(1.6) Computer equipment

(2) มีการตรวจสอบรายงานที่ใช้ควบคุมการปฏิบัติงาน เช่น computer operation logs, time records, console sheet และรายงานอื่น ๆ ที่เป็นประโยชน์ต่อการควบคุมเป็นประจำ

(3) มี utility program ควบคุมการใช้โปรแกรมสั่งงานที่เก็บไว้ใน library และช่วยจัดทำ activity logs บันทึกการใช้ library ไปด้วย

(4) ควบคุมการใช้ system utility program ในการปฏิบัติงานด้านการพัฒนาโปรแกรมปรับปรุงแก้ไขโปรแกรม การ catalog โปรแกรม อย่างรัดกุม

(5) ควบคุมการใช้ password ที่อาจเป็นอันตรายต่อโปรแกรมที่ใช้ประมวลผล มิให้รั่วไหลไปสู่บุคคลอื่นที่ไม่ได้รับมอบหมาย

3.12 การควบคุมการปรับปรุงแก้ไขโปรแกรม

การปรับปรุงที่ใช้ประมวผล ควรจัดให้มีการควบคุมดังนี้

- (1) กำหนดให้ผู้ที่จะปรับปรุงแก้ไขโปรแกรมต้องยื่นใบคำขอปรับปรุงแก้ไขโปรแกรม เพื่อขออนุมัติจากพนักงานชั้นบริหารที่ได้รับมอบหมายในการปรับปรุงแก้ไขโปรแกรมทุกครั้ง
- (2) จัดทำทะเบียนบันทึกรายละเอียดการปรับปรุงแก้ไขโปรแกรม เพื่อใช้ควบคุมดูแลและติดตามผลการปฏิบัติงาน
- (3) จัดให้มีการทดสอบโปรแกรมที่มีการปรับปรุงและดำเนินการเช่นเดียวกับการนำระบบงานและโปรแกรมใหม่ออกใช้งาน
- (4) พนักงานชั้นบริหารที่ได้รับมอบหมายให้รับผิดชอบควบคุมดูแลการปรับปรุงแก้ไขโปรแกรมควรตรวจสอบการปรับปรุงแก้ไขโปรแกรมโดยละเอียด เพื่อป้องกันความเสียหายและผลกระทบต่อโปรแกรมอื่นที่มีได้แก้ไข นอกจากนี้ยังเป็นการป้องกันปรับปรุงแก้ไขโปรแกรมนอกเหนือไปจากใบขออนุมัติด้วย
- (5) หาก system programmer ต้องการปรับปรุงแก้ไข operating system ให้ดำเนินการเช่นเดียวกับ application programmer
- (6) ให้ปรับปรุงแก้ไขเอกสารสนับสนุนการปฏิบัติงาน (documentation) ในส่วนที่เกี่ยวข้องกับการปรับปรุงแก้ไขโปรแกรมให้เรียบร้อยพร้อมๆ กัน
- (7) ผู้ตรวจสอบภายในควรควบคุมดูแลการปรับปรุงแก้ไขโปรแกรมโดยใกล้ชิดทุกขั้นตอน

3.13 การควบคุมการปรับปรุงแก้ไขโปรแกรมในกรณีเร่งด่วนเป็นการชั่วคราว

ในบางครั้งอาจจำเป็นต้องปรับปรุงแก้ไขโปรแกรมอย่างเร่งด่วน เพื่อแก้ปัญหาเฉพาะหน้าไม่สามารถที่จะปฏิบัติตามกระบวนการปรับปรุงแก้ไขโปรแกรมตามที่กล่าวไว้ข้างต้นได้ จึงควรนำวิธีการควบคุมดังต่อไปนี้มาใช้ทดแทน

- (1) ควรกำหนดว่าจะสามารถปรับปรุงแก้ไขโปรแกรมอย่างเร่งด่วนเป็นการชั่วคราวได้ในกรณีใดบ้าง
- (2) มอบหมายให้พนักงานชั้นบริหารที่รับผิดชอบในการควบคุมดูแลการปรับปรุงแก้ไขโปรแกรมตรวจสอบคำสั่งที่มีการแก้ไขโดยละเอียด
- (3) ให้จัดทำรายงานการปรับปรุงแก้ไขโปรแกรมในกรณีนี้เสนอต่อพนักงานชั้นบริหารที่รับผิดชอบให้ทราบโดยละเอียดทันที
- (4) หลังจากการปรับปรุงแก้ไขโปรแกรมในกรณีเร่งด่วนเป็นการชั่วคราว เพื่อแก้ปัญหาเฉพาะหน้าเสร็จเรียบร้อยแล้ว ให้ทบทวนและดำเนินการปรับปรุงแก้ไขโปรแกรกดังกล่าวใหม่ตามกระบวนการปรับปรุงแก้ไขโปรแกรมตามปกติ
- (5) ควรห้ามใช้วิธีแก้ไข object program โดยตรง หรือแก้ไขผ่านทาง console ทั้งนี้เพราะวิธีการแก้ไขดังกล่าวจะไม่ปรากฏร่องรอยของการแก้ไขให้ตรวจสอบ

3.14 การตรวจสอบมาตรฐานของระบบงาน

วัตถุประสงค์

1. เพื่อตรวจสอบการควบคุมโดยทั่วไป (General Controls) ในด้านระบบงานที่จะมีผลกระทบต่อความถูกต้องของรายการทางการเงิน
2. เพื่อตรวจสอบมาตรฐานของระบบงานที่จะใช้เป็นแหล่งอ้างอิง สำหรับการพัฒนาระบบงานใหม่ การบำรุงรักษา หรือการปรับปรุงระบบงานคอมพิวเตอร์ให้ดีขึ้น
3. เพื่อประเมินความเหมาะสม วัตถุประสงค์ของระบบงาน และการตัดสินใจในระดับนโยบายของสถาบันการเงิน
4. เพื่อประเมินว่าวิธีปฏิบัติของสถาบันการเงินได้ดำเนินการอย่างสอดคล้องกับมาตรฐานที่วางไว้เป็นลายลักษณ์อักษรและดูแลให้มีการปฏิบัติที่ผิดแผกไปจากมาตรฐานที่กำหนดไว้

แผนงานการตรวจสอบโดยย่อ

1. คู่มือระเบียบในการพัฒนาระบบงาน
2. โครงการที่สถาบันการเงินจะใช้คอมพิวเตอร์ประมวลผลในอนาคต
3. รายงานผลการปฏิบัติงานตามโครงการที่ใช้คอมพิวเตอร์
4. วิธีจัดหาหรือจัดซื้อ software package
5. คู่มือหรือระเบียบในการเขียนโปรแกรม
6. การทดสอบระบบงานและโปรแกรมเท่าที่เห็นสมควร
7. ระเบียบการนำระบบงานใหม่ออกใช้งาน และรายงานผลการนำระบบงานใหม่ออกใช้งาน
8. การควบคุมการปฏิบัติงานของผู้วิเคราะห์ระบบ (System Analyst) และผู้เขียนโปรแกรม
9. คู่มือหรือระเบียบการปรับปรุงแก้ไขระบบงานและโปรแกรมทั้งกรณีปกติและกรณีเร่งด่วน
10. การรักษาความปลอดภัยเกี่ยวกับระบบงานและโปรแกรมเท่าที่จำเป็น
11. เอกสารเกี่ยวกับระบบงานและโปรแกรมที่ใช้ประมวลผลบางประเภทที่จำเป็นต้องตรวจสอบ

Application Controls

4. เอกสารสนับสนุนการปฏิบัติงาน

เอกสารสนับสนุนการปฏิบัติงาน (documentation) ด้านคอมพิวเตอร์คือเอกสารที่บันทึกเรื่องราวเกี่ยวกับการประมวลผลด้วยคอมพิวเตอร์โดยละเอียด เป็นแหล่งให้ข้อมูลเบื้องต้นเกี่ยวกับระบบงานที่ใช้ประมวล ซึ่งจะประกอบขึ้นต่อการบริหารงาน การปฏิบัติงาน การบำรุงรักษา และการตรวจสอบ ดังนั้นเอกสารเหล่านี้จะต้องถูกต้อง ทันเวลาและสมบูรณ์อยู่เสมอ ระบบเอกสารที่ดีย่อมช่วยให้การควบคุมดูแล การเปลี่ยนแปลงระบบงาน การสับเปลี่ยนพนักงานและการมอบหมายหน้าที่ความรับผิดชอบทำได้ง่ายขึ้น ช่วยให้สามารถดำเนินงานต่อเนื่องกันโดยไม่หยุดชะงัก

ผู้บริหารควรมีส่วนร่วมอย่างแข็งขันในอันที่จะกำหนดมาตรฐานที่เหมาะสมในการจัดทำเอกสารสนับสนุนการปฏิบัติงาน ความสำเร็จในการจัดทำเอกสารขึ้นอยู่กับความเอาใจใส่ของผู้บริหารระดับสูงที่จะสั่งการและควบคุมให้มีการจัดทำเอกสารอันเป็นเครื่องมือที่จำเป็นต่อการบริหารงาน การปฏิบัติงาน การบำรุงรักษา และตรวจสอบ ทั้งโดยผู้ตรวจสอบภายในของสถาบันการเงินและผู้ตรวจสอบจากองค์กรที่มีหน้าที่กำกับและตรวจสอบสถาบันการเงิน

ระบบเอกสารสนับสนุนการปฏิบัติงานที่ดีอาจพิจารณาได้จาก

- 4.1 มาตรฐานการจัดทำเอกสารสนับสนุนการปฏิบัติงาน
- 4.2 คู่มือที่ใช้เป็นมาตรฐานในการปฏิบัติงานด้านคอมพิวเตอร์โดยทั่วไป
- 4.3 เอกสารสนับสนุนการปฏิบัติงานด้าน software
- 4.4 การควบคุมดูแลและการบำรุงรักษาเอกสาร
- 4.5 คู่มือสำหรับผู้ใช้อุปกรณ์
- 4.6 เอกสารสนับสนุนการปฏิบัติงานที่ประกอบมากับ software สำเร็จรูปที่สถาบันการเงินจัดหาหรือจัด

ซื้อมาใช้งาน

4.1 มาตรฐานการจัดทำเอกสารสนับสนุนการปฏิบัติงาน

สถาบันการเงินควรจัดให้มีคณะกรรมการหรือผู้รับผิดชอบในการกำหนดมาตรฐาน การควบคุมดูแล และตรวจสอบการจัดทำเอกสาร ตลอดจนการปรับปรุงแก้ไขเอกสารโดยใกล้ชิด สำหรับสถาบันการเงินที่ยังไม่มี มาตรฐานแน่นอน ควรศึกษาวิธีการจัดทำเอกสารสำหรับงานทั่ว ๆ ไปในสถาบันการเงิน และอาศัยการวิเคราะห์ สภาพแวดล้อมของระบบคอมพิวเตอร์ที่ใช้ประมวลผลและจัดรูปแบบของเอกสารตามความเหมาะสม

4.2 คู่มือที่ใช้เป็นมาตรฐานในการปฏิบัติงานด้านคอมพิวเตอร์โดยทั่วไป

คู่มือที่ใช้เป็นมาตรฐานในการปฏิบัติงานด้านคอมพิวเตอร์โดยทั่วไปจะเป็นแนวทางกว้าง ๆ เกี่ยวกับวิธีการออกแบบระบบงาน การเขียนโปรแกรม การจัดทำเอกสารประกอบโปรแกรม อุปกรณ์คอมพิวเตอร์ที่ใช้ประมวลผล การกำหนดนโยบายการบริหารบุคคลเพื่อประโยชน์ในการปฏิบัติงานประจำวัน และใช้เป็นเครื่องมือในการฝึกอบรมพนักงาน ใหม่

เนื้อหาและรูปแบบของคู่มือมาตรฐานการปฏิบัติงานขึ้นอยู่กับขนาดของระบบคอมพิวเตอร์ ระบบคอมพิวเตอร์ขนาดใหญ่อาจมีคู่มือหลายเล่ม โดยกำหนดเป็นเรื่องละหนึ่งเล่ม เช่น เรื่องการออกแบบระบบงาน (System design) เรื่องการเขียนโปรแกรมสั่งงาน (programming) เรื่องการจัดทำและการใช้เอกสาร (Documentation) และ เรื่องการปฏิบัติการ (Operation) ตัวอย่างเช่น คู่มือเรื่องที่เกี่ยวข้องกับมาตรฐานการปฏิบัติการอาจแยกเป็นหัวข้อย่อยตามส่วนงานได้อีก เช่น แผนกจัดทำข้อมูลป้อนเข้าคอมพิวเตอร์ (input) แผนกควบคุมตารางการประมวลผล (Scheduling) แผนกรวบรวมข้อมูลที่ได้จากการประมวลผล (output) แผนกกระทบยอด (reconciliation) แผนกเจาะบัตร (keypunch) และแผนกควบคุมเครื่องคอมพิวเตอร์ สำหรับระบบคอมพิวเตอร์ขนาดเล็กอาจรวมวิธีการปฏิบัติงานของแผนกงานดังกล่าวไว้เป็นเล่มเดียวกันก็ได้ อย่างไรก็ตามทุกหน่วยงานควรกำหนดวิธีการปฏิบัติงานไว้ในคู่มือและรวบรวมไว้ในระเบียบปฏิบัติงานเพื่อแสดงโครงสร้างและการควบคุม

นอกจากนี้ ควรมีคู่มือที่ใช้เป็นแนวทางในการพัฒนางานและคู่มือการจัดเก็บรักษาเอกสารที่ใช้ในการจัดทำโปรแกรมสั่งงานด้วย

4.3 เอกสารสนับสนุนการปฏิบัติงานด้าน software

เอกสารสนับสนุนการปฏิบัติงานด้าน software ที่ใช้ประมวลผล ควรประกอบด้วย

4.3.1 ปัญหาและอุปสรรคในการปฏิบัติงาน (Problem definition) ควรแสดงรายละเอียดเกี่ยวกับการปฏิบัติงานตามโครงการ ปัญหาและอุปสรรคในการปฏิบัติงานวิธีการและเหตุผลในการแก้ปัญหา โดยอาจแบ่งเรื่องเป็นส่วน ๆ เช่น เบื้องหลังการเสนอโครงการ รายงานการประชุมคณะกรรมการบริหารงานด้านคอมพิวเตอร์เกี่ยวกับการพิจารณาโครงการ ปัญหาทางด้านโปรแกรมที่ใช้ประมวล ค่าใช้จ่ายของโครงการตามประมาณการเปรียบเทียบกับค่าใช้จ่ายที่เกิดขึ้นจริง จำนวนชั่วโมงแรงงานตามประมาณการเปรียบเทียบกับจำนวนชั่วโมงแรงงานที่ใช้จริง และหลักเกณฑ์ที่ใช้ในการตัดสินใจ เป็นต้น

4.3.2 รายละเอียดเกี่ยวกับระบบงาน (Application system description) ควรแสดงรายละเอียดเกี่ยวกับระบบงานและความสัมพันธ์ของโปรแกรมต่าง ๆ ภายในระบบงานประกอบด้วย

(1) ผังแสดงระบบงาน (System flowchart) เป็นผังแสดงแหล่งที่มาและลักษณะของข้อมูลที่ใช้ประมวล เครื่องจักรและอุปกรณ์ที่ใช้ประมวลผล ขั้นตอนการปฏิบัติงาน โปรแกรมที่ใช้ในระบบงาน ผู้ใช้ข้อมูลและลักษณะของข้อมูลที่ได้จากการประมวลผล

(2) คำอธิบายเกี่ยวกับระบบงาน (System narrative) อธิบายลักษณะทั่ว ๆ ไปของระบบงาน โปรแกรมที่ใช้ประมวลผล วิธีปฏิบัติงาน ผู้ใช้ข้อมูลและความสัมพันธ์ของระบบงานที่มีต่อหน่วยงานอื่น

(3) ผังแสดงลักษณะการบันทึกข้อมูล (Record layout schmeatics) แสดงรูปแบบในการบันทึกข้อมูลลงใน media ต่าง ๆ เช่น card, magnetic tape, paper tape และ disk ชนิดต่าง ๆ ฯลฯ

(4) ลักษณะของรายงานที่ได้จากการประมวล (Print layouts) แสดงรูปของข้อมูลที่ปรากฏในรายงานที่ได้จากการประมวลผล เช่น การพิมพ์หัวรายงาน การจัดคอลัมน์ข้อมูล การออกยอด การเว้นบรรทัด เป็นต้น

(5) รายละเอียดเกี่ยวกับแฟ้มข้อมูล (File description) อธิบายลักษณะของ record ที่เก็บไว้ในแฟ้มข้อมูล (file) และอาจมีข้อกำหนดให้ผู้ใช้งานแฟ้มข้อมูลต้องปฏิบัติก่อน/หลังการใช้แฟ้มข้อมูลด้วย

(6) รหัสพิเศษ (Special codes) อธิบายความหมายของรหัสต่าง ๆ เช่น ประเภทของรายการ ประเภทบัญชี ฯลฯ

(7) การควบคุมดูแล (Control functions) อธิบายวิธีการควบคุมทั้งด้านบัญชีและด้านปฏิบัติการการรักษาความปลอดภัย รายชื่อพนักงานที่ได้รับมอบอำนาจให้ใช้ข้อมูล ฯลฯ

4.3.3 รายละเอียดเกี่ยวกับโปรแกรม (Program description) เป็นรายละเอียดเกี่ยวกับโปรแกรมที่ใช้ประมวลผล ประกอบด้วย

(1) ผังแสดงขั้นตอนในการประมวลผลของโปรแกรม (Program flowcharts) เป็นผังแสดง logic ขั้นตอนการทำงานของโปรแกรม และ subroutine หรือ module ที่ใช้ร่วมกับโปรแกรมหลัก

(2) ตารางแสดงการตัดสินใจ (Decision tables) อาจใช้แทน flowchart หรือใช้เป็นส่วนประกอบของ flowchart ในกรณีที่โปรแกรมมีความยุ่งยากและสลับซับซ้อน เพื่อแสดงขั้นตอนการตัดสินใจให้สัมพันธ์กับกฎเกณฑ์หรือเงื่อนไขที่ผู้ใช้ข้อมูลกำหนดไว้ นอกจากนี้ Decision table ยังใช้เป็นประโยชน์ในการเตรียมข้อมูลเพื่อการทดสอบ (Test data) ระบบงานด้วย

(3) รายละเอียดของตารางข้อมูล (Table descriptions) อธิบายรายละเอียดของข้อมูลที่เก็บไว้ใน table เพื่อให้โปรแกรมต่าง ๆ นำไปใช้อ้างอิง ซึ่งเป็นส่วนสำคัญของ program documentation

(4) คำอธิบาย Flags และ Switches เป็นรายละเอียดอธิบายการทดสอบ condition ต่าง ๆ ภายในโปรแกรม เพื่อเลือกวิธีการประมวลผลอย่างใดอย่างหนึ่งสุดแล้วแต่ instruction หรือ logic ของโปรแกรมที่กำหนดไว้

(5) รายละเอียดในการปรับปรุงแก้ไขระบบงานและโปรแกรม (Program change and system modification forms) อธิบายการปรับปรุงแก้ไข application program, application system, operating system รวมทั้งผลดีและผลเสียของการปรับปรุงแก้ไขดังกล่าว และควรกล่าวถึงอำนาจในการปฏิบัติการปรับปรุงแก้ไขระบบงานและโปรแกรมไว้ด้วย

(6) รายละเอียดของโปรแกรม (Program listing) เป็นเอกสารหลักของ program documentation ซึ่งควรมีรายละเอียดให้ครบถ้วน รวมทั้งข้อสังเกตที่จะช่วยให้เข้าใจโปรแกรมได้ง่าย และความหมายของ data name ในกรณีที่มีการแก้ไขโปรแกรมจะต้องแก้ไข program listing ด้วย

(7) รายละเอียดเกี่ยวกับโปรแกรมที่ใช้ควบคุมและตรวจสอบความถูกต้องของข้อมูล (Programmed Controls) เป็นรายละเอียดที่อธิบายวิธีการตรวจสอบความถูกต้องข้อมูลของโปรแกรมต่าง ๆ ที่ใช้ในการ edit

4.3.4 รายละเอียดในการปฏิบัติงานของ Operator (Operator instructions) อธิบายวิธีปฏิบัติงานของ operator โดยละเอียดทุกงาน หน้าที่ความรับผิดชอบของ operator วิธีปฏิบัติในกรณีเครื่องหยุดทำงานโดยกะทันหัน เอกสารชุดนี้จะต้องไม่มีรายละเอียดที่เกี่ยวกับโปรแกรมที่ใช้ประมวลผล เช่น source listings, record layouts และ program flowcharts เข้ามาปะปน เพราะอาจเป็นอันตรายต่อการรักษาความปลอดภัย แต่ควรมีรายละเอียดเพียงพอที่จะช่วยให้ operator ที่ผ่านงานมาพอสมควรสามารถใช้เป็นคู่มือปฏิบัติงานได้โดยไม่ติดขัดและไม่ต้องอาศัยผู้อื่นมาช่วยแนะนำ

4.3.5 บันทึกการรับรองหรือการอนุมัติให้ใช้ระบบงานประมวลผล (Record of acceptance) เป็นหลักฐานแสดงรายละเอียดการตรวจรับระบบงานทุกขั้นตอน จากหน่วยงานต่าง ๆ ของสถาบันการเงินดังนี้

(1) ผู้ใช้ข้อมูล (User department) ควรมีหลักฐานแสดงการตรวจสอบผลงานที่ได้จากการทดลองประมวลผลของระบบงานที่นำมาใช้นั้น ได้ผลลัพธ์ถูกต้องตามที่กำหนดไว้

(2) ผู้บริหารศูนย์คอมพิวเตอร์ (EDP department management) ควรมีหลักฐานแสดงว่าระบบงานดังกล่าวได้จัดทำขึ้นตามมาตรฐานที่สถาบันการเงินกำหนดไว้

(3) ผู้ตรวจสอบ (Audit department) ควรมีหลักฐานแสดงการทดสอบระบบงานและแสดงว่าได้ตรวจสอบวิธีการควบคุมต่างๆ จนพอใจแล้ว

(4) ผู้ปฏิบัติงานประมวล (EDP operations) ควรมีหลักฐานแสดงผลการใช้คู่มือทดลองปฏิบัติงาน ความเพียงพอของเครื่องจักรและอุปกรณ์ที่จะใช้งานและการสำรองเวลาเครื่องคอมพิวเตอร์ที่จะใช้ประมวลผล

(5) บรรณารักษ์ผู้ควบคุมดูแลรักษาเอกสารสนับสนุนการปฏิบัติงาน (Documentation Librarian Function) ควรมีหลักฐานการตรวจสอบเอกสารต่าง ๆ ให้สมบูรณ์และเรียบเรียงตามมาตรฐานที่กำหนดไว้

4.4 การควบคุมดูแลและการบำรุงรักษาเอกสาร

บรรณารักษ์ (Documentation Librarian) จะเป็นผู้รับผิดชอบในการควบคุม เก็บรักษา และแจกจ่ายเอกสาร ซึ่งมีวิธีปฏิบัติแตกต่างกันสุดแล้วแต่ขนาดความซับซ้อนของการประมวลผลด้วยระบบคอมพิวเตอร์ของสถาบันการเงินแต่ละแห่ง

การควบคุมดูแลและการบำรุงรักษาเอกสาร ควรดำเนินการดังนี้

4.4.1 จัดให้มีบรรณารักษ์เป็นผู้รับผิดชอบในการควบคุมดูแล บำรุงรักษาเอกสาร โดยมีหน้าที่

- (1) ตรวจทานความเรียบร้อยของเอกสารในระหว่างที่มีการพัฒนาระบบงาน
- (2) ควบคุมและเก็บรักษาเอกสาร
- (3) ปรับปรุงแก้ไขเอกสาร
- (4) ติดต่อและจัดส่งเอกสารให้กับผู้ที่ได้รับอนุญาตให้ใช้เอกสาร
- (5) ควบคุมการจัดทำเอกสารให้ได้มาตรฐาน

4.4.2 จัดให้มีระเบียบการใช้เอกสาร และกำหนดตัวผู้ที่ได้รับอนุญาตให้ใช้เอกสารบางประเภท

4.4.3 ควรปรับปรุงแก้ไขเอกสารให้ถูกต้องและทันเวลาอยู่เสมอ

4.4.4 มีสำเนาเอกสารสำรองเก็บรักษาไว้ที่อื่น และมีการปรับปรุงแก้ไขเอกสารชุดสำเนานี้ให้ถูกต้องทันเวลา เช่นเดียวกับเอกสารชุดที่ใช้งานอยู่เสมอ

4.5 คู่มือสำหรับผู้ใช้ข้อมูล

สถาบันควรจัดทำคู่มือสำหรับผู้ใช้ข้อมูล เพื่อช่วยให้ผู้ใช้ข้อมูลเข้าใจ เชื่อถือยอมรับระบบงาน และให้ความร่วมมือปฏิบัติงาน นอกจากนี้ยังเป็นการป้องกันความเสียหายที่อาจเกิดจากผู้ใช้อุปกรณ์การแก้ปัญหาด้วยตนเอง หรือผู้ใช้อาจเข้าใจข้อมูลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์จนเกินไป ทำให้ละเลยไม่ตรวจสอบข้อมูลบางชนิดที่จำเป็นต้องตรวจสอบก่อนนำไปใช้

คู่มือสำหรับผู้ใช้ข้อมูลแบ่งออกเป็น 2 ตอน คือ ตอนที่ว่าด้วยข้อมูลที่ใช้ในการประมวลผล (input) และข้อมูลที่ได้จากการประมวลผล (output) ถ้อยคำที่ใช้ในคู่มือดังกล่าวจะต้องเป็นภาษาที่เข้าใจง่าย ควรมีภาพประกอบแสดงวิธีการออกแบบฟอร์มต่าง ๆ และมีวิธีปฏิบัติงานทุกขั้นตอนโดยละเอียด นอกจากนี้ควรตรวจสอบการใช้รายงานที่ได้จากการประมวลผลเป็นครั้งคราว เพื่อดูว่ามีการนำไปใช้ประโยชน์ตามวัตถุประสงค์หรือไม่

4.6 เอกสารสนับสนุนการปฏิบัติงานที่ประกอบมากับ software สำเร็จรูปที่สถาบันการเงินจัดหาหรือซื้อมาใช้งาน

ในกรณีที่สถาบันการเงินจัดหาหรือซื้อ software จากภายนอกมาใช้โดยไม่จัดทำขึ้นเอง ควรพิจารณาเอกสารสนับสนุนการปฏิบัติงานที่ประกอบมามีรายละเอียดสมบูรณ์เพียงพอและเป็นไปตามมาตรฐานที่กำหนดไว้หรือไม่ โดยดำเนินการตรวจสอบเอกสารเหล่านี้ก่อนที่จะซื้อหรือเช่ามาใช้ เพื่อให้แน่ใจว่า software ที่จะนำมาใช้สามารถใช้กับระบบคอมพิวเตอร์ของสถาบันการเงินได้

4.7 การตรวจสอบ เอกสารสนับสนุนการปฏิบัติงาน

วัตถุประสงค์

1. เพื่อประเมินความเหมาะสมและความเพียงพอในการจัดทำเอกสารสนับสนุนการปฏิบัติงาน การรักษาความปลอดภัยเกี่ยวกับเอกสารของสถาบันการเงินและเพื่อความสะดวก ประหยัดเวลาในการปฏิบัติงานการตรวจสอบ สำหรับผู้ที่เกี่ยวข้องทุกฝ่าย

2. เพื่อให้ผู้ตรวจสอบ ได้ข้อมูลเบื้องต้นเกี่ยวกับงานประมวลผลด้วยคอมพิวเตอร์ในด้านต่าง ๆ ของสถาบันการเงิน ซึ่งสามารถใช้เป็นแนวทางในการตรวจสอบและประเมินบทบาทของฝ่ายบริหาร มาตรฐานการปฏิบัติงานประมวลผล การควบคุมโดยทั่วไปของสถาบันการเงิน ซึ่งเป็นพื้นฐานขั้นต้นของการตรวจสอบด้านคอมพิวเตอร์

แผนงานการตรวจสอบโดยย่อ

1. คู่มือหรือระเบียบการจัดทำเอกสารสนับสนุนการปฏิบัติงาน
2. คู่มือหรือระเบียบเกี่ยวกับมาตรฐานการปฏิบัติงานในระบบคอมพิวเตอร์โดยทั่วไป
3. เอกสารสนับสนุนการปฏิบัติงานด้าน software บางประเภทที่จำเป็นต้องตรวจสอบเกี่ยวกับการควบคุมทั่วไป (General Controls) และการควบคุมเฉพาะงานในแต่ละด้าน (Application Controls)
4. คู่มือหรือระเบียบสำหรับผู้ใช้อุปกรณ์ (User Manuals)
5. การควบคุม การเก็บรักษา และมาตรการรักษาความปลอดภัยเกี่ยวกับเอกสาร สนับสนุนการปฏิบัติงาน

5. การปฏิบัติงานคอมพิวเตอร์

แผนกปฏิบัติการคอมพิวเตอร์ของสถาบันการเงินควรทำงานด้วยความรวดเร็วและมีประสิทธิภาพมีการป้องกันแฟ้มข้อมูล โปรแกรม เครื่องมือและอุปกรณ์ต่างๆ มิให้เสียหายเจ้าหน้าที่ที่ทำงานในห้องเครื่องคอมพิวเตอร์จะต้องได้รับมอบหมายให้รับผิดชอบเฉพาะงานที่เกี่ยวกับการใช้เครื่องคอมพิวเตอร์เท่านั้นมิให้เข้าไปก้าวก่ายหน้าที่อื่นๆ เช่น การเตรียมข้อมูล การจัดทำโปรแกรม การตรวจสอบข้อมูลที่ได้จากการประมวลผลหรือหน้าที่อื่น ๆ ในทำนองนี้

เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์จะปฏิบัติงานได้ผลเต็มที่ หากมีคู่มือการปฏิบัติงาน อธิบายวิธีใช้เครื่องคอมพิวเตอร์ โปรแกรมและอุปกรณ์ต่าง ๆ โดยละเอียดทุกงาน คู่มือนี้ควรถูกต้องสามารถใช้ปฏิบัติงานได้จริงและมีการปรับปรุงแก้ไขให้ทันเวลาอยู่เสมอ และควรมีรายละเอียดดังนี้

5.1 การรักษาความสะอาดภายในห้องคอมพิวเตอร์

ควรมีระเบียบการรักษาความสะอาดในห้องคอมพิวเตอร์ กำหนดให้เจ้าหน้าที่ปฏิบัติการภายในห้องคอมพิวเตอร์ถือปฏิบัติโดยเคร่งครัด เพื่อป้องกันความเสียหายแก่เครื่องคอมพิวเตอร์ อุปกรณ์และเครื่องมืออื่น ๆ

5.2 การบำรุงรักษาเครื่องคอมพิวเตอร์

เพื่อให้เครื่องคอมพิวเตอร์เสื่อมสภาพเร็วกว่าที่ควรและสามารถทำงานได้ โดยไม่มีข้อบกพร่องควรกำหนดให้เจ้าหน้าที่ปฏิบัติการภายในห้องคอมพิวเตอร์ทำความสะอาดเครื่องตามกำหนดเวลาและวิธีการที่บริษัทผู้ผลิตคอมพิวเตอร์กำหนดมาให้ถือปฏิบัติ และจัดเวลาให้บริษัทผู้ให้เช่าเครื่องหรือผู้ขายดำเนินการบำรุงรักษาเครื่องเสมอ

5.3 การแบ่งแยกและสับเปลี่ยนหน้าที่

เพื่อประโยชน์ในการควบคุมภายใน ผู้บริหารงานด้านคอมพิวเตอร์ควรมีนโยบายและวิธีการในการแบ่งแยกและสับเปลี่ยนหน้าที่พนักงาน รวมทั้งการฝึกอบรมให้พนักงานมีความรู้ความชำนาญหลาย ๆ ด้านตามความเหมาะสม

5.4 การใช้เครื่องคอมพิวเตอร์ในการประมวลผล

ในการใช้เครื่องคอมพิวเตอร์ควรมีคู่มือจากบริษัทผู้ผลิตคอมพิวเตอร์และคำสั่งในการปฏิบัติงาน (Operation Instructions) เป็นหลักในการปฏิบัติงาน คู่มือเหล่านี้จะต้องถูกต้อง ทันเวลาและสามารถหยิบใช้ได้ทันที นอกจากนี้ควรมอบหมายให้เจ้าหน้าที่ปฏิบัติการระดับหัวหน้างานเป็นผู้บันทึกการปฏิบัติงานของเจ้าหน้าที่ปฏิบัติการเพื่อจัดทำรายงานเสนอผู้บริหารให้ตรวจสอบทุกวัน

5.5 การจัดทำตารางการใช้เครื่องคอมพิวเตอร์

เพื่อให้การใช้เครื่องคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ควรจัดทำตารางการใช้เครื่องคอมพิวเตอร์กำหนดไว้ให้แน่นอน หากศูนย์คอมพิวเตอร์มีขนาดใหญ่และซับซ้อน อาจใช้โปรแกรมสำหรับกำหนดตารางการทำงานโดยอัตโนมัติ หากมีการใช้เครื่อง run งานพิเศษที่มีได้กำหนดไว้ในตารางฯ เช่น งานทดสอบโปรแกรมควรจัดทำใบคำขอหรือหนังสือขออนุมัติต่อผู้บริหารที่มีหน้าที่รับผิดชอบก่อนดำเนินการ

5.6 การควบคุมการใช้เครื่องคอมพิวเตอร์

สถาบันการเงินควรมีมาตรการควบคุมการใช้เครื่องคอมพิวเตอร์เพื่อป้องกันหรือตรวจสอบการใช้โปรแกรมและการใช้เครื่องคอมพิวเตอร์โดยมิได้รับอนุญาต โดยอาศัยเครื่องมือต่าง ๆ เช่น Console printer, CPU-Clock, Activity logs เป็นต้น

5.7 การควบคุมการปฏิบัติงานของเจ้าหน้าที่ปฏิบัติการในห้องคอมพิวเตอร์

เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์เป็นผู้ที่นำโปรแกรมและข้อมูลเข้าคอมพิวเตอร์ ซึ่งเป็นขั้นตอนที่สำคัญของการประมวลผล จึงควรกำหนดขอบเขตการปฏิบัติงานของเจ้าหน้าที่ปฏิบัติการ เพื่อประโยชน์ในการรักษาความปลอดภัยและการควบคุมภายใน โดยจัดให้มีการควบคุมเจ้าหน้าที่ปฏิบัติการในการใช้ข้อมูลและโปรแกรมโดยใกล้ชิด มิให้ไปปฏิบัติงานหน้าที่อื่นที่เป็นอันตรายต่อการประมวลผล เช่น การตรวจสอบความถูกต้องของยอดรวมข้อมูลและเข้าไปยุ่งเกี่ยวกับ Source Program หรือ Program Listing รวมทั้งเอกสารอื่นที่ไม่เกี่ยวกับการใช้เครื่อง

5.8 การควบคุม Library

เพื่อป้องกันการใช้แฟ้มข้อมูล โปรแกรม และเอกสารสนับสนุนการปฏิบัติงานโดยมิได้รับอนุญาต ควรมี library จัดเก็บ ข้อมูล โปรแกรม และเอกสารแยกต่างหากจากห้องคอมพิวเตอร์ โดยมีระบบควบคุมและรักษาความปลอดภัยที่รัดกุม นอกจากนี้สถาบันการเงินอาจใช้ software package ควบคุม library ควบคุมการใช้ข้อมูลและโปรแกรมอีกชั้นหนึ่ง หรืออาจใช้วิธีการควบคุมอื่นทดแทนได้ เช่น

- กำหนดให้มีเจ้าหน้าที่รับผิดชอบในการควบคุมและเก็บรักษา production library

- กำหนดวิธีการขออนุมัติแก้ไขโปรแกรม
- ห้าม Operator ใช้ magnetic file เกินจำนวนที่จะใช้ปฏิบัติงาน
- ห้าม Operator นำโปรแกรมที่อยู่ระหว่างการทดสอบใน Test library ไปใช้ในเวลาที่มีการปฏิบัติงานจริงตามปกติ

5.9 การตรวจสอบ การปฏิบัติงานคอมพิวเตอร์ โดยผู้ตรวจการธนาคารพาณิชย์

วัตถุประสงค์

1. เพื่อประเมินผลการปฏิบัติงานของเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) ของสถาบัน การเงินมีความถูกต้อง และสมบูรณ์เพียงใด ข้อมูลที่ได้จากการปฏิบัติงานของเจ้าหน้าที่ดังกล่าวเชื่อถือได้เพียงใด

2. เพื่อตรวจสอบความเหมาะสมของการควบคุมการปฏิบัติงาน การบำรุงรักษาและมาตรการในการรักษาความปลอดภัยในห้องคอมพิวเตอร์ ซึ่งอาจมีผลกระทบต่อการประกอบธุรกิจสถาบันการเงิน

แผนงานการตรวจสอบโดยย่อ ผู้ตรวจการธนาคารพาณิชย์จะตรวจสอบและรวบรวมในเรื่องต่อไปนี้

1. รายละเอียดเกี่ยวกับเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ
2. เงื่อนไขและสัญญา การเช่าหรือซื้อเครื่องคอมพิวเตอร์และอุปกรณ์อื่น ๆ
3. คู่มือมาตรฐานการปฏิบัติงานของเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (standard manual for computer operation) และระเบียบปฏิบัติอื่น ๆ ที่กำหนดให้พนักงานดังกล่าวถือปฏิบัติ เช่น housekeeping, equipment maintenance scheduling, equipment operation และระเบียบการใช้ data and file library เป็นต้น
4. ตารางการใช้เครื่องคอมพิวเตอร์ (operating schedule) และรายงานการปฏิบัติงานคอมพิวเตอร์ที่เสนอต่อฝ่ายบริหาร
5. รายละเอียดเกี่ยวกับการใช้เครื่องคอมพิวเตอร์ที่บันทึกเก็บไว้ใน activity logs
6. รายชื่อผู้ที่ได้รับมอบหมายให้ปฏิบัติงานในห้องคอมพิวเตอร์ และการสับเปลี่ยนหน้าที่ของพนักงานเหล่านี้
7. รายงานการบำรุงรักษาและซ่อมแซมเครื่องคอมพิวเตอร์
8. การควบคุมภายในและมาตรการในการรักษาความปลอดภัยเกี่ยวกับการใช้เครื่องคอมพิวเตอร์

6. การจัดทำข้อมูลที่น่าเชื่อถือได้

วิธีการควบคุมการจัดทำข้อมูลที่ดีและเหมาะสม ทั้งในส่วนของผู้ใช้ข้อมูลและศูนย์คอมพิวเตอร์เป็นสิ่งที่ทำให้ข้อมูลมีความถูกต้องสมบูรณ์ และเชื่อถือได้ วิธีการควบคุมดังกล่าวอาจใช้ระบบอัตโนมัติหรือใช้พนักงานทำหน้าที่ในการควบคุม หรือใช้ทั้งสองวิธีร่วมกันก็ได้ การควบคุมควรกระทำทุกขั้นตอนนับตั้งแต่การเริ่มสร้างข้อมูล การประมวลผล จนถึงการจัดส่งรายงานที่ได้จากการประมวลผลไปยังผู้ใช้ข้อมูล

สถาบันการเงินควรดำเนินการควบคุมเพื่อให้ข้อมูลที่มีประมวลผลมีความสมบูรณ์ ถูกต้องและน่าเชื่อถือได้ วิธีการควบคุมต่อไปนี้เป็นเพียงลักษณะหนึ่งมิได้ครอบคลุมทุกกรณี ความเหมาะสมในการใช้จึงขึ้นกับสภาพของศูนย์ประมวลผลแต่ละแห่ง

6.1 งานขั้นต้นในการจัดทำและการจัดส่งข้อมูลเพื่อประมวลผล

(Transaction Initiation and Data Entry)Q

งานขั้นต้นในการจัดทำข้อมูลที่จะกล่าวต่อไปนี้จะแบ่งออกเป็น 2 ชนิด คือ ชนิดที่ใช้ MICR และชนิดที่ไม่ใช้ MICR (NON-MICR)

6.1.1 การจัดทำข้อมูลแบบ MICR (MICR Data Entry)

MICR (Magnetic Ink Character Recognition) คือ การกำหนดข้อความที่เป็นรหัสลงในแบบฟอร์มที่พิมพ์ไว้ล่วงหน้า และมีช่องเว้นไว้สำหรับให้กรอกจำนวนเงินในภายหลัง ตามแบบฟอร์มมาตรฐานที่ใช้กันทั่วไปในสถาบันการเงินที่ใช้คอมพิวเตอร์ในการประมวลผล โดยใช้เครื่อง proof machine กรอกจำนวนเงินเมื่อเกิดรายการขึ้นแล้ว และเพื่อให้เกิดความถูกต้องเชื่อถือได้ จึงมีการสรุปยอดเงินทั้งสิ้นที่ผ่านเครื่องให้ในตัว

วิธีการง่าย ๆ ที่ใช้ในการคุมยอดข้อมูลในระบบ MICR คือ การจัดเก็บแบบฟอร์มที่กรอกข้อมูลแล้วเป็นกลุ่ม ๆ เรียกว่า batch โดยให้แต่ละ batch ประกอบด้วยแบบฟอร์มประมาณ 150 แผ่น ถึง 300 แผ่น และเป็นที่น่าสังเกตว่าการจัดเก็บแบบฟอร์มข้อมูลดังกล่าวเป็น batch เล็ก ๆ จะช่วยให้เกิดความสะดวกในการปฏิบัติงานทั้งในด้านผู้ใช้อข้อมูลและพนักงานกระทบบยอดพิสูจน์ความถูกต้องของข้อมูลของศูนย์ประมวลผลด้วย

การจัดเก็บข้อมูลเป็น batch อาจทำได้หลายวิธีตามความต้องการของผู้ใช้ข้อมูล แต่ส่งไปยังศูนย์ประมวลผลของสถาบันการเงินแห่งนั้นเอง หรือศูนย์ประมวลผลของเอกชนอื่น ๆ ที่สถาบันการเงินว่าจ้างให้ประมวลผล ในการจัดส่งข้อมูลดังกล่าวจะมีการบันทึกรายละเอียดของ batch ต่าง ๆ รวมทั้งยอดรวมด้านเดบิตและด้านเครดิตของข้อมูลแต่ละ batch ในวันนั้นลงในใบรับส่งเอกสารซึ่งจะช่วยให้สามารถตรวจกระทบบยอดย้อนไปยังรายการบัญชีแยกประเภททั่วไปในวันนั้นได้ และช่วยให้พนักงานของศูนย์ประมวลผลทราบยอดข้อมูลที่ส่งมาประมวลผลด้วย

สำหรับหน่วยงานที่ใช้ข้อมูลและหน่วยงานที่ทำหน้าที่ลงรหัสและพิสูจน์ความถูกต้องของข้อมูลที่สายการบังคับบัญชาได้ขึ้นอยู่กับศูนย์ประมวลผล ควรใช้ยอดคุมที่จัดส่งให้ศูนย์ประมวลผลครั้งแรกเป็นหลักในการคุมยอดบัญชีทุกประเภทที่จะจัดทำขึ้นในภายหลัง รวมทั้งรายงานขั้นสุดท้ายที่ได้จากการประมวลผลด้วย วิธีการควบคุมภายในที่กล่าวมานี้สามารถนำไปใช้กับการจัดทำ data entry เพื่อสร้างข้อมูลป้อนเข้าคอมพิวเตอร์ได้ทุกวิธี เช่น MICR การเจาะบัตร การบันทึกข้อมูลสู่ tape หรือ disk โดยตรงเป็นต้น

สำหรับสำนักงานสาขาสถาบันการเงินหรือส่วนงานเล็ก ๆ ที่ไม่มี proof machine ก็สามารถใช้ batch ในการคุมยอดได้เช่นเดียวกัน โดยพนักงานจะคัดแยกเอกสารออกเป็นกลุ่ม ๆ ตามประเภทของเช็ค ใบรับฝาก ค่าใช้จ่าย ฯลฯ แล้วใช้เครื่องบวกเลขรวมยอดเงินเพื่อทำใบปะหน้าคุมยอดแต่ละ batch

สำหรับสถาบันการเงินที่ใช้ multipocket proof machine ซึ่งประกอบด้วยช่องต่าง ๆ สำหรับคัดแยกประเภทของเอกสารจะมีขั้นตอนในการปฏิบัติงาน ดังนี้

(1) พนักงานจะป้อนยอดเงินด้านเครดิตและเดบิตซึ่งเป็นคู่บัญชีของแต่ละรายการด้วยยอดที่เท่า ๆ กัน เข้า proof machine เพื่อนำรายการเหล่านี้มาเข้ารหัสและคัดแยกเอกสารที่เป็นรายการเครดิตและเดบิตออกจากกันตามช่องที่กำหนดไว้

(2) ยอดเครดิตและเดบิตทุกรายการจะถูกบวกสะสมเก็บไว้ในกระดาชบวกเลขแยกตามช่องเอกสารที่ถูกคัดแยก

(3) เมื่อเอกสารตามช่องที่คัดแยกครบจำนวนที่จะเข้า batch ก็จะทำออกยอดเงินรวมของ batch และนำเอกสารออกจากช่องคัดแยก

(4) นำเอกสารที่ได้จากช่องคัดแยกเอกสารมาจัดรวมกันเป็น batch และแนบรายละเอียดที่ปรากฏในกระดาดขาวเลขไว้ทุก batch

(5) ทำใบปะหน้า batch แสดงยอดเงินรวมทุกรายการที่อยู่ใน batch

เมื่อสิ้นวัน proof machine จะออกยอดเงินรวมทั้งสิ้นของเอกสารที่นำมาคัดแยกในแต่ละช่องเพื่อใช้เป็นยอดคุมรายการที่เกิดขึ้นในวันนั้น

สถาบันการเงินขนาดใหญ่ซึ่งมีปริมาณงานมากอาจตั้งเป็นศูนย์พิสูจน์ยอด (proof center) เพื่อประหยัดค่าใช้จ่าย โดยรวบรวมเอาเอกสารที่จะใช้ในการจัดทำข้อมูลของสำนักงานสาขาทุกแห่งมาจัดทำ batch แต่เพียงแห่งเดียว สำหรับขั้นตอนในการปฏิบัติงานของ proof center นั้น จะมีลักษณะคล้ายกับสำนักงานสาขาที่มี proof machine ตามที่กล่าวมาแล้ว

ในการจัดทำ batch ข้อมูล ควรแบ่งแยกหน้าที่ของพนักงานให้ชัดเจน เช่น ในสำนักงานสาขาที่ไม่มี proof machine อาจกำหนดให้พนักงานคนแรกที่ได้รับเอกสารเป็นผู้จัดทำ batch โดยมีพนักงานอีกคนหนึ่งทำหน้าที่ตรวจสอบการจัดทำ batch และทำยอดคุมจำนวนเงินทุก batch ที่ทำขึ้นในวันนั้น สำหรับสำนักงานสาขาที่มี proof machine ไม่ควรให้พนักงานที่ได้รับเอกสารเป็นผู้นำเอกสารป้อนเข้า proof machine ควรมีพนักงานอีกคนหนึ่งทำหน้าที่เดินเครื่อง proof machine เพื่อจัดทำ batch และจัดให้มีพนักงานชั้นบริหารเป็นผู้ตรวจสอบยอดเงินรวมทุก batch และทำยอดคุมสิ้นวัน ก่อนจัดส่งเอกสารที่เข้า batch เรียบร้อยแล้วให้ศูนย์ประมวลผล

การพิสูจน์ความถูกต้องของข้อมูลอีกวิธีหนึ่งที่สถาบันการเงินนิยมใช้กันมากคือวิธีพิสูจน์ยอดเงินฝาก (proof of deposit method) โดยจำนวนเงินและรายละเอียดที่จำเป็นต้องใช้ในการประมวลผลจะถูกเข้ารหัส (encode) ให้อยู่ในรูปที่เครื่องจักรสามารถอ่านความหมายได้ ใบรับฝากเงินหรือถอนเงินของลูกค้ารายเดียวกันจะถูกคัดแยกให้มารวมอยู่ในที่เดียวกัน หากรายการที่มียอดเป็นเครดิตของลูกค้าถูกป้อนเข้าเครื่อง proof machine จะบวกยอดเก็บไว้เพื่อรอกหักกับยอดเดบิตของลูกค้ารายเดียวกัน และก่อนที่ป้อนยอดเครดิตของลูกค้ารายอื่นเข้าไปจะต้องล้างยอดเครดิตของลูกค้ารายเก่าที่มีอยู่เดิมให้เป็นศูนย์เสียก่อน วิธีการดังกล่าวจะช่วยให้สามารถพิสูจน์ยอดเงินฝากของลูกค้าแต่ละรายได้เช่นเดียวกัน

งานขั้นต่อไปในการจัดทำข้อมูลก็คือ การนำข้อมูลที่บันทึกไว้ในระบบ MICR ซึ่งได้จัดทำ batch เรียบร้อยแล้วมาป้อนเข้าเครื่องอ่านและคัดแยกข้อมูล (reader and sorter) ดำเนินการแยกประเภทของข้อมูล และรวมยอดเงินเพื่อให้คอมพิวเตอร์ผ่านรายการไปยังบัญชีแยกประเภทที่เกี่ยวข้องต่อไป สำหรับรายการที่เครื่องไม่ยอมรับเนื่องจากอ่านความหมายไม่ได้ (rejected item) จะถูกบันทึกไว้ในบัญชีหัก (overnight general ledger suspense or hold over account) เพื่อดำเนินการจัดทำข้อมูลใหม่ตามขบวนการที่ได้กล่าวมาแล้ว สำหรับสถาบันการเงินที่ใช้บัญชีคุม (general ledger control account) ในการคุมยอด ข้อมูลที่รับมาจากฝ่ายพิสูจน์ยอด (proof department) ในแต่ละวันจะใช้วิธีล้างรายการ (reverse) ด้วยยอดรวมของรายการที่เครื่องไม่ยอมรับในวันรุ่งขึ้น โดยจะนำรายการที่เครื่องไม่ยอมรับนี้กลับไปทำใหม่และถือเป็นรายการที่จะส่งเข้าประมวลผลในวันถัดไป

สำหรับสถาบันการเงินขนาดใหญ่ที่ใช้คอมพิวเตอร์บันทึกรายการในบัญชีแยกประเภทโดยอัตโนมัติจะให้ส่วนงานต่างๆ หรือศูนย์พิสูจน์ยอด (Central proof department) เป็นผู้รวบรวมข้อมูลที่เกิดขึ้นในแต่ละวัน เพื่อจัดทำ batch ให้ศูนย์ประมวลผล โดยบันทึกรายการที่ส่งไปประมวลผลไว้ในบัญชีเคลียร์สำนักงานใหญ่ (head office clearing account) บัญชีเคลียร์สาขา (branch clearing account) หรือบัญชีงานระหว่างการประมวลผล (computer work-in-process account) แล้วแต่กรณี และศูนย์ประมวลผลจะใช้บัญชีเหล่านี้บันทึกรายการที่เครื่องไม่ยอมรับที่ส่งกลับคืนเช่นเดียวกัน ซึ่งทางสำนักงานสาขาหรือหน่วยงานที่ใช้ข้อมูลจะให้พนักงานลงบัญชีปรับปรุงรายการที่เครื่องไม่ยอมรับนี้ด้วยมือ (manual) สถาบันการเงินบางแห่งที่ใช้คอมพิวเตอร์จัดทำบัญชีแยกประเภททั่วไป อาจไม่ยอมให้พนักงานสาขาหรือหน่วยงานที่ใช้ข้อมูลปรับปรุงแก้ไขรายการในบัญชีแยกประเภทด้วยมือ ดังนั้น รายการที่สามารถประมวลผลด้วยเหตุใดก็ตาม จะถูกส่งกลับมายังหน่วยงานต้นเรื่องที่จัดทำข้อมูล และบันทึกไว้ในบัญชีคุมยอดรายการที่ยังไม่ได้ลงบัญชี (unposted debit/credit account) เมื่อพบข้อผิดพลาดที่เครื่องไม่ยอมรับก็จะล้างรายการออกจากบัญชีคุมยอดและบันทึกรายการลงในบัญชีรายตัวลูกค้ำหรือบัญชีย่อย (detail account) แล้วแต่กรณี ในการใช้คอมพิวเตอร์ลงบัญชีแยกประเภททั่วไปโดยอัตโนมัติดังกล่าวควรห้ามมิให้สำนักงานสาขาหรือหน่วยงานที่ใช้ข้อมูลลงรายการบัญชีด้วยมือได้โดยตรง และจะต้องปฏิบัติตามวิธีการที่กำหนดไว้เท่านั้น

6.1.2 การจัดทำข้อมูลแบบ (Non-MICR Data Entry)

NON-MICR คือ การแปลงข้อมูลจากเอกสารขั้นต้นให้อยู่ในรูปที่เครื่องสามารถอ่านข้อมูลได้ โดยการเจาะข้อมูลลงบัตร บันทึกข้อมูลลงเทปหรือ disk หรือป้อนข้อมูลเข้าเครื่อง terminal ไปสู่คอมพิวเตอร์โดยตรง ซึ่งข้อมูลที่ป้อนเข้าคอมพิวเตอร์อาจผิดพลาดได้เพราะต้องใช้เจ้าหน้าที่ปฏิบัติงานเป็นส่วนใหญ่

สถาบันการเงินบางแห่งใช้วิธีพิมพ์แบบฟอร์มสำหรับกรอกข้อมูลและจำนวนเงินลงในบัตรคอมพิวเตอร์ที่จะนำไปเจาะ ซึ่งอาจใช้วิธีคุมยอดเงินแต่ละ batch ได้เช่น ในกรณีเงินให้กู้ชนิดผ่อนชำระ จะพิมพ์คู่มือการผ่อนชำระในรูปบัตรคอมพิวเตอร์ไว้ล่วงหน้าในวันทำสัญญา คู่คู้ดังกล่าวจะพิมพ์และเจาะข้อมูลเกี่ยวกับเลขที่บัญชี เงินกู้ จำนวนเงินกู้ประเภทเงินกู้ และข้อมูลอื่น ๆ รวมทั้งเดือนที่ครบกำหนดชำระเงินกู้ ซึ่งสามารถคุมยอดได้เช่นกัน

6.2 การป้อนข้อมูลโดยใช้เครื่อง terminal (Terminal Entry)

ปัจจุบันนิยมการป้อนข้อมูลโดยเจ้าหน้าที่เป็นผู้ key ข้อมูลผ่านเครื่อง Terminal เข้าคอมพิวเตอร์เป็นส่วนใหญ่ เนื่องจากสามารถลดขั้นตอนในการแก้ไขข้อผิดพลาดลงได้มาก โดยเจ้าหน้าที่ควบคุมเครื่อง Terminal สามารถแก้ไขข้อมูลให้ถูกต้องได้ทันที เครื่อง Terminal ที่นิยมใช้กันมีอยู่ 2 ระบบ คือ ระบบ key-to-tape และระบบ key-to-disk และในเครื่อง Terminal จะมีระบบ software ที่สามารถป้องกันข้อผิดพลาดได้ค่อนข้างมาก

โปรแกรมต่าง ๆ (software programs) ที่ใช้ในการควบคุมการจัดทำข้อมูลควรกำหนดให้เฉพาะ programmer เท่านั้น เป็นผู้นำออกมาใช้และเก็บรักษาไว้ในที่ปลอดภัย ส่วนวิธีการควบคุมอื่น ๆ เช่น การทำ hash totals การทำ block and record counts และการกระทบยอดรวมในแนวนอนกับแนวตั้ง (crossfooting balancing) ควรนำมาใช้ภายหลังการประมวลผล เพื่อให้แน่ใจว่าข้อมูลที่นำไปประมวลผลมีความสมบูรณ์และถูกต้อง

6.3 การพิสูจน์ยอด Batch และการควบคุมข้อมูล

(Batch proof and Controls)

เอกสารขั้นต้นที่ศูนย์คอมพิวเตอร์ได้รับ จะถูกจัดส่งมาเป็นชุด (batch) แยกรายการด้านเดบิตและด้านเครดิตมิให้ปะปนกัน และมีใบปะหน้าหรือเทปกระดาษบวกเลขแสดงยอดเงินรวมของแต่ละ batch พนักงานของศูนย์ประมวลผลจะให้เลขที่ batch โดยเขียนไว้ที่ใบปะหน้า หรือทำใบปะหน้าพร้อมให้เลขที่ batch ในกรณีที่ใช้เทปกระดาษบวกเลขปะหน้ามา ต่อจากนั้นจะนำ batch มารวมกันจัดเป็น block พร้อมทั้งทำใบปะหน้าระบุเลขที่ block และยอดเงินรวมของแต่ละ block

ต่อจากนั้นจะนำเอกสารที่จัดเป็น block แล้วป้อนเข้าเครื่องคอมพิวเตอร์เอกสารที่คอมพิวเตอร์ไม่ยอมรับ (rejected items) ควรแยกออกมาต่างหาก และส่งไปให้พนักงานกระทบยอด พร้อมกับสำเนาแสดงรายการที่ป้อนเข้าคอมพิวเตอร์ ซึ่งสำเนาดังกล่าวจะมีรายละเอียดดังนี้ หมายเลข batch หมายเลข block หมายเลขลำดับของเอกสาร (เอกสารแต่ละฉบับจะมีเลขลำดับ เพื่อความสะดวกในการค้นหา) เลขที่บัญชี จำนวนเงินของแต่ละรายการ จำนวนเงินรวมของ batch และจำนวนเงินรวมของ block ผลต่างของจำนวนเงินในแต่ละ batch และแต่ละ block ที่คอมพิวเตอร์รวมแล้วไม่เท่ากับยอดที่ปรากฏในใบปะหน้า batch และ block

นอกจากนี้ พนักงานที่ทำหน้าที่กระทบยอดจะได้รับ reconciliation form จากหน่วยงานต้นสังกัดที่ส่งเอกสารมาให้ ซึ่งจะระบุยอดรวมรายการเดบิตและยอดรวมรายการเครดิตที่ส่งเข้าประมวลผล และได้รับเทปรายละเอียดจำนวนเงินของแต่ละรายการในเอกสารแต่ละ batch ด้วย เพื่อช่วยในการกระทบยอดรายการต่าง ๆ ที่ส่งไปประมวลผลกับรายการที่ป้อนเข้าคอมพิวเตอร์และรายการที่เครื่องคอมพิวเตอร์ไม่ยอมรับ

พนักงานกระทบยอดมีหน้าที่รับผิดชอบตรวจสอบความถูกต้องในยอดเงินรวมของเอกสารแต่ละ batch กับรายงานคุมยอด สำหรับเอกสารที่คอมพิวเตอร์ไม่ยอมรับ (rejected items) ก็จะทำเทปรายละเอียดแสดงจำนวนเงินของแต่ละรายการและรวบรวมไว้แล้วส่งไปให้หน่วยงานที่ทำหน้าที่นำเอกสารที่เครื่องไม่ยอมรับ ป้อนเข้าคอมพิวเตอร์อีกครั้ง รายการที่คอมพิวเตอร์ยังไม่ยอมรับอีกจะถูกส่งกลับมาให้พนักงานกระทบยอดรวมเป็นครั้งสุดท้าย เพื่อส่งไปยังหน่วยงานต้นสังกัดเดิม เพื่อค้นหาและแก้ไขข้อผิดพลาดต่อไป

ระบบ key-to-disk และ key-to-tape มีประสิทธิภาพในการป้อนข้อมูลเข้าคอมพิวเตอร์ดีกว่าระบบเจาะบัตร โดยพนักงานคนแรกจะป้อนข้อมูลผ่านทางแป้นอักษรของเครื่องบันทึกข้อมูล ซึ่งมีจอภาพคล้ายทีวี แสดงข้อมูลที่ป้อนเข้าไปในเครื่อง และเก็บไว้รอการสอบถามในหน่วยความจำ ต่อจากนั้น พนักงานอีกคนหนึ่งจะป้อนข้อมูลชุดเดียวกันเข้าเครื่อง เพื่อสอบถามความถูกต้องและทำการแก้ไขที่จำเป็น นอกจากนี้ ระบบ key-to-disk และระบบ key-to-tape ยังสามารถผลิตข้อมูลทางสถิติที่ช่วยให้ทราบถึงประสิทธิภาพการทำงานของฝ่ายที่ทำหน้าที่ key ข้อมูล (keying department) อีกด้วย สำหรับการใช้โปรแกรมในการควบคุมข้อมูลที่ป้อนเข้าเครื่อง terminal จะอยู่ในเรื่อง Terminal Entry

งานขั้นต้นในการสร้างข้อมูล การใช้ข้อมูล และการแก้ไขปรับปรุงข้อมูล ในส่วนที่ไม่เกี่ยวกับสื่อกลางที่ใช้บันทึกและส่งข้อมูลหรือเทคโนโลยีที่ใช้ในการประมวลผล จะต้องมีการควบคุมที่ดี ซึ่งอาจเป็นระบบ manual หรือระบบอัตโนมัติก็ได้ เพื่อให้ข้อมูลมีความสมบูรณ์ (integrity) เชื่อถือได้ (reliability) และถูกต้อง (accuracy)

หน่วยงานที่ทำหน้าที่สร้างข้อมูลขั้นต้น ควรมีแฟ้มเอกสารเก็บแบบฟอร์มข้อมูลขั้นต้นที่จะป้อนเข้าคอมพิวเตอร์ เพื่อประมวลผลไว้ทุกประเภท พร้อมทั้งวิธีการสร้างข้อมูลและการปฏิบัติงานของพนักงานทุกขั้นตอน เพื่อประโยชน์ในการฝึกฝนพนักงานและใช้เป็นเอกสารอ้างอิงสำหรับข้อมูลที่บันทึกลง tape หรือ disk โดยตรงจะมีจอภาพทีวี แสดง format ของข้อมูลที่ใช้ป้อนคอมพิวเตอร์ รวมทั้ง field ต่าง ๆ ที่ใช้ในการบันทึกข้อมูล

กล่าวโดยสรุป ข้อมูลที่ส่งไปเจาะบัตรนั้นควรจัดรวม batch และบันทึกยอดเงินรวมของแต่ละ batch ไว้ และจะต้องมียอดคุมสิ้นวันระบุไว้ในใบกระทบบยอด เพื่อให้พนักงานใช้กระทบบยอดกับรายงานที่คอมพิวเตอร์พิมพ์ยอดเงินของเอกสารแต่ละ batch ออกมาควรพิสูจน์ความถูกต้องของบัตรที่เจาะอีกครั้ง โดยให้พนักงานที่อยู่ในหน่วยงานอิสระหรือพนักงานของหน่วยงานที่ส่งข้อมูลมาประมวลผลเจาะซ้ำ และควรมอบให้ศูนย์ประมวลผลเป็นผู้รับผิดชอบ หากมีการนำเอาวิธีการควบคุมยอดมาใช้กับงานเจาะบัตร

6.4 การควบคุมการจัดทำข้อมูล (Transaction Control)

การควบคุมภายในเกี่ยวกับการจัดทำข้อมูลที่ดี ควรมีลักษณะดังนี้

(1) มีการแบ่งแยกหน้าที่ไว้อย่างชัดเจน มีการตรวจสอบข้อมูลที่จะป้อนเข้าคอมพิวเตอร์ และการใช้ข้อมูลที่ได้จากการประมวลผล

(2) มีวิธีการคุมยอดเงินสำหรับรายการที่เครื่องไม่ยอมรับ (reject) และรายการหัก (holdover item) ที่ดีและมีประสิทธิภาพ

(3) มีการกระทบบยอดจากรายงานที่ได้จากการประมวลผลกับยอดคุมที่หน่วยงานต้นสังกัดส่งมาให้ทุกครั้ง

(4) สามารถแก้ไขข้อผิดพลาดได้โดยฉับพลัน

(5) มีพนักงานระดับสูงและระดับหัวหน้าหน่วยเป็นผู้ตรวจสอบข้อผิดพลาดที่ปรากฏตามรายงานที่ได้จากการประมวลผล

(6) มีการควบคุมการจัดส่งรายงานที่ได้จากการประมวลผลทุกชนิดไปให้ผู้ใช้อข้อมูลอย่างดี

หากการควบคุมภายในดังกล่าว มีความบกพร่องและขาดประสิทธิภาพ ย่อมก่อให้เกิดความเสี่ยงซึ่งอาจมีผลเสียต่อสถาบันการเงินได้

การควบคุมเอกสารข้อมูลเบื้องต้นที่อยู่ในแบบฟอร์มซึ่งได้รับมาจากหน่วยงานต่าง ๆ ควรควบคุมโดยวิธีแยกเอกสารของแต่ละหน่วยงานมิให้ปะปนกัน การควบคุมงาน batch ที่ดี และมีประสิทธิภาพควรมีการบันทึกเลขที่ batch และจำนวนเงินรวมของ batch ไว้ในแบบฟอร์มในขณะที่รับเอกสารโดยแยกตามหน่วยงาน

หน่วยงานที่รับเอกสารข้อมูลจากหน่วยงานที่ใช้ข้อมูล อาจมีวิธีปฏิบัติแตกต่างกันสุดแล้วแต่ขนาดของศูนย์ประมวลผล หากเป็นศูนย์ประมวลผลขนาดใหญ่ พนักงานรับเอกสารส่วนใหญ่จะทำหน้าที่รวบรวมเอกสารเข้า batch และจัด block ส่วนในศูนย์ประมวลผลขนาดเล็ก พนักงานรับเอกสารอาจต้องทำหน้าที่หลายอย่าง เช่น รับเอกสาร จัดบันทึกการรับเอกสาร รวบรวมเอกสารเข้า batch และจัด block ป้อนเอกสารเข้าเครื่องอ่าน MICR และคัดแยกเอกสารออกเป็นพวก ๆ โดยใช้ MICR reader/sorters กระทบบยอดที่ได้จากการประมวลผล และรวบรวมข้อมูลและรายงานที่ได้จากการประมวลผลส่งคืนหน่วยงานที่ใช้ข้อมูล ซึ่งถ้าไม่มีการแบ่งแยกหน้าที่ย่อมก่อให้เกิดช่องโหว่ในการควบคุม แม้ว่าพนักงานรับเอกสารจะยอมรับงานเพิ่มขึ้น เช่น เตรียมข้อมูล ป้อนข้อมูล รวบรวมรายงานหลังจากได้

กระตบยอตแล้วส่งคืนหน่วยงานที่ใช้ข้อมูลก็ตาม ไม่ควรยอมให้พนักงานรับเอกสารทำหน้าที่เดินเครื่องคอมพิวเตอร์ และ/หรือกระตบยอตข้อมูลที่ได้จากการประมวลผลอย่างเด็ดขาด

โดยทั่วไปการแบ่งแยกหน้าที่ จะบรรลุผลได้ก็ต่อเมื่อไม่ปล่อยให้บุคคลคนเดียว รับผิดชอบงานต่อไปนี้ 2 หน้าที่พร้อมกัน

- (1) จัดทำข้อมูลขึ้นต้น
- (2) เดินเครื่องป้อนข้อมูลเข้าคอมพิวเตอร์
- (3) เดินเครื่องคอมพิวเตอร์และเครื่องแยกเอกสาร
- (4) รวบรวมรายการที่เครื่องไม่ยอมรับ (reject) หรืออ่านไม่ได้ เพื่อกลับไปทำใหม่
- (5) กระตบยอตข้อมูลที่ได้จากการประมวลผล
- (6) จัดส่งข้อมูลที่ได้จากการประมวลผลไปยังผู้ใช้ข้อมูล

นอกจากนี้ควรกำหนดให้พนักงานปฏิบัติงานอยู่ในกรอบที่จำกัด พนักงานประจำเครื่องคอมพิวเตอร์ (computer operator) ควรมีหน้าที่เดินเครื่องเพียงอย่างเดียว ไม่ควรมีหน้าที่เก็บยอตตัวเลขใดๆ ทั้งสิ้น พนักงานเจาะบัตร (Key punch operator) มีหน้าที่เจาะบัตรเท่านั้น หากไม่สามารถจำกัดให้พนักงานทำหน้าที่เพียงอย่างเดียวได้ ก็อาจยอมให้ทำหน้าที่เป็นผู้ช่วยงานด้านอื่นได้ ฝ่ายบริหารควรคำนึงถึง "การแบ่งแยกหน้าที่" เพื่อประโยชน์ในการควบคุมเป็นสำคัญ โดยเฉพาะการแบ่งแยกหน้าที่ของพนักงานในระบบคอมพิวเตอร์เพราะงานที่สำคัญ ๆ อาจตกอยู่ในมือของบุคคลเพียงไม่กี่คน

6.5 การควบคุมอุปกรณ์ที่ใช้บันทึกข้อมูล (Control of Data File Media)

อุปกรณ์บันทึกข้อมูลพื้นฐานที่ใช้กับคอมพิวเตอร์ (ได้แก่ disk, tape, drum และ card) อาจเสียหายหรือถูกทำลายได้ง่ายกว่าเอกสาร จึงต้องใช้ความระมัดระวังในการ เก็บอุปกรณ์ที่ใช้ในการบันทึกข้อมูลต่าง ๆ เพื่อป้องกันมิให้เกิดความเสียหายอย่างรุดกมที่สุด

ควรใช้เครื่องปรับอากาศและเครื่องปรับอากาศขึ้น เพื่อรักษาอุณหภูมิและความชื้นให้เหมาะสมในการเก็บรักษาอุปกรณ์เก็บข้อมูลทั้งในห้องคอมพิวเตอร์ ห้องเก็บอุปกรณ์ที่เชื่อมกับคอมพิวเตอร์ และสถานที่ภายนอกที่ใช้เก็บอุปกรณ์ที่บันทึกข้อมูลสำรองไว้ใช้ยามฉุกเฉิน (backup) นอกจากนี้จะต้องระมัดระวังความเสี่ยงภัยที่เกิดจากการแพร่สนามแม่เหล็กของเครื่องกำเนิดไฟฟ้า และต้นกำเนิดพลังงานอื่น ๆ ที่ตั้งอยู่บริเวณใกล้เคียงกับสถานที่เก็บอุปกรณ์

อันตรายที่เกิดจากไฟไหม้เป็นสิ่งสำคัญอีกประการหนึ่งที่ต้องหาทางควบคุมและป้องกันไว้ หากเกิดไฟไหม้สถานที่ใกล้ ๆ ที่เก็บอุปกรณ์ ความร้อนจะทำลายข้อมูลที่บันทึกไว้ได้ และถ้าอุปกรณ์ดังกล่าวเปียกน้ำ ที่ใช้ดับเพลิงก็ย่อมจะเสียหายมากขึ้น

การใช้เครื่องมือและการวางระเบียบควบคุมในการรักษาความปลอดภัย อุปกรณ์ที่ใช้บันทึกข้อมูลเป็นประจำหรือข้อมูลสำรองที่เก็บไว้ใช้ยามฉุกเฉิน ต้องมีประสิทธิภาพพอที่จะป้องกันอุปกรณ์ที่ใช้ในการบันทึกข้อมูลจากภัยพิบัติต่าง ๆ ได้ วิธีที่เหมาะสมที่สุดในการจัดเก็บอุปกรณ์ที่ใช้ในการบันทึกข้อมูล (data file) และอุปกรณ์อื่น ๆ ที่ใช้ประโยชน์ในการถ่ายเทข้อมูลก็คือ นำอุปกรณ์ดังกล่าวไปเก็บในห้องที่แยกต่างหากจากห้องคอมพิวเตอร์ โดยมีผู้เก็บรักษา data file ที่เรียกว่า librarian เท่านั้น ที่เข้าออกห้องนี้ได้ (ในกรณีฉุกเฉินอาจยอมให้พนักงานระดับหัวหน้าที่

ทำงานในขณะนั้นเข้าออกได้ด้วย) และในทางปฏิบัติจะต้องห้ามมิให้นำ tape หรือ disk ออกนอกห้อง เว้นแต่นำไปประมวลผล หรือนำออกไปเก็บยังที่เก็บสำรองนอกสถานที่ หรือมีการอนุมัติเป็นกรณีพิเศษเท่านั้น

กรณีที่จะต้องเข้าไปในห้องเก็บอุปกรณ์ (library) อย่างเร่งด่วน ต้องทำบันทึกเสนอผู้บริหารระดับสูงของศูนย์ประมวลผลทันที

สำหรับข้อมูลสำรองที่เก็บไว้ใช้ยามฉุกเฉิน ควรเก็บไว้ในสถานที่ไกลพอสมควร หากศูนย์คอมพิวเตอร์มีภัยใด ๆ ก็ตาม จะต้องถูกลบไปไม่ถึงสถานที่เก็บอุปกรณ์ดังกล่าว อย่างไรก็ตาม ข้อมูลสำรองที่เก็บไว้ในสถานที่ห่างไกลก็ควรจะต้องนำเอาข้อมูลมาใช้ได้รวดเร็วในกรณีที่ข้อมูลที่ศูนย์ประมวลผลเสียหาย มาตรการรักษาความปลอดภัย สถานที่เก็บอุปกรณ์ที่ใช้ในการบันทึกข้อมูลสำรองก็ต้องเหมือนกับของ Library ณ ศูนย์ประมวลผล นอกจากนี้ควรมีบันทึกการเข้าออกสถานที่เก็บข้อมูลสำรองและควรให้มีบุคคล 2 คน ร่วมกันรับผิดชอบในการควบคุมสถานที่เก็บข้อมูลสำรอง ถ้าฝ่ายบริหารจำเป็นต้องจัดเก็บข้อมูลสำรองไว้ในศูนย์ประมวลผล แม้จะมีมาตรการรักษาความปลอดภัยที่ดีเพียงใดก็ตาม คณะกรรมการธนาคารควรทบทวนการอนุมัติให้มีการปฏิบัติเช่นนั้น และร่วมรับความเสี่ยงภัยด้วย

ในศูนย์ประมวลผลขนาดเล็กจะมี librarian เพียงคนเดียว และอาจทำหน้าที่อื่นด้วย แต่ก็ยังต้องมีการควบคุมการใช้ tape หรือ disk เช่นเดียวกับในศูนย์ประมวลผลขนาดใหญ่ คือใช้วิธีเก็บ date file ทั้งหมดไว้ในห้องนิรภัยที่กันไฟได้ การเปิดประตูต้องใช้กุญแจ 2 ดอกร่วมกัน หรือมอบหมายให้บุคคล 2 คน ถือรหัสเปิดห้องคนละชุด ควรใช้ความระมัดระวังในการคัดเลือกบุคคลที่มีหน้าที่ถือรหัสเปิดห้องนิรภัย การมอบหมายให้บุคคล 2 คน ซึ่งทำหน้าที่เดียวกันถือรหัสคนละชุดย่อมทำให้ขาดประสิทธิภาพในการควบคุม อาจอนุญาตให้หัวหน้างานประจำจะเข้าไปหยิบ tape หรือ disk ใน library ได้ ในกรณีเร่งด่วนและ librarian ไม่อยู่ โดยจะต้องมีการควบคุมบันทึกการใช้ library และตรวจสอบจากฝ่ายบริหาร

วิธีการปฏิบัติในการเก็บรักษา tape หรือ disk ควรเขียนเป็นระเบียบปฏิบัติในเรื่องเหล่านี้

- (1) ระบบจัดเก็บ tape
- (2) การดูแลรักษาประจำวัน
- (3) วิธีปฏิบัติในการรับ tape หรือ disk ที่ซื้อใหม่ และวิธีปฏิบัติเมื่อเลิกใช้ของเก่าหรือชำรุด
- (4) การทำบัญชีและตรวจนับ tape หรือ disk คงเหลือ
- (5) การตรวจสอบข้อมูลที่บันทึกไว้ใน tape หรือ disk ที่เก็บไว้ และกำหนดเวลาทำลายข้อมูลที่บันทึกไว้ใน tape หรือ disk ที่ใช้ในงานต่าง ๆ

อุปกรณ์ที่ใช้ในการบันทึกข้อมูลในรูปแบบแม่เหล็กหรือการ์ดที่เจาะรูแล้ว ต้องป้องกันให้พ้นจากการเสียหายหรือนำไปใช้โดยมิได้รับอนุญาต ฝ่ายบริหารควรพิจารณาข้อบกพร่องที่จะทำให้เกิดการควบคุมขาดประสิทธิภาพ ซึ่งจะก่อให้เกิดผลเสียหายทางการเงินได้ ความเสี่ยงภัยดังกล่าวอาจเกิดขึ้นจากการให้ข้อมูลอันเป็นความลับของลูกค้ายกบุคคลภายนอกโดยพนักงานซึ่งจะตั้งใจหรือไม่ก็ตามอันจะทำให้สถาบันการเงินสูญเสียลูกค้าและอาจถูกฟ้องเรียกค่าเสียหายได้

วิธีง่าย ๆ ที่ใช้ป้องกันมิให้ข้อมูลใน tape ถูกทำลาย คือการใช้ ring ซึ่งมีลักษณะเป็นวงแหวนพลาสติก เมื่อต้องการบันทึกข้อมูล ก็นำเอา ring มาใส่ในร่องที่ทำไว้รอบ ๆ แกนกลางของม้วน tape หากดึง ring

ออกจากม้วน tape เครื่องจะไม่สามารถบันทึกข้อมูลใหม่ทับข้อมูลที่มีอยู่เดิมได้ การป้องกันในลักษณะนี้อาจนำไปปรับปรุงใช้กับเครื่องมืออื่น ๆ ได้เช่นเดียวกัน

การป้องกันข้อมูลที่บันทึกไว้ใน disk สามารถทำได้โดยใช้ software ควบคุมโดยวิธี label checking ซึ่งอาศัยคำสั่งให้เครื่องเปิด file ย่อมให้ใช้ข้อมูลที่บันทึกอยู่ใน file ได้ โดยเครื่องจะเปรียบเทียบวันที่สร้าง file เลขที่ file ชื่อ file และวันที่ file หมดอายุการใช้งานที่อ่านได้จาก file กับข้อมูลที่อ่านได้จากตัวโปรแกรมหรือ job control cards หากข้อมูลดังกล่าวไม่ตรงกัน เครื่องจะบอกให้ทราบทางแผงควบคุม (console) ถ้ามีการปฏิบัติงานข้ามขั้นตอน พนักงานควบคุมเครื่องก็ต้องติดต่อผ่านแผงควบคุม (console) ซึ่งจะถูกบันทึกไว้เพื่อให้ฝ่ายบริหารใช้ในการควบคุมและตรวจสอบ

วิธีการควบคุมที่สำคัญอีกประการหนึ่ง ก็คือ การใช้ label บันทึกไว้ในอุปกรณ์เก็บข้อมูลและปิดไว้ภายนอกอุปกรณ์บันทึกข้อมูล สำหรับแถบชื่อที่ติดภายนอกอุปกรณ์เก็บข้อมูลนั้นช่วยให้พนักงานคุมเครื่อง (operator) และพนักงานควบคุมดูแลอุปกรณ์ที่ใช้เป็นข้อมูล (librarian) สามารถหยิบใช้ได้โดยสะดวกและถูกต้อง บางแห่งอาจทำรหัสสีต่างๆ ไว้บนตลับ tape หรือ disk ด้วย

ในระบบ automated librarian systems ซึ่งเป็นระบบจัดเก็บอุปกรณ์ที่ใช้บันทึกข้อมูลโดยอัตโนมัติ จะมีเพียงเลขลำดับ (serial number) ของ tape หรือ disk ระบุไว้ในแถบชื่อที่ติดภายนอกเท่านั้น สำหรับข้อมูลภายใน tape หรือ disk จะทราบได้โดยดูจากรายงานที่ระบบอัตโนมัติพิมพ์ออกมา หรือสอบถามระบบควบคุมผ่านเครื่อง terminal

สำหรับ label ที่บันทึกไว้ในอุปกรณ์ที่ใช้เก็บข้อมูล (internal label) จะช่วยควบคุมและป้องกันมิให้ใช้ tape หรือ disk ผิด แต่ operator อาจจะไม่เอาใจใส่หรือมองข้ามไปโดยไม่ตั้งใจ จึงควรชี้แจงและมีระเบียบกำหนดให้ปฏิบัติตามขั้นตอน หากจำเป็นต้องประมวลผลโดยไม่มีการตรวจสอบ internal label ต้องให้พนักงานชั้นบริหารเป็นผู้อนุมัติ

internal label จะบันทึกไว้ที่หัวและท้าย file สำหรับ label ที่อยู่หัว file (header label) จะประกอบด้วยชื่อ file วันที่สร้าง file หมายเลขลำดับ volume เลขที่ม้วน และวันที่หมดอายุการใช้งาน ส่วน label ที่อยู่ท้าย file (trailer label) จะประกอบด้วยจำนวน record หรือ จำนวน block ข้อมูลที่บรรจุอยู่ใน file นั้น นอกจากนี้อาจมียอดรวมและข้อมูลอื่นที่แสดงการสิ้นสุดของ file หรือม้วน tape

internal label ควรอยู่ในรูปมาตรฐานใช้ได้กับโปรแกรมย่อย และงานทุกชนิดไม่ว่าจะเป็น file ที่ใช้ทดสอบการทำงาน (test file) หรือ file ข้อมูลหลัก (master file) การใช้ label ที่ไม่มีมาตรฐานในบางครั้ง อาจทำให้ operator ต้องข้ามขั้นตอนการตรวจสอบ label ก่อนใช้ file เป็นการลดประสิทธิภาพในการควบคุมด้วยวิธีนี้ลงและเพิ่มโอกาสให้เกิดอุบัติเหตุ ทำให้ข้อมูลเสียหายได้ง่าย นอกจากนี้ยังทำให้ประสิทธิภาพการทำงานทดลองเพราะต้องอาศัยคู่มือการทำงานเข้าช่วยในการปฏิบัติงานมากขึ้น

6.6 การจัดส่งรายงานให้ผู้ใช้อข้อมูลและการควบคุม

(Output Distribution and Control)

output ที่พิมพ์ออกมาและเอกสารข้อมูลขั้นต้นที่นำมาประมวลผลจะต้องมีการป้องกันอย่างดี เพื่อให้แน่ใจว่าข้อมูลถูกจัดส่งไปยังสาขาหรือหน่วยงานที่ถูกต้อง วิธีที่ดีที่สุดก็คือจัดตั้งแผนกจัดส่งรายงานขึ้นภายใต้การควบคุมของหน่วยงานรับส่งเอกสาร (mail room) การจัดส่งรายงานและเอกสารขั้นต้น ควรให้ผู้รับออกไปรับเอกสาร โดยระบุจำนวนหีบห่อเอกสารที่ผู้รับไป หีบห่อใส่เอกสารที่จัดส่งควรมีกุญแจระหว่างศูนย์ประมวลผลกับผู้ใช้อข้อมูล

คู่มือที่ใช้ในการควบคุมการจัดส่งรายงานควรมีรายละเอียดดังนี้

- (1) รายชื่อรายงานทุกชนิดที่ได้จากการประมวล
- (2) วิธีการแยกแยะรายงาน
- (3) จำนวนสำเนาของรายงานแต่ละชุดที่จัดส่งให้แต่ละสาขาหรือหน่วยงาน
- (4) ความถี่ที่ใช้รายงานแต่ละชุด
- (5) ลำดับก่อนหลังในการจัดส่งรายงานให้สาขาหรือหน่วยงานแต่ละแห่ง หรืออาจจัดเป็นตาราง

กำหนดเวลาจัดส่งรายงานก็ได้

- (6) คำอธิบายพิเศษประกอบรายงาน

ควรมีเอกสารเป็นรายการตรวจสอบ (checklists) การจัดทำรายงานทุกวัน ทุกสัปดาห์ ทุกเดือน และทุก 3 เดือน เพื่อบันทึกการจัดทำรายงานให้ผู้ใช้อข้อมูลทุกครั้งเป็นการประกันว่าหน่วยงานที่มีหน้าที่จัดส่งรายงานได้รับรายงานที่ต้องการทั้งหมดไปแล้ว อาจมีการใช้โปรแกรมทำหน้าที่บันทึกการจัดทำรายงานที่ต้องจัดส่งให้ผู้ใช้อข้อมูลประจำวันทั้งหมด เพื่อแสดงให้เห็นว่าได้จัดทำรายงานนั้น ๆ ไปแล้วหรือยัง หรืออาจจะแสดงรายละเอียดเฉพาะรายงานที่จัดทำแล้ว หรือเฉพาะรายงานที่ยังมิได้จัดทำก็ได้ เพื่อให้ทราบว่ายานงานนั้นได้ทำขึ้นแล้วหรือยัง และผู้ใช้ได้รับรายงานนั้นแล้วหรือไม่นั่นเอง การใช้ checklist ตรวจสอบการจัดทำรายงานควรกระทำทั้งฝ่ายจัดส่งรายงานและผู้ใช้ข้อมูล นอกจากนี้ผู้ใช้อข้อมูลควรตรวจสอบดูรายงานที่ได้จากการประมวลผลที่ได้รับมากับบันทึกการจัดทำรายงานประจำวันว่าใช้รายงานที่ได้จากการประมวลผลที่ตนต้องใช้หรือไม่ และให้ผู้ใช้อรายงานเซ็นชื่อรับรายงานดังกล่าวด้วยเพื่อความปลอดภัยในการจัดส่งข้อมูล

หน่วยงานที่มีหน้าที่จัดส่งรายงานที่ได้จากการประมวลผล ควรตรวจตราควบคุมคุณภาพว่ารายงานนั้นอ่านออกชัดเจน ไม่มีข้อผิดพลาด และควรมีการควบคุมยอดรวมต่าง ๆ ที่ปรากฏในรายงานที่เกี่ยวข้อง เพื่อช่วยให้แน่ใจว่ายอดรวมที่ปรากฏในรายงานนั้นถูกต้อง

6.7 การสอบทานและการกระทบยอดรายงาน

(Review and Reconciliation of Output)

รายการต่าง ๆ ที่ประมวลผลได้ประจำวัน ควรให้หน่วยงานที่ใช้อข้อมูล หรือหน่วยงานอิสระที่ทำหน้าที่ควบคุม เป็นผู้ตรวจกระทบยอดรวมที่ส่งมาประมวลผลกับยอดในบัญชีแยกประเภททั่วไปที่เกี่ยวข้อง ในการตรวจกระทบยอดจะมีการปรับปรุงรายการที่ศูนย์ประมวลผลรับมาประมวลผล รายการที่สูญหาย รายการพิเศษ และรายการที่เครื่องไม่ยอมรับ (rejected) หรือรายการที่ไม่สามารถผ่านบัญชี (nonpostable) ได้

หน่วยงานที่ใช้ข้อมูลหรือหน่วยงานอิสระที่ทำหน้าที่ควบคุม ควรตรวจระบยอด ดังนี้

(1) ตรวจทานตัวเลขที่ปรากฏตามรายการระบยอดตามที่หน่วยงานต้นสังกัดส่งให้ศูนย์ประมวลผลอีกครั้งหนึ่ง (double checking)

(2) ตรวจทานตัวเลขที่ปรากฏตามรายการระบยอดที่ศูนย์ประมวลผลจัดทำอีกครั้ง (double checking)

(3) ระบยอดจากงบทดลองและรายงานประกอบอื่น ๆ กับยอดคุมในบัญชีแยกประเภททั่วไป

หากมีการบันทึกยอดในบัญชีแยกประเภททั่วไปโดยอัตโนมัติ ยอดรวมในบัญชีแยกประเภททั่วไปจะเท่ากับยอดที่ได้จากการประมวลผลโดยไม่ต้องทำการปรับปรุงอีก ในกรณีเช่นนี้ ควรสอบหาสาเหตุเพื่อควบคุมรายการที่เครื่องไม่ยอมรับ (reject) และรายการพัก (holdover) โดยพิจารณาจากระยะเวลาที่ค้างอยู่ในบัญชีเป็นหลัก

การละเลยไม่ทำการระบยอด ณ ที่ศูนย์ประมวลผล หรือหน่วยงานที่ใช้ข้อมูลเพื่อพิสูจน์ความถูกต้องของข้อมูลในบางส่วน อาจทำให้สถาบันการเงินประสบความเสียหายได้

รายการที่ไม่อาจประมวลผลด้วยเครื่องจักรได้ (reject) เนื่องจากเครื่องอ่านไม่ได้หรือผ่านรายการไปบัญชีแยกประเภทไม่ได้ ควรคัดแยกออกจากรายการปกติ แล้วตรวจสอบทุกรายการเพื่อให้พนักงานแก้ไขและป้อนเข้าคอมพิวเตอร์ใหม่หรือส่งกลับไปยังหน่วยงานต้นสังกัดเพื่อแก้ไข และดำเนินการตามขั้นตอนใหม่ หรือดำเนินการอย่างอื่นแล้วแต่กรณี รายการ reject ที่นำไปแก้ไขหรือทำใหม่ ควรได้รับการตรวจสอบจากพนักงานชั้นบริหารของหน่วยงานที่ใช้ข้อมูลอีกครั้ง เพื่อให้แน่ใจว่าได้แก้ไขจนถูกต้องแล้วจริง ๆ และสามารถประมวลผลได้ ทั้งนี้ เพื่อช่วยประหยัดเวลาในการสอบหาข้อผิดพลาดที่ทำให้ประมวลผลไม่ได้

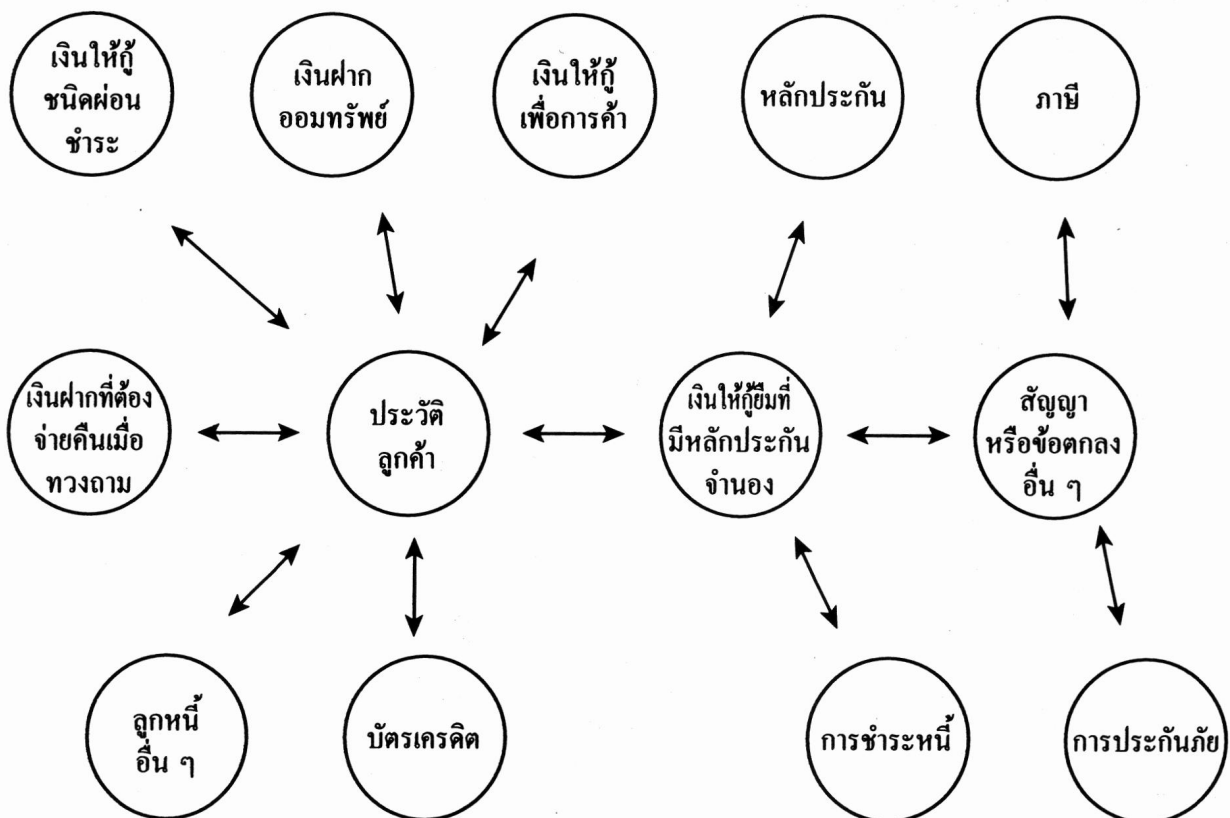
รายงานที่มีข้อสังเกตประกอบข้อมูลที่ปรากฏในรายงานที่ได้จากการประมวลผลต่าง ๆ ควรจัดทำอย่างสม่ำเสมอ โดยไม่คำนึงถึงว่าจะมีเรื่องที่น่าสังเกตเกิดขึ้นหรือไม่ ถ้าไม่มีเรื่องน่าสังเกต ก็ให้รายงานว่ามี เพื่อให้แน่ใจว่าได้รายงานครบถ้วน ตัวอย่างรายงานที่มีข้อสังเกตเหล่านี้ ได้แก่ เงินเบิกเกินบัญชี ลูกหนี้รายใหญ่ บัญชีพัก เงินที่ยังเรียกเก็บไม่ได้ รายงานหนี้ที่ครบกำหนดชำระ และรายการที่เป็นเงินจำนวนสูง ๆ รายงานเหล่านี้ ควรให้พนักงานชั้นบริหารของสถาบันการเงินเป็นผู้ทบทวน ส่วนรายงานที่ได้จากการประมวลผลที่ไม่มีผลต่อการเปลี่ยนแปลงทางการเงิน ควรให้หน่วยงานต้นสังกัดที่ใช้ข้อมูลเป็นผู้ตรวจสอบ เปรียบเทียบข้อมูลเดิม (original input) เช่น ชื่อและที่อยู่ เงินที่ให้กู้ยืมใหม่ เป็นต้น

หน้าที่รับผิดชอบความถูกต้องของยอดดุลแต่ละรายการ และงบทดลองที่ปรากฏในบัญชีแยกประเภททั่วไป จะเป็นหน้าที่ของพนักงานในหน่วยงานที่ใช้ข้อมูล หรือหน่วยควบคุมกลาง ผู้สอบบัญชีของสถาบันการเงินหรือพนักงานของสถาบันการเงินที่ควบคุมดูแล ควรตรวจสอบการระบยอดของหน่วยงานต่าง ๆ โดยไม่แจ้งให้ทราบล่วงหน้าเป็นบางครั้งบางคราว รวมทั้งการสอบทานกระดาษทำงานสอบหาสาเหตุผิดพลาดของรายการที่ไม่สามารถผ่านบัญชีได้ (unposted item) และรายการที่ผิดปกติอื่น ๆ ที่ปรากฏในรายงาน สำหรับรายการที่มีจำนวนเงินสูง ๆ หรือรายการที่ผิดปกติควรติดตามตรวจสอบให้ถึงที่สุด ผู้สอบบัญชีของสถาบันการเงินหรือพนักงานของสถาบันการเงินที่ควบคุมดูแลต้องทำบันทึกการระบยอดโดยระบุวันที่ทำการระบยอด และข้อผิดพลาดที่พบไว้ด้วย

6.8 การจัดเก็บข้อมูลในระบบ data base

Data Base คือการนำ data elements ซึ่งเป็นส่วนประกอบของข้อมูลที่ใช้ในโปรแกรมใดโปรแกรมหนึ่ง หรือหลายโปรแกรมที่สัมพันธ์กันมารวบรวมไว้และตัดส่วนที่ซ้ำซ้อนกันออกไป เพื่อจัดองค์ประกอบใหม่เป็นแฟ้มข้อมูลต่าง ๆ โดยมีการกำหนดลำดับความสำคัญลดหลั่นกันไปตามลำดับชั้น (hierarchical) แฟ้มข้อมูลเหล่านี้จะมี key กำกับ ซึ่งอาจเป็นเลขที่บัญชีหรือ เลขประจำตัวพนักงาน และอาจมี pointer เป็นตรรกะสำหรับบัญชีรายการตัวลูกค่าทุกรายด้วย และมี Data Base Management System (DBMS) เป็น software program ทำหน้าที่ควบคุมการใช้ข้อมูล ซึ่งอาจหาซื้อได้จากผู้ผลิตคอมพิวเตอร์หรือผู้สร้าง software program จำหน่ายโดยอิสระ นอกจากนี้ DBMS ยังอำนวยความสะดวกแก่โปรแกรมงานให้สามารถดึงข้อมูลที่ต้องการไปใช้ได้ โดยไม่ต้องคำนึงถึงตำแหน่งที่เก็บข้อมูล (Location) หรือ format ของข้อมูล

รูปที่จะแสดงต่อไปนี้เป็นตัวอย่างของระบบ data base ของสถาบันการเงินแห่งหนึ่ง สำหรับรายละเอียดของ hierarchical ในที่นี้แสดงเฉพาะด้านเงินให้กู้ยืมที่มีหลักประกันจำนองเท่านั้น



การใช้ data base มีทั้งผลดีและผลเสีย จึงควรพิจารณาปัจจัยต่อไปนี้ให้รอบคอบก่อนนำมาใช้ดังนี้

ประโยชน์ของการใช้ data base

(1) ลดความซ้ำซ้อนของข้อมูล ในระบบแฟ้มข้อมูลแบบเก่าที่ประกอบด้วยแฟ้มข้อมูลหลายชนิด (multiple file system) จะมีข้อมูลรายการเดียวกันแยกเก็บไว้ในแฟ้มข้อมูลต่าง ๆ ซ้ำกันหลายแฟ้ม ทำให้มีปัญหาในการปรับปรุงแก้ไขข้อมูล เนื่องจากต้องแก้ไขข้อมูลที่อยู่ในแฟ้มเหล่านี้ทุกแฟ้มเมื่อข้อมูลเปลี่ยนแปลงไป ส่วนในระบบ data base จะเก็บข้อมูลแต่ละรายการไว้เพียงแห่งเดียว การแก้ไขข้อมูลย่อมกระทำเพียงครั้งเดียวลดความยุ่งยากในการแก้ไขข้อมูลซ้ำซาก และประหยัดเนื้อที่ในการเก็บข้อมูล

(2) สามารถแยกตัวโปรแกรมออกจากข้อมูลได้อย่างอิสระ ในการเขียนโปรแกรมแบบเก่า จำเป็นต้องกำหนด format และ character ของข้อมูลที่อยู่ใน storage ทุกโปรแกรม แต่ในระบบ data base จะแบ่งแยกหน้าที่ในการเก็บรักษาข้อมูลมิให้ปะปนกับการใช้ข้อมูลโดยเด็ดขาด ดังนั้นจึงสามารถเปลี่ยนแปลงแก้ไขหรือขยายระบบข้อมูลได้โดยไม่ต้องแก้ไขโปรแกรมงาน นอกจากนี้โปรแกรมต่าง ๆ จะถือเอาตัวข้อมูลที่เกี่ยวข้องที่เก็บไว้ (content) เป็นหลักแทนที่จะใช้ตำแหน่งที่เก็บข้อมูล (location) เป็นหลักตามแบบเก่า ซึ่งจะช่วยอำนวยความสะดวกในการนำงานไปประมวลผลกับคอมพิวเตอร์เครื่องอื่น

(3) ช่วยกำหนดมาตรฐานของข้อมูล และเอกสาร โดยอาศัย data dictionary ซึ่งมีพนักงานชั้นบริหารที่ทำหน้าที่ควบคุมดูแลงาน data base เป็นผู้ควบคุมมาตรฐาน

(4) สามารถเชื่อมโยงข้อมูลให้สัมพันธ์กันได้โดยไม่มีขีดจำกัด เนื่องจากในระบบ data base มี pointer เป็นตรรกะช่วยให้สามารถใส่แฟ้มข้อมูลต่าง ๆ ร่วมกันได้ โดยอาศัยความสัมพันธ์ของข้อมูลที่สร้างขึ้นมาอย่างไม่มีขีดจำกัด ทำให้มีข้อมูลมากพอที่จะป้อนให้กับโปรแกรมต่าง ๆ ได้

(5) ประหยัดค่าใช้จ่ายในการปรับปรุงแก้ไขโปรแกรม โดยลดความยุ่งยากในการแบ่งเนื้อที่ในการเก็บข้อมูล และลดขั้นตอนในการดึงข้อมูลออกไปใช้

ผลเสียของการใช้ data base

(1) มีความยุ่งยากในการจัดทำข้อมูล เนื่องจากข้อมูลที่เก็บไว้ในระบบจะต้องเป็นข้อมูลที่ถูกต้องและสมบูรณ์ มีความสัมพันธ์เชื่อมโยงกันทุกรายการ โดยปกติในระบบนี้จะเก็บข้อมูลแต่ละรายการไว้เพียงแห่งเดียวสามารถนำข้อมูลเหล่านี้ไปประมวลผลซ้ำกันได้หลายงาน หากข้อมูลรายการใดผิดพลาด จำนวนผู้ใช้ข้อมูลที่ผิดพลาดย่อมมากกว่าการเก็บข้อมูลในระบบเก่า นอกจากนี้หากจะต้องขยายระบบ data base ให้ใหญ่ขึ้นย่อมเพิ่มปัญหาในการเชื่อมโยงข้อมูลให้สัมพันธ์กันมากขึ้น เพราะต้องกำหนดความสัมพันธ์ให้แน่ชัดและข้อมูลทุกรายการต้องเป็นไปตามนัยที่กำหนดไว้อย่างแท้จริงตลอดเวลาด้วย

(2) สร้างปัญหาในการตรวจสอบ การตรวจสอบระบบ data base จำเป็นต้องอาศัยเทคนิคที่ทันสมัย

(3) ไม่ได้ช่วยประหยัดค่าใช้จ่ายอย่างแท้จริง แม้ว่าในระบบนี้จะลดค่าใช้จ่ายในการปรับปรุงแก้ไขโปรแกรมลงบ้างก็ตาม แต่จะมีค่าใช้จ่ายอื่น ๆ มาทดแทนดังนี้

(3.1) ค่าใช้จ่ายในการพัฒนา DBMS

(3.2) ค่าใช้จ่ายในการติดตั้งอุปกรณ์ที่ใช้ร่วมกับคอมพิวเตอร์เพิ่มขึ้น

(3.3) ค่าใช้จ่ายในการวางแผนงานเพิ่มขึ้น

(3.4) ค่าใช้จ่ายในการจัดระบบควบคุมใหม่ที่ละเอียดมากกว่าเดิม ซึ่งจะต้องใช้พนักงานที่ทำงานด้านโปรแกรมที่มีความรู้สูงขึ้น

(3.5) ค่าใช้จ่ายในการปรับปรุงแก้ไขเพื่อให้ทันกับเทคนิคที่ทันสมัย

(4) มีความยุ่งยากในการปรับปรุงการรักษาปลอดภัย โดยปกติแฟ้มข้อมูลที่ใช้ประมวลผลสำหรับงานต่าง ๆ ในระบบ data base จะติดตั้งไว้กับเครื่องคอมพิวเตอร์ ส่วนใน batch system ซึ่งเป็นระบบจัดเก็บข้อมูลแบบเก่าจะถอดแฟ้มข้อมูลที่ไม่ได้ใช้ในการประมวลผลออกจากเครื่องคอมพิวเตอร์เก็บรักษาไว้ในห้องเก็บแฟ้มข้อมูล (library) แต่ข้อแตกต่างที่สำคัญที่สุดคือความรับผิดชอบในการเก็บรักษาไว้ในห้องเก็บแฟ้มข้อมูล หากเป็น batch system หน่วยงานที่ใช้ข้อมูลจะเป็นเจ้าของแฟ้มข้อมูลที่ใช้ในการประมวลผล ส่วนในระบบ data base หรือ DBMS หน่วยงานต่าง ๆ ที่ใช้ข้อมูลจะร่วมกันเป็นเจ้าของแฟ้มข้อมูลไม่มีผู้รับผิดชอบโดยตรงหน้าที่ในการควบคุมดูแลจึงตกเป็นของส่วนกลาง ซึ่งได้แก่พนักงานชั้นบริหารที่รับผิดชอบงาน data base ซึ่งควบคุมอยู่แล้วเป็นผู้พิจารณาการใช้ข้อมูลในการประมวลผล เช่น การบวก การลบข้อมูลทั้ง การขยายข้อมูลเพิ่มขึ้น หรืออนุญาตให้ผู้ใช้อ่านข้อมูลได้เพียงอย่างเดียว เป็นต้น ในกรณีที่มีการใช้ข้อมูลผ่านเครื่อง terminal หลาย ๆ เครื่อง หากมีการป้อนข้อมูลที่อยู่ใน field ต่าง ๆ ควรพิจารณาควบคุมการทำงาน เพื่อป้องกันมิให้ข้อมูลถูกเปิดเผยและเสียหายด้วย

(5) แฟ้มข้อมูลอาจถูกทำลายได้ง่าย เนื่องจากข้อมูลในระบบนี้มีขนาดใหญ่ยากแก่การทำสำเนา และมีค่าใช้จ่ายสูง การปรับปรุงแก้ไขข้อมูล (update) ในระบบ data base จะทำให้แฟ้มข้อมูลเก่าถูกทำลาย เป็นปัญหาในการจัดทำแฟ้มข้อมูลสำรอง (back up) ซึ่งจะต้องจัดทำเก็บไว้ทุกระยะ ดังนั้นในการจัดทำแฟ้มข้อมูลสำรองควรเลือกทำเฉพาะรายการสำคัญจำเป็นต้องทำจริง ๆ เท่านั้น และยอมให้รายการที่มีสาระสำคัญน้อยถูกทำลายสูญหายไปบ้าง

(6) software อาจทำงานผิดพลาด หรือทำงานช้าลงทั้งนี้เพราะ ในระบบ data base มีองค์ประกอบมากมาย โอกาสที่ software จะเสียหายย่อมมากขึ้น และขั้นตอนในการทำงานจะเพิ่มขึ้นด้วย ทำให้ต้องใช้เวลาในการประมวลผลมากขึ้น

6.9 การรักษาความปลอดภัยในระบบ data base

การรักษาความปลอดภัยในที่นี้หมายถึง data security และ privacy ซึ่ง data security คือการป้องกันมิให้ข้อมูลถูกเปิดเผย หรือถูกแก้ไข หรือถูกทำลายโดยบุคคลอื่นที่ไม่ได้รับมอบหมายให้ปฏิบัติงานโดยจงใจหรือไม่ก็ตาม ส่วน privacy เป็นสิทธิของบุคคลและองค์การในการพิจารณาตัดสินใจด้วยตนเอง ในการกำหนดเวลา วิธีการขอบเขต การใช้ข้อมูลและการเสนอข้อมูลแก่ผู้ที่เกี่ยวข้อง

6.9.1 หลักการรักษาความปลอดภัยในระบบ data base

การรักษาความปลอดภัยในระบบ data base มีดังนี้

- (1) มีการป้องกันมิให้ข้อมูลถูกไฟไหม้ หรือถูกโจรกรรม หรือถูกทำลายโดยวิธีอื่นๆ
- (2) สามารถสร้างข้อมูลขึ้นใหม่ได้ เพื่อป้องกันการถูกทำลาย หรือสูญหายโดยจงใจหรือไม่ก็ตาม
- (3) สามารถตรวจสอบหาสาเหตุที่ข้อมูลสูญหายได้โดยฉับพลัน

- (4) มีการป้องกันมิให้ผู้เขียนโปรแกรมสามารถหลีกเลี่ยงมาตรการที่ใช้ในการควบคุมที่วางไว้ในระบบได้
- (5) มีการมอบอำนาจให้แก่ผู้ใช้ data base ให้แนชดก่อนยินยอมให้ใช้ข้อมูล
- (6) มีการจัดระบบให้สามารถตรวจสอบการปฏิบัติงานของผู้ที่ได้รับมอบอำนาจให้ใช้ข้อมูลได้
- (7) มีการบันทึกการปฏิบัติงานของผู้ที่ได้รับมอบอำนาจให้ใช้ข้อมูลเก็บไว้ในระบบโดยอัตโนมัติ เพื่อให้สามารถตรวจสอบการปฏิบัติที่น่าสงสัยหรือเกินอำนาจที่ได้รับมอบหมายได้

6.9.2 การปฏิบัติไม่ชอบ

การปฏิบัติไม่ชอบในระบบ data base อาจมากกว่าการประมวลผลในระบบเก่า ซึ่งพอสรุปได้ดังนี้

- (1) จงใจปฏิบัติไม่ชอบภายในระบบ โดย

(1.1) ยินยอมให้ผู้เขียนโปรแกรมใช้ "trapdoor" หรือ "window" หลีกเลี่ยงมาตรการควบคุมที่วางไว้ในระบบ เพื่อความคล่องตัวในการใช้โปรแกรม โดยเฉพาะอย่างยิ่งในระบบ data base ที่ซับซ้อน และมีการสลับเปลี่ยนโปรแกรมที่ใช้ในการประมวลผล จึงเป็นจุดอ่อนในการป้องกันการใช้ข้อมูลในระบบโดยไม่ชอบ

(1.2) ยินยอมให้ dump ข้อมูล โดยให้คอมพิวเตอร์พิมพ์ข้อมูลที่อยู่ใน core storage บางส่วนออกมาทั้งหมด เพื่อดึงเอาข้อมูลที่ใช้ในการควบคุมเช่นรหัสที่ใช้ในการประมวลผล (code) และรหัสลับประจำตัวผู้รับมอบอำนาจ (password) ออกมาใช้ประโยชน์ (การปฏิบัติดังกล่าวมีประโยชน์ในการเริ่มรับจ้างใหม่ เนื่องจากข้อมูลที่อยู่ในแฟ้มต่าง ๆ รวมทั้งรหัสควบคุมการป้อนข้อมูลเข้าสู่ระบบจะถูกเผยออกมาให้เห็น) ดังนั้นมาตรการที่ใช้ในการปกปิดข้อมูลลับย่อมไม่ได้ผลหากยังปล่อยให้มีการ dump ข้อมูลโดยตรงจาก storage ที่เก็บข้อมูล

(1.3) ผู้รับมอบอำนาจใช้รหัสในการประมวลผล หรือรหัสลับประจำตัว หรือรหัสอื่น ๆ ของผู้รับมอบอำนาจคนอื่น ซึ่งผิดไปจากรหัสที่ตนได้รับมอบอำนาจ

- (2) จงใจปฏิบัติไม่ชอบภายนอกระบบ โดย

(2.1) เก็บรายงานที่ได้จากการประมวลผลที่ทิ้งไว้ตามถังขยะ เพื่อค้นหารหัสหรือข้อมูลลับอื่น ๆ

(2.2) จารกรรมข้อมูลจากคีย์บอร์ดหรือที่พิมพ์ข้อความเข้าคอมพิวเตอร์ เพื่อค้นหารหัสหรือข้อมูลลับอื่น ๆ

- (3) ปฏิบัติไม่ชอบโดยบังเอิญ

(3.1) ระบบสื่อสารไม่ทำงานตามปกติ ย่อมทำให้ข้อมูลที่ป้อนเข้าสู่ระบบ data base ผิดพลาดด้วย

(3.2) หากคอมพิวเตอร์หรือโปรแกรมทำงานผิดพลาด ย่อมทำให้ระบบรักษาความปลอดภัยที่อยู่ภายในระบบทำงานผิดพลาดด้วย ตัวอย่างเช่น ในช่วงที่คอมพิวเตอร์ทำงานผิดปกติ หรือในช่วงที่พื้นตัวกลับคืนมาสู่สภาพการทำงานตามปกติ ข้อมูลลับต่าง ๆ เช่น รหัสลับประจำตัวผู้รับมอบอำนาจอาจถูกพิมพ์พร้อมกับข้อมูลอื่นที่ถูก dump ออกมาด้วย

6.9.3 การควบคุมทางด้าน software (Program Control)

การควบคุมโปรแกรมและข้อมูลในระบบ data base จะต้องรัดกุมเช่นเดียวกับการควบคุมการใช้เครื่อง terminal และเนื่องจากการปฏิบัติงานในระบบนี้ไม่สามารถนำวิธีการทางด้าน library มาควบคุมการใช้โปรแกรมและแฟ้มข้อมูลได้เหมือนระบบเก่า จึงจำเป็นต้องใช้วิธีการอื่นมาทดแทนดังนี้

(1) มอบอำนาจหน้าที่ในการปฏิบัติงาน (authorization controls) โดยกำหนดขอบเขตการ access ในระบบโดยทั่วไป การใช้โปรแกรม แฟ้มข้อมูล หรือ record แต่ละชนิด รวมทั้งหน้าที่อันพึงปฏิบัติ (เช่น การอ่านข้อมูล การเขียนข้อมูล และการแก้ไขเพิ่มเติมข้อมูล เป็นต้น)

(2) ควบคุมการประมวลผล (processing controls) โดยทำ edit checks เพื่อตรวจสอบความถูกต้องของข้อมูล เช่น ทดสอบความถูกต้องของข้อมูลตามหลักเกณฑ์ที่วางไว้ (validity tests) ทดสอบความสมเหตุสมผล (reasonableness tests) ทดสอบว่าข้อมูลอยู่ในช่วงที่กำหนดไว้หรือไม่ (range and limit tests) และการสร้างข้อมูลที่สามารถติดตามตรวจสอบได้ (audit trail)

6.9.4 การควบคุมในระบบ Data Base

ในระบบเก่า ส่วนใหญ่จะใช้วิธีการควบคุมอุปกรณ์ และเครื่องมือที่ใช้ในการประมวลผลซึ่งเป็น physical control แต่ในระบบ data base จะใช้วิธีการดังนี้

(1) ควบคุมข้อมูลที่ป้อนเข้าสู่ระบบ (control over input) โดย

(1.1) มีกุญแจเปิดเครื่อง terminal

(1.2) มีกุญแจตัดต่อคู่สายโทรศัพท์ที่พ่วงเข้าคอมพิวเตอร์

(1.3) กำหนดรหัสประจำเครื่อง terminal และระเบียบการใช้เครื่อง

(1.4) กำหนดรหัสประจำตัวผู้รับมอบอำนาจให้ใช้เครื่อง terminal และหน้าที่ในการ

ปฏิบัติงาน

(1.5) กำหนดรหัสลับประจำตัวผู้รับมอบอำนาจ

(2) ควบคุมโปรแกรมและข้อมูลภายในระบบ (internal software controls) โดย

(2.1) ห้ามใช้โปรแกรมบางโปรแกรม (program locks)

(2.2) ห้ามใช้แฟ้มข้อมูลบางแฟ้ม (file locks)

(2.3) กำหนด record หรือ field ที่ยอมให้ผู้ใช้อ้างอิงข้อมูลบางคนอาจนำข้อมูลไปใช้ได้ภายในขอบเขตที่จำกัด (record or field locks)

(2.4) ควบคุมการทดสอบผลลัพธ์ที่ได้จากการประมวลผล (test of result)

สำหรับแฟ้มข้อมูลที่ล้นมาก ควรเก็บไว้ใน disk pack แยกต่างหากจากแฟ้มอื่นในระบบ data base เมื่อจะประมวลผล จึงจะนำออกมาใช้และการเก็บรักษาแฟ้มข้อมูลดังกล่าวจะต้องมีมาตรการรักษาความปลอดภัยที่เข้มงวดและรัดกุมอย่างยิ่ง

ในกรณีที่ข้อมูลมีปริมาณมากไม่สามารถจัดทำสำเนาข้อมูลสำรอง (back up) เก็บไว้ใช้ยามฉุกเฉินได้ หรือระบบงานที่วางไว้ไม่สามารถจัดทำแฟ้มข้อมูลสำรองควบคู่ไปกับแฟ้มข้อมูลใช้งานจริงได้ก็อาจจัดทำข้อมูลสำรองไว้ใช้ได้ โดยการ dump แฟ้มข้อมูลที่ถูกทำลาย เนื่องจากการปรับปรุงแก้ไขไว้ทุกระยะ พร้อมกับรายการ

ที่เกี่ยวข้องที่เกิดขึ้นในระหว่างที่ทำการ dump ซึ่งจะสามารถนำข้อมูลที่ได้จากการ dump ครั้งหลังสุดไปสร้างแฟ้มข้อมูลขึ้นมาใหม่ได้ แต่อย่างไรก็ดีในระบบ data base ขนาดใหญ่ ตามปกติจะไม่มีการจัดทำสำเนาไว้ทั้งระบบ ดังนั้นจึงจำเป็นต้องแบ่งข้อมูลออกเป็น 2 ประเภท คือ ประเภทที่มีการเปลี่ยนแปลงได้และประเภทที่ไม่มีการเปลี่ยนแปลง โดยจะจัดทำสำเนาเฉพาะข้อมูลที่มีการเปลี่ยนแปลงเท่านั้น สำหรับในกรณีที่ข้อมูลมีการเปลี่ยนแปลงบ่อย ๆ ยกแก่การจัดทำสำเนา ก็อาจปรับปรุงแก้ไขข้อมูล (update) จากรายการที่เกิดขึ้น (transaction record) ได้โดยง่าย ในระบบ realtime จำเป็นอย่างยิ่งที่จะต้องจัดทำแฟ้มข้อมูลสำรองเก็บไว้ พร้อมทั้งจะนำออกใช้แทนแฟ้มข้อมูลที่อาจถูกทำลายได้ทันที แต่อย่างไรก็ดีแฟ้มข้อมูลที่ใช้งานจริงและแฟ้มข้อมูลสำรอง ทั้งสองชนิดอาจถูกทำลายได้หากโปรแกรมมีข้อผิดพลาด ดังนั้น จึงต้องใช้เทคนิคไม่ให้มีการทำลายข้อมูลเมื่อโปรแกรมทำงานผิดพลาด เพื่อให้สามารถสร้างข้อมูลขึ้นมาใหม่จากแฟ้มสำเนาข้อมูลเก่าได้

6.9.5 หน้าที่ของหัวหน้างาน data base

หัวหน้างาน data base โดยทั่วไปมีหน้าที่เป็นผู้ตัดสินใจหาข้อขัดแย้งและเป็นสื่อกลางในการพัฒนา การใช้ประโยชน์ และการบำรุงรักษา data base นอกจากนี้ยังทำหน้าที่เป็นผู้ประสานงานกับหน่วยงานอื่นในส่วนที่เกี่ยวข้องกับ data base อีกด้วย

สำหรับหน้าที่โดยตรงของหัวหน้างาน data base มีดังนี้

- (1) กำหนดคุณลักษณะทุกชนิดที่อยู่ในระบบ
 - (1.1) ตั้งชื่อข้อมูลทุกชนิดที่อยู่ในระบบ
 - (1.2) จัดทำ data dictionary แสดงรายละเอียดของข้อมูล
 - (1.3) รวบรวมข้อมูลรายการต่าง ๆ เพื่อนำมาจัดกลุ่ม
 - (1.4) สร้างความสัมพันธ์ระหว่างข้อมูลกลุ่มต่าง ๆ อย่างมีเหตุผล
 - (1.5) กำหนดมาตรฐานของ data record และแฟ้มข้อมูล (data file) เพื่อให้ผู้เขียน

โปรแกรมใช้เป็นบรรทัดฐาน

- (1.6) กำหนดระยะเวลาในการเก็บรักษาข้อมูล
- (2) วางระบบ data base
 - (2.1) กำหนดโครงสร้าง (physical structure) ของอุปกรณ์ที่ใช้บันทึกข้อมูล
 - (2.2) พัฒนาวิธีการใช้ data base
 - (2.3) กำหนดวิธีการจัดทำ data base และกำหนดวิธีการปรับปรุงแก้ไข data base

ที่เสียหายให้ถูกต้องดังเดิม สามารถนำไปประมวลผลได้อีก

- (2.4) พัฒนามาตรการรักษาความปลอดภัย
- (3) ดำเนินการสร้างข้อมูล
 - (3.1) สอบหาสาเหตุผิดพลาดของข้อมูลทั้งหมด
 - (3.2) ควบคุมดูแลการจัดทำ data base และการปรับปรุงแก้ไข data base ที่เสียหายให้ถูกต้องดังเดิม สามารถนำไปประมวลผลได้อีก
 - (3.3) ควบคุมดูแลปรับปรุงสายการบังคับบัญชาของหน่วยงาน data base

(3.4) ควบคุมการปรับปรุง และเปลี่ยนแปลงเอกสารที่ใช้ในงาน data base และฝึกอบรมให้ความรู้แก่ผู้ใช้ข้อมูล

(4) รักษาความปลอดภัย

(4.1) สอบสวนการฝ่าฝืนมาตรการรักษาความปลอดภัยที่เกิดขึ้น

(4.2) สอบสวนพฤติกรรมที่น่าสงสัยที่ปรากฏในรายงานการปฏิบัติงานขั้ระดับ

(4.3) แต่งตั้งและมอบอำนาจการปฏิบัติงานตามลำดับชั้น (โดยกำหนดจากตัวบุคคลที่ใช้ข้อมูลเป็นหลัก)

(4.4) กำหนดรหัสลับที่ใช้ในการรักษาความปลอดภัย (security code) รหัสลับประจำตัวผู้รับมอบอำนาจ (password) และรหัสลับอื่น ๆ

(4.5) ตรวจตราการรักษาความปลอดภัย

(4.6) ดำเนินการตรวจสอบการรักษาความปลอดภัยทุกระยะเพื่อทดสอบสมรรถภาพ

หัวหน้างาน data base อาจมีผู้ช่วยอย่างน้อยอีก 1 คน เพื่อช่วยปฏิบัติงานในรายละเอียดหรืออาจแบ่งงานให้พนักงานที่มีตำแหน่งรองลงมาหลาย ๆ คนที่มีอำนาจและหน้าที่เท่า ๆ กันเป็นผู้รับผิดชอบในส่วนที่ตน เกี่ยวข้อง ซึ่งค่อนข้างดีกว่าวิธีแรก เพราะพนักงานที่ได้รับมอบหมายงานดังกล่าว แต่ละคนย่อมมีความสามารถ และแนวคิดต่างกันตามที่ตนถนัดจึงเป็นผู้เหมาะสมในการวางแผนปฏิบัติงาน และการประกอบภารกิจประจำวัน

นอกจากนี้ ควรแบ่งแยกหน้าที่ของหัวหน้างาน data base ให้ชัดเจนด้วย เนื่องจากหัวหน้างาน data base เป็นผู้ควบคุมดูแลการจัดทำข้อมูลที่อยู่ในระบบ ดังนั้นจึงควรห้ามมิให้หัวหน้างาน data base นำข้อมูลที่ตนมีส่วนเกี่ยวข้องในการจัดทำข้อมูลดังกล่าวไปใช้งาน และควรควบคุมหัวหน้างาน data base ในการใช้รายงาน แสดงรายละเอียดของข้อมูลขั้นต้นที่จะนำไปใช้ประมวลผล รวมทั้งเอกสารที่เกี่ยวกับโปรแกรมงานต่าง ๆ ด้วย

6.9.6 การจัดทำ data dictionary

Data dictionary คือบัญชีชื่อข้อมูลกลาง (central catalog) มีรายละเอียดแสดงลักษณะของข้อมูล (data definition) ที่ใช้ในการจัดองค์ประกอบ (organization) และส่วนประกอบอื่น ๆ ดังนี้

(1) มีข้อสนเทศ (information) ที่แสดงว่ามีข้อมูลที่จะนำไปใช้งานได้อยู่จริง

(2) มี format, segment และรายละเอียดอื่น ๆ ที่ใช้เป็นเครื่องมือในการวางระบบ data base

(3) มีรายละเอียดเกี่ยวกับข้อมูลที่ประมวลผลด้วยคอมพิวเตอร์และข้อมูลที่ไม่ได้ประมวลผลด้วยคอมพิวเตอร์ (computerized and non-computerized data) ที่อยู่ในระบบแฟ้มข้อมูลแบบเก่า และในระบบ data base (สำหรับ data dictionary ที่ใช้ในปัจุบัน ตามปกติจะแสดงรายละเอียดเฉพาะในส่วนที่เกี่ยวข้องกับ data base เท่านั้น)

(4) มีรายละเอียดแสดงลักษณะของข้อมูลที่เก็บไว้ และตำแหน่งของหน่วยความจำที่เก็บข้อมูล (physical storage location) และวิธีการนำข้อมูลไปใช้ (data access method)

ในมาตรฐานการปฏิบัติงาน ควรกำหนดตัวบุคคลที่เหมาะสมในการตรวจสอบจัดทำเอกสาร และติดต่อประสานงาน หากมีการเปลี่ยนแปลง Data Dictionary/Directory System (DD/DS) โดย

- (1) มอบอำนาจการเปลี่ยนแปลงการปฏิบัติงานผ่านทางหัวหน้างาน data base
- (2) มอบหมายให้ผู้ใช้ข้อมูลเป็นผู้อนุมัติการเปลี่ยนแปลง
- (3) ปรับปรุงแก้ไขเอกสารของผู้ใช้ข้อมูล
- (4) ทดสอบผลกระทบกระเทือนในการใช้งาน
- (5) สอบทานประสิทธิภาพในการตรวจสอบแบบ audit trail และการควบคุมอื่นๆ

6.9.7 บันทึกการปฏิบัติงานในระบบ data base

ลักษณะที่สำคัญอีกประการหนึ่งของระบบ data base คือ บันทึกการปฏิบัติงานประจำวัน บันทึกการปฏิบัติงานเหล่านี้ควรมีรายละเอียดมากพอที่จะช่วยอำนวยความสะดวกในกรณีที่อุปกรณ์ย่อย ๆ ที่ใช้ร่วมกับคอมพิวเตอร์ (minor-hardware) และ software เกิดขัดข้อง สามารถบอกได้ว่าเพิ่มข้อมูลในระบบ data base เพิ่มได้บ้างที่เสียหายหรือถูกทำลาย นอกจากนี้ควรบันทึกการปฏิบัติงานไว้ทุกรายการ รวมทั้งคำสั่งที่ใช้ในการสั่งการ และข้อความที่พนักงานคอมพิวเตอร์ (operator) ใช้ติดต่อกับคอมพิวเตอร์ในระหว่างการประมวลผลด้วย

บันทึกการปฏิบัติงานประจำวัน (log หรือ journal) ดังกล่าวควรมีข้อมูลที่ช่วยให้สามารถตรวจสอบร่องรอยที่มาของรายการและหาสาเหตุแห่งความผิดพลาดได้ นอกจากนี้ยังสามารถนำข้อมูลที่ได้จากบันทึกดังกล่าวมาใช้ประโยชน์ที่จะช่วยให้ทราบการปฏิบัติงานที่ขัดต่อระเบียบที่สำคัญ ซึ่งอาจชี้ให้เห็นวิธีการหลีกเลี่ยงมาตรการในการรักษาความปลอดภัยด้วย

สำหรับ DBMS ที่ทันสมัย จะบันทึกการปฏิบัติงานดังกล่าวโดยอัตโนมัติ บางระบบผู้ใช้ DBMS อาจพัฒนาให้สามารถบันทึกการปฏิบัติงานโดยอัตโนมัติได้เช่นเดียวกัน นอกจากนี้บางระบบอาจมีการควบคุมโดยตัดระบบการทำงานของอุปกรณ์ที่ใช้ร่วมกับคอมพิวเตอร์ที่ขัดข้องและเปลี่ยนไปใช้อุปกรณ์อื่นให้ทำงานแทน เพื่อให้การทำงานต่อเนื่องกันอย่างเหมาะสมโดยอัตโนมัติ

6.10 การตรวจสอบ การจัดทำข้อมูลที่น่าเชื่อถือได้

วัตถุประสงค์

1. เพื่อตรวจสอบวิธีการควบคุมและระเบียบปฏิบัติต่าง ๆ ในการจัดทำข้อมูลที่มีอยู่จริงของสถาบันการเงิน ทั้งในส่วนของระบบอัตโนมัติและส่วนที่ใช้พนักงานปฏิบัติข้อมูล โดยเริ่มตั้งแต่การสร้างข้อมูลขั้นต้น การประมวลผลด้วยเครื่องคอมพิวเตอร์ จนถึงการจัดส่งข้อมูลผลลัพธ์ ทั้งนี้เพื่อให้แน่ใจว่ามีการปฏิบัติตามมาตรการต่าง ๆ ที่กำหนดไว้ ซึ่งเป็นผลให้ข้อมูลของสถาบันถูกต้องและเชื่อถือได้

2. เพื่อประเมินและประสานงานตรวจสอบเกี่ยวกับงบแสดงฐานะการเงินและการดำเนินงานต่าง ๆ ของสถาบันการเงินที่ผู้ตรวจสอบด้าน Financial Examination ใช้ในการตรวจสอบว่า น่าเชื่อถือได้เพียงใดและสมควรจะใช้เทคนิคในการตรวจสอบอย่างไรจึงจะรัดกุมและได้ผลดีในทางปฏิบัติงานตรวจสอบ

แผนงานการตรวจสอบโดยย่อ

1. คู่มือ ระเบียบ คำสั่งและวิธีการที่ใช้ในปัจจุบันเกี่ยวกับ
 - การจัดทำข้อมูลทุกขั้นตอน
 - การควบคุมและตรวจสอบการปฏิบัติตามระเบียบปฏิบัติต่าง ๆ
 - การแบ่งแยกและมอบหมายอำนาจหน้าที่ในการปฏิบัติงาน
2. สังเกตการประมวลข้อมูลทั้งในระบบอัตโนมัติและระบบที่ใช้พนักงานปฏิบัติ
3. การพิสูจน์ยอดของการรวบรวมข้อมูลขั้นตอนต่าง ๆ และการแก้ไขรายการผิดพลาดหรือรายการที่เครื่องไม่ยอมรับ เพื่อพิจารณาว่ามีหลักฐานสำหรับการตรวจสอบและมีการควบคุมเหมาะสมเพียงพอตลอดวงจรการผลิตหรือไม่
4. วิธีการเก็บรักษา การควบคุมภายในเกี่ยวกับข้อมูลและโปรแกรมปฏิบัติงานและระบบงาน
5. มาตรการในการรักษาความปลอดภัยข้อมูลต่าง ๆ

7. การรักษาความปลอดภัย

สถาบันการเงินควรมีการรักษาความปลอดภัยเพื่อให้ความคุ้มครองป้องกัน และลดความเสียหายของทรัพย์สินที่เกี่ยวข้องระบบคอมพิวเตอร์จากเหตุการณ์ที่เกิดขึ้นโดยไม่คาดฝัน หรือโดยจงใจ โดยจัดให้มี

- 7.1 แผนการรักษาความปลอดภัย
- 7.2 การรักษาความปลอดภัยอาคารสถานที่
- 7.3 การรักษาความปลอดภัยตู้নিরภัยและห้องมั่นคง
- 7.4 การป้องกันความเสียหายเนื่องจากภัยต่าง ๆ โดยทั่วไป
- 7.5 การรักษาความปลอดภัยแฟ้มข้อมูล
- 7.6 การจัดระบบสำรอง
- 7.7 การประกันภัย

7.1 แผนการรักษาความปลอดภัย

ธนาคารควรมีแผนการรักษาความปลอดภัยที่สามารถให้ความคุ้มครองป้องกันข้อมูล บุคคลผู้ปฏิบัติงาน และทรัพย์สินต่าง ๆ ที่ใช้ในการประมวลผลให้ได้รับความปลอดภัยหรือแก้ไขปัญหาทรัพย์สินที่เสียหายให้กลับคืนสู่สภาวะปกติใช้งานได้โดยไม่ขาดตอนและผู้บริหารระดับสูงควรพิจารณากำหนดวิธีการปฏิบัติงานในกรณีฉุกเฉินเตรียมไว้ตลอดเวลา นอกจากนี้ควรให้ผู้ตรวจสอบดำเนินการประเมินขอบเขตและการปฏิบัติตามแผนการรักษาความปลอดภัยด้วย

7.2 การรักษาความปลอดภัยอาคารสถานที่

การรักษาความปลอดภัยอาคารสถานที่ตั้งศูนย์คอมพิวเตอร์อาจแบ่งได้เป็น 2 ระยะ คือ

(1) **ระยะก่อนการก่อสร้างอาคารสถานที่** ควรคำนึงถึงสภาพแวดล้อมเป็นสำคัญ เช่น ไม่ควรอยู่ในบริเวณที่อาจเกิดเพลิงไหม้ได้ง่าย น้ำท่วมถึง บริเวณที่มีบุคคลที่ไม่เกี่ยวข้องกับการประมวลผลทั้งภายในและภายนอกเดินผ่านพลุกพล่าน บริเวณที่ไม่ปลอดภัยจากการเกิดฟ้าผ่าหรือถูกรบกวนจากคลื่นวิทยุ คลื่นแม่เหล็กและคลื่นไฟฟ้า

(2) **ระยะหลังการก่อสร้างอาคารสถานที่** หากตัวอาคารที่ตั้งศูนย์คอมพิวเตอร์แยกต่างหากจากหน่วยงานอื่น การรักษาความปลอดภัยจะต้องกระทำให้ทั่วถึงโดยรอบบริเวณ แต่ถ้าศูนย์คอมพิวเตอร์อยู่ภายในอาคารเดียวกับหน่วยงานอื่น การรักษาความปลอดภัยจะต้องเน้นที่บริเวณทางเข้าออกของศูนย์คอมพิวเตอร์

7.3 การรักษาความปลอดภัยตู้নিরภัยและห้องมั่นคง

ตู้নিরภัยและห้องมั่นคงที่นำมาใช้เก็บทรัพย์สินในระบบคอมพิวเตอร์ควรใช้ชนิดที่เป็นมาตรฐาน ซึ่งยอมรับกันโดยทั่วไป

7.4 การป้องกันความเสียหายเนื่องจากภัยต่าง ๆ โดยทั่วไป

ควรมีมาตรการป้องกันความเสียหายเนื่องจากอุทกภัย อัคคีภัย การก่อวินาศกรรม การจลาจล กระแสไฟฟ้าขัดข้อง การปฏิบัติที่ไม่เหมาะสมในห้องคอมพิวเตอร์ การทุจริตการจารกรรมและความเสียหายของอุปกรณ์ ฯลฯ โดยการกำหนดขั้นตอนในการปฏิบัติในแต่ละกรณีอย่างชัดเจนเพื่อป้องกันระบบคอมพิวเตอร์ทั้งหมดให้ปลอดภัยหรือเสียหายน้อยที่สุดและสามารถแก้ไขปัญหาหรือความเสียหายที่เกิดขึ้นให้กลับคืนสภาพปกติหรือสร้างระบบใหม่ขึ้นทดแทน ได้อย่างรวดเร็วและไม่ยุ่งยาก

ขอบเขตในการป้องกันไฟในศูนย์คอมพิวเตอร์แต่ละแห่งขึ้นอยู่กับอัตราความเสี่ยงที่คาดว่าพอจะยอมรับได้ ถ้าหากปริมาณที่ใช้คอมพิวเตอร์มีจำนวนมากและ/หรือไม่มีระบบหรืออุปกรณ์สำรองเตรียมไว้สำหรับการปฏิบัติงานในกรณีฉุกเฉินเพียงพอ ก็จำเป็นต้องมีระบบการป้องกันไฟที่ให้ความคุ้มครองหรือมีประสิทธิภาพสูง

7.5 การรักษาความปลอดภัยแฟ้มข้อมูล

ควรกำหนดระเบียบการใช้เครื่องคอมพิวเตอร์ การเก็บรักษา การเคลื่อนย้ายและการควบคุม media ที่ใช้บันทึกข้อมูล เช่น เทป และ disk โดยละเอียดชัดเจน และจะต้องทบทวนระเบียบดังกล่าวให้มีความรัดกุมอยู่เสมอ นอกจากนี้ ผู้ที่จะเข้าไปในห้องคอมพิวเตอร์ได้จะต้องเป็นผู้ได้รับมอบหมายเท่านั้น หากเป็นบุคคล ภายนอกควรตรวจสอบก่อนอนุญาตให้เข้าไปและควรห้าม computer operator ใช้เอกสารที่เกี่ยวข้องกับระบบงานและโปรแกรม สำหรับผู้ที่เกี่ยวข้องกับการจัดทำระบบงานและโปรแกรมก็ควรห้ามทำหน้าที่แทน computer operator ด้วย

7.6 การจัดระบบสำรอง

ในระบบประมวลผลข้อมูลด้วยคอมพิวเตอร์ ควรจัดให้มีระบบสำรองไว้ทดแทนระบบที่ใช้ปฏิบัติงาน ในยามฉุกเฉิน ซึ่งได้แก่ เครื่องคอมพิวเตอร์ โปรแกรมเอกสารสนับสนุนการปฏิบัติงานทุกชนิดที่จำเป็นต่อการประมวลผล โดยมีวิธีการปฏิบัติงานและแฟ้มข้อมูลเตรียมพร้อมไว้รับเหตุการณ์ที่ไม่คาดฝันที่อาจจะเกิดขึ้นได้ตลอดเวลา

7.7 การประกันภัย

ควรจัดให้มีการประกันภัยเพื่อป้องกันความสูญเสีย ซึ่งอาจเกิดขึ้นจากภัยหรือความเสี่ยงที่ไม่สามารถป้องกันได้ โดยทั่วไปการทำประกันภัยจะคำนึงถึงความสูญเสียทางธุรกิจและผลกระทบข้างเคียงที่เกิดขึ้น อันเนื่องจากภัยนั้นฝ่ายจัดการจะเป็นผู้ประเมินความเสี่ยงภัยและความเสียหายที่อาจเกิดขึ้นโดยเปรียบเทียบกับต้นทุนของการประกันภัย สิ่งที่ต้องพิจารณาในการทำประกันภัย มีดังนี้

- (1) เครื่องคอมพิวเตอร์และอุปกรณ์หรือเครื่องมืออื่น ๆ
- (2) ความซื่อสัตย์ของพนักงาน
- (3) Media ที่เก็บข้อมูลและโปรแกรม
- (4) ค่าใช้จ่ายพิเศษที่อาจเกิดขึ้น
- (5) การหยุดชะงักของธุรกิจ
- (6) ข้อผิดพลาดและบกพร่องจากการปฏิบัติงาน
- (7) การสูญหายของข้อมูลในขณะที่เครื่องคอมพิวเตอร์ขัดข้อง
- (8) ความรับผิดชอบที่มีต่อลูกค้า

7.8 การตรวจสอบ การรักษาความปลอดภัย

วัตถุประสงค์

1. เพื่อพิจารณาความเหมาะสมและความเพียงพอในการให้ความคุ้มครองป้องกัน และลดความเสียหายซึ่งอาจเกิดขึ้นกับทรัพย์สิน บุคคล และข้อมูลที่เป็นองค์ประกอบสำคัญในการประมวลผลด้วยคอมพิวเตอร์
2. เพื่อพิจารณาแนวทางแก้ไขและการปฏิบัติของสถาบันการเงินในกรณีที่สถาบันการเงินประสบกับเหตุการณ์ที่มีผลกระทบต่อระบบคอมพิวเตอร์ทั้งโดยตรงหรือโดยทางอ้อม

แผนงานการตรวจสอบโดยย่อ

1. แผนการรักษาความปลอดภัยด้านคอมพิวเตอร์
2. การรักษาความปลอดภัยในบริเวณที่ตั้งศูนย์คอมพิวเตอร์
3. มาตรการในการป้องกันความเสียหายเนื่องจากภัยต่าง ๆ โดยทั่วไปเช่น อุทกภัย อัคคีภัย การก่อวินาศกรรม การจลาจล เป็นต้น
4. การรักษาความปลอดภัยเกี่ยวกับ media ที่เก็บข้อมูลและโปรแกรมเช่น tape และ disk เป็นต้น
5. การจัดระบบสำรอง (backup) เตรียมรับเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้นและวิธีปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน
6. การประกันภัย

8. การประมวลผลโดยอาศัยระบบสื่อสาร

การประมวลผลของระบบคอมพิวเตอร์ในปัจจุบันและในอนาคตมีแนวโน้มที่จะใช้ระบบสื่อสารเข้าช่วยเพื่อกระจายงานออกไปภายนอกศูนย์คอมพิวเตอร์มากยิ่งขึ้น ซึ่งจำเป็นต้องใช้วิธีการควบคุมที่รัดกุมพอสมควร สำหรับเรื่องที่จะกล่าวต่อไปนี้จะเป็นเรื่องทั่วไปเกี่ยวกับการประมวลผลโดยอาศัยระบบสื่อสาร (Teleprocessing) และการควบคุมที่เกี่ยวข้องซึ่งส่วนใหญ่ ณ ที่นี้ได้เน้นในด้านการประมวลผลโดยระบบ On-line เป็นสำคัญ

8.1 การประมวลผลในระบบ On-line

ระบบ On-line คือการนำเครื่องมือสื่อสาร (เช่นโทรศัพท์) มาใช้สำหรับรับส่งข้อมูลระหว่างเครื่อง terminal กับหน่วยประมวลผลกลางคือ CPU การประมวลผลที่นิยมกันในระบบนี้มี 3 แบบ คือ ระบบ inquiry ระบบ memo-post และระบบ realtime ซึ่งการควบคุมในระบบ On-line นี้จะยุ่งยากกว่าการประมวลผลในระบบ batch เพราะต้องจัดให้มีการควบคุมทั้งด้าน software และ hardware ฝ่ายบริหารและฝ่ายตรวจสอบจะต้องศึกษาวิธีการควบคุมที่นำมาใช้ทั้งหมดโดยละเอียดเพื่อให้แน่ใจว่า ระบบการควบคุมดังกล่าวเชื่อถือได้และปลอดภัยต่อการประมวลผล

8.2 การควบคุมการประมวลผลที่ใช้ระบบสื่อสาร

สถาบันการเงินที่มีขายงานในระบบ On-line ควรมีการควบคุมที่เหมาะสมและใช้การได้ตลอดเวลา
ดังนี้

8.2.1 การรักษาความปลอดภัยเกี่ยวกับการใช้เครื่อง terminal

การรักษาความปลอดภัยเกี่ยวกับการใช้เครื่อง terminal ควรกระทำทั้งด้าน hardware และ software

- (1) การควบคุมด้าน hardware ควรดำเนินการตามความเหมาะสมในแต่ละกรณี เช่น
 - (1.1) จัดให้มีกุญแจปิดเปิดเครื่อง terminal
 - (1.2) มีระบบการควบคุม keyboard
 - (1.3) กำหนดหมายเลขคู่สายประจำเครื่อง terminal
 - (1.4) กำหนดรหัสประจำตัวผู้ใช้เครื่อง terminal
 - (1.5) สับเปลี่ยนเส้นทางหรือสายรับส่งข้อมูล
 - (1.6) ทำ multiplexing ในสายรับส่งข้อมูล
 - (1.7) ใช้วิธีการ Synchronous ในการรับส่งข้อมูล
 - (1.8) มีการตรวจสอบแบบ parity checks
 - (1.9) ใช้อุปกรณ์แปลงรูปข้อมูลให้ผิดไปจากรูปเดิม
- (2) ควรใช้ software ในส่วนที่เกี่ยวข้องกับ operating system
 - (2.1) ควบคุมเวลาปิดเปิดเครื่อง
 - (2.2) จัดให้มีการตรวจสอบเพื่อพิสูจน์ตัวผู้ปฏิบัติงาน
 - (2.3) มีวิธีการเรียกข้อมูลกลับมาตรวจสอบโดยอัตโนมัติ
 - (2.4) ทดสอบการปฏิบัติงานของผู้ที่ได้รับมอบอำนาจอยู่เสมอ

- (2.5) จัดให้มีการบันทึกข้อมูลเพื่อประโยชน์ในการรักษาความปลอดภัย (security logs)
- (2.6) ใช้สูตรแปลงรูปข้อมูลให้ผิดไปจากรูปเดิม
- (2.7) มีการบันทึกเวลาปิดเครื่องโดยอัตโนมัติ

การสร้างรหัสลับในการควบคุมและรักษาความปลอดภัย ควรสร้างให้เดาได้ยาก มีการเปลี่ยนแปลงอยู่เสมอ และมีการป้องกันรักษาความปลอดภัยอย่างเข้มงวด เช่น

- เก็บรหัสลับไว้ในที่ที่มีการป้องกันภัย
- ทำรหัสลับที่เก็บไว้ให้มีรูปแบบผิดไปจากเดิม
- หากมีการพิมพ์รหัสลับให้ปรากฏทางเครื่อง terminal ให้พิมพ์ตัวอักษรหรือเครื่องหมายอื่น ๆ ทับเพื่อทำลายมิให้เห็นอีกต่อไป
- ใช้รหัสลับ 2 ชุด เป็นการคุมซ้อน (dual control)
- พิมพ์ข้อความที่ช่วยให้เข้าใจว่าเป็นรหัสลับ เพื่อกลบเกลื่อนรหัสลับที่แท้จริง

8.2.2 การรักษาความปลอดภัยโดยอาศัย log บันทึกเหตุการณ์ที่เกิดขึ้นเพื่อประโยชน์ในการรักษาความปลอดภัย (security and transaction logging)

การประมวลผลในระบบ On-line ควรมี log บันทึกการใช้เครื่องและระบบต่าง ๆ โดยอัตโนมัติ เช่น

- (1) การเข้าไปใช้ระบบโดยไม่ได้รับอนุญาต
- (2) การใช้ข้อมูลเกินอำนาจที่ได้รับมอบหมาย
- (3) รายละเอียดของข้อมูลที่ใช้ประมวลผล
- (4) รายละเอียดของรายการที่ผ่านเครื่อง terminal

8.2.3 การรักษาความปลอดภัยในสายรับส่งข้อมูล (Line Security)

สถาบันการเงินควรจัดให้มีระบบรักษาความปลอดภัยในสายรับส่งข้อมูลตามความเหมาะสม และควรตรวจสอบระบบรักษาความปลอดภัยทุกระยะอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าระบบดังกล่าวยังใช้งานได้อยู่เสมอ

8.2.4 ข้อผิดพลาดในการรับส่งข้อมูล (Transmission Errors)

การรับส่งข้อมูลในระบบคอมพิวเตอร์อาจมีข้อผิดพลาด จึงจำเป็นต้องมีการควบคุมโปรแกรม และข้อมูลสำคัญที่ใช้งานอย่างรัดกุม การควบคุมข้อผิดพลาดในการรับส่งข้อมูล อาจทำได้โดยใช้วิธีการตรวจจับข้อผิดพลาด และ/หรือใช้รหัสในการแก้ไขข้อผิดพลาด แต่ส่วนใหญ่นิยมใช้วิธีแรกมากกว่าวิธีหลัง เพราะวิธีหลังมีค่าใช้จ่ายสูงและไม่สามารถแก้ไขข้อผิดพลาดได้ทุกกรณี วิธีการตรวจจับข้อผิดพลาดที่ใช้กันมากได้แก่วิธีการ check bit และวิธี redundant checking ตรวจสอบนับจำนวนอักขระ (character) หรือ patterns ของ bit ที่รับส่งในแต่ละช่วง

8.2.5 การดิ่งข้อมูลทางสายรับส่งข้อมูล (Line Penetration/Interception)

แม้ว่าการดิ่งข้อมูลทางสายรับส่งข้อมูลไม่อาจจะกระทำได้โดยง่ายแต่ผู้ที่มีความรู้ความสามารถและมีเครื่องมือเพียงพอ อาจทำการเข้าสู่ระบบได้ ทั้งนี้เพราะระบบสื่อสารโดยใช้สายโทรศัพท์รับส่งข้อมูลดังกล่าวไม่มีมาตรการในการรักษาความปลอดภัย ไม่เป็นเครื่องมือป้องกันการกระทำดังกล่าวแต่อย่างใด จึงควรศึกษาวิธีการดิ่งข้อมูลทางสายรับส่งข้อมูลเพื่อหาทางลดภัยที่อาจเกิดขึ้นในแต่ละกรณีให้น้อยลง

8.2.6 การควบคุมสายรับส่งข้อมูล (Line Controls)

สถาบันการเงินควรจัดให้มีการควบคุมสายรับส่งข้อมูลตามความเหมาะสม เช่น

(1) จำกัดตัวผู้ใช้เอกสารเกี่ยวกับระบบงานและการพัฒนาระบบงาน (system design and development) ตลอดจนสถานที่ติดตั้งอุปกรณ์โทรศัพท์ และส่วนประกอบอื่น ๆ ที่เกี่ยวกับ teleprocessing communication lines ควรสอดส่องดูแลผู้ที่ไม่มีหน้าที่เกี่ยวข้องที่เข้ามาวนเวียนใกล้ ๆ กับเครื่องมือสื่อสารที่อาจถูกจารกรรมได้ง่ายอย่างใกล้ชิด นอกจากนี้ไม่ควรทำเครื่องหมายหรือจัดสายโทรศัพท์ที่ใช้ในงาน on-line ให้เป็นระเบียบเพื่อป้องกันการลักลอบพ่วงสายหรือพยายามทำลายสายส่งข้อมูล

(2) กลบเกลื่อนรหัสลับประจำตัวผู้รับมอบอำนาจในการใช้ข้อมูลและข้อมูลที่รับส่งในระบบ เพื่อป้องกันมิให้ผู้อื่นที่ไม่มีสิทธิใช้ข้อมูล ดัดหน้านำไปใช้ประโยชน์ได้โดยง่ายและเพื่อให้เกิดความมั่นใจในการรับส่งข้อมูล

(3) จัดให้มีการพิสูจน์ตัวผู้ใช้ข้อมูล (authentication checks) เพื่อให้สถานีรับส่งข้อมูลมั่นใจว่าข้อมูลที่รับและส่งนั้นถูกต้อง จึงจำเป็นต้องใช้รหัสสอดแทรกเข้าไปในข้อมูล โดยอาศัยหมายเลขลำดับของข้อมูลเป็นหลัก และอาจมีการคำนวณ หรือใช้สูตรคณิตศาสตร์ร่วมกับข้อมูลที่ใช้ในการพิสูจน์ตัวผู้ใช้ข้อมูลด้วย

(4) จัดให้มีผู้เชี่ยวชาญด้านสื่อสาร (communications specialists) ตรวจสอบระบบโทรศัพท์หรือติดตั้งเครื่องมือตรวจสอบการใช้เครื่อง terminal อยู่เสมอ

(5) ใช้ callback procedures โดยกำหนดตัวผู้ใช้ข้อมูลไว้ในระบบและใช้เทคนิคการส่งสัญญาณขอใช้ระบบ (sign-on) หรือรหัสลับแสดงตัวผู้รับมอบอำนาจ (password) และกำหนดสถานที่ตั้งเครื่อง terminal ที่แน่นอน ป้องกันการตัดเครื่อง terminal ออกจากระบบคอมพิวเตอร์ นอกจากนี้ ยังอาจใช้ data facility ทำหน้าที่ส่งข้อมูลกลับคืนไปยังสถานที่ส่งข้อมูลเพื่อยืนยันความถูกต้องของข้อมูลอีกครั้งหนึ่ง

(6) มีการให้หมายเลขลำดับกำกับข้อมูลที่ได้รับจากเครื่อง terminal ทุกรายการพร้อมทั้ง unique identifier เช่น มีการใส่วันที่และเวลาลงในระบบตัวเลขที่ใช้อ้างอิงเป็นต้น

(7) มีระบบตัดการใช้เครื่อง terminal ที่พ่วงกับระบบคอมพิวเตอร์โดยอัตโนมัติ ในกรณีที่เครื่อง terminal ขาดการติดต่อกับระบบคอมพิวเตอร์เป็นระยะเวลาเกินกว่าเวลาที่กำหนดไว้

(8) ควบคุมเวลาใช้เครื่อง terminal โดยกำหนดให้ผู้ใช้ข้อมูลที่ได้รับมอบอำนาจใช้เครื่อง terminal ได้ตามเวลาที่กำหนดไว้เท่านั้น หากต้องการใช้เครื่อง terminal นอกเวลาที่กำหนดไว้ต้องได้รับอนุมัติจากผู้บังคับบัญชาก่อนเสมอ

8.2.7 การควบคุมการปฏิบัติงาน (Applicability of Controls)

การควบคุมการปฏิบัติงานในระบบ on-line แบบ inquiry และแบบ inquiry/memo/post ส่วนใหญ่จะใช้วิธีควบคุมเครื่อง terminal ซึ่งเป็นการรักษาความปลอดภัยแบบ physical security เช่น ใช้กุญแจล็อกเครื่อง terminal เมื่อเลิกใช้งานมีการควบคุมแฟ้มข้อมูลที่ได้จากเครื่อง terminal และข้อมูลต่าง ๆ ที่พนักงานแต่ละคนหรือแต่ละกลุ่มรับผิดชอบอย่างใกล้ชิด นอกจากนี้ ควรมี inquiry file บันทึกการใช้เครื่อง terminal บัญชีที่มีการประมวลผล และชนิดของ inquiry ที่ติดต่อกับคอมพิวเตอร์ด้วย

ในกรณีที่ เป็น memo-post system ซึ่งใช้วิธีบันทึกรายการคู่ duplicate file หรือ dummy file ควรระบุชนิดและจำนวนรายการที่เกิดขึ้นพร้อมทั้ง operator ที่ปฏิบัติงานสำหรับการป้องกันและควบคุมในระบบ realtime ซึ่งมีลักษณะการทำงานคล้ายกับระบบ on-line inquiry และ memo-post แต่สามารถบันทึกการเข้าสู่ live file ที่ใช้งานอยู่ได้ทันทีนั้น ควรพิจารณาหาวิธีการรักษาความปลอดภัยด้วยความระมัดระวังก่อนที่จะนำระบบนี้มาใช้งาน การควบคุมบางอย่างที่ใช้ในระบบ inquiry และ memo-post อาจนำมาใช้ในระบบ realtime ได้เป็นอย่างดี

8.3 การเตรียมอุปกรณ์และวิธีการปฏิบัติงานกรณีระบบสื่อสารขัดข้อง

(Teleprocessing Backup)

ศูนย์คอมพิวเตอร์ที่มีประสิทธิภาพจะมีแผนพัฒนาและแผนการจัดเตรียมอุปกรณ์และวิธีการปฏิบัติงานที่จำเป็นและต่อเนื่อง โดยมีให้งานหยุดชะงัก ในกรณีระบบการรับส่งข้อมูลทางสายโทรศัพท์หรือระบบสื่อสารอื่น ๆ ขัดข้อง โดยจัดทำข้อตกลงในการเปลี่ยนแปลงหรือย้ายสถานที่ในการประมวลผลชั่วคราว

สถาบันการเงินควรมี back up ที่เกี่ยวกับระบบสื่อสารดังนี้

(1) มีการเข้าสู่สายโทรศัพท์สำรองไว้ทดแทนคู่สายที่ใช้ปฏิบัติงานที่อาจขัดข้องและเครื่อง terminal ที่ใช้ควรเป็นชนิดที่มีหน่วยความจำ สามารถใช้กับโปรแกรมและเก็บข้อมูลไว้ในเครื่องรอการติดต่อสื่อสารกับระบบคอมพิวเตอร์ขนาดใหญ่เพื่อถ่ายข้อมูลได้ นอกจากนี้ ในกรณีที่ระบบสื่อสารหรือคอมพิวเตอร์เสียเป็นเวลานาน ก็ สามารถนำข้อมูลที่บันทึกเก็บไว้ใน media (ส่วนใหญ่เป็นเทป) ไปประมวลผลด้วยคอมพิวเตอร์ที่ศูนย์ประมวลผลหรือที่อื่นในระบบธรรมดาแบบ batch ได้

(2) ในกรณีที่ศูนย์ประมวลผลได้รับความเสียหายมากอาจต้องประมวลผลในระบบธรรมดาแบบ batch ซึ่งพนักงานอาจไม่เคยชินต่อระบบนี้ จึงควรมีแผนงานเตรียมไว้ด้วย

(3) ควรคำนึงถึงวิธีการใช้เครื่อง terminal อย่างมีประสิทธิภาพในกรณีที่ hardware หรือ software ทำงานขัดข้องบางส่วน แต่ไม่เสียทั้งระบบ เพื่อให้ terminal ที่ใช้การได้ทำงานต่อไป และกำหนดวิธีการปรับปรุงแก้ไข ข้อมูลที่ประมวลผลไม่เสร็จ หรือผิดพลาดให้ถูกต้องด้วย นอกจากนี้ ควรมีระบบปิดเครื่อง terminal ที่ทำงานขัดข้องและเปลี่ยนไปใช้อุปกรณ์ที่ยังทำงานได้โดยอัตโนมัติด้วย

8.4 การตรวจสอบ การประมวลผลโดยอาศัยระบบสื่อสาร

วัตถุประสงค์

1. เพื่อให้แน่ใจว่าข้อมูลทางการเงินที่ได้จากการประมวลผลโดยอาศัยระบบสื่อสาร มีความถูกต้อง สมบูรณ์ และเชื่อถือได้
2. เพื่อตรวจสอบการรักษาความปลอดภัยของข้อมูลที่ได้รับส่งภายในศูนย์ประมวลผลและระหว่าง ศูนย์ประมวลผลของสถาบันการเงินกับสำนักงานสาขาต่าง ๆ มีความเหมาะสมเพียงพอหรือไม่
3. เพื่อประเมินความพร้อมและการแก้ไขปัญหาและอุปสรรคของสถาบันการเงินในกรณีที่มีการประมวลผลโดยอาศัยระบบสื่อสารมีปัญหาเกิดขึ้น

แผนงานการตรวจสอบโดยย่อ

1. รายละเอียดเกี่ยวกับเครื่องมือและอุปกรณ์ที่ใช้ในระบบสื่อสารข้อมูล
2. ระบบงานที่ประมวลผลโดยอาศัยระบบสื่อสาร
3. คู่มือปฏิบัติงานของ operator ในห้องคอมพิวเตอร์เฉพาะงานที่ใช้ระบบสื่อสารช่วยในการประมวลผล
4. คู่มือปฏิบัติงานหรือคู่มือการใช้เครื่องรับส่งข้อมูล (เครื่อง terminal) สำหรับพนักงาน
5. การรักษาความปลอดภัยในระบบสื่อสารข้อมูล
6. การจัดระบบสำรอง (back-up) สำหรับการประมวลผลโดยอาศัยระบบสื่อสารเพื่อเตรียมรับเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น และวิธีปฏิบัติงานประมวลผลเฉพาะงานที่อาศัยระบบสื่อสารในกรณีเกิดเหตุฉุกเฉิน
7. ทดสอบข้อมูลบางประเภทผ่านระบบสื่อสารที่เกี่ยวข้อง

9. การใช้บริการด้านคอมพิวเตอร์ภายนอกสถาบันการเงิน

ในกรณีที่สถาบันการเงินตัดสินใจเลือกใช้บริการด้านการประมวลผลของศูนย์บริการคอมพิวเตอร์ (service bureau) โดยองค์กรอื่นภายนอกสถาบันการเงิน ซึ่งเจ้าหน้าที่ผู้ปฏิบัติงานมิได้เป็นพนักงานของสถาบันการเงิน และมีได้อยู่ภายใต้การควบคุมดูแลของสถาบันการเงิน เพื่อให้งานด้านการประมวลผลเชื่อถือได้ จึงควรกำหนดหน้าที่และความรับผิดชอบบางประการไว้ในสัญญาการใช้บริการ และควรร่วมกันหาวิธีการควบคุมที่เหมาะสมมาใช้

9.1 การคัดเลือกศูนย์บริการคอมพิวเตอร์

ควรพิจารณาศูนย์บริการคอมพิวเตอร์ที่มีชื่อเสียงดีในด้านการปฏิบัติงานและการให้บริการที่อยู่ไม่ไกลจากสถาบันการเงินจนเกินไปเพื่อความสะดวกและประหยัดค่าใช้จ่ายในการติดต่อสื่อสาร และควรพิจารณาเรื่องอื่น ๆ ประกอบด้วย เช่น ผู้ที่เป็นเจ้าของกิจการ ฐานะความมั่นคงทางการเงิน ความเข้าใจในธุรกิจการสถาบันการเงินของศูนย์บริการฯ โปรแกรมที่ใช้ประมวลผล อัตราและวิธีคิดค่าบริการ นอกจากนี้สถาบันการเงินควรเข้าชมการปฏิบัติงานของศูนย์บริการคอมพิวเตอร์ เพื่อดูการปฏิบัติงานทั่ว ๆ ไปประกอบการพิจารณาและซักถามเพิ่มเติมจนเป็นที่พอใจ เพื่อให้แน่ใจว่าศูนย์บริการฯ จะสามารถให้บริการต่อไปได้ แม้จะเกิดภาวะผันแปรทางเศรษฐกิจ และควรติดต่อสอบถามบรรดาค่าของศูนย์บริการฯ นั้น ๆ ในเรื่องความถูกต้องของงาน การตรงต่อเวลา และการให้ความร่วมมือเพื่อเป็นการยืนยันคุณภาพในการปฏิบัติงาน

9.2 การทำสัญญาระหว่างสถาบันการเงินกับศูนย์บริการคอมพิวเตอร์

ในการทำสัญญาระหว่างสถาบันการเงินกับศูนย์บริการคอมพิวเตอร์จะต้องระบุความรับผิดชอบของทั้งสองฝ่ายเกี่ยวกับการให้บริการด้านคอมพิวเตอร์ให้ครบถ้วนเพื่อป้องกันปัญหาที่อาจเกิดขึ้นภายหลัง โดยควรระบุเรื่องต่อไปนี้ไว้ในสัญญา

- (1) ระบุงานที่สถาบันการเงินใช้บริการ ระยะเวลาในการประมวลผล และข้อมูลที่ปรากฏในรายงานต่าง ๆ
 - (2) หลักเกณฑ์ในการคำนวณค่าบริการ
 - (3) กำหนดเวลาในการรับส่งงานระหว่างศูนย์บริการฯ กับสถาบันการเงิน
 - (4) กำหนดความรับผิดชอบในการตรวจสอบ รวมทั้งสิทธิของสถาบันการเงินและองค์กรที่มีหน้าที่กำกับและตรวจสอบธนาคารพาณิชย์ ในการส่งตัวแทนเข้าไปตรวจสอบการทำงานของศูนย์บริการฯ ฐานะของกิจการ และการดำเนินงานที่จำเป็น
 - (5) การจัดมาตรการและอุปกรณ์ที่จำเป็นในการปฏิบัติงานและการป้องกันข้อมูลที่อาจเสียหาย เพื่อให้แน่ใจว่าศูนย์บริการฯ สามารถประมวลผลได้ทันตามกำหนดแม้จะมีเหตุฉุกเฉินเกิดขึ้น
 - (6) ความรับผิดชอบในการขนส่งเอกสาร ข้อมูลต่าง ๆ ระหว่างสถาบันการเงินกับศูนย์บริการฯ ถ้าศูนย์บริการฯ เป็นผู้รับผิดชอบ ศูนย์บริการฯ จะต้องทำการประกันภัย ให้คุ้มกับค่าเสียหายที่อาจเกิดขึ้นด้วย
 - (7) ควรประกันภัยข้อมูลที่อาจสูญหายเนื่องจากเจ้าหน้าที่ปฏิบัติงานผิดพลาดและบกพร่องละเลยไม่ปฏิบัติตามหน้าที่ด้วย
 - (8) การรักษาความลับของข้อมูล
 - (9) กรรมสิทธิ์ในโปรแกรมและเอกสารที่ใช้ปฏิบัติงานที่เกี่ยวข้อง
 - (10) กรรมสิทธิ์ในแฟ้มข้อมูล (data files)
 - (11) การเปลี่ยนแปลงราคาค่าบริการและวิธีการยกเลิกสัญญา รวมทั้งระยะเวลาที่ใช้ในการเปลี่ยนแปลงข้างต้น
 - (12) ลำดับความสำคัญในการปฏิบัติงาน
 - (13) กำหนดให้ศูนย์บริการฯ แจ้งการเปลี่ยนแปลงระบบงานใด ๆ ที่จะมีผลกระทบต่อวิธีการปฏิบัติงานให้สถาบันการเงินทราบ
 - (14) กำหนดให้ศูนย์บริการฯ ส่งงบการเงินของตนไปให้สถาบันการเงินทุกงวดการบัญชีเพื่อวิเคราะห์ฐานะทางการเงินของศูนย์บริการฯ
- หากมีข้อตกลงอื่นนอกจากที่กล่าวข้างต้น ทั้งสองฝ่ายควรร่วมกันพิจารณาข้อตกลงนั้น โดยละเอียด

9.3 การควบคุมการปฏิบัติงาน

เมื่อสถาบันการเงินเลือกใช้บริการด้านคอมพิวเตอร์จากสถาบันภายนอก ศูนย์บริการฯ จะทำหน้าที่ควบคุมการปฏิบัติงานแทนสถาบันการเงิน การควบคุมโดยทั่วไปส่วนใหญ่จะคล้ายกับการควบคุมในระบบเดิม (manual system) โดยมีหลักการโดยทั่วไปดังนี้

(1) การแบ่งแยกหน้าที่

การแบ่งแยกหน้าที่เป็นการควบคุมขั้นพื้นฐานเพื่อป้องกันการทุจริตที่อาจเกิดขึ้นจากพนักงานผู้ปฏิบัติงาน ตัวอย่างในการแบ่งแยกหน้าที่ได้แก่

(1.1) กำหนดไม่ให้พนักงานคนใดคนหนึ่งมีอำนาจอนุมัติแต่เพียงผู้เดียวหรือทำงานคนเดียวทุกขั้นตอน

(1.2) สับเปลี่ยนหน้าที่ของพนักงานหมุนเวียนกันไปเป็นประจำ และกำหนดให้พนักงานในแต่ละหน้าที่ลาหยุดพักผ่อนเป็นระยะ ๆ

(1.3) ควรใช้วิธีการคุมซ้อน (dual control) เช่นเดียวกับที่ใช้ในการทำงานตามระบบเดิม

(2) การควบคุมภายใน

การควบคุมภายในมี 3 ชนิดคือ การควบคุมด้านการบริหารงาน การควบคุมด้านการเงิน และการควบคุมด้านอื่น ๆ ที่ไม่เกี่ยวกับการเงิน

(2.1) การควบคุมด้านการบริหารงาน คือการตรวจตราดูแลการปฏิบัติงานประจำวัน และรายงานที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ เพื่อให้เกิดประสิทธิภาพในการปฏิบัติงานโดยอาศัย exception report และวิธีการควบคุมที่เหมาะสม

(2.2) การควบคุมด้านการเงิน เป็นการควบคุมเพื่อให้แน่ใจว่ารายการด้านการเงินที่เกิดขึ้นมีการอนุมัติตามขั้นตอนที่กำหนดไว้ เช่น มีการควบคุมและตรวจสอบยอดทั้งก่อนและหลังการประมวลผล มีระเบียบการจัดส่งรายงาน การแก้ไขข้อมูลและการควบคุมดูแลโดยใช้ exception report ต่าง ๆ

(2.3) การควบคุมด้านอื่นๆที่ไม่เกี่ยวกับการเงินจะใช้เฉพาะกรณีที่ไม่มีตัวเงินเข้ามาเกี่ยวข้องเช่น ชื่อหรือที่อยู่ของลูกค้า เป็นต้น โดยดำเนินการควบคุมและตรวจสอบจนแน่ใจว่าข้อมูลเหล่านี้ถูกต้องพร้อมที่จะใช้งานได้

(3) การสื่อสารข้อมูล

สถาบันการเงินจะต้องมีความรับผิดชอบในการควบคุมบางส่วนด้านการติดต่อสื่อสารรับส่งข้อมูลกับศูนย์บริการคอมพิวเตอร์ ทั้งด้าน software hardware และการสื่อสารในระบบ on-line โดยจัดให้มีการควบคุมตามความเหมาะสม เช่น

(3.1) การควบคุมโดยวิธีกำหนดตัวผู้ปฏิบัติงาน การควบคุมตามวิธีนี้จะอนุญาตให้พนักงานที่ได้รับมอบหมายเท่านั้นที่จะใช้ระบบคอมพิวเตอร์ได้ โดยกำหนดตัวพนักงานและเครื่อง Terminal ที่จะใช้ด้วยการให้ผู้ปฏิบัติงานมีกุญแจสำหรับเปิดปิดเครื่อง มีบัตรอนุญาต (machine readable badge) หรือมีรหัสลับประจำตัวผู้ที่ได้รับมอบอำนาจให้ใช้เครื่อง (password) ฯลฯ

(3.2) การควบคุมการใช้ข้อมูล คือ การกำหนดให้ผู้ปฏิบัติงานใช้ข้อมูลเฉพาะส่วนที่ตนมีหน้าที่เกี่ยวข้องเท่านั้น

(3.3) การควบคุมโดยการจำกัดอำนาจในการบันทึกรายการ (Restricted Transaction) สำหรับรายการที่มีความสำคัญเป็นพิเศษควรกำหนดให้พนักงานชั้นบริหารเป็นผู้บันทึกรายการด้วยตนเอง ตัวอย่างเช่น การล้างรายการ การแก้ไขจำนวนเงินในบัญชีของลูกค้า หรือการออกยอดคงการเงินประจำวัน เป็นต้น

(3.4) การควบคุมการปฏิบัติงานโดยอาศัย exception reports

(4) การตรวจสอบ

เพื่อป้องกันความเสียหายที่อาจเกิดจากการควบคุมและวิธีการปฏิบัติงานที่ขาดประสิทธิภาพ การปฏิบัติงานที่ผิดพลาดไม่ถูกต้องตามระเบียบและการทุจริตของพนักงานสถาบันการเงินควรจัดให้มีการตรวจสอบงานด้านคอมพิวเตอร์ทุกระยะ ส่วนวิธีการและเทคนิคในการตรวจสอบนั้นขึ้นอยู่กับความรู้ความสามารถของผู้ตรวจสอบและการพิจารณาตัดสินใจของสถาบันการเงิน ซึ่งได้ให้แนวทางไว้แล้วในเรื่องการตรวจสอบภายใน

9.4 การป้องกันและเก็บรักษาข้อมูลของสถาบันการเงิน

สถาบันการเงินมีมาตรการป้องกันและเก็บรักษาข้อมูลที่ส่งไปประมวลผล ณ ศูนย์บริการคอมพิวเตอร์ ดังนี้

- (1) ให้ศูนย์บริการฯ จัดทำ data files program files และ documentation ชุดสำรอง โดยสถาบันการเงินจะต้องตรวจสอบการปฏิบัติงานด้านนี้และตรวจดูอุปกรณ์ที่ใช้ในการประมวลผลชุดสำรองของศูนย์บริการฯ ด้วย เพื่อให้อยู่ในสภาพพร้อมที่จะใช้งานในกรณีที่ศูนย์บริการฯ ดำเนินงานไม่ได้
- (2) จัดทำสำเนาข้อมูลทุกรายการ ก่อนที่จะส่งไปประมวลผลเป็นการป้องกันข้อมูลสูญหายหรือถูกทำลาย และจัดให้มีการประกันภัยการขนส่งข้อมูลดังกล่าวด้วย
- (3) เพื่อความปลอดภัยของข้อมูลชุดสำคัญ ๆ สถาบันการเงินควรกำหนดให้ศูนย์บริการฯ เก็บแฟ้มข้อมูลชุดสำรองดังกล่าวไว้ที่อื่นภายนอกที่ทำการ

9.5 การพิจารณาฐานะการเงินของศูนย์บริการคอมพิวเตอร์

การที่ศูนย์บริการคอมพิวเตอร์เกิดเหตุขัดข้องไม่สามารถให้บริการได้ติดต่อกันเป็นเวลานานหรือต้องหยุดให้บริการย่อมจะก่อให้เกิดความเสียหายแก่สถาบันการเงินได้ ดังนั้นสถาบันการเงินที่เลือกใช้บริการด้านการประมวลผลจากภายนอกจึงควรเตรียมการแก้ปัญหาไว้ล่วงหน้า เช่น

- (1) กำหนดให้ศูนย์บริการฯ แจ้งล่วงหน้า 60-120 วัน ก่อนสัญญาจะครบกำหนด เพื่อให้สถาบันการเงินมีเวลาพอที่จะติดต่อและเปลี่ยนไปใช้บริการที่อื่น
- (2) กำหนดให้ศูนย์บริการฯ เตรียมแผนการป้องกันล่วงหน้าในกรณีที่อาจประสบภัยพิบัติต่าง ๆ โดยให้เก็บรักษาแฟ้มข้อมูลและโปรแกรมชุดสำรองไว้ที่อื่น และสำรองเวลาประมวลผลไว้ที่ศูนย์ประมวลผลแห่งอื่นที่ใช้อุปกรณ์ในการประมวลผลทดแทนกันได้
- (3) ขอบการเงินของศูนย์บริการฯ จากผู้สอบบัญชีมาวิเคราะห์อย่างละเอียดและควรเตรียมหาทางเลือกไว้หากฐานะการเงินของศูนย์บริการฯ ไม่มั่นคงหรือเลวลง

9.6 การตรวจสอบ การใช้บริการด้านคอมพิวเตอร์ภายนอกสถาบันการเงิน

วัตถุประสงค์

1. เพื่อให้แน่ใจว่าข้อมูลที่ได้จากการประมวลผลของศูนย์บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน มีความถูกต้องสมบูรณ์ และเชื่อถือได้
2. เพื่อตรวจสอบการรักษาความปลอดภัยและการรักษาความลับเกี่ยวกับข้อมูลต่าง ๆ ที่สถาบันการเงินให้ศูนย์บริการคอมพิวเตอร์ภายนอกสถาบันการเงินประมวลผล
3. เพื่อให้แน่ใจว่าสถาบันการเงินสามารถดำเนินธุรกิจต่อไปได้ แม้ศูนย์บริการคอมพิวเตอร์ภายนอกสถาบันการเงินจะต้องหยุดประมวลผลด้วยเหตุใด ๆ ก็ตาม
4. เพื่อวิเคราะห์ฐานะทางการเงินของผู้ให้บริการทางด้านคอมพิวเตอร์เพื่อให้แน่ใจว่าผู้บริการสามารถให้บริการได้ตลอดไป โดยไม่ก่อให้เกิดความเสียหายแก่ผู้ใช้บริการ

แผนงานการตรวจสอบโดยย่อ

1. สัญญาการใช้บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน
2. รายชื่อผู้ถือหุ้นรายใหญ่ กรรมการบริหาร และเจ้าหน้าที่ชั้นบริหารของศูนย์บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน
3. งบการเงินของศูนย์บริการคอมพิวเตอร์ที่สถาบันการเงินใช้บริการ
4. รายชื่อลูกค้าอื่นของศูนย์บริการคอมพิวเตอร์ที่สถาบันการเงินใช้บริการ
5. ทดสอบข้อมูลและตรวจสอบระบบงาน และเอกสารที่เกี่ยวข้องบางประเภทที่สถาบันการเงินใช้บริการจากศูนย์คอมพิวเตอร์ภายนอกสถาบันการเงิน
6. การควบคุมการรับและการส่งเอกสารข้อมูลระหว่างสถาบันการเงินกับศูนย์บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน



6

มาตรฐานการสอบบัญชีของไทยใน
ส่วนที่เกี่ยวข้องกับคอมพิวเตอร์

- ฉบับที่ 28
- ฉบับที่ 29
- ฉบับที่ 36

มาตรฐานการสอบบัญชี ฉบับที่ 28

สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย

เรื่อง การสอบบัญชี ในกรณีที่ธุรกิจใช้คอมพิวเตอร์

1. วัตถุประสงค์เพื่อให้แนวทางเพิ่มเติมเกี่ยวกับการสอบบัญชีในกรณีที่ธุรกิจใช้คอมพิวเตอร์ประมวลผลข้อมูลทางการเงินในส่วนที่เป็นสาระสำคัญไม่ว่าธุรกิจนั้นจะดำเนินการประมวลผลข้อมูลเองหรือให้บุคคลภายนอกดำเนินการ ทั้งนี้ เพื่อให้การสอบบัญชีเป็นไปตามมาตรฐานการสอบบัญชีที่รับรองทั่วไปยิ่งขึ้น อย่างไรก็ตาม มาตรฐานการสอบบัญชีฉบับนี้มีได้ครอบคลุมถึงการกำหนดวิธีการและเทคนิคในการตรวจสอบที่ผู้สอบบัญชีจะต้องใช้กับธุรกิจที่ใช้คอมพิวเตอร์
2. การที่ธุรกิจใช้คอมพิวเตอร์ในการประมวลผลข้อมูลทางการเงินนั้นไม่ได้ทำให้วัตถุประสงค์และขอบเขตของการสอบบัญชีเปลี่ยนแปลงไป แต่การใช้คอมพิวเตอร์ดังกล่าว จะทำให้วิธีการประมวลผลข้อมูลและการจัดเก็บข้อมูลทางการเงินเปลี่ยนแปลงไปซึ่งอาจมีผลให้ธุรกิจต้องใช้ระบบการควบคุมภายในที่แตกต่างไปจากเดิมก่อนที่มีการใช้คอมพิวเตอร์ ดังนั้นวิธีการศึกษาระบบบัญชีและประเมินประสิทธิภาพของการควบคุมภายในที่เกี่ยวข้องเพื่อกำหนดชนิดเวลา และขอบเขตการตรวจสอบของผู้สอบบัญชีจะต้องเปลี่ยนแปลงไปให้เหมาะสมกับธุรกิจที่ใช้คอมพิวเตอร์ด้วย

ความรู้และความชำนาญ

3. ในการสอบบัญชีธุรกิจที่ใช้คอมพิวเตอร์ ผู้สอบบัญชีต้องมีความรู้และความชำนาญเกี่ยวกับเครื่องคอมพิวเตอร์และอุปกรณ์โปรแกรม และระบบการประมวลผลข้อมูลอย่างเพียงพอ ทั้งนี้ขึ้นอยู่กับความยุ่งยากซับซ้อนของระบบบัญชีที่ใช้คอมพิวเตอร์นั้น
4. ผู้สอบบัญชีที่มีความรู้ความชำนาญทางคอมพิวเตอร์ จะสามารถเข้าใจถึงผลที่เปลี่ยนแปลงไปอันเนื่องมาจากการที่ธุรกิจนำคอมพิวเตอร์มาใช้ ซึ่งจะช่วยในการวางแผนงานสอบบัญชี การกำหนดวิธีการศึกษาระบบบัญชีและประเมินประสิทธิภาพของการควบคุมภายใน การกำหนดขั้นตอนและวิธีการของการสอบบัญชีตลอดจนการนำเครื่องคอมพิวเตอร์มาช่วยในการสอบบัญชี
5. ผู้สอบบัญชีจะต้องมีความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์เพียงพอที่จะตรวจสอบธุรกิจที่ใช้คอมพิวเตอร์ มิฉะนั้นจะต้องใช้ผู้ชำนาญซึ่งเป็นบุคคลอื่นช่วยในการตรวจสอบ

การใช้บุคคลอื่นช่วยตรวจสอบ

6. ผู้สอบบัญชีจะต้องรับผิดชอบในการแสดงความเห็นต่อการเงินในกรณีที่ได้อบรมหมายงานตรวจสอบโดยทั่ว ๆ ไปบางส่วนให้แก่บุคคลอื่น เช่น ผู้ช่วย ผู้ช่วยผู้เชี่ยวชาญหรือผู้สอบบัญชีอื่น ในกรณีของการใช้บุคคลอื่นซึ่งเป็นผู้ชำนาญตรวจสอบกิจการที่ใช้คอมพิวเตอร์ ผู้สอบบัญชีก็มีความรับผิดชอบเช่นเดียวกันดังนั้นผู้สอบบัญชีจึงต้องมีความรู้ทางคอมพิวเตอร์เพียงพอที่จะมอบหมายงานควบคุมดูแลและสอบทานงานที่มอบหมายให้บุคคลอื่นดังกล่าว หรือที่จะพิจารณาให้แน่ใจว่าขอบเขตของการปฏิบัติงานและผลงานนั้นเป็นไปตามวัตถุประสงค์ของตนแล้ว

7. ด้วยเหตุนี้ ถ้าธุรกิจใช้คอมพิวเตอร์ประมวลผลข้อมูลทางการเงินในส่วนที่เป็นสาระสำคัญและมีผลอย่างมากต่อการควบคุมภายในของธุรกิจ ผู้สอบบัญชีไม่ควรใช้ผลงานของผู้เชี่ยวชาญทางด้านคอมพิวเตอร์โดยไม่ผ่านการพิจารณาหรือสอบทานของตนก่อนที่จะนำผลงานนั้นมาเป็นข้อมูลในการแสดงความเห็นต่อการเงิน

การวางแผนงาน

8. ในการวางแผนงานสอบบัญชี ผู้สอบบัญชีจะต้องรวบรวมข้อมูลเกี่ยวกับระบบคอมพิวเตอร์อาทิเช่น
 - 8.1 การจัดองค์การและการแบ่งสายงานในหน้าที่ที่เกี่ยวข้องกับระบบการประมวลผลข้อมูล
 - 8.2 ขอบเขตของการใช้งานของคอมพิวเตอร์ในธุรกิจ
 - 8.3 ลักษณะของคอมพิวเตอร์และอุปกรณ์พร้อมทั้งโปรแกรม
 - 8.4 วิธีการประมวลผลข้อมูลของระบบงานที่มีสาระสำคัญต่อการเงินรวมทั้งวิธีการจัดเก็บข้อมูลและนโยบายการรักษาข้อมูล
 - 8.5 โครงการปัจจุบันของธุรกิจเกี่ยวกับการจัดทำระบบใหม่หรือการแก้ไขเปลี่ยนแปลงระบบที่ใช้อยู่ในปัจจุบัน
9. ผู้สอบบัญชีจะต้องมีความรู้เกี่ยวกับการควบคุมภายในของระบบการประมวลผลข้อมูลโดยคอมพิวเตอร์ การควบคุมภายในของธุรกิจที่ต้องใช้คอมพิวเตอร์แบ่งได้ 2 ลักษณะ ดังนี้
 - 9.1 การควบคุมภายในทั่วไป ได้แก่ การควบคุมที่เกี่ยวกับกิจกรรมของหน่วยงานคอมพิวเตอร์
 - 9.2 การควบคุมภายในเฉพาะระบบงาน ได้แก่ การควบคุมภายในซึ่งเกี่ยวกับความสมบูรณ์และถูกต้องของข้อมูลในแต่ละระบบงาน
10. ผู้สอบบัญชีต้องพิจารณาเรื่องต่างๆ ในวรรคที่ 8 และ 9 เพื่อใช้ในการวางแผนงานสอบบัญชี เช่น
 - 10.1 การวางแผนเพื่อสอบทานการปฏิบัติงานของระบบคอมพิวเตอร์ว่าควรจะใช้วิธีการและเทคนิคในการตรวจสอบใด เมื่อไร และในส่วนไหนของระบบ
 - 10.2 การประเมินหาจุดอ่อนของระบบการประมวลผลข้อมูลซึ่งอาจเกิดข้อผิดพลาด หรือระบบผิดปกติได้
 - 10.3 การพิจารณาระดับความเชื่อถือเกี่ยวกับการควบคุมต่าง ๆ ในการประเมินประสิทธิภาพการควบคุมภายในทั้งหมดของธุรกิจ
 - 10.4 การวางแผนการใช้คอมพิวเตอร์มาช่วยในการปฏิบัติงานสอบบัญชี
 - 10.5 การวางแผนการใช้บุคลากรที่มีความสามารถเฉพาะด้านคอมพิวเตอร์ในกรณีที่จำเป็น

หลักฐานการสอบบัญชี

11. การใช้คอมพิวเตอร์ในการประมวลผลข้อมูลจะมีผลต่อการทดสอบการปฏิบัติตามระบบ และการทดสอบความถูกต้องของรายการบัญชีเพื่อให้ได้มาซึ่งหลักฐานที่เพียงพอในหลาย ๆ ด้านด้วยกันดังนี้
 - 11.1 ผู้สอบบัญชีจะต้องใช้คอมพิวเตอร์มาช่วยในการปฏิบัติงานสอบบัญชี เนื่องจากลักษณะบางประการของระบบคอมพิวเตอร์ เช่น

11.1.1 รายการที่ไม่มีเอกสารอ้างอิง เช่น การสั่งซื้อโดยการป้อนข้อมูลทางจอภาพและไม่มี การจัดทำเอกสารประกอบทำให้ผู้สอบบัญชีไม่สามารถทราบรายการนั้น ๆ กับเอกสารได้ หรือการกำหนดอัตราส่วนลด ไว้ในโปรแกรม ทำให้ผู้สอบบัญชีไม่สามารถตรวจสอบหลักฐานการอนุมัติการให้ส่วนลดของแต่ละรายการได้ เป็นต้น

11.1.2 รายการที่ไม่มีหลักฐานให้ตรวจสอบได้ด้วยตาทำให้ผู้สอบบัญชีไม่สามารถตรวจสอบได้ ว่ารายการดังกล่าวได้บันทึกบัญชีไว้อย่างไร

11.1.3 การจัดเก็บข้อมูลในรูปแฟ้มสารแม่เหล็ก ซึ่งจะนำข้อมูลมาใช้ได้โดยคอมพิวเตอร์เท่านั้น

11.2 ระยะเวลาในการเก็บรักษาข้อมูลในรูปแฟ้มสารแม่เหล็ก ซึ่งอาจมีระยะเวลาจำกัดผู้สอบบัญชีจะ ต้องวางแผนการปฏิบัติงานและแจ้งให้ลูกค้าทราบล่วงหน้า ถ้าต้องการให้มีการเก็บรักษาแฟ้มข้อมูลใด ๆ นานกว่าปกติ เพื่อตรวจสอบและใช้เป็นหลักฐานการสอบบัญชี

11.3 การทดสอบรายการเพื่อให้ได้มาซึ่งหลักฐานการสอบบัญชี และการประเมินผลของหลักฐานนั้น ๆ อาจมีประสิทธิภาพมากขึ้นเมื่อใช้คอมพิวเตอร์ช่วยในการปฏิบัติงาน เช่น

11.3.1 การใช้คอมพิวเตอร์ทำให้สามารถตรวจสอบรายการทุกรายการในแฟ้มสารแม่เหล็ก แทนการส่งตัวอย่างจากแฟ้มโดยเสียค่าใช้จ่ายในจำนวนที่เท่ากันหรือน้อยกว่า

11.3.2 การใช้โปรแกรมวิเคราะห์เปรียบเทียบและแสดงอัตราส่วนที่ผิดปกติเพื่อการสอบทาน ซึ่งจะใช้เวลาน้อยกว่าการคำนวณด้วยมือ

ระบบบัญชีและการควบคุมภายใน

12. ในการวางระบบบัญชีสำหรับธุรกิจที่ใช้คอมพิวเตอร์ ผู้บริหารจะต้องคำนึงถึงการควบคุมภายในที่ สอดคล้องกับลักษณะของการประมวลผลข้อมูล การควบคุมภายในดังกล่าวหมายถึงการควบคุมภายในทั่วไปและการ ควบคุมภายในเฉพาะระบบงาน ดังนั้น ในการสอบบัญชีผู้สอบบัญชีจะต้องพิจารณาถึงความเพียงพอและความเชื่อถือได้ ของระบบการควบคุมภายในทั้งสองประเภท พร้อมทั้งที่มีต่อการประมวลผลข้อมูลทั้งหมดไม่ว่าจะเป็นส่วนที่ปฏิบัติด้วย มือหรือคอมพิวเตอร์

วันถือปฏิบัติ

13. มาตรฐานการสอบบัญชี ฉบับที่ 29 เรื่อง การสอบบัญชีในกรณีที่ธุรกิจใช้คอมพิวเตอร์ให้เริ่มถือ ปฏิบัติกับการตรวจสอบงบการเงินสำหรับงวดหรือปีสิ้นสุดในหรือหลังวันที่ 30 มิถุนายน 2533 เป็นต้นไป

มาตรฐานการสอบบัญชี ฉบับที่ 29
สมาคมบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย
เรื่อง การประเมินประสิทธิภาพการควบคุมภายใน

กรณีการใช้คอมพิวเตอร์

1. มาตรฐานการปฏิบัติงานข้อ 5 ของประกาศ ก.บช.ฉบับที่ 19 (พ.ศ. 2518) เรื่อง มาตรฐานการสอบบัญชี กำหนดให้ผู้สอบบัญชีต้องประเมินประสิทธิภาพการควบคุมภายในของกิจการที่ตรวจสอบเพื่อกำหนดขอบเขตการปฏิบัติงานให้รัดกุมและเหมาะสม คณะอนุกรรมการมาตรฐานการสอบบัญชี ของสมาคมบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทยได้ออกมาตรฐานการสอบบัญชี ฉบับที่ 18 เรื่องการประเมินประสิทธิภาพการควบคุมภายใน เพื่อให้ผู้สอบบัญชีใช้เป็นแนวทางในการปฏิบัติตามมาตรฐานดังกล่าวอย่างไรก็ดี ในปัจจุบัน มีการนำคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลทางการเงินเพื่อจัดทำบัญชีและงบการเงินมาก ดังนั้นผู้สอบบัญชี ซึ่งตรวจสอบงบการเงินที่ได้จากการประมวลผลข้อมูลทางการเงินโดยคอมพิวเตอร์จึงจำเป็นต้องประเมินประสิทธิภาพระบบควบคุมภายในของกิจการที่ใช้คอมพิวเตอร์ด้วย มาตรฐานการสอบบัญชีฉบับนี้มีวัตถุประสงค์ที่จะให้แนวทางในการประเมินประสิทธิภาพดังกล่าว

2. เมื่อกิจการใช้คอมพิวเตอร์ในการประมวลผลข้อมูลทางการเงินอย่างมีสาระสำคัญต่อการตรวจสอบไม่ว่าจะเป็นคอมพิวเตอร์ชนิดใด ขนาดใด และไม่ว่ากิจการนั้นจะดำเนินการประมวลผลข้อมูลเอง หรือมอบหมายบุคคลภายนอกดำเนินการให้ ก็ถือว่ากิจการนั้นได้ใช้คอมพิวเตอร์แล้วตามความหมายของมาตรฐานการสอบบัญชีฉบับนี้ ในการประเมินประสิทธิภาพการควบคุมภายในของกิจการดังกล่าว เพื่อประโยชน์ในการตรวจสอบผู้สอบบัญชีจะต้องพิจารณาผลกระทบของการใช้คอมพิวเตอร์ประมวลผลข้อมูลทางการเงินที่มีต่อระบบบัญชีและการควบคุมภายในเสมอ

3. แนวทางในมาตรฐานการสอบบัญชีฉบับนี้กำหนดไว้สำหรับใช้กับกิจการที่ใช้คอมพิวเตอร์โดยทั่ว ๆ ไป การนำมาตรฐานการสอบบัญชีฉบับนี้ไปใช้จะต้องปรับปรุงให้เข้ากับลักษณะเฉพาะของการใช้คอมพิวเตอร์ในแต่ละธุรกิจด้วยตัวอย่างเช่น การควบคุมภายในทุกชนิดที่ควรกำหนดให้มีขึ้นเมื่อมีการใช้คอมพิวเตอร์ประมวลผลข้อมูลย่อมไม่เหมาะที่จะใช้กับธุรกิจขนาดเล็กหรือธุรกิจที่ใช้เพียงไมโครคอมพิวเตอร์ ในการประเมินผลข้อมูลเท่านั้น เป็นต้น นอกจากนี้เมื่อการประมวลผลข้อมูลกระทำโดยบุคคลภายนอกการพิจารณาถึงผลของการใช้คอมพิวเตอร์ย่อมจะขึ้นกับปริมาณงานที่บุคคลภายนอกใช้คอมพิวเตอร์นั้นในการประมวลผลด้วย

ลักษณะที่สำคัญของกิจการใช้คอมพิวเตอร์

4. การที่กิจการใช้คอมพิวเตอร์ ย่อมทำให้ลักษณะของการประมวลผลและการจัดเก็บข้อมูลทางการเงินเปลี่ยนแปลงไปจากการบันทึกรายการบัญชีโดยไม่ใช้คอมพิวเตอร์ ลักษณะที่เปลี่ยนแปลงนี้จะมีผลกระทบต่อการจัดระบบบัญชี และการควบคุมภายในของกิจการเอง ตลอดจนความเชื่อถือของผู้สอบบัญชีต่อการควบคุมภายในนั้น รวมถึงชนิด เวลา และขอบเขตของการใช้วิธีการตรวจสอบด้วยลักษณะดังกล่าว ได้แก่

- 4.1 การจัดโครงสร้างขององค์การ
- 4.2 วิธีการประมวลผล
- 4.3 การออกแบบและวิธีการปฏิบัติงาน

การจัดโครงสร้างขององค์การ

5. ในธุรกิจที่ใช้คอมพิวเตอร์นั้น การจัดโครงสร้างขององค์การ จะหมายความรวมถึงการบริหารงานด้านคอมพิวเตอร์ด้วย และลักษณะโครงสร้างขององค์การที่ใช้คอมพิวเตอร์จะแตกต่างจากที่ไม่ใช้คอมพิวเตอร์ดังนี้

5.1 การแบ่งแยกหน้าที่

ถึงแม้ว่าระบบงานส่วนใหญ่ที่ใช้คอมพิวเตอร์จะยังคงมีการปฏิบัติงานด้วยมืออยู่ด้วยส่วนหนึ่งก็ตาม แต่โดยทั่ว ๆ ไปแล้ว จำนวนคนที่ใช้ในการประมวลผลข้อมูลทางการเงินมักจะมีจำนวนลดลงมาก การควบคุมภายในที่ใช้หลักการแบ่งแยกหน้าที่ที่เหมาะสมจึงอาจทำได้เท่าที่ควร ยิ่งไปกว่านั้นบุคลากรที่ทำหน้าที่ประมวลผลข้อมูลจะเป็นผู้ที่มีความรู้อย่างละเอียดในเรื่องความสัมพันธ์ระหว่างแหล่งที่มาของข้อมูล วิธีการประมวลผลตลอดจนการเสนอและการใช้ผลการประมวลนั้น เช่น ในกรณีที่ผู้วางระบบเป็นผู้เขียนโปรแกรมคำสั่งงานและควบคุมการทำงานของเครื่องด้วยบุคคลเหล่านี้มักจะรู้ถึงข้อบกพร่องของระบบการควบคุมภายในและอยู่ในฐานะที่จะเปลี่ยนแปลง แก้ไขโปรแกรมและข้อมูลได้ ไม่ว่าจะอยู่ในระหว่างการเก็บรักษา หรือกำลังดำเนินการประมวลผลอยู่ ดังนั้นการควบคุมโดยใช้การแบ่งแยกหน้าที่จึงอาจมีประสิทธิภาพลดน้อยลง ได้กิจกรรมที่ใช้คอมพิวเตอร์จึงต้องมีการควบคุมภายในชนิดอื่นเพื่อชดเชยประสิทธิภาพที่ลดน้อยลงดังกล่าว ในการนี้ย่อมมีผลกระทบถึงการประเมินประสิทธิภาพของการควบคุมภายในเพื่อการสอบบัญชี

5.2 การจัดเก็บโปรแกรมและแฟ้มข้อมูล

ในกิจการที่ใช้คอมพิวเตอร์ ข้อมูลต่าง ๆ จะเก็บในแฟ้มข้อมูลทั้งที่เป็นแฟ้มข้อมูลหลักและชั่วคราว แฟ้มเหล่านี้ปกติจะจัดเก็บอยู่ในรูปแบบที่อ่านได้โดยเครื่องการเรียกหรือเปลี่ยนแปลงข้อมูลดังกล่าวจำเป็นต้องใช้โปรแกรมคำสั่งงาน ซึ่งกิจการส่วนใหญ่มักจะเก็บโปรแกรมคำสั่งงานไว้ในที่เดียวกับข้อมูล เพราะฉะนั้นจึงจำเป็นต้องมีการควบคุมการเรียกใช้ หรือเปลี่ยนแปลงแก้ไขทั้งข้อมูลและโปรแกรมคำสั่งงานเพิ่มเติมจากการควบคุมภายในของระบบที่ไม่ใช้คอมพิวเตอร์

วิธีการประมวลผล

6. การนำคอมพิวเตอร์มาใช้มีผลให้ระบบงานมีหลักฐานที่มองเห็นได้น้อยกว่าในระบบงานที่ไม่ได้ใช้คอมพิวเตอร์ นอกจากนั้นจำนวนคนที่สามารถเรียกใช้ข้อมูลจากระบบงานก็มีมากขึ้นด้วย

6.1 การขาดเอกสารที่ใช้ในการนำข้อมูลเข้าคอมพิวเตอร์

เอกสารเบื้องต้นซึ่งเป็นหลักฐานทางการบัญชีต่าง ๆ ไม่ว่าจะเป็นเอกสารประกอบรายการในบัญชี เช่น คำสั่งซื้อจากลูกค้า หรือเอกสารแสดงการอนุมัติรายการ เช่น การอนุมัติวงเงินสินเชื่ออันเมื่อธุรกิจใช้คอมพิวเตอร์ในการประมวลผลแล้ว ข้อมูลต่าง ๆ อาจถูกนำเข้าสู่เครื่องคอมพิวเตอร์โดยตรงไม่มีเอกสารเบื้องต้นดังกล่าวประกอบ

โดยเฉพาะในระบบที่ข้อมูลถูกส่งมาตามสายหลักฐานของการอนุมัติรายการและข้อมูลที่นำเข้าคอมพิวเตอร์อาจใช้วิธีการปฏิบัติอย่างอื่น เป็นต้นว่าการนำการควบคุมในเรื่องการอนุมัติไปรวมเข้าไว้ในโปรแกรมคำสั่งงานตั้งแต่แรก แล้วให้คอมพิวเตอร์ควบคุมการอนุมัติ เช่น เกณฑ์ในการอนุมัติคำสั่งซื้อจากลูกค้าได้นำเข้าไว้ในคอมพิวเตอร์ล่วงหน้าเมื่อนำคำสั่งซื้อจากลูกค้าเข้าเครื่องคอมพิวเตอร์ และคำสั่งซื้อนั้นอยู่ในเกณฑ์ที่กำหนดคอมพิวเตอร์ก็จะอนุมัติและดำเนินการในขั้นตอนต่อไป เป็นต้น ฉะนั้นวิธีการตรวจสอบอาจต้องเปลี่ยนแปลงให้สอดคล้องกับวิธีการประมวลผลของแต่ละระบบงานนั้น

6.2 การขาดหลักฐานอ้างอิงที่มองเห็นได้

ในระบบการลงรายการบัญชีด้วยมือนั้น หลักฐานอ้างอิงของรายการตั้งแต่เริ่มต้นลงบัญชีตามขั้นตอนต่างๆ ของการประมวลผลจนถึงการรายงาน สามารถตรวจสอบได้จากเอกสารเบื้องต้น สมุดบัญชี และรายการทางการเงินแต่ในระบบงานที่ใช้คอมพิวเตอร์จะมีข้อมูลที่เก็บอยู่ในแฟ้มคอมพิวเตอร์เพียงบางอย่างเท่านั้น ซึ่งสามารถตรวจสอบและอ้างอิงได้ นอกจากนี้รายการทางบัญชีส่วนใหญ่จะเก็บอยู่ในลักษณะที่อ่านได้โดยคอมพิวเตอร์ และอาจเก็บไว้เพียงช่วงระยะเวลาหนึ่งเท่านั้น ในการนี้ผู้สอบบัญชีต้องเปลี่ยนแปลงวิธีการตรวจสอบ และจัดตารางการทำงานให้สอดคล้องกับลักษณะและระยะเวลาในการประมวลและการจัดเก็บข้อมูลของกิจการด้วย

6.3 การขาดผลซึ่งสามารถมองเห็นได้จากการประมวลผลของคอมพิวเตอร์

รายการหรือผลจากการประมวลผลบางอย่างอาจจะไม่ได้พิมพ์ออกมาใช้ซึ่งผิดกับระบบที่ลงรายการบัญชีที่ไม่ใช้คอมพิวเตอร์ ซึ่งมักจะติดตามผลลัพธ์จากการประมวลผลได้จากบัญชีและเอกสารประกอบรายการบัญชีได้โดยตรง ในระบบงานที่ใช้คอมพิวเตอร์นั้นเมื่อต้องการใช้ข้อมูลอาจจะต้องมีการเรียกข้อมูล ซึ่งคอมพิวเตอร์มีได้พิมพ์ออกมาจากแฟ้มข้อมูลในคอมพิวเตอร์โดยตรง และเนื่องจากข้อมูลถูกเก็บในลักษณะที่อ่านได้โดยคอมพิวเตอร์เท่านั้น การเรียกข้อมูลดังกล่าวจึงจำเป็นต้องอาศัยคอมพิวเตอร์เรียกให้อีกเช่นกัน

6.4 การเรียกข้อมูลหรือโปรแกรมคำสั่งงานมาใช้ทำได้ง่าย

ข้อมูลและโปรแกรมคำสั่งงานอาจถูกเรียกใช้หรือเปลี่ยนแปลงที่ศูนย์คอมพิวเตอร์ หรือจากสถานที่ที่อยู่ไกล ๆ โดยผ่านอุปกรณ์ของคอมพิวเตอร์ได้ ดังนั้นถ้าขาดการควบคุมที่เหมาะสมก็จะเป็นการเพิ่มโอกาสในการเรียกใช้หรือเปลี่ยนแปลงข้อมูลและโปรแกรมคำสั่งงาน โดยที่ไม่ได้รับอนุมัติทั้งจากบุคคลภายในและภายนอกกิจการมากขึ้น

การออกแบบและวิธีปฏิบัติงาน

7. โดยทั่ว ๆ ไปแล้วการพัฒนาระบบงานของคอมพิวเตอร์มักจะมีผลต่อการออกแบบและการกำหนดขั้นตอนวิธีการปฏิบัติงาน ซึ่งจะแตกต่างจากที่พบในระบบที่ลงรายการบัญชีด้วยมือลักษณะของการออกแบบ และการกำหนดขั้นตอนวิธีการปฏิบัติงานที่แตกต่างออกไปของระบบงานคอมพิวเตอร์มีรายละเอียดดังนี้

7.1 ความสม่ำเสมอของการปฏิบัติงาน

เนื่องจากระบบงานคอมพิวเตอร์นั้น จะให้รายการทุกรายการผ่านวิธีการและการควบคุมตามที่เขียนไว้ในโปรแกรมคำสั่งงานเหมือนกันหมด ถ้ามีการกำหนดชนิดของรายการและเงื่อนไขต่าง ๆ ที่อาจเกิดขึ้นทั้งหมดไว้ในระบบแล้ว ระบบคอมพิวเตอร์มีแนวโน้มว่าจะเชื่อถือได้มากกว่าในระบบที่ไม่ได้ใช้คอมพิวเตอร์ในทางตรงกันข้าม

ถ้าโปรแกรมคำสั่งงานได้เขียนและทดสอบอย่างถูกต้อง การปฏิบัติงานตามโปรแกรกดังกล่าวก็จะก่อให้เกิดข้อผิดพลาดอย่างสม่ำเสมอได้

7.2 การนำการควบคุมไปรวมอยู่ในโปรแกรมคำสั่งงาน

ลักษณะของการประมวลผลโดยคอมพิวเตอร์ สามารถที่จะออกแบบให้มีขั้นตอนของการควบคุมภายในรวมอยู่ในโปรแกรมคำสั่งงานได้ ขั้นตอนการควบคุมเหล่านี้อาจจะมองไม่เห็นด้วยตา เช่น การควบคุมป้องกัน การเรียกใช้ข้อมูลโดยไม่ได้รับอนุมัติอาจกำหนดให้ทำได้โดยใช้รหัสลับ เป็นต้น นอกจากนี้อาจออกแบบขั้นตอนการควบคุมให้ใช้ร่วมกับส่วนงานที่ทำด้วยมือก็ได้ เช่น การสอบทานรายงานคอมพิวเตอร์ที่แสดงรายการผิดปกติ หรือการตรวจสอบความเหมาะสมของข้อมูล เป็นต้น

7.3 รายการทางบัญชีหนึ่งรายการอาจนำไปปรับปรุงเพิ่มข้อมูลของคอมพิวเตอร์ได้มากกว่าหนึ่งแฟ้ม

ข้อมูลที่น่าเข้าคอมพิวเตอร์หนึ่งรายการบัญชีอาจปรับปรุงข้อมูลทางบัญชีที่เกี่ยวข้องกับรายการนั้นได้พร้อมกันทั้งหมด เช่น เอกสารการประกอบการส่งสินค้าอาจใช้ปรับปรุงแฟ้มข้อมูลขาย ลูกหนี้ตลอดจนสินค้าคงเหลือในขณะเดียวกัน เป็นต้น ดังนั้นโอกาสที่จะเกิดความผิดพลาดในการปรับปรุงข้อมูลดังกล่าวจะลดลง ในทางตรงกันข้ามถ้าข้อมูลที่นำเข้าคอมพิวเตอร์ผิดพลาด รายการบัญชีนั้นอาจก่อให้เกิดความผิดพลาดต่อข้อมูลทางบัญชีมากกว่าหนึ่งรายการได้เช่นเดียวกัน

7.4 ระบบงานอาจเป็นผู้สร้างรายการทางบัญชีนั้น

รายการทางบัญชีบางรายการอาจถูกสร้างจากระบบงานคอมพิวเตอร์เองโดยไม่ต้องใช้เอกสารเป็นสื่อในการนำข้อมูลเข้าคอมพิวเตอร์ การอนุมัติรายการดังกล่าวอาจไม่มีหลักฐานจากเอกสารเบื้องต้นดังเช่นรายการบัญชีที่เกิดขึ้นโดยมิได้ใช้คอมพิวเตอร์ ตัวอย่างเช่น การคำนวณดอกเบี้ยแล้วผ่านรายการไปสู่บัญชีลูกค้าโดยอัตโนมัติ ตามคำสั่งที่ให้ไว้แก่คอมพิวเตอร์ภายใต้เงื่อนไขที่อนุมัติไว้ก่อนหน้านี้แล้วในโปรแกรมคำสั่งงาน ดังนั้นจึงจำเป็นต้องมีการควบคุมการออกแบบระบบงานและวิธีการปฏิบัติงานให้เป็นไปตามที่อนุมัติไว้

7.5 สื่อที่ใช้ในการเก็บโปรแกรมคำสั่งงานและข้อมูลนั้นมีโอกาสเสียหายได้ง่าย

ข้อมูลหรือโปรแกรมคำสั่งงานของเครื่องคอมพิวเตอร์ที่ใช้ในการประมวลผลนั้นอาจเก็บอยู่ในสื่อที่เคลื่อนย้ายได้หรือไม่ได้ เช่น แผ่นจานเสียงหรือเทปแม่เหล็ก เป็นต้น สื่อกลางเหล่านี้ง่ายต่อการถูกลักขโมย สูญหาย หรือถูกทำลายทั้งโดยเจตนาและไม่เจตนาได้ ฉะนั้นจึงจำเป็นต้องมีการออกแบบมาตรการรักษาความปลอดภัยของสื่อเหล่านี้ให้รัดกุมด้วย

8. ระบบงานที่ใช้คอมพิวเตอร์ดังกล่าวมาแล้วนั้น มีลักษณะบางประการที่เป็นผลให้การควบคุมภายในที่เคยใช้อยู่มีประสิทธิภาพมากขึ้น เช่น ผลจากความสม่ำเสมอของการปฏิบัติงานของเครื่องคอมพิวเตอร์ในทางตรงกันข้ามก็มีลักษณะบางประการที่ทำให้ต้องมีการควบคุมภายในในส่วนงานของระบบคอมพิวเตอร์เพิ่มเติมขึ้น เช่น การควบคุมการเรียกใช้ และการแก้ไขโปรแกรมคำสั่งงาน เป็นต้น

การควบคุมภายในของระบบงานคอมพิวเตอร์

9. การจัดให้มีระบบการควบคุมภายในของการประมวลผลด้วยคอมพิวเตอร์ให้มีประสิทธิภาพและเป็นไปตามวัตถุประสงค์ของการควบคุมภายในทั้งหมดนั้น จะต้องรวมถึงขั้นตอนการปฏิบัติงานด้วยมือและที่กำหนดไว้ในโปรแกรมคำสั่งงานของคอมพิวเตอร์ ขั้นตอนการปฏิบัติงานดังกล่าวจะประกอบด้วย การควบคุมทั้งหมดที่มีผลต่อการทำงานของคอมพิวเตอร์ซึ่งเป็นการควบคุมทั่วไปและการควบคุมเฉพาะระบบงานบัญชีแต่ละระบบซึ่งเป็นการควบคุมเฉพาะระบบ

การควบคุมทั่วไป

10. วัตถุประสงค์ของการควบคุมทั่วไปคือ การกำหนดแนวทางการควบคุมการทำงานและกิจกรรมต่างๆ ของคอมพิวเตอร์ เพื่อให้เกิดความมั่นใจว่าการควบคุมนั้นจะบรรลุถึงวัตถุประสงค์ โดยรวมของการควบคุมภายใน การควบคุมทั่วไปประกอบด้วย

10.1 การควบคุมการจัดสายงานและการดำเนินงาน การควบคุมในส่วนนี้ได้แก่

10.1.1 การกำหนดนโยบายและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับหน้าที่การควบคุม

10.1.2 การแบ่งแยกหน้าที่ซึ่งขัดแย้งกันในแต่ละของการควบคุมภายในให้เหมาะสม เช่น หน้าที่จัดการเตรียมเอกสารเพื่อส่งข้อมูลเข้าคอมพิวเตอร์ กับหน้าที่ในการเขียนโปรแกรม และหน้าที่ในการควบคุมคอมพิวเตอร์ เป็นต้น

10.2 การควบคุมการพัฒนาและการดูแลรักษาระบบงาน การควบคุมนี้ช่วยให้เกิดความมั่นใจว่าระบบงานได้รับการพัฒนาและดูแลรักษาอย่างมีประสิทธิภาพและมีการอนุมัติโดยถูกต้อง ซึ่งได้แก่การควบคุมในเรื่อง

10.2.1 การทดสอบ การแปลงสภาพ การใช้ ตลอดจนการจัดทำเอกสารของทั้งระบบงานใหม่ และการแก้ไขระบบงานบางส่วน

10.2.2 การเปลี่ยนแปลงระบบงานใดระบบงานหนึ่ง

10.2.3 การใช้เอกสารคู่มือระบบงาน

10.2.4 การนำระบบงานของบุคคลภายนอกมาใช้

10.3 การควบคุมการทำงานของเครื่องคอมพิวเตอร์ การควบคุมนี้มีไว้เพื่อควบคุมการทำงานของระบบและให้ความมั่นใจว่า

10.3.1 มีการใช้ระบบงานตามวัตถุประสงค์ที่ได้รับอนุมัติแล้ว

10.3.2 มีการจำกัดการใช้เครื่องคอมพิวเตอร์เฉพาะผู้ที่ได้รับอนุมัติเท่านั้น

10.3.3 โปรแกรมคำสั่งงานที่ใช้เป็นโปรแกรมที่ได้รับอนุมัติแล้วเท่านั้น

10.3.4 ข้อผิดพลาดจากการประมวลผลจะต้องมีการติดตามและแก้ไขเสมอ

10.4 การควบคุมชุดคำสั่งงาน การควบคุมนี้มีวัตถุประสงค์เพื่อให้มั่นใจว่าการได้มาหรือการพัฒนาชุดคำสั่งงาน มีการอนุมัติและเป็นไปอย่างมีประสิทธิภาพ ซึ่งประกอบด้วย การควบคุมต่อไปนี้

10.4.1 การอนุมัติ การทดสอบ การนำมาใช้ ตลอดจนการทำเอกสารคู่มือของชุดคำสั่งงานระบบใหม่ และที่แก้ไขเพิ่มเติมในภายหลัง

10.4.2 การจำกัดการเรียกใช้ชุดคำสั่งงานและการใช้เอกสารคู่มือไว้เฉพาะผู้ที่ได้รับอนุมัติ

10.5 การควบคุมการนำข้อมูลเข้าคอมพิวเตอร์และโปรแกรมคำสั่งงาน การควบคุมนี้เพื่อให้แน่ใจว่า

10.5.1 มีการจัดขั้นตอนการอนุมัติรายการต่าง ๆ ที่จะนำเข้าสู่ระบบคอมพิวเตอร์

10.5.2 การเรียกใช้ข้อมูลและโปรแกรมคำสั่งงานจำกัดเฉพาะผู้ที่ได้รับอนุมัติเท่านั้น

11. นอกจากที่กล่าวมาแล้ว มีมาตรการป้องกันเพื่อให้การประมวลผลด้วยคอมพิวเตอร์สามารถกระทำได้อย่างต่อเนื่อง มาตรการเหล่านี้ได้แก่

11.1 การเก็บข้อมูลและโปรแกรมคำสั่งงานของคอมพิวเตอร์สำรองไว้ภายนอกกิจการ

11.2 การกำหนดขั้นตอนการปฏิบัติงานฉุกเฉิน ในกรณีที่เกิดโจรกรรมหรือความเสียหายที่เกิดขึ้นโดยเจตนาและไม่เจตนา

11.3 การจัดหาเครื่องคอมพิวเตอร์สำรองไว้ภายนอกกิจการ ในกรณีที่เกิดภัยอันตราย

การควบคุมเฉพาะระบบ

12. วัตถุประสงค์ของการควบคุมเฉพาะระบบคือ การจัดให้มีขั้นตอนการควบคุมในส่วนของระบบงานบัญชี เพื่อให้แน่ใจว่า รายการทั้งหมดได้รับการอนุมัติ บันทึกและประมวลผลอย่างครบถ้วนถูกต้องภายในระยะเวลาที่กำหนด การควบคุมเฉพาะระบบประกอบด้วย

12.1 การควบคุมการนำข้อมูลเข้าคอมพิวเตอร์ จัดให้มีขึ้นเพื่อให้มั่นใจได้ว่า

12.1.1 รายการทุกรายการได้รับการอนุมัติ ก่อนจะถูกประมวลผลโดยคอมพิวเตอร์

12.1.2 รายการทุกรายการได้รับการแปลงสภาพให้อยู่ในรูปแบบที่เครื่องคอมพิวเตอร์อ่านได้ และบันทึกลงในแฟ้มข้อมูลอย่างถูกต้อง

12.1.3 รายการนำเข้านั้นจะไม่มีการสูญหายเพิ่มเติม ถูกนำเข้าซ้ำหรือแก้ไขอย่างไม่มีเหตุผลสมควร

12.1.4 รายการที่ไม่ถูกต้องจะต้องได้รับการปฏิเสธ หรือแก้ไขและถ้าจำเป็นจะถูกส่งกลับไปเข้าคอมพิวเตอร์ใหม่อีกครั้งภายในเวลาที่กำหนด

12.2 การควบคุมในส่วนการประมวลผลและแฟ้มข้อมูลคอมพิวเตอร์ ซึ่งจัดให้มีขึ้นเพื่อให้มั่นใจได้ว่า

12.2.1 รายการต่าง ๆ รวมทั้งรายการที่สร้างขึ้นโดยระบบงานได้รับการประมวลผลที่เหมาะสม

12.2.2 รายการต่าง ๆ ภายหลังจากนำเข้าหรือสร้างขึ้นโดยระบบงานแล้วจะไม่สูญหายมีการเพิ่มเติม ถูกประมวลผลซ้ำ หรือมีการเปลี่ยนแปลงอย่างไม่มีเหตุผล

12.2.3 ข้อผิดพลาดจากการประมวลผลจะถูกรายงานและแก้ไขทันเวลา

12.3 การควบคุมข้อมูลส่งออก จัดให้มีขึ้นเพื่อให้มั่นใจได้ว่า

12.3.1 ผลลัพธ์จากการประมวลผลนั้นถูกต้อง

12.3.2 มีการจำกัดการเข้าไปเกี่ยวข้อง หรือใช้ข้อมูลที่ส่งออกจากคอมพิวเตอร์เฉพาะผู้ได้รับ

อนุมัติเท่านั้น

12.3.3 การส่งข้อมูลที่ส่งออกมาจากคอมพิวเตอร์จะไปถึงผู้ใช้ซึ่งได้รับอนุมัติทันเวลา

การสอบทานการควบคุมภายในและการประเมินประสิทธิภาพขั้นต้น

13. ผู้สอบบัญชีควรสอบทานระบบประมวลผลข้อมูลทางการเงินโดยคอมพิวเตอร์ในขอบเขตที่เห็นว่าจำเป็น เพื่อทำความเข้าใจถึงการควบคุมภายในโดยทั่วไปของกิจการตลอดจนทางเดินของเอกสาร นอกจากนี้การสอบทานดังกล่าวจะรวมถึงการจัดสายงาน การดำเนินงาน บุคลากร และลักษณะของรายการที่จะประมวลผลด้วยคอมพิวเตอร์ ผู้สอบบัญชีซึ่งต้องการจะเชื่อถือและใช้ประโยชน์ของการควบคุมภายในนั้นในการปฏิบัติงานสอบบัญชี จะต้องสอบทานการควบคุมภายในและประเมินประสิทธิภาพในขั้นต้นว่าการควบคุมภายในเหล่านั้นมีประสิทธิภาพพอเพียงที่จะเชื่อถือได้หรือไม่

การสอบทานการควบคุมทั่วไป

14. การควบคุมทั่วไปซึ่งผู้สอบบัญชีอาจต้องการเชื่อถือก็คือการควบคุมตามที่กล่าวไว้แล้วในวรรคที่ 10 ผู้สอบบัญชีอาจต้องพิจารณาว่าการควบคุมทั่วไปเหล่านี้มีผลต่อระบบงานทางคอมพิวเตอร์ที่มีสาระสำคัญต่อการตรวจสอบอย่างไร การควบคุมทั่วไปที่เกี่ยวข้องกับระบบงานบางระบบหรือทุกระบบมักจะมีความสัมพันธ์กันในการดำเนินงานและช่วยให้การควบคุมเฉพาะระบบมีประสิทธิภาพยิ่งขึ้น ดังนั้นการสอบทานการควบคุมภายในทั่วไปก่อนการสอบทานการควบคุมภายในเฉพาะระบบจะทำให้การประเมินประสิทธิภาพการควบคุมภายในได้ผลดีกว่า

การสอบทานการควบคุมเฉพาะระบบ

15. การควบคุมเฉพาะระบบ ซึ่งผู้สอบบัญชีอาจต้องการเชื่อถือก็คือ การควบคุมที่กล่าวไว้ในวรรคที่ 12 อย่างไรก็ตามการควบคุมการนำข้อมูลเข้าคอมพิวเตอร์ การประมวลผล แพ้มข้อมูลและการส่งข้อมูลออกจากคอมพิวเตอร์ อาจกระทำได้โดยผู้ที่ปฏิบัติงานในแผนงานคอมพิวเตอร์ หรือโดยผู้ใช้ระบบงาน หรืออาจใช้บุคลากรต่างหากทำหน้าที่ควบคุมโดยเฉพาะ หรืออาจเขียนเป็นคำสั่งงานในโปรแกรมเฉพาะระบบงานก็ได้การควบคุมเฉพาะระบบซึ่งผู้สอบบัญชีอาจจะเชื่อถือได้ประกอบด้วย

15.1 การควบคุมจากผู้ใช้งาน

ถ้าการควบคุมที่ทำด้วยมือจากผู้ใช้งานสามารถให้ความมั่นใจว่า ผลจากการประมวลผลของระบบนั้นครบถ้วน ถูกต้อง และได้รับการอนุมัติแล้ว ผู้สอบบัญชีอาจตัดสินใจที่จะเชื่อถือและทดสอบการปฏิบัติตามระบบเฉพาะในส่วนของการควบคุมที่ทำด้วยมือก็ได้ เช่น การควบคุมที่ทำด้วยมือของผู้ใช้ระบบงานเงินเดือนที่ประมวล

ผลโดยคอมพิวเตอร์ เพื่อคำนวณเงินเดือนของพนักงานบริษัทอาจประกอบด้วย การหายอดรวมสำหรับเงินเดือนเพื่อควบคุมข้อมูลที่จะนำเข้าคอมพิวเตอร์ ทดสอบผลลัพธ์จากการคำนวณเงินเดือนจ่ายสุทธิ การอนุมัติจ่ายและการโอนเงินเปรียบเทียบกับจำนวนเงินในทะเบียนเงินเดือน และทำการกระทบยอดเงินฝากธนาคารในเวลาที่เหมาะสม เป็นต้น ในกรณีนี้ ผู้สอบบัญชีอาจต้องการความเชื่อถือและทดสอบเฉพาะการควบคุมที่ทำด้วยมือจากผู้ใช้ระบบ

15.2 การควบคุมข้อมูลที่ส่งออกจากระบบคอมพิวเตอร์

นอกจากการควบคุมของผู้ใช้ระบบแล้ว ก็ยังมีการควบคุมที่ใช้ผลจากข้อมูลในการประมวลผลของเครื่องคอมพิวเตอร์ หรือเก็บไว้ในโปรแกรมคำสั่งงาน ผู้สอบบัญชีอาจจะเชื่อถือและทดสอบการควบคุม ดังกล่าวนั้นโดยการตรวจสอบข้อมูลที่ส่งออกมาจากระบบคอมพิวเตอร์ ไม่ว่าจะใช้การตรวจสอบด้วยมือหรือใช้คอมพิวเตอร์ช่วยในการสอบบัญชีก็ตาม ข้อมูลส่งออกดังกล่าวอาจเก็บในสื่อแม่เหล็ก ไมโครฟิล์ม หรือรายงานคอมพิวเตอร์ ตัวอย่างเช่น ผู้สอบบัญชีอาจเชื่อถือในการควบคุมที่กิจการมีการกระทบยอดระหว่างยอดรวมของรายงานต่าง ๆ กับยอดบัญชีคุมในบัญชีแยกประเภทและอาจทดสอบการทำการกระทบยอดด้วยมือก็ได้ หรือถ้าการกระทบยอดนั้นทำโดยคอมพิวเตอร์ ผู้สอบบัญชีอาจทดสอบการกระทบยอดโดยใช้คอมพิวเตอร์ทำเลียนแบบการควบคุมดังกล่าวก็ได้

15.3 การควบคุมโดยใช้โปรแกรมคำสั่งงาน

ในระบบงานที่ใช้คอมพิวเตอร์บางระบบ ผู้สอบบัญชีอาจไม่สามารถที่จะตรวจสอบการควบคุมจากผู้ใช้หรือข้อมูลที่ส่งออกของระบบได้ เช่น ในกรณีที่ระบบงานไม่มีรายงานคอมพิวเตอร์แสดงการอนุมัติที่สำคัญ หรือการอนุมัติผ่านรายการผิดจากนโยบายที่วางไว้ ผู้สอบบัญชีจะต้องเชื่อถือในวิธีการควบคุมที่รวมอยู่ในโปรแกรมคำสั่งงานของระบบ ผู้สอบบัญชีจะต้องทดสอบการปฏิบัติตามระบบโดยใช้คอมพิวเตอร์ช่วยในการสอบบัญชี เช่น การใช้ข้อมูลทดสอบ ประมวลผลรายการซ้ำใหม่ หรือในบางครั้งอาจต้องตรวจสอบรายละเอียดของโปรแกรมคำสั่งงานนั้น

การประเมินประสิทธิภาพการควบคุมภายในขั้นต้น

16. ผู้สอบบัญชีต้องทำการประเมินประสิทธิภาพการควบคุมภายในขั้นต้นของทั้งการควบคุมทั่วไปและการควบคุมเฉพาะระบบเพื่อดูว่ามีประสิทธิภาพและพอเพียงที่จะเชื่อถือ และใช้ประโยชน์ในการปฏิบัติงานสอบบัญชีได้เพียงใด การควบคุมทั่วไปนั้นมีผลต่อการประมวลผลการทางบัญชีในทุก ๆ ระบบงาน ถ้าการควบคุมทั่วไปไม่มีประสิทธิภาพพออาจมีความเสี่ยงที่จะเกิดข้อผิดพลาดและไม่สามารถตรวจพบข้อผิดพลาดที่มีอยู่ในระบบงานได้ ดังนั้นข้อบกพร่องของการควบคุมทั่วไปอาจทำให้ผู้สอบบัญชีไม่เชื่อถือในการควบคุมเฉพาะระบบ อย่างไรก็ตาม การควบคุมที่ทำด้วยมือจากผู้ใช้ระบบงานก็อาจจะเป็นการควบคุมของระบบงานที่มีประสิทธิภาพได้

17. ถ้าผู้สอบบัญชีสรุปผลว่ามีข้อบกพร่องในการควบคุมทั่วไปหรือการควบคุมเฉพาะระบบอันทำให้ไม่สามารถเชื่อถือในการควบคุมเหล่านั้นได้ ผู้สอบบัญชีไม่จำเป็นต้องทำการสอบทาน จดบันทึกหรือทดสอบการปฏิบัติตามระบบ ผู้สอบบัญชีอาจหาวิธีการเพื่อให้บรรลุวัตถุประสงค์ของการตรวจสอบจากการใช้วิธีการทดสอบความถูกต้องของรายการบัญชีแทน

การทดสอบการปฏิบัติตามระบบและการประเมินประสิทธิภาพ ขั้นสุดท้าย

18. ในกรณีที่ผู้สอบบัญชีเชื่อถือในระบบการควบคุมภายในจากการประเมินประสิทธิภาพขั้นต้นผู้สอบบัญชีจะสอบทาน และจดบันทึกระบบบัญชีในกิจการที่ใช้คอมพิวเตอร์ เพื่อทดสอบการปฏิบัติตามระบบต่อไปในการสอบทานและการจดบันทึกนั้น ผู้สอบบัญชีจะสอบถามและสอบทานโดยใช้วิธีเดียวกันกับที่ได้กำหนดไว้ในย่อหน้าที่ 17-19 ของแถลงการณ์มาตรฐานการสอบบัญชีที่ 18 เรื่อง การประเมินประสิทธิภาพการควบคุมภายใน การจดบันทึกการควบคุมทั่วไปและการควบคุมเฉพาะเรื่องอาจใช้เทคนิคการเขียนผังทางเดินเอกสารการใช้อย่างสอบถาม หรือการจดย่อก็ได้

19. ในธุรกิจที่ใช้คอมพิวเตอร์ วัตถุประสงค์ของการทดสอบการปฏิบัติตามระบบยังคงเหมือนกันกับในระบบงานที่ไม่ใช้คอมพิวเตอร์ อย่างไรก็ตาม วิธีการตรวจสอบบางอย่างอาจเปลี่ยนแปลงไปบ้าง นอกเหนือจากการสอบถาม การสังเกตการณ์ และวิธีการสุ่มตัวอย่างแล้วผู้สอบบัญชีอาจจำเป็นต้องใช้คอมพิวเตอร์ช่วยในการสอบบัญชีด้วย

20. ประสิทธิภาพของการทดสอบการปฏิบัติงานตามระบบนั้นอาจจะสูงขึ้น เมื่อมีการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี การใช้เทคนิคดังกล่าวอาจจะเหมาะกับระบบที่ไม่มีหลักฐานที่มองเห็นได้ด้วยตา เพื่อแสดงถึงการควบคุมที่ต้องการความเชื่อถือ ในกรณีเช่นนี้ การใช้ข้อมูลทดสอบอาจจะช่วยให้ได้หลักฐานที่ต้องการ เช่น การสอบทานการควบคุมการเรียกใช้ข้อมูลในระบบงานตามสายว่าทำหน้าที่ตามระบบที่วางไว้หรือไม่

21. การทดสอบการปฏิบัติตามระบบและการประเมินประสิทธิภาพในขั้นสุดท้ายนั้นมิวัตถุประสงค์จะพิจารณาว่า การควบคุมที่ผู้สอบบัญชีต้องการจะเชื่อถือได้นั้นได้มีการปฏิบัติตามระบบตลอดช่วงเวลาที่ต้องการจะเชื่อถือ ตลอดจนการควบคุมเหล่านั้นยังควรแก่การเชื่อถือตามที่วางแผนไว้จากการประเมินประสิทธิภาพในขั้นต้นหรือไม่ ถ้าผู้สอบบัญชีมีหลักฐานว่า การควบคุมดังกล่าวไม่เป็นไปตามระบบที่วางไว้ หรือจากการทดสอบการปฏิบัติตามระบบชี้ให้เห็นว่า การควบคุมทั่วไปไม่ได้ควบคุมการควบคุมเฉพาะระบบให้ทำหน้าที่ตลอดช่วงเวลาที่ต้องการเชื่อถืออย่างเพียงพอแล้ว การประเมินผลในขั้นสุดท้ายของผู้สอบบัญชีอาจไม่เชื่อถือในการควบคุมนั้นตามที่วางแผนไว้ก็ได้ และผู้สอบบัญชีจะต้องใช้การทดสอบความถูกต้องของรายการบัญชีตรวจสอบแทน

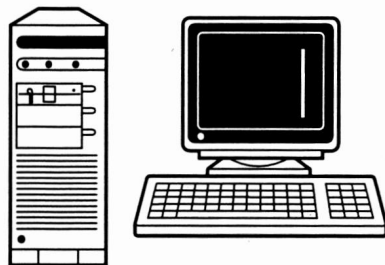
การรายงานถึงจุดอ่อนของการควบคุมภายใน

22. ในการศึกษาและประเมินประสิทธิภาพการควบคุมภายในของกิจการที่ใช้คอมพิวเตอร์ผู้สอบบัญชีอาจทราบถึงจุดอ่อนของการควบคุมภายในด้านบัญชี ผู้สอบบัญชีควรแจ้งให้ฝ่ายบริหารได้ทราบถึงจุดอ่อนดังเช่นที่กล่าวไว้ในย่อหน้าที่ 36 ของแถลงการณ์มาตรฐานการสอบบัญชี ฉบับที่ 18 เรื่อง การประเมินประสิทธิภาพการควบคุมภายใน

23. นอกจากนี้ผู้สอบบัญชียังอาจทราบถึงข้อบกพร่องอื่น ๆ ทางคอมพิวเตอร์ ซึ่งไม่ได้เกี่ยวข้องกับการศึกษาและประเมินประสิทธิภาพการควบคุมภายในโดยตรง แต่เกี่ยวกับการควบคุมเพื่อป้องกันข้อมูลและให้การประมวลผลดำเนินงานได้อย่างต่อเนื่อง ตามตัวอย่างที่กล่าวไว้ในย่อหน้าที่ 10.5 และ 11 เมื่อผู้สอบบัญชีทราบถึงข้อบกพร่องที่มีสาระสำคัญนี้ ผู้สอบบัญชีควรแจ้งให้ฝ่ายบริหารทราบด้วยเช่นกัน

วันถือปฏิบัติ

24. มาตรฐานการสอบบัญชี ฉบับที่ 29 เรื่อง การประเมินประสิทธิภาพการควบคุมภายในกรณีการใช้คอมพิวเตอร์นี้ ให้เริ่มถือปฏิบัติกับการตรวจสอบงบการเงินสำหรับงวดหรือปีสิ้นสุดในหรือหลัง วันที่ 30 มิถุนายน 2533 เป็นต้นไป



มาตรฐานการสอบบัญชีฉบับที่ 36
สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย
เรื่อง การใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

1. มาตรฐานการสอบบัญชี ฉบับที่ 28 เรื่องการสอบบัญชีในกรณีที่กิจการใช้คอมพิวเตอร์ได้กล่าวถึงวัตถุประสงค์และขอบเขตการสอบบัญชีโดยสรุปได้ว่า ในกรณีที่กิจการใช้คอมพิวเตอร์ในการประมวลผลข้อมูลทางการเงินในส่วนที่เป็นสาระสำคัญ ไม่ว่ากิจการนั้นจะดำเนินการประมวลผลเองหรือให้บุคคลภายนอกดำเนินการก็ตาม ไม่ได้ทำให้วัตถุประสงค์และขอบเขตของการสอบบัญชีเปลี่ยนแปลงไป แต่อย่างไรการเปลี่ยนแปลงไปใช้คอมพิวเตอร์เพื่อประมวลผลข้อมูลและจัดเก็บข้อมูลทางการเงิน อาจมีผลทำให้กิจการต้องใช้ระบบการควบคุมภายในที่แตกต่างไปจากเดิม ดังนั้นวิธีการศึกษาระบบบัญชีและประเมินประสิทธิภาพของการควบคุมภายในที่เกี่ยวข้องเพื่อกำหนดวิธีการตรวจสอบเวลาและขอบเขตการตรวจสอบของผู้สอบบัญชีจะต้องเปลี่ยนแปลงไปให้เหมาะสมกับกิจการที่ใช้คอมพิวเตอร์

2. มาตรฐานการสอบบัญชี ฉบับที่ 29 เรื่องการประเมินประสิทธิภาพการควบคุมภายในกรณีที่กิจการใช้คอมพิวเตอร์ ได้กล่าวถึงการประเมินประสิทธิภาพระบบการควบคุมภายในของกิจการที่ใช้คอมพิวเตอร์โดยสรุปไว้ว่ากรณีที่กิจการใช้คอมพิวเตอร์ในการประมวลผลข้อมูลทางการเงินอย่างมีสาระสำคัญต่อการตรวจสอบ ไม่ว่าจะเป็นการใช้คอมพิวเตอร์ชนิดใด ขนาดใด และจะดำเนินการประมวลผลข้อมูลเองหรือมอบหมายให้บุคคลภายนอก ดำเนินการก็ตาม ผู้สอบบัญชีของกิจการนั้นจำเป็นต้องประเมินประสิทธิภาพระบบการควบคุมภายในของกิจการด้วยและจะต้องพิจารณาผลกระทบของการใช้คอมพิวเตอร์ประมวลผลข้อมูลทางการเงินที่มีต่อระบบบัญชีและการควบคุมภายใน

3. มาตรฐานการสอบบัญชีตามที่ย่ออ้างถึงในข้อ 1 และ 2 ได้สรุปถึง ลักษณะบางประการของการประมวลผลข้อมูลโดยใช้คอมพิวเตอร์ ซึ่งมีผลต่อผู้สอบบัญชีในการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีเช่น

- 3.1 รายการที่ไม่มีเอกสารอ้างอิง
- 3.2 รายการที่ไม่มีหลักฐานให้ตรวจสอบได้ด้วยตา
- 3.3 การจัดเก็บข้อมูลในรูปแฟ้มสารแม่เหล็ก

4. มาตรฐานการสอบบัญชีฉบับนี้มีวัตถุประสงค์เพื่อให้แนวทางในการพิจารณาใช้คอมพิวเตอร์ช่วยในการสอบบัญชีรวมทั้งเทคนิคต่าง ๆ ของการสอบบัญชีโดยใช้คอมพิวเตอร์

5. มาตรฐานการสอบบัญชีฉบับนี้จะเน้นถึงเทคนิคการสอบบัญชีโดยใช้คอมพิวเตอร์ที่นิยมใช้กันอย่างแพร่หลายซึ่งมีอยู่ 2 วิธีคือ

- 5.1 การใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี
- 5.2 การใช้ข้อมูลทดสอบ

การใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี

6. ผู้สอบบัญชีสามารถพิจารณาเลือกใช้โปรแกรมคอมพิวเตอร์ช่วยในการตรวจสอบข้อมูลทางการเงินของกิจการได้หลายแบบ ดังนี้

6.1 การใช้โปรแกรมการตรวจสอบสำเร็จรูป ซึ่งเป็นโปรแกรมที่พัฒนาขึ้นสำหรับใช้ช่วยในการตรวจสอบบัญชีโดยเฉพาะ

6.2 การใช้โปรแกรมคอมพิวเตอร์ที่พัฒนาเพื่อช่วยในการตรวจสอบเฉพาะเรื่อง เช่น โปรแกรมการคำนวณดอกเบี้ยการผิดนัดชำระหนี้ตามสัญญาเช่าซื้อ เป็นต้น ซึ่งผู้สอบบัญชีอาจจัดหาได้จากแหล่งต่าง ๆ ดังนี้

6.2.1 พัฒนาขึ้นเอง ในกรณีที่ผู้สอบบัญชีมีความรู้ความชำนาญในการเขียนโปรแกรมและเข้าใจระบบคอมพิวเตอร์ของกิจการที่ตรวจสอบเพียงพอ

6.2.2 ให้กิจการเป็นผู้พัฒนา ผู้สอบบัญชีอาจทำความตกลงกับกิจการเพื่อร่วมกันพัฒนาโปรแกรมเพื่อตรวจสอบตามวัตถุประสงค์เฉพาะอย่างได้ กรณีนี้จะช่วยให้งานของผู้สอบบัญชีลุล่วงไปได้ด้วยดี เนื่องจากบุคลากรของกิจการมีความคุ้นเคยกับระบบคอมพิวเตอร์นั้นอยู่แล้ว

6.2.3 ให้บุคคลที่สามพัฒนา

6.2.4 ใช้โปรแกรมเพื่อการตรวจสอบที่กิจการมีอยู่แล้ว กรณีนี้ผู้สอบบัญชีควรแน่ใจว่าโปรแกรมนั้นสามารถให้ผลลัพธ์ที่ถูกต้องและตรงกับวัตถุประสงค์ที่กำหนด

6.2.5 นำโปรแกรมของกิจการมาปรับปรุงเพื่อใช้ในการตรวจสอบ

6.3 การใช้โปรแกรมคำสั่งงานอรรถประโยชน์ ซึ่งรวมถึงโปรแกรมการสร้างรายงานต่างๆ โปรแกรมการเรียกถามข้อมูลผ่านทางหน้าจอ และโปรแกรมอื่น ๆ ในลักษณะเดียวกับที่กิจการใช้อยู่

6.4 การถ่ายข้อมูลที่ต้องการตรวจสอบจากเครื่องคอมพิวเตอร์ของกิจการลงมายังเครื่องไมโครคอมพิวเตอร์ และใช้โปรแกรมคอมพิวเตอร์สำเร็จรูปทั่ว ๆ ไปช่วยในการตรวจสอบเช่น การใช้โปรแกรมตารางทำการช่วยคำนวณดอกเบี้ยรับของลูกหนี้ ตัวเงินรับหรือช่วยคำนวณราคาสินค้าคงเหลือสิ้นงวด เป็นต้น

การใช้ข้อมูลทดสอบ

7. วิธีการใช้ข้อมูลทดสอบนี้ทำได้โดยการป้อนข้อมูลเข้าไปในระบบคอมพิวเตอร์ของกิจการและเปรียบเทียบผลลัพธ์ที่ได้จากการประมวลผลกับผลที่กำหนดไว้หรือทราบล่วงหน้า ตัวอย่างของวิธีการใช้ข้อมูลทดสอบ ได้แก่

7.1 การใช้ข้อมูลทดสอบในการทดสอบประสิทธิภาพการควบคุมบางเรื่องที่กำหนดไว้ในโปรแกรมคำสั่งงาน เช่น ทดสอบรหัสผ่านที่ใช้ในระบบเชื่อมต่อตรงและการควบคุมการเข้าถึงข้อมูล เป็นต้น

7.2 การใช้รายการที่ได้ประมวลผลมาก่อนแล้ว หรือรายการที่ผู้สอบบัญชีสมมุติขึ้น เพื่อทดสอบลักษณะการประมวลผลอย่างใดอย่างหนึ่งของระบบคอมพิวเตอร์ของกิจการ การประมวลผลดังกล่าวควรจะประมวลผลแตกต่างหากจากการประมวลผลตามปกติของกิจการ

7.3 การสมมุติข้อมูลเพื่อใช้ในการทดสอบร่วมกับข้อมูลจริง ข้อมูลที่สมมุติขึ้นเพื่อใช้ในการทดสอบอาจทำได้โดยการตั้งหน่วยงานสมมุติหรือพนักงานสมมุติ เป็นต้น และทำการทดสอบโดยนำข้อมูลที่ทดสอบนั้นผ่านการ

ประมวลผลในระหว่างวัน ซึ่งเป็นการประมวลผลตามปกติของกิจการ ถ้าการประมวลผลข้อมูลที่สมมุติขึ้นดังกล่าวทำ ร่วมกับการประมวลผลตามปกติของกิจการแล้ว ผู้สอบบัญชีต้องตรวจสอบให้แน่ใจว่าข้อมูลที่สมมุติขึ้นนั้นได้มีการลบทิ้ง หลังจากที่ได้ทราบผลการทดสอบข้อมูลแล้ว

ผู้สอบบัญชีควรสอบทานให้แน่ใจว่าโปรแกรมคำสั่งงานที่ใช้กับข้อมูลทดสอบนั้นเป็นโปรแกรมคำสั่งงาน ที่กิจการใช้ประมวลผลกับงานที่ผู้สอบบัญชีกำลังตรวจสอบจริง

ลักษณะงานที่สามารถใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

8. ลักษณะงานที่สามารถใช้คอมพิวเตอร์ช่วยในการสอบบัญชีตามที่กล่าวในข้อ 6 และข้อ 7

8.1 การทดสอบรายละเอียดของรายการบัญชีและยอดคงเหลือ ตัวอย่างเช่น

8.1.1 การใช้โปรแกรมเพื่อการตรวจสอบ ทดสอบข้อมูลในแฟ้มข้อมูลทั้งหมดหรือบางส่วน เช่น การบวกลบยอดบดลอง การคำนวณค่านายหน้าและดอกเบี้ย การคำนวณอายุลูกค้า การคำนวณการคิดราคาสินค้า คงเหลือ เป็นต้น

8.1.2 การใช้โปรแกรมเพื่อการตรวจสอบเลือกข้อมูลเพื่อใช้ในการตรวจสอบโดยอาจใช้วิธีการ เลือกตัวอย่างเชิงสถิติ หรือเลือกรายการที่มีจำนวนเงินเกินจำนวนที่ตั้งไว้ เช่น การเลือกรายการเพื่อส่งหนังสือยืนยันยอด ลูกหนี้ การสุ่มตัวอย่างรายการสินค้าคงเหลือเพื่อใช้ในการสังเกตการณ์การตรวจนับสินค้าคงเหลือ เป็นต้น

8.1.3 การใช้โปรแกรมเพื่อการตรวจสอบประมวลผลข้อมูลที่อยู่ในแฟ้มและนำผลไปเปรียบเทียบกับข้อมูลที่บันทึกไว้ในบัญชี เช่น การเปรียบเทียบปริมาณการส่งสินค้ากับปริมาณที่สั่งซื้อ เป็นต้น

8.2 การวิเคราะห์เปรียบเทียบ ตัวอย่างเช่น

8.2.1 การใช้โปรแกรมเพื่อการตรวจสอบอ่านแฟ้มข้อมูลคั่นรายการที่ผิดปกติ เช่น การสอบ ทานราคาขายหรือต้นทุนสินค้าที่มีราคาสูงหรือต่ำกว่าปกติ การสอบทานรายการสินค้าคงเหลือที่มีปริมาณคงเหลือเป็น ยอดติดลบ หรือการสอบทานยอดลูกค้าคงเหลือที่มีจำนวนเกินวงเงินสินเชื่อที่ได้รับอนุมัติ เป็นต้น

8.2.2 การใช้โปรแกรมเพื่อการตรวจสอบสรุปผลข้อมูลในรูปรายงานเพื่อใช้ในการวิเคราะห์เปรียบเทียบ เช่น รายการวิเคราะห์สินค้าล้าสมัย รายงานสรุปปริมาณการขายและกำไรขั้นต้นแยกตามประเภทสินค้า เป็นต้น

8.3 การทดสอบการปฏิบัติตามระบบการควบคุมภายในทั่วไป เช่น การใช้โปรแกรมเพื่อการตรวจ สอบเปรียบเทียบโปรแกรมคำสั่งงานก่อนการแก้ไขกับโปรแกรมคำสั่งงานหลังการแก้ไขเพื่อดูว่าคำสั่งใดบ้างที่เปลี่ยนแปลง ไป และการเปลี่ยนแปลงนั้นตรงกับความต้องการของผู้ใช้ที่ได้รับการอนุมัติหรือไม่ เป็นต้น

8.4 การทดสอบการปฏิบัติตามระบบการควบคุมภายในเฉพาะระบบ ตัวอย่างเช่น

8.4.1 การสอบทานความเหมาะสมของค่าของข้อมูล ได้แก่ การกำหนดให้คอมพิวเตอร์อ่าน ข้อมูลนำเข้า แล้วนำค่าที่อ่านได้เปรียบเทียบกับค่าที่ได้กำหนดไว้แล้วล่วงหน้าในโปรแกรมคำสั่งงาน เช่น การจ่ายค่าใช้จ่ายบางชนิดอาจมีการกำหนดวงเงินสูงสุดของที่จะจ่ายได้ในแต่ละครั้งไว้ เช่น ไม่เกิน 50,000 บาท หากมีการจ่ายเกิน วงเงินนี้เครื่องคอมพิวเตอร์จะไม่รับการจ่ายครั้งนี้นั้นจนกว่าจะได้รับการอนุมัติจากผู้มีอำนาจ เป็นต้น

8.4.2 การสอบทานประเภทของข้อมูล ได้แก่ การตรวจสอบข้อมูลนำเข้าว่าข้อมูลนั้นเป็นข้อมูลประเภทที่กำหนดไว้หรือไม่ เช่น ข้อมูลราคาต่อหน่วยต้องเป็นตัวเลขล้วน ๆ ไม่ควรมีตัวอักษรหรือข้อมูลอื่นที่มีใช้ตัวเลขปะปน เป็นต้น

8.4.3 การสอบทานเครื่องหมาย ได้แก่ การตรวจสอบข้อมูลนำเข้าว่าข้อมูลนั้นมีเครื่องหมายตามกำหนดไว้หรือไม่ เช่น จำนวนสินค้าคงเหลือจะแสดงปริมาณติดลบไม่ได้ เป็นต้น

ข้อควรพิจารณาเมื่อใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

9. เมื่อวางแผนสอบบัญชี ผู้สอบบัญชีควรคำนึงถึงการใช้วิธีการตรวจสอบร่วมกันระหว่างวิธีการตรวจสอบที่ไม่ใช้คอมพิวเตอร์กับวิธีที่ใช้คอมพิวเตอร์ ในการพิจารณาว่าจะใช้คอมพิวเตอร์ช่วยในการสอบบัญชีหรือไม่นั้น ปัจจัยที่ควรนำมาพิจารณามีดังนี้

9.1 ความรู้ ความสามารถและความชำนาญ ตลอดจนประสบการณ์ทางด้านคอมพิวเตอร์ของผู้สอบบัญชี

9.2 ความเหมาะสมและสอดคล้องกันระหว่างโปรแกรมคอมพิวเตอร์ที่ใช้เพื่อการตรวจสอบกับอุปกรณ์คอมพิวเตอร์ของกิจการ

9.3 สถานการณ์ที่จำเป็นต้องใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

9.4 ลักษณะการจัดเก็บและขนาดของแฟ้มข้อมูลที่จะทดสอบ

9.5 ประสิทธิภาพและประสิทธิผลในการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

5.6 ช่วยเวลาการตรวจสอบ

ความรู้ ความสามารถ ความชำนาญ ตลอดจนประสบการณ์ทางด้านคอมพิวเตอร์ของผู้สอบบัญชี

10. จากมาตรฐานการสอบบัญชี ฉบับที่ 28 เรื่อง การสอบบัญชีในธุรกิจที่ใช้คอมพิวเตอร์ได้กล่าวถึงระดับความรู้และความชำนาญของผู้สอบบัญชีเมื่อต้องสอบบัญชีธุรกิจที่ใช้คอมพิวเตอร์ และได้ให้แนวทางในการปฏิบัติเมื่อต้องมีการมอบหมายหน้าที่ในงานตรวจสอบบางส่วนให้แก่ผู้ช่วยที่มีความชำนาญด้านคอมพิวเตอร์ หรือเมื่อต้องใช้ผลงานของผู้เชี่ยวชาญหรือผู้สอบบัญชีอื่นที่มีความชำนาญทางด้านคอมพิวเตอร์ ผู้สอบบัญชีควรมีความรู้ในการวางแผนปฏิบัติงาน และใช้ผลงานจากการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีระดับความรู้ความสามารถที่ต้องการนั้นขึ้นอยู่กับความยุ่งยากซับซ้อนและลักษณะของการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีตลอดจนระบบบัญชีของกิจการนั้นด้วย ผู้สอบบัญชีควรตระหนักว่าการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีในสถานการณ์หนึ่ง อาจต้องการความรู้และความชำนาญด้านคอมพิวเตอร์มากกว่าในอีกสถานการณ์หนึ่ง

ความเหมาะสมและสอดคล้องกันระหว่างโปรแกรมคอมพิวเตอร์ ที่ใช้เพื่อการตรวจสอบกับอุปกรณ์คอมพิวเตอร์ของกิจการ

11. เมื่อผู้สอบบัญชีพิจารณาว่าโปรแกรมคอมพิวเตอร์เพื่อการตรวจสอบมาช่วยในการสอบบัญชีแล้ว ผู้สอบบัญชีควรพิจารณาว่าโปรแกรมคอมพิวเตอร์ดังกล่าวสามารถนำมาใช้กับอุปกรณ์คอมพิวเตอร์ของกิจการได้หรือไม่ ผู้สอบบัญชีอาจต้องวางแผนและที่จะใช้อุปกรณ์คอมพิวเตอร์อื่นเมื่อพบว่าการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี ณ สถานที่ของกิจการไม่เป็นการประหยัดหรือไม่สามารถกระทำได้

12. ผู้สอบบัญชีอาจต้องการความร่วมมือจากบุคลากรของกิจการในการจัดหาอุปกรณ์คอมพิวเตอร์เพื่อใช้ในการประมวลผล รวมทั้งให้ความช่วยเหลือในการทำงานบางอย่าง เช่น การบรรจุโปรแกรมเพื่อการตรวจสอบเข้าในเครื่องคอมพิวเตอร์ของกิจการ การทำสำเนาแฟ้มข้อมูลให้อยู่ในรูปแบบที่ผู้สอบบัญชีต้องการ

สถานการณ์ที่จำเป็นต้องใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

13. ระบบบัญชีหลาย ๆ ระบบที่ใช้คอมพิวเตอร์ในการประมวลผลอาจประมวลผลโดยไม่ปรากฏหลักฐานที่สามารถมองเห็นได้ ซึ่งในสถานการณ์เช่นนี้ผู้สอบบัญชีย่อมไม่สามารถตรวจสอบได้ด้วยวิธีตามปกติซึ่งทำให้ต้องใช้คอมพิวเตอร์เข้าช่วย

การขาดหลักฐานที่มองเห็นได้ดังกล่าวอาจเกิดขึ้นจากขั้นตอนต่าง ๆ ในกระบวนการประมวลผลตามตัวอย่างดังต่อไปนี้

13.1 การขาดเอกสารข้อมูลนำเข้า เช่น ในกรณีที่ข้อมูลการสั่งขายถูกป้อนเข้าเครื่องคอมพิวเตอร์โดยระบบเชื่อมต่อตรง ในกรณีการคำนวณดอกเบี้ยและส่วนลดด้วยโปรแกรม คำสั่งงานคอมพิวเตอร์โดยอัตโนมัติ หรือโดยไม่มี การอนุมัติในแต่ละรายการ เป็นต้น

13.2 ระบบงานคอมพิวเตอร์อาจไม่ได้สร้างร่องรอยเพื่อการตรวจสอบสำหรับรายการที่ประมวลผลโดยเครื่องคอมพิวเตอร์ เช่น ใบส่งของและใบกำกับสินค้าอาจจะถูกจับคู่กันโดยโปรแกรมคำสั่งงานคอมพิวเตอร์โดยไม่ปรากฏหลักฐานให้ตรวจสอบ หรือในกรณีที่การตรวจสอบวงเงินสินเชื่อของลูกค้าทุกครั้งที่มีการขายสินค้านั้น จะมีการจัดพิมพ์เป็นรายงานก็ต่อเมื่อมีรายการขายที่จะทำให้เกินวงเงินสินเชื่อในกรณีเช่นนั้นก็จะไม่มีหลักฐานที่แสดงให้เห็นว่ารายการอื่น ๆ นั้นได้ผ่านการตรวจสอบวงเงินสินเชื่อทุกรายการ เป็นต้น

13.3 รายงานต่าง ๆ ที่จำเป็นสำหรับการตรวจสอบอาจไม่ได้ถูกกำหนดให้พิมพ์ออกมาหรืออาจพิมพ์เฉพาะยอดรวม ในขณะที่รายละเอียดประกอบยังคงเก็บอยู่ในแฟ้มข้อมูลคอมพิวเตอร์

ลักษณะการจัดเก็บและขนาดของแฟ้มข้อมูลที่จะทำการทดสอบ

14. ผู้สอบบัญชีควรพิจารณาปัจจัยที่เกี่ยวข้องกับแฟ้มข้อมูลของกิจการที่จะใช้คอมพิวเตอร์ช่วยในการตรวจสอบดังต่อไปนี้

14.1 ขนาดของแฟ้มข้อมูลจะมีผลทำให้ผู้สอบบัญชีใช้เวลาในการตรวจสอบอย่างมีประสิทธิภาพและประสิทธิผลต่างกันคือ แฟ้มข้อมูลที่มีขนาดใหญ่ต้องใช้เวลาในการอ่านมากกว่าแฟ้มข้อมูลขนาดเล็ก และหากเป็นแฟ้มข้อมูลขนาดใหญ่มากอาจไม่สามารถนำมาตรวจสอบบนเครื่องไมโครคอมพิวเตอร์ได้ ผู้สอบบัญชีต้องใช้โปรแกรมเพื่อการตรวจสอบบนเครื่องมินิคอมพิวเตอร์หรือเมนเฟรม ซึ่งต้องใช้ความรู้ความชำนาญแตกต่างกัน

14.2 ลักษณะการจัดเก็บ การจัดเก็บข้อมูลในแฟ้มข้อมูลมีได้หลายแบบคือ ในแฟ้มลำดับหรือแฟ้มสุ่ม ซึ่งจะมีผลทำให้ลักษณะและการใช้เวลาในการเข้าถึงแฟ้มข้อมูลนั้นต่างกัน เช่น ในแฟ้มลำดับซึ่งจัดเก็บอยู่ในเทป ผู้สอบบัญชีจะใช้เวลาในการเลือกข้อมูลเพื่อการตรวจสอบจากแฟ้มลำดับมากกว่าการเลือกข้อมูลจากแฟ้มสุ่ม เป็นต้น

14.3 ลักษณะของระเบียบ ซึ่งจะมีอยู่ 2 ประเภท คือ ความยาวของระเบียบแบบกำหนดตัวกับความยาวของระเบียบแบบแปรได้ ซึ่งนอกจากจะมีผลต่อขนาดของข้อมูลแล้วยังมีผลต่อผู้สอบบัญชีในการพิจารณาประเภทของโปรแกรมคอมพิวเตอร์ที่ใช้ในการตรวจสอบเพื่อให้ได้ผลลัพธ์ตามที่ผู้สอบบัญชีต้องการอีกด้วย เช่น การใช้โปรแกรมคอมพิวเตอร์เพื่อการตรวจสอบทั่วไปในการตรวจสอบแฟ้มข้อมูลที่มีความยาวของระเบียบแบบแปรได้มักไม่ได้ผลตามต้องการ เป็นต้น ดังนั้นผู้สอบบัญชีอาจต้องใช้โปรแกรมคอมพิวเตอร์เพื่อการตรวจสอบเฉพาะอย่างตรวจสอบแฟ้มข้อมูลดังกล่าว การใช้โปรแกรมคอมพิวเตอร์ช่วยในการตรวจสอบได้กล่าวไว้แล้วในย่อหน้าที่ 6

14.4 ประเภทของแฟ้มข้อมูล ลักษณะของข้อมูลที่จัดเก็บในแฟ้มข้อมูลมีหลายประเภทคือ แอสกีและเอ็บซีดิก การที่ผู้สอบบัญชีจะใช้ข้อมูลในการตรวจสอบจึงทำได้ในลักษณะที่ต่างกันเช่น ถ้าเป็นข้อมูลที่จัดเก็บอยู่ในรูปแอสกี ผู้สอบบัญชีที่สามารถใช้โปรแกรมสำเร็จรูปทั่วไปตรวจสอบในไมโครคอมพิวเตอร์ได้ แต่ถ้าเป็นข้อมูลที่จัดเก็บอยู่ในรูปเอ็บซีดิก ผู้สอบบัญชีไม่สามารถใช้โปรแกรมสำเร็จรูปทั่วไปตรวจสอบได้ ต้องใช้โปรแกรมในการเปลี่ยนข้อมูลจากรูปเอ็บซีดิกเป็นแอสกี ซึ่งอาจมีต้นทุนหรือต้องการความรู้และความชำนาญในการใช้โปรแกรมเพื่อการตรวจสอบมากกว่ากรณีที่ตรวจสอบข้อมูลซึ่งจัดเก็บอยู่ในรูปแอสกี เป็นต้น

ประสิทธิภาพและประสิทธิผลในการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

15. การใช้คอมพิวเตอร์ช่วยในการสอบบัญชีอาจเพิ่มประสิทธิภาพและประสิทธิผลของการตรวจสอบในแง่การได้มาซึ่งหลักฐานอย่างเพียงพอ และการประเมินหลักฐานเพื่อการตรวจสอบ

15.1 ในการทดสอบรายการบางอย่าง การใช้คอมพิวเตอร์อาจก่อให้เกิดประสิทธิผลมากกว่าวิธีปกติที่ไม่ใช้คอมพิวเตอร์ในระดับทุนที่เท่าหรือใกล้เคียงกัน เนื่องจากคอมพิวเตอร์สามารถตรวจสอบเอกสารได้จำนวนมากขึ้นหรือทั้งหมดแทนที่จะต้องเลือกตรวจเพียงบางรายการ

15.2 ในการตรวจวิเคราะห์เพื่อค้นหารายการที่ผิดปกติ อาจใช้คอมพิวเตอร์สอบทานรายการและรายละเอียดยอดคงเหลือ รวมทั้งพิมพ์รายงานรายการที่ผิดปกติได้อย่างมีประสิทธิภาพสูงกว่าวิธีที่ไม่ใช้คอมพิวเตอร์

15.3 การนำคอมพิวเตอร์เข้ามาช่วยในการสอบบัญชีอาจทำให้การเพิ่มปริมาณการทดสอบความถูกต้องของรายการบัญชีในเรื่องใดเรื่องหนึ่งได้ประสิทธิผลมากกว่าการเชื่อถือระบบและผลการทดสอบการปฏิบัติตามระบบที่เกี่ยวข้องกับเรื่องนั้น

16. เพื่อให้การใช้คอมพิวเตอร์ช่วยในการสอบบัญชีมีประสิทธิภาพ ผู้สอบบัญชีควรพิจารณาเรื่องต่าง ๆ ดังนี้

16.1 การวางแผนงาน การใช้คอมพิวเตอร์ช่วยในการสอบบัญชี โดยครอบคลุมถึงกำหนดเวลา การออกแบบ การปฏิบัติงานและการประเมินผล

16.2 จำนวนชั่วโมงที่ต้องใช้บริการของผู้เชี่ยวชาญในการสอบทานงานหรือความช่วยเหลือที่ต้องการในด้านเทคนิค

16.3 การออกแบบและการจัดพิมพ์แบบฟอร์มและรายงาน เช่น บันทึกแบบยืนยันยอด

16.4 การบันทึกข้อมูลเข้าและการตรวจทานข้อมูลที่บันทึก

16.5 ช่วงและระยะเวลาทำงานของเครื่องคอมพิวเตอร์

ในการประเมินผลควมมีประสิทธิภาพและประสิทธิผลของการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีนั้น ผู้สอบบัญชีอาจต้องพิจารณาถึงอายุหรือรอบการใช้งานของระบบงานและโปรแกรมคำสั่งงานที่ใช้คอมพิวเตอร์ช่วยในการสอบบัญชีด้วย การวางแผนในครั้งแรกการออกแบบและการพัฒนาโปรแกรมคำสั่งงานคอมพิวเตอร์ช่วยในการสอบบัญชีนั้น โดยทั่วไปแล้วมักจะนำมาใช้ประโยชน์ต่องานตรวจสอบในครั้งต่อไปได้

ช่วงเวลาในการตรวจสอบ

17. แฟ้มข้อมูลคอมพิวเตอร์บางชนิด ตัวอย่างเช่น แฟ้มรายละเอียดรายการของข้อมูลมักจะถูกเก็บไว้ในเครื่องคอมพิวเตอร์เพียงแค่ช่วงระยะเวลานั้น ๆ เท่านั้น ดังนั้นผู้สอบบัญชีอาจต้องแจ้งให้ลูกค้าทราบล่วงหน้า หากผู้สอบบัญชีต้องการให้มีการเก็บแฟ้มรายละเอียดรายการข้อมูลได้นานกว่าปกติ เพื่อนำมาใช้ในการตรวจสอบโดยคอมพิวเตอร์ หรือถ้าจำเป็นผู้สอบบัญชีอาจต้องเปลี่ยนช่วงเวลาในการสอบบัญชีให้อยู่ในช่วงเวลาที่ยังมีการจัดเก็บแฟ้มข้อมูลที่ต้องการนั้น เป็นต้น

18. ในกรณีที่มีความจำกัดในเรื่องของเวลาที่จะใช้ในการตรวจสอบ ผู้สอบบัญชีต้องวางแผนการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีให้ดี ทั้งนี้ เพื่อให้การตรวจสอบสามารถเสร็จสิ้นทันเวลา

ลำดับขั้นตอนของการนำคอมพิวเตอร์ช่วยในการสอบบัญชี

19. การที่ผู้สอบบัญชีนำเทคนิคการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีมาใช้นั้นจะมีลำดับขั้นตอนการทำงานที่สำคัญดังนี้

19.1 กำหนดวัตถุประสงค์ของการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

19.2 พิจารณาลักษณะการจัดเก็บและการเข้าถึงแฟ้มข้อมูลของกิจการ

19.3 กำหนดประเภทของรายการที่ทดสอบ

19.4 กำหนดวิธีที่จะใช้ในการตรวจสอบข้อมูล

19.5 กำหนดรูปแบบของผลลัพธ์ที่จะได้จากการทดสอบ

19.6 กำหนดบุคลากรทางฝ่ายคอมพิวเตอร์ของกิจการและฝ่ายผู้สอบบัญชี ซึ่งจะเข้ามามีส่วนร่วมในการออกแบบและใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

19.7 ทบทวนประมาณการค่าใช้จ่ายที่จะเกิดขึ้นและเปรียบเทียบกับประโยชน์ที่จะได้รับ

19.8 กำหนดวิธีการควบคุมการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีและการจัดทำเอกสารให้เหมาะสมและเพียงพอ

19.9 เตรียมการในด้านอุปกรณ์และเครื่องคอมพิวเตอร์ รวมถึงทักษะความชำนาญที่จำเป็น

19.10 ดำเนินการทดสอบ

19.11 สรุปและประเมินผลลัพธ์ที่ได้จากการทดสอบ

การควบคุมการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

20. ผู้สอบบัญชีจะต้องควบคุมการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี เพื่อให้แน่ใจว่าผลที่ได้รับเป็นไปตามขั้นตอนการทำงานโดยละเอียดที่ได้กำหนดไว้ และบรรลุวัตถุประสงค์ของการตรวจสอบรวมถึงการควบคุมมิให้พนักงานของกิจการหรือบุคคลอื่นแก้ไขกระบวนการในการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีโดยไม่สมควร วิธีการควบคุมการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีขึ้นอยู่กับลักษณะเฉพาะอย่างของระบบงาน และในการวางแผนการควบคุมการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี ผู้สอบบัญชีควรพิจารณาถึงความจำเป็นที่ตนจะต้องดำเนินการในเรื่องต่อไปนี้

20.1 การอนุมัติข้อกำหนดทางด้านเทคนิคที่ผู้เชี่ยวชาญและสอบทานงานด้านเทคนิคที่เกี่ยวข้องในการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

20.2 การสอบทานระบบการควบคุมภายในทั่วไปทางด้านคอมพิวเตอร์ของกิจการ ซึ่งอาจจะมีผลต่อความน่าเชื่อถือของการใช้คอมพิวเตอร์มาช่วยในการสอบบัญชี เช่น ระบบการควบคุมภายในเรื่องการเปลี่ยนแปลงและแก้ไขโปรแกรมคำสั่งงาน รวมทั้งการเข้าถึงแฟ้มข้อมูลที่จัดเก็บอยู่ในคอมพิวเตอร์ ถ้าการควบคุมภายในดังกล่าวไม่สามารถเชื่อถือได้ ผู้สอบบัญชีอาจจะต้องพิจารณาถึงการประมวลผลโปรแกรมคอมพิวเตอร์ที่ใช้ช่วยในการสอบบัญชีในศูนย์คอมพิวเตอร์อื่นที่เหมาะสมกว่า เป็นต้น

20.3 การนำผลลัพธ์ที่ได้จากการใช้คอมพิวเตอร์ช่วยในการสอบบัญชีไปใช้ในกระบวนการตรวจสอบอย่างเหมาะสม

21. ผู้สอบบัญชีอาจใช้วิธีการต่อไปนี้ในการควบคุมการใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี

21.1 การเข้ามามีส่วนร่วมในการออกแบบและทดสอบโปรแกรมคอมพิวเตอร์นั้น

21.2 การตรวจสอบความถูกต้องของการลงรหัสเพื่อให้แน่ใจว่ารายละเอียดต่าง ๆ ในโปรแกรมที่พัฒนานั้นเป็นไปตามที่กำหนดไว้

21.3 การขอความร่วมมือจากพนักงานฝ่ายคอมพิวเตอร์ของกิจการในการสอบทานการใช้คำสั่งโปรแกรมระบบปฏิบัติการมาใช้ในโปรแกรมที่พัฒนาขึ้น เพื่อให้แน่ใจว่าโปรแกรมนั้นสามารถปฏิบัติการด้วยเครื่องคอมพิวเตอร์ของกิจการได้

21.4 ทดลองใช้โปรแกรมคำสั่งงานเพื่อการตรวจสอบประมวลผลแฟ้มข้อมูลทดสอบบางส่วนก่อนจะนำไปใช้ประมวลผลกับแฟ้มข้อมูลจริงของกิจการ

21.5 ตรวจสอบให้แน่ใจว่าแฟ้มข้อมูลที่นำมาใช้นั้นเป็นแฟ้มที่ถูกต้องซึ่งอาจจะกระทำได้โดยตรวจสอบกับหลักฐานอื่นของกิจการ เช่นเปรียบเทียบยอดรวมของลูกหนี้ในแฟ้มข้อมูลกับรายงานการวิเคราะห์อายุลูกหนี้ที่จัดพิมพ์โดยกิจการในงวดเดียวกัน เป็นต้น

21.6 การรวบรวมหลักฐานที่แสดงว่าโปรแกรมที่ใช้เพื่อการตรวจสอบนั้นทำงานตามที่ได้วางแผนไว้

21.7 การจัดให้มีมาตรการรักษาความปลอดภัยสำหรับแฟ้มข้อมูลที่ใช้ในการทดสอบเพื่อป้องกันมิให้มีการแก้ไขบิดเบือนแฟ้มข้อมูล

22. ผู้สอบบัญชีอาจไม่จำเป็นต้องอยู่ที่ศูนย์คอมพิวเตอร์ในขณะที่ประมวลผลข้อมูลโดยโปรแกรมคอมพิวเตอร์ที่ช่วยในการสอบบัญชีถ้าหากแน่ใจว่าการควบคุมที่ดีพอ อย่างไรก็ตาม การที่ผู้สอบบัญชีอยู่ด้วยมีข้อได้เปรียบในทางปฏิบัติ ตัวอย่างเช่น สามารถป้องกันการแก้ไขและควบคุมการแจกจ่ายผลลัพธ์ที่ได้จากการประมวลผล ตลอดจนช่วยให้แน่ใจว่าหากมีข้อผิดพลาด ผู้สอบบัญชีจะสามารถแก้ไขได้ทันเวลา ตัวอย่างเช่น ในกรณีที่มีการหยาบแฟ้มข้อมูลที่ผิด ๆ มาใช้ในการประมวลผล เป็นต้น

23. ผู้สอบบัญชีอาจใช้วิธีการต่อไปนี้ควบคุมการใช้ข้อมูลทดสอบ

23.1 การควบคุมลำดับที่ของการส่งข้อมูลที่ใช้ในการทดสอบเข้าทำการประมวลผลในกรณีที่มีการทดสอบนั้นครอบคลุมการประมวลผลในหลาย ๆ ระบบงาน หรือในรอบระยะเวลาที่แตกต่างกัน

23.2 การทดลองประมวลผลข้อมูลทดสอบในปริมาณน้อยก่อนที่จะไปประมวลผลข้อมูลที่ใช้ในการทดสอบจริง ๆ

23.3 การเปรียบเทียบผลลัพธ์ที่ได้จากการประมวลผลทุกรายการ และยอดรวมกับผลลัพธ์ที่กำหนดไว้ล่วงหน้า

23.4 การตรวจสอบให้แน่ใจว่าได้ใช้โปรแกรมคำสั่งงานชุดที่ถูกต้องในการประมวลผลตลอดช่วงระยะเวลาของการทดสอบ นอกจากนี้ ในกรณีที่กิจการเปลี่ยนแปลงชุดคำสั่งงานในรอบระยะเวลาบัญชีที่ตรวจสอบ ผู้สอบบัญชีอาจจำเป็นต้องขยายขอบเขตการทดสอบ เพื่อให้แน่ใจว่าการประมวลผลเชื่อถือได้ตลอดรอบระยะเวลาบัญชี

24. เมื่อผู้สอบบัญชีใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี ผู้สอบบัญชีจะต้องอาศัยความร่วมมือจากพนักงานของกิจการที่มีความรู้ในเรื่องเครื่องและระบบคอมพิวเตอร์ของกิจการเป็นอย่างดี ในสถานการณ์เช่นนั้น ผู้สอบบัญชีควรมั่นใจว่าพนักงานของกิจการนั้นไม่ได้แก้ไขเปลี่ยนแปลงผลลัพธ์ที่ได้จากการประมวลผลการใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชีอย่างเช่น การสอบทานปูมบันทึกประวัติการใช้งานในช่วงระหว่างการตรวจสอบ เป็นต้น

กระดาษทำการ

25. มาตรฐานของกระดาษทำการและขั้นตอนการเก็บรักษาเอกสารสำหรับการใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชานั้น ควรจะสอดคล้องกับการตรวจสอบโดยปกติการแยกเก็บกระดาษทำการที่เกี่ยวข้องกับการใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชีออกจากกระดาษทำการอื่นอาจช่วยให้การค้นหาค้นหาสะดวกขึ้น

26. กระดาษทำการควรให้ข้อมูลอย่างเพียงพอที่จะอธิบายถึงการใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี ตัวอย่างเช่น

26.1 การวางแผน

26.1.1 วัตถุประสงค์ของการใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี

26.1.2 ชนิดของโปรแกรมคอมพิวเตอร์ที่นำมาช่วยในการสอบบัญชี

26.1.3 วิธีการควบคุมที่จะนำมาใช้

26.1.4 กำลังคน กำหนดเวลาในการเข้าตรวจสอบค่าใช้จ่ายในการตรวจสอบ

26.2 การปฏิบัติงาน

26.2.1 การจัดเตรียม การใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชีรวมถึงวิธีการและการควบคุมที่จะใช้ในการทดสอบ

26.2.2 รายละเอียดการทดสอบที่ได้ปฏิบัติโดยใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี

26.2.3 รายละเอียดของข้อมูลนำเข้า การประมวลผลและผลลัพธ์จากการประมวลผล

26.2.4 รายละเอียดของข้อมูลทางเทคนิคที่เกี่ยวข้องกับระบบบัญชีคอมพิวเตอร์ของกิจการ เช่น ผังแฟ้มข้อมูล เป็นต้น

26.3 หลักฐานการสอบบัญชี

26.3.1 ผลลัพธ์ที่ได้จากการประมวลผล

26.3.2 คำอธิบายวิธีการตรวจสอบผลลัพธ์ที่ได้จากการประมวลผล

26.3.3 ผลสรุปการตรวจสอบ

26.4 อื่นๆ

26.4.1 ข้อเสนอแนะต่อผู้บริหารของกิจการ

26.4.2 สิ่งที่ต้องแก้ไขปรับปรุงในการใช้โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชีสำหรับต่อไป

ข้อควรพิจารณาอื่นในการใช้คอมพิวเตอร์ช่วยในการสอบบัญชี

27. ในกรณีที่การควบคุมภายในทั่วไปทางด้านคอมพิวเตอร์ไม่เพียงพอ ผู้สอบบัญชีอาจให้ความเชื่อถือต่อระบบการควบคุมภายในได้น้อยลง ซึ่งมีผลดังนี้

27.1 ผู้สอบบัญชีจะเน้นในการทดสอบรายละเอียดของรายการบัญชีและยอดคงเหลือตลอดจนใช้เทคนิคการวิเคราะห์เปรียบเทียบให้มากขึ้น ซึ่งจะช่วยให้การใช้โปรแกรมคอมพิวเตอร์บางโปรแกรมช่วยในการสอบบัญชีได้ประสิทธิผลมากขึ้น

27.2 ผู้สอบบัญชีจะต้องใช้วิธีการตรวจสอบอื่นควบคู่กันไปเพื่อให้แน่ใจว่าโปรแกรมคอมพิวเตอร์ที่นำมาช่วยในการสอบบัญชี จะสามารถทำงานได้อย่างถูกต้องตามวัตถุประสงค์และข้อมูลของกิจการถูกต้อง

28. ในกรณีที่ข้อมูลที่ทำการประมวลผลมีปริมาณน้อย การใช้วิธีการตรวจสอบที่ไม่ใช้คอมพิวเตอร์อาจประหยัดค่าใช้จ่ายได้มากกว่า

29. ในกรณีที่กิจการไม่สามารถให้ความช่วยเหลือทางด้านเทคนิคอย่างเพียงพอผู้สอบบัญชีอาจไม่สามารถนำคอมพิวเตอร์ช่วยในการสอบบัญชี

30. โปรแกรมคอมพิวเตอร์สำเร็จรูปบางโปรแกรมที่ใช้ในการสอบบัญชีอาจไม่สามารถนำมาใช้ประมวลผลกับเครื่องคอมพิวเตอร์ขนาดเล็กได้ ในกรณีเช่นนี้ จะเป็นการจำกัดทางเลือกในการนำโปรแกรมคอมพิวเตอร์มาช่วยในการสอบบัญชี อย่างไรก็ตาม ผู้สอบบัญชีอาจคัดลอกหรือจัดทำสำเนาแฟ้มข้อมูลของกิจการแล้วนำไปประมวลผลกับเครื่องคอมพิวเตอร์อื่นที่เหมาะสม

วันถือปฏิบัติ

31. มาตรฐานการสอบบัญชี ฉบับที่ 36 เรื่อง การใช้คอมพิวเตอร์ช่วยในการสอบบัญชีให้เริ่มถือปฏิบัติ การตรวจสอบงบการเงินสำหรับรอบระยะเวลาบัญชีสิ้นสุดในหรือหลังวันที่ 31 ธันวาคม เป็นต้นไป



ภาคผนวก
คำอธิบายศัพท์เทคนิคที่ใช้ในผลการสัมภาษณ์การสอบบัญชีฉบับนี้

โปรแกรมคอมพิวเตอร์ช่วยในการสอบบัญชี	Audit Software	โปรแกรมคอมพิวเตอร์ที่จัดทำขึ้นโดยผู้สอบบัญชีบุคคลภายนอก หรือโปรแกรมเมอร์ของกิจการ เพื่อใช้ในการสอบบัญชีของกิจการ
ข้อมูลทดสอบ	Test Data	ข้อมูลที่ผู้สอบบัญชีสมมติขึ้นเพื่อใช้ในการทดสอบโปรแกรมของกิจการ
โปรแกรมคอมพิวเตอร์เพื่อการตรวจสอบทั่วไป	Generalized Audit Software (GAS)	โปรแกรมสำเร็จรูปที่ทำหน้าที่ผลิตโปรแกรม เพื่อนำไปใช้ในการอ่านข้อมูลที่จะตรวจสอบคำนวณ วิเคราะห์ และพิมพ์รายงานให้ผู้สอบบัญชีนำไปวิเคราะห์ตรวจสอบ และดำเนินการต่อไปได้โดยง่าย
โปรแกรมคอมพิวเตอร์เพื่อการตรวจสอบเฉพาะอย่าง	Specialized Audit Software	โปรแกรมที่ผู้สอบบัญชีได้จัดทำขึ้นเอง หรือมอบหมายให้ผู้อื่นเขียนให้ตามวัตถุประสงค์ที่ผู้สอบบัญชีต้องการ
โปรแกรมคำสั่งงานอรรถประโยชน์	Utility Programs	ชุดคำสั่งระบบที่มีเขียนและเก็บไว้ให้แล้วในตัวเครื่องคอมพิวเตอร์ เพื่ออำนวยความสะดวกแก่ผู้ใช้ เนื่องจากเป็นโปรแกรมที่ผู้ใช้งานมักมักจะใช้อยู่บ่อย ๆ เช่น โปรแกรมเรียงลำดับ โปรแกรมย้ายข้อมูลจากบัตรสู่แถบบันทึก เป็นต้น
ระบบเชื่อมต่อ	On-line	การประมวลผลที่ทำโดยอุปกรณ์ที่อยู่ภายใต้การควบคุมของเครื่องคอมพิวเตอร์ ไม่ว่าอุปกรณ์นั้นจะเป็นส่วนหนึ่งของตัวเครื่อง (เช่น เครื่องอ่านบัตร) หรืออุปกรณ์นั้นจะอยู่ห่างออกไปแต่สามารถติดต่อโดยตรงกับเครื่องได้ เช่น การประมวลผลโดยมีการสื่อสารระหว่างเครื่องปลายทางหรือเทอร์มินัล และหน่วยประมวลผลกลางโดยทางโทรศัพท์หรือวิธีอื่น ๆ การทำเช่นนี้เครื่องจะประมวลผลทันทีที่ได้รับข้อมูล ซึ่งจะเข้าสู่ตัวเครื่องคอมพิวเตอร์ตลอดเวลา

แฟ้มลำดับ	Sequential File	แฟ้มข้อมูลที่เกิดจากลำดับที่ติดกัน การจะค้นหาข้อมูลใดๆ ต้องเป็นไปตามลำดับ
แฟ้มสุ่ม	Random File	แฟ้มข้อมูลที่เกิดจากระเบียบการจะออกไปในเนื้อที่ที่ติดกันหรือไม่ โดยไม่เรียงไปตามลำดับก่อนหลังอย่างแฟ้มข้อมูลที่เกิดตามลำดับที่ระบุไว้
แอสกี	ASCII (American Standard Code for Information Interchange)	รหัสมาตรฐานของสหรัฐอเมริกาเพื่อแลกเปลี่ยนสารสนเทศ
เอ็บซีดิก	EBCDIC (Extended Binary Coded Decimal Interchange Code)	รหัสแลกเปลี่ยนเลขฐานสิบเข้ารหัสฐานสองแบบขยาย
ระเบียบ	Record	หลายๆ ฟิลด์ที่มารวมกัน
ความยาวของระเบียบแบบกำหนดตายตัว	Fixed Length Record	จำนวนบิตหรือไบต์ (อักขระ) ในระเบียบหนึ่ง ๆ ซึ่งกำหนดจำนวนตายตัวไม่แปรเปลี่ยนจำนวนตามความต้องการผู้ใช้
ความยาวของระเบียบแบบแปรได้	Variable Length Record	จำนวนบิตหรือไบต์ (อักขระ) ในระเบียบหนึ่ง ๆ ซึ่งไม่ได้กำหนดจำนวนตายตัว แต่จะแปรเปลี่ยนจำนวนได้ตามความต้องการใช้
ผังแฟ้มข้อมูล	File Layout	โครงสร้างของแฟ้มข้อมูล
บูมบันทึกระบบการใช้งาน	History Log	รายงานที่บันทึกประวัติการใช้งานของผู้ใช้งานในช่วงเวลาหนึ่ง ๆ ซึ่งอาจจัดเก็บอยู่ในรูปของแฟ้มข้อมูล หรือจัดพิมพ์เป็นรูปรายงาน



**ข้อคิดและแนวทางบางประการ
ในการบริหารงานตรวจสอบ
องค์กรที่ใช้คอมพิวเตอร์**

ข้อคิดเห็นและแนวทางบางประการในการบริหารงาน ตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

การนำคอมพิวเตอร์มาใช้อย่างแพร่หลายของกิจการต่าง ๆ ในปัจจุบันได้ก่อให้เกิดผลกระทบในด้านต่าง ๆ ซึ่งรวมทั้งงานตรวจสอบองค์กรที่ระบบงานต่าง ๆ ประมวลผลด้วยคอมพิวเตอร์ผู้ตรวจสอบจึงควรได้ทราบถึงวิวัฒนาการของการตรวจสอบกิจการที่นำคอมพิวเตอร์มาใช้ในการงานด้านต่าง ๆ การเปลี่ยนแปลงวัตถุประสงค์ ขอบเขต และแนวการตรวจสอบตั้งแต่อดีตจนถึงปัจจุบันที่เกิดขึ้นแล้วแนวโน้มการเปลี่ยนแปลงในอนาคต และแนวความคิดในการพัฒนาการตรวจสอบ ให้สอดคล้องกับความก้าวหน้าทางเทคโนโลยีที่เป็นไปอย่างรวดเร็ว และแนวความคิดในการพิจารณาความเสี่ยงเพื่อการเข้าถึงจุดควบคุมหลักต่าง ๆ จะมีประโยชน์ในการวางแผนและการตรวจสอบในองค์กรที่ใช้คอมพิวเตอร์ประมวลข้อมูล

1. ผู้ตรวจสอบกับการเปลี่ยนแปลงทางเทคโนโลยีที่เกี่ยวกับการบันทึกข้อมูล

ในฐานะผู้ตรวจสอบเมื่อมีการเปลี่ยนแปลงใหม่ ๆ เกิดขึ้น ย่อมรู้สึกว่ามีปัญหา เช่น เดิมมนุษย์เคยบันทึกข้อมูลไว้บนก้อนหิน เมื่อต่อ ๆ มารู้จักทำกระดาษ รู้จักเย็บเป็นเล่ม รู้จักทำเป็นแผ่น Ledger Card หรือแบบฟอร์มต่าง ๆ ก็บันทึกข้อมูลบนสิ่งเหล่านี้แทน ในปัจจุบันเราสามารถบันทึกข้อมูลบนสื่อข้อมูลต่าง ๆ เช่น Magnetic Tape, Magnetic Disk, Floppy Disk ฯลฯ

ทุกครั้งที่มีการเปลี่ยนแปลงก็เกิดข้อสงสัยเกี่ยวกับความเชื่อถือในวิธีการบันทึกแบบใหม่ ๆ ทั้งในเรื่องการรักษาความลับของข้อมูลและความปลอดภัยของสื่อข้อมูล แม้จะถูกคัดค้านในระยะแรก แต่การค้นพบเหล่านั้นก็ทำให้วิทยาการและธุรกิจเจริญก้าวหน้าขึ้น

วิชาชีพตรวจสอบก็ถูกผลักดันให้ต้องคิดค้นวิธีการตรวจสอบใหม่ ๆ ที่จะมาประเมินและทดสอบความถูกต้องของระบบงานและความเชื่อถือได้ของข้อมูลที่เปลี่ยนแปลงไปตามเทคโนโลยีใหม่ ๆ จึงจำเป็นที่ผู้ตรวจสอบจะต้องติดตามและศึกษาวิธีการตรวจสอบใหม่ ๆ เพื่อทดแทนวิธีการตรวจสอบบางอย่างที่ใช้อยู่เดิมซึ่งไม่เหมาะสมกับเทคโนโลยีในปัจจุบัน

2. สภาพการตรวจสอบด้าน EDP ในปัจจุบัน

ผู้ตรวจสอบส่วนใหญ่ยังต้องการเพิ่มประสบการณ์ในการตรวจสอบงานที่ประมวลผลด้วยคอมพิวเตอร์มากขึ้น เมื่อเทียบกับระบบงานที่ย่างยากซับซ้อนในปัจจุบัน การฝึกอบรมผู้ที่มาทำงานด้านนี้มีปัญหาหลายประการ การตรวจสอบที่ทำกันอยู่ในปัจจุบันยังใช้ขอบเขต ทิศทาง และวิธีการที่น่าจะปรับปรุงได้ในหลายประการ เช่น การใช้คอมพิวเตอร์เป็นเครื่องมือช่วยในการตรวจสอบ และการกำหนดแนวทางการตรวจสอบจากความเข้าใจในระบบงานที่ประมวลผลโดยคอมพิวเตอร์ และเทคโนโลยีคอมพิวเตอร์ เช่น Terminal, off line, On line, Communications, Storage media, Programming, Database, System ต่าง ๆ เป็นต้น

3. สรุปปัญหาที่เกิดขึ้นแล้ว

3.1 เทคโนโลยีด้านคอมพิวเตอร์ได้พัฒนาเร็วกว่าพัฒนาการทางด้านการตรวจสอบและการสร้างระบบควบคุม ทั้งที่ผู้ตรวจสอบพยายามชี้ให้ผู้บริหารของกิจการต่าง ๆ เข้ามามีบทบาทในเรื่องการควบคุม แต่ก็ไม่เข้าไปช่วยเหลือในการสร้างระบบควบคุมอย่างจริงจัง ข้อเสนอแนะต่าง ๆ จากการตรวจสอบมักจะไม่ได้นำมาซึ่งความเห็นของผู้ปฏิบัติงานด้านต่าง ๆ

3.2 กิจการต่าง ๆ เปลี่ยนไปใช้ระบบงานใหม่ ๆ ที่ยุ่งยากซับซ้อน

3.3 การตรวจสอบด้านนี้เพิ่งได้รับความสนใจ

3.4 ยังขาดบุคลากรที่มีความรู้และประสบการณ์ด้านนี้

3.5 ยังขาดวิธีการตรวจสอบที่จะทันกับการเปลี่ยนแปลงที่เกิดขึ้น

3.6 การตรวจสอบยังขาดการวางแผน และการควบคุมที่ดี

3.7 ยังขาดการประสานงานที่ดีระหว่างผู้บริหาร เจ้าของงาน เจ้าหน้าที่ EDP และผู้ตรวจสอบ

4. แนวโน้มการเปลี่ยนแปลงของการตรวจสอบในอนาคต

วิธีการตรวจสอบเท่าที่เคยทำกันมาพอจะสรุปได้เป็น 2 ลักษณะ คือ รวบรวมเอกสารต่างๆ และสอบถามเกี่ยวกับการดำเนินการของหน่วยงานและระบบงานที่ใช้คอมพิวเตอร์ แล้วประเมินความเพียงพอของการควบคุมที่มีอยู่ซึ่งเป็นวิธีการที่ใช้เวลามากและไม่ใคร่ได้ผลหลังจากนั้นจึงทำการทดสอบความถูกต้องของการทำงานในระบบคอมพิวเตอร์ ซึ่งทำได้ทั้งวิธีไม่ใช้เครื่องคอมพิวเตอร์และใช้คอมพิวเตอร์ดังได้กล่าวมาแล้ว ในเรื่องผลกระทบจากการใช้คอมพิวเตอร์ซึ่งมีปัญหาในทางปฏิบัติมากมาย

อย่างไรก็ตามในขณะที่เทคโนโลยีด้านนี้ได้เปลี่ยนแปลงไปอย่างรวดเร็ว แต่งานด้านการตรวจสอบยังขาดทั้งบุคลากรที่มีประสบการณ์ และวิธีการตรวจสอบที่ทันกับการเปลี่ยนแปลงที่เกิดขึ้นเป็นผลให้การทำงานของผู้ตรวจสอบเท่าที่ผ่านมาอยู่ในลักษณะที่ทำงานให้ลุล่วงไปเป็นเรื่อง ๆ เท่านั้น ขาดการวางแผนและควบคุมที่เหมาะสม สภาพการณ์ดังกล่าวย่อมผลักดันให้แนวโน้มการตรวจสอบในอนาคตต้องเปลี่ยนแปลงไปจากเดิมใน 4 ลักษณะ ดังนี้

4.1 การเปลี่ยนแปลงในตัวผู้ตรวจสอบ

ในระยะต่อไปนี้ ผู้ตรวจสอบทั่วไปที่ตรวจงานเฉพาะด้าน Manual อย่างเดียวจะค่อย ๆ หดไป ผู้ตรวจสอบทั่วไปจะต้องเข้ามาตรวจสอบงานที่ประมวลด้วยระบบคอมพิวเตอร์มากขึ้น ส่วนผู้ตรวจสอบด้าน EDP จะเปลี่ยนสภาพไปในลักษณะผู้ตรวจสอบด้าน Information System ซึ่งเน้นการตรวจสอบระบบงานที่ยุ่งยากซับซ้อน ผู้ตรวจสอบด้าน Information System จะต้องรู้ระบบงานที่ใช้เทคโนโลยีสูง ๆ การใช้คอมพิวเตอร์ และโปรแกรมขั้นสูง วิธีการทางสถิติ การใช้โปรแกรมการตรวจสอบ วิธีการต่าง ๆ ที่จะนำมาใช้ทดสอบข้อมูลและระบบงาน

4.2 การเปลี่ยนแปลงกระบวนการตัดสินใจเกี่ยวกับเรื่องที่จะตรวจ

ในการเลือกเรื่องตรวจ ผู้ตรวจสอบจะต้องมีความรู้ความเข้าใจเกี่ยวกับเป้าหมายและนโยบายของกิจการทั้งในปัจจุบันและอนาคตเข้าใจหน้าที่เกี่ยวกับการประมวลผลมีการติดต่อที่ดีระหว่างส่วนงานต่าง ๆ ที่เกี่ยวข้อง ควรจะมีการสะสมระบบงานต่าง ๆ และจัดลำดับตามชนิดและความสำคัญไว้ และเมื่อมีการเปลี่ยนแปลงเกิดขึ้น ควร

ทบทวนใหม่ รมั้ดระวังการตรวจสอบเรื่องที่เกินขอบเขต ไม่ควรเสียเวลาประเมินผลการควบคุมภายในของระบบงานเก่าที่กำลังจะมีการยกเลิกเปลี่ยนแปลงแก้ไข แต่ควรจะให้ความสนใจวิธีการที่จะสร้างการควบคุมที่ดีที่จะนำมาใช้กับระบบงานใหม่

4.3 การเปลี่ยนแปลงความคิดเห็นเกี่ยวกับการควบคุมภายใน

การสร้างระบบการควบคุมภายใน ควรจะเริ่มจากระดับสูงของกิจการ แต่ผู้ตรวจสอบจะต้องเข้าใจด้วยว่า รายการต่างๆ เกิดขึ้นอย่างไร และผ่านขบวนการปฏิบัติอย่างไรจึงจะบรรลุผลและจุดประสงค์ตามที่คาดไว้ การดูเฉพาะจุดที่เตรียมไว้อาจเป็นผลให้ไม่พบสิ่งที่ผิดปกติด้านมาตรฐานการตรวจสอบของ AICPA ไม่ได้บังคับ ผู้ตรวจสอบจะต้องใช้ Audit through the computer แต่บังคับว่าผู้ตรวจสอบต้องเข้าใจระบบเพียงพอที่จะทำการตัดสินใจกำหนดขอบเขตการตรวจสอบที่ถูกต้องตามเหตุผลได้นอกจากนี้การสำรวจระบบการควบคุมภายในของระบบ EDP จะทำให้มั่นใจในขอบเขตการตรวจสอบที่สมบูรณ์และเข้าใจง่าย

4.4 การเปลี่ยนแปลงวิธีการประเมินผลการควบคุมของผู้ตรวจสอบ

เนื่องจากการพัฒนาระบบงานใหม่ ๆ ที่จะเพิ่มขึ้นอย่างรวดเร็ว และปัญหาเรื่องการขาดแคลนบุคลากรด้านนี้จะเป็นแรงผลักดันให้จำเป็นต้องมีการคิดค้นวิธีการวิเคราะห์และประเมินผลการควบคุมของกิจการที่ใช้คอมพิวเตอร์ให้เป็นไปตามหลักเหตุผล และมีประสิทธิภาพมากขึ้นสามารถสนองวัตถุประสงค์ในหลาย ๆ ด้าน โดยมีหลักการเป็นขั้น ๆ ดังนี้

- (1) ทำความเข้าใจกับผลกระทบของระบบคอมพิวเตอร์ในด้านต่างๆ
- (2) พิจารณาว่าจะทำอะไรกับระบบงานใด ต้องใช้ความพยายามในระดับไหน
- (3) ดูว่าในระบบงานนั้น ๆ มีผลเสียที่อาจเกิดขึ้นหรือไม่ มีระบบการควบคุมหรือไม่ และทำการประเมินการควบคุมต่าง ๆ
- (4) หยิบยกการควบคุมสำคัญ ๆ มาทำการทดสอบ
- (5) ให้มีการรวบรวมและจัดทำเอกสารประกอบการตรวจสอบอย่างมีประสิทธิภาพและสามารถสอบทานได้
- (6) รายงานผลการตรวจสอบในลักษณะที่จะช่วยให้การทำงานดีขึ้นและให้ข้อเสนอแนะในทางสร้างสรรค์

5. แนวความคิดในการพัฒนาการตรวจสอบ

ตามที่กล่าวมาแล้วในข้างต้นสรุปได้ว่า พัฒนาการต่าง ๆ ทางด้านการควบคุมและตรวจสอบตามไม่ทันกับการเปลี่ยนแปลง ทำให้หน่วยงานที่รับผิดชอบประสบปัญหาทั้งด้านบุคลากรและวิธีการตรวจสอบ ในการแก้ไขปัญหานี้ หน่วยงานที่รับผิดชอบด้านการตรวจสอบจำเป็นต้องคิดสร้างระบบวิธีการที่เป็นพื้นฐานสำหรับการตรวจสอบที่เข้าใจง่าย และชัดเจนสามารถใช้เป็นแนวทางการตรวจสอบของผู้ตรวจสอบได้ในระยะเริ่มแรก และผู้ตรวจสอบคนอื่นสามารถติดตามการเปลี่ยนแปลงของระบบงาน ในจุดที่ต้องการได้อย่างมีประสิทธิภาพ

"TOTAL SYSTEMS APPROACH" เป็นระบบการตรวจสอบแบบหนึ่งที่น่าจะตรวจสอบในลักษณะทั้งระบบ นั่นคือ เป็นการตรวจที่ผู้ตรวจสอบจะต้องเข้าใจระบบงานทั้งในส่วนที่ใช้คอมพิวเตอร์ และในส่วนที่ไม่ใช้คอมพิวเตอร์

หรือทั้งสองอย่างรวมกัน แทนที่จะแยกการตรวจสอบเป็นส่วน ๆ เช่นตรวจเฉพาะระบบ Manual เพียงอย่างเดียว ทั้งนี้สามารถใช้กับผู้ตรวจสอบที่มีความรู้คอมพิวเตอร์เพียงเบื้องต้น แต่ผู้ตรวจสอบผู้นั้นต้องเข้าใจระบบงานขององค์กรทั้งหมดโดยรวม ซึ่งจะช่วยให้ผู้ตรวจสอบเข้าใจระบบงานอย่างง่าย ๆ โดยการวิเคราะห์การควบคุมของระบบงานเป็นขั้น ๆ เป็นวิธีการทำงานตามหลักโครงสร้าง (Structure Approach) จะช่วยให้การตรวจสอบเป็นไปอย่างมีประสิทธิภาพและเป็นระเบียบ โดยคำนึงถึงว่า

(1) ในการตรวจสอบงานด้านคอมพิวเตอร์ ผู้ตรวจสอบไม่สามารถตรวจสอบส่วนต่าง ๆ ของระบบแยกกันได้อิสระในเมื่อต้องวิเคราะห์ถึงผลกระทบของการตรวจสอบส่วนนั้น ๆ ต่อส่วนอื่น ๆ ของระบบ เนื่องจากระบบงานที่ประมวลผลด้วยเครื่องคอมพิวเตอร์เกี่ยวพันต่อเนื่องกันตลอดการใช้ข้อมูลชุดเดียวกัน ความเชื่อถือได้ของระบบงานหนึ่ง ๆ ขึ้นอยู่กับความแน่นอนและครบถ้วนของระบบงานก่อน ในลักษณะนี้ข้อผิดพลาดอันหนึ่งสามารถตกทอดไปอยู่ในระบบงานต่าง ๆ ก่อให้เกิดการทำงานผิดพลาดได้ เช่น การตรวจสอบระบบบัญชีเงินฝากกระแสรายวัน ผู้ตรวจสอบต้องพิจารณาถึงระบบเงินฝากอื่น ระบบการหักบัญชี และระบบบัญชี เป็นต้น

(2) งานประมวลผลด้วยคอมพิวเตอร์เป็นเพียงส่วนหนึ่งของทั้งระบบงานเท่านั้นทั้งระบบงานจะรวมทั้งส่วนที่ประมวลผลด้วยคนและเครื่อง ปัญหาหลายอย่างที่เกี่ยวกับการประมวลผล มักสืบเนื่องจากผู้วางระบบไม่สนใจระบบงานส่วนที่ยังเป็น Manual โดยถือข้อสมมุติฐานที่ว่าข้อมูลที่รับเข้าไปถูกต้องและไม่สนใจถึงผลของข้อมูลที่ผลิตออกไปแล้วของระบบงานนั้น ๆ ว่าจะถูกนำไปใช้อย่างไร ผู้ตรวจสอบจึงต้องประเมินทั้งระบบ และไม่ละทิ้งงานส่วนที่เป็น Manual

อย่างไรก็ตามการที่จะใช้วิธีการตรวจสอบดังกล่าว ผู้ตรวจสอบต้องยอมรับความคิดที่ว่างานด้านคอมพิวเตอร์ไม่สามารถตรวจสอบได้โดยไม่มีความเข้าใจผลกระทบต่าง ๆ ที่มีต่อระบบงานของกิจการนั้น ผู้ตรวจสอบจะต้องชี้แจงให้ผู้ที่เกี่ยวข้องในระบบต่าง ๆ ของกิจการเห็นความจำเป็นในการสร้างระบบควบคุม ซึ่งควรจะเริ่มจากผู้บริหารที่จะกำหนดให้ใครรับผิดชอบการทำเอกสารเกี่ยวกับระบบควบคุมในลักษณะสร้างมาตรฐาน หรือตัวแทนของการควบคุมที่ควรจะมีอยู่ในที่ต่าง ๆ ของกิจการนั้นซึ่งผู้ตรวจสอบในระยะเริ่มแรกมักจะต้องเป็นผู้จัดทำ ซึ่งต้องใช้เวลามากเกินกว่าครึ่งหนึ่งของเวลาการตรวจสอบแต่ก็เป็นงานสำคัญในการตรวจสอบ แทนที่จะมุ่งใช้เวลาตรวจสอบระบบการควบคุมที่กิจการกำลังใช้อยู่โดยประมวลจากเอกสารและการสอบถาม แล้วประเมินไปตามความเห็นของผู้ตรวจสอบโดยไม่คำนึงถึงความเห็นของผู้เกี่ยวข้อง เช่นที่ปฏิบัติกันอยู่ในปัจจุบัน

ในระยะยาวมาตรฐานและการควบคุมต่าง ๆ จะต้องมีการพัฒนา และใช้โดยเจ้าของงาน เจ้าหน้าที่ EDP และผู้บริหาร ซึ่งมีหน้าที่โดยตรง บทบาทของผู้ตรวจสอบก็ควรอยู่ในลักษณะกระตุ้นเตือนผู้บริหาร เจ้าของงาน และเจ้าหน้าที่ EDP เกี่ยวกับการควบคุมในจุดที่ต้องปรับปรุง และทำหน้าที่ตรวจและประเมินผลการควบคุมต่าง ๆ อย่างแท้จริงได้

6. การเปลี่ยนแปลงที่ได้เกิดขึ้นในระบบงานยุคใหม่ที่ใช้คอมพิวเตอร์

การตรวจสอบการบันทึกรายการบัญชีในระบบเดิม (Manual System) จะต้องคำนึงถึงความไม่แน่นอนในการปฏิบัติงานของพนักงาน (inconsistency of people) เป็นหลักในการตรวจสอบ แต่จะนำหลักการนี้มาใช้ในการตรวจสอบระบบบัญชีที่ใช้คอมพิวเตอร์ไม่ได้ เพราะเป็นที่ยอมรับกันโดยทั่วไปแล้วว่า การทำงานของคอมพิวเตอร์นั้นแม่นยำแน่นอน และสม่ำเสมอ เพราะใช้โปรแกรมชุดเดียวกันในการประมวลผลข้อมูลด้านบัญชีที่เหมือน ๆ กันไปบันทึกบัญชีตามที่กำหนดไว้ด้วยคอมพิวเตอร์ (consistency of computers) เช่น

- การบันทึกบัญชีเงินฝากรายตัวแต่ละประเภท
- การคำนวณดอกเบี้ยเงินฝากตามประเภทเงินฝาก อัตราดอกเบี้ย และระยะเวลา
- การบันทึกเงินให้สินเชื่อรายตัวแต่ละประเภท
- การควบคุมอำนาจการให้สินเชื่อของผู้มีอำนาจในการปล่อยสินเชื่อ
- การคำนวณดอกเบี้ยส่วนลดเงินให้สินเชื่อตามประเภทเงินให้สินเชื่อ อัตราดอกเบี้ย และระยะเวลา
- การออกรายงานแยกประเภทหลักประกันสินเชื่อ ประเภทสินเชื่อ ธุรกิจที่ธนาคารให้สินเชื่อ
- การแยกประเภทการออกหนังสือค้ำประกันลูกค้า
- การคำนวณค่าเสื่อมราคาทรัพย์สินถาวร
- การบันทึกบัญชีรายได้ รายจ่าย กำไรขาดทุน
- การบันทึกบัญชีทรัพย์สิน หนี้สิน ส่วนของผู้ถือหุ้น
- การบันทึกบัญชีแยกประเภททั่วไป
- การจัดทำงบการเงิน เช่น งบดุล งบกำไรขาดทุน งบกำไรสะสม
- อื่น ๆ

ดังนั้นผู้ตรวจสอบจึงจำเป็นต้องปรับปรุงวิธีการตรวจสอบให้เหมาะสมและสอดคล้องกับวิธีการปฏิบัติงานขององค์กรที่เปลี่ยนจากระบบ Manual เป็นระบบ Computer ด้วย

6.1 วัตถุประสงค์ในการตรวจสอบ

ผู้ตรวจสอบภายใน (Internal Auditor) และผู้สอบบัญชี (External Auditor) เป็นกลุ่มบุคคลที่ทำหน้าที่ตรวจสอบการปฏิบัติงานและฐานะการเงินขององค์กร ผู้ตรวจสอบภายในจะเน้นความสำคัญของการตรวจสอบของการปฏิบัติงาน ในขณะที่ผู้สอบบัญชีให้ความสำคัญเกี่ยวกับการตรวจสอบระบบการบัญชีและงบการเงิน แต่อย่างไรก็ตามบุคคลทั้งสองกลุ่มก็มีวัตถุประสงค์ของการตรวจสอบเหมือนกันคือ

- 6.1.1 ตรวจสอบเพื่อให้แน่ใจว่า ในองค์กรนั้นมีและใช้ระบบการควบคุมที่เหมาะสม
- 6.1.2 ตรวจสอบว่าการใช้ทรัพย์สินมีประสิทธิภาพหรือไม่
- 6.1.3 ตรวจสอบว่ามีการป้องกันรักษาทรัพย์สินขององค์กรอย่างเหมาะสมหรือไม่
- 6.1.4 ตรวจสอบว่าระบบการบันทึกข้อมูลและการจัดทำงบการเงิน ถูกต้องและเชื่อถือได้หรือไม่

ในปัจจุบันมีการนำคอมพิวเตอร์มาใช้งานด้านบัญชีและการจัดทำงบการเงินกันอย่างแพร่หลายก็มีได้ทำให้วัตถุประสงค์ในการตรวจสอบของผู้ตรวจสอบภายในและผู้สอบบัญชีเปลี่ยนแปลงไปแต่ที่เปลี่ยนแปลงไปอย่างชัดเจนก็คือ วิธีและเทคนิคที่ใช้ในการตรวจสอบ

6.2 สาเหตุที่คอมพิวเตอร์ทำให้ผู้ตรวจสอบต้องเปลี่ยนแปลงวิธีและเทคนิคในการตรวจสอบ

การนำคอมพิวเตอร์มาใช้งานด้านการบัญชีขององค์กร ไม่ทำให้ระบบการบัญชีมาตรฐานที่ผู้ตรวจสอบส่วนใหญ่คุ้นเคยอยู่แล้วเปลี่ยนแปลงไป แต่สิ่งที่เปลี่ยนแปลงไปและมีผลต่องานตรวจสอบก็คือ

6.2.1 ลักษณะภายในและภายนอกของแฟ้มหรือทะเบียน (Logical and Physical Structure of File) ที่ใช้บันทึกข้อมูลทางบัญชี

- 1) วิธีการนำข้อมูลไปบันทึก (The way to access)
- 2) วิธีการนำข้อมูลมาใช้ (The way to read)
- 3) วิธีการนำข้อมูลไปประมวลผล (The way to process)

นอกจากนี้ เมื่อข้อมูลที่อยู่ใน File เปลี่ยนแปลง จะไม่มีร่องรอยการเปลี่ยนแปลงให้เห็น (Trace) ดังเช่น วิธีการบันทึกบัญชีแบบเดิม จึงไม่สามารถตรวจสอบความถูกต้องของข้อมูลใน File ได้โดยใช้วิธีและเทคนิคการตรวจสอบแบบธรรมดา

6.2.2 รอยทางสำหรับการตรวจสอบ (audit trails) เปลี่ยนแปลงไปผู้ตรวจสอบไม่สามารถติดตามการเคลื่อนไหวของเอกสาร (flow of paper documentation) ตามวิธีการตรวจสอบแบบธรรมดาได้อีกต่อไปเพราะข้อมูลในเอกสารการบัญชีเบื้องต้นจะถูกแปลงสภาพเป็นรหัสหรือสัญญาณที่ผู้ตรวจสอบไม่สามารถอ่านเข้าใจได้และเก็บไว้ในสื่อ (medium) ที่ไม่สามารถสัมผัสหรือมองด้วยตาเปล่าได้ ดังนั้น ผู้ตรวจสอบอาจจำเป็นต้องใช้วิธีอื่นและ/หรือโปรแกรมคอมพิวเตอร์ช่วยในการตรวจสอบ

6.2.3 การเปลี่ยนแปลงที่สำคัญคือ การเปลี่ยนแปลงวิธีปฏิบัติการด้านการบัญชีทั้งหมดซึ่งแต่เดิมเป็นหน้าที่ของพนักงานบัญชี (book keepers and clerks) โดยเปลี่ยนมาใช้โปรแกรมคอมพิวเตอร์ทำหน้าที่แทน ซึ่งจะก่อให้เกิดขั้นตอนการปฏิบัติงานและจัดการควบคุมภายในแบบดั้งเดิมหมดไป ทำให้ผู้ตรวจสอบทางการเงินทั่วไปอาจประสบกับปัญหาที่ไม่อาจประเมินงานควบคุมภายในระบบคอมพิวเตอร์ได้ และทำให้มีปัญหาในการกำหนดขอบเขตและวิธีการตรวจสอบที่เหมาะสม

การมอบหมายให้คอมพิวเตอร์ทำหน้าที่แทนพนักงานบัญชี มีข้อที่ผู้ตรวจสอบควรพิจารณา 2 ประการคือ

- 1) บุคคลที่ได้รับมอบหมายให้ควบคุมระบบคอมพิวเตอร์อาจจะมีความรู้ความเข้าใจระบบการบัญชีไม่เพียงพอและ
- 2) ไม่เข้าใจระบบการควบคุมและการตรวจสอบระบบงานด้านคอมพิวเตอร์อย่างถ่องแท้

ปัจจัยทั้งสองประการจะมีผลทำให้ระบบคอมพิวเตอร์มีจุดอ่อนที่ง่ายต่อการผิดพลาดหรือที่ร้ายแรงก็คือการทุจริต ดังนั้นหน้าที่ประการแรกของผู้ตรวจสอบเมื่อเข้าไปตรวจสอบระบบคอมพิวเตอร์ คือ การประเมินระบบการควบคุมภายในซึ่งเป็นงานสำคัญของ EDP auditor

6.3 ร่องรอยสำหรับการตรวจสอบในระบบคอมพิวเตอร์

ร่องรอยการตรวจสอบ (Audit trail) สำหรับระบบการประมวลผลข้อมูลที่ไม่ได้ใช้คอมพิวเตอร์ ได้แก่

6.3.1 เอกสารหรือข้อมูลเบื้องต้น เช่น พวกร Slip และเอกสารประกอบรายการทางการเงินอื่น ๆ

6.3.2 สมุดรายวัน การ์ดบัญชี

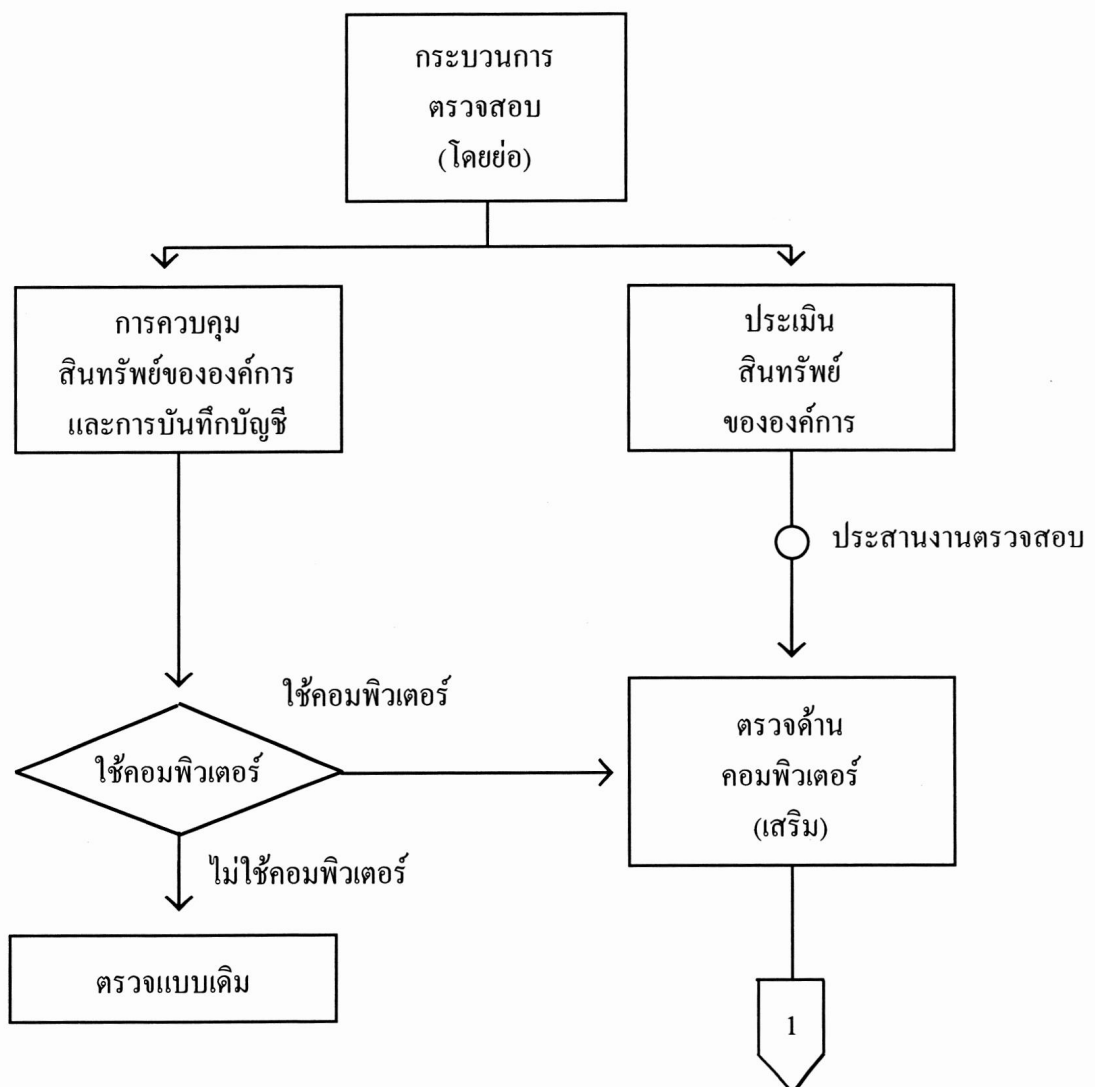
6.3.3 สมุดบัญชีแยกประเภททั่วไป และทะเบียนต่าง ๆ

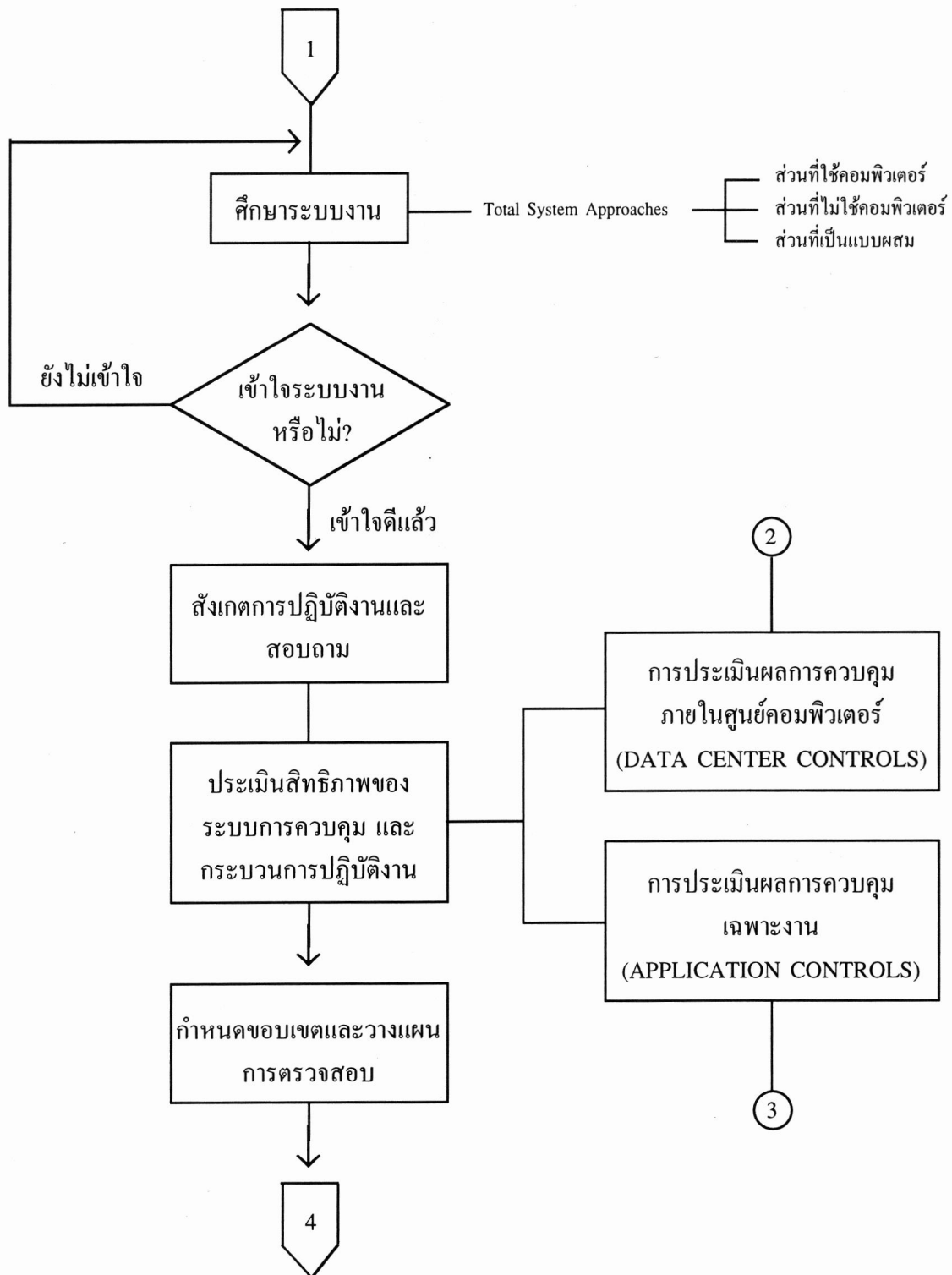
6.3.4 รายงานงบการเงิน

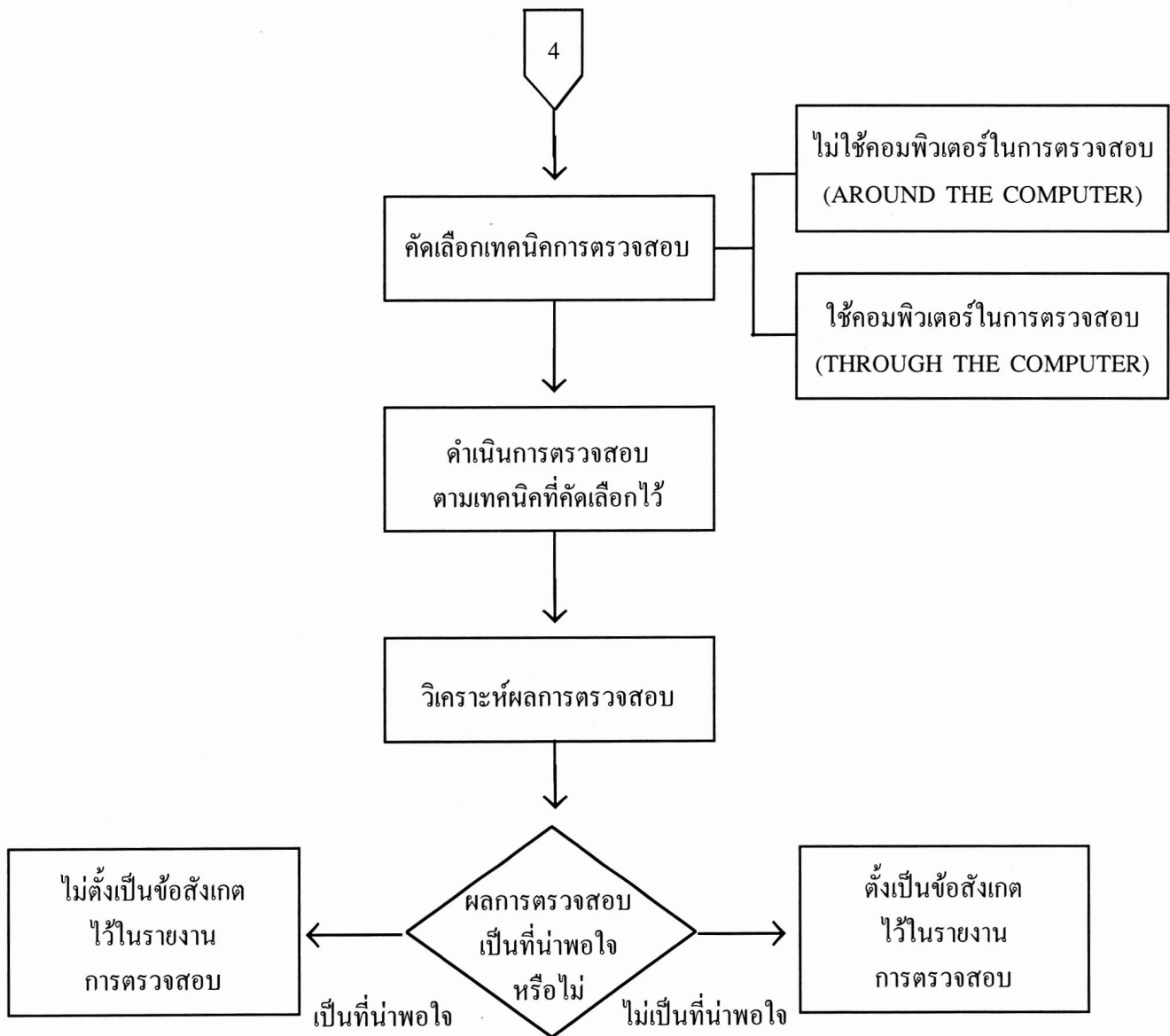
ร่องรอยดังกล่าวจะช่วยให้ผู้ตรวจสอบสามารถตรวจสอบย้อนกลับไประหว่างจุดเริ่มต้นที่เกิดรายการทางการเงิน (Transactions) กับรายการสรุปผลทางการเงิน (Summarized total) เพื่อให้แน่ใจว่ารายงานทางการเงินที่ได้นั้นสะท้อนให้เห็นธุรกรรมทางการเงินขององค์กรอย่างแท้จริง

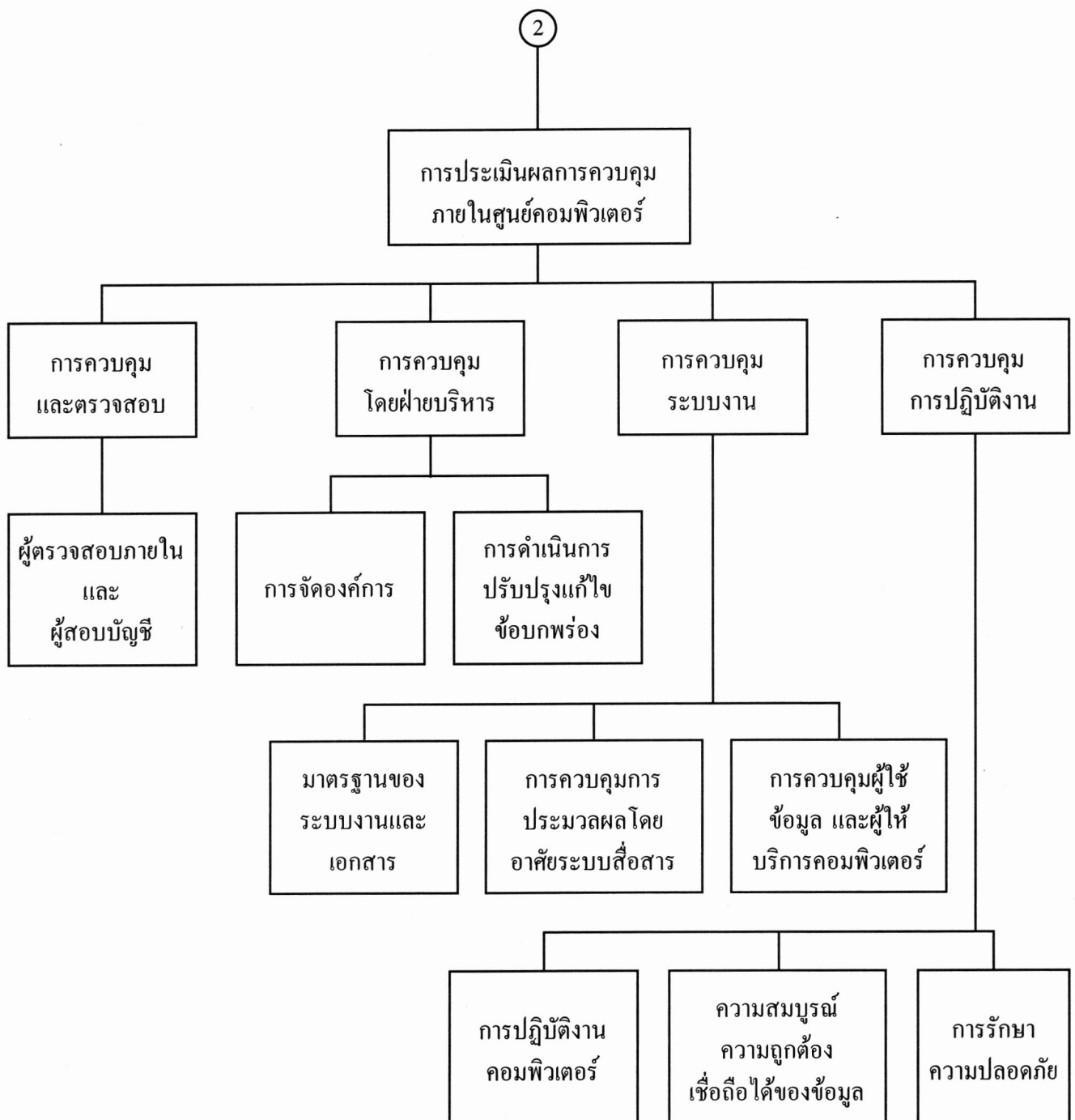
เพื่อไม่ให้เกิดการเข้าใจผิด เราควรจะเรียกร่องรอยนี้ว่า management trail มากกว่าจะเรียกว่า audit trail เพราะสิ่งนี้จะเป็ประโยชน์แก่ผู้บริหารงานประจำมากกว่าผู้สอบบัญชี โดยเฉพาะในกรณีที่แหล่งภายนอกต้องการข้อมูลบางอย่างเป็นพิเศษ

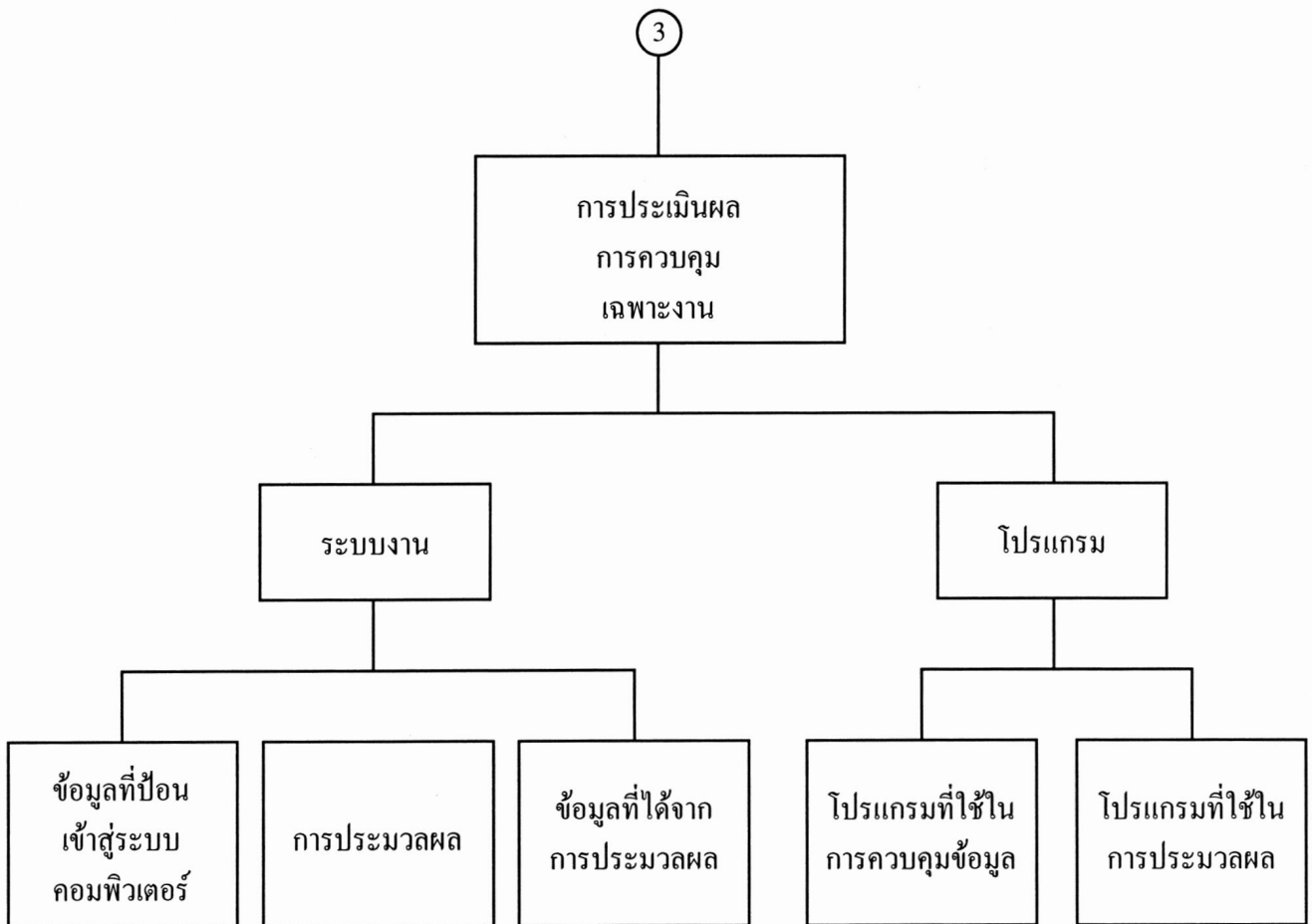
6.4 การกำหนดขอบเขตและวางแผนตรวจสอบและกระบวนการวางแผนโดยแผนภูมิ











7. ความคิดบางประการของการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

7.1 คอมพิวเตอร์กับผลของการประเมินการควบคุมภายใน

- อาจไม่มีผลประการใด ๆ
- อาจมีผลกระทบเล็กน้อย
- อาจมีผลกระทบอย่างสำคัญ

ผู้บริหารขององค์กรต้องกำหนดให้มีการวางแผนกฎเกณฑ์ในการควบคุมภายในอย่างมีประสิทธิภาพ เช่น การกำหนดอำนาจและการแบ่งแยกหน้าที่ การกำหนดให้มีเอกสารและการบันทึกบัญชีที่สมบูรณ์ ถูกต้อง ทันกาล ฯลฯ

7.2 ความรับผิดชอบของผู้บริหารต่อการควบคุมและการตรวจสอบ

มีผู้เกี่ยวข้อง 3 กลุ่มในการวางแผนการปฏิบัติงานและการควบคุม คือ

- 1) คณะกรรมการบริหารและ Audit Committee
- 2) ผู้ดำเนินงาน (Operating management) และ
- 3) ผู้สอบบัญชีภายใน (Internal Auditors) หรืออาจมี (External auditors) ร่วมด้วยก็ได้

7.3 บทบาทของคณะกรรมการบริหาร (Board of Directors)

วางแผนและจัดให้มีการควบคุมภายในของระบบงานต่าง ๆ ในภาพรวมอย่างกว้าง ๆ เพื่อลดความเสี่ยงต่าง ๆ ในส่วนที่เกี่ยวข้องกับ Operating และกำหนดให้มี Audit functions ขึ้นมาติดตามดูแลการปฏิบัติตามกฎเกณฑ์ต่าง ๆ ที่ได้จัดให้มีขึ้น

7.4 บทบาทของฝ่ายจัดการหรือผู้ดำเนินงาน

เป็นผู้รับผิดชอบการควบคุมภายในของคณะกรรมการบริหารมาปฏิบัติ โดยจัดให้มีระเบียบ พิธีปฏิบัติ และกำหนดกฎเกณฑ์ต่าง ๆ ให้ User และผู้ที่เกี่ยวข้องได้ปฏิบัติเพื่อให้การบันทึกบัญชีต่าง ๆ มีความน่าเชื่อถือได้ และเป็นไปตามตัวบทกฎหมายที่เกี่ยวข้อง

7.5 หน้าที่ของ Board of Directors หรือ Audit Committee ในองค์กรที่ใช้คอมพิวเตอร์ ควรจะครอบคลุมถึงการดูแลฝ่ายจัดการให้มีการปฏิบัติในเรื่องต่อไปนี้ :-

- ระบุประเภทของความเสี่ยงต่าง ๆ ในแต่ละกิจกรรม รวมถึงสาเหตุความผิดพลาด และความผิดปกติต่าง ๆ ที่อาจจะเกิดขึ้นในองค์กรของตน
- จัดให้มีการควบคุมเพื่อลดความเสี่ยงและความผิดปกติต่าง ๆ ที่ได้พิจารณาแล้วนั้น โดยกำหนดเป็นระเบียบและวิธีปฏิบัติงานเป็นลายลักษณ์อักษร ให้ผู้เกี่ยวข้องยึดถือเป็นแนวปฏิบัติงานเพื่อให้งานดำเนินไปอย่างมีประสิทธิภาพน่าเชื่อถือได้
- ดูแลให้มีการปฏิบัติตามหลักการที่ได้กำหนดขึ้นแล้ว

7.6 บทบาทของผู้สอบบัญชีภายใน

- ติดตามดูแลให้มีการปฏิบัติตามนโยบายและวิธีการปฏิบัติงานตามที่คณะกรรมการบริหารและฝ่ายจัดการได้กำหนดขึ้น
- ช่วยเหลือคณะกรรมการบริหารงานและฝ่ายจัดการตามที่ได้รับมอบหมาย โดยเฉพาะอย่างยิ่งเข้าไปมีส่วนร่วมการจัดวางให้มีระบบการควบคุมและระบบตรวจสอบตั้งแต่ในระยะขั้นตอนการพัฒนากระบวนการ
- ปรับปรุง ศึกษา ค้นคว้า เทคนิคที่เกี่ยวข้องกับการพัฒนาทางเทคโนโลยีทางด้านคอมพิวเตอร์ เพื่อรักษามาตรฐานการปฏิบัติงานให้เหมาะสมกับสิ่งแวดล้อมที่เปลี่ยนแปลงไป

7.7 บทบาทของผู้สอบบัญชีภายนอก

- ประเมินความน่าเชื่อถือได้ของระบบการควบคุมภายใน เพื่อกำหนดขอบเขตการปฏิบัติงานตรวจสอบในเรื่องที่เกี่ยวข้อง
- ทดสอบการควบคุมภายในและการปฏิบัติงานที่สำคัญ หากพิจารณาว่าการควบคุมภายในน่าเชื่อถือได้
- ทดสอบความน่าเชื่อถือได้ของข้อมูลทางการเงินและการเงินในงบการเงิน ในกรณีที่ External auditor พบจุดอ่อนหรือความผิดปกติของการควบคุมภายในที่มีนัยสำคัญหรือพบเรื่องที่มีการปฏิบัติฝ่าฝืนกฎหมาย หรือ กฎระเบียบ ข้อบังคับของบริษัท External auditor จะต้องแจ้งให้ Operating Management ทราบด้วยเสมอ

7.8 ความรับผิดชอบของการตรวจสอบทางด้าน Computer หรือ IS

มาตรฐานการตรวจสอบทางด้าน Field work ที่เกี่ยวข้องกับการประเมินการควบคุมภายใน ในองค์กรที่ใช้คอมพิวเตอร์ ผู้ตรวจสอบจะครอบคลุมถึงเรื่องต่อไปนี้ด้วย คือ

- ความเข้าใจพื้นฐานของทางเดินของรายการในแต่ละระบบงานตั้งแต่ต้นจนจบ
- ความเข้าใจพื้นฐานของโครงสร้างการควบคุม (Basic control structure) ทั้งในส่วนที่เป็น Manual และส่วนที่เป็น Computer
- ความตั้งใจถึงการตรวจสอบใน file ต่าง ๆ ที่ใช้ในการทำงานการเงิน
- ในกรณีที่ใช้คอมพิวเตอร์เข้าช่วยในการตรวจสอบ หากโปรแกรมนั้นพัฒนาโดยองค์กรที่ถูกตรวจสอบแล้ว ผู้สอบบัญชีจะต้องทดสอบโปรแกรมนั้นก่อนให้ความเชื่อถือข้อมูลที่ได้จากการตรวจสอบด้วยเสมอ
- การประเมินการควบคุมภายในด้านคอมพิวเตอร์และการใช้คอมพิวเตอร์เข้าช่วยในการตรวจสอบ จะต้องดำเนินการโดยผู้ตรวจสอบที่มีประสบการณ์ด้านคอมพิวเตอร์อย่างเพียงพอ
- การประเมินการควบคุมในด้านคอมพิวเตอร์ ผู้ประเมินจะต้องมีความเข้าใจในลักษณะโครงสร้างของการควบคุมในองค์กรที่ตรวจสอบอย่างแท้จริง นั่นคือ ผู้ตรวจสอบควรจะทราบว่าองค์กรนั้น

ควรต้องมีการควบคุมภายในอย่างไรบ้างแทนที่จะประเมินหรือติดตามแต่เพียงว่าองค์กรนั้นได้ปฏิบัติตามการควบคุมที่มีอย่างไร เป็นต้น

- ผู้ประเมินต้องรวบรวมหลักฐานที่มีเพื่อยืนยันความเข้าใจในระบบการควบคุมภายในด้านคอมพิวเตอร์

7.9 วิธีการตรวจสอบระหว่างระบบงานด้านคอมพิวเตอร์

ผู้ตรวจสอบงานด้าน Computer หรือ Computer/EDP auditor หรือ Information System (IS) auditor ที่ประสบความสำเร็จ การตรวจสอบนั้นควรจะตั้งอยู่บนพื้นฐานดังนี้

- มีความเข้าใจในวิธีการตรวจสอบขององค์กรที่ใช้คอมพิวเตอร์อย่างเพียงพอ และ
- มีพื้นฐานความรู้ทางคอมพิวเตอร์ เทคโนโลยีและ Concept ของการตรวจสอบงานด้าน Computer ที่จะกำหนดขอบเขตและขั้นตอนการตรวจสอบที่ได้ผล

ขั้นตอนการตรวจสอบข้างต้นนั้น มีรายละเอียดและขั้นตอนที่ผู้ตรวจสอบพึงทราบและพึงเข้าใจหลายประการในเรื่องระบบงานและรายการต่าง ๆ ที่ประมวลผล โดยเฉพาะอย่างยิ่งขั้นตอนการรวบรวมและประมวลเอกสาร และหลักฐานการตรวจสอบที่เกี่ยวข้อง

วิธีการตรวจสอบดังกล่าว ได้ครอบคลุมโครงสร้างขององค์กรทั้งในแนวดิ่งและแนวนอน ผู้ตรวจสอบต้องเข้าใจธุรกิจที่จะตรวจสอบอย่างถ่องแท้ต้องเข้าใจกิจกรรมต่าง ๆ ในแต่ละงาน (Application) ที่ตรวจสอบ และแน่นอนว่าผู้ตรวจสอบต้องเข้าใจโครงสร้างของการควบคุม (Structure of control) ที่จำเป็นในแต่ละกิจกรรมนั้น เพื่อบรรลุวัตถุประสงค์ของการตรวจสอบด้วยเสมอ

โดยสรุป วิธีการตรวจสอบขององค์กรที่ใช้คอมพิวเตอร์จะช่วยให้ผู้ตรวจสอบคำนึงถึง

- ผู้ตรวจสอบจะต้องตรวจสอบอะไร อย่างไร ด้วยวิธีการใด
- เมื่อใดที่ควรจะมีการตรวจสอบหรือทดสอบ
- เอกสารอะไรบ้างที่ต้องการตรวจสอบ





ขั้นตอนและกระบวนการ
ตรวจสอบโดยย่อ

ขั้นตอนและกระบวนการตรวจสอบโดยย่อ

1. ขั้นตอนการตรวจสอบ

อาจแบ่งขั้นตอนการตรวจสอบเป็น 3 ขั้นตอนใหญ่ ๆ ได้ดังนี้

ขั้นตอนที่ 1 การวิเคราะห์ความเพียงพอของการควบคุมภายใน

โดยการตั้งวัตถุประสงค์การตรวจสอบขอบเขตการตรวจสอบ และการวางแผนการตรวจสอบ แล้วรวบรวมข้อมูลเบื้องต้นที่เกี่ยวข้องกับการตรวจสอบ เพื่อประเมินความน่าเชื่อถือได้ของการดำเนินงานและการควบคุมภายในแบบ Total system approach คือ ดูทั้งส่วนที่เป็น Manual และ Computer จากนั้นก็กำหนดแนวการตรวจสอบขั้นตอนต่อไป

ในขั้นตอนนี้ ผู้ตรวจสอบควรประเมินและวิเคราะห์ความเสี่ยงในแต่ละรายงานและในแต่ละกิจกรรมของงานที่ตรวจสอบ วิธีที่ดีที่สุด คือ การตั้งคำถามว่า "มีอะไรที่จะก่อให้เกิดข้อผิดพลาดขึ้นได้" ระบุจุดที่การควบคุมเพื่อลดความเสี่ยง อันจะก่อให้เกิดความเสียหายนั้น

เทคนิคที่ใช้วิเคราะห์ก็คือ การสัมภาษณ์ การใช้แบบสอบถาม การวิเคราะห์ Flowchart

ขั้นตอนที่ 2 ทดสอบการปฏิบัติงานตามระเบียบที่ได้กำหนดไว้ (Compliance Tests)

เมื่อผู้ตรวจสอบได้ทำการระบุจุดที่ควรมีการควบคุมในความเสี่ยงแต่ละจุดแล้วก็ต้องประเมินว่า การควบคุมนั้นน่าเชื่อถือหรือไม่ ถ้าเชื่อถือได้ก็จะได้ทำการทดสอบการปฏิบัติงาน (Computer Tests) ที่เกี่ยวข้องกับการควบคุมภายในเพื่อประเมินจุดอ่อนหรือข้อผิดพลาดที่อาจยังมีและมีความสำคัญต่อไป โดยเฉพาะอย่างยิ่ง ข้อผิดพลาดที่อาจเกี่ยวข้องกับข้อมูลทางการ ซึ่งอาจต้องทำการทดสอบต่อไป ขั้นตอนนี้ ยังมีการรวบรวมรายละเอียดเพื่อการตรวจสอบเพิ่มเติมด้วย

เทคนิคที่ใช้ในการตรวจสอบขั้นนี้ก็คือ การสังเกตการณ์ การทำ Test data หรือ Manual trading

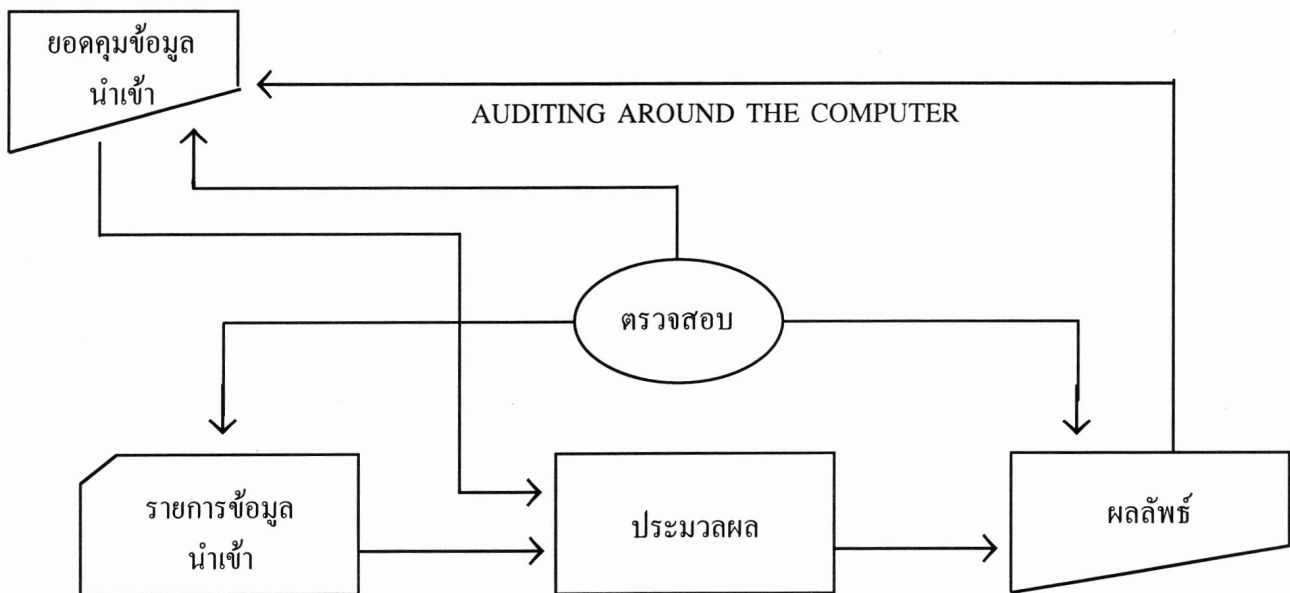
ขั้นตอนที่ 3 ทดสอบข้อมูลทางการเงิน (Substantive tests) เช่น ยอดคงเหลือ รายการทางบัญชีต่าง ๆ และยอดรวมของบัญชีในงบการเงิน ด้วยวิธีการที่เหมาะสมแล้ว ทำรายงานการตรวจสอบ

ขั้นตอนย่อยในการตรวจสอบจากสามขั้นตอนใหญ่ ๆ ข้างต้นอาจใช้การตรวจสอบแบบ Around หรือ Through the computer

2. การตรวจสอบ

2.1 การตรวจสอบแบบ Around/through the computer

การตรวจสอบคอมพิวเตอร์ในระยะเริ่มแรกเป็นการตรวจสอบแบบ "Auditing around the computer" เพื่อสอบถามความถูกต้องของข้อมูลที่ปรากฏในรายงานคอมพิวเตอร์คล้ายกับการตรวจสอบสมุดทะเบียนบัญชีแยกประเภทและเอกสารที่เกี่ยวข้องในระบบเดิมที่ใช้พนักงานบันทึกรายการ ดังรูป



ในปี ค.ศ. 1966 คณะทำงานพิเศษ Audit EDP Task Force ของ The American Institute of Certified Public Accountants (AICPA) ขอให้ใช้คำอื่น ๆ เช่น "Auditing without using the computer" แทนคำ "Auditing around the computer" เพราะอาจทำให้ผู้ตรวจสอบเกิดความเข้าใจคลาดเคลื่อนว่า ไม่จำเป็นต้องประเมินผลการควบคุมภายในด้านคอมพิวเตอร์ก็ได้ หากผู้ตรวจสอบได้ดำเนินการติดตามความเคลื่อนไหวของรายการที่ปรากฏในรายงานคอมพิวเตอร์ เพื่อพิสูจน์ความถูกต้องของข้อมูล

สำหรับการตรวจสอบแบบ "Auditing through the computer" หรือ Computer assisted audit techniques" มีความหมายชัดเจนอยู่ในตัวแล้ว แต่อย่างไรก็ดี คำ "Auditing around/through the computer" ได้มีความสำคัญลดน้อยลง เมื่อสถาบันที่ทำหน้าที่ควบคุมการประกอบวิชาชีพสอบบัญชีหลายประเทศได้กำหนดมาตรฐานตรวจสอบคอมพิวเตอร์ให้ผู้ตรวจสอบถือปฏิบัติ

2.2 มาตรฐานการตรวจสอบ

มาตรฐานการตรวจสอบคอมพิวเตอร์ที่ควรทราบ มีดังนี้

ประเทศสหรัฐอเมริกา

เมื่อเดือนธันวาคม ค.ศ. 1974 AICPA ได้ออก Statement of Auditing Standard No.3 (SAS #3) มี 3 ประเด็นสำคัญสรุปได้ดังนี้

- (1) กรณีที่มีการใช้คอมพิวเตอร์กับงานบัญชีที่มีนัยสำคัญ ผู้ตรวจสอบควรสอบทานระบบเพื่อทำความเข้าใจในเรื่องต่อไปนี้
 - (1.1) ทางเดินของรายการบัญชี
 - (1.2) ขอบเขตการใช้คอมพิวเตอร์

- (1.3) โครงสร้างพื้นฐานของการควบคุมภายใน
- (2) กรณีงานคอมพิวเตอร์มีความสลับซับซ้อน จะต้องให้ผู้เชี่ยวชาญร่วมงานตรวจสอบด้วย
- (3) การใช้คอมพิวเตอร์ไม่มีผลกระทบต่อการควบคุมทางบัญชี แต่อาจมีผลกระทบต่อการองค์กรและวิธีการที่จะทำให้บรรลุเป้าหมายในการควบคุม ซึ่งมีอิทธิพลต่อวิธีการตรวจสอบ

ประเทศแคนาดา

The Canadian Institute of Chartered Accountants (CICA) ได้ออก Guideline : Auditing in an Electronic Data Processing Environment เมื่อเดือนสิงหาคม ค.ศ.1981 เพิ่มเติมจาก Computer Control Guidelines และ Computer Audit Guidelines ซึ่งออกในปี ค.ศ.1970 และปี ค.ศ. 1974 ตามลำดับ สารสำคัญสรุปได้ดังนี้

- (1) กรณีใช้ผู้เชี่ยวชาญคอมพิวเตอร์ ผู้ตรวจสอบต้องมีความรู้ด้านคอมพิวเตอร์ เพื่อควบคุมการปฏิบัติงานของผู้เชี่ยวชาญให้เหมาะสม
- (2) ผู้ตรวจสอบต้องประเมินความเพียงพอเกี่ยวกับความรู้ด้านคอมพิวเตอร์ของตนเอง
- (3) ควรพิจารณาหรือศึกษาระบบทั้งด้าน Manual และด้านคอมพิวเตอร์พร้อมๆ กับการพัฒนาวิธีการตรวจสอบ แต่ผู้ตรวจสอบไม่จำเป็นต้องตรวจสอบระบบโดยละเอียด หากพิจารณาในขั้นต้นแล้วเห็นว่าเป็นระบบที่เชื่อถือไม่ได้
- (4) ผู้ตรวจสอบต้องประเมินผลการควบคุมภายในทั่วไป (General controls) และ Operating system ด้านคอมพิวเตอร์
- (5) กรณีใช้คอมพิวเตอร์ช่วยตรวจสอบต้องจัดให้มีการควบคุมอย่างเพียงพอ เพื่อให้ได้ผลลัพธ์ครบถ้วนและเป็นไปตามวัตถุประสงค์ในการตรวจสอบ
- (6) ผู้ตรวจสอบควรมีส่วนร่วมในการพัฒนาระบบงานด้วย

สหราชอาณาจักร (United Kingdom)

Auditing Practices Committee Exposure Draft : Internal Controls in Computer-Based Accounting System ออกเมื่อเดือนพฤษภาคม ค.ศ.1982 มีสาระสำคัญสรุปได้ ดังนี้

- (1) ผู้ตรวจสอบไม่จำเป็นต้องเข้าใจระบบโดยละเอียด เว้นแต่จะมีแผนการตรวจสอบเพื่อให้ความเชื่อถือต่อระบบงานนั้น
- (2) ผู้ตรวจสอบต้องประเมินผลการควบคุมภายในเฉพาะงาน (Application controls) และการควบคุมภายในทั่วไป (General controls)
- (3) ผู้ตรวจสอบสามารถใช้คอมพิวเตอร์ช่วยตรวจสอบเพื่อที่จะได้หลักฐานการปฏิบัติงานที่อยู่ภายใต้การควบคุมภายในเฉพาะงาน
- (4) ผู้ตรวจสอบควรรู้จักวิธีปฏิบัติในการตรวจสอบคอมพิวเตอร์ไว้หลาย ๆ วิธี

ประเทศไทย

คณะกรรมการควบคุมการประกอบวิชาชีพสอบบัญชี (ก.บช.) และสมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย ได้ประกาศใช้มาตรฐานการสอบบัญชี ฉบับที่ 28 และ 29 เรื่อง "การสอบบัญชีในกรณีที่ธุรกิจใช้คอมพิวเตอร์" และเรื่อง "การประเมินประสิทธิภาพการควบคุมภายในกรณีกิจการใช้คอมพิวเตอร์" ซึ่งมีรายละเอียดค่อนข้างมากและได้มีผลบังคับใช้แล้ว ตั้งแต่ เดือนมิถุนายน 2533 เป็นต้น

3. การจัดประเภทการตรวจสอบด้านคอมพิวเตอร์

การตรวจสอบคอมพิวเตอร์แบ่งได้เป็น 2 ประเภท คือ การตรวจสอบกิจกรรมหรือการดำเนินงานของหน่วยงานคอมพิวเตอร์ (General Controls และการตรวจสอบระบบงานที่ใช้คอมพิวเตอร์ประมวลผล (Application Controls)

3.1 การตรวจสอบการดำเนินงานของหน่วยงานคอมพิวเตอร์ (General Controls)

เป็นการตรวจสอบเพื่อประเมินผลการควบคุมภายในทั่วไป ซึ่งส่วนใหญ่เป็นเรื่องเกี่ยวกับมาตรฐานการปฏิบัติงาน ระเบียบ ข้อบังคับ และเอกสารสนับสนุนการปฏิบัติงานหน่วยงานคอมพิวเตอร์และหน่วยงานอื่นที่เกี่ยวข้อง มีหัวข้อการตรวจสอบดังนี้

- 3.1.1 การตรวจสอบภายในและการสอบบัญชี เป็นการตรวจสอบเพื่อประเมินผลการปฏิบัติงานของผู้ตรวจสอบภายในและผู้สอบบัญชี ซึ่งได้รับมอบหมายจากฝ่ายบริหาร และผู้ถือหุ้นให้เป็นผู้ดำเนินการจัดระบบควบคุมภายในและตรวจสอบมีขอบเขตการปฏิบัติงานครอบคลุมในเรื่องต่าง ๆ เพียงพอหรือไม่ และเชื่อถือได้เพียงใด
- 3.1.2 การจัดการเป็นการตรวจสอบเพื่อพิจารณาถึงความสามารถในการบริหารงานคอมพิวเตอร์ ความเหมาะสมในการแบ่งแยกหน้าที่การจัดสายการบังคับบัญชาและการรายงานผลการปฏิบัติงาน
- 3.1.3 การพัฒนาระบบงานและโปรแกรม เป็นการตรวจสอบเพื่อประเมินผลการพัฒนาระบบงานและโปรแกรม การแก้ไขระบบงานและโปรแกรม และความสมบูรณ์ของเอกสารสนับสนุนการปฏิบัติงาน
- 3.1.4 การปฏิบัติงานข้อมูลเป็นการตรวจสอบงานเตรียมข้อมูลการกระทบบยอดข้อมูล และการจัดส่งข้อมูลให้ผู้ใช้ข้อมูลเพื่อประเมินผลคุณภาพของข้อมูลว่ามีความถูกต้องครบถ้วนและเชื่อถือได้ (Data integrity) เพียงใด
- 3.1.5 การปฏิบัติงานคอมพิวเตอร์ (Computer operations) เป็นการตรวจสอบการปฏิบัติงานภายในห้องคอมพิวเตอร์ การจัดเก็บแฟ้มข้อมูล การรักษาความปลอดภัย การจัดระบบสำรองเตรียมไว้ทดแทนยามฉุกเฉิน
- 3.1.6 การสื่อสารข้อมูล (กรณีใช้ Hardware และ/หรือ Software ร่วมกันหลายระบบงาน) เป็นการตรวจสอบเพื่อประเมินผลการรักษาความปลอดภัยของข้อมูลที่มีประมวลผลผ่านระบบสื่อสาร

- 3.1.7 การใช้บริการคอมพิวเตอร์ของผู้อื่นภายนอกกิจการ กรณีไม่มีเครื่องคอมพิวเตอร์เป็นของตนเอง ควรมีการตรวจสอบสัญญาการใช้บริการ การคิดค่าบริการฐานะและการดำเนินงานของศูนย์บริการคอมพิวเตอร์ นอกเหนือจากการตรวจสอบตามหัวข้อที่กล่าวมาแล้วด้วย เพื่อป้องกันธุรกิจที่จำเป็นต้องใช้ข้อมูลที่ประมวลผลด้วยคอมพิวเตอร์ต้องหยุดชะงัก หากศูนย์คอมพิวเตอร์ไม่สามารถให้บริการได้ตามปกติด้วยเหตุใด ๆ ก็ตาม

3.2 การตรวจสอบระบบงานที่ใช้คอมพิวเตอร์ประมวลผล (Application Controls)

เป็นการตรวจสอบเพื่อประเมินผลการควบคุมภายในเฉพาะงาน ซึ่งผู้ตรวจสอบจะสัมผัสกับรายการข้อมูลทุกรูปแบบ ในแต่ละระบบงานมากกว่าการตรวจสอบการดำเนินงานของหน่วยงานคอมพิวเตอร์ มีหัวข้อการตรวจสอบ ดังนี้

- 3.2.1 แหล่งกำเนิดรายการหรือแหล่งที่มาของรายการเป็นการตรวจสอบ
- การจัดทำเอกสารขั้นต้น หรือเอกสารประกอบรายการ (Source document organization)
 - การอนุมัติรายการ (Authorization)
 - การเตรียมข้อมูลนำเข้า (Data processing input preparation)
 - การเก็บรักษาเอกสารขั้นต้น (Source document retention)
 - การแก้ไขเอกสารที่มีข้อผิดพลาด (Source document error handling)
- 3.2.2 การทำรายการป้อนเข้าสู่ระบบงาน เป็นการตรวจสอบ
- การทำรายการป้อนข้อมูลเข้าสู่ระบบงาน ซึ่งอาจทำได้ 2 วิธีคือ
 - Terminal data entry
 - Batch data entry
 - หลักเกณฑ์ที่ใช้ในการควบคุมการทำรายการเพื่อให้ได้ข้อมูลที่ถูกต้องและครบถ้วน (Transaction data validation)
 - การแก้ไขข้อผิดพลาดในการทำรายการป้อนเข้าสู่ระบบงาน (Transaction error handling)
- 3.2.3 การสื่อสารข้อมูล เป็นการตรวจสอบทางเดินของข้อมูลผ่านระบบสื่อสาร ซึ่งประกอบด้วย
- การใช้เครื่อง Terminal ส่งข้อมูลหรือข่าวสาร ป้อนเข้าสู่ระบบงาน (message input)
 - การเคลื่อนย้ายข้อมูลในระบบสื่อสาร (Message transmission) ซึ่งต้องอาศัย Hardware และ Software ควบคุมการเคลื่อนย้ายข้อมูล
 - การบันทึกรายละเอียดในการติดต่อสื่อสารระหว่างเครื่อง Terminal กับ CPU ไว้ที่ศูนย์คอมพิวเตอร์ (Message reception and accounting)

3.2.4 การประมวลผล ได้แก่ การตรวจสอบ

- ความเคลื่อนไหว หรือทางเดินของข้อมูลที่ประมวลผลในแต่ละโปรแกรมหรือระบบงานเพื่อพิจารณาว่าการประมวลผลทุกขั้นตอนมีความถูกต้องครบถ้วนและเชื่อถือได้ (processing integrity) เพียงใด
- การกำหนดจุดตั้งต้นในแต่ละขั้นตอนของการประมวลผล และการแก้ไขสถานการณ์ให้กลับคืนสู่สภาพปกติเมื่อเกิดเหตุขัดข้อง (Restart and recovery)
- ความถูกต้องแม่นยำของโปรแกรมที่ใช้ประมวล (Processing accuracy)
- การปฏิบัติงานของพนักงานคุมเครื่องคอมพิวเตอร์ในระหว่างดำเนินการประมวลผล (Operator intervention)
- การมอบอำนาจปฏิบัติงานและการรักษาความปลอดภัยในการดำเนินการประมวลผล (Security and privacy)
- การแก้ไขข้อผิดพลาดที่อาจเกิดขึ้นในระหว่างการประมวลผล

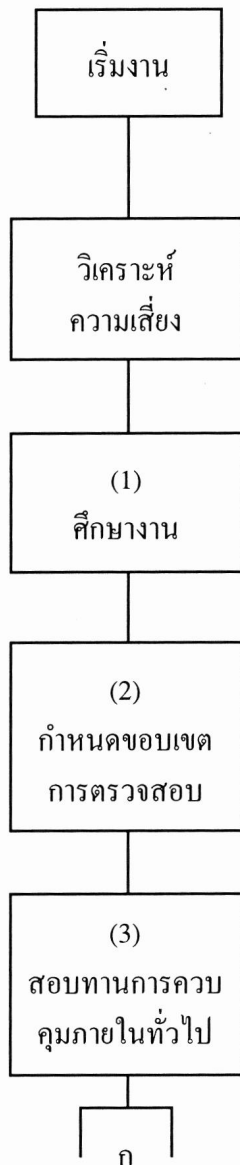
3.2.5 การเก็บรักษาข้อมูลและการนำข้อมูลไปใช้งาน เป็นการตรวจสอบ

- การบันทึกข้อมูลใหม่ลงในแฟ้มข้อมูล (Master file updating)
- การตัดยอดรายการและหรือแฟ้มข้อมูล (Transaction/master file cutoff) ตามวันหรือเวลาที่กำหนดไว้ ในระบบงานเพื่อให้รายการข้อมูลที่ประมวลผลสอดคล้องกับการจัดทำงบการเงิน
- การมอบอำนาจปฏิบัติงานและการรักษาความปลอดภัยเกี่ยวกับแฟ้มข้อมูล (Data security and privacy)
- การแก้ไขข้อผิดพลาดในการบำรุงรักษาแฟ้มข้อมูล และการใช้แฟ้มข้อมูล

3.2.6 ผลลัพธ์ที่ได้จากการประมวลผล เป็นการตรวจสอบ

- การกระทบยอดข้อมูล (Balancing and reconciliation)
- การจัดส่งข้อมูลที่ได้จากการประมวลผลให้ผู้ใช้อ้างอิง (output Distribution)
- การจัดทำทะเบียนคุมเอกสารสำคัญทางการเงิน (Accountable document control)
- การเก็บรักษาข้อมูลที่ได้จากการประมวลผล
- การแก้ไขข้อมูลหรือผลลัพธ์ที่ผิดพลาด

4. กระบวนการตรวจสอบ



(1) ศึกษางานก่อนตรวจสอบ (Preliminary phase of review)

วัตถุประสงค์

เพื่อทำความเข้าใจระบบบัญชีที่ใช้คอมพิวเตอร์ และส่วนที่ไม่ได้ใช้คอมพิวเตอร์ โดยศึกษา

- ทางเดินของรายการและรายงานที่มีความสำคัญ
- ขอบเขตการใช้คอมพิวเตอร์ของฝ่ายบริหารและงานบัญชีที่มีความสำคัญ
- โครงสร้างพื้นฐานของการควบคุมทางการบัญชีการควบคุมภายในด้านคอมพิวเตอร์ และการควบคุมผู้ใช้ข้อมูล

วิธีการ

โดยการสอบถาม สังเกตการณ์ ศึกษาจากเอกสารที่พอจะหาได้ ติดตามความเคลื่อนไหวของรายการ ใช้แบบสอบถามการควบคุมภายใน และ Check list

(2) กำหนดขอบเขตการตรวจสอบ (Determine scope of audit)

วัตถุประสงค์

- เพื่อประเมินขอบเขตการควบคุมภายในด้านคอมพิวเตอร์และด้านอื่น ๆ
- เพื่อกำหนดขอบเขตการตรวจสอบ

วิธีการ

ขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบ

(3) สอบทานการควบคุมภายในทั่วไป (Review of general controls)

วัตถุประสงค์

- เพื่อศึกษาการควบคุมภายในทั่วไปและลักษณะการทำงานของ การควบคุมภายในทั่วไป
- เพื่อศึกษาความรัดกุมและจุดอ่อนของการควบคุมภายในทั่วไป และผลกระทบที่มีต่อการควบคุมเฉพาะงาน
- พิจารณาถึงความจำเป็นในการทดสอบการควบคุมภายในทั่วไปบางประเภท

วิธีการ

ศึกษาระเบียบ ข้อบังคับ และมาตรฐานการปฏิบัติงานของหน่วยงานคอมพิวเตอร์ สอบถาม และสังเกตการณ์



(4) สอบทานการควบคุมภายในเฉพาะงาน (Review of application controls)

วัตถุประสงค์

- เพื่อศึกษาการควบคุมภายในเฉพาะงาน และลักษณะการทำงานของ การควบคุมภายในเฉพาะงาน
- พิจารณาถึงความจำเป็นในการทดสอบการควบคุมภายในเฉพาะงานบางประเภท

วิธีการ

ศึกษาเอกสารระบบงานและโปรแกรมระเบียบ ข้อบังคับ หรือคู่มือปฏิบัติงานของหน่วยงานผู้ใช้ข้อมูล สอบถาม และสังเกตการณ์

(5) ประเมินความรัดกุมของการควบคุมภายในที่สอบทานแล้ว

(Assessment of controls)

วัตถุประสงค์

- เพื่อพิจารณาว่าข้อผิดพลาดหรือสิ่งผิดปกติที่จะเกิดขึ้นในแต่ละระบบงานเป็นข้อผิดพลาดชนิดใด
- วิธีการควบคุมที่ใช้สามารถและค้นหาข้อผิดพลาดได้เพียงพอ
- เพื่อประเมินประสิทธิภาพการควบคุมภายในด้านคอมพิวเตอร์และด้านอื่น ๆ ที่เกี่ยวข้อง

วิธีการ

ขึ้นอยู่กับ การตัดสินใจของผู้ตรวจสอบ

(6) ทดสอบการปฏิบัติงานตามระเบียบข้อบังคับหรือข้อกำหนดในการประมวลผลข้อมูล

(Test of Compliance)

วัตถุประสงค์

- เพื่อพิจารณาว่ามีการปฏิบัติตามระเบียบ ข้อบังคับ หรือข้อกำหนดในการประมวลผลข้อมูลเพียงพอ
- เพื่อหาเหตุผลสนับสนุนก่อนที่จะแน่ใจว่าการควบคุมภายในที่ต้องการทดสอบทำหน้าที่ได้อย่างเหมาะสม
- เพื่อพิจารณาความเหมาะสมของขอบเขตการควบคุมภายในเอกสารหลักฐาน ผู้รับผิดชอบ กำหนดเวลา และวิธีการที่ใช้เพื่อประโยชน์ในการควบคุมภายใน

วิธีการ

ตรวจสอบบันทึกการปฏิบัติงาน ทดสอบวิธีการควบคุม สอบถาม และสังเกตการณ์



(7) ประเมินสรุปผลการควบคุมภายใน (Evaluation of controls)

วัตถุประสงค์

- เพื่อพิจารณาว่าข้อผิดพลาดหรือสิ่งผิดปกติที่อาจเกิดขึ้นในแต่ละระบบงาน เป็นข้อผิดพลาดชนิดใด
- วิธีการควบคุมที่ใช้ สามารถป้องกันและค้นหาข้อผิดพลาดได้เพียงใด
- พิจารณาว่าได้จัดให้มีการควบคุมภายในที่สำคัญไว้หรือไม่ และมีการปฏิบัติตามระเบียบการควบคุมภายในดังกล่าวเป็นที่น่าสนใจเพียงใด
- ประเมินจุดอ่อนและผลกระทบที่มีต่อลักษณะ เวลา และขอบเขตการตรวจสอบ

วิธีการ

ขึ้นอยู่กับ การตัดสินใจของผู้ตรวจสอบ



5. หลักการสอบทานการควบคุมภายในที่สำคัญ

แม้ว่าในการนำคอมพิวเตอร์มาใช้ จะไม่เปลี่ยนแปลงวัตถุประสงค์ในการตรวจสอบแต่ลักษณะการประเมินการควบคุมภายในและวิธีการตรวจสอบจะเปลี่ยนแปลงไป

ในระบบที่ทำด้วยมือนั้น มักเน้นการทำ Substantive test ซึ่งเป็นการทดสอบรายการทางการเงิน เพราะการใช้คนในการประมวลผลข้อมูล ย่อมมีโอกาสเกิดความผิดพลาดได้ง่าย ซึ่งก่อให้เกิดความเสี่ยงสูง ดังนั้น การใช้ Substantive test จะช่วยลดความเสี่ยงได้มาก

แต่ในระบบคอมพิวเตอร์ที่มีการพัฒนาก้าวหน้าไปไกลนั้น สภาพแวดล้อมต่าง ๆ ทางธุรกิจได้รับการออกแบบให้ควบคุมด้วยระบบคอมพิวเตอร์เป็นอย่างดี ดังนั้นจึงควรเปลี่ยนจากการเน้นตรวจ Substantive test ไปเป็นการประเมินการควบคุมภายในแทน ด้วยเหตุผล 3 ประการ คือ

- 1) ความสม่ำเสมอของการประมวลผลด้วยคอมพิวเตอร์ช่วยให้มั่นใจได้ว่าการประมวลผลจะมีความสม่ำเสมอด้วย
- 2) การตรวจสอบที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ ในลักษณะของการทำ substantive test นั้นทำได้ยากขึ้น เพราะหลักฐานการตรวจสอบต่าง ๆ ตลอดจน audit trail ได้เปลี่ยนแปลงไปมาก และหลาย ๆ กรณีก็ไม่อาจกระทำการตรวจสอบแบบ manual ได้ด้วยวิธีการปกติ
- 3) ผู้ตรวจสอบถูกกำหนดให้มีความรับผิดชอบมากขึ้นในการตรวจสอบความเพียงพอของการควบคุมภายใน

ดังนั้น จะเห็นว่าผู้ตรวจสอบจำเป็นต้องฝึกฝนทักษะของตน ในการประเมินการควบคุมภายในของธุรกิจที่มีการประมวลผลด้วยคอมพิวเตอร์

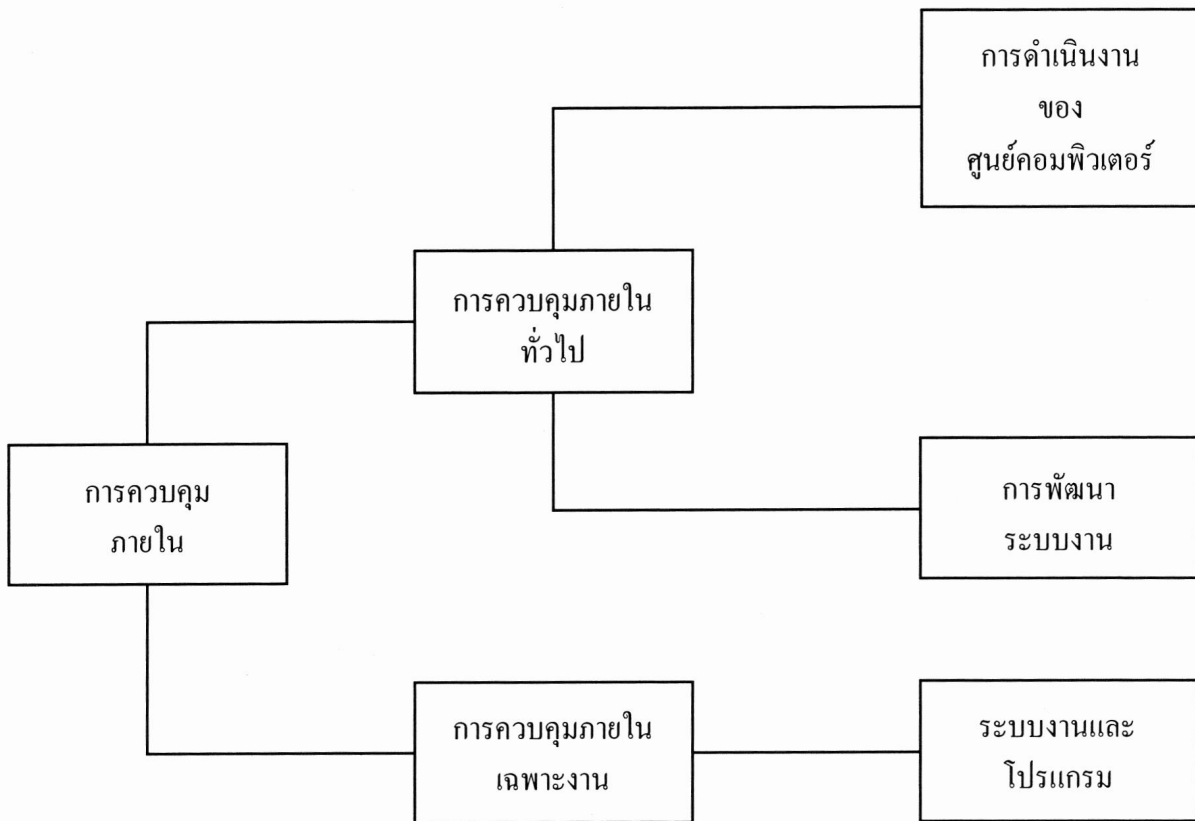
ก่อนที่จะมีการประเมินประสิทธิภาพการควบคุมภายใน ควรมีการกำหนดเป้าหมายเฉพาะในการตรวจสอบเสียก่อน เพราะจะช่วยให้ทำการตรวจสอบได้โดยมีประสิทธิภาพมากขึ้น และสามารถใช้เป็นเกณฑ์ที่ดีในการประเมินผลการตรวจสอบได้อีกด้วย

ผู้ตรวจสอบจำเป็นต้องมีทักษะใหม่ ๆ ที่จะช่วยในการตรวจสอบธุรกิจที่มีการนำเอาคอมพิวเตอร์เข้ามาใช้อย่างมีประสิทธิภาพ ทักษะทาง EDP ของผู้ตรวจสอบแต่ละคนอาจแตกต่างกันออกไป แต่สำหรับทั้งทีมงานแล้วต้องมีทักษะทาง EDP ที่เหมาะสมและเพียงพอแก่การปฏิบัติหน้าที่ นอกจากนี้ผู้ที่ควบคุมหรือสอบทาน งานตรวจสอบต้องมีคุณสมบัติลึกไปทางด้านเทคนิคเพียงพอแก่การสอบทานงานของผู้ตรวจสอบระบบคอมพิวเตอร์ได้

ในที่สุดแล้ว ผู้ตรวจสอบจะไม่สามารถทำงานเหล่านี้ทั้งหมดได้ตามลำพัง จากความก้าวหน้าอันรวดเร็ว จำเป็นต้องให้ผู้บริหารและผู้ใช้ ได้รับการฝึกอบรมทางด้าน EDP และผู้บริหาร ผู้ใช้ และบุคลากรฝ่าย EDP เอง ควรได้รับการฝึกอบรมเกี่ยวกับมาตรฐานระบบงานและการควบคุมด้วย

การควบคุมภายใน

การควบคุมภายในด้านคอมพิวเตอร์แบ่งเป็น 2 ลักษณะ คือ การควบคุมภายในทั่วไป (General controls) และการควบคุมภายในเฉพาะงาน (Application controls) ซึ่งมีความสัมพันธ์กับองค์ประกอบที่สำคัญในการประมวลผลข้อมูล คือการดำเนินงานของศูนย์คอมพิวเตอร์ (Computer center operations) การพัฒนาระบบงาน (Application system development) และระบบงานและโปรแกรมที่ใช้เฉพาะงาน (Application systems and programs) ดังรูป



5.1 การควบคุมภายในทั่วไป

การควบคุมภายในทั่วไป เป็นการควบคุมที่อาศัยนโยบาย และระเบียบปฏิบัติงาน (procedures) เป็นหลักในการควบคุมกิจกรรม (Activity) ของหน่วยงานคอมพิวเตอร์ ซึ่งประกอบด้วย

(1) การควบคุมการดำเนินงานของศูนย์คอมพิวเตอร์ (Computer center controls)

การควบคุมศูนย์คอมพิวเตอร์ เป็นการควบคุมเกี่ยวกับเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์และพนักงานด้านปฏิบัติการของศูนย์คอมพิวเตอร์ มีขอบเขตดังนี้

(1.1) การจัดการปฏิบัติงาน การควบคุมข้อมูลนำเข้า และการควบคุมข้อมูลที่ได้จากการประมวลผล (Input/output scheduling and control) ได้แก่ การจัดการกำหนดเวลาปฏิบัติงาน การควบคุมการปฏิบัติงานข้อมูลที่นำเข้าประมวลผลและการควบคุมการใช้ข้อมูลเพื่อให้การจัดทำข้อมูลขั้นตอนต่อเนื่องแล้วเสร็จทันเวลา มีความถูกต้องครบถ้วนทุกรายการ และป้องกันข้อมูลที่เป็นความลับรั่วไหลไปสู่ภายนอก

(1.2) การควบคุมการจัดเก็บแฟ้มข้อมูลและโปรแกรม (Media library controls) เช่น เทป และจานแม่เหล็ก เป็นต้น ให้ปลอดภัยและเพียงพอในการประมวลผล

(1.3) การรายงานเหตุขัดข้องและการซ่อมบำรุงเพื่อป้องกันความเสียหาย (Malfunction reporting and preventive maintenance) จะช่วยให้ทราบถึงสภาพของเครื่องจักรและโปรแกรมจัดระบบการทำงานของเครื่องคอมพิวเตอร์ (Operating system software) และการดำเนินการให้เครื่องจักรและโปรแกรมหาดังกล่าวอยู่

ในสภาพสมบูรณ์ สามารถตรวจสอบข้อผิดพลาดหรือบกพร่องในระบบด้วยตนเอง ซึ่งอาจตรวจไม่พบหากมีส่วนประกอบชำรุดเสียหายซ่อนอยู่ ไม่ปรากฏอาการที่เห็นได้ชัดเจน

(1.4) การควบคุมสภาพแวดล้อม และการรักษาความปลอดภัยของศูนย์คอมพิวเตอร์ (Environmental controls and physical security) ได้แก่ การควบคุมการใช้ทรัพย์สิน การป้องกันทรัพย์สินเสียหาย และการจัดเตรียมระบบสำรอง (Backup) ไว้ให้ทดแทน

(1.5) การแบ่งแยกหน้าที่ (Separation of Duties) ได้แก่ การแบ่งแยกหน้าที่ในหน่วยงานคอมพิวเตอร์ และหน่วยงานผู้ใช้ข้อมูลเพื่อให้การปฏิบัติงานไม่ซ้ำซ้อนกัน และป้องกันความเสียหายที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ และแฟ้มข้อมูลเนื่องจากการปฏิบัติไม่ชอบ

(1.6) การกำกับ (Supervision) ได้แก่ การควบคุมดูแลให้มีการปฏิบัติตามระเบียบหรือหน้าที่อย่างเคร่งครัด หากมีการปฏิบัติที่ผิดแตกต่างจากระบบแบบแผนที่เคยถือปฏิบัติ จะต้องมีเอกสารหลักฐานรายงานให้ทราบทุกครั้ง

(1.7) การวางแผนทรัพยากร (Resource planning) เป็นการวางแผนและประเมินสถานะของทรัพยากรในหน่วยงานคอมพิวเตอร์ และหน่วยงานผู้ใช้ข้อมูลทั้งปัจจุบันและอนาคต เพื่อให้มีทรัพยากรเพียงพอต่อการดำเนินงาน ทรัพยากรเหล่านี้ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์โปรแกรม และบุคลากร

(1.8) การคำนวณค่าบริการคอมพิวเตอร์จากผู้ใช้ข้อมูล (User billing chargeout procedures) เป็นการคำนวณเพื่อประโยชน์ในการควบคุม ทางการบริหาร (Administration controls) นอกจากนี้กรณีกิจการไม่มีคอมพิวเตอร์เป็นของตนเอง ควรคำนึงถึงการจัดทำสัญญาใช้บริการและระเบียบปฏิบัติที่ใช้ควบคุมการชำระค่าบริการด้วย

(1.9) การเตรียมวิธีการปรับปรุงแก้ไขระบบคอมพิวเตอร์ที่ได้รับความเสียหายให้ปฏิบัติงานได้ตามปกติ (Disaster recovery procedures) วิธีการที่นำมาใช้ต้องสามารถแก้ไขสถานการณ์ที่เลวร้ายได้รวดเร็ว และป้องกันธุรกิจหยุดชะงักได้แน่นอน

(2) การควบคุมการพัฒนาระบบงาน

(Application system development controls)

การควบคุมภายในเฉพาะงาน (Application controls) ที่สร้างไว้ภายในระบบงานคอมพิวเตอร์จะรัดกุมและเหมาะสมเพียงใด ขึ้นอยู่กับความรู้ความชำนาญหรือประสบการณ์ของการออกแบบระบบงานเป็นสำคัญ ในปัจจุบันการถ่ายทอดวิทยาการเกี่ยวกับการควบคุมเฉพาะงานค่อนข้างเชื่องช้า มีค่าใช้จ่ายสูง ต้องอาศัยความร่วมมือจากผู้ที่เกี่ยวข้องหลายฝ่ายและไม่สามารถนำวิธีการควบคุมภายในที่ใช้กับระบบงานใดระบบงานหนึ่งไปใช้กับระบบงานอื่นได้ จึงจำเป็นต้องอาศัยการควบคุมการพัฒนาระบบงานช่วยแก้ปัญหาที่กล่าวข้างต้นเพื่อ

- ควบคุมค่าใช้จ่ายและระยะเวลาที่ใช้ในการพัฒนาระบบงาน
- ช่วยให้แน่ใจว่าการควบคุมภายในเฉพาะงานที่สร้างไว้ในระบบ มีความรัดกุมและเหมาะสม
- ช่วยให้แน่ใจว่ามีการทดสอบการควบคุมภายในเฉพาะงาน ด้วยวิธีการที่เหมาะสมก่อนนำไปใช้ข้างหน้า

การควบคุมการพัฒนาระบบงานมีขอบเขตดังนี้

(2.1) System Development Life Cycle (SDLC) ได้แก่การแบ่งงานพัฒนาระบบออกเป็นขั้นตอนต่าง ๆ หลายขั้นตอน เพื่อความสะดวกในการกำหนดจุดที่จะจัดการควบคุมซึ่งนอกจากจะช่วยให้ฝ่ายบริหารมีเครื่องมือในการควบคุมค่าใช้จ่ายและระยะเวลาในการพัฒนาระบบงานแล้วยังช่วยทำให้เกิดช่องทางการติดต่อประสานงานกับผู้ใช้ข้อมูล ผู้ตรวจสอบ พนักงานวางแผนจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์มาใช้งาน พนักงานที่รับผิดชอบในการพัฒนาระบบและพนักงานชั้นบริหาร

(2.2) การบริหารโครงการ (Project management) ได้แก่ การใช้เทคนิคในการวัดความก้าวหน้าของโครงการในแต่ละขั้นตอน เป็นหลักในการควบคุมเพื่อ

- ให้ทราบว่าผู้ใช้ข้อมูลให้ความเห็นชอบผลงานที่อยู่ในระหว่างการพัฒนาถึงขั้นตอนใดแล้ว
- เปรียบเทียบค่าใช้จ่ายที่เกิดขึ้นจริงกับค่าใช้จ่ายตามงบประมาณ และเปรียบเทียบระยะเวลาที่ปฏิบัติงานจริง กับระยะเวลาที่กำหนดไว้ล่วงหน้า
- เสนอรายงานสถานะของโครงการให้ผู้บริหารระดับสูงได้ทราบทุกระยะ

(2.3) การกำหนดมาตรฐานหรือระเบียบปฏิบัติในการเขียนโปรแกรม เพื่อเป็นแนวทางปฏิบัติงานของผู้เขียนโปรแกรม ปัจจุบันนิยมใช้เทคนิคการเขียนโปรแกรมโครงสร้าง (Structured programming) ช่วยลดความซ้ำซ้อนของงานเขียนโปรแกรม และเพื่อให้ผู้อื่นที่จะมาใช้โปรแกรมในภายหลังหรือผู้ที่มาปฏิบัติงานแทนผู้เขียนโปรแกรม ตั้งแต่เริ่มแรกสามารถทำความเข้าใจ และทำงานต่อไปได้

(2.4) การทดสอบเพื่อตรวจรับระบบงาน (Acceptance testing) คือการทดสอบระบบงานและโปรแกรมก่อนนำไปใช้งานจริง เพื่อให้แน่ใจว่าระบบงานและโปรแกรมสามารถทำงานได้ตามความประสงค์ของผู้ใช้ข้อมูลและสอดคล้องกับระเบียบปฏิบัติในการประมวลข้อมูลของศูนย์คอมพิวเตอร์

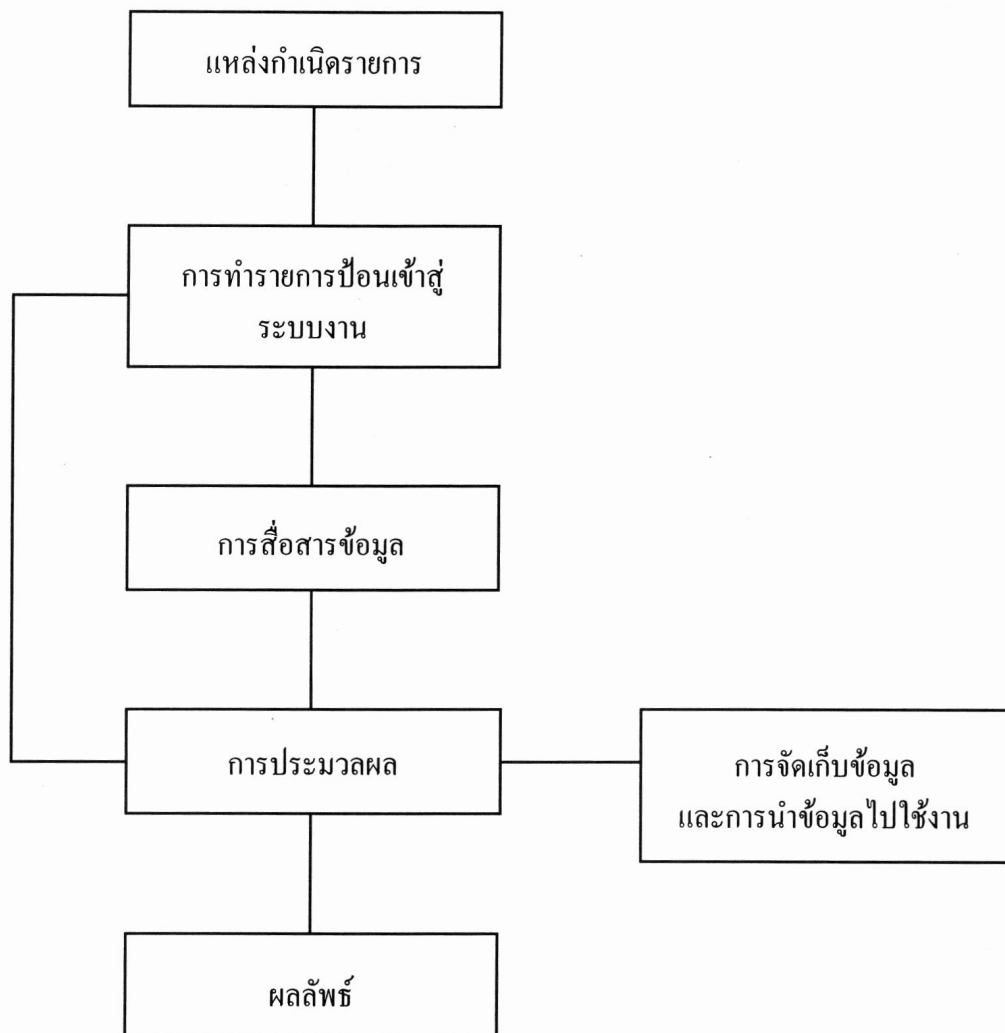
(2.5) การควบคุมการแก้ไขโปรแกรม (Program change control) ได้แก่การกำหนดระเบียบปฏิบัติในการปรับปรุงแก้ไข Application program และ Operating systems โดยจัดให้มีเอกสารหลักฐาน และการขอความเห็นชอบในการแก้ไขโปรแกรม เพื่อป้องกันการปฏิบัติไม่ชอบ

(2.6) การจัดทำเอกสารสนับสนุนการปฏิบัติงาน (Documentation) ซึ่งได้แก่ เอกสารที่อธิบายลักษณะการทำงานของระบบงานโดยละเอียด เพื่อให้ผู้อื่นที่ไม่ได้มีส่วนเกี่ยวข้องกับการพัฒนาระบบงาน เช่น ผู้ใช้ข้อมูล ผู้ตรวจสอบและพนักงานปฏิบัติการประมวลผล เป็นต้น สามารถทำความเข้าใจและประเมินผลได้

(2.7) การบริหารงานฐานข้อมูล (Data base administration) กรณีที่มีการนำระบบฐานข้อมูลมาใช้เพื่อให้ระบบงานต่าง ๆ สามารถใช้ข้อมูลร่วมกันและช่วยลดความซ้ำซ้อนในการจัดเก็บข้อมูลจะมีผลกระทบต่อการจัดองค์กรของศูนย์คอมพิวเตอร์ และการพัฒนาระบบงาน ซึ่งจำเป็นต้องปรับปรุงการควบคุมให้เหมาะสมด้วย

5.2 การควบคุมภายในเฉพาะงาน

การควบคุมภายในเฉพาะงาน คือการควบคุมรายการข้อมูล (Transaction data) ในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของข้อมูล (Flow of data) เป็นแนวทางในการกำหนดขอบเขตการควบคุม ซึ่งส่วนใหญ่มี 6 ขั้นตอน ดังนี้



(1) การควบคุมแหล่งกำเนิดรายการ (Transaction Origination) ได้แก่ การควบคุมเกี่ยวกับงานจัดทำข้อมูลก่อนป้อนเข้าสู่ระบบคอมพิวเตอร์ ซึ่งส่วนใหญ่เป็นงานด้าน Manual ละอาจมีบุคคลหลายฝ่ายเข้ามาเกี่ยวข้อง เริ่มตั้งแต่จุดเริ่มต้นของแหล่งกำเนิดรายการการจัดทำเอกสารขั้นต้นประกอบรายการ การขอความเห็นชอบในการจัดทำรายการ การเตรียมข้อมูลนำเข้า การป้องกันข้อผิดพลาด การค้นหาข้อผิดพลาด และการแก้ไขข้อผิดพลาด

(2) การควบคุมการทำรายการป้อนเข้าสู่ระบบงาน (Data Processing transaction entry) ได้แก่ การควบคุมการทำรายการป้อนเข้าสู่ระบบงาน ซึ่งอาจทำได้ 2 วิธี คือแบบ Remote terminal data entry และแบบ Batch data entry โดย ข้อมูลที่ป้อนเข้าสู่ระบบจะต้องถูกหลักเกณฑ์ในการทำรายการ นอกจากนี้ยังรวมถึงเรื่อง ที่เกี่ยวกับการกระหายอดข้อมูลนำเข้าเพื่อพิสูจน์ความถูกต้อง การชี้แนะให้เห็นข้อผิดพลาดการทำรายการแก้ไขข้อ ผิดพลาด และการนำข้อมูลที่มีการแก้ไขข้อผิดพลาดป้อนเข้าสู่ระบบใหม่อีกครั้ง

(3) การควบคุมการสื่อสารข้อมูล (Data communications) เป็นการควบคุมข้อมูลและข่าวสารที่ ผ่านระบบสื่อสารให้มีความถูกต้องและครบถ้วน ซึ่งจะต้องคำนึงถึง Hardware และ Software ที่ใช้ในการสื่อสาร ข้อมูลการมอบอำนาจปฏิบัติงาน การป้องกันข้อมูลเสียหาย การรักษาความปลอดภัยในระบบสื่อสาร การชี้แนะให้เห็น ข้อผิดพลาด และการรายงาน

(4) การควบคุมการประมวลผลด้วยคอมพิวเตอร์ (Computer Proecssing) ได้แก่ การควบคุม การประมวลผลข้อมูลให้มีความแม่นยำ ถูกต้อง และครบถ้วนเป็นไปตามหลักเกณฑ์การใช้แฟ้มข้อมูล การชี้แนะให้เห็น ข้อผิดพลาด และการรายงาน

(5) การควบคุมการจัดเก็บข้อมูลไว้ในระบบ และการนำข้อมูลที่เก็บไว้ในระบบไปใช้งาน (Data storage and retrieval) เป็นการควบคุมที่เกี่ยวกับแฟ้มข้อมูลการตัดตอนข้อมูลเพื่อจัดเก็บหรือเลิกเก็บไว้ในแฟ้มข้อมูล การกำหนดสิทธิการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การเตรียมแฟ้มข้อมูลชุดสำรองไว้ใช้ ทดแทนการแก้ไขสถานการณ์ที่เลวร้ายให้กลับคืนสู่สภาพปกติ และการกำหนดอายุการจัดเก็บแฟ้มข้อมูล

(6) การควบคุมผลลัพธ์ (Output processing) ได้แก่ การกระหายอดข้อมูลนำเข้าและผลลัพธ์ เพื่อพิสูจน์ความถูกต้องด้วยระบบ Manual ซึ่งเป็นหน้าที่โดยตรงของหน่วยงานควบคุมคุณภาพข้อมูล (Input/output control section) และหน่วยงานผู้ใช้ข้อมูล การจัดส่งข้อมูลจากศูนย์คอมพิวเตอร์ให้หน่วยงานอื่น ความปลอดภัยใน การจัดเก็บเอกสารสำคัญในศูนย์คอมพิวเตอร์และหน่วยงานผู้ใช้ข้อมูลและการกำหนดอายุการจัดเก็บข้อมูลที่ได้จากการ ประมวลผล



5.3 โครงสร้างการควบคุมภายใน

โครงสร้างการควบคุมภายในด้านคอมพิวเตอร์โดยย่อมีดังนี้

COMPUTER SERVICE CENTER CONTROL STRUCTURE

Control Area	Control
Input/output scheduling and control	Input/output control group Job handling procedures Scheduling procedures Processing schedules Cutoff dates Job submission/authorization Input/output control group Daily work schedules
Media library controls	Access controls File release Separate library area Physical security Media restriction issuance Media inventory control procedures Media restriction quantity Media use records Handling equipment Security vaults Temperature and Humidity control off-site storage Duplicate file storage Redundancy and backup procedures

Malfunction reporting
and preventive
maintenance

Procedures reporting
Problem documentation
System utilization report
System utilization reports review
Vendor failures logging
Trouble reporting responsibility

Environmental controls
and physical security

Physical security
Access controls
Backup for power, cooling, etc.
Software backup
Hardware backup

Separation of duties

Separation of duties within data processing
Separation of data processing from other organizational units
Computer programs to enforce separation between systems
Automated controls to separate on-line users

Resources planning

Plan for facilities, equipment, software and personnel
Variance between actual and planned goals

User billing/charge-out
procedures

Service contracts between the user and data processing
Procedures to arbitrate disputes
Chargeable versus free services
Billing procedures tied to the computerized
job accounting system
Billing algorithm, periodic user billing statements,
rerun cost allocation procedure

Disaster recovery

Disaster plan
Disaster scenarios to update the disaster plan
Top management's commitment to the disaster plan
Maintenance and updating of the disaster plan
User responsibility for the disaster plan
Testing of the disaster plan
User training in use of the disaster plan

APPLICATION SYSTEM DEVELOPMENT CONTROL STRUCTURE

Control Area	Control
System development life cycle	Review user requirements Review project organization Review hardware requirements Review internal controls Require user or internal auditor sign-off Review detailed design documents Review file requirements Review costs and schedules Review test plan Review user and operational documentation Review test results Require user and internal audit sign-off Review conversion plan Review adequacy of documentation Identify user problem areas Identify system development problems
Project management	PERT control technique
Structured programming	Audit trail
Acceptance testing	Comparison of base case data to system produced data manual review of output reports
Program change control	Require formal written request Review all changes Use of change control committee Restrict number and type of persons who make changes Require operator and programmer to make changes Modify SMF to obtain reports of all changes to load libraries

Require report of quick fixes

Limit number of times changes are made per time period

Use program packages to control access to source libraries

Documentation

Provide flow of all application system data flow

Specify how the programs implement controls

Specify how programs are to be operated, backed up,
and recovered

Maintain up-to-date changes to accepted documents

Specify allowable user commands and functions

Date base administration

Develop standards

Establish and monitor standards

Document and provide procedures to control operations

Measure effectiveness of performance and integrity controls

Develop security/control education programs



TRANSACTION ORIGINATION CONTROL STRUCTURE

control Area	Control Type	Control
Source document origination	Written procedures	control documentation User procedures and manuals
	Source document design	Special purpose forms Source document numbers Transaction identification Cross reference Sequence log
	Source document storage	Restricted access Accountable source document storage Intermediate storage and transportation
	Source document handling	Dual custody
Authorization	Source document preparation	Separation of duties Signatures
	Written procedures	Written authorization
	Approval of source documents	Evidence of approval Transaction conflicts matrix
Data processing input preparation	Transaction identification	Transaction numbering User identification Schedule desk
	User review of input	Manual review
	Batching	Batch serial number Limit the number of transactions in a batch Batch and balance source data at point of origin

	Logging	Logs of source document transmittal between organizations
	Transmittal	Transmittal document Mail and message carrier Physically secure input
Source document retention	Source document retention characteristics	Source turn around Retention dates on source documents Source document storage index
	Filing of source documents	File of source documents Batch storage Source documents maintained at origin
	Retention storage	Filing in user areas Limited access to retention facilities Removal from retention
Source document error handling	Error procedures	Written error handling procedures Source document correction procedures Responsibility for error correction
	Error detection	Error logging Visual review of source documents
	Error correction processing	Error notification Identification of error correction
	Corrected date resubmission	verification of reentered data Monitoring of error corrections

TRANSACTION ENTRY CONTROL STRUCTURE

control Area	Control Type	Control
Transaction (batch) data entry	Written procedures	Control documentation User procedures
	Physical hardware	Location of data conversion operation Simultaneous recording
Terminal data entry	Terminal software features	Security of data entry terminal
		Preformatting
		Interactive display
		Computer-aided instruction
		User application system access
		Terminal authority levels
		Data access matrix
		Master commands
		Terminal sign-on procedures
		Review of terminal assignments
	Hardware control features	Terminal features
		Intelligent terminals
Transaction data validation	Transcription verification techniques Data content validation techniques	Key verification
		Preprogrammed keying formats
		Editing and validating routines
		Transaction data cutoff
Batch proof and balancing		Passwords
	Data input controls	Processing schedules
		Turnaround documents
		Cancellation of source documents
		Logging
		Manual check of control figures
	Proof and balancing methods	Batch control
		Batch header records

Transaction entry
error handling

Error detection

Error correction

Corrected data
resubmission

Error display

Unauthorized access attempts

Error listings

Corrective action

Warning messages

Error message

Corrected data editing

Control totals and rejects



DATA COMMUNICATION CONTROL STRUCTURE

control Area	Control Type	Control
Message input	Hardware related Software and procedure related	Electronic identification code
		Secure phone equipment room
		Network configuration polling table
		Sending message identification
		Security table
		Communication system control log
Message transmission	Hardware related Software and procedure related	Communication line routing
		Line conditioning
		Automatic store and forward
		Automatic dial backup
		Modem loop-back switch
		Forward error correction
		Validity check
		Echo checking
		Message intercept function
		Packet switching networks
		Local loop security
		Encryption techniques
		Multipurpose modems
		Backup modems
		Backup lines
		Transmission batch controls

Message recaption
and accountion

Hardware related

Software and
procedure related

Detection with retransmission

Backup electrical power

Validation

Line usage records

Message sequence number

Input/output message log

Dial-up modems

Message backup log

Error recording

Error correction procedures



COMPUTER PROCESSING CONTROL STRUCTURE

control Area	Control Type	Control
Computer process integrity	Transaction identification	Transaction codes
		Monitoring of computer generated transactions
	Computation and logic	Control totals
		Default option
		Anticipation control
		Dual fields
		Arithmetic accuracy
		Exception reporting
		File control totals
	File maintenance	File completion check
		Balancing the computer file
		Dummy records
Computer processing error handing	Computer operations personnel	Operator instructions
		Computer program run books
		Computer console
		Display messages
	Error reporting	Error reporting
		Batch control header balancing
	Error correction	production report of rejected conditions
		Automated error suspense file
		Discrepancy report
	Corrected data resubmission	Error serial numbers
		Destructive update
		Error suspense reentry

DATA STORAGE AND RETRIEVAL CONTROL STRUCTURE

control Area	Control Type	Control
File handling	Library	Operation procedures On-line library Source program statement library
	File access	Conflict prevention feature Group files File classification Data base control table Program linkage control table Header/trailer labels System inquiries System logging Manual authorization of security table Program modification
	File maintenance	Folio number Before and after looks Masterfile changes Dormant files Excessive activity Scanning of critical files
	Backup	Activity tape Separate computer Copy masterfiles Backup procedures Disaster plan Recovery procedures
File error handling	Error reporting	Operator intervention Comparison programs
	Error correction	Restart procedures Backup file usage
	Correction reentry	Job stream log

OUTPUT PROCESSING CONTROL STRUCTURE

control Area	Control Type	Control
Data processing balancing and Reconciliation	Data processing control group	Reconciliation Transaction log Computer console log Systems output logs Record of output reports Monitoring process flow Job control card review Graphical charts
Output distribution	Output handling	Handling procedures for computer output Output report distribution Report copies
User balancing and reconciliation	Monitoring procedures Testing procedures	User department changes in masterfiles Report heading Transaction tracing list Internally generated transactions Control totals Statistical sampling of final report List of all transactions
Records retention	User retention and disposal methods	Waste disposal procedures Deletion of unused reports
Accountable documents	Accountable document handling	Negotiable documents storage Printing of additional sequence number on preprinted forms
Output error handling	Error reporting	Independent history file of errors

	Aging open items
	Error logging by control groups
	Output activity review
Error correction	Error correction processing
	Identification of error correction
	Correction procedures
	Responsibility for error correction
correction reentry	Error logging
	Verification of reentered data
	Monitoring of error conditions



6. การจัดทำรายงานการตรวจสอบ

การจัดทำรายงานหลังจากการตรวจสอบนั้น เป็นสิ่งที่จำเป็นเพราะ

1. เพื่อบันทึกสิ่งที่ตรวจพบและข้อสรุป ตลอดจนข้อเสนอแนะของผู้ตรวจสอบ
2. เพื่อใช้เป็นเอกสารขั้นต้นสำหรับการทำให้องค์การนั้นสมบูรณ์ขึ้น
3. เพื่อใช้เป็นเอกสารอ้างอิงในภายภาคหน้า

ดังนั้น การเสนอรายงานเป็นเทคนิคที่สำคัญที่สุดอันหนึ่งให้ผู้ตรวจสอบต้องเอาใจใส่เป็นพิเศษ เพราะเป็นสื่อที่แสดงถึงการทำงานของผู้ตรวจสอบทั้งหมด ผู้บริหารจะยกย่องหรือไม่เห็นความสำคัญของผู้ตรวจสอบก็เนื่องจากรายงานที่เสนอไป ผู้ตรวจสอบจะต้องเสนอรายงานที่ถูกต้อง ให้ข้อมูลที่แท้จริงและประเมินผลจากข้อเท็จจริง ให้ข้อเสนอแนะที่มีเหตุผล การเสนอแนะนั้นจะต้องพิจารณาอย่างรอบคอบ ผู้ตรวจสอบจะต้องพิจารณาข้อเท็จจริง และให้เหตุผลได้สำหรับข้อเสนอแนะนั้น ๆ

การทำรายงานที่ดีจำเป็นต้องเขียนอย่างมีหลักเกณฑ์ สมเหตุสมผลและเป็นขั้นตอน ใช้คำที่ถูกต้อง รายงานต้องรัดกุม ชัดเจน และสมบูรณ์ รายงานที่ชัดเจนจะทำให้ผู้บริหารอ่านเข้าใจได้ตั้งแต่การอ่านครั้งแรก รายงานที่ถูกต้องจะต้องประกอบด้วยข้อมูลที่ถูกต้อง รายงานที่สมบูรณ์จะต้องประกอบด้วยข้อมูลที่จำเป็น และอยู่ในประเด็นที่เกี่ยวข้องเท่านั้น

การจัดทำรายงานที่ดี ควรประกอบด้วย

1. ความถูกต้อง (Accuracy)
2. ความชัดเจน (Clarity)
3. ความกระชับรัดกุม (Conciseness)
4. ข้อเสนอแนะ (Comments)
5. ความทันกาล (Timeliness)

1. ความถูกต้อง (Accuracy)

รายงานการตรวจสอบมีความถูกต้อง ข้อความทุกประโยค ตัวเลขทุกตัวเอกสารอ้างอิงทุกชนิดจะต้องมาจากหลักฐานที่น่าเชื่อถือ และผู้ตรวจสอบได้ทำการประเมินข้อมูลเหล่านั้นแล้ว ความถูกต้องที่กล่าวถึงในรายงานต้องรวมถึงการทราบถึง หรือสังเกตการณ์ จนกระทั่งทราบอย่างแน่ชัดว่าได้ข้อเท็จจริงแล้ว ถ้ารายงานเกี่ยวกับสิ่งใดแล้วย่อมหมายถึงว่าสิ่งนั้นผู้ตรวจสอบได้ทราบ และ/หรือได้ยอมรับแล้วเป็นสิ่งที่ตรงตามข้อเท็จจริง

2. ความชัดเจน (Clarity)

หมายถึง ความสามารถในการส่งข้อความหรือความต้องการของผู้ตรวจสอบหรือสิ่งที่ต้องการเสนอไปสู่ผู้อ่านรายงานให้เข้าใจเหมือนดังที่ตนตั้งใจ หากใช้ถ้อยคำที่คลุมเครืออาจจะทำให้ผู้อ่านรายงานเกิดความเข้าใจแตกต่างจากที่เป็น ซึ่งอาจจะนำไปสู่การปรับปรุงแก้ไขในแนวทางที่แตกต่างกันไปจากเป้าหมายที่ตั้งใจ

ในเบื้องต้น ผู้ตรวจสอบต้องทำความเข้าใจในเรื่องที่จะเสนอรายงานให้แจ่มแจ้งเสียก่อน หากไม่ทำความเข้าใจให้เกิดขึ้นแล้วก็คงยากที่จะเขียนรายงานได้อย่างชัดเจนผู้ตรวจสอบต้องแน่ใจว่าเรื่องที่จะเขียนในรายงานนั้นมีอยู่แล้วอย่างเพียงพอหรือไม่ ควรที่จะหาข้อมูลเพิ่มเติมอีกหรือไม่

ความต่อเนื่องหรือการจัดลำดับข้อความในรายงานเป็นการช่วยให้รายงานนั้นเกิดความเด่นชัด หรือชัดเจนยิ่งขึ้น การสร้างความชัดเจนอาจจำเป็นต้องมีตารางตัวเลขประกอบไปด้วยเพื่อให้เกิดความเข้าใจยิ่งขึ้น

3. ความกระชับ (Conciseness)

หมายถึง การตัดสิ่งที่ไม่จำเป็นหรือไร้สาระออกจากรายงานการตรวจสอบ แต่ไม่ได้หมายถึงการเขียนรายงานสั้น รายงานจะยาวหรือสั้นขึ้นอยู่กับสิ่งที่จะเสนอในรายงานนั้นมีมากน้อยเพียงใด ถึงแม้ว่าการตัดทอนจะมีมากน้อยเพียงใดก็ตาม ผู้ตรวจสอบยังคงต้องรักษาความต่อเนื่องของแนวความคิด เพื่อให้ผู้อ่านได้รับความคิดอย่างต่อเนื่อง

4. ข้อเสนอแนะ (Comments)

การวิจารณ์ข้อบกพร่องโดยไม่มีการให้ข้อเสนอแนะเป็นสิ่งที่ไม่ควรกระทำในตนเองเดียวกัน การวิจารณ์โดยปราศจากการเสนอแนะข้อยุติที่ข้อบด้วยเหตุผลก็ไม่ใช่การเหมาะสมเช่นกัน และจะทำให้รายงานไม่มีความหมาย เพื่อที่จะทำให้รายงานเป็นที่ยอมรับ การเสนอแนะเพื่อการปรับปรุงการปฏิบัติงาน แทนที่จะเป็นการตำหนิการปฏิบัติงาน จะทำให้รายงานมีคุณค่าขึ้น

5. ความทันกาล (Timeliness)

หมายถึงการเสนอรายงานต้องกระทำภายในเวลาที่เหมาะสมเพราะต้องมีการนำรายงานไปดำเนินการต่อการสั่งการของผู้บริหารต้องใช้ข้อมูลที่ดีและทันเวลาเพื่อให้เกิดการปรับปรุงแก้ไขได้ทันทั่วทั้ง

วิธีการจัดทำรายงานนั้น เป็นเรื่องของแต่ละบุคคล เป็นการยากที่จะวางรูปแบบและวิธีการจัดทำรายงานตายตัวที่จะใช้ได้ในทุกกรณี รายงานที่ดีจะต้องมาจากเนื้อหา รูปแบบที่เป็นมาตรฐาน และจะต้องมีเอกลักษณ์ภายในตัวของมันเอง ผู้ตรวจสอบจำเป็นต้องคำนึงถึงจุดประสงค์ใหญ่ของรายงานซึ่งได้แก่ เพื่อนำการเปลี่ยนแปลงในองค์กร เพื่อนำไปสู่การปฏิบัติและเพื่อใช้อ้างอิงได้ในภายหลัง รายงานที่เขียนขึ้นคร่าว ๆ ไม่ถูกต้อง หรือเขียนอย่างขอไปที จะไม่สามารถชักจูงให้ผู้อ่านยอมรับข้อสรุปนั้นได้ โดยเฉพาะอย่างยิ่งจะไม่นำไปสู่การนำข้อเสนอแนะไปใช้

ผู้ตรวจสอบจะต้องนำเสนอรายงานที่ตนคิดว่าถูกต้อง ถึงแม้ว่าข้อเสนอแนะนั้นจะส่งผลออกมาในรูปแบบที่ไม่ทำความเข้าใจให้แก่ผู้บริหารก็ตาม บางครั้งเป็นสิ่งที่หลีกเลี่ยงไม่ได้ ข้อเสนอแนะขั้นสุดท้ายนั้นไม่เป็นที่ยอมรับทั้งหมดของผู้บริหารแต่อย่างไรก็ตามเหตุการณ์นี้ไม่ควรจะเป็นเหตุผลให้ผู้ตรวจสอบถอนคำเสนอแนะที่ตนคิดว่าถูกต้อง

9

ความจำเป็นต้องมีหน่วยงาน
ตรวจสอบด้านคอมพิวเตอร์
กับความเสี่ยง

ความจำเป็นต้องมีหน่วยงานตรวจสอบ ด้านคอมพิวเตอร์กับความเสี่ยง

ดังที่ได้กล่าวแล้วว่า องค์กรที่ใช้คอมพิวเตอร์ในการประมวลข้อมูลทางการเงิน ได้นำมาซึ่งความเสี่ยงใหม่ๆ ที่จะก่อให้เกิดจุดอ่อนและความเสียหายต่อองค์กรได้ในหลาย ๆ ประการ (โปรดดูเรื่องความเสี่ยงและการวิเคราะห์ความเสี่ยงแทน) ผู้บริหารที่มีความรับผิดชอบจึงควรตระหนักถึงประเด็นนี้ เพราะความเสียหายที่อาจเกิดขึ้นนั้น บางกรณีไม้อาจจะยอมให้เกิดขึ้นได้ เช่น การหยุดชะงักการดำเนินงานอันมีผลจากระบบคอมพิวเตอร์ล้มเหลวตั้งแต่ Hardware Software หรืออาจเกิดจากอุบัติเหตุต่าง ๆ เช่น ไฟไหม้ น้ำท่วม ฯลฯ ไปจนถึง People ware ที่เกิดจากการจงใจทำลายระบบหรือทำลายระบบโดยไม่ได้ตั้งใจ ข้อสำคัญที่สุดถึงแม้จะไม่มีปัญหาเรื่อง Hardware Software people ware หรืออุบัติเหตุใดๆ ก็ตาม ความเสี่ยงต่าง ๆ ก็ยังคงรอวันอุบัติขึ้นจากระบบงานมีจุดอ่อนในตัวของมันเอง ซึ่งสิ่งเหล่านี้ อาจเกิดขึ้นได้จากการพัฒนาระบบงานที่ไม่ได้มาตรฐานและจะส่งผลกระทบต่อความน่าเชื่อถือได้ของข้อมูลทางการเงินและการดำเนินงาน ตลอดจนการตัดสินใจของฝ่ายบริหารที่ผิดพลาดจากจุดอ่อนที่มีในระบบงานนั้น ๆ ได้ องค์กรจึงมีความจำเป็นต้องมีบุคคลหรือคณะบุคคลเข้ามาช่วยฝ่ายบริหารดูแลในด้านนี้ และควรจัดตั้งเป็นหน่วยงานต่างหาก ซึ่งเรียกโดยรวม ๆ ว่าหน่วยงานตรวจสอบคอมพิวเตอร์ ในปัจจุบันมีหลายสถาบันที่แยกหน่วยงานเป็นฝ่ายตรวจสอบด้านคอมพิวเตอร์ สำนักงานตรวจสอบคอมพิวเตอร์ ฯลฯ เพื่อความคล่องตัวในการปฏิบัติงานเฉพาะด้าน แต่ในองค์กรขนาดเล็กความจำเป็นด้านนี้อาจมีน้อยลงไป โดยอาจมีพนักงานตรวจสอบด้านคอมพิวเตอร์อยู่ร่วมกับฝ่ายตรวจสอบทั่วไปได้ อย่างไรก็ตามการพิจารณาจัดตั้งหน่วยงานตรวจสอบด้านคอมพิวเตอร์นั้น มีปัจจัยที่ต้องพิจารณาประกอบดังนี้

1. สภาพแวดล้อมที่เปลี่ยนไปเมื่อองค์กรนำคอมพิวเตอร์มาใช้ในการประมวลข้อมูล

จากแถลงการณ์มาตรฐานการสอบบัญชี ฉบับที่ 28 และ 29 เรื่อง การสอบบัญชีในกรณีธุรกิจใช้คอมพิวเตอร์ และเรื่องการประเมินประสิทธิภาพการควบคุมภายในกรณีกิจการใช้คอมพิวเตอร์ ซึ่งสรุปได้ว่าคอมพิวเตอร์มีผลต่อธุรกิจดังนี้

1.1 ลักษณะการเปลี่ยนแปลงที่สำคัญมีผลกระทบต่อการจัดระบบบัญชี การควบคุมภายในของกิจการ และความเชื่อถือของผู้สอบบัญชีต่อการควบคุมภายในตลอดจนชนิด เวลา และขอบเขตของการใช้วิธีการตรวจสอบ ได้แก่

1.1.1 การจัดโครงสร้างขององค์กร

- การแบ่งหน้าที่

อาจมีประสิทธิภาพน้อยลง กิจการที่ใช้คอมพิวเตอร์จึงต้องมีการควบคุมอื่นเพื่อชดเชย

- การจัดเก็บโปรแกรมและแฟ้มข้อมูล

การจัดเก็บ การอ่าน การเรียกใช้ การเปลี่ยนแปลง ต้องใช้โปรแกรมคำสั่งงาน ซึ่งกิจการส่วนใหญ่มักจะเก็บโปรแกรมคำสั่งงานไว้ในที่เดียวกับข้อมูล จึงต้องมีการควบคุมเพิ่มเติม จากระบบ Manual เป็นต้น

1.1.2 วิธีการประมวลผล

- การขาดเอกสารที่ใช้ในการนำข้อมูลเข้าคอมพิวเตอร์
- การขาดหลักฐานอ้างอิงที่มองเห็นได้
- การขาดผลซึ่งสามารถมองเห็นได้จากการประมวลผลของคอมพิวเตอร์
- การเรียกข้อมูลหรือโปรแกรมคำสั่งงานมาใช้ทำได้ง่าย

1.1.3 การออกแบบและวิธีปฏิบัติงาน

- ความสม่ำเสมอของการปฏิบัติงาน
- การทำการควบคุมรวมอยู่ในโปรแกรมคำสั่งงาน
- รายการทางบัญชีหนึ่งรายการอาจนำไปปรับปรุงเพิ่มข้อมูลของคอมพิวเตอร์ ได้มากกว่าหนึ่งแฟ้ม
- ระบบงานอาจเป็นผู้สร้างรายการทางบัญชีขึ้นเอง
- สื่อที่ใช้ในการเก็บโปรแกรมคำสั่งงานและข้อมูลนั้นมีโอกาสเสียหายได้ง่าย

2. ความเสี่ยงของระบบการประมวลข้อมูลด้วยคอมพิวเตอร์

เทคโนโลยีด้านคอมพิวเตอร์นำความเสี่ยงใหม่ ๆ และความเสียหายใหม่ ๆ มาสู่องค์กรได้ดังนี้

ก. รายการทางการเงินผิดพลาด เกิดจากการบันทึกรายการไม่ตรงตามวันเวลาจำนวนเงินและประเภทบัญชีไม่ถูกต้อง

ข. รายการบันทึกบัญชีไม่เป็นที่ยอมรับ เกิดจากการกำหนดนโยบายทางการบัญชีที่ไม่ถูกต้องหรือไม่เหมาะสม

ค. ธุรกิจหยุดชะงัก ในองค์การที่ใช้คอมพิวเตอร์ในการประมวลผลและปฏิบัติงาน เช่น ธนาคารพาณิชย์ และบริษัทการเงิน เป็นต้น การที่เครื่องคอมพิวเตอร์และโปรแกรมหยุดการทำงาน หรือทำงานอย่างวิปริตโดยไม่ทราบสาเหตุ อาจเป็นเหตุให้การประกอบธุรกิจขององค์การหยุดชะงักชั่วคราวหรือเป็นเวลานานได้ นั้นหมายถึงการสูญเสียธุรกิจและรายได้จำนวนหนึ่ง

ง. การตัดสินใจที่ผิดพลาด เกิดจากการได้รับข้อมูลที่ไม่ถูกต้องหรือไม่มีข้อมูลในการตัดสินใจ

จ. การทุจริตและฉ้อฉลเกิดจากการนำเงินไปใช้เพื่อประโยชน์ส่วนตัวหรือหลอกลวงผู้อื่น

ฉ. การถูกดำเนินคดีหรือถูกลงโทษโดยทางราชการ เช่น การถูกเปรียบเทียบปรับเนื่องจากการกระทำการฝ่าฝืนกฎหมายเฉพาะที่ควบคุมกิจการนั้น หรือถูกคำพิพากษาให้ชดเชยค่าสินไหม เป็นต้น

ช. ทรัพย์สินสูญหายหรือถูกทำลาย หมายถึง สินทรัพย์ทั่วไป เงินสด และข้อมูลสำคัญสูญหายหรือทำลายโดยไม่ตั้งใจ

ฌ. ผลเสียค่าการแข่งขันทางการค้า หมายถึง ไม่สามารถสนองความต้องการของตลาดได้ทัน หรือโต้ตอบกับคู่แข่งได้อย่างมีประสิทธิภาพ

ญ. ความลึกลับรั่วไหล หมายถึง ความเสียหายโดยส่วนตัวหรือส่วนรวมอันเนื่องมาจากข้อมูลที่สำคัญถูกนำออกไปใช้โดยไม่ได้รับอนุญาตหรือไม่ตั้งใจ

ฎ. ความต้องการของ User ไม่ได้รับการสนองตอบ หมายถึง วิธีการปฏิบัติงานหรือระบบงานไม่ตรงเป้าหมายและความต้องการของ User

ฏ. ภาพพจน์ถูกทำลาย หมายถึง การที่ลูกค้า, สาธารณชน และรัฐบาลลดความไว้วางใจต่อองค์กร ความเสียหายตามข้างต้น อาจวัดเป็นจำนวนได้หากผู้วิเคราะห์มีข้อมูลและประสบการณ์เพียงพอ ดังวิธีการประเมินความเสี่ยงและความเสียหายที่กล่าวไปแล้ว

2.1 การจัดการกับความเสี่ยง

เมื่อทราบมูลเหตุ ความเสี่ยงและความเสียหายแล้ว ต่อไปก็จำเป็นต้องพิจารณาว่าจะจัดการกับมัน อย่างไร การจัดการกับความเสี่ยงมี 2 แบบ คือ

1. Risk Control คือ การใช้มาตรการทางด้านการควบคุมเพื่อขจัดหรือลดความเสี่ยงและความเสียหาย ซึ่งจะได้กล่าวเพิ่มเติมในเรื่องของการพิจารณาและประเมินประสิทธิภาพของการควบคุมต่อไป

2. Risk Financing คือ การโอนความเสี่ยงไปให้บุคคลอื่น เช่น ประกันภัย ปกติการประกันภัย มักจะถูกใช้ควบคู่ไปกับการควบคุมความเสี่ยงเสมอ ทั้งนี้เพราะการควบคุมแต่เพียงอย่างเดียวไม่อาจป้องกันหรือบรรเทาความเสียหายได้ร้อยเปอร์เซ็นต์ หรือได้ทุกกรณี เราไม่อาจเสี่ยงต่อความเสียหายได้แม้จะมีโอกาสเกิดน้อยก็ตาม เนื่องจากความเสียหายบางอย่างมีมูลค่าสูงเกินกว่าที่จะยอมรับได้ เช่น เครื่องคอมพิวเตอร์ถูกทำลายเสียหายจนใช้การไม่ได้ เป็นต้น

2.2 การประกันภัยทางด้านคอมพิวเตอร์

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

สิ่งที่ควรเอาประกันภัยเกี่ยวกับคอมพิวเตอร์

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

2.3 การพิจารณาวิธีการควบคุมความเสี่ยงและความเสียหาย

การควบคุมมีความมุ่งหมายเพื่อขจัดหรือลดความเสี่ยงและความเสี่ยงที่อาจเกิดแก่องค์กรอย่างน้อยที่สุดหากมีภัยและความเสียหายเกิดขึ้น ก็อยู่ในวิสัยที่จะรับได้ หรือทำให้กลับคืนสู่สภาวะปกติได้แนวคิดในการสร้างระบบการควบคุมมีหลายแนวทาง แต่การวิเคราะห์ความเสี่ยง เป็นแนวทางที่ทำให้การสร้างระบบการควบคุมเป็นไปอย่างรัดกุมและมีประสิทธิภาพมากที่สุด เนื่องจากตั้งอยู่บนพื้นฐานของแนวความคิดที่เป็นระบบและมีเหตุผล

จากการวิเคราะห์ความเสี่ยง ผู้วิเคราะห์จะได้ข้อมูลนำไปพิจารณาเพื่อควบคุมต่อไป

ก. ลักษณะของความเสี่ยง (Description of Risk)

ข. ความเสียหาย (Magnitude of Risk)

สิ่งที่ต้องพิจารณาในขั้นนี้เพื่อกำหนดเป็นนโยบาย และเป้าหมายของการควบคุมก็คือ ความมีนัยสำคัญ หรือระดับความเสี่ยงและความเสียหายที่ไม่อาจยอมรับได้จำเป็นต้องมีการควบคุม ทั้งนี้เพราะการควบคุมความเสียหายให้ได้ทั้งหมดเป็นเรื่องที่ทำได้ยาก หรือหากกระทำได้อาจเป็นการลงทุนที่ไม่คุ้มค่า

2.4 สิ่งที่ต้องพิจารณาเกี่ยวกับการควบคุม

(1) จุดที่ควรควบคุมตามที่กล่าวมาแล้วเราสามารถควบคุมตัวความเสี่ยงได้โดยตรง แต่ควบคุมที่เกิดเหตุและความเสียหายได้ ดังนั้นจุดที่เกิดความเสี่ยงและจุดที่มีการควบคุมจึงเป็นจุดเดียวกัน การเลือกจุดที่ควรควบคุมมีอยู่ 2 แนวทาง ซึ่งขึ้นอยู่กับความเสี่ยงว่าเป็นความเสี่ยงของระบบคอมพิวเตอร์ (EDP Resource) หรือ ระบบงานคอมพิวเตอร์ (EDP Application)

ก. ความเสี่ยงของระบบคอมพิวเตอร์ส่วนใหญ่จะเกิดกับ Hardware Software Data Files และ Operation เป็นต้น จุดที่ควรควบคุมก็คือจุดที่สามารถเข้าถึงสิ่งที่กล่าวมาแล้วได้

ข. ความเสี่ยงของระบบงานคอมพิวเตอร์ ส่วนใหญ่เกิดกับ Transactions หรือ Functions ของระบบงานอันเนื่องมาจาก

- ข้อมูลถูกเปลี่ยนแปลงแก้ไข
- รายการถูกดึงออกไปจากระบบงาน
- ผู้รับประโยชน์ถูกเปลี่ยนแปลงแก้ไข
- รายการเพิ่มเข้ามาในระบบงาน
- ข้อมูลบางส่วนหายไป

ฯลฯ

ดังนั้นจุดที่ควบคุมก็คือ จุดที่อาจทำให้ Transactions มีการเปลี่ยนแปลงดังกล่าว

(2) ลักษณะของการควบคุม การควบคุมโดยทั่วไปอาจแบ่งออกได้เป็นประเภทคือ

- การควบคุมทางการเงิน (Financial Control) และ
- การควบคุมการปฏิบัติงาน (Operation Control)

การควบคุมทางการเงิน หมายถึง การควบคุมเพื่อให้รายการทางการเงินถูกต้องสมบูรณ์ และเป็นไปตามหลักการบัญชีที่ยอมรับกันโดยทั่วไป

การควบคุมการปฏิบัติงาน หมายถึง การควบคุมให้มีการปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพ และประสิทธิผล

นอกจากนั้นการควบคุมอาจแบ่งออกได้เป็น 3 ลักษณะคือ

ก. การป้องกันหรือหลีกเลี่ยง มูลเหตุที่นำไปสู่ความเสียหาย (Prevention controls) ควรใช้กับความเสียหายที่ก่อให้เกิดความเสียหายและยากต่อการแก้ไขหรือเสียค่าใช้จ่ายมาก เช่น การป้องกันมิให้เข้าไปในห้องคอมพิวเตอร์ และใช้เครื่องโดยไม่ได้รับอนุญาต เป็นต้น การป้องกันอาจทำได้โดยมียามรักษาการ และออก Password ให้แก่ผู้มีสิทธิใช้เครื่อง เป็นต้น

ข. การตรวจให้พบมูลเหตุหรือปัญหาที่อาจนำไปสู่ความเสียหาย (Detection controls) ควรใช้กับความเสียหายที่ยังไม่เกิดความเสียหายโดยทันทีหรืออาจไม่เกิดความเสียหายร้ายแรง หรือถ้าจะคิดป้องกันก็คงทำได้ยากและเสียค่าใช้จ่ายมาก เช่น การบ่อนข้อมูล การป้องกันมิให้มีการบ่อนข้อมูลผิดพลาด ย่อมทำได้ยากกว่าตรวจสอบว่ามีข้อมูลที่ผิดพลาดหรือไม่ เป็นต้น การควบคุมในลักษณะนี้มักใช้เพื่อเสริมให้การควบคุมในแบบแรกมีประสิทธิภาพมากยิ่งขึ้น มีข้อที่ควรระวังก็คือการควบคุมนี้เป็นเพียงเครื่องมือค้นพบปัญหา แต่หากปัญหานั้นไม่ได้รับการแก้ไขหรือแก้ไขไม่ถูกต้อง ความเสียหายก็ยังคงเกิดขึ้นได้อีก โดยเฉพาะกรณีที่มีเจตนาละเมิด (Override) การควบคุมนั้น

ค. การตรวจให้พบมูลเหตุหรือปัญหาที่นำไปสู่ความเสียหาย และพร้อมกับการกำหนดวิธีการแก้ไขไว้ล่วงหน้า (Detection and Correction Controls) การควบคุมแบบนี้ดีกว่าแบบที่สอง เพราะว่าปัญหาที่ตรวจพบจะได้รับการแก้ไขอย่างเหมาะสมและรวดเร็ว เช่น การควบคุมความเสี่ยงอันเกิดจากไฟไหม้ โดยการติดตั้งเครื่อง Fire Alarm แต่เน้นอย่างเดียวยังไม่เพียงพอ เพราะแม้จะได้รับการเตือนว่าเกิดไฟไหม้ขึ้นแล้ว หากไม่สามารถดับไฟได้อย่างรวดเร็ว ความเสียหายก็ยังคงมีอยู่ ฉะนั้นจึงควรติดตั้งเครื่องดับไฟอัตโนมัติที่ควบคู่กันไปด้วย ซึ่งจะทำให้สามารถควบคุมความเสียหายได้ดีขึ้น

(3) เทคนิคที่ใช้ในการควบคุม หมายถึง วิธีปฏิบัติในการควบคุม อาจแยกได้เป็น 7 วิธี ดังนี้

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

ข. Verify หมายถึง การตรวจสอบกับหลักฐานที่เชื่อถือได้ เช่น ตรวจสอบเลขบัญชีของผู้ฝาก/ถอนกับ Data Base เป็นต้น

ค. Confirmation หมายถึง การให้ยืนยันความถูกต้อง เช่น กำหนดให้ผู้ป้อนรายการข้อมูลในระบบ Online ยืนยันความถูกต้องของข้อมูลที่ปรากฏอยู่บนจอเทอร์มินัล ก่อนที่ข้อมูลจะเข้าสู่ระบบ

ง. Recalculation หมายถึง การคำนวณซ้ำในจุดที่มีการคำนวณปกติจะให้คำนวณด้วยมือ (Manual) แล้วเทียบกับการคำนวณด้วยคอมพิวเตอร์ หรือ สลับกันโดยสูตรในการคำนวณเหมือนกัน

จ. Limit หมายถึง การกำหนดขอบเขตของหน้าที่ การกระทำหรือรายการไว้แน่นอน ซึ่งสามารถทำได้ทั้ง ปริมาณ และจำนวนเงิน เวลาและความถี่ เช่น การยินยอมให้ป้อนรหัสประจำตัว (Password) ผิดพลาดได้ไม่เกิน 3 ครั้ง ติดต่อกัน ครั้งที่ 4 เครื่องจะยึดบัตร หรือยกเลิกรายการที่จะทำต่อไป

ฉ. Containment หมายถึง การสกัดกั้นมิให้ความเสียหายระบอบหรือลุกลามไปยังที่อื่น เช่น กรณีเครื่อง คอมพิวเตอร์ตั้งอยู่ใกล้ๆ กัน 2 เครื่อง ควรกันผนังทึบไฟระหว่างเครื่องคอมพิวเตอร์ เพื่อป้องกันมิให้ไฟลุกลามจาก เครื่องหนึ่งไปอีกเครื่องหนึ่ง เป็นต้น

ช. Fallback หมายถึง การกำหนดวิธีปฏิบัติหรือระบบสำรองในกรณีเกิดความเสียหายบางส่วนหรือ ทั้งหมด เพื่อให้สามารถดำเนินงานต่อไปได้ เช่น กรณี Data Base ถูกทำลาย หรือ Memory บางส่วนไม่สามารถ ใช้งานได้ เป็นต้น

(4) การควบคุมทุกระบบควรมีการแก้ไขควบคู่กันไปด้วย เพราะการทราบว่ามีปัญหาแต่ไม่ทราบวิธี การแก้ไขที่เหมาะสมย่อมไม่สามารถป้องกันหรือบรรเทาความเสียหายได้

(5) การควบคุมด้วยคอมพิวเตอร์หรือเครื่องมือกลอื่น ๆ ย่อมดีกว่าการควบคุมด้วยมือ (Manual Controls) ถึงแม้ว่าการควบคุมโดยทั่วไปอาจทำได้ทั้งโดยบุคคลและโดยเครื่องมือกล แต่ก็เป็นที่ยอมรับกันว่าการ ควบคุมโดยเครื่องมือกลมีประสิทธิภาพมากกว่า

(6) การควบคุมที่ดีควรมีหลักฐานที่แสดงให้เห็นว่า ได้ควบคุมจริงและเป็นไปตามระเบียบและกฎ เกณฑ์ที่กำหนดไว้

2.5 การวางแผนการตรวจสอบ

ขั้นตอนที่สำคัญที่สุดของการตรวจสอบส่วนใหญ่ คือ การวางแผน ถ้าได้มีการทำการวางแผนล่วงหน้า ก่อนที่งานการตรวจสอบอย่างละเอียดจะเริ่มขึ้นแล้ว จะมีความเป็นไปได้สูงที่งานการตรวจสอบนั้นจะประสบความสำเร็จอย่างมีประสิทธิภาพ

2.5.1 มาตรฐานการสอบบัญชีตามประกาศ กบช. ฉบับที่ 19 (พ.ศ.2518) ข้อ 4 ได้กำหนดไว้ ว่า "ผู้สอบบัญชีต้องวางแผนการตรวจสอบและควบคุมผู้ช่วย (ถ้ามี) ให้ปฏิบัติงานโดยถูกต้อง" ดังนั้นคณะอนุกรรมการ มาตรฐานการสอบบัญชี สมาคมนักบัญชีรับอนุญาตแห่งประเทศไทย จึงเห็นสมควรกำหนดแนวทางและวิธีการในการ วางแผนและควบคุมงานสอบบัญชีให้เป็นไปตามมาตรฐานการสอบบัญชีที่รับรองทั่วไป เพื่อให้ผู้สอบบัญชีได้ไปปฏิบัติ เป็นแนวเดียวกัน

2.5.2 ผู้สอบบัญชีต้องวางแผนก่อนการตรวจสอบ การวางแผน หมายถึง การกำหนดขอบเขต เทคนิคและวิธีการที่ใช้ในการสอบบัญชี ความรู้และประสบการณ์ของผู้สอบบัญชีเกี่ยวกับกิจการที่ตรวจสอบเป็นปัจจัย สำคัญที่ช่วยในการวางแผน การวางแผนขึ้นอยู่กับขนาดของกิจการและความซับซ้อนของธุรกิจที่กิจการนั้นประกอบกิจการอยู่ ดังนั้น เพื่อให้การวางแผนมีประสิทธิภาพและได้ผล ผู้สอบบัญชีควรมีความรู้ในเรื่องต่าง ๆ เกี่ยวกับกิจการดังนี้

- 1) เรื่องต่าง ๆ เกี่ยวกับธุรกิจที่กิจการนั้นประกอบอยู่
- 2) ระบบและวิธีการบัญชี ทั้งทางด้าน Manual และ Computer
- 3) ระบบการควบคุมภายใน ทั้งทางด้าน Manual และ Computer
- 4) ขนาดและประเภทของรายการที่ถือว่าเป็นสาระสำคัญ
- 5) รายการปรับปรุงการเงินที่คาดว่าจะมี
- 6) สภาวะที่อาจก่อให้เกิดการเปลี่ยนแปลงในปริมาณหรือวิธีการทดสอบ
- 7) ลักษณะของรายงานการสอบบัญชีที่คาดว่าจะเสนอ

2.5.3 ในการวางแผนการสอบบัญชี ผู้สอบบัญชีจะต้องรวบรวมข้อมูลเกี่ยวกับระบบงานคอมพิวเตอร์

อาทิเช่น

- 1) การจัดองค์การและการแบ่งงานในหน้าที่ที่เกี่ยวข้อง กับระบบการประมวลผลข้อมูล
- 2) ขอบเขตของการใช้งานของคอมพิวเตอร์ในธุรกิจ
- 3) ลักษณะของคอมพิวเตอร์และอุปกรณ์พร้อมทั้งโปรแกรม
- 4) วิธีการประมวลผลข้อมูลของระบบงานที่มีสาระสำคัญต่องานการเงินรวมทั้งวิธีการจัดเก็บข้อมูลและนโยบายการรักษาข้อมูล
- 5) โครงการปัจจุบันของธุรกิจเกี่ยวกับการจัดทำระบบใหม่ หรือการแก้ไขเปลี่ยนแปลงระบบที่ใช้อยู่ในปัจจุบัน

2.5.4 ผู้สอบบัญชีจะต้องมีความรู้เกี่ยวกับการควบคุมภายในของระบบการประมวลผลข้อมูลโดยคอมพิวเตอร์ การควบคุมภายในของธุรกิจที่ใช้คอมพิวเตอร์ แบ่งได้ 2 ลักษณะ ดังนี้

- 1) การควบคุมภายในทั่วไป ได้แก่ การควบคุมที่เกี่ยวกับกิจการของหน่วยงานคอมพิวเตอร์
- 2) การควบคุมภายในเฉพาะระบบงาน ได้แก่ การควบคุมภายในซึ่งเกี่ยวกับความสมบูรณ์และถูกต้องของข้อมูลในแต่ละระบบงาน

2.5.5 ผู้สอบบัญชีจะต้องพิจารณาเรื่องต่าง ๆ ในข้อ 1 และข้อ 2 เพื่อใช้ในการวางแผนสอบบัญชี

เช่น

- 1) การวางแผนเพื่อสอบทานการปฏิบัติงานของระบบคอมพิวเตอร์ว่า ควรจะใช้วิธีการและเทคนิคการตรวจสอบได้เมื่อไรและในส่วนไหนของระบบ
- 2) การค้นหาจุดอ่อนของระบบการประมวลผลข้อมูล ซึ่งอาจมีข้อผิดพลาดหรือเปิดโอกาสให้มีการทุจริตได้
- 3) การพิจารณาระดับความเชื่อถือเกี่ยวกับการควบคุมต่าง ๆ ในการประเมินประสิทธิภาพการควบคุมภายในทั้งหมดของธุรกิจ
- 4) การวางแผนการใช้คอมพิวเตอร์มาช่วยในการปฏิบัติงานสอบบัญชี
- 5) การวางแผนการใช้บุคลากรที่มีความสามารถเฉพาะทางคอมพิวเตอร์ในกรณีที่จำเป็น

2.6 การวางแผนสอบบัญชีกับการวิเคราะห์ความเสี่ยง เพื่อให้เข้าถึงจุดควบคุมต่าง ๆ

ผลกระทบ TECHNOLOGY ทำให้ขั้นตอนและวิธีการปฏิบัติงานเปลี่ยนแปลงไปมาก การเปลี่ยนแปลงบางลักษณะได้ก่อให้เกิดความเสี่ยง (RISK) ที่ติดตามมาในรูปแบบต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อองค์กรได้ เช่น

ความเสี่ยงทางด้านการบริหารงานและการดำเนินงาน ในกรณีที่ระบบการควบคุมและรักษาความปลอดภัยไม่เพียงพอ เช่น การสูญหายของข้อมูลทางการเงินในระบบคอมพิวเตอร์ ความเสี่ยงจากระบบงานขัดข้องหรือเสียหาย ซึ่งอาจมีผลกระทบต่อชื่อเสียงหรือฐานะของกิจการอย่างร้ายแรงได้ หากองค์กรนั้นเป็นองค์กรที่เกี่ยวข้องกับการเงิน ที่ต้องติดต่อกับประชาชนจำนวนมาก ๆ

ผู้ตรวจสอบควรพยายามมองเห็นภาพพจน์ของกิจกรรมขบวนการขั้นตอนต่าง ๆ ในระบบ ในขณะที่จะเริ่มขบวนการรวบรวมเอกสารข้อมูล และอาจใช้เทคนิคการตั้งคำถามเพื่อหาจุดที่สามารถก่อให้เกิดข้อผิดพลาดขึ้นได้ ในแต่ละขบวนการและในแต่ละขั้นตอน คำตอบที่ได้จะชี้ถึงลักษณะของสาเหตุและความเฉพาะของความผิดพลาดที่เกิดขึ้น เช่น สาเหตุหนึ่งที่ทำให้เกิดจุดอ่อน คือ การบันทึกบัญชีผิดพลาด ซึ่งเป็นความผิดพลาดจากการทำด้วยมือ ลักษณะของความผิดพลาดก็อาจมีผลมาจากความผิดพลาดของพนักงาน เช่น ไม่บันทึกรายการให้ครบถ้วนหรือบันทึกรายการผิดพลาด หรือจำแนกประเภทรายการผิด เป็นต้น

คำถามที่ผู้ตรวจสอบควรถามต่อไป คือ ความผิดพลาดที่เกิดขึ้นนั้นมีสาระสำคัญหรือไม่ มีการควบคุมอะไรบ้าง ณ จุดนั้น ถ้าจะป้องกันมิให้เกิดจุดอ่อนขึ้นจะต้องมีการควบคุมอย่างไร

ผู้ตรวจสอบควรพัฒนาแผนแสดงกิจกรรมที่มีการปฏิบัติต่อรายการต่าง ๆ (TRANSACTION ACTIVITY FLOWCHARTS) ก่อนที่จะมุ่งรวบรวมข้อมูลในรายละเอียดและทำความเข้าใจให้ถ่องแท้ ซึ่งจะช่วยให้ผู้ตรวจสอบสามารถเข้าใจจุดที่จะตรวจสอบและลักษณะของข้อมูลที่ต้องการได้

ข้อมูลต่าง ๆ ที่รวบรวมได้ โดยเฉพาะกิจกรรมที่มีความสัมพันธ์กับข้อผิดพลาดหรือการควบคุม จะทำให้ผู้ตรวจสอบวางแผนการตรวจสอบได้อย่างมีประสิทธิภาพได้มากกว่าการใช้คำถามทั่วไป

2.6.1 ความเสี่ยงกับผู้ตรวจสอบ

การวิเคราะห์ความเสี่ยงโดยผู้ตรวจสอบเป็นแนวคิดใหม่ที่สำคัญยิ่งในการตรวจสอบขององค์กรที่ใช้คอมพิวเตอร์ และการใช้เทคนิคการวิเคราะห์ความเสี่ยงที่มีประสิทธิภาพจะช่วยให้ผู้ควบคุมงานและผู้บริหารมีความมั่นใจในประสิทธิภาพของการตรวจสอบได้อย่างเต็มที่ ไม่ว่าการตรวจสอบนั้นจะเป็นการตรวจสอบฐานะและการดำเนินงานตามปกติ (FINANCIAL OF REGULAR AUDIT) ขององค์กรหรือเป็นการตรวจสอบทางด้านคอมพิวเตอร์โดยเฉพาะ (EDP AUDIT) และโดยเฉพาะอย่างยิ่งการตรวจสอบการทุจริตการใช้เทคนิคการวิเคราะห์ความเสี่ยงจะช่วยกำหนดขอบเขต กำหนดขั้นตอน และใช้เครื่องมือการตรวจสอบได้อย่างมีประสิทธิภาพเพิ่มขึ้น

การวิเคราะห์ความเสี่ยงจะมีบทบาทที่สำคัญยิ่งในการวางแผนการตรวจสอบ โดยเฉพาะในเรื่องที่เกี่ยวข้องกับการพิจารณาจุดอ่อนที่อาจมีได้ในองค์กร ตั้งแต่ระบบสูงสุดถึงระบบต่ำสุด การวิเคราะห์ความเสี่ยงจึงควรทำในลักษณะ TOP-DOWN เสมอ เพื่อให้ผู้ตรวจสอบจะได้เห็นภาพความเสี่ยงที่มีผลกระทบและเกี่ยวเนื่องซึ่งกันและกัน เพราะโดยทั่วไปหากมีจุดอ่อนในการบริหารงาน ระดับนโยบาย ซึ่งเป็นระดับ TOP แล้ว จุดอ่อนที่มีความเสี่ยงก็จะมีผลกระทบต่อระดับล่างอย่างหลีกเลี่ยงไม่ได้

2.6.2 ความเสี่ยงกับผู้บริหารระดับสูง

ในการประเมินความเสี่ยงภัย และการวิเคราะห์หาจุดสำคัญๆ ในแต่ละระดับของการควบคุมทั่วไป ในระดับของผู้บริหารระดับสูงนั้น มีขั้นตอนโดยสรุปดังนี้

- ขั้นที่ 1 พิจารณาว่าความรับผิดชอบของผู้บริหารระดับสูงเพียงพอกับความเสี่ยงภัยในแต่ละเรื่องหรือไม่
- ขั้นที่ 2 เรื่องใดที่ไม่เพียงพอ ก็ให้บทวนขั้นตอนการปฏิบัติที่ใช้อยู่ในเรื่องความรับผิดชอบของผู้บริหาร ซึ่งเป็นเรื่องการจัดองค์กร การวางแผน การสั่งการ การควบคุม รวมทั้งขั้นตอนการควบคุม (CONTROL FUNCTIONS) ของฝ่ายบริหารในด้านการอนุมัติรายการ การแบ่งแยกหน้าที่ การรับทราบผลการปฏิบัติงานและการติดตามให้ปฏิบัติตามระเบียบ ขององค์กร
- ขั้นที่ 3 ความเสี่ยงภัยในเรื่องใด ที่สรุปว่ามีการควบคุมไม่เพียงพอ ก็ให้ประเมินค่าความเสียหายที่อาจเกิดขึ้นออกมาและต้องตรวจสอบการควบคุมต่าง ๆ ภายในระบบงาน (APPLICATION CONTROLS) ด้วยว่าจะสามารถชดเชยการควบคุมทั่วไป (ENVIRONMENTAL CONTROLS) ที่ขาดหายไปในระดับบริหารในเรื่องที่เกี่ยวข้องได้หรือไม่ แต่อย่างไรก็ดี มักจะเป็นเรื่องผิดปกติที่การควบคุมภายในระบบงานจะใช้ได้ผลถ้าการควบคุมทั่วไปบกพร่อง

ผู้สอบบัญชีจำเป็นต้องพิจารณาถึงวัตถุประสงค์ของการควบคุมทั่วไปกับความเสี่ยง (EXPOSURES) ที่อาจเกิดขึ้น เริ่มง่าย ๆ โดยนึกถึงวัตถุประสงค์ในการควบคุมว่า "ความถูกต้องในการปฏิบัติงานควรเป็นอย่างไร" แล้วพิจารณาถึงความเสี่ยงภัยที่อาจเกิดขึ้นได้ประกอบกันไปว่า "มีอะไรบ้างที่เป็นปัจจัยที่ทำให้เกิดข้อมูลผิดพลาดได้" การพิจารณาในลักษณะนี้ มักจะทำให้พบวัตถุประสงค์ของการควบคุมทั่วไปไว้ตั้งแต่ต้น

ความเสี่ยงภัยกับผู้บริหารโดยแท้จริงแล้วก็คือ การสะท้อนให้เห็นถึงวัตถุประสงค์ของการควบคุมทั่วไปอย่างมีหลักเกณฑ์ในด้านที่เกี่ยวข้อง

2.6.3 ความเสี่ยงกับการวางแผน

การประเมินควบคุมภายใน เป็นขั้นตอนหนึ่งของการวางแผนงานสอบบัญชี ความเสี่ยงเป็นนามธรรมที่ไม่อาจตรวจสอบได้ แต่การวิเคราะห์ความเสี่ยงเป็นหลักสำคัญที่จะทำให้ผู้ตรวจสอบทราบถึงกิจกรรมที่อาจมีจุดอ่อนที่มีผลกระทบอย่างสำคัญต่อองค์กร เพื่อค้นหาจุดควบคุมหลักและจุดควบคุมรองต่าง ๆ ที่มีอยู่ในองค์กรได้อย่างเหมาะสม ซึ่งจะช่วยให้การวางแผนการตรวจสอบมีหลักเกณฑ์ และช่วยให้ผู้บริหารมั่นใจประสิทธิภาพผลการตรวจสอบมากขึ้น

การวิเคราะห์และประเมินระบบการควบคุมภายในของระบบงานจะรวมทั้งส่วนที่เป็น PHYSICAL และ LOGICAL เพื่อให้การตรวจสอบมีประสิทธิภาพและประสิทธิผลเต็มที่นั้นผู้ตรวจสอบต้องสามารถกำหนดขอบเขตของระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ หรือ ด้วย MANUAL ให้ได้เสียก่อน แล้วจึงค่อย ๆ แยกแยะไปในส่วนย่อย ๆ แยกแขนงกันออกไปในลักษณะของ TOP-DOWN BASIS เช่น ระบบเงินฝากก็ต้องมีระบบการ

คำนวณดอกเบี้ยด้วย เป็นต้น กระบวนการวิเคราะห์แยกแยะในลักษณะของระบบงานนี้ผู้ตรวจสอบจะต้องเข้าใจความหมายของคำว่า "มาตรฐานระบบงาน" ว่ามีขอบเขตเพียงใดก่อนด้วย

การประเมินจุดที่ควรมีการควบคุมนั้น ผู้ตรวจสอบไม่อาจกำหนดหรือคาดคะเนได้ล่วงหน้าเลย ถ้าไม่มีหลักการในการกำหนดจุดอ่อนที่ว่่านั้น แนวความคิดในที่นี้ก็คือ การตั้งคำถามที่มีแบบแผนในแต่ละส่วนและในแต่ละหน้าที่ของงานที่ตรวจสอบนั้น ๆ เพื่อที่จะกำหนดได้ว่าควรมีจุดควบคุมอะไรบ้างในขั้นตอนใด และในเวลาไหนของส่วนงานนั้น ๆ เช่น การตั้งคำถามดังนี้

- ขั้นตอนนั้นเกี่ยวข้องกับหลักการบัญชีที่เป็นที่ยอมรับกันหรือไม่
- ขั้นตอนนั้นเกี่ยวข้องกับสินทรัพย์ในปัจจุบันหรือในภายหน้าหรือไม่
- ขั้นตอนนั้นเป็นขั้นตอนรับเงินหรือจ่ายเงิน
- ระบบงานนั้น ๆ จะมีผลกระทบต่อการบันทึกความถูกต้องของข้อมูลหรือไม่
- มีนโยบายหรือมีข้อผูกพันทางกฎหมาย และระเบียบข้อบังคับใดๆ เกี่ยวข้องและต้องพิจารณาหรือไม่
- มีความเสี่ยงในขั้นตอนใด เมื่อพิจารณาในลักษณะ TOP-DOWN ของส่วนงานนั้นๆ

จากคำถามข้างต้น จะทำให้ผู้ตรวจสอบสามารถบ่งชี้ถึงจุดควบคุมภายในที่ควรจะมีได้ทั้งในแบบ AUTOMATED และในระบบ MANUAL และสามารถกำหนดถึงจุดควบคุมหลักและจุดควบคุมรอง เพื่อการวางแผนและการทดสอบต่อไปได้

2.6.4 ตัวอย่างของการวิเคราะห์ความเสี่ยง โดยระบุถึงสาเหตุความเสียหายและการควบคุมภายในของการพัฒนาระบบงาน



สาเหตุ	ผลเสียหาย	การควบคุมภายใน		
		เพื่อการป้องกัน	เพื่อการค้นหา	เพื่อการแก้ไข
การวิเคราะห์และประเมินผลได้และเสียทางเศรษฐกิจไม่ครบถ้วน	สูญเสียค่าใช้จ่ายเกินความจำเป็น เนื่องจากการพัฒนาระบบงานไม่คุ้มค่า (Unjustified systems) และไม่ก่อให้เกิดประโยชน์ต่อการแข่งขันในทางธุรกิจอันเนื่องมาจากการพัฒนาระบบงานที่มีได้สนองตอบความต้องการขององค์กร	กำหนดประเภทของกิจกรรม (Activities) และเป้าหมายหลัก (Objectives) ในการพัฒนาระบบงานให้เป็นมาตรฐาน	1. ให้ผู้บริหารระดับสูงและผู้ใช้ข้อมูลทบทวนและประเมินผลงานทุกขั้นตอนของการพัฒนาระบบงาน เมื่อพบว่าข้อที่ไม่สมเหตุสมผลอย่างร้ายแรงในขั้นตอนใดให้สั่งหยุดการพัฒนาขั้นตอนถัดไปทันทีจนกว่าจะแก้ไขแล้ว / หรือ 2. ผู้บริหารระดับสูงอาจมอบหมายให้ผู้ตรวจสอบภายในขององค์กรเป็นผู้ทำหน้าที่ทบทวนและประเมินผลขั้นตอนของการพัฒนาระบบงาน โดยเฉพาะความเหมาะสมของการควบคุมภายในของระบบงาน	
ผู้บริหารระดับอาวุโสละเลยความรับผิดชอบและการตัดสินใจที่เกี่ยวข้องกับการพัฒนาระบบงาน โดยอ้างเหตุผลว่าเป็นเรื่องทางเทคนิค เกินกว่าจะทำความเข้าใจได้	นอกจากจะสูญเสียค่าใช้จ่ายและไม่ก่อให้เกิดประโยชน์ทางด้านการแข่งขันแล้ว ยังทำให้ฝ่ายบริหารขององค์กรตัดสินใจผิดพลาดด้วย	กำหนดประเภทของกิจกรรม (Activities) และเป้าหมายหลัก (Objectives) ในการพัฒนาระบบงานให้เป็นมาตรฐาน	ให้ผู้บริหารระดับสูงขององค์กรหรือมอบหมายให้ผู้ตรวจสอบภายในทำหน้าที่ทบทวนและประเมินผลทุกขั้นตอนของการพัฒนาระบบงานทุกระบบ	

สาเหตุ	ผลเสียหาย	การควบคุมภายใน		
		เพื่อการป้องกัน	เพื่อการค้นหา	เพื่อการแก้ไข
ผู้วิเคราะห์ระบบงานไม่เข้าใจระบบงานและความต้องการของผู้ใช้ข้อมูล (Users) ดีพอ รวมทั้งการใช้เทคนิคทางการประมวลข้อมูลที่ไม่เหมาะสม ซึ่งจะส่งผลให้คู่มือการปฏิบัติงานและโปรแกรมงานขาดสาระที่สำคัญไปหรือเกินความเป็นจริง	สูญเสียค่าใช้จ่ายและทำให้ฝ่ายบริหารตัดสินใจผิดพลาดได้	1. การจ้างบุคคลที่ได้รับการอบรมและฝึกฝนทางด้านนี้โดยเฉพาะหรือส่งพนักงานที่มีอยู่ไปเข้ารับการอบรมและฝึกฝนทางด้านเทคนิคเพิ่มเติมทั้งภายในและภายนอกอยู่เสมอ 2. ให้จัดทำเอกสารประกอบการวิเคราะห์ทุกขั้นตอน :- 2.1 รายงานการศึกษาระบบงาน 2.2 รายงานความต้องการของระบบงาน 2.3 รายงานเกี่ยวกับด้านเทคนิค 2.4 แผนการสร้างระบบงาน ฯลฯ	ให้ผู้ใช้อ้างอิงข้อมูลเป็นผู้ทดสอบระบบงานหรือที่เรียกว่า Acceptance Test หรืออาจมอบหมายให้ผู้ตรวจสอบภายในเป็นผู้ทำหน้าที่ทดสอบระบบงาน	

สาเหตุ	ผลเสียหาย	การควบคุมภายใน		
		เพื่อการป้องกัน	เพื่อการค้นหา	เพื่อการแก้ไข
การออกแบบระบบงานผิดพลาดทั้งๆ ที่มีรายละเอียดความต้องการของผู้ใช้ข้อมูล และด้านเทคนิคครบถ้วน สาเหตุประการหนึ่งเนื่องมาจากการใช้วิจารณ์งานที่ต่างกันของผู้ออกแบบระบบงานแต่ละคน	การบันทึกข้อมูลทางบัญชีผิดพลาดหรือใช้ระบบการบัญชีที่ไม่เป็นที่ยอมรับกันโดยทั่วไป ทำให้ผู้บริหารตัดสินใจผิดพลาดหรือเสียค่าใช้จ่ายในการประมวลผลเกินความจำเป็น		1. ให้ผู้ใช้ข้อมูลหรือผู้ตรวจสอบภายในเป็นผู้ทำหน้าที่ทดสอบระบบงาน (Acceptance Test) 2. ให้ผู้ออกแบบระบบงาน จัดทำเอกสารประกอบโดยละเอียด	
พนักงานที่มีส่วนในการออกแบบระบบงานไม่มีความสามารถ	การบันทึกข้อมูลทางบัญชีผิดพลาดหรือระบบบัญชีไม่เป็นที่ยอมรับกันโดยทั่วไป ทำให้ผู้บริหารตัดสินใจผิดพลาดหรือเสียค่าใช้จ่ายเกินความจำเป็น	การว่าจ้างบุคคลที่มีความสามารถเฉพาะหรือส่งพนักงานที่มีอยู่ไปเข้ารับการอบรมและฝึกฝนทางด้านเทคนิคเพิ่มเติมอยู่เสมอ	1. มอบหมายให้ผู้ควบคุมงาน ด้านการวิเคราะห์และการเขียนโปรแกรม ทบทวนผลลัพธ์ของการดำเนินงานพัฒนาระบบทุกขั้นตอน ก่อนส่งให้ฝ่ายบริหารและผู้ใช้อุปกรณ์ให้ความเห็นชอบ 2. ให้ผู้ใช้ข้อมูลหรือผู้ตรวจสอบภายในเป็นผู้ทำหน้าที่ทดสอบความถูกต้องของระบบงาน	

สาเหตุ	ผลเสียหาย	การควบคุมภายใน		
		เพื่อการป้องกัน	เพื่อการค้นหา	เพื่อการแก้ไข
ผู้วิเคราะห์ระบบงานและผู้เขียนโปรแกรมออกแบบระบบงานและโปรแกรมตามความพอใจของตนเอง โดยไม่คำนึงถึงผู้ใช้ข้อมูลซึ่งเป็นเจ้าของระบบงาน หรือคิดว่าตนเองเข้าใจความต้องการดีกว่าผู้ใช้ข้อมูลเอง จนบางครั้งการออกแบบระบบงานที่ยากเกินความสามารถของผู้ใช้ข้อมูล	สูญเสียค่าใช้จ่ายในการพัฒนาระบบงานโดยไม่ได้รับผลประโยชน์ใดๆ เนื่องจากผู้ใช้ข้อมูลไม่สามารถปฏิบัติงานตามที่ออกแบบไว้ได้ ทำให้ระบบงานนั้นถูกละเลยโดยสิ้นเชิง หรือทำให้การประกอบธุรกิจขององค์กรชะงักงันได้	การกำหนดให้ผู้บริหารโครงการพัฒนาระบบใหม่ (Project Leader) จัดทำแผนและตารางการปฏิบัติงานแต่ละโครงการ (Project Planing) และการมอบหมายงานให้พนักงานที่อยู่ในความรับผิดชอบการประเมินผลงานและการรายงานความคืบหน้าของโครงการ (Status report)	1. มอบหมายให้ผู้ควบคุมงานทบทวนผลลัพธ์ที่ได้จากงานทุกขั้นตอน 2. มอบหมายให้ผู้ตรวจสอบภายในหรือผู้ออกแบบระบบงานทบทวนระบบงานนั้นอีกครั้งหลังจากที่ปล่อยให้ใช้กับงานจริงแล้ว 3-6 เดือน เพื่อค้นหาข้อผิดพลาดที่ยังหลงเหลือ เช่น เสียค่าใช้จ่ายในการปฏิบัติงานมากเกินไป	
การสื่อสารความเข้าใจระหว่างฝ่ายพัฒนาระบบงาน ฝ่ายผู้ใช้ข้อมูล และฝ่ายบริหารระดับสูงอยู่ในสภาพที่ใช้ไม่ได้	การบันทึกข้อมูลทางบัญชีผิดพลาดหรือระบบบัญชีไม่เป็นที่ยอมรับกันโดยทั่วไป ทำให้ผู้บริหารตัดสินใจผิดพลาดหรือเสียค่าใช้จ่ายเกินความจำเป็น	1. ให้ฝ่ายพัฒนาระบบงานจัดทำแผนในการพัฒนาระบบงานประเมินผลงานตามที่ปรากฏในแผน และจัดทำรายงานความคืบหน้าของโครงการ เพื่อเสนอต่อฝ่ายผู้ใช้ข้อมูล และฝ่ายบริหารระดับสูง 2. ให้ฝ่ายพัฒนาระบบงานจัดทำเอกสารประกอบการปฏิบัติงานทุกขั้นตอนโดยละเอียดและเรียบร้อย เพื่อส่งให้ฝ่ายผู้ใช้ข้อมูลและฝ่ายบริหารระดับสูงทบทวนได้ทุกขณะเมื่อมีปัญหาเกิดขึ้น		

สาเหตุ	ผลเสียหาย	การควบคุมภายใน		
		เพื่อการป้องกัน	เพื่อการค้นหา	เพื่อการแก้ไข
ไม่ได้วางหลักเกณฑ์ไว้ว่าเมื่อใดจึงควรจะหยุดการพัฒนาระบบนั้นได้แล้วอย่าหลงทำไปจนกระทั่งงานสิ้นสุด เช่นการคาดคะเนค่าใช้จ่ายไว้ต่ำเกินไปมาก ความต้องการของหน่วยงานเปลี่ยนแปลงไปหรือมีกฎหมายใหม่ๆ เกิดขึ้นจะมีผลทำให้ได้รับผลประโยชน์ไม่คุ้มกับค่าใช้จ่ายที่เสียไป	สูญเสียค่าใช้จ่ายไปโดยไม่ได้รับประโยชน์คุ้มค่า		1. ให้ฝ่ายบริหารระดับสูงและผู้ใช้ข้อมูลทบทวนผลลัพธ์ที่ได้จากการพัฒนาระบบงานทุกขั้นตอน เมื่อเห็นว่าขั้นตอนใดมีผลลัพธ์ต่างไปจากที่ต้องการมากหรือไม่เหมาะสมกับสถานการณ์ในขณะนั้นให้สั่งระงับการพัฒนากระบวนการนั้นทันที หรือ 2. มอบหมายให้ผู้ตรวจสอบภายในกระทำหน้าที่แทน ภายใต้การรับผิดชอบของผู้บริหารระดับสูง	
มีช่องทางล่อใจให้พนักงานผู้มีส่วนร่วมในการพัฒนาระบบงานบางคนพยายามสร้างวิธีการคดโกงหรือทำลายระบบงานนั้นระหว่างการพัฒนากระบวนการ เช่น ผู้เขียนโปรแกรมอาจเขียนบางส่วนของโปรแกรมให้สามารถลวงผลการควบคุมของโปรแกรมระบบงานอื่นเพื่อประโยชน์ของตนเอง โดยวิธีนี้ผู้เขียน	การบันทึกข้อมูลทางบัญชีผิดพลาดก่อให้เกิดการทุจริต หรือทรัพย์สินสูญหายหรือถูกทำลาย	ให้จัดทำเอกสารประกอบการพัฒนาระบบงานทุกขั้นตอนอย่างละเอียดและเรียบร้อย	1. ให้ฝ่ายบริหารระดับสูงและผู้ใช้ข้อมูลทบทวน 2. หรือมอบหมายให้ผู้ตรวจสอบภายในมีส่วนในการพัฒนาระบบงานแต่เริ่มแรก 3. หรือมอบหมายให้ผู้ตรวจสอบภายในทดสอบระบบงานนี้ก่อนนำออกไปใช้งานจริง	

สาเหตุ	ผลเสียหาย	การควบคุมภายใน		
		เพื่อการป้องกัน	เพื่อการค้นหา	เพื่อการแก้ไข
โปรแกรมไม่จำเป็นต้องเข้าไปในศูนย์คอมพิวเตอร์ก็สามารถฉ้อฉลข้อมูลได้			4. ให้ผู้บริหารฝ่ายพัฒนาระบบงาน ทบทวนความถูกต้องทางด้านเทคนิคทั้งหมด ก่อนส่งมอบให้ผู้บริหารระดับสูง หรือผู้ใช้ข้อมูล เห็นชอบ	
ระบบงานซึ่งไม่สามารถปรับปรุงแก้ไขทางเทคนิคหรือทางด้านค่าใช้จ่ายให้เหมาะสมกับความต้องการขององค์กรที่เปลี่ยนแปลงไป ซึ่งเท่ากับเป็นการบีบบังคับหรือกดขี่องค์กรคงอยู่ในสภาพเช่นนั้นตลอดไม่สามารถปรับตัวให้ทันต่อสภาวะแวดล้อมที่เปลี่ยนแปลงไป	สูญเสียค่าใช้จ่ายโดยไม่ได้รับประโยชน์คุ้มค่าและอาจต้องพัฒนาระบบงานขึ้นใหม่ทั้งหมด แทนที่จะเปลี่ยนแปลงเพียงบางส่วนซึ่งจะทำให้เสียค่าใช้จ่ายเพิ่มขึ้นมาก	ให้ฝ่ายพัฒนาระบบงานจัดทำเอกสารประกอบทุกขั้นตอนอย่างละเอียดและเรียบร้อย	1. มอบหมายให้ผู้ตรวจสอบภายใน ทดสอบระบบงานนั้น ก่อนนำออกไปใช้งานจริง 2. ให้บริหารฝ่ายพัฒนาระบบงาน ทบทวนความถูกต้องทางด้านเทคนิคทั้งหมด	การจัดทำเอกสารประกอบระบบงานโดยละเอียดทั้งหมด
แนวความคิดและความเข้าใจของพนักงานมีส่วนร่วมในการพัฒนาระบบงานแต่ละคนแตกต่างกัน ทำให้ผลลัพธ์ที่ได้ไม่บรรลุเป้าหมาย	การบันทึกข้อมูลทางบัญชีอาจผิดพลาด สูญเสียค่าใช้จ่ายไปโดยไม่ได้รับผลประโยชน์คุ้มค่า และยังสามารถทำให้อำนาจขององค์กรชะงักงันได้	ให้ฝ่ายพัฒนาระบบงานจัดทำแผนงานและเป้าหมายของงานแต่ละชั้น เพื่อเป็นแนวทางในการปฏิบัติงานแก่พนักงานที่เกี่ยวข้อง - System Planning Steps	1. ให้ฝ่ายพัฒนาระบบงานทบทวนความถูกต้องทางด้านเทคนิคทั้งหมด 2. มอบหมายให้ผู้ตรวจสอบภายในเข้าไปร่วมในการพัฒนาระบบงานและทดสอบความ	

สาเหตุ	ผลเสียหาย	การควบคุมภายใน		
		เพื่อการป้องกัน	เพื่อการค้นหา	เพื่อการแก้ไข
		- Development Steps - Implementation Steps	ถูกต้องของระบบงานนั้น ก่อนนำออกไปใช้งานจริง 3. ให้ฝ่ายพัฒนาระบบงานทบทวนความถูกต้องของระบบงานนั้นอีกครั้งเมื่อปล่อยให้ใช้กับงานจริงแล้ว 3-6 เดือน 4. ให้จัดทำเอกสารประกอบระบบงานโดยละเอียดทั้งหมด	



2.7 การประเมินประสิทธิภาพของการควบคุม

เป็นขั้นตอนสุดท้ายของวัฏจักรในการวิเคราะห์ความเสี่ยง เพื่อจัดทำข้อมูลสำหรับการตัดสินใจของฝ่ายบริหารว่าควรมีการควบคุมหรือไม่และอย่างไร

จากการวิเคราะห์ความเสี่ยงทำให้เราทราบมูลเหตุที่เกิดความเสี่ยงและความเสียหาย ดังนั้น การควบคุมที่ดีหรือที่มีประสิทธิภาพจึงควรเป็นการควบคุมที่สามารถลดความเสียหายลงให้น้อยที่สุด (Minimize Loss) หรืออีกนัยหนึ่งก็คือให้ผลตอบแทนต่อการลงทุนมากที่สุด (Maximize Benefit) วิธีการพิจารณาอย่างง่าย ๆ ดีคือ การเปรียบเทียบระหว่างความเสียหายที่คาดว่าจะเกิดขึ้น (Expected Loss) กับรายจ่ายในการควบคุม (Control Cost) ถ้าหากความเสียหายมากกว่ารายจ่ายในการควบคุมก็แสดงว่าการควบคุมนั้นมีประสิทธิภาพ ในกรณีที่มีหลายทางเลือกการควบคุมแบบที่เสียค่าใช้จ่ายน้อยสุด โดยมีเงื่อนไขว่าการควบคุมทุกแบบสามารถคุ้มครองความเสียหายได้เท่าเทียมกัน

ในกรณีที่ไมทราบหรือไม่สามารถคำนวณความเสี่ยงในรูปจำนวนเงินได้การตัดสินใจในการควบคุมอาจต้องใช้เกณฑ์อื่น อาทิเช่น การเปรียบเทียบรายจ่ายในการควบคุมกับมูลค่าความเสียหายทั้งสิ้น (Total Loss) สมมติว่ากิจการมีเงินให้กู้ยืมทั้งสิ้น 1,000 ล้านบาท อาจกำหนดเกณฑ์ในการตัดสินใจว่า รายจ่ายในการควบคุมไม่ควรเกินร้อยละ 0.5 ของมูลค่าเงินให้กู้ยืม ซึ่งเท่ากับ 5 ล้านบาท เป็นต้น

อย่างไรก็ตาม การตัดสินใจควบคุมบางอย่างมิได้ขึ้นอยู่กับประสิทธิภาพของการควบคุม แต่จำเป็นต้องมีการควบคุมเพื่อความอยู่รอดของกิจการ เช่น การควบคุมที่เกิดจากระเบียบหรือข้อบังคับของรัฐ เป็นต้น

2.8 การควบคุมในระบบงานที่ใช้คอมพิวเตอร์ (Controls in EDP)

1) ทบทวนวัตถุประสงค์ในการควบคุมภายใน

- เพื่อป้องกันมิให้ทรัพย์สินสูญหายเสียหายจากการทุจริต ความผิดพลาด และภัยพิบัติ
- เพื่อให้ข้อมูลทางการเงินและบัญชีถูกต้อง เชื่อถือได้
- เพื่อให้การปฏิบัติงานมีประสิทธิภาพและเป็นไปตามนโยบายของฝ่ายบริหาร

ผู้ตรวจสอบในปัจจุบันให้ความสำคัญต่อการควบคุมภายในเป็นอย่างมากเพราะนอกจากผู้ตรวจสอบจะทำการตรวจสอบร่างงบทางการเงินและระบบบัญชีถูกต้อง ณ วันตรวจสอบแล้วยังต้องการให้แน่ใจต่ออีกว่าสิ่งนี้จะยังถูกต้องตลอดไป (Ongoing basis) ถ้ามีระบบการควบคุมภายในที่ดี

2) Basic Type of Control

2.1 Administrative Controls การควบคุมในเชิงบริหารหรือที่เรียกกันว่า Management Controls หรือ non-financial controls เป็นเรื่องของการบริหารที่นำมาใช้เพื่อให้การปฏิบัติงานในองค์กรบรรลุคุณสมบัติที่สำคัญ 3 ประการ คือ

- มีประสิทธิภาพ
- มีประสิทธิผล
- เป็นไปตามนโยบาย

การควบคุมเหล่านี้ ได้แก่

(1) การควบคุมโดยการจัดองค์การ (Organization Controls)

– การแบ่งหน้าที่และความรับผิดชอบให้ชัดเจน

(2) การควบคุมการปฏิบัติงาน (Operation Controls)

– การกำหนดนโยบายดำเนินงาน (Policies)

– การกำหนดวิธีปฏิบัติงาน (Procedures)

(3) การควบคุมโดยใช้ระบบรายงาน (Management Reports)

เพื่อให้ฝ่ายบริหารได้ข้อมูลต่าง ๆ มาใช้ในการตัดสินใจวางแผนและควบคุมการปฏิบัติงานจุดใดจุดหนึ่งเป็นพิเศษ เป็นเครื่องชี้ให้ทราบว่า

– จุดใดบ้างที่อาจก่อให้เกิดปัญหา

– ใช้ในการวางแผน

– ใช้ในการตัดสินใจ

(4) การควบคุมโดยการจัดให้มีการตรวจสอบภายใน (Audit Function)

เพื่อเป็นหูเป็นตาแทนฝ่ายบริหาร

2.2 Accounting Controls การควบคุมทางบัญชี หรือการควบคุมทางการเงิน เป็นเรื่องของการควบคุมที่มุ่งหวังเพื่อป้องกันทรัพย์สินและความถูกต้องของข้อมูลทางการเงินและการบัญชี

– การควบคุมดูแลรักษาทรัพย์สินให้มีอยู่ครบถ้วน และปลอดภัย

– การบันทึกรายการครบถ้วนและถูกต้อง

การควบคุมเหล่านี้ได้แก่

(1) การแบ่งแยกหน้าที่และความรับผิดชอบ เพื่อไม่ให้อุบัติการณ์ใดบุคคลหนึ่งสามารถควบคุมงานโดยตลอดครบวงจร

(2) การควบคุมโดยวิธีปฏิบัติงาน

– ใช้แบบฟอร์ม

– ขั้นตอนสำหรับการทำรายการใดรายการหนึ่งตั้งแต่ต้นจนจบ (Work Flow หรือ Document Flow)

(3) การควบคุมโดยการทำหน้าที่ให้มี Reconciliation & Balancing Function

– การพิสูจน์ยอดคงเหลือเป็นครั้งคราว

– การตรวจนับทรัพย์สิน

– การขอคำรับรองจากบุคคลภายนอก

2.3 EDP Controls

(1) General Controls (ศูนย์ฯ)

- Separation of Duties
- Environmental Control
- Security Control
- Hardware Control
- Program Control
- Documentation Control
- Data Control
- Backup & Recovery Control

(2) Application Control (งาน)

- Data Preparation control input control
- Data Entry Control
- Processing Control
- Output Control
- Backup & recovery Control

2.9 สรุป

ผู้สอบบัญชียุคใหม่ จะพบกับความท้าทายทางเทคโนโลยีกว่าสมัยก่อนมาก ผู้สอบบัญชีจึงต้องเข้าใจถึงความเป็นไปขององค์การและการประมวลผลข้อมูล ตลอดจนสภาพแวดล้อมที่เปลี่ยนแปลงไปในการประมวลผลข้อมูลให้่องแท้ ผู้สอบบัญชีจะต้องประสบกับปัญหาของการกำหนดขอบเขต และทิศทางของการตรวจสอบ ตลอดจนเทคนิคการตรวจสอบที่ต้องใช้ให้เหมาะสมกับสภาพขององค์การที่ใช้คอมพิวเตอร์ ผู้สอบบัญชีขององค์การที่ใช้คอมพิวเตอร์จะต้องประเมินการควบคุมภายในของระบบงานในลักษณะทาง "ลึก" และต้องรู้จักทำผลประเมินการควบคุมภายในของระบบงานมาเป็นประโยชน์ในการตัดสินใจเกี่ยวกับการวางแผนงานการตรวจสอบต่อไปด้วย เพราะหากผู้ตรวจสอบไม่เข้าใจ "ระบบงาน" ที่จะตรวจสอบอย่างเพียงพอแล้ว จะทำให้ไม่อาจวางแผนการตรวจสอบและกำหนดกระบวนการตรวจสอบ ตลอดจนมอบหมายและควบคุมงานตรวจสอบที่มีประสิทธิภาพได้

ความรู้เกี่ยวกับการจัดองค์การและการแบ่งหน้าที่ที่เกี่ยวข้องกับระบบการประมวลผลข้อมูลขอบเขตของการทำงานของคอมพิวเตอร์ในธุรกิจ ลักษณะของคอมพิวเตอร์และอุปกรณ์พร้อมทั้งโปรแกรม วิธีการประมวลผลข้อมูลรวมทั้งวิธีการจัดเก็บข้อมูลและนโยบายการรักษาข้อมูลโครงการปัจจุบันของธุรกิจเกี่ยวกับการจัดทำระบบข้อมูลด้วยคอมพิวเตอร์หรือการแก้ไขเปลี่ยนแปลงระบบที่ใช้อยู่ในปัจจุบันพร้อมทั้งความรอบรู้ในด้านการควบคุมภายในทั่วไป และการควบคุมภายในเฉพาะระบบงาน การค้นหาจุดอ่อนของระบบงาน การพิจารณาระดับความเชื่อถือเกี่ยวกับการควบคุมต่าง ๆ ในการประเมินประสิทธิภาพการควบคุมภายในทั้งหมดของธุรกิจ ความรู้เกี่ยวกับกระบวนการตรวจสอบและเทคนิคต่าง ๆ

ของระบบที่ใช้คอมพิวเตอร์ มีเรื่องและรายละเอียดที่ผู้ตรวจสอบต้องทำความเข้าใจมากมาย แต่ก็เป็นสิ่งจำเป็นที่ผู้ตรวจสอบไม่อาจหลีกเลี่ยงได้ ถ้าต้องการก้าวไปให้ทันกับความท้าทายทางเทคโนโลยียุคใหม่เกี่ยวกับการวางแผนงานและการตรวจสอบ

4. การควบคุมงานตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

4.1 การขยายขอบเขตความรับผิดชอบการควบคุมภายในใหม่ของผู้สอบบัญชี

สมาคมผู้สอบบัญชีรับอนุญาตของอเมริกา (AICPA) ได้ออกแถลงการณ์เกี่ยวกับมาตรฐานการสอบบัญชีใหม่ ฉบับที่ 55 เรื่อง ข้อควรพิจารณาในการตรวจสอบงบการเงินเกี่ยวกับโครงสร้างการควบคุมภายใน โดยมีผลข้อบังคับใช้แล้วตั้งแต่วันที่ 1 มกราคม 2533

แถลงการณ์ใหม่ได้ขยายขอบเขตความรับผิดชอบออกไป 2 ทาง คือ

- (1) ขยายการควบคุมภายในเป็นโครงสร้างการควบคุมภายใน
โครงสร้างการควบคุมภายใน ประกอบด้วย
 - สภาพแวดล้อมของการควบคุม
 - ระบบการบัญชีและ
 - มาตรการควบคุม

ทั้ง 3 องค์ประกอบเป็นแหล่งข้อมูลที่สำคัญของประเภทและความเสี่ยง (Risks) ของข้อผิดพลาดที่มีสาระสำคัญที่อาจเกิดขึ้นได้ ไม่ใช่ผิดพลาดแต่มาตรการควบคุมเพียงอย่างเดียว

(2) เพิ่มความรู้ ความเข้าใจของผู้สอบบัญชีเกี่ยวกับการควบคุมภายใน ผู้สอบบัญชีต้องเข้าใจว่านโยบายและมาตรการควบคุมต่าง ๆ ถูกออกแบบมาได้อย่างไร และยังคงถือปฏิบัติอยู่หรือไม่

4.2 ความเข้าใจอย่างเพียงพอต่อความรับผิดชอบของผู้สอบบัญชี

ผู้สอบบัญชีจะต้องมีความเข้าใจในโครงสร้างการควบคุมภายในอย่างเพียงพอต่อการ

- วางแผนการตรวจสอบ และ
- ควบคุมการตรวจสอบให้เป็นไปตามแผนงาน และ
- เป้าหมายที่กำหนดไว้

4.3 ความรู้และความชำนาญ

– ในการสอบบัญชีธุรกิจที่ใช้คอมพิวเตอร์ ผู้สอบบัญชีต้องมีความรู้และความชำนาญเกี่ยวกับเครื่องคอมพิวเตอร์และอุปกรณ์โปรแกรม และระบบการประมวลผลข้อมูลอย่างเพียงพอ ทั้งนี้ขึ้นอยู่กับความยุ่งยาก ซับซ้อนของระบบบัญชีที่ใช้คอมพิวเตอร์นั้น

– ผู้สอบบัญชีที่มีความรู้ความสามารถทางคอมพิวเตอร์จะสามารถเข้าใจถึงผลที่เปลี่ยนแปลงไปอันเนื่องมาจากการที่ธุรกิจนำคอมพิวเตอร์มาใช้ ซึ่งจะช่วยในการวางแผนงานสอบบัญชี การกำหนดวิธี การศึกษาและ

ประเมินประสิทธิภาพระบบการควบคุมภายใน การกำหนดขั้นตอนและวิธีการของการสอบบัญชี ตลอดจนการนำคอมพิวเตอร์มาช่วยในการสอบบัญชี

– ผู้สอบบัญชีจะต้องมีความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์เพียงพอที่จะตรวจสอบธุรกิจที่ใช้คอมพิวเตอร์ มิฉะนั้นจะต้องใช้ผู้ชำนาญอื่นช่วยในการตรวจสอบ

4.4 ความรับผิดชอบและการควบคุมภายในของผู้สอบบัญชี

– ผู้สอบบัญชียังคงต้องรับผิดชอบในการแสดงความเห็นต่องบการเงิน แม้ว่าจะได้มอบหมายหน้าที่ในงานตรวจสอบบางส่วนให้แก่ผู้ช่วย ผู้เชี่ยวชาญ หรือผู้สอบบัญชีอื่น ดังนั้นผู้สอบบัญชีต้องมีความรู้ทางคอมพิวเตอร์เพียงพอที่จะมอบหมายงาน ควบคุมดูแลและสอบทานงานที่มอบหมายให้ผู้อื่นดังกล่าว หรือที่จะพิจารณาให้แน่ใจว่าขอบเขตของการปฏิบัติงานและผลงานของผู้เชี่ยวชาญหรือผู้สอบบัญชีอื่นเป็นไปตามวัตถุประสงค์ของตนแล้ว

– อย่างไรก็ดี ถ้าธุรกิจใช้คอมพิวเตอร์ประมวลผลข้อมูลทางการเงินในส่วนที่เป็นสาระสำคัญ รวมทั้งการควบคุมภายในของธุรกิจแล้ว ผู้สอบบัญชีไม่ควรใช้ผลงานของผู้เชี่ยวชาญทางด้านคอมพิวเตอร์โดยไม่ได้ผ่านการพิจารณาหรือสอบทานก่อนที่จะนำผลงานนั้นมาเป็นข้อมูลในการแสดงความเห็นต่องบการเงิน

4.5 โครงสร้างของการตรวจสอบกับการควบคุม

ผู้สอบบัญชีควรมีความเข้าใจเกี่ยวกับ

- โครงสร้างของระบบงาน
- การประมวลงาน
- ที่มาของข้อมูล

การเก็บข้อมูลในระบบงานที่ใช้คอมพิวเตอร์อย่างเพียงพอ โดยเฉพาะอย่างยิ่งโครงสร้างการควบคุมภายในที่ประกอบไปด้วย สภาพแวดล้อมของการควบคุมใหม่ทั้งในส่วนที่เป็น Manual และ Computer เพื่อที่จะได้ควบคุมดูแลงานตรวจสอบของตนได้อย่างเหมาะสม

การที่องค์กรใช้คอมพิวเตอร์ในการประมวลงาน จะมีผลกระทบต่อการวางแผนงานวิธีการตรวจสอบ และกระบวนการตรวจสอบได้อย่างสำคัญ จึงใคร่ขอสรุปเรื่องราวดังกล่าวข้างต้นเพียงย่อ ๆ เพื่อชักชวนความเข้าใจในเรื่องนี้ร่วมกัน

4.6 การวางแผนงานสอบบัญชี

ผู้สอบบัญชีต้องวางแผนก่อนการตรวจสอบ การวางแผน หมายถึง การกำหนดขอบเขตเทคนิคและวิธีการที่ใช้ในการตรวจสอบบัญชี ความรู้และประสบการณ์ของผู้สอบบัญชีเกี่ยวกับกิจการที่ตรวจสอบเป็นปัจจัยสำคัญที่ช่วยในการวางแผน การวางแผนขึ้นอยู่กับขนาดของกิจการและความซับซ้อนของธุรกิจที่กิจการนั้นประกอบกิจการอยู่ ดังนั้น เพื่อให้การวางแผนมีประสิทธิภาพและได้ผล ผู้สอบบัญชีควรมีความรู้ในเรื่องต่าง ๆ เกี่ยวกับกิจการดังนี้

- 1) เรื่องต่าง ๆ เกี่ยวกับธุรกิจที่มีกิจการนั้นประกอบกิจการอยู่
- 2) ระบบและวิธีการบัญชี
- 3) ระบบการควบคุมภายใน

- 4) ขนาดและประเภทของรายการที่ถือว่าเป็นสาระสำคัญ
- 5) รายการปรับปรุงงบการเงินที่คาดว่าจะมี
- 6) สภาวะที่อาจก่อให้เกิดการเปลี่ยนแปลงในปริมาณหรือวิธีการทดสอบ
- 7) ลักษณะของรายงานการสอบบัญชีที่คาดว่าจะเสนอ



10

**การวางแผนกับ
วิธีการตรวจสอบ**

การวางแผนกับวิธีการตรวจสอบ

1. การวางแผน การจัดคณะผู้ตรวจสอบ และการกำกับการตรวจสอบด้านคอมพิวเตอร์

1.1 การวางแผนการตรวจสอบ (Planning) หมายถึงการกำหนดวัตถุประสงค์และวิธีการ ตรวจสอบ โดยละเอียด เพื่อใช้เป็นแนวทางในการตรวจสอบ ลักษณะการตรวจสอบทั่วไปแบ่งวิธีการตรวจสอบออกเป็นหลายขั้นตอน โดยทุกขั้นตอนจะมีจุดมุ่งหมายในการตรวจสอบดังนี้

วิธีการตรวจสอบโดยย่อ

(1) การตรวจสอบขั้นต้น (Preliminary review) มีจุดมุ่งหมายเพื่อทำความเข้าใจระบบบัญชีทั้งส่วนที่ใช้คอมพิวเตอร์ และส่วนที่ไม่ใช้คอมพิวเตอร์ ทั้งนี้ ควรศึกษาขั้นตอนในการบันทึกบัญชีขอบเขตการใช้ข้อมูล โครงสร้างพื้นฐานของการควบคุมทางบัญชีในศูนย์ประมวลผลและผู้ให้ข้อมูลโดยอาจจะใช้วิธีการสอบถาม สังเกตการณ์ ตรวจ-สอบเอกสารสำคัญ (Documentation) ติดตามการจัดทำข้อมูล และใช้แบบสอบถามเกี่ยวกับการควบคุมภายใน หรือ Check Lists

(2) การกำหนดขอบเขตของการตรวจสอบ เพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบมีจุดมุ่งหมายเพื่อ ประเมินผลการควบคุมภายในที่สำคัญ เช่น การควบคุมทางบัญชี โปรแกรมและการปฏิบัติงาน เป็นต้น วิธีการและขอบเขตของการตรวจสอบขึ้นอยู่กับความคิดเห็นของผู้ตรวจสอบ

(3) สอบทานระบบการควบคุมทั่วไป (Review of General Controls) มีจุดมุ่งหมายเพื่อศึกษาระบบ ควบคุมทั่วไปภายในศูนย์คอมพิวเตอร์และหน่วยงานที่ใช้ข้อมูล พิจารณาข้อดีและข้อเสีย และทดสอบการควบคุมที่ จำเป็น การสอบทานทำได้โดยการศึกษาดokumentation อย่างละเอียด สอบถามพนักงานในศูนย์ คอมพิวเตอร์และหน่วยงานที่ใช้ข้อมูลและการสังเกตการณ์

(4) สอบทานระบบควบคุมสำหรับงานใดงานหนึ่งโดยเฉพาะ มีจุดมุ่งหมายเพื่อศึกษาระบบควบคุม และ พิจารณาทดสอบการควบคุมที่จำเป็น วิธีสอบทานเป็นทำนองเดียวกับ ข้อ (3)

(5) การประเมินผลขั้นต้นเกี่ยวกับการควบคุมภายใน (Assessment of controls) มีจุดมุ่งหมายเพื่อ ประเมินผลการควบคุมภายในที่สำคัญ เป็นการพิจารณาชนิดของข้อผิดพลาด วิธีควบคุม วิธีค้นหา วิธีการตรวจสอบ ขึ้นอยู่กับความคิดเห็นของผู้ตรวจสอบ

(6) การทดสอบการปฏิบัติงานตามระเบียบที่ได้กำหนดไว้ (Test of Compliance) มีจุดมุ่งหมายเพื่อ พิจารณาว่า มีวิธีการควบคุมภายในที่จำเป็นและผลของการควบคุมน่าพอใจเพียงใด วิธีการที่ใช้คือ การตรวจสอบ บันทึกการทำงาน ทดสอบวิธีการควบคุม สอบถามและสังเกตการณ์

(7) การประเมินผลขั้นสุดท้ายเกี่ยวกับการควบคุมภายใน (Evaluation of Controls) มีจุดมุ่งหมายเพื่อ พิจารณาชนิดของข้อผิดพลาด และวิธีป้องกันหรือค้นหาข้อผิดพลาดผลที่กระทบต่อลักษณะเวลา และขอบเขตของการ ตรวจสอบ วิธีการที่ใช้ขึ้นอยู่กับความคิดเห็นของผู้ตรวจสอบ

1.2 การจัดคณะผู้ตรวจสอบ (Organizing) หมายถึง การจัดผู้ตรวจสอบและเครื่องมือที่จะใช้ในการตรวจสอบ กำหนดหน้าที่ความรับผิดชอบแต่ละบุคคล ตามแผนงานที่วางไว้และประเมินประสิทธิภาพของโครงสร้างและแผนงานที่กำหนดไว้

1.3 การกำกับการตรวจสอบ (Supervising) หมายถึง การกำหนดขอบเขตความถี่ และมาตรฐานการตรวจสอบ ดูแลให้มีการปฏิบัติตามมาตรฐานการตรวจสอบ ติดตามควบคุม และปรับปรุงมาตรฐานการตรวจสอบที่กำหนดไว้ให้สอดคล้องกับสถานการณ์อย่างใกล้ชิด เพื่อนำผลการตรวจสอบมาปรับปรุงแก้ไขตามควรแก่กรณี

2. วิธีการตรวจสอบ (Audit Procedures)

การตรวจสอบด้านคอมพิวเตอร์มีอยู่หลายวิธี สดแล้วแต่ความรู้ความชำนาญของผู้ตรวจสอบและสภาพของธนาคารแต่ละแห่ง แต่พอสรุปวิธีการตรวจสอบที่เป็นมาตรฐานได้ 2 วิธี คือ วิธีที่ไม่ใช้คอมพิวเตอร์ช่วยในการตรวจสอบ และวิธีที่ใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

2.1 การตรวจสอบโดยไม่ใช้คอมพิวเตอร์

การตรวจสอบตามวิธีนี้อาศัยการพิจารณาสภาพการดำเนินงาน ประมวลผลเป็นหลักในการทดสอบข้อมูล โดยการสุ่มตัวอย่างข้อมูลมาทำการทดสอบ ซึ่งไม่จำเป็นต้องใช้โปรแกรมและคอมพิวเตอร์เข้าช่วย ผู้ตรวจสอบภายในจะนำข้อมูลที่คัดเลือกมาทดสอบนี้เปรียบเทียบกับเอกสารขั้นต้นที่เป็นแหล่งกำเนิดข้อมูล และ/หรือสอบถามยืนยันยอดข้อมูลแต่ละรายการกับเอกสารต้นฉบับโดยตรงเป็นการกระหนาบยอดข้อมูล ซึ่งจะได้ผลเช่นเดียวกับการตรวจสอบสมุดบัญชีตามแบบเก่าที่ใช้พนักงานบันทึกบัญชี

นอกจากนี้ ผู้ตรวจสอบภายในควรตรวจสอบการปฏิบัติงาน ทดสอบการปฏิบัติตามระเบียบ และทำการทดสอบในเรื่องอื่น ๆ ที่มีความสำคัญ รวมทั้งประเมินคุณภาพของข้อมูลด้วย แม้ว่าการตรวจสอบดังกล่าวไม่ได้ระบุไว้ในโปรแกรมการตรวจสอบด้านคอมพิวเตอร์ก็ตาม ทั้งนี้เพื่อสอบถามความถูกต้องในการประมวลผล โดยดำเนินการ ดังนี้

- (1) ตรวจสอบการปฏิบัติงาน (Application Review)
 - (1.1) ใช้แบบสอบถาม
 - (1.2) สอบถามพนักงานของศูนย์ประมวลผล
 - (1.3) ศึกษากระบวนการทั่วไปโดยละเอียด
 - (1.4) ตรวจสอบวิธีการควบคุมที่สำคัญในส่วนที่เกี่ยวกับหน่วยงานที่ใช้ข้อมูลและศูนย์ประมวลผล
 - (1.5) ตรวจสอบวิธีการใช้โปรแกรมงานควบคุมข้อมูลที่นำมาประมวลผลเพื่อประโยชน์ในการตรวจสอบที่สำคัญ
- (2) ทำการทดสอบการปฏิบัติตามระเบียบที่ได้กำหนดไว้ (Compliance Test)
 - (2.1) ตรวจสอบเอกสารหลักฐานที่ใช้ในการควบคุมภายใน เช่น รายละเอียดเกี่ยวกับข้อผิดพลาด ยอดรวม batch ต่าง ๆ เป็นต้นไป)

- (2.2) ตรวจสอบรายงานที่ได้จากการประมวลผล ย้อนกลับไปยังเอกสารขั้นต้น หรือในทางกลับกันอาจตรวจจากเอกสารขั้นต้นมายังรายงานและตรวจสอบยอดรวมข้อมูลที่ปรากฏตามรายงานกับยอดคุมขั้นต้นด้วย
 - (2.3) สุ่มตัวอย่างข้อมูลมาตรวจสอบความถูกต้องในการประมวลผล
 - (2.4) ประเมินคุณภาพการทดสอบข้อมูล
 - (2.5) ตรวจสอบความถูกต้องในการสรุปยอดบัญชี (ยอดรวมย่อยกับยอดรวมทั้งสิ้น)
 - (2.6) สุ่มตัวอย่างข้อมูลมาทำการทดสอบ โดยการยืนยันยอด (confirmation) ทดสอบความจริง (reasonableness test) ฯลฯ
- (3) การประเมินข้อมูล
- (3.1) กระทบยอดคุมของหน่วยงานที่ใช้ข้อมูลกับยอดคุมข้อมูลที่ได้ในระหว่างการประมวลและกระทบยอดตามรายงานที่ได้จากการประมวลผลกับตัวเลขในบัญชีแยกประเภททั่วไป
 - (3.2) พิจารณาการควบคุมภายในของหน่วยงานที่ใช้ข้อมูล ศูนย์ประมวลผลและวิธีการควบคุมในโปรแกรมเป็นไปตามระเบียบที่วางไว้หรือไม่

2.2 การตรวจสอบโดยใช้คอมพิวเตอร์

การใช้คอมพิวเตอร์ช่วยตรวจสอบจะสามารถลดค่าใช้จ่ายในการทดสอบและสุ่มตัวอย่างลงได้ นอกจากนี้ยังช่วยให้ผู้ตรวจสอบคุ้นเคยกับการใช้อุปกรณ์ในศูนย์ประมวลผลด้วย

ตัวอย่างการใช้คอมพิวเตอร์

- (1) ทดสอบยอดรวมและการคำนวณ เพื่อสอบทานความถูกต้องในการประมวล
- (2) ทดสอบความสมบูรณ์ (completeness) ความมีเหตุผลสอดคล้องกันอย่างสม่าเสมอ (logical consistency) ความถูกต้องในเงื่อนไข (Validity of conditions) และความสมจริง (reasonableness) ของข้อมูล
- (3) สรุปยอดข้อมูลและวิเคราะห์การปฏิบัติงาน
- (4) ใช้เทคนิคการสุ่มตัวอย่างทางสถิติคัดเลือกข้อมูลมาใช้ในการยืนยันยอด
- (5) ดำเนินการประมวลผลโดยอิสระเลียนแบบของจริง เพื่อสอบทานความถูกต้อง (correctness) และความสม่าเสมอ (consistency) ในการประมวลผลของโปรแกรมที่ใช้
- (6) ออกงบทดลองและรายงานสำหรับการตรวจสอบ

โปรแกรมที่ใช้ในการตรวจสอบ มีดังนี้

- (1) โปรแกรมที่เขียนขึ้นโดยคณะผู้ตรวจสอบภายในด้านคอมพิวเตอร์
- (2) โปรแกรมตรวจสอบทั่วไป (เช่น software audit package ของผู้ผลิตคอมพิวเตอร์ หรือสำนักงานสอบบัญชี)
- (3) โปรแกรมที่จ้างให้บุคคลภายนอกเขียนขึ้น

โปรแกรมที่ใช้ในการตรวจสอบเหล่านี้ ควรมีการควบคุมอย่างเข้มงวด ดังนั้นจะต้องควบคุมเอกสารที่เกี่ยวข้องกับโปรแกรม ข้อมูลที่ใช้ในการทดสอบ รายละเอียดเกี่ยวกับข้อมูลที่ทดสอบ (source listings) รวมทั้ง source และ object โปรแกรมที่ใช้ตรวจสอบ นอกจากนี้ จะต้องควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรมด้วย ในศูนย์ประมวลผลที่มีการควบคุม software library ที่ทันสมัย object audit program จะถูก catalogue เก็บไว้ และใช้รหัสลับ (password) ป้องกัน ในกรณีนี้ ผู้ตรวจสอบจะต้องควบคุมเอกสารและ job control instructions ให้รัดกุม เพื่อควบคุมการใช้โปรแกรมตรวจสอบที่เก็บไว้ใน library หากวิธีการดังกล่าวขัดต่อระเบียบการควบคุมภายใน ก็ไม่ควรจะ catalogue โปรแกรมที่ใช้ในการตรวจสอบเก็บไว้ใน library โปรแกรมต่าง ๆ ที่ใช้ในการตรวจสอบ ควรจัดทำเอกสารประกอบโดยละเอียดเพื่อทราบจุดมุ่งหมายและวิธีใช้โปรแกรมอย่างถูกต้อง

การนำเอา audit software ไปใช้ในการตรวจสอบ ควรดำเนินการ

- (1) จัดให้มีการควบคุมอุปกรณ์ (physical control) audit software เว้นแต่ software ดังกล่าวจะถูก catalogue เก็บไว้ในระบบ และมีการป้องกันเป็นอย่างดี
- (2) สังเกตการประมวลผลงานตรวจสอบ
- (3) ใช้โปรแกรมอิสระควบคุมหรือติดตามการประมวลผลด้วย audit software
- (4) ควบคุมแฟ้มข้อมูลที่จะใช้ในการประมวลผลและจัดทำรายงานให้สมบูรณ์และถูกต้อง

2.3 สรุป

1. ในการวางแผนงานสอบบัญชี ผู้สอบบัญชีจะต้องรวบรวมข้อมูลเกี่ยวกับระบบคอมพิวเตอร์ อาทิ
เช่น
 - 1.1 การจัดองค์การและการแบ่งงานในหน้าที่ที่เกี่ยวข้องกับระบบการประมวลผลข้อมูล
 - 1.2 ขอบเขตของการใช้งานคอมพิวเตอร์ในธุรกิจ
 - 1.3 ลักษณะของคอมพิวเตอร์และอุปกรณ์พร้อมทั้งโปรแกรม
 - 1.4 วิธีการประมวลผลข้อมูลของระบบงานที่มีสาระสำคัญต่องานการเงิน รวมทั้งวิธีการจัดเก็บข้อมูลและนโยบายการรักษาข้อมูล
 - 1.5 โครงการปัจจุบันของธุรกิจเกี่ยวกับจัดทำระบบใหม่ หรือ การแก้ไขเปลี่ยนแปลงระบบที่ใช้
อยู่ในปัจจุบัน
2. ผู้สอบบัญชีจะต้องมีความรู้เกี่ยวกับการควบคุมภายในของระบบการประมวลผลข้อมูลโดยคอมพิวเตอร์ การควบคุมภายในของธุรกิจที่ใช้คอมพิวเตอร์ แบ่งได้เป็น 2 ลักษณะ ดังนี้
 - 2.1 การควบคุมภายในทั่วไป ได้แก่ การควบคุมที่เกี่ยวกับกิจการของหน่วยงานคอมพิวเตอร์
 - 2.2 การควบคุมภายในเฉพาะระบบงาน ได้แก่ การควบคุมภายในซึ่งเกี่ยวกับความสมบูรณ์และถูกต้องของข้อมูลในแต่ละระบบงาน

3. ผู้สอบบัญชีจะต้องพิจารณาเรื่องต่าง ๆ ในข้อ 1 และ 2 เพื่อใช้ในการวางแผนสอบบัญชี เช่น
 - 3.1 การวางแผนเพื่อสอบทานการปฏิบัติงานของระบบคอมพิวเตอร์ว่าควรจะใช้วิธีและเทคนิคการตรวจสอบใดเมื่อไรและในส่วนไหนของระบบ
 - 3.2 การค้นหาจุดอ่อนของระบบการประมวลผลข้อมูลซึ่งอาจมีข้อผิดพลาดหรือเปิดโอกาสให้มีการทุจริตได้
 - 3.3 การพิจารณาระดับความเชื่อถือเกี่ยวกับการควบคุมต่าง ๆ ในการประเมินประสิทธิภาพการควบคุมภายในทั้งหมดของธุรกิจ
 - 3.4 การวางแผนการใช้คอมพิวเตอร์มาช่วยในการปฏิบัติงานสอบบัญชี
 - 3.5 การวางแผนในการใช้บุคลากรที่มีความสามารถเฉพาะทางคอมพิวเตอร์ในกรณีจำเป็น



11

การตรวจสอบของ
ผู้ตรวจสอบภายในและ
ผู้สอบบัญชี

การตรวจสอบของผู้ตรวจสอบภายใน และผู้สอบบัญชี

องค์กรที่นำคอมพิวเตอร์มาใช้งาน ควรจัดให้มีการควบคุมภายในอย่างเพียงพอเพื่อให้แน่ใจว่า การปฏิบัติข้อมูลถูกต้องและปลอดภัย ยึดมั่นตามนโยบาย มาตรฐานการบริหารงานและระเบียบปฏิบัติที่เหมาะสม การควบคุมภายในจะมีประสิทธิภาพได้ก็ต่อเมื่อมีการตรวจสอบที่เป็นอิสระ ดังนั้น ภาระรับผิดชอบเบื้องต้นของคณะกรรมการบริหารขององค์กรคือ การจัดให้มีการตรวจสอบเพื่อประเมินผลการควบคุมภายใน

ผู้ตรวจสอบควรเสนอรายงานและแจ้งผลการตรวจสอบโดยตรงต่อคณะกรรมการบริหารองค์กร เพื่อป้องกันมิให้ผู้ตรวจสอบอยู่ภายใต้การบังคับบัญชาของผู้ที่ถูกตรวจสอบ ซึ่งอาจทำให้ขาดความเป็นอิสระในการตรวจสอบได้

1. การคัดเลือกคณะผู้ตรวจสอบ

องค์กรควรคัดเลือกบุคคลที่มีความรู้ความชำนาญพอที่จะตรวจสอบงานประมวลผลได้มาเป็นผู้ตรวจสอบในด้านคอมพิวเตอร์ขององค์กร ในกรณีที่ผู้ตรวจสอบภายในขององค์กรยังไม่มีความรู้ความชำนาญดีพอ ควรขอความช่วยเหลือหรือมอบหมายหน้าที่ให้ผู้อื่น เช่น สำนักงานสอบบัญชี หรือผู้เชี่ยวชาญด้านคอมพิวเตอร์ หรือองค์กรอื่นที่เคยร่วมมือให้ความช่วยเหลือกัน ทำหน้าที่ตรวจสอบให้ จนกว่าองค์กรจะพัฒนาผู้ตรวจสอบภายในด้านคอมพิวเตอร์ที่มีคุณสมบัติเหมาะสมได้

สำหรับองค์กรที่ใช้บริการด้านคอมพิวเตอร์จากภายนอกธนาคาร ควรระบุนความรับผิดชอบในการตรวจสอบไว้ในสัญญาจ้างให้แน่ชัด ซึ่งอาจเลือกวิธีใดวิธีหนึ่งหรือหลายวิธีรวมกันดังนี้

- (1) ให้ผู้ตรวจสอบภายในของบริษัทที่รับจ้างขององค์กรประมวลผลช่วยตรวจสอบ วิธีนี้จะใช้ได้ผล หากองค์กรแน่ใจในความเป็นอิสระของผู้ตรวจสอบ
- (2) ใช้ผู้ตรวจสอบภายในและ/หรือผู้สอบบัญชีขององค์กรดำเนินการตรวจสอบ
- (3) ใช้บุคคลที่สาม (Third-party) ที่มีคุณสมบัติเหมาะสมมาดำเนินการตรวจสอบโดยอิสระไม่ขึ้นกับใครทั้งสองฝ่าย
- (4) ตรวจสอบร่วมกันหลายองค์กร ในกรณีที่องค์กรหลายแห่งใช้บริการด้านคอมพิวเตอร์จากบริษัทที่จ้าง ประมวลผลแห่งเดียวกัน โดยอาจตกลงร่วมกันตรวจสอบงานประมวลผล

2. หน้าที่และความรับผิดชอบของผู้ตรวจสอบภายใน

องค์กรควรกำหนดหน้าที่และความรับผิดชอบของผู้ตรวจสอบภายในเป็นลายลักษณ์อักษรให้ชัดเจน งานของผู้ตรวจสอบภายใน ได้แก่

- (1) ตรวจสอบ ประเมินผล และรายงานเกี่ยวกับการบัญชี การเงิน และการควบคุมภายใน มีการปฏิบัติงานที่ถูกต้องและน่าพอใจเพียงใด

- (2) ช่วยให้การควบคุมภายในมีประสิทธิภาพ
- (3) ควบคุมการใช้ทรัพย์สินและป้องกันมิให้สูญหาย
- (4) ควบคุมการบริหารงานข้อมูลที่น่ามาใช้งาน
- (5) ประเมินประสิทธิภาพการทำงานของหน่วยงานต่างๆ
- (6) เสนอแนะแนวทางการแก้ไขข้อบกพร่องของการควบคุมภายใน

ผู้ตรวจสอบภายในจะต้องศึกษาลึกเข้าไปในเรื่องการบันทึกบัญชี การควบคุมงานทุกขั้นตอนเพื่อทำความเข้าใจเกี่ยวกับงานที่ตรวจสอบอย่างเต็มที่ และจะต้องวิเคราะห์ประเมินผล ให้คำแนะนำ ตั้งข้อสังเกตเกี่ยวกับงานที่ตรวจสอบ เสนอต่อฝ่ายบริหาร

3. ความรู้ความสามารถของผู้ตรวจสอบภายในด้านคอมพิวเตอร์

ผู้ตรวจสอบภายในด้านคอมพิวเตอร์ควรมีความรู้ความชำนาญ ดังนี้

- (1) มีความรู้ความเข้าใจในระบบการบัญชีและการจัดเก็บข้อมูลเป็นอย่างดี
- (2) มีความเข้าใจในหลักการควบคุมภายในอย่างลึกซึ้ง
- (3) มีความสามารถในการตรวจสอบและจัดทำรายงานการตรวจสอบ
- (4) มีความสามารถในการติดต่อกับผู้ที่ถูกตรวจสอบและฝ่ายบริหารระดับสูง
- (5) มีความสามารถในการตรวจสอบสาเหตุ ข้อสรุป และเขียนรายงานวิจารณ์ในทางสร้างสรรค์
- (6) มีความเข้าใจในการปฏิบัติงานด้านคอมพิวเตอร์ และการควบคุมภายในของระบบคอมพิวเตอร์
- (7) มีความรู้เชี่ยวชาญเกี่ยวกับการตรวจสอบ ตลอดจนเทคนิคในการตรวจสอบ
- (8) มีความรู้ทางวิชาการ (Technology) ด้านการปฏิบัติข้อมูล (ดูรายการแนบ)

องค์กรควรมีแผนฝึกอบรมแก่ผู้ตรวจสอบอย่างเพียงพอ เพื่อให้ทันกับความเจริญทางด้านคอมพิวเตอร์

มีการฝึกอบรมตามหลักสูตรของผู้ผลิตคอมพิวเตอร์ ผู้จำหน่ายโปรแกรมสำเร็จรูปที่ใช้ในการตรวจสอบและในมหาวิทยาลัย

4. ความเป็นอิสระของผู้ตรวจสอบ

ผู้ตรวจสอบภายในควรมีสายการบังคับบัญชาขึ้นตรงต่อคณะกรรมการบริหารองค์กร หรือคณะกรรมการตรวจสอบ คณะกรรมการองค์กรจะต้องมอบอำนาจให้ผู้ตรวจสอบอย่างเพียงพอ เพื่อให้สามารถตรวจสอบข้อมูลและการปฏิบัติงานได้ทุกชนิด รวมทั้งการแก้ไขข้อบกพร่องที่ตรวจพบได้ตามความเหมาะสม การรายงานผลการตรวจสอบให้คณะกรรมการบริหารองค์กรทราบโดยตรงจะช่วยให้คณะกรรมการบริหารรับผิดชอบดูแลการตรวจสอบได้สมบูรณ์ยิ่งขึ้น

5. คู่มือการตรวจสอบภายใน

ฝ่ายตรวจสอบภายในขององค์กรควรจัดทำคู่มือการตรวจสอบ เสนอให้คณะกรรมการการบริหารหรือผู้รับผิดชอบขององค์กรพิจารณาเกี่ยวกับมาตรฐานและวิธีการตรวจสอบ ก่อนที่จะนำมาใช้เป็นมาตรฐานในการตรวจสอบและฝึกอบรมผู้ตรวจสอบต่อไป คู่มือตรวจสอบควรระบุนโยบาย มาตรฐานและวิธีการตรวจสอบอย่างน้อย ในเรื่อง ต่อไปนี้

- (1) งานหรือหน้าที่ในการตรวจสอบ
- (2) ความถี่หรือระยะเวลาที่เข้าตรวจสอบ
- (3) วิธีการตรวจสอบงานประมวลผลที่สำคัญโดยละเอียด
- (4) วิธีการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ
- (5) มาตรฐานของกระดาษทำการ
- (6) มาตรฐานการรายงานและติดตามผลการตรวจสอบ
- (7) มาตรฐานของ Audit software (ได้แก่ เอกสารเกี่ยวกับ Software ที่นำมาใช้ การใช้ Software และการจัดซื้อ Software)
- (8) แนวการตรวจสอบระบบงานที่จะนำคอมพิวเตอร์ ซึ่งอยู่ระหว่างการพัฒนา

คู่มือดังกล่าวควรมีการปรับปรุงแก้ไข เพื่อให้สอดคล้องกับวิธีการตรวจสอบที่เปลี่ยนแปลงไป เนื่องจากการเปลี่ยนแปลงของเขตการตรวจสอบหรือระบบการปฏิบัติข้อมูลที่เปลี่ยนแปลงไปจากเดิม

6. การจัดทำเอกสารและรายงานการตรวจสอบ

(Documenting and Reporting Audit work)

ในคู่มือการตรวจสอบ ควรกำหนดมาตรฐานในการจัดทำกระดาษทำการและรายงานตรวจสอบมาตรฐานในการจัดทำกระดาษทำการ ควรประกอบด้วย :-

- (1) วิธีการปฏิบัติงานตรวจสอบ
- (2) วิธีการปฏิบัติงาน การบริหารงาน และควบคุมโปรแกรมของศูนย์คอมพิวเตอร์
- (3) รายละเอียดเกี่ยวกับ Hardware และระบบงานที่ตรวจสอบ
- (4) ลักษณะและขอบเขตของการทดสอบ
- (5) ผลการทดสอบ

การสรุปสิ่งที่ตรวจพบให้ฝ่ายบริหารทราบ ควรเป็นทางการโดยมีแนวปฏิบัติ ดังนี้

- (1) สรุปประเด็นสำคัญที่ตรวจพบเพื่อแจ้งให้ผู้บริหารตามสายงานทราบก่อนแล้วเขียนรายงานเสนอฝ่ายบริหารระดับสูงและคณะกรรมการบริหารขององค์กรต่อไป
- (2) ขอบกพร่องในการควบคุมที่สำคัญที่ตรวจพบและปัญหาสำคัญที่ยังไม่มีข้อยุติควรให้ผู้ตรวจสอบอาวุโสยกขึ้นปรึกษาคณะกรรมการบริหารขององค์กร
- (3) การเขียนรายงาน ควรใช้สำนวนที่สละสลวย ข้อสังเกตที่สำคัญควรเขียนให้รวบรัด มีข้อเท็จจริงและข้อเสนอแนะแก้ไข

- (4) ในรายงานการตรวจสอบ ควรแสดงเหตุผลในการเปลี่ยนแปลงวิธีการตรวจสอบที่ต่างไปจากการตรวจสอบครั้งก่อน
- (5) ข้อวิจารณ์ (criticisms) และข้อสังเกตต่างๆ (observations) ที่ระบุในรายงานการตรวจสอบ ควรมีเอกสารกระดาษาทำการสนับสนุนอย่างเพียงพอ
- (6) ควรให้เจ้าหน้าที่บริหารตามสายงานตอบชี้แจงข้อสังเกตต่างๆ ตามรายงานมาในเวลาอันควร
- (7) ผู้ตรวจสอบภายในต้องติดตามผลตามข้อสังเกตที่ระบุไว้ดังกล่าว เพื่อให้แน่ใจว่า ได้มีการแก้ไขให้ถูกต้องแล้ว หรือคณะกรรมการบริหารองค์กรได้ยอมรับความเสี่ยงภัยที่อาจเกิดขึ้น โดยไม่ทำการแก้ไขตามข้อสังเกตในรายงาน

รายงานสรุปผลการตรวจสอบ (Reporting Conclusions)

เมื่อการตรวจสอบเสร็จสิ้นลง ผู้ตรวจสอบควรสรุปผลการตรวจสอบตามข้อเท็จจริงและเอกสารต่าง ๆ ที่ตรวจสอบพบแยกตามความสำคัญ เพื่อมิให้รายงานการตรวจสอบสับสนไร้สาระ ซึ่งอาจทำให้คณะกรรมการบริหารองค์กรและฝ่ายบริหารระดับสูงมองไม่เห็นคุณค่าของรายงานดังกล่าวได้

รายงานการตรวจสอบจะแสดงข้อมูลที่เป็นประโยชน์ต่อฝ่ายที่ถูกตรวจสอบซึ่งมีหน้าที่รับผิดชอบช่วยให้สามารถประเมินผลการปฏิบัติงานของศูนย์ประมวลผลได้ ในรายงานการตรวจสอบไม่ควรระบุเพียงเรื่องที่ชี้ให้เห็นถึงการปฏิบัติงานที่ไม่ถูกต้องหรือความหละหลวมในการควบคุมงานประจำวันเท่านั้น แต่ควรรายงานให้ทราบถึงสภาพอันไม่เหมาะสมต่าง ๆ ที่ตรวจพบพร้อมทั้งแนะนำวิธีการเพื่อแก้ไขหรือปรับปรุงให้ถูกต้องด้วย การจัดทำรายงานการตรวจสอบควรรวดเร็วและทันเวลา โดยสรุปข้อเท็จจริงและชี้ให้เห็นถึงสภาพการปฏิบัติงานที่น่าสังเกต เนื้อหาของรายงานควรเขียนเป็นแนวสร้างสรรค์ ถูกต้อง และชัดเจน มีเหตุผลเพื่อให้ฝ่ายบริหารใช้เป็นแนวทางตัดสินใจ

นอกจากนี้ ผู้ตรวจสอบควรมีความสามารถในการติดต่อสนทนา เช่นเดียวกับการเขียนรายงาน เพื่อชี้แจงข้อเท็จจริงที่ตรวจพบ และเข้าใจปัญหาในระหว่างที่ทำการตรวจสอบ

7. การติดตามผลการตรวจสอบ (Audit Follow-up)

การติดตามผลการตรวจสอบว่า ฝ่ายบริหารได้ปฏิบัติตามข้อแนะนำต่าง ๆ ตามรายงานการตรวจสอบได้รวดเร็วและได้ผลเพียงใดนั้น ย่อมเป็นเครื่องชี้ให้เห็นถึงประสิทธิภาพในการตรวจสอบได้อย่างประการหนึ่ง ฝ่ายตรวจสอบควรกำหนดรายละเอียดวิธีการในการติดตามผล ไว้ในคู่มือตรวจสอบเพื่อเป็นแนวทางในการติดตามผลข้อแนะนำต่อไป การติดตามผลการตรวจสอบสามารถทำได้ โดย

- (1) ให้เจ้าหน้าที่ตรวจสอบไปตรวจสอบติดตามผลในภายหลัง
- (2) กำหนดให้ทำหนังสือรายงาน เมื่อได้ทำการแก้ไขตามข้อแนะนำ
- (3) พิจารณารายงานการแก้ไข แล้วนำเสนอคณะกรรมการบริหารขององค์กร

ส่วนข้อบกพร่องสำคัญ ๆ ที่พบระหว่างตรวจสอบ ผู้ตรวจสอบควรติดตามผลขณะนั้นได้เลย เพื่อให้แน่ใจว่าได้มีการแก้ไขเป็นที่น่าพอใจแล้ว หากไม่มีการปฏิบัติตามข้อเสนอแนะแล้วข้อบกพร่องนั้นยังคงมีอยู่ ควรแจ้งไว้ในรายงานการติดตามผล แล้วเสนอให้คณะกรรมการบริหารองค์กรทราบต่อไป

การติดตามผลการตรวจสอบจะช่วยให้การตรวจสอบได้ผลดี แต่ไม่ควรจะเร่งดำเนินการให้เร็วจนเกินไปจนกว่าจะแน่ใจว่า เทคนิคการติดตามผลที่ใช้ได้ผล

8. ความรับผิดชอบของผู้สอบบัญชี

หน้าที่ความรับผิดชอบ ควรจะกำหนดให้ชัดเจน โดยทำเป็นหนังสือเสนอคณะกรรมการบริหารองค์กร และฝ่ายจัดการระดับสูงให้ทราบก่อนที่ผู้สอบบัญชีจะเริ่มปฏิบัติงานตรวจสอบ โดยระบุขอบเขตในการตรวจสอบ ระยะเวลาที่ใช้ในการตรวจสอบ และเวลาที่คาดว่าจะส่งรายงานได้ ควรสรุปเรื่องสำคัญ ๆ พร้อมทั้งแนบรายละเอียดในการตรวจสอบไว้ทุกเรื่อง ประวัติของผู้ตรวจสอบที่เกี่ยวข้อง และการเปิดเผยข้อมูลในรายงานการตรวจสอบ นอกจากนี้อาจจะระบุวิธีการตรวจสอบที่ไม่นำมาใช้ เช่น การยืนยันยอดลูกหนี้หรือเงินฝาก และอาจจะระบุไว้ด้วยว่าผู้สอบบัญชีจะแสดงความเห็นต่อการเงินขององค์กรหรือไม่

ผู้สอบบัญชีควรสอบทานวิธีการควบคุมภายในด้านคอมพิวเตอร์ โดยถือเป็นส่วนหนึ่งของการประเมินผลระบบการควบคุมภายในทางการบัญชีทั้งหมด ดังนี้

- (1) ผู้สอบบัญชีต้องสรุปความเห็นเกี่ยวกับวิธีการควบคุมด้านบัญชีที่ใช้คอมพิวเตอร์ในการประมวลผล และกำหนดขอบเขตการทดสอบที่จำเป็น
- (2) เมื่อผู้สอบบัญชีเห็นว่า การควบคุมด้านบัญชีที่ใช้คอมพิวเตอร์ในการประมวลผลมีจุดอ่อนโดยปราศจากข้อสงสัย ผู้สอบบัญชีจะต้องปรับผลกระทบของจุดอ่อนดังกล่าวที่มีต่อการเงินที่ตรวจสอบ และวิธีการตรวจสอบอื่น เพื่อให้บรรลุวัตถุประสงค์ของการตรวจสอบ
- (3) หากผู้สอบบัญชีไม่ให้ความเห็นเกี่ยวกับวิธีการควบคุมด้านบัญชีที่ใช้คอมพิวเตอร์ในการประมวลผลให้กล่าวไว้ในรายงานการตรวจด้วย

โดยปกติผู้สอบบัญชีต้องตรวจสอบการควบคุมภายในทั้งในด้าน General Controls และในด้าน Application controls ซึ่งมีผลกระทบต่อการบันทึกและการป้องกันดูแลรักษาทรัพย์สินตลอดจนความถูกต้องของการเงิน

General Controls ได้แก่ การควบคุมเกี่ยวกับการจัดองค์กร การปฏิบัติ วิธีการจัดทำเอกสาร การใช้อุปกรณ์และแฟ้มข้อมูล รวมทั้งการควบคุมอื่น ๆ ที่มีผลกระทบต่อการปฏิบัติงานด้านคอมพิวเตอร์

Application controls ได้แก่ วิธีการควบคุมที่ใช้กับงานใดงานหนึ่งโดยเฉพาะเพื่อให้แน่ใจว่าการบันทึกข้อมูล การประมวลผล และการรายงาน ได้กระทำโดยถูกต้อง

ในระหว่างที่ผู้สอบบัญชีตรวจสอบระบบการควบคุมภายในทางการบัญชีควรพิจารณาถึงขอบเขตการนำเอาคอมพิวเตอร์ไปใช้ปฏิบัติงานด้านการบัญชีที่สำคัญ ๆ ทุกงานเพื่อกำหนดขอบเขตในการตรวจสอบการควบคุมภายในด้านคอมพิวเตอร์ที่จำเป็น

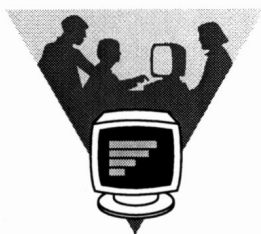
ผู้สอบบัญชีแต่ละคนจะมีวิธีการศึกษาและประเมินผลการควบคุมด้านคอมพิวเตอร์แตกต่างกัน ส่วนใหญ่จะใช้แบบสอบถาม (Questionnaire) หรือ Work program เป็นเอกสารหลักฐานในการสอบทานวิธีการควบคุมด้านคอมพิวเตอร์ทั้งแบบ General และ Application Controls ในเรื่องต่อไปนี้

- (1) การจัดรูปองค์กร (organization) เกี่ยวกับอุปกรณ์ที่ใช้ร่วมกับคอมพิวเตอร์ (equipment) และ Software ที่ใช้ในการประมวลผล
- (2) การควบคุมข้อมูลที่ได้จากการประมวลผลของหน่วยงานที่ใช้ข้อมูล
- (3) เอกสารแสดงรายละเอียดเกี่ยวกับโปรแกรมและคู่มือปฏิบัติงาน
- (4) การควบคุมการประมวลผล
- (5) การรักษาความปลอดภัย
- (6) การตรวจสอบภายใน

9. การตรวจสอบกิจการที่รับจ้างประมวลผล

ผู้ตรวจสอบภายในขององค์กรจำเป็นต้องตรวจสอบการปฏิบัติงานของกิจการที่องค์กรว่าจ้างประมวลผลด้วย ผู้ตรวจสอบดังกล่าวทำการตรวจสอบในเรื่องคล้ายกันเป็นส่วนใหญ่ อย่างไรก็ตาม วัตถุประสงค์ ขอบเขต และวิธีการตรวจสอบทั้ง 2 ประเภท จะแตกต่างกัน

การตรวจสอบกิจการที่รับจ้างประมวลผลควรกระทำทุกด้าน เช่นเดียวกับการตรวจสอบศูนย์ประมวลผลขององค์กรเอง โดยพิจารณาความเพียงพอของการควบคุมในทุก ๆ ด้าน รวมทั้งการปฏิบัติงานในห้องคอมพิวเตอร์ ระบบงานและโปรแกรม ตลอดจนการควบคุมข้อมูลที่ป้อนเข้าคอมพิวเตอร์ และข้อมูลที่ได้จากการประมวลผลที่จะนำไปใช้



12

**เทคนิคการตรวจสอบ
คอมพิวเตอร์ในระบบที่ทันสมัย**

เทคนิคการตรวจสอบคอมพิวเตอร์ในระบบที่ทันสมัย (Advanced EDP Audit Techniques)

ในระบบคอมพิวเตอร์ที่ทันสมัย เช่น on-line realtime ระบบ database และ distributive processing เป็นต้น การประเมินระบบงานจำเป็นต้องใช้ผู้ตรวจสอบที่มีความรู้ความชำนาญสูง และเคยผ่านงานตรวจสอบด้านคอมพิวเตอร์มาพอสมควร นอกจากนี้ ยังสิ้นเปลืองค่าใช้จ่ายสูงและใช้เวลาตรวจสอบมาก แต่จำเป็นต้องใช้เทคนิคต่าง ๆ เข้าช่วยตรวจสอบเนื่องจากการประมวลผลในระบบใหม่จะทำให้ข้อมูลเปลี่ยนแปลงอยู่ตลอดเวลา การตรวจสอบแบบเก่าที่ใช้วิธี snapshot โดยการ dump ข้อมูลออกมาตรวจสอบทีละครั้งในระหว่างการประมวลผลย่อมไร้ผล สำหรับวิธีการตรวจสอบแนวใหม่ที่จะกล่าวต่อไปนี้เป็นเพียงหลักการย่อ ๆ ที่นิยมใช้กันดังนี้

1. Integrated test facility

เป็นการทดสอบข้อมูลในระหว่างการประมวลผลจริง ผู้ตรวจสอบจะสร้างข้อมูลสำหรับการตรวจสอบซึ่งมีลักษณะข้อมูลจริงของหน่วยงานที่ใช้ข้อมูล แล้วป้อนเข้าคอมพิวเตอร์ให้ประมวลผลไปกับข้อมูลจริง ต่อจากนั้นจึงนำผลลัพธ์ที่ได้จากการประมวลผลเปรียบเทียบกับผลลัพธ์ที่ผู้ตรวจสอบคำนวณไว้ล่วงหน้า แต่การใช้วิธีนี้จะต้องระมัดระวังในการแยกบัญชีและยอดรวมของข้อมูลที่ทดสอบเป็นพิเศษ เพื่อหลีกเลี่ยงความสับสนที่อาจทำให้ผู้ใช้รายงานเข้าใจผิดคิดว่า มีการบันทึกสินทรัพย์สูงกว่าความเป็นจริง นอกจากนี้ธนาคารบางแห่งยังไม่ยอมรับวิธีการนี้

2. Simulation

เป็นการพิสูจน์ความถูกต้องของข้อมูลโดยอิสระแยกต่างหากจากการประมวลผลจริง โดยใช้โปรแกรมอีกชุดหนึ่งของผู้ตรวจสอบ ซึ่งมีลักษณะการประมวลผลเหมือนกับโปรแกรมใช้งาน เพื่อเลียนแบบการประมวลผลและใช้ข้อมูลจริงแล้วนำผลลัพธ์เปรียบเทียบกับการประมวลผลจริง

3. Audit logging

คือ การบันทึกการปฏิบัติงานของพนักงานที่เกี่ยวข้องกับการประมวลผล เพื่อใช้เป็นข้อมูลสำหรับตรวจสอบในเรื่องที่เกี่ยวกับการใช้แฟ้มข้อมูล รวมทั้งการป้อนข้อมูลผ่านทางเครื่อง Terminal และข้อมูลอ้างอิงเกี่ยวกับตัวผู้ใช้เครื่อง Terminal

4. Parallel operations

เป็นการสอบทานความถูกต้องของโปรแกรมใหม่ ๆ ที่จะนำมาใช้งานหรือโปรแกรมที่ถูกปรับปรุงแก้ไขใหม่ โดยนำโปรแกรมใหม่นี้ไปประมวลผลด้วยข้อมูลจริง ในขณะเดียวกันก็ให้ปฏิบัติงานที่จะใช้โปรแกรมใหม่ทำแทนไปตามเดิมควบคู่กันไปก่อนหากเป็นการแก้ไขโปรแกรมใหม่เก่าประมวลผลด้วย เพื่อนำผลมาเปรียบเทียบหาข้อแตกต่างที่เป็นจุดบกพร่องของโปรแกรมใหม่ โดยปกติผู้เขียนโปรแกรมและผู้วิเคราะห์ระบบงานจะใช้วิธีดังกล่าว ทดสอบความถูกต้องของโปรแกรมอยู่แล้ว แต่ผู้ตรวจสอบจำเป็นต้องทดสอบให้แน่ใจอีกครั้ง

5. Base case system operation

คือ การใช้ข้อมูลที่ทำขึ้นสำหรับทดสอบโปรแกรมใหม่ที่จะนำมาใช้งานเพื่อศึกษาการทำงานของโปรแกรมทุกขั้นตอนโดยละเอียดเป็นการสอบทานความถูกต้องในการประมวลผล โดยนำผลการประมวลผลทุกขั้นตอนเปรียบเทียบกับผลลัพธ์ที่คำนวณไว้ล่วงหน้า

6. Embedded audit data collecting

คือ การใช้โปรแกรมย่อยที่ทำหน้าที่ตรวจสอบ (audit subroutine) เก็บไว้ใน software ร่วมกับโปรแกรมงานอยู่ตลอดเวลาที่คัดเลือกข้อมูลที่ป้อนเข้าคอมพิวเตอร์และข้อมูลที่ได้จากการประมวลผลที่ควรนำมาตรวจสอบ

7. Transaction tagging

เป็นวิธีการตรวจสอบโดยการเติมรหัสพิเศษ (Special code) ลงในท้าย record ที่บันทึกข้อมูลที่ป้อนเข้าสู่ระบบคอมพิวเตอร์ เพื่อให้ทำหน้าที่ตรวจสอบการประมวลผลในจุดที่สำคัญ

8. Extended records

คือ การขยาย record ที่บันทึกข้อมูลเพื่อเพิ่ม (Control field) สำหรับใส่ข้อมูลที่ใช้ในการควบคุมการประมวลผลเรียกว่า spacial field หรือ trailer record สามารถใช้ร่วมกับข้อมูลอื่นที่ป้อนเข้าคอมพิวเตอร์ได้ทุกงานเพื่อประโยชน์ในการตรวจสอบ เช่น

- (8.1) ทำ hash totals ซึ่งเป็นการรวมยอดข้อมูล เพื่อตรวจสอบความถูกต้องของข้อมูลที่ได้จากการประมวลผลโดยโปรแกรมที่สำคัญ และมีผลกระทบต่องานทั้งระบบ
- (8.2) คัดเลือกข้อมูลบางชนิด เพื่อประโยชน์ในการวิเคราะห์ประวัติแฟ้มข้อมูล
- (8.3) หาผลลัพธ์เพื่อนำไปคำนวณเปรียบเทียบกับข้อมูลที่ได้จากการประมวลผลในภายหลัง

9. การเข้าร่วมพัฒนาและทดสอบงานที่นำเข้าคอมพิวเตอร์

(Audit Participation in application Development and testing)

ผู้ตรวจสอบควรเข้าร่วมพัฒนาระบบงาน เพื่อให้การควบคุมภายในระบบงานมีประสิทธิภาพตั้งแต่เริ่มแรก โดยศึกษาความเหมาะสมของการควบคุมภายในและข้อมูลที่ควรเหลือไว้สำหรับการตรวจสอบ (Audit Trails) ในแต่ละงาน เพื่อเสนอแนะวิธีการควบคุมที่ดีต่อฝ่ายบริหารและเมื่อผู้ออกแบบระบบงานออกแบบเสร็จเรียบร้อยแล้ว ผู้ตรวจสอบควรเข้าร่วมจัดทำข้อมูลที่ใช้ในการทดสอบ และประเมินผลของการทดสอบก่อนนำระบบงานใหม่ไปใช้ โดย ผู้ตรวจสอบด้านคอมพิวเตอร์ ควรทราบเกี่ยวกับสาเหตุของข้อผิดพลาด (sources of error) วิธีการทดสอบความถูกต้องของข้อมูล (Tests for valid data) และองค์ประกอบของยอดรวม (Control total composition)

13

**ความรู้ด้านคอมพิวเตอร์
กับผู้ตรวจสอบ**

ความรู้ด้านคอมพิวเตอร์กับผู้ตรวจสอบ

ผู้ตรวจสอบด้านคอมพิวเตอร์ควรมีความรู้มาตรฐานในเรื่องต่อไปนี้

1. การตรวจสอบโดยผู้ตรวจสอบภายใน

- 1.1 การตรวจสอบการประมวลผลข้อมูล – วิธีปฏิบัติ (Data Processing Auditing – Operations)
- 1.2 การตรวจสอบระบบงาน (Systems Auditing)
- 1.3 คู่มือการตรวจสอบการประมวลผลด้วยคอมพิวเตอร์ (EDP Audit Manual)
- 1.4 รายงานการตรวจสอบและกระดาษทำการ (Audit Reports and Work Papers)
- 1.5 การฝึกอบรมการตรวจสอบการประมวลผลข้อมูล (EDP Audit Training)
- 1.6 โปรแกรมคอมพิวเตอร์ที่ใช้ในงานตรวจสอบ – วิธีใช้และการควบคุม (Audit Automated Systems)
- 1.7 การตรวจสอบข้อมูลแบบพิสูจน์ยอด – ระบบอัตโนมัติ (Reconciliation Auditing – Automated Systems)
- 1.8 การควบคุมข้อมูลนำเข้าและผลลัพธ์ (Input/Output Control)
- 1.9 เทคนิคการตรวจสอบที่ทันสมัย * (Advanced Audit Techniques)
- 1.10 การตรวจสอบโดยบุคคลที่สามหรือสถาบันที่ชำนาญเป็นพิเศษ (Third part Reviews คุณวุฒิและคุณสมบัติของผู้ตรวจสอบด้านคอมพิวเตอร์ (Edp Auditor Qualifications)
- 1.11 การตรวจสอบก่อนหน้าและหลังจากที่ใช้ระบบงานใหม่ไประยะหนึ่ง (Pre–Post Implementation Auditing)

2. การจัดองค์การด้านคอมพิวเตอร์

- 2.1 คำบรรยายลักษณะงาน – การปฏิบัติงานประมวลผลข้อมูลและการตรวจสอบ (Job Descriptions – D.P.Operations and Audit)
- 2.2 ลักษณะการจัดองค์การและการรายงาน (Organization and Reporting Structure)
- 2.3 การวางแผนงานและบริหารงานตามนโยบาย (Planning and Policy Administration)
- 2.4 ประวัติของเจ้าหน้าที่ระดับบริหาร (Resumes of Key Employees)
- 2.5 การวางแผนการประมวลผลในกรณีเร่งด่วน (Emergency Procedures Planning)
- 2.6 การวิเคราะห์อัตรากำลังคน (MANPOWER – ANALYSIS)
- 2.7 หน่วยงานที่ทำหน้าที่ศึกษาค้นคว้าและพัฒนาการใช้คอมพิวเตอร์ (Research and Development Functions)

* เทคนิคการตรวจสอบที่ทันสมัย เช่น Integrated test facility, Simulation,

Audit Logging, Base case system evaluation,

Embedded audit data collection, Transaction

3. มาตรฐานของระบบงานและการจัดทำเอกสารสนับสนุน

- 3.1 ภาษาของโปรแกรมสั่งงาน (Programming Languages)
- 3.2 การบริหารงานจัดทำโปรแกรมสั่งงาน (Programming Administration)
- 3.3 การวิเคราะห์และออกแบบระบบงาน (Systems Analysis/Design)
- 3.4 ขั้นตอนในการพัฒนาระบบงาน (Systems Procedures Development)
- 3.5 การบริหารงานในการวางแผนพัฒนาระบบงาน (System Planning Administration)
- 3.6 การศึกษาถึงความเหมาะสม (Feasibility Studies)
- 3.7 การวิเคราะห์ด้านเครื่องมือและอุปกรณ์ (Equipment Analysis)
- 3.8 การวิเคราะห์โปรแกรมสั่งงาน (Software Analysis)
- 3.9 การควบคุมข้อมูลในแฟ้มและรายงานผลลัพธ์ (Record and Reprot controls)
- 3.10 มาตรฐานการจัดทำโปรแกรมคำสั่งงาน (Programming Standards)
- 3.11 มาตรฐานของระบบงานและการคัดเลือกโปรแกรมสั่งงาน (Systems Standards/Software Selection and Standards)
- 3.12 มาตรฐานของเอกสารสนับสนุนระบบงานและการวิเคราะห์ระบบงาน (Documentation Standards and Analysis)
- 3.13 การบริหารงานด้านการจัดเก็บเอกสารสนับสนุนและการควบคุม (Documentation Library Administration and Control)
- 3.14 การจัดทำผังระบบงาน (Flow Charting)
- 3.15 การทบทวนระบบงานของผู้ใช้ข้อมูล (Application Review)
- 3.16 วิธีการทดสอบระบบงาน (Testing Procedures)
- 3.17 คู่มือปฏิบัติงานของผู้ใช้ข้อมูล (User Manuals)
- 3.18 การควบคุมโดยโปรแกรม (Programmed Control)
- 3.19 การตรวจสอบและแก้ไขโปรแกรมและการควบคุม (program Patching/control)
- 3.20 ขั้นตอนในการนำระบบงานใหม่ออกมาใช้ (Implementation Procedures–New Systems)
- 3.21 การป้องกันและรักษาโปรแกรม (Program Security)
- 3.22 วิธีการทำนุบำรุงรักษาเอกสารสนับสนุนระบบงาน (Documentation Maintenance Procedures)

4. การปฏิบัติงานคอมพิวเตอร์

- 4.1 การจัดลำดับความสำคัญของงานประมวผลและการกำหนดตารางการทำงานของเครื่องคอมพิวเตอร์ (Job Control/Scheduling)
- 4.2 การควบคุมข้อมูลนำเข้าและผลลัพธ์ (Input/Output control)
- 4.3 ระบบคอมพิวเตอร์และเครื่องมืออุปกรณ์ (Computer System/Equipment)
- 4.4 ระบบควบคุมการทำงานของคอมพิวเตอร์ (Operating System)

- 4.5 การบริหารงานประมวลผลข้อมูลด้วยคอมพิวเตอร์ (Data Processing Operations Administration)
- 4.6 การใช้เครื่องมือควบคุมการใช้เครื่องคอมพิวเตอร์ (Console Operation)
- 4.7 การใช้เทปและจานแม่เหล็ก (Tape/Disk Operation)
- 4.8 การใช้ MICR และ ORC (MICR/ORC Operation)
- 4.9 การพิสูจน์ยอดและการลงรหัส (Proof/Encoding)
- 4.10 การจัดเก็บและควบคุมแฟ้มข้อมูล (File Library Function)
- 4.11 การใช้รายงานแบบไมโครฟิล์ม (COM Operation)
- 4.12 สัญญาเช่าเครื่องและอุปกรณ์คอมพิวเตอร์ (Computer Equipment Leases)
- 4.13 การประกันภัยเครื่องและอุปกรณ์คอมพิวเตอร์ (Computer Equipment Insurance)
- 4.14 คู่มือปฏิบัติงานคอมพิวเตอร์ (Operation Procedures Manual)
- 4.15 เครื่องและอุปกรณ์คอมพิวเตอร์ชุดสำรอง (Equipment Back up)
- 4.16 แฟ้มข้อมูลสำรอง (file Back up)
- 4.17 โปรแกรมสำรอง (Program Back up)
- 4.18 การทำนุบำรุงเพื่อป้องกันความเสียหาย (Preventative Maintenance)
- 4.19 การจัดเก็บและควบคุมโปรแกรม (Program Library Function)
- 4.20 การประมวลผลร่วมกันระหว่างคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป (Multiprocessing)
- 4.21 แฟ้มบันทึกข้อมูลเกี่ยวกับการใช้เครื่องและการติดต่อระหว่างส่วนต่าง ๆ ของระบบคอมพิวเตอร์ (System Activity Logs)
- 4.22 ระบบการควบคุมและจัดเก็บเอกสารสนับสนุน, แฟ้มข้อมูลและโปรแกรม (Librarian Systems)
- 4.23 การรักษาความสะอาดภายในห้องคอมพิวเตอร์ (Computer Room Housekeeping)

5. ความถูกต้องและสมบูรณ์ของข้อมูล

- 5.1 การจัดองค์การและการแบ่งแยกหน้าที่และความรับผิดชอบ (Organization/Separation on duties)
- 5.2 การควบคุมความถูกต้องของข้อมูลโดยวิธีพิสูจน์ยอด (Reconciliation Procedures)
- 5.3 ระบบเตือนภัย - การตรวจจับความร้อนและควันไฟ (Alarm Systems - Smoke and Heat Detection)
- 5.4 การป้องกันข้อมูลที่เก็บไว้ในแฟ้ม (Record Protection)
- 5.5 การควบคุมงานรักษาความปลอดภัย (Security Control)
- 5.6 ขั้นตอนในการปฏิบัติงานฉุกเฉินและการแก้ไขให้กลับคืนสู่สภาพปกติ (Emergency Procedures/ Recovery Procedures)
- 5.7 การรักษาความปลอดภัยแฟ้มข้อมูล (File Security)
- 5.8 วิธีการจัดเก็บและควบคุมแฟ้มข้อมูล (File Library Procedures)
- 5.9 การจัดตารางเวลาของงานที่ประมวลผล (Job Scheduling)
- 5.10 การจัดทำสลากปิดภายนอกและภายในแฟ้มข้อมูล (File Labeling)

- 5.11 การประกันภัยระบบคอมพิวเตอร์ – ค้ำครองภัยหลายประเภท (EDP Insurance – All Types)
- 5.12 ระบบดับเพลิงอัตโนมัติ (File Extinguisher Systems)

6. เทคนิคที่เกี่ยวกับคอมพิวเตอร์

- 6.1 ระบบหรือโปรแกรมควบคุมการทำงานของคอมพิวเตอร์ (Operating Systems)
- 6.2 โปรแกรมเอนกประสงค์ที่ผู้ผลิตให้มาพร้อมกับเครื่อง – การใช้และการควบคุม (Utility Programs – Use and control)
- 6.3 การจัดทำโปรแกรมควบคุมการทำงานของคอมพิวเตอร์ (System Programming)
- 6.4 เอกสารสนับสนุนระบบควบคุมการทำงานของคอมพิวเตอร์ (Operating Systems Documentation)
- 6.5 การรักษาความปลอดภัยโปรแกรมควบคุมการทำงานของคอมพิวเตอร์ (Operating Systems Security)
- 6.6 โปรแกรมควบคุมการสั่งการและประสานงานภายในระบบคอมพิวเตอร์ (Supervisor)
- 6.7 การจัดทำโปรแกรมคำสั่งระบบงานของผู้ใช้ข้อมูล (Application Programming)
- 6.8 การป้องกันการถ่ายทอดข้อมูลบางส่วนหรือทั้งหมดจากส่วนความจำ (Storage Dump Protection)
- 6.9 การเตรียมข้อมูลนำเข้าและการส่งข้อมูลเข้าไปประมวลผล (Input Preparation/Data Entry)
- 6.10 วิธีการประมวลผลข้อมูลที่ค้างการลงบัญชีและข้อมูลที่เครื่องไม่รับ (Unposted/Reject Item Processing)
- 6.11 การออกแบบระบบการจัดเก็บข้อมูลแบบ Data Base (Data Base Design)
- 6.12 วิธีการบันทึกหลักฐานยืนยันข้อมูลนำเข้าและผลลัพธ์ที่ได้จากการประมวลผล (Input/Output Logging Procedures)
- 6.13 การพิสูจน์ยอดรวมข้อมูล (Proof Operations)
- 6.14 วิธีการควบคุมข้อผิดพลาดและการปรับปรุงแก้ไข (Error and Adjustment Control Procedures)
- 6.15 การบันทึกข้อมูลลงเทปและจานแม่เหล็ก (Key-to-Tape and Key-to-Disk Operations)
- 6.16 วิธีการควบคุมความถูกต้องของข้อมูลและการควบคุม (Output Distribution and Control)
- 6.17 การพิสูจน์ยอดข้อมูลแบบรายกลุ่มและการควบคุม (Batch Proof-and Control)
- 6.18 วิธีการควบคุมภายในศูนย์คอมพิวเตอร์ (Data Center Control Procedures)
- 6.19 การควบคุมแฟ้มข้อมูล (Data File Control)
- 6.20 การสอบทานผลลัพธ์จากการประมวลผล (Output Review)

7. การรักษาความปลอดภัยเครื่องและอุปกรณ์คอมพิวเตอร์

- 7.1 สิ่งกีดขวางบริเวณอาคาร, สถานที่ตั้งอาคารคอมพิวเตอร์ และระบบการรักษาความปลอดภัย (Physical Barriers/Building Location and Security)
- 7.2 วิธีการบันทึกหลักฐานการเข้าและออกห้องคอมพิวเตอร์ (In/Out Logging Procedures)
- 7.3 สถานที่ตั้งห้องคอมพิวเตอร์, ผังการจัดห้อง และระบบการรักษาความปลอดภัย (Computer Room Location/Layout/Security)

- 7.4 หองมั่นคง, ตู้นิรภัย, เครื่องมือสำหรับเก็บข้อมูลและโปรแกรม และการรักษาความปลอดภัย (Vault/Safe/Storage Devices and Security)
- 7.5 อำนาจของเจ้าหน้าที่ผู้มีสิทธิใช้เครื่องและอุปกรณ์คอมพิวเตอร์ (Personnel Authorization)
- 7.6 การแบ่งแยกหน้าที่ - ผู้จัดทำโปรแกรมควบคุมการทำงานของคอมพิวเตอร์กับผู้จัดทำโปรแกรมคำสั่งระบบงานของผู้ใช้ข้อมูล (Separation of Duties System Programmers Versus Application Programmers)
- 7.7 ระบบการประมวลผลข้อมูลทันทีโดยอาศัยการสื่อสาร (On-Line Systems)
- 7.8 การควบคุมการใช้เทอร์มินอล (Terminal Control)
- 7.9 การควบคุมการรับส่งข้อมูลระหว่าง CPU และ Terminal (Transmission Control)
- 7.10 การตรวจสอบความถูกต้องข้อมูลโดยเครื่อง (Message Verification)
- 7.11 ระบบการประมวลผลตามเวลาที่เกิดขึ้นจริง (Real Time Systems)
- 7.12 การรับและส่งข้อมูลในสถานที่ที่ไกลจากศูนย์คอมพิวเตอร์ (Remote Job Entry)
- 7.13 การจัดทำโปรแกรมคำสั่งระบบงานที่ประมวลผลทันที (On-Line Programming)
- 7.14 การประมวลผลในระบบกระจายศูนย์ (Satellite Processing System)
- 7.15 การประมวลผลในระบบรวมศูนย์เพื่อแบ่งเบาภาระในการประมวลผล (Distributive Processing System)
- 7.16 ระบบการโอนเงินโดยอัตโนมัติ (EFTS - Electronic Fund Transfer System)
- 7.17 แฟ้มข้อมูลร่วม (CIF - Central Information System)

8. การใช้บริการด้านคอมพิวเตอร์จากบุคคลภายนอก

- 8.1 กฎหมายหรือข้อตกลงเกี่ยวกับการใช้บริการด้านคอมพิวเตอร์ (Applicable Laws, regulation, rulings)
- 8.2 การประกันภัยของผู้ใช้ข้อมูลและผู้ให้บริการคอมพิวเตอร์ (Insurance)
- 8.3 สัญญาระหว่างผู้ใช้ข้อมูลกับผู้ให้บริการคอมพิวเตอร์ (Service Contracts)
- 8.4 บริการด้านการบริหารคอมพิวเตอร์ (Facilities Management)
- 8.5 การประมวลผลร่วมกับบุคคลอื่นในเวลาเดียวกัน (Time Sharing)
- 8.6 ขั้นตอนการออกใบเสร็จเรียกเก็บค่าธรรมเนียมในการใช้บริการคอมพิวเตอร์ (Billing Procedures)
- 8.7 การวิเคราะห์ฐานะการเงินของผู้ให้บริการคอมพิวเตอร์ (Financial Statement Analysis)
- 8.8 บริการด้านจัดทำโปรแกรมสำเร็จ (Software Marketing)

14

ผู้บริหารกับคอมพิวเตอร์

ผู้บริหารกับคอมพิวเตอร์

1. ปัญหาของสถาบันการเงินและองค์กรต่าง ๆ ที่ใช้คอมพิวเตอร์

1.1 องค์กรไม่ให้ความสนใจเท่าที่ควร

ทั้ง ๆ ที่เป็นความประสงค์ขององค์กรที่จะใช้เครื่องมือที่มี Technology สูงและมีการพัฒนาในอัตราที่รวดเร็วมาก มีการมอบหมายงานต่อเนื่องกันลงไปเรื่อย ๆ จนกระทั่งขาดการพิจารณา โดยคณะกรรมการบริหารระดับสูง และในที่สุดเป็นงานที่ขึ้นกับการตัดสินใจของคน ๆ เดียว หรือเพียงไม่กี่คนแทนที่จะเป็นการตัดสินใจร่วมกันของคณะกรรมการ

1.2 วางโครงการไม่ดีและขาดความรัดกุมและการมองการณ์ไกลตั้งแต่เริ่มแรก

ระบบงานที่ซับซ้อนเกินไป หรือไม่เตรียมโครงการให้สอดคล้องกับความต้องการขององค์กรในระยะต่อ ๆ ไป ระบบงานเดิมจึงไม่อาจเข้ากับระบบงานใหม่ที่จะขยายใหญ่โตออกไปได้ ทำให้สิ้นเปลืองค่าใช้จ่ายสูงมากในการปรับปรุงระบบงานใหญ่ และรวมถึงการเปลี่ยนเครื่องมือให้เข้ากับระบบงานที่ขยายใหญ่โตขึ้น

1.3 พนักงานมีคุณสมบัติไม่เพียงพอ

การประมวลผลด้วยคอมพิวเตอร์เป็นงานที่จะต้องใช้พนักงานที่มีความชำนาญทางเทคนิคสูงได้รับการอบรมและฝึกฝนเป็นอย่างดี ฉลาด มีไหวพริบ มีความคิดสร้างสรรค์ และซื่อสัตย์

1.4 ขาดบุคลากรในระดับผู้อำนวยการให้เป็นไปตามแผนงาน

บางองค์กรมีผู้เชี่ยวชาญทางด้านคอมพิวเตอร์มาก แต่ก็ขาดประสบการณ์และความรู้เกี่ยวกับระบบงานองค์กรนั้น จึงไม่อาจประสานความรู้ทั้ง 2 ประเภทเข้าด้วยกันให้เกิดเป็นผลดีต่อองค์กรเท่าที่ควร จึงมีปัญหาทั้งในการพัฒนาระบบงานและการฝึกพนักงานให้เรียนรู้งาน เป็นเหตุให้เกิดการล่าช้าในการพัฒนาระบบงาน และเสียค่าใช้จ่ายสูง และเป็นสาเหตุส่วนหนึ่งที่ทำให้ผู้บริหารขององค์กรบางแห่งไม่แน่ใจในความสำเร็จหรือผลดีของการใช้คอมพิวเตอร์ในการประมวลงานขององค์กรนั้น ๆ

1.5 ขาดบุคลากรผู้มีความสามารถในการตรวจสอบงานด้านคอมพิวเตอร์

เป็นปัญหาสำคัญยิ่งในปัจจุบัน เพราะผู้ตรวจสอบงานด้านนี้ต้องการคุณสมบัติหลาย ๆ ประการในคน ๆ เดียวกัน จึงต้องใช้เวลาในการฝึกฝนและพัฒนาผู้ตรวจสอบประเภทนี้อยู่มาก

1.6 เกิดความไม่เข้าใจในความต้องการใช้ข้อมูลของฝ่ายบริหาร

ความสำเร็จของการประมวลด้านคอมพิวเตอร์ขึ้นอยู่กับความพอใจของผู้ใช้ข้อมูลในฝ่ายต่าง ๆ ที่เกี่ยวข้องกับการใช้งาน ฉะนั้น จึงขึ้นกับว่าองค์กรกำหนดให้ใครเป็นผู้ให้บริการ และควรเข้าใจความต้องการของผู้ใช้บริการ เพราะการให้ข้อมูลที่ถูกต้องแก่ผู้ใช้ที่ผิดประเภทก็เป็นปัญหากับองค์กรได้เช่นกัน

1.7 ขาดการวางแผนงานที่เหมาะสม

ศูนย์ประมวลผลและระบบงานด้านคอมพิวเตอร์ที่ประสบผลสำเร็จส่วนใหญ่ต้องอาศัย ทั้งด้านการวางแผนงานและการควบคุมตรวจสอบความถูกต้องของระบบงาน และการปรับปรุงตามความจำเป็น ถ้าปราศจากการวางแผนที่ดี การควบคุมก็ทำไม่ได้ผลเท่า ๆ กับการไม่มีการควบคุม การวางแผนก็ไร้ประโยชน์ นอกจากนี้ หากมีการเปลี่ยนแผนงานก็ทำให้เกิดการล่าช้าและเสียค่าใช้จ่ายเพิ่ม

1.8 ขาดผู้รับผิดชอบต่อโครงการ

การกำหนดบุคคลผู้รับผิดชอบโดยตรงต่อโครงการที่เกี่ยวข้อง ทั้งระบบและบุคคลผู้รับผิดชอบต่อการนำไปใช้ ทำให้ผู้บริหารสามารถมอบอำนาจได้โดยถูกต้อง หากไม่มีการกำหนดผู้รับผิดชอบในแต่ละด้านแล้ว จะขาดผู้ควบคุมให้การปฏิบัติงานดำเนินการต่อไปได้อย่างมีประสิทธิภาพ

1.9 ไม่ยอมยกเลิกโครงการ

เมื่อใดที่วิเคราะห์แล้วและพบว่าไม่ควรนำคอมพิวเตอร์มาใช้ในระบบงานใด ก็ควรยกเลิกโครงการนี้ทันที อย่าฝืนทำต่อไป เพราะการยกเลิกโครงการหลังเสร็จสิ้นขั้นตอนการพัฒนาระบบงานขั้นที่ 1 ซึ่งเป็นการกำหนดรายละเอียดของขั้นตอนต่าง ๆ ยังนับว่าจะได้ประโยชน์กว่าและประหยัดกว่าการทำการพัฒนาต่อไปแล้วใช้ไม่ได้

1.10 การควบคุมโครงการไม่ดีพอ

การควบคุมที่ดีจะทำให้องค์กรสามารถบรรลุเป้าหมายของแผนงานได้ การควบคุมจะเป็นเครื่องวัดความสำเร็จของแผนงาน ค้นพบสิ่งที่คลาดเคลื่อนไปจากแผนงาน และการสั่งการเพื่อแก้ไขข้อผิดพลาดเท่าที่จำเป็นได้

1.11 องค์กรขาดแผนงานด้านการฝึกอบรมพนักงาน

การให้การศึกษาด้านคอมพิวเตอร์แก่พนักงานทุกระดับเป็นสิ่งจำเป็นมาก ทั้งนี้เพราะโครงการที่นำคอมพิวเตอร์มาใช้งานขึ้นอยู่กับ การสนับสนุน และร่วมมือของพนักงานทุกระดับ อย่างไรก็ตาม การจัดทำคู่มือที่เกี่ยวข้องกับการปฏิบัติงานเป็นสิ่งที่สำคัญมาก ซึ่งจะต้องจัดทำให้เรียบร้อยก่อนการนำระบบงานใหม่มาใช้

1.12 เลือก Hardware และรูปแบบ Software ที่นำมาใช้งานไม่เหมาะสม

การตัดสินใจเลือกระบบคอมพิวเตอร์ระบบใดระบบหนึ่ง ที่จะให้ประโยชน์ตรงตามแผนงานในปัจจุบัน และสอดคล้องกับแผนงานในอนาคตเป็นสิ่งที่สำคัญมาก และจะมีผลกระทบถึงรูปแบบของโปรแกรมคำสั่งงานที่จะใช้ด้วย ดังนั้น องค์กรควรให้บุคคลซึ่งมีความชำนาญทางเทคนิคด้านคอมพิวเตอร์ และเข้าใจแผนงานและระบบงานขององค์กรดี เป็นผู้มีส่วนตัดสินใจด้วย

2. บทบาทของฝ่ายบริหารที่มีต่อคอมพิวเตอร์ และสาเหตุที่ผู้บริหารไม่ให้ความสำคัญต่อผู้ตรวจสอบด้านคอมพิวเตอร์

3.1 บทบาทของฝ่ายบริหารที่มีต่อคอมพิวเตอร์

- 3.1.1 ฝ่ายบริหารระดับสูงส่วนใหญ่มีความเข้าใจเกี่ยวกับคอมพิวเตอร์น้อยมาก แม้ในธนาคารบางแห่งที่ใช้คอมพิวเตอร์เอง ในต่างประเทศเองก็มีปัญหานี้ ทางธนาคารบางแห่งจัดให้มีการอบรมพนักงานบริหารระดับสูง แต่ก็ล้มเหลว เพราะผู้บริหารมักทนรับฟังคำบรรยายที่ฟังแล้วเกิดอาการง่วงนอน และมีความสับสนในเทคนิคทางด้านคอมพิวเตอร์จนจบ และมักอ้างว่ามีงานอื่นที่สำคัญกว่า
- 3.1.2 ฝ่ายบริหารมักโยนภาระความรับผิดชอบด้านคอมพิวเตอร์ไปให้ผู้จัดการฝ่ายคอมพิวเตอร์ และหวังให้ฝ่ายคอมพิวเตอร์เป็นผู้วางแผนและดำเนินการเอง
- 3.1.3 ผู้บริหารของหน่วยงานที่ใช้ข้อมูล (user) ไม่ตระหนักตามปกติแล้วตนต้องรับผิดชอบด้านการปฏิบัติงานและคุณภาพของข้อมูล
- 3.1.4 ผู้บริหารระดับสูงมักจะอนุมัติหรือไม่อนุมัติโครงการตั้งแต่เริ่มแรกเท่านั้น ไม่กำหนดแนวทางและคอยชี้นำต่อไป

3.2 สาเหตุที่ผู้บริหารไม่ให้ความสำคัญต่อผู้ตรวจสอบด้านคอมพิวเตอร์ คือ

- 3.2.1 ผู้บริหารไม่เข้าใจถึงระบบการทำงานของเครื่องคอมพิวเตอร์ จึงไม่ต้องการเกี่ยวข้องในเรื่องต่างๆ ที่เกี่ยวกับระบบคอมพิวเตอร์
- 3.2.2 ผู้บริหารมีความพอใจในระบบงานที่จัดทำขึ้นโดยพัฒนาระบบงาน และสามารถนำระบบงานนั้นไปใช้งานตามเป้าหมายที่วางไว้โดยไม่สนใจว่าระบบงานนั้นมีข้อบกพร่องหรือไม่
- 3.2.3 ผู้บริหารเชื่อมั่นในความรู้ ความสามารถของเจ้าหน้าที่ด้านคอมพิวเตอร์มากกว่าผู้ตรวจสอบด้านคอมพิวเตอร์ และไม่สนใจว่าระบบงานบางอย่างผู้พัฒนาระบบงานจะต้องมีความรู้ดีด้านอื่นด้วย เช่น ความรู้ด้านบัญชี เป็นต้น
- 3.2.4 ผู้บริหารองค์กรมีความเห็นอย่างคลาดเคลื่อนว่า หน้าที่ของผู้ตรวจสอบด้านคอมพิวเตอร์ เพียงเพื่อค้นหาการทุจริตที่เกิดจากการใช้คอมพิวเตอร์เท่านั้น โดยไม่คำนึงถึงวิธีการป้องกันความเสียหาย อันเนื่องมาจากการใช้ระบบคอมพิวเตอร์ในการประมวลผลไม่ถูกต้อง หรือเนื่องจากการละเลยขั้นตอนการปฏิบัติงานบางอย่าง ซึ่งก่อให้เกิดความเสียหายได้เช่นกัน

15

อุปสรรคเกี่ยวกับ
การใช้คอมพิวเตอร์

อุปสรรคเกี่ยวกับการใช้คอมพิวเตอร์

สรุปได้ 4 ประการ คือ

1. การดำเนินงานของสถาบันการเงินที่มีผลกระทบต่อการนำเอาคอมพิวเตอร์มาใช้
2. ความเชื่อที่ไม่ถูกต้องเกี่ยวกับคอมพิวเตอร์
3. ข้อกังวลของสถาบันการเงินเกี่ยวกับการใช้คอมพิวเตอร์
4. ปัญหาที่บรรดาศูนย์คอมพิวเตอร์ต่าง ๆ ส่วนใหญ่ประสบ

1. การดำเนินงานของสถาบันการเงินที่มีผลกระทบต่อการนำเอาคอมพิวเตอร์มาใช้

1.1 ด้านการบริหาร

- โดยมากมักจะเป็นการบริหารที่มอบอำนาจในการตัดสินใจไว้กับคนไม่กี่คน
- ผู้บริหารระดับสูงมักไม่มีเวลามาสนใจกับงานด้านคอมพิวเตอร์ ซึ่งนับวันจะมีความสำคัญ มากขึ้น
- ไม่ค่อยให้ความร่วมมือกันเต็มที่ในระหว่างหน่วยงานต่าง ๆ
- ขาดการพัฒนาทางด้านการบริหาร
- มีการมอบหมายหน้าที่และความรับผิดชอบ ๆ กันมากเกินไป
- มักจะเกิดความแตกแยกในระหว่างพวกหัวเก่า (Traditional group) กับพวกหัวก้าวหน้า (Pro-gressive group)

1.2 ด้านการจัดองค์การ

- การแบ่งแยกและมอบหมายหน้าที่ความรับผิดชอบไม่เหมาะสม เช่น ผู้ตรวจสอบภายในด้านคอมพิวเตอร์อยู่ภายใต้การบังคับบัญชาของหัวหน้าศูนย์คอมพิวเตอร์
- การติดต่อประสานงานภายในองค์กรมักล่าช้า
- มีปัญหาด้านการพัฒนาและการควบคุมบุคลากร เช่น มีงานด้านเอกสาร (Clerical work) และการตรวจสอบหลายขั้นตอนมากเกินไป
- การจัดเก็บเอกสารยากแก่การค้นหาและแก้ไขปรับปรุง เช่น Report ต่าง ๆ ที่ผู้ใช้มักจะเลยไม่เอาใจใส่ในการเก็บรักษา

1.3 ด้านการใช้คอมพิวเตอร์

- ใช้คอมพิวเตอร์ภายในขอบเขตที่จำกัด
- หาบุคลากรที่ดีด้านนี้ไม่ค่อยจะได้
- แนวโน้มในการพัฒนามาสู่ระบบคอมพิวเตอร์ในระยะแรกเป็นเพียงเปลี่ยนระบบงานที่ใช้อยู่ให้เป็นระบบที่ทำงานด้วยคอมพิวเตอร์ ทำให้มีขั้นตอนมากมาย ทั้ง ๆ ที่บางขั้นตอนอาจใช้ระบบคอมพิวเตอร์ทำแทนได้ดีกว่า หากเข้าใจการทำงานของเครื่องคอมพิวเตอร์ที่แท้จริง

2. ความเชื่อที่ไม่ถูกต้องเกี่ยวกับคอมพิวเตอร์

- 2.1 กลัวคอมพิวเตอร์จะมาแย่งงานของตน
- 2.2 การนำเอาคอมพิวเตอร์มาใช้นั้นไม่จำเป็นต้องเปลี่ยนแปลงวิธีการปฏิบัติงานเลย
- 2.3 การวางแผนนำคอมพิวเตอร์มาใช้คือ การตัดสินใจว่าจะใช้คอมพิวเตอร์ยี่ห้อไหนดี
- 2.4 การใช้คอมพิวเตอร์จะเปิดโอกาสให้มีการปฏิบัติงานผิดพลาดและทุจริตมากขึ้น
- 2.5 คอมพิวเตอร์จะเปิดเผยข้อมูลของสถาบันการเงินให้แก่บุคคลผู้ไม่มีหน้าที่เกี่ยวข้อง
- 2.6 ข้อมูลที่ได้จากคอมพิวเตอร์ไม่น่าเชื่อถือ
- 2.7 การนำคอมพิวเตอร์มาใช้งานหมายถึง การผจญภัยกับปัญหาทางด้านเทคนิคมากมายและสิ้นเปลือง
- 2.8 การลงทุนใช้คอมพิวเตอร์จะเสียเงินมากเมื่อเปรียบเทียบกับการทำงานในระบบเดิมเพิ่มขึ้น

3. ข้อกังวลของสถาบันการเงินเกี่ยวกับการใช้คอมพิวเตอร์

- 3.1 การใช้คอมพิวเตอร์นำไปสู่การเปลี่ยนแปลงที่สถาบันการเงิน หรือองค์กรไม่คุ้นเคยมาก่อน สถาบันการเงินหรือองค์กรควรที่จะเปลี่ยนแปลงไปใช้คอมพิวเตอร์หรือไม่
- 3.2 การใช้คอมพิวเตอร์นั้นอาจจะต้องเสี่ยงกับปัญหาในระยะต่อไป เช่น ความล้มเหลวการขาดการ ควบคุม สถาบันการเงินหรือองค์กรจะหามาตรการป้องกันได้อย่างไร
- 3.3 วิธีการควบคุมปฏิบัติงาน และตรวจสอบที่ใช้กันอยู่ในปัจจุบันไม่เหมาะกับระบบงานที่ใช้คอมพิวเตอร์ มีวิธีการควบคุมและตรวจสอบการทำงานของคอมพิวเตอร์อย่างเพียงพอหรือไม่
- 3.4 พนักงานระดับต่างๆ ของสถาบันการเงิน หรือองค์กรซึ่งคุ้นเคยกับการปฏิบัติงานที่เป็นอยู่ จะปรับตัวให้เข้ากับวิธีการใหม่ ๆ เมื่อใช้คอมพิวเตอร์ได้เพียงใด
- 3.5 บุคลากรด้านคอมพิวเตอร์ที่มีความสามารถนั้นค่อนข้างจะหายาก สถาบันการเงิน หรือองค์กรจะสามารถหาบุคลากรที่มีความสามารถด้านนี้และดึงตัวไว้ให้ยังทำงานกับสถาบันการเงินหรือองค์กรนาน ๆ ได้เพียงใด
- 3.6 ผู้บริหารระดับสูงซึ่งคุ้นเคยกับวิธีการง่าย ๆ ในการหาข้อมูลจากสมุดบัญชีต่าง ๆ จะรู้สึกไม่สะดวก และกังวลใจหรือไม่ เมื่อข้อมูลเหล่านั้นไปเก็บอยู่ใน Computer files
- 3.7 ข้อมูลต่าง ๆ ในการดำเนินงานของสถาบันการเงินหรือองค์กรมักถูกควบคุมไม่เปิดเผยให้บุคคลที่ไม่ มีหน้าที่เกี่ยวข้องทราบ การใช้คอมพิวเตอร์จะรักษาความลับของข้อมูลต่าง ๆ ได้เพียงใด
- 3.8 มีการสอบยันการทำงาน (double-checked) ในระหว่างพนักงานของสถาบันการเงินหรือองค์กร และมีการควบคุมอีกชั้น การใช้คอมพิวเตอร์จะเปิดโอกาสให้มีการทุจริตได้มากขึ้นหรือไม่

4. ปัญหาที่บรรดาศูนย์คอมพิวเตอร์ต่าง ๆ ส่วนใหญ่ประสบ

- 4.1 พึ่งพาอาศัยผู้จำหน่ายคอมพิวเตอร์มากเกินไป
การหวังความช่วยเหลือจากผู้จำหน่ายคอมพิวเตอร์ในการศึกษา และวางระบบงานให้โดยรักษาผลประโยชน์ของลูกค้าอย่างเต็มที่นั้นไม่มีทางเป็นจริงได้ แต่อย่างไรก็ดีหน่วยงานที่กำลังจะหันมาใช้คอมพิวเตอร์นั้นยากนักที่จะมีทีมงานที่มีความรู้ความสามารถพอที่จะวางแผนและออกแบบระบบงานได้เอง การเพิ่มจำนวนอย่างรวดเร็วของศูนย์คอมพิวเตอร์นั้น ทำให้การให้ความช่วยเหลือด้านต่าง ๆ จากผู้จำหน่ายคอมพิวเตอร์ทำได้ไม่เต็มที่
- 4.2 วางแผนเตรียมจัดตั้งศูนย์คอมพิวเตอร์ไว้ไม่ดีพอ
มีศูนย์คอมพิวเตอร์หลายแห่งที่ดำเนินงานได้อย่างซุกซลัก เนื่องมาจากศึกษา และวางแผนได้ง่าย ๆ ไม่กำหนดระบบงานที่จะต้องให้มีแน่ชัด จัดหาเครื่องคอมพิวเตอร์มาก่อนศึกษาระบบงานและบุคลากรขาดการติดตามเอาใจใส่จากฝ่ายบริหาร
- 4.3 เน้นค่าใช้จ่ายเกี่ยวกับเครื่องคอมพิวเตอร์และบุคลากรด้านนี้มากเกินไป
ให้ความสนใจเฉพาะค่าใช้จ่ายด้านคอมพิวเตอร์ที่เกิดขึ้นตามรายงาน โดยไม่ให้ความสนใจกับค่าใช้จ่ายที่ต้องสูญเสียไป อันเนื่องมาจากระบบงานไม่มีประสิทธิภาพ และการทำงานไม่ได้ตามเป้าหมาย เช่น การทำงานที่มีความสำคัญน้อย ปริมาณงานไม่มากนัก ความต้องการเร่งด่วนไม่มี แต่ผู้จัดการศูนย์ประมวลผลซึ่งอาจเป็นผู้ผูกขาดในการตัดสินใจเพียงผู้เดียว ในบางครั้งก็ตั้งใจเพียงทดสอบสมรรถภาพของเครื่องคอมพิวเตอร์ เพื่อหาประสบการณ์ให้กับตนเองเพิ่มขึ้นเท่านั้น
- 4.4 ออกแบบระบบงานง่าย ๆ เพียงระดับพื้นฐาน
มีระบบงานจำนวนมากที่โดยเนื้อแท้แล้ว เป็นเพียงการใช้คอมพิวเตอร์ทำงานแบบเดียวกับระบบเดิมเคยทำอยู่แล้ว มากกว่าที่จะออกแบบให้คอมพิวเตอร์ทำงานที่ไม่เคยทำมาก่อน
- 4.5 ประสบความล้มเหลวเมื่อนำระบบงานออกใช้หรือใช้ไม่ได้ไม่สมบูรณ์
ความยุ่งยากในช่วงนำระบบงานออกใช้นั้นมักจะถูกประเมินต่ำไป เพราะผู้ใช้ข้อมูล (user) ขาดการเอาใจใส่ในช่วงพัฒนาระบบงาน ทำให้ไม่ตระหนักว่าพวกเขาเองก็เป็นส่วนหนึ่งของระบบงาน ผู้มีความคิดเห็นต่อต้านระบบงานใหม่ไม่ได้รับการชี้แจงทำความเข้าใจอย่างเพียงพอ และผู้บริหารระดับสูงไม่ให้ความสนใจเท่าที่ควร
- 4.6 ประโยชน์ด้านการบริหารงานถูกจำกัด
ผู้วิเคราะห์ระบบงาน ซึ่งมีความชำนาญด้านเทคนิคคอมพิวเตอร์ด้านเดียวยากที่จะเข้าใจความต้องการของฝ่ายบริหาร และสิ่งที่จะมีประโยชน์ต่อการบริหารงานฝ่ายบริหารก็ไม่ทราบว่าคุณคอมพิวเตอร์จะช่วยงานอะไรได้บ้าง และผู้บริหารระดับสูงบางแห่งกลับไม่ได้รับการพิจารณาว่าเป็นผู้ใช้ข้อมูล (user)

16

อาชญากรรมทาง
เทคโนโลยี (คอมพิวเตอร์)

อาชญากรรมทางเทคโนโลยี (คอมพิวเตอร์)

การขยายตัวอย่างรวดเร็วของวิทยาการคอมพิวเตอร์ในวงการธุรกิจโดยเฉพาะธนาคารพาณิชย์และสถาบันการเงิน เป็นความหวังใหม่ที่ผู้บริหารในองค์กรจะเอาชนะใจลูกค้า/ประชาชน โดยการให้บริการที่รวดเร็ว แปลกใหม่ ที่องค์กรอื่นที่ประกอบธุรกิจประเภทเดียวกันยังทำไม่ได้

1. พัฒนาการทางคอมพิวเตอร์ 3 ประการ ที่ทำให้อาชญากรรมทางเทคโนโลยีเพิ่มขึ้น

- 1.1 การแพร่หลายของเครื่องคอมพิวเตอร์ขนาดเล็กในราคาต่ำ
- 1.2 อัตราเติบโตของการใช้เครื่องคอมพิวเตอร์เป็นไปอย่างกว้างขวาง อาชญากรยุคใหม่ที่มาในคราบของพนักงานระดับสูงในห้างแอร์ก็เพิ่มมากขึ้น โดยเฉพาะคอมพิวเตอร์ระบบรวมศูนย์ที่สามารถใช้ผ่านโทรศัพท์สายตรงติดต่อได้ ยิ่งเปิดโอกาสให้อาชญากรคอมพิวเตอร์สามารถใช้เครื่องคอมพิวเตอร์ส่วนตัวเข้าถึงข้อมูลอันมีค่าอย่างสะดวก
- 1.3 การแพร่หลายของการศึกษาด้านคอมพิวเตอร์ในโรงเรียน สถาบันต่าง ๆ ได้สอนให้คนที่ฉลาดอยู่แล้วฉลาดยิ่งขึ้น และสามารถนำมาใช้ในทางผิด ๆ เช่น เมื่อรู้จุดอ่อนของระบบรักษาความปลอดภัยของคอมพิวเตอร์แล้ว

2. คนฉลาดกว่าคอมพิวเตอร์

การที่ใคร ๆ ก็สามารถเป็นเจ้าของเครื่องคอมพิวเตอร์เล็ก ๆ แต่มีประสิทธิภาพสูงได้ง่าย ๆ และส่วนมากก็สามารถพ่วงติดต่อเข้าถึงเครื่องคอมพิวเตอร์ใหญ่โดยระบบสื่อสารทางสายโทรศัพท์ ทำให้แนวโน้มของผู้ประกอบอาชญากรรมทางด้านคอมพิวเตอร์ลดลงไปถึงระบบสมัยพนักงาน ผู้ที่ไม่ซื่อสัตย์ต่อองค์กร อาจเปลี่ยนหรือปลอมแปลงฐานะความมั่นคงของลูกค้าขององค์กรหรือผู้ที่ต้องการได้ หากรู้ถึงระบบงานและจุดอ่อนของการเข้าถึงระบบงานอื่นๆ

3. การควบคุมภายในขาดประสิทธิภาพ

การที่ผู้บริหารระดับสูง และ/หรือผู้มีส่วนรับผิดชอบในการบริหารงานด้านคอมพิวเตอร์ขาดความเอาใจใส่ ในด้านการควบคุมภายในอย่างเพียงพอ ก็มีผลสำคัญที่เพิ่มอาชญากรรมทางคอมพิวเตอร์และนำความสูญเสียอย่างใหญ่หลวงมาให้แก่ธนาคารได้ทั้งสิ้น

4. การทุจริตทางคอมพิวเตอร์

โอกาสที่พนักงานระดับปฏิบัติงานจะมีโอกาสกระทำการทุจริต โดยใช้คอมพิวเตอร์เป็นเครื่องมือหรืออาศัยจุดอ่อนของระบบงาน หรือจุดอ่อนของการปฏิบัติงาน และการควบคุมภายในในองค์กรที่ใช้คอมพิวเตอร์ในทางทุจริตก็มีโอกาสมากกว่าการป้องกันด้านนี้โดยฝ่ายบริหาร โดยเฉพาะอย่างยิ่งหากผู้ตรวจสอบได้ติดตามอ่านปัญหาของสถาบันการเงินหรือองค์กรอื่นที่ใช้คอมพิวเตอร์ตามที่ได้ลำดับมาจึงขอสรุปเรื่องคอมพิวเตอร์กับการทุจริตในวงการสถาบันการเงินโดยใช้เรื่องข้างต้นประกอบเป็นสำคัญ ดังนี้

4.1 สาเหตุการทุจริต

มีองค์ประกอบที่สำคัญ 3 ประการ คือ

- 4.1.1 ความประพฤติด้านตัวของผู้ไม่รักดี และ
- 4.1.2 องค์การมีจุดอ่อนในด้านระบบงานและการควบคุมภายใน และ
- 4.1.3 ผู้ปฏิบัติงานมีโอกาสทุจริตได้

4.1.1 ความประพฤติด้านตัวของผู้ไม่รักดี ได้แก่

- การเล่นการพนัน และหมกมุ่นอบายมุข
- ความทะเยอทะยานจนเกินควร
- ใช้จ่ายเกินฐานะ
- ไม่รักดีต่อองค์กร
- มีความต้องการจะทุจริตหรือต้องการทดลองวิชาในทางที่มีชอบ

4.1.2 องค์การมีจุดอ่อนในด้านระบบงานและการควบคุมภายใน

4.1.2.1 จุดอ่อนในขั้นตอนพัฒนาระบบงาน

- ผู้วิเคราะห์ระบบงานไม่เข้าใจระบบงานที่แท้จริงที่ตนกำลังจะพัฒนาทั้งระบบ
- ไม่ได้ประเมินความเสี่ยงของการปฏิบัติงานไว้ในแต่ละขั้นตอนของการออกแบบงาน
- ไม่ได้กำหนดขั้นตอนการควบคุม และวิธีการตรวจสอบให้แน่ชัดไว้ในแต่ละกระบวนการประมวลข้อมูลและกระบวนการปฏิบัติงาน
- ผู้ใช้และผู้บริหารไม่รู้จักความต้องการที่แท้จริงของตน ที่จะได้รับจากระบบงานด้านคอมพิวเตอร์ ทำให้ต้องมีการแก้ไขระบบงานกันบ่อย ๆ
- ผู้ตรวจสอบภายในมิได้มีโอกาสร่วมพัฒนาระบบงานตั้งแต่ต้น

4.1.2.2 จุดอ่อนในขั้นตอนการปฏิบัติงาน

- ผู้ใช้ระบบ เช่น Teller หรือ Supervisor ไม่ทราบว่าตนจะต้องทำอะไรบ้าง เมื่อมีปัญหาหรือมีการปฏิบัติงานที่ผิดไปจากการปฏิบัติงานตามปกติ
- ผู้ใช้เชื่อระบบคอมพิวเตอร์มากเกินไป
- ผู้ใช้เข้าใจผิดว่า ความถูกต้องของข้อมูลที่ประมวลด้วยระบบคอมพิวเตอร์หากมีข้อผิดพลาดขึ้นมาก็คงไม่ใช่ความรับผิดชอบของตน
- ผู้ควบคุมไม่เอาใจใส่งานเท่าที่ควร ไม่ปฏิบัติตามกฎเกณฑ์
- ระบบงานที่พัฒนาขึ้นมาใหม่เพื่อใช้คอมพิวเตอร์ ถูกนำมาใช้งานโดยมิได้มีการทดสอบจนเป็นที่พอใจของผู้ใช้และผู้ตรวจสอบก่อน เมื่อนำงานนั้นมาใช้แล้วก็ไม่มีผู้รับผิดชอบโดยตรง

4.1.2.3 จุดอ่อนในด้านการตรวจสอบ

- ผู้ตรวจสอบขาดความรู้ และประสบการณ์ทางด้านการตรวจสอบงานที่ใช้คอมพิวเตอร์

- ผู้ตรวจสอบอยู่ภายใต้การบังคับบัญชาของผู้พัฒนาระบบงาน ไม่ว่าทางตรงหรือทางอ้อม
- ไม่ได้เข้าไปมีส่วนร่วมกำหนดจุดควบคุม และวิธีการตรวจในขั้นตอนพัฒนาระบบงาน
- ผู้ตรวจสอบไม่ได้ติดตามผลและ/หรือปัญหาในการปฏิบัติงานอย่างใกล้ชิด
- ผู้รับผิดชอบไม่กำหนดแผนงานและจัดทำคู่มือการตรวจสอบให้เหมาะสม
- ผู้รับผิดชอบเกรงใจต่อผู้จัดการฝ่ายพัฒนาระบบงาน

5.1.2.4 จุดอ่อนในการบริหาร

- ขาดการติดตามผลการปฏิบัติงาน
- ไม่ให้ความสำคัญของการตรวจสอบงานด้านคอมพิวเตอร์เท่าที่ควร
- เน้นและให้ความสำคัญต่อการพัฒนาระบบงานใหม่ๆ เร็วกว่าเวลาที่ควร

4.1.3 ผู้ปฏิบัติงานมีโอกาสทุจริตได้

- การปฏิบัติงานที่ขึ้นอยู่กับความเชื่อใจในความสุจริตของพนักงานเป็นสำคัญ
- ผู้บริหารหรือผู้ควบคุมไม่เข้าใจระบบงานและกฎเกณฑ์การควบคุม
- องค์กรมีจุดอ่อนในด้านระบบงานและการควบคุมภายใน (ตามข้อ 5.2)

4.2 จุดที่สามารถจะทุจริตได้

- การทุจริตทางด้าน Input
- การทุจริตทางด้าน Processing
- การทุจริตทางด้าน Output

4.3 ประเภทของการทุจริตทางด้านคอมพิวเตอร์ในวงการสถาบันการเงิน

5.3.1 ประเภทการทุจริตทางด้าน Input

5.3.2 ประเภทการทุจริตทางด้าน Processing

5.3.3 ประเภทการทุจริตทางด้าน Output

4.4 การป้องกันภัยจากการทุจริต

- การป้องกันทางด้านผู้บริหาร
- การป้องกันทางด้านผู้ให้บริการทางด้านคอมพิวเตอร์
- การป้องกันทางด้านผู้ใช้บริการ

4.5 แนวทางในการตรวจสอบการทุจริตด้านคอมพิวเตอร์

- สร้างเป้าหมายในการตรวจสอบให้แน่นอน
- ประเมินระบบงานและวิธีการปฏิบัติงานที่ตรวจสอบว่ามีจุดใดที่ควรจะมีการควบคุมบ้าง
- ประเมินประสิทธิภาพระบบการควบคุมภายในที่มีอยู่ว่าน่าเชื่อถือได้เพียงใด
- เลือกเทคนิคการทดสอบเพื่อประเมินจุดอ่อนมาใช้ให้สอดคล้องกับเป้าหมาย และแนวความคิดของผู้ตรวจสอบ
- ดำเนินการตรวจสอบตามเทคนิคที่เลือกไว้แล้ว
- วิเคราะห์ผลการตรวจสอบ

- สรุปลจุดอ่อน (ถ้ามี) เกี่ยวกับการควบคุมภายในนั้น
- ประเมินผลกระทบ และความเสี่ยงของจุดอ่อนที่มีอยู่ โดยรวบรวมจุดอ่อนทั้งที่ไม่มีการควบคุม หรือจุดอ่อนที่มีการควบคุมแต่ไม่เพียงพอ
- ประเมินประเภทของการทุจริต โอกาสการทุจริต สถานที่ที่จะเกิดการทุจริต วิธีการทุจริตที่เป็นไปได้ ผู้ที่จะทุจริตได้ และผู้ที่เสียหาย ในแต่ละช่วง หรือแต่ละขั้นตอนของจุดอ่อนนั้น
- เลือกเทคนิคที่จะทดสอบการทุจริตตามแนวความคิดของผู้ตรวจสอบที่จะเป็นไปได้มากที่สุดก่อน
- ปฏิบัติการทดสอบตามเทคนิคที่เลือกไว้แล้ว
- วิเคราะห์ผลการตรวจสอบ
- สรุปผลการตรวจสอบ
- จัดทำรายงานการตรวจสอบ

4.6 สิ่งที่จะตามมาในอนาคต

- การทุจริตโดยใช้คอมพิวเตอร์หรือเกี่ยวกับคอมพิวเตอร์จะมีมากขึ้น
- จะมีองค์กรผู้เสียหายมากขึ้น
- หน่วยงานและการพิพากษาคดีคอมพิวเตอร์จะมีปัญหาในการสืบคดี และการพิจารณามากขึ้น

4.7 สิ่งที่ต้องดำเนินการ

- ผู้ตรวจสอบภายในด้านคอมพิวเตอร์ควรจะได้มีบทบาทมากขึ้นในด้านการป้องกันการทุจริตและควรจะได้มีจำนวนเพิ่มขึ้นอย่างเร่งด่วนตามปริมาณการใช้คอมพิวเตอร์
- ผู้บริหารควรจะได้ให้ความสนใจในด้านการตรวจสอบงาน และข้อสังเกตของผู้ตรวจสอบทางด้านคอมพิวเตอร์มากขึ้น โปรดอย่าได้เร่งรัดพัฒนางานจนลืมนึกถึงผลกระทบต่อองค์กรได้ที่เกิดขึ้นจากจุดอ่อนในการพัฒนาระบบงานตั้งแต่ต้น
- องค์กรไม่ควรพึ่งพาบุคคลภายนอกผู้ให้บริการทางด้านคอมพิวเตอร์จนเกินไป องค์กรพึงตระหนักว่าผู้ที่มีความเชี่ยวชาญทางด้านคอมพิวเตอร์ หรือผู้สนับสนุนทางด้านการขายอุปกรณ์เทคนิคคอมพิวเตอร์ ไม่สามารถจะช่วยงานด้านพัฒนางานขององค์กรได้มากนัก หากผู้ให้บริการไม่มีความรู้ความชำนาญงานในระบบงานขององค์กรดีพอ โดยเฉพาะอย่างยิ่งระบบงานทางด้านธนาคารพาณิชย์และสถาบันการเงิน
- องค์กรพึงตระหนักว่า บุคลากรภายในองค์กรที่มีความเข้าใจในระบบงานขององค์กรดีจะสามารถช่วยงานพัฒนางานขององค์กรได้มาก หากเขาเหล่านั้นสามารถจะเข้าใจระบบงานทางด้านคอมพิวเตอร์ และสามารถประยุกต์การปฏิบัติงานให้เข้ากับระบบงานด้านคอมพิวเตอร์ได้
- การแลกเปลี่ยนทักษะระหว่างหน่วยงานที่ใช้คอมพิวเตอร์เป็นสิ่งจำเป็น
- องค์กรที่ใช้เครื่องคอมพิวเตอร์ขนาดเล็กจรมัควัฒนเป็นพิเศษ

17

**ประเภทการตรวจสอบ/
ลักษณะการตรวจสอบ**

ประเภทการตรวจสอบ

1. การตรวจสอบทางการเงิน (FINANCIAL AUDITING)
2. การตรวจสอบการปฏิบัติตามการควบคุมภายใน (COMPLIANCE AUDITING)
3. การตรวจสอบการปฏิบัติงาน (OPERATIONAL AUDITING)
4. การตรวจสอบการบริหารงาน (MANAGEMENT AUDITING)
5. การตรวจสอบการทุจริต (FRAUD AUDITING)
6. การตรวจสอบด้านคอมพิวเตอร์ (EDP AUDITING)

ลักษณะการตรวจสอบ

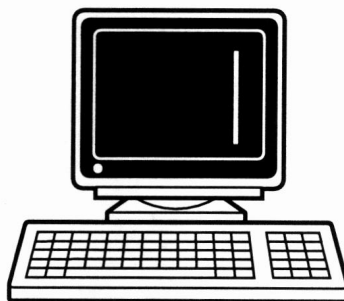
1. การตรวจสอบทางการเงิน (FINANCIAL AUDITING) มีวัตถุประสงค์ดังนี้.-
 - เพื่อให้แน่ใจว่าข้อมูลทางการเงินของกิจการมีความถูกต้องน่าเชื่อถือได้เพียงพอ
 - เพื่อรับรองความถูกต้องของรายงานทางการเงินที่เสนอต่อสาธารณชน
2. การตรวจสอบการปฏิบัติตามการควบคุมภายใน (COMPLIANCE AUDITING)
มีวัตถุประสงค์ดังนี้.-
 - เพื่อประเมินประสิทธิภาพของผู้ปฏิบัติงาน
 - เพื่อประเมินประสิทธิภาพของระบบควบคุมภายในที่มีอยู่ให้ทราบถึงข้อบกพร่องหรือจุดอ่อนที่จะต้องดำเนินการแก้ไข
3. การตรวจสอบการปฏิบัติงาน (OPERATIONAL AUDIT)
หรือ FUNCTIONAL AUDIT หรือ PERFORMANCE AUDIT มีวัตถุประสงค์ดังนี้.-
 - เพื่อประเมินประสิทธิภาพและประสิทธิผลของการดำเนินงานตามนโยบายและแนวทางการปฏิบัติงานที่ฝ่ายบริหารกำหนด และพิจารณาความเหมาะสมของนโยบายดังกล่าว
4. การตรวจสอบการจัดการ (MANAGEMENT AUDITING)
 - เพื่อประเมินระบบการควบคุมทางการบริหารที่กิจการนั้นกำลังใช้อยู่ เพื่อดูว่าระบบการควบคุมที่ใช้อยู่ขณะนั้นเป็นระบบที่มีประสิทธิภาพพอหรือไม่ หรือมีข้อเสนอแนะเพื่อปรับปรุงแก้ไขจุดใด อย่างไร

5. การตรวจสอบการทุจริต (FRAUD AUDITING) มีวัตถุประสงค์ดังนี้-

- เพื่อประเมินผลเสียหายจากการทุจริต และประเมินผลการป้องกันการทุจริตที่อาจเกิดขึ้น

6. การตรวจสอบด้านคอมพิวเตอร์ (EDP AUDITING) มีวัตถุประสงค์ดังนี้-

- (1) ความปลอดภัยของทรัพย์สิน
- (2) ความถูกต้องเชื่อถือได้ของข้อมูล
- (3) ประสิทธิภาพในการบรรลุเป้าหมายของกิจการ
- (4) ประสิทธิภาพในการใช้ทรัพยากร
- (5) ความสามารถในการดำเนินงานอย่างต่อเนื่อง
- (6) การประเมินและควบคุมความเสี่ยงต่าง ๆ ในการดำเนินงานด้านคอมพิวเตอร์ ทั้งทางด้าน "องค์กร" (Data center หรือ General control) และทางด้าน "งาน" (Applications)



18

**หลักฐานการตรวจสอบ
ด้านคอมพิวเตอร์**

หลักฐานการตรวจสอบด้านคอมพิวเตอร์

ในการตรวจสอบ ผู้ตรวจสอบจำเป็นต้องหาหลักฐานเพื่อยืนยันความเพียงพอของการควบคุมในระบบการประมวลผล ซึ่งในระบบที่ทำด้วยมือ (Manual System) หลักฐานส่วนใหญ่มักได้แก่เอกสารต่าง ๆ ที่สามารถมองเห็นได้ แต่ในระบบงานที่ใช้คอมพิวเตอร์ประมวลผล รูปแบบของหลักฐานได้เปลี่ยนแปลงไปอยู่ในรูปของสื่อแม่เหล็กเป็นส่วนใหญ่ ทำให้ไม่สามารถใช้วิธีการตรวจสอบแบบเดิมที่อาศัยเอกสารเป็นสำคัญต่อไปได้ ดังนั้น การที่ผู้ตรวจสอบจะสามารถตรวจสอบจะสามารถตรวจสอบทาง EDP ให้ได้ผลดีจึงจำเป็นต้องทราบถึงผลกระทบของเทคโนโลยีทางคอมพิวเตอร์ที่มีต่อหลักฐานที่จะใช้ในการตรวจสอบ เพื่อกำหนดแนวทางการตรวจสอบที่เหมาะสมต่อไปได้

1. รูปแบบของหลักฐานที่ผู้ตรวจสอบมักใช้ในการตรวจสอบระบบที่ทำด้วยมือ

(Traditional versus computerized Audit Evidence)

1.1 เอกสารต้นกำเนิด เช่น สลิปฝากและถอนเงิน และแบบฟอร์มใบคำขอ

1.2 หลักฐานการอนุมัติ คือการลงลายมือชื่อของผู้มีอำนาจในเอกสารต้นกำเนิดและการประทับวันที่และเวลาที่จัดทำเอกสารและผ่านการอนุมัติ

1.3 หลักฐานการประมวลผล เช่น แบบฟอร์มแสดงการคำนวณ คู่มือที่แสดงรายละเอียดข้อมูลหลักและกระดาษจากเครื่องบวกเลข

1.4 หลักฐานทางผลลัพธ์ เช่น เช็ค รายงานแสดงรายการเคลื่อนไหวทางบัญชีจากธนาคาร (Bank Statement) ใบเสร็จรับเงิน และรายงานต่าง ๆ

2. การเปลี่ยนแปลงลักษณะของหลักฐานเมื่อมีการนำเครื่องคอมพิวเตอร์มาใช้

2.1 รายการที่ทำโดยคน (People Initiated Transaction)

ในระบบที่ทำด้วยมือ บุคคลมักเป็นผู้ให้กำเนิดรายการ และส่งเข้าสู่ระบบประมวลผล แต่ในกรณีที่ใช้คอมพิวเตอร์ ระบบงานคอมพิวเตอร์อาจให้กำเนิดรายการเองโดยอัตโนมัติ เช่น เครื่องจะพิมพ์ Bank Statement โดยอัตโนมัติเมื่อมีรายการมากกว่าที่กำหนดไว้ในแฟ้มข้อมูลของลูกค้า

2.2 ข้อมูลนำเข้าที่บันทึกในกระดาษ (Hard Copy Input)

เมื่อมีรายการเกิดขึ้น ในระบบที่ทำด้วยมือจะมีการจัดทำและบันทึกข้อมูลในเอกสารที่เป็นกระดาษ แต่ในระบบงานคอมพิวเตอร์ ข้อมูลจะบันทึกผ่านเครื่องเทอร์มินอลซึ่งจะไม่ปรากฏอยู่ในเอกสารอีก เช่น การเปลี่ยนแปลงอัตราดอกเบี้ย พนักงานจะป้อนอัตราใหม่เข้าไปปรับปรุงที่แฟ้มข้อมูลหลักของลูกค้าเงินให้กู้ยืม ผ่านทางเครื่องเทอร์มินอลได้โดยทันที

2.3 การอนุมัติรายการ (Manual Authorization)

ในระบบที่ทำด้วยมือ จะมีการอนุมัติรายการโดยผู้มีอำนาจอนุมัติ ลงลายมือชื่อ ชื่อย่อ หรือประทับตราแสดงการอนุมัติ แต่ในระบบงานคอมพิวเตอร์ จะมีการกำหนดการอนุมัติไว้ล่วงหน้า เช่นการกำหนดวงเงินการให้สินเชื่อไว้ในระบบ เมื่อมีการให้สินเชื่อระบบจะตรวจสอบว่าเกินวงเงินหรือไม่ หากไม่เกินที่กำหนด ระบบก็จะอนุมัติให้รายการผ่านได้โดยอัตโนมัติ นอกจากนี้ การอนุมัติอาจกระทำได้ในรูปของการใช้ password การรูดบัตรที่มีรหัสลับบันทึกไว้บนแถบแม่เหล็ก หรือการกำหนดระดับกฎเกณฑ์ที่ต้องใช้ประกอบการทำรายการที่เครื่องเทอร์มินอล

2.4 การจัดส่งข้อมูล (Document Transmission)

ในระบบที่ทำด้วยมือ จะมีการจัดส่งข้อมูลในรูปของเอกสารโดยใช้คนนำส่งส่งเป็นไปรษณีย์ภัณฑ์หรือส่งไปทางเรือ แต่ในระบบงานคอมพิวเตอร์ จะมีการจัดส่งข้อมูลหลังจากที่ได้บันทึกแปลงรหัส และรวบรวมไว้พร้อมแล้วในลักษณะของข้อมูลทางอิเล็กทรอนิกส์

2.5 การประมวลผลในรูปแบบที่มองเห็นได้ (Hard Copy Processing)

ในระบบที่ทำด้วยมือ มักมีการกำหนดขั้นตอนการประมวลผลแต่ละขั้นโดยไม่ซับซ้อน เพื่อลดความผิดพลาดที่อาจเกิดขึ้นจากบุคคล (human error) ให้มากที่สุด แต่ในระบบคอมพิวเตอร์ การประมวลผลจะเป็นไปโดยอัตโนมัติตามขั้นตอนที่กำหนดไว้ในโปรแกรมคำสั่งงาน ซึ่งมักมีความสลับซับซ้อน อันเนื่องมาจากความต้องการให้เครื่องคอมพิวเตอร์สามารถปฏิบัติงานได้อย่างรวดเร็วและถูกต้องแม่นยำ เช่น การหักชำระเงินกู้ของลูกค้าหนี้รายที่ครบกำหนดชำระจากบัญชีเงินฝากกระแสรายวันไปบัญชีเงินกู้ยืม

2.6 ข้อมูลหลัก (Manuals of Master Information)

ข้อมูลหลักหรือข้อมูลที่ถาวรที่จำเป็นต้องใช้ในการประมวลผล เช่น อัตราดอกเบี้ย วงเงินเบิกเกินบัญชี มักบันทึกอยู่ในรูปข้อมูลที่อ่านได้ด้วยตาเปล่า แต่ในระบบงานคอมพิวเตอร์ จะบันทึกอยู่ในรูปของสื่อแม่เหล็ก

2.7 รายงานข้อมูลผลลัพธ์ (Hard Copy Output)

ในระบบที่ทำด้วยมือ ข้อมูลที่ได้จากการประมวลผลมักอยู่ในรูปของเอกสาร เช่น รายงาน หรือเช็คที่พิมพ์รายการเรียบร้อย แต่ในระบบงานคอมพิวเตอร์มักไม่เป็นเช่นนั้น เช่นการโอนเงิน จะใช้วิธีโอนเงินทางอิเล็กทรอนิกส์ และข้อมูลผลลัพธ์ก็จะนำเสนอบนจอภาพ (video screen) และในบางระบบอาจแสดงเฉพาะข้อมูลที่ไม่ปกติให้ทราบเพื่อปฏิบัติการต่อไปก็ได้

2.8 การจัดแฟ้มเอกสาร (Document Filing)

ในระบบที่ประมวลผลด้วยมือ มักมีการจัดเก็บเอกสารข้อมูลในลักษณะที่เราพบเห็นกันโดยทั่วไป และเมื่อต้องการใช้ก็หาได้ไม่ลำบากนัก แต่ในระบบงานคอมพิวเตอร์มักเก็บข้อมูลอยู่ใน tapes หรือ disks ซึ่งการเรียกใช้หรือดึงข้อมูลออกมานั้นต้องใช้โปรแกรมคำสั่งงานดึงข้อมูลออกมาตามความต้องการ

2.9 ร่องรอยการตรวจสอบ (Hard Copy Audit Trail)

ในระบบที่ทำด้วยมือ ข้อมูลต่าง ๆ มักบันทึกอยู่ในรูปของเอกสาร ซึ่งจะมีทั้งข้อมูลต้นกำเนิดลายมือชื่อแสดงการอนุมัติ วิธีการประมวลผล และผลลัพธ์ ซึ่งเพียงพอแก่การใช้เป็นร่องรอยในการตรวจสอบ ไม่ว่าจะเป็นเริ่มจากจุดกำเนิดรายการไปถึงยอดจำนวนรวมหรือย้อนกลับจากยอดจำนวนรวมไปยังเอกสารต้นกำเนิด แต่ในระบบงานคอมพิวเตอร์ร่องรอยในการตรวจสอบมักจะกระเจาอยู่ตามจุดต่าง ๆ ขึ้นอยู่กับลักษณะของระบบฐานข้อมูล (Database system) และข้อมูลส่วนใหญ่เก็บอยู่ในรูปของสื่อแม่เหล็ก ผู้ตรวจสอบจึงจำเป็นต้องเข้าใจถึง concept ของระบบการประมวลผล จึงจะสามารถทราบถึงขั้นตอนการประมวลผลและร่องรอยที่จะใช้ในการตรวจสอบ ซึ่งก็ไม่ใช่เรื่องที่ย่างยาก โดยเฉพาะอย่างยิ่งในระบบที่ค่อนข้างสลับซับซ้อน

2.10 คู่มือปฏิบัติงาน (Procedure Manual)

ในระบบที่ทำด้วยมือ มักมีคู่มือปฏิบัติงานที่แสดงรายละเอียดแต่ละขั้นตอนของการประมวลผลรายการเพื่อเป็นแนวทางสำหรับผู้ปฏิบัติงาน แต่ในระบบงานคอมพิวเตอร์คู่มือเหล่านี้อาจอยู่ในรูปของ computer program listing, data dictionary listings และเอกสารที่ผู้ขาย software มอบให้แก่ธนาคาร

2.11 การติดตามรายการ (Manual Monitoring)

ในระบบที่ทำด้วยมือ ผู้มีอำนาจอนุมัติมักสอบถามการประมวลผลข้อมูลเพื่อให้เกิดความมั่นใจว่าข้อมูลดังกล่าวมีความสมเหตุสมผล มีความถูกต้องครบถ้วนสมบูรณ์และผ่านการอนุมัติ แต่ในระบบงานคอมพิวเตอร์โปรแกรมที่ได้กำหนด logic ไว้ล่วงหน้าจะเช็คสอบข้อมูลเหล่านี้โดยอัตโนมัติ การใช้คนสอบถามแทบจะเป็นไปไม่ได้ โดยเฉพาะอย่างยิ่งในระบบคอมพิวเตอร์ที่มีความสลับซับซ้อนและเป็นระบบรวม และมีวงจรการประมวลผลที่สั้นขึ้นกว่าเดิม

2.12 การแบ่งแยกหน้าที่ (Segregation of Duties)

ในระบบที่ทำด้วยมือ การแบ่งแยกหน้าที่มักกระทำโดยการแบ่งแยกงานในระหว่างบุคคลต่าง ๆ เพื่อเกิดการควบคุมซึ่งกันและกัน ซึ่งก็มักเพียงพอและไม่มีใครมีปัญหาแต่ในระบบงานคอมพิวเตอร์การแบ่งแยกงานในระหว่างบุคคลต่าง ๆ นั้นยังไม่เพียงพอจำเป็นต้องมีการแบ่งแยกงานระหว่างขั้นตอน การประมวลผลโดยอัตโนมัติในแต่ละขั้นด้วย

2.13 การประมวลผลรายการจำนวนมาก (Bulk Processing)

ในระบบที่ทำด้วยมือ มักใช้วิธี resequencing หรือ matching diverse data elements แต่วิธีดังกล่าวก็ยุ่งยากและสิ้นเปลือง และจะกระทำเมื่อจำเป็นเท่านั้น แต่ในระบบงานคอมพิวเตอร์ ข้อมูลจำนวนมากเหล่านั้นสามารถนำไปเก็บไว้ใน database เพียงอันเดียว และเนื่องจากคอมพิวเตอร์มีความสามารถในการประมวลผลด้วยความเร็วสูงมาก จึงสามารถนำเสนอข้อมูลดังกล่าวได้ในรูปแบบที่ต้องการได้ทุกเมื่อ และสามารถทำการวิเคราะห์ข้อมูลได้ละเอียดซับซ้อนกว่า อีกทั้งจะเรียกใช้ข้อมูลมากกว่าหนึ่งครั้งก็ได้

19

บทบาทและขั้นตอนบางประการ
ที่ผู้ตรวจสอบภายในด้านคอมพิวเตอร์
ควรเข้าไปมีส่วนเกี่ยวข้อง

บทบาทและขั้นตอนบางประการที่ผู้ตรวจสอบภายในด้าน คอมพิวเตอร์ควรเข้าไปมีส่วนเกี่ยวข้อง

เนื่องจากผู้ตรวจสอบภายในด้านคอมพิวเตอร์มีหน้าที่และความรับผิดชอบในการตรวจสอบเพื่อประเมินผล การควบคุมภายใน ซึ่งคณะกรรมการบริหารของธนาคารเป็นผู้มอบให้เพราะการควบคุมภายในอย่างเพียงพอจะทำให้ ผู้บริหารมีความมั่นใจว่า การปฏิบัติงานเป็นไปตามโครงการและตามนโยบายที่ได้ให้ไว้ มาตรฐานการบริหารงานและ ระเบียบปฏิบัติที่เหมาะสมเพื่อให้แข่งขันกับธุรกิจอื่นได้ ตลอดจนทำให้การปฏิบัติงานการประมวลผลข้อมูลได้ถูกต้อง ปลอดภัยและเชื่อถือได้

ธนาคารควรกำหนดหน้าที่และความรับผิดชอบของผู้ตรวจสอบภายในเป็นลายลักษณ์อักษรให้ชัดเจน

งานของผู้ตรวจสอบภายในได้แก่

- ตรวจสอบทางด้าน General control ซึ่งได้แก่การตรวจ Data Center หรือศูนย์ประมวลผลข้อมูล และตรวจ application controls ซึ่งเป็นการตรวจงานต่าง ๆ แต่ละด้าน
- ตรวจสอบ ประเมินผล และรายงานเกี่ยวกับการบัญชี การเงิน และการควบคุมภายในมีการปฏิบัติที่ ถูกต้องและน่าพอใจเพียงใด
- ช่วยเหลือให้มีการนำเอาวิธีการควบคุมภายในที่มีประสิทธิภาพมาใช้
- ควบคุมให้มีการปฏิบัติตามนโยบาย แผนงาน วิธีการและระเบียบที่วางไว้
- ควบคุมการใช้ทรัพย์สินและป้องกันมิให้สูญหาย
- ควบคุมการบริหารงานข้อมูลที่น่ามาใช้งาน
- ประเมินประสิทธิภาพการทำงานของหน่วยงานต่าง ๆ
- เสนอแนะแนวทางการแก้ไขข้อบกพร่องของการควบคุมภายใน

ผู้ตรวจสอบภายในจะต้องศึกษาเข้าไปในเรื่องรายงาน การบันทึกบัญชีการควบคุมงานทุกขั้นตอน เพื่อทำ ความเข้าใจเกี่ยวกับงานที่ตรวจสอบอย่างเต็มที่ และจำต้องวิเคราะห์ ประเมินผล ให้คำแนะนำตั้งข้อสังเกตเกี่ยวกับงาน ที่ตรวจสอบ เสนอต่อฝ่ายบริหาร

สำหรับขั้นตอนต่าง ๆ ที่ผู้ตรวจสอบภายในด้านคอมพิวเตอร์ควรเข้าไปมีส่วนเกี่ยวข้องนอกเหนือจากการ ตรวจสอบงานด้านอื่น ๆ ตามหน้าที่โดยปกติแล้วควรมีดังนี้

1. ขั้นตอนการทำสัญญาซื้อหรือเช่า เกี่ยวกับ
 - 1.1 เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบระบบคอมพิวเตอร์
 - 1.2 โปรแกรมต่าง ๆ
2. ขั้นตอนการตรวจรับและการปฏิบัติตามสัญญา
 - 2.1 การติดตั้งและการทดสอบการทำงานของเครื่องหรืออุปกรณ์ประกอบ (เอกสารประกอบการบรรยายเรื่อง "การตรวจสอบงานคอมพิวเตอร์" ให้พนักงานตรวจสอบภายในด้านคอมพิวเตอร์ของธนาคารพาณิชย์ ครั้งที่ 1)
 - 2.2 การทดสอบการทำงานของโปรแกรมและข้อมูลที่จัดทำขึ้นเพื่อวัดประสิทธิภาพการทำงานของเครื่อง
 - 2.3 เอกสารประกอบระบบงานขั้นต่ำที่ควรจะได้รับและการจัดฝึกอบรม
 - 2.4 การติดตามผลการปฏิบัติงานตามสัญญาด้านการบำรุงรักษา
3. การร่วมพัฒนาและทดสอบงานที่นำเข้าประมวลผลด้วยคอมพิวเตอร์และเอกสารสนับสนุนการปฏิบัติงาน
4. ขั้นตอนการนำระบบงานใหม่เข้ามาใช้
 - 4.1 การเปลี่ยนข้อมูลจากระบบงานเดิมให้อยู่ในรูปแบบระบบงานใหม่
 - 4.2 การปฏิบัติงานแบบคู่ขนาน
 - 4.3 การจัดฝึกอบรมพนักงานที่เกี่ยวข้อง
5. ขั้นตอนการรักษาความปลอดภัยและการลดความเสี่ยงภัยด้านคอมพิวเตอร์ ด้วยการประกันภัย
6. การทำสัญญาในการใช้หรือการให้บริการบุคคลภายนอก

1. ขั้นตอนการทำสัญญาซื้อหรือเช่า เกี่ยวกับ

1.1 เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบระบบคอมพิวเตอร์

ผู้ตรวจสอบควรเป็นผู้ให้ข้อมูลบางส่วนแก่ผู้บริหารในการจัดหาเครื่องคอมพิวเตอร์ ได้แก่

- การเปรียบเทียบราคาของเครื่องและอุปกรณ์ประกอบในลักษณะของอุปกรณ์ขั้นต่อขั้นที่ใช้ในการทำงานที่เหมือนกันเพราะมีผู้ขายได้ตั้งราคาเครื่องคอมพิวเตอร์ต่ำแต่เพิ่มราคาของอุปกรณ์ขั้นอีกซึ่งธนาคารจะต้องซื้อเป็นจำนวนมากและในเวลาที่นานกว่า
- ความสามารถของเครื่องที่จะใช้ทำงานได้อย่างมีประสิทธิภาพ
- ระยะเวลาในการติดตั้งเครื่องให้สมบูรณ์พร้อมที่จะทำงานได้ตามหมายกำหนดของโครงการที่ธนาคารวางไว้
- ความช่วยเหลือของผู้ขายในด้านการวางระบบคอมพิวเตอร์
- ระบบการบำรุงที่บริษัทผู้ขายจะให้แก่ธนาคารเพื่อให้ระบบคอมพิวเตอร์ของธนาคารดำเนินไปโดยไม่ติดขัด
- ความมั่นคงของบริษัทผู้ขายที่จะอยู่ให้บริการแก่ธนาคารได้ตลอดไป

- อุปกรณ์ของยี่ห้ออื่นที่จะนำมาใช้ทดแทนได้
- ระบบการ Back Up เครื่องคอมพิวเตอร์เมื่อเครื่องของธนาคารเสีย เพราะในประเทศไทยซึ่งอุปกรณ์อะไหล่ส่วนมากต้องสั่งจากต่างประเทศ ซึ่งต้องใช้เวลานานดังนั้นการเตรียมระบบอุปกรณ์อะไหล่ส่วนมากต้องสั่ง Back Up ที่ดีจึงเป็นสิ่งจำเป็น
- การจัดฝึกอบรมพนักงานในทุกด้านที่จำเป็นซึ่งผู้ขายจะให้ความช่วยเหลือ
- ค่าใช้จ่ายอื่น ๆ จะต้องระบุให้ละเอียดเช่นภาษีนำเข้าใครเป็นผู้จ่าย

1.2 โปรแกรมต่าง ๆ

เนื่องจากงานที่ใช้ระบบคอมพิวเตอร์ส่วนใหญ่จะเป็นระบบงานที่คล้ายกัน ดังนั้นบริษัทผู้ขายจึงมักออกแบบระบบงานต่าง ๆ ให้เป็นมาตรฐานสากล ซึ่งลูกค้านำไปดัดแปลง โดยการแก้ไขเพียงเล็กน้อยก็ใช้งานได้ แต่ผู้ตรวจสอบภายในจะต้องให้ข้อมูลแก่ผู้บริหารดังต่อไปนี้

- โปรแกรมสำเร็จรูปที่จะซื้อ ทำงานกับ Operating System ของเครื่องคอมพิวเตอร์ที่มีอยู่อย่างมีประสิทธิภาพหรือไม่ เพราะเคยมีผู้ซื้อโปรแกรมสำเร็จรูปมาแล้วทำงานได้ไม่มีประสิทธิภาพต้องไปเช่าเครื่องคอมพิวเตอร์อีกยี่ห้อหนึ่งมาเพื่อใช้กับโปรแกรมที่ซื้อมา ซึ่งทำให้เสียค่าใช้จ่ายเพิ่มขึ้น
- เอกสารประกอบโปรแกรมสำเร็จรูปที่จะต้องได้รับจากผู้ขาย เพื่อให้สามารถใช้โปรแกรมดังกล่าวได้ และสามารถแก้ไขได้เมื่อจำเป็น
- ราคาที่จะทำการซื้อขายกัน ต้องพิจารณาจากความยากง่ายของระบบงานและผลประโยชน์ที่จะได้รับเมื่อเทียบกับการพัฒนาระบบงานเอง
- ผู้ขายให้การฝึกอบรมแก่ผู้ซื้ออย่างเพียงพอที่จะใช้โปรแกรมระบบงานนั้นเพียงใด

2. ขั้นตอนการตรวจรับและการปฏิบัติตามสัญญา

2.1 การติดตั้งและการทดสอบการทำงานของเครื่องและอุปกรณ์ประกอบด้านคอมพิวเตอร์

เนื่องจากธนาคารมีโครงการที่วางไว้ซึ่งการปฏิบัติงานทุกจุดจะต้องสัมพันธ์กันและเสร็จสิ้นตามเป้าหมายที่วางไว้ หากเกิดข้อผิดพลาดขึ้นอาจเป็นผลเสียต่อธนาคารในด้านการแข่งขันหรือเสียค่าใช้จ่ายเพิ่มขึ้นได้ ดังนั้นผู้ตรวจสอบจะต้อง

- ติดตามการติดตั้งระบบคอมพิวเตอร์ทุกระยะและรายงานให้ผู้บริหารทราบและจะต้องให้เสร็จสมบูรณ์ตามสัญญา
- ตรวจสอบการติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบตรงตามข้อกำหนดที่ระบุไว้ในสัญญาและครบถ้วนตามจำนวนที่ระบุไว้ในสัญญาด้วย

2.2 ทดสอบการทำงานของระบบคอมพิวเตอร์ด้วยโปรแกรมและข้อมูลที่จัดทำขึ้นเพื่อวัด

ประสิทธิภาพ การทำงานของระบบคอมพิวเตอร์ที่ติดตั้ง

เนื่องจากผู้ขายเครื่องคอมพิวเตอร์และอุปกรณ์ทั้งระบบชอบโอ้อวดคุณภาพของสินค้าเกินความเป็นจริงหรือให้ข้อมูลที่อาจทำให้เกิดความเข้าใจผิดได้ ดังนั้น ผู้ตรวจสอบภายในควรจะมีบทบาทและจะต้องป้องกันในเรื่องที่กล่าวโดยให้มีระบุประสิทธิภาพในการทำงานของเครื่องและอุปกรณ์ประกอบไว้ในสัญญาอย่างชัดเจน และผู้ตรวจสอบควรจะต้อง

- จัดเตรียมโปรแกรมระบบงานที่จะใช้กับระบบคอมพิวเตอร์ที่ซื้อมา
- จัดเตรียมพนักงานและข้อมูลที่จะต้องใช้ในการประมวลผลทั้งหมด เหมือนการปฏิบัติงานจริง และใช้เวลาตามที่กำหนดไว้ ถ้าไม่เสร็จตามกำหนดก็ไม่รับระบบคอมพิวเตอร์นั้น

ทั้งนี้เพราะงานของธนาคารจะต้องทำให้เสร็จและสามารถตรวจสอบความถูกต้องได้ภายในเวลาที่กำหนดเวลาที่จำกัด ถ้าหากระบบคอมพิวเตอร์ที่ติดตั้งไม่สามารถทำได้ก็ย่อมเกิดผลเสียต่อธนาคารได้ ซึ่งได้เกิดเหตุการณ์ดังกล่าวขึ้นแล้ว กล่าวคือบริษัทผู้ขายระบุว่าเครื่องคอมพิวเตอร์ของตนสามารถเชื่อมต่อกับเครื่องเทอร์มินอลได้ 18 เครื่อง โดยไม่ได้ระบุว่าสามารถใช้เครื่องเทอร์มินอลติดต่อกับคอมพิวเตอร์ในขณะเดียวกันได้ทั้ง 18 เครื่อง โดยประสิทธิภาพของเครื่องคอมพิวเตอร์ทำงานอย่างมีประสิทธิภาพ เมื่อผู้ซื้อระบบคอมพิวเตอร์ดังกล่าวแล้ว นำมาใช้งานจริงปรากฏว่า สามารถนำข้อมูลเข้าเครื่องทางเทอร์มินอลพร้อมกันได้ไม่เกิน 12 เครื่อง เท่านั้น จึงจะทำงานได้อย่างมีประสิทธิภาพ ซึ่งผู้ขายได้แก้ตัวว่าไม่ทราบงานของผู้ซื้อจะใช้เครื่องเทอร์มินอลพร้อมกัน 18 เครื่อง ในขณะเดียวกัน ซึ่งต่อมาผู้ซื้อต้องซื้อเครื่องคอมพิวเตอร์ที่ใหญ่ขึ้นและเสียค่าใช้จ่ายเพิ่มขึ้นเพราะไม่ศึกษารายละเอียดอย่างเพียงพอ

2.3 เอกสารประกอบระบบงานขั้นต่ำที่ควรจะได้รับและการฝึกอบรม

โดยปกติแล้วบริษัทผู้ขายจะต้องให้คู่มือเกี่ยวกับตัวเครื่องและอุปกรณ์ประกอบ Operating system และคู่มือด้าน Operation มาซึ่งพนักงานทุกคนของธนาคารที่เกี่ยวข้องจะต้องเข้ารับการฝึกอบรมรวมทั้งผู้ตรวจสอบภายในด้วย เพราะหากผู้ตรวจสอบภายในมีความรู้ในทุกด้านที่เกี่ยวกับระบบคอมพิวเตอร์ที่ใช้อยู่มาก ย่อมจะทำให้ประสิทธิภาพของการตรวจสอบด้านคอมพิวเตอร์สูงขึ้น เนื่องจากผู้ตรวจสอบสามารถใช้เทคนิคการตรวจสอบได้มากขึ้นด้วย

2.4 การติดตามการปฏิบัติตามสัญญาด้านการบำรุงรักษา

การปฏิบัติตามสัญญาด้านการบำรุงรักษาและซ่อมแซมจะมีข้อความในสัญญาให้ทั้งผู้ขายและผู้ซื้อปฏิบัติตาม ดังนั้นผู้ตรวจสอบจะต้องศึกษาและแยกแยะข้อตกลงออกมา โดยผู้ตรวจสอบภายในจะต้องติดตามให้ผู้ขายปฏิบัติตามสัญญาอย่างเคร่งครัดและสัญญาด้านผู้ซื้อจะต้องปฏิบัติผู้ตรวจสอบจะต้องวางระเบียบปฏิบัติงานให้พนักงานที่มีส่วนเกี่ยวข้องปฏิบัติตามอย่างเคร่งครัดด้วย เช่น ข้อตกลงมีว่าผู้ขายจะทำการซ่อมแซมรักษาเครื่องให้ผู้ซื้อฟรีเป็นเวลา 1 ปี แต่ความเสียหายของเครื่องจะต้องไม่เกิดจากความประมาทของพนักงานธนาคาร จากตัวอย่างที่เกิดขึ้นจริงคือผู้ซื้อแจ้งต่อผู้ขายให้ซ่อมเครื่องพิมพ์แบบใช้หัวพิมพ์ เมื่อช่างทำการแก้ไขก็ทราบสาเหตุการเสียของเครื่องเนื่องจากพนักงานของผู้ซื้อได้ทำคลิป์หนีกระดาษตกลงไปในเครื่องพิมพ์ดังกล่าว ดังนั้นบริษัทผู้ขายจึงคิดค่าซ่อมแซมจากผู้ซื้อได้

3. การร่วมพัฒนาและทดสอบงานที่นำเข้าประมวลผลด้วยคอมพิวเตอร์และเอกสารประกอบระบบงาน

ขั้นตอนการพัฒนากระบวนการมีหลายขั้นตอนซึ่งหากผู้ตรวจสอบได้เข้าร่วมพัฒนาระบบงานตั้งแต่ต้นแล้วจะมีประโยชน์มากทั้งในด้านการประหยัดและประสิทธิภาพของโปรแกรมระบบงานด้านการควบคุมภายใน โดยผู้ตรวจสอบควรเข้าไปเกี่ยวข้องและพิจารณาในเรื่องต่อไปนี้

- การปรับปรุงงานให้เข้าสู่ระบบคอมพิวเตอร์มีความจำเป็นเพียงใด
- มีวิธีการอื่นที่จะปรับปรุงระบบงานที่ใช้อยู่ได้บ้างหรือไม่
- ถ้าจำเป็นจะต้องปรับปรุงแค่ไหนจึงจะทำให้การปฏิบัติงานดีขึ้นเพราะ การปรับปรุงงานที่ใช้อยู่ในปัจจุบันโดยสิ้นเชิงไม่อาจประหยัด เพราะการปฏิบัติงานยังมีขั้นตอนของระบบ Manual ผสมอยู่ด้วย
- ศึกษาวิเคราะห์ค่าใช้จ่ายและผลตอบแทนโดยวิเคราะห์เปรียบเทียบต้นทุน ในการพัฒนาโปรแกรมระบบงานขึ้นเองกับการซื้อโปรแกรมระบบงานสำเร็จรูป
- ความประหยัดที่เกิดขึ้นจากการนำระบบงานใหม่เข้ามาใช้
- ไม่ควรยอมรับโครงการที่พัฒนานั้นหากไม่มีความปลอดภัยและการป้องกันที่ดีพอ

สำหรับเอกสารสนับสนุนการปฏิบัติงานผู้ตรวจสอบจะต้องสอดส่องดูแลอย่างใกล้ชิดเพราะเอกสารดังกล่าวเป็นแหล่งให้ข้อมูลและรายละเอียดเบื้องต้นของระบบงาน เพื่อใช้ในการตรวจสอบ แก้ไข ปรับปรุง บริหารงานและวิธีการใช้ระบบงาน ซึ่งจะต้องถูกต้องทันเวลาและมีความสมบูรณ์อยู่เสมอ ระบบการจัดทำเอกสารที่ดีย่อมช่วยให้การดูแลและเปลี่ยนระบบงานเดิมเป็นระบบงานใหม่ได้ง่ายขึ้น นอกจากนั้นยังมีประโยชน์ในการฝึกอบรมพนักงานใหม่เพื่อสับเปลี่ยนพนักงาน ซึ่งจะช่วยให้สามารถดำเนินงานต่อไปได้ไม่หยุดชะงัก ผู้ตรวจสอบภายในควรพิจารณาดำเนินการต่อไปนี้

- ตรวจสอบให้มีการจัดทำเอกสารสนับสนุนระบบงานให้เสร็จก่อนมีการนำระบบงานใหม่ออกใช้
- คำนึงว่าเอกสารสนับสนุนการปฏิบัติงานที่ไม่เพียงพอแสดงถึงความอ่อนแอของการควบคุมภายใน และการอ่อนแอของฝ่ายบริหารที่ไม่สามารถควบคุมและตระหนักถึงผลกระทบที่อาจติดตามมาได้มาก

เนื่องจากในปัจจุบันอัตรากรหมุนเวียนของพนักงานในศูนย์คอมพิวเตอร์ค่อนข้างสูงจึงเป็นสิ่งจำเป็นที่จะต้องเข้มงวดในการจัดทำมากขึ้น จากตัวอย่างที่เกิดขึ้นจริงธุรกิจแห่งหนึ่งพนักงานผู้พัฒนาโปรแกรมได้ลาออกไปโดยไม่จัดทำเอกสารสนับสนุนการปฏิบัติงาน เมื่อธุรกิจนั้นได้รับพนักงานใหม่เข้ามาและมอบหมายให้ดำเนินโปรแกรมระบบงาน นั้นต่อไปพนักงานใหม่ตอบทันทีว่าให้ผมเขียนระบบงานขึ้นใหม่ยังใช้เวลาน้อยกว่าที่จะมานั่งแกะระบบงานเก่าเพื่อเขียนเอกสารสนับสนุนระบบงาน ดังนั้น จึงต้องมีการยกเลิกระบบงานเก่าไป

4. ขั้นตอนการนำระบบงานใหม่เข้ามาใช้งาน

หลังจากที่ได้พัฒนาระบบงานหรือซื้อระบบงานใหม่มาเรียบร้อยแล้ว ขั้นตอนต่อไปก็คือ

4.1 การเปลี่ยนข้อมูลจากระบบงานเดิมให้อยู่ในรูปแบบของระบบงานใหม่

ขั้นตอนนี้เป็นขั้นตอนที่สำคัญต่อความถูกต้องของข้อมูลอย่างมาก เพราะเป็นการเปลี่ยนรูปแบบจากของเดิมให้อยู่ในรูปแบบของข้อมูลที่เครื่องคอมพิวเตอร์ของธนาคารใช้อยู่ในปัจจุบันอ่านได้ ดังนั้นผู้ตรวจสอบจะต้องตรวจสอบความถูกต้องของข้อมูลอย่างละเอียดโดยเฉพาะข้อมูลทางการเงิน ได้เคยมีธุรกิจบางแห่งได้ว่าจ้างให้บุคคลภายนอกทำการเปลี่ยนรูปแบบข้อมูลด้านการเงินให้ โดยไม่เฉลียวใจว่าผู้รับจ้างทำงานดังกล่าวมีความเชี่ยวชาญในการปฏิบัติงานทางด้านสถิติเท่าไร เมื่อผู้ว่าจ้างได้นำข้อมูลมาใช้งานปรากฏว่าข้อมูลดังกล่าวมีข้อผิดพลาดขึ้น จึงได้สอบถามผู้รับจ้างก็ได้คำตอบว่า การปฏิบัติงานของผู้รับจ้างข้อมูลผิดพลาดไม่เกินร้อยละ 10 ถือว่าข้อมูลถูกต้อง ซึ่งทำให้ผู้ว่าจ้างต้องเสียค่าใช้จ่ายในการแก้ไขข้อมูลให้ถูกต้องอีกเป็นจำนวนมาก

4.2 การปฏิบัติงานแบบคู่ขนาน

เป็นขั้นตอนหนึ่งที่สามารถตรวจสอบการทำงานของโปรแกรมระบบงานว่าถูกต้องเพียงใด โดยการปฏิบัติงานแบบเก่าควบคู่ไปกับการปฏิบัติงานแบบใหม่ชั่วระยะเวลาหนึ่งจนแน่ใจว่าระบบงานใหม่ใช้ได้ผลและสามารถดำเนินการต่อไปโดยไม่มีปัญหาเกี่ยวกับระบบงานเก่าไปใช้ระบบงานใหม่เพียงอย่างเดียว ดังนั้นผู้ตรวจสอบภายในจะต้องดำเนินการตรวจสอบอย่างใกล้ชิดว่ามีการใช้วิธีการปฏิบัติงานแบบคู่ขนานถูกต้องหรือไม่ เพราะเคยมีผู้ปฏิบัติงานของธุรกิจบางแห่งเข้าใจผิดว่าการประมวลผลด้วยคอมพิวเตอร์จัดเก็บข้อมูลไว้ในแฟ้มข้อมูลและในขณะเดียวกันก็พิมพ์ผลของการประมวลออกมาในการ์ดรายตัวลูกค้าด้วยเป็นการปฏิบัติงานแบบคู่ขนาน เป็นผลให้ไม่สามารถเช็คสอบความถูกต้องของการคำนวณดอกเบี้ยได้ เพราะไม่ได้ใช้การประมวลผลแบบเก่าที่ถูกต้องแล้ว ควบคู่ไปกับระบบงานใหม่ ซึ่งก่อให้เกิดความเสียหายให้แก่ธุรกิจนั้นได้

อย่างไรก็ดีการปฏิบัติงานแบบคู่ขนานเป็นวิธีการที่ดี แต่ต้องเสียค่าใช้จ่ายและเวลามากเพราะเป็นการทำงานแบบซ้ำซ้อนกัน 2 ระบบ ดังนั้นผู้ตรวจสอบภายในควรจะต้องติดตามการปฏิบัติงานแบบนี้อย่างใกล้ชิด เพื่อให้มีการปฏิบัติงานอย่างประหยัดและมีประสิทธิภาพเพราะมีธุรกิจบางแห่งได้ทำการใช้วิธีการปฏิบัติงานแบบคู่ขนานระหว่างระบบงานเก่ากับระบบงานใหม่เป็นเวลานานกว่า 4 ปีแล้วก็ยังไม่มีการยกเลิกระบบงานเก่าไปและยังไม่ทราบว่า จะยกเลิกการปฏิบัติงานเก่าไปเมื่อใด เพราะมีปัญหาระหว่างผู้ใช้ระบบงานกับผู้พัฒนาระบบงานและไม่มีใครรายงานให้ผู้บริหารทราบในปัญหาดังกล่าว ซึ่งเรื่องนี้พิจารณาได้ว่าเป็นความล้มเหลวของหน่วยงานตรวจสอบภายในและเป็นความล้มเหลวของผู้บริหารงานด้วย

5. ขั้นตอนการรักษาความปลอดภัยและลดความเสี่ยงภัยด้านคอมพิวเตอร์ด้วยการประกันภัย

การประกันภัยเป็นสิ่งที่ใหม่ที่ผู้ตรวจสอบภายในจะต้องศึกษาเรียนรู้เพราะเป็นการป้องกันความสูญเสียซึ่งอาจเกิดขึ้นจากภัยหรือความเสี่ยงที่ไม่สามารถป้องกันได้โดยสมบูรณ์ โดยทั่วไปการทำประกันภัยจะคำนึงถึงความสูญเสียทางธุรกิจและผลกระทบข้างเคียงที่เกิดขึ้นจากภัยนั้น ถ้าหากผู้ตรวจสอบภายในสามารถให้คำแนะนำต่อผู้บริหารได้ก็จะเพิ่มคุณค่าของผู้ตรวจสอบมากขึ้น การประกันภัยโดยหลักใหญ่ ๆ ที่มีอยู่ในปัจจุบันมี ดังนี้

- **การประกันภัยระบบคอมพิวเตอร์** เพื่อป้องกันความเสียหายทางกายภาพของเครื่องและอุปกรณ์ประกอบ การหยุดชะงักของธุรกิจ เอกสารหรือรายการบันทึกที่มีค่าและความสำคัญที่เทียบค่าเป็นเงินได้
- **การประกันภัยความผิดพลาดและบกพร่อง** เป็นการคุ้มครองกรณีที่เกิดการเรียกร้องความเสียหายเนื่องจากการปฏิบัติงานของที่เกี่ยวข้องกับด้านคอมพิวเตอร์ที่ให้บริการแก่บุคคลภายนอกและปรากฏข้อผิดพลาดขึ้น
- **การประกันภัยการขนส่งอุปกรณ์หรือแฟ้มข้อมูล** ในกรณีที่มีการขนส่งแฟ้มข้อมูลเพื่อไปจัดเก็บหรือประมวลผลภายนอกสถานที่ทำงาน การประกันประเภทนี้เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์หรือแฟ้มข้อมูลในระหว่างการขนส่ง
- **การประกันภัยระบบการโอนเงินอัตโนมัติ** เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์ต่าง ๆ หรือจากบุคคลภายนอกที่เกี่ยวกับอุปกรณ์คอมพิวเตอร์และอุปกรณ์ EFTS. ที่ติดตั้งนอกสถานที่ สถานที่ตั้ง ATM. และเครื่องจ่ายเงินสด

6. การทำสัญญาในการใช้บริการหรือให้บริการบุคคลภายนอก

ผู้ตรวจสอบภายในควรจะมีส่วนร่วมอย่างแข็งขันในการจัดทำสัญญาการใช้หรือการให้บริการด้านคอมพิวเตอร์แก่หรือจากบุคคลภายนอก (หากมี) เพราะผู้ตรวจสอบรู้ถึงวิธีการตรวจสอบและระบบการควบคุมภายในอย่างดีอยู่แล้ว ทั้งนี้เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อธนาคารได้

การทำสัญญาระหว่างธนาคารกับผู้รับบริการหรือผู้ให้บริการด้านคอมพิวเตอร์จะต้องระบุความรับผิดชอบของทั้ง 2 ฝ่าย เกี่ยวกับการใช้และการให้บริการด้านคอมพิวเตอร์ของธนาคารทั้งหมด เพราะหากสัญญาดังกล่าวไม่สมบูรณ์พออาจมีข้อโต้แย้งหรือหลีกเลี่ยงการชดเชยความเสียหายได้

เงื่อนไขในการจัดทำสัญญาการใช้หรือการให้บริการด้านคอมพิวเตอร์ควรมีดังนี้

- ระบุงานที่ใช้หรือให้บริการระยะเวลาในการประมวลผลและข้อมูลที่ปรากฏในรายงานต่าง ๆ ที่ได้จากการประมวลผล
- หลักการคำนวณค่าบริการที่เรียกเก็บจากผู้ให้บริการหรือจ่ายแก่ผู้ให้บริการ
- ตารางกำหนดเวลาในการรับส่งงานระหว่างผู้ให้บริการกับผู้ให้บริการ
- ความรับผิดชอบในการตรวจสอบรวมทั้งสิทธิของผู้ให้บริการในการส่งตัวแทนเข้าไปตรวจสอบการทำงานของผู้ให้บริการ
- ข้อตกลงในการจัดระบบสำรองและการป้องกันข้อมูลที่อาจเสียหาย เพื่อให้แน่ใจว่าศูนย์คอมพิวเตอร์ที่ให้บริการสามารถประมวลผลต่อไปได้แม้จะมีเหตุฉุกเฉินเกิดขึ้น
- ความรับผิดชอบในการขนส่งเอกสารข้อมูลต่าง ๆ ระหว่างผู้ให้บริการกับผู้ให้บริการ

- ให้มีการประกันภัยข้อมูลที่อาจเสียหายเนื่องจากการปฏิบัติงานผิดพลาดและบกพร่องละเลยไม่ปฏิบัติงานตามหน้าที่
- การรักษาความลับของข้อมูล
- การรักษาความปลอดภัยของข้อมูล
- สิทธิในการเป็นเจ้าของโปรแกรมและเอกสารที่เกี่ยวข้องที่ใช้ในการปฏิบัติงาน
- สิทธิในการเป็นเจ้าของ Master files, Transaction file รวมทั้งการส่งข้อมูลที่อยู่ในรูปแบบของภาษาเครื่องจักรดังกล่าวคือผู้รับบริการเมื่อสัญญาสิ้นสุดลง
- การเปลี่ยนแปลงราคาค่าบริการและวิธีการยกเลิกสัญญาหรือการถอนตัวจากการให้บริการหรือใช้บริการโดยฝ่ายหนึ่งฝ่ายใด รวมทั้งเวลาที่ใช้ในการเปลี่ยนแปลงข้างต้น
- ลำดับการปฏิบัติงานก่อนหลัง
- กำหนดให้ผู้ให้บริการแจ้งการเปลี่ยนแปลงระบบงานซึ่งมีผลกระทบต่อการปฏิบัติงานและรายงานที่ได้จากการประมวลผลให้ผู้ใช้บริการทราบ
- กำหนดความรับผิดชอบในการจัดทำคู่มือและเอกสารประกอบระบบงานและสิทธิของคู่มือและเอกสารประกอบระบบงานอื่น ๆ ให้ชัดเจน

หากมีข้อตกลงอื่นนอกเหนือจากที่กล่าวข้างต้นทั้ง 2 ฝ่าย ควรพิจารณาในข้อตกลงนั้นร่วมกันโดยละเอียด กล่าวโดยสรุป ผู้ตรวจสอบควรจะได้มีบทบาทช่วยฝ่ายบริหารในการพิจารณาและให้ความเห็นต่อการใช้หรือการให้บริการจาก/ต่อบุคคลภายนอกโดยพิจารณาถึงความเสี่ยงที่อาจเกิดขึ้นต่ออนาคตเป็นหลัก ซึ่งเรื่องนี้คงจะต้องขึ้นอยู่กับภูมิรู้และทักษะของผู้ตรวจสอบงานด้านคอมพิวเตอร์เป็นสำคัญ

อย่างไรก็ดี ข้อตกลงหรือสัญญาใด ๆ ระหว่างธนาคารพาณิชย์ผู้ใช้หรือผู้ให้บริการจาก/ต่อบุคคลภายนอกที่ขัดต่อกฎหมายหรือพระราชบัญญัติการธนาคารพาณิชย์จะไม่มีผลในการปฏิบัติต่อพนักงานเจ้าหน้าที่ผู้รักษาและปฏิบัติตามกฎหมายหรือพระราชบัญญัตินั้น



20

การทดสอบข้อมูลโดยวิธี

Test Data

การทดสอบข้อมูลโดยวิธี Test Data

1. เหตุผลและความจำเป็น

เนื่องจากการใช้คอมพิวเตอร์ประมวลผลข้อมูลทางธุรกิจเพิ่มมากขึ้นอย่างต่อเนื่องตามลำดับ ประกอบกับคอมพิวเตอร์รุ่นใหม่ ๆ มักมีระบบการทำงานตลอดจนเทคนิคที่ใช้สลับซับซ้อน ตลอดจนการใช้เทคนิคบางอย่างอาจเปลี่ยนแปลงรูปแบบ และระบบการทำงานไปจากระบบ MANUAL โดยสิ้นเชิง จึงก่อให้เกิดการตื่นตัวและท้าทายความสามารถของผู้ตรวจสอบเป็นอย่างยิ่ง ในปัจจุบันผู้ตรวจสอบจำนวนมากจึงได้หันมาใช้คอมพิวเตอร์ เป็นเครื่องมือช่วยในการปฏิบัติงานอย่างกว้างขวาง ทำให้วิธีการตรวจสอบพัฒนาไปเป็นอันมากด้วย

เครื่องมือและเทคนิคที่ใช้ในการตรวจสอบมี 2 กลุ่มใหญ่ ๆ คือ

1. เทคนิคการตรวจสอบคอมพิวเตอร์ที่ใช้ตรวจสอบภายหลังจากการประมวลผล
2. เทคนิคการตรวจสอบคอมพิวเตอร์ที่ใช้ตรวจสอบขณะที่ทำการประมวลผล

ซึ่งในแต่ละกลุ่มก็มีวิธีการตรวจสอบข้อมูลและโปรแกรม รวมทั้งระบบการทำงานถูกต้อง เชื่อถือได้หรือไม่ การใช้ Test Data จัดอยู่ในกลุ่มเทคนิคการตรวจสอบคอมพิวเตอร์ที่ใช้ตรวจสอบภายหลังจากการประมวลผล เป็นเทคนิคที่นิยมแพร่หลาย โดยมีเหตุผลของการนำมาใช้คือ

1. เพื่อทดสอบระบบการควบคุมภายในของโปรแกรม คือ

- พิจารณาว่าการประมวลผลรายการปกติถูกต้องหรือไม่
- พิจารณาว่าได้มีการพบรายการที่ไม่สมเหตุสมผล ไม่เหมาะสม ไม่สมบูรณ์ ไม่ถูกต้อง จากระบบ

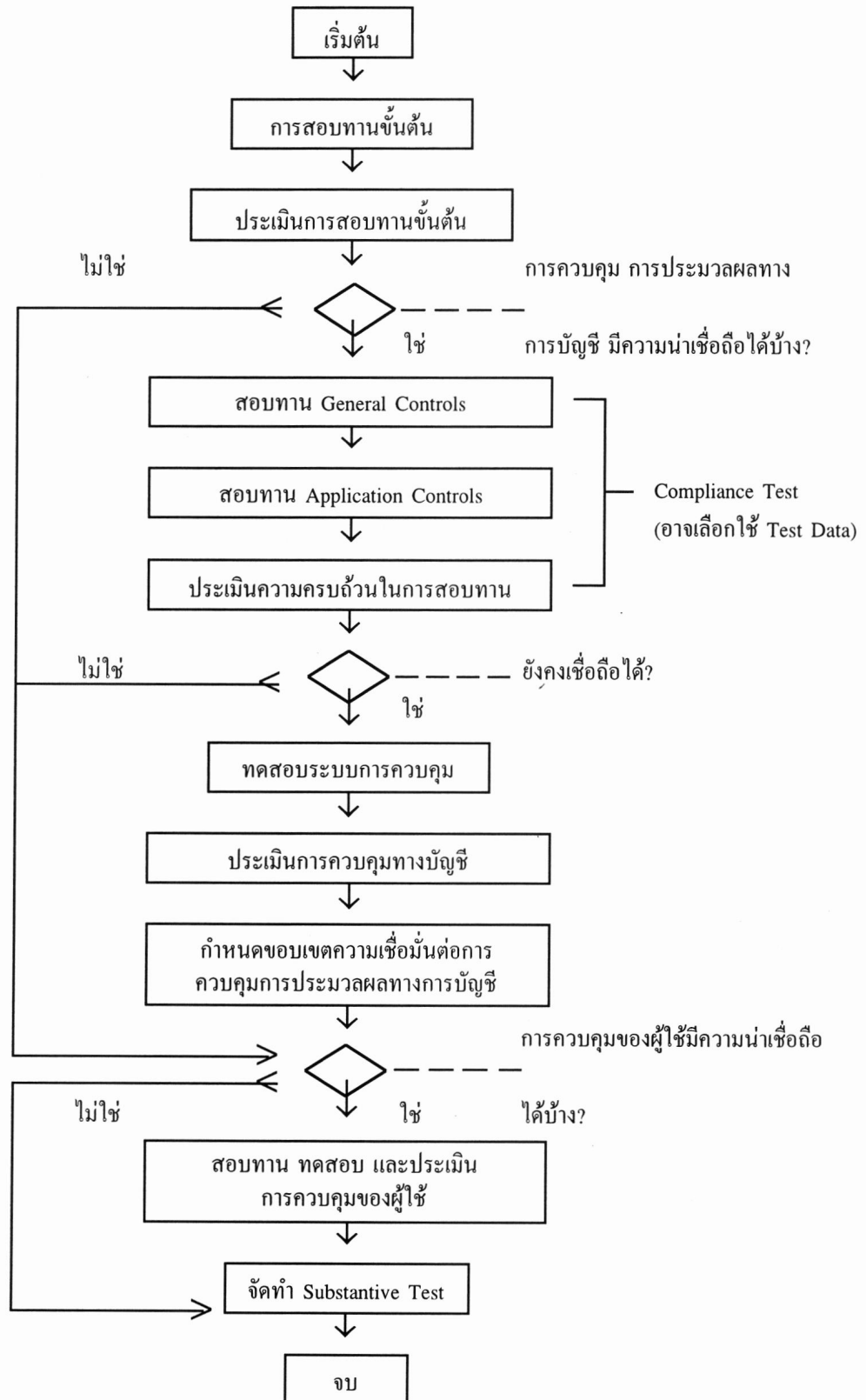
การควบคุมของโปรแกรม และมีการแก้ไขที่ถูกต้องหรือไม่

2. เป็นวิธีที่มีประสิทธิภาพในการยืนยันความเข้าใจของผู้สอบบัญชีต่อระบบงานที่สลับซับซ้อน ผู้ตรวจสอบอาจต้องการใช้ Test Data เพื่อช่วยเสริมสร้างความเข้าใจในระบบโปรแกรมบางอย่างภายหลังจากที่ศึกษาและประเมินการควบคุมภายในขั้นต้น ซึ่งการใช้ Test Data นี้แตกต่างจากการใช้เพื่อทดสอบการปฏิบัติตามระบบการควบคุมภายในที่ได้กำหนดไว้ ซึ่งเป็นข้อหนึ่งของการตรวจสอบ



2. การนำ Test Data มาใช้ในการตรวจสอบ

2.1 ขั้นตอนการตรวจสอบงานด้านคอมพิวเตอร์



จากผังแสดงขั้นตอนงานตรวจสอบงานด้านคอมพิวเตอร์ข้างต้น จะเห็นว่าเมื่อผู้ตรวจสอบเข้าทำการตรวจสอบ จะต้องศึกษาและประเมินประสิทธิภาพการควบคุมภายในเสียก่อน ทั้งนี้เพื่อกำหนดขอบเขต วิธีการตรวจสอบ และ ระยะเวลาที่จะใช้ หากผู้ตรวจสอบมีความพึงพอใจและเชื่อมั่นในระบบการควบคุมภายในของกิจการ ก็จะทำให้การ ทดสอบว่ามีการปฏิบัติตามระบบการควบคุมที่วางไว้หรือไม่ เรียกว่าทำ Compliance Test ซึ่งประกอบด้วยการสอบทาน General Controls และ Application Controls หากพบว่าระบบที่วางไว้แต่ยังไม่พอใจในการปฏิบัติตามระบบ ก็ ต้องพิจารณาว่ามีการควบคุมอย่างอื่นมาชดเชยหรือไม่ (เช่น การควบคุมทางด้านผู้ใช้) หากไม่มีก็ต้องจัดทำ Substantive Test ที่ครอบคลุมถึง 100% เพื่อให้ได้มาซึ่งหลักฐานในการยืนยันความถูกต้องของยอดคงเหลือทางบัญชี เช่นเดียวกับในกรณีที่ประเมินประสิทธิภาพการควบคุมภายใน แล้วผู้ตรวจสอบไม่มีความเชื่อถือในระบบก็ต้องจัดทำ Substantive Test 100% เช่นกัน

ในการจัดทำ Compliance Test และ Substantive Test ผู้ตรวจสอบสามารถเลือกใช้วิธีการตรวจสอบที่มีอยู่อย่างมากมายได้ตามความเหมาะสม "Test Data" เป็นเทคนิคอย่างหนึ่งที่สามารถเลือกใช้ในการทำ Compliance Test ภายหลังจากทำการศึกษาและประเมินประสิทธิภาพการควบคุมภายในแล้วมีความเชื่อถือในระบบพอสมควร ก็จะ ใช้ Test Data เพื่อทดสอบการปฏิบัติตามระบบการควบคุมภายในที่กำหนดไว้ แต่เทคนิคนี้ค่อนข้างจะเน้นการ ทดสอบการควบคุมภายในของ Program หรือ Application Software คือ การควบคุมด้านข้อมูลนำเข้า (Input) การประมวลผล (Processing) และข้อมูลผลลัพธ์ (Output)

2.2 การใช้ Test Data ตรวจสอบความถูกต้องของโปรแกรม

คอมพิวเตอร์จะทำงานถูกต้องหรือไม่ขึ้นอยู่กับการทำงานของโปรแกรม ดังนั้น ก่อนที่จะนำ โปรแกรมมาใช้งาน จึงต้องมีการทดสอบจนแน่ใจว่าโปรแกรมนั้นทำงานได้ถูกต้องสำหรับทุกประเภทรายการ การ ทดสอบโปรแกรมเป็นงานที่สำคัญในขั้นตอนการพัฒนาระบบงาน ผู้ตรวจสอบมีหน้าที่ตรวจสอบรายงาน และการแก้ไข ข้อผิดพลาด/บกพร่องของโปรแกรม จนมั่นใจได้ว่าการควบคุมภายในอย่างเพียงพอและเหมาะสม

วิธีการตรวจสอบความถูกต้องของโปรแกรมวิธีหนึ่ง คือ "การตรวจสอบจาก Source Program Listing" ผู้ตรวจสอบจะต้องไล่ดูทีละ Statement ตามลำดับ เพื่อค้นหาข้อผิดพลาดและจุดอ่อนของโปรแกรม ซึ่ง กระทำได้ยากในทางปฏิบัติ ด้วยเหตุผลดังต่อไปนี้

1) การตรวจสอบโปรแกรมต้องใช้ความรู้ความชำนาญในด้านโปรแกรมมากกว่าการเขียนโปรแกรม เองตั้งแต่ต้น และการติดตามรายละเอียดในโปรแกรมที่บรรจุคำสั่งนับพัน ทั้งยังมีขั้นตอนการประมวลผลที่สลับซับซ้อน ย่อมเป็นงานที่ยากลำบากยิ่ง ถึงแม้ผู้ตรวจสอบและผู้ช่วยจะเป็นผู้เชี่ยวชาญในด้านโปรแกรมก็ตาม นอกจากนี้ยังต้องใช้ เวลาและค่าใช้จ่ายสูงด้วย

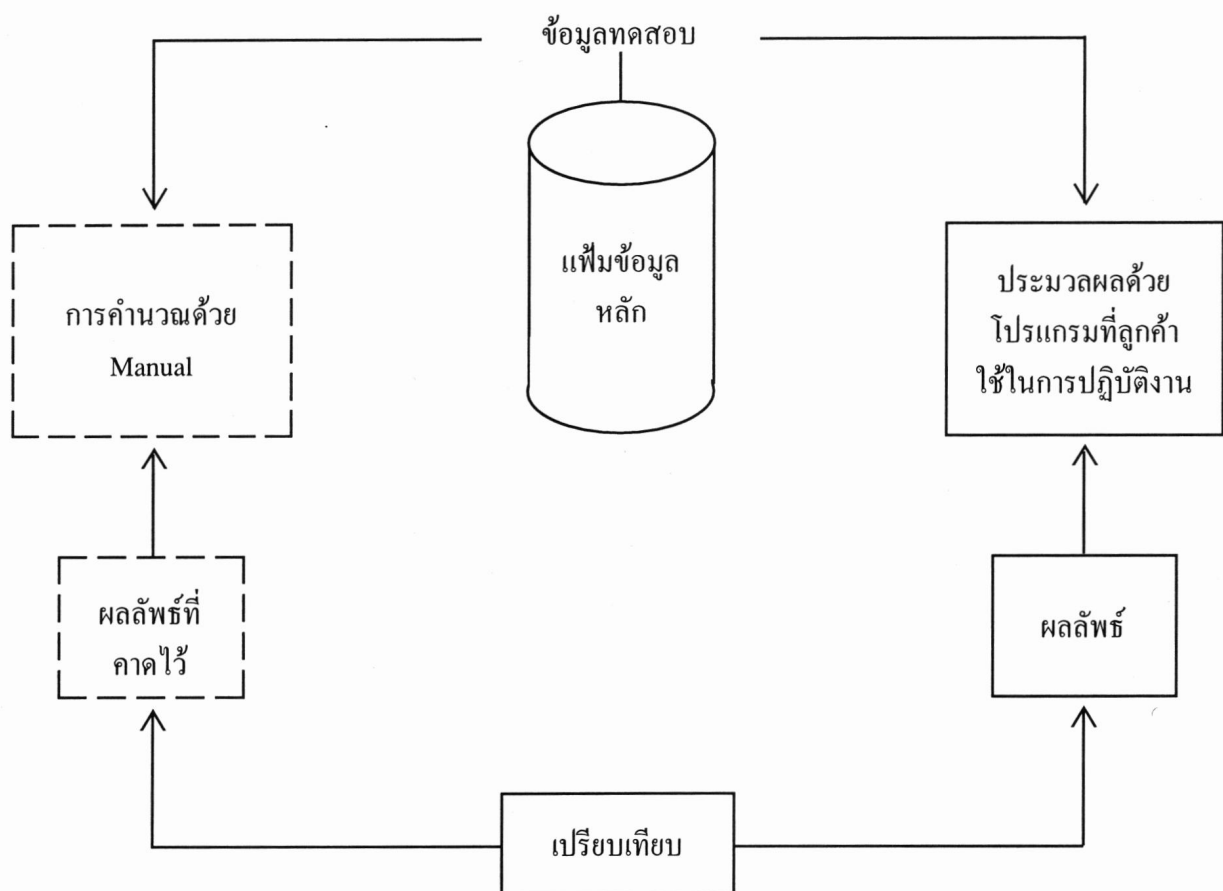
2) ผู้ตรวจสอบอาจมองข้ามจุดอ่อนเสียเอง การพัฒนาโปรแกรมให้ใช้งานได้จะต้องใช้เวลานาน และทำการทดสอบนับครั้งไม่ถ้วน การตรวจสอบในช่วงเวลาสั้น ๆ จึงไม่อาจมองแง่มุมต่าง ๆ ที่แฝงอยู่ได้อย่างถี่ถ้วน

3) โปรแกรมที่ใช่มักมีการเปลี่ยนแปลงแก้ไขอยู่ตลอดเวลา ถ้าผู้ตรวจสอบวางแผนการตรวจสอบ แบบกระจายเป็นระยะตลอดปีบัญชี การที่จะติดตามรายการเปลี่ยนแปลงซึ่งมีจำนวนมาก ทุกรายการย่อมเป็นไปได้ยาก ในทางปฏิบัติ

ด้วยเหตุผลดังกล่าว การตรวจสอบความถูกต้องของโปรแกรม จึงนิยมใช้วิธีการตรวจสอบทางอ้อมคือ การใช้เทคนิค Test Data มากกว่าการตรวจสอบจาก Source Program Listing

2.3 Test Data คือ อะไร

Test Data เป็นข้อมูล que ผู้ตรวจสอบจัดทำขึ้น เพื่อใช้ตรวจสอบความถูกต้องของการทำงานและการควบคุมของโปรแกรมระบบงาน โดยนำข้อมูลที่สมมติขึ้นไปประมวลผลกับโปรแกรมที่องค์การใช้อยู่จริงแล้วนำผลลัพธ์ที่ได้ไปเปรียบเทียบกับผลลัพธ์ที่ผู้ตรวจสอบคำนวณหรือคาดไว้ล่วงหน้าด้วย Manual ดังรูป



การใช้ตัวอย่างข้อมูลเพื่อประเมินคุณภาพของโปรแกรม เป็นเทคนิคเบื้องต้นในการเก็บรวบรวมหลักฐานอย่างหนึ่ง โดยตั้งอยู่บนพื้นฐานที่ว่าผู้ตรวจสอบจะให้ความเชื่อถือต่อโปรแกรมที่ใช้งาน หากผลการทดสอบเป็นที่น่าพอใจ

ผู้ตรวจสอบจะใช้เทคนิค Test Data ในการทดสอบและตรวจสอบประเด็นต่าง ๆ ดังต่อไปนี้

1. ขั้นตอนและวิธีการในการอนุมัติรายการข้อมูลนำเข้า การหาสาเหตุของข้อผิดพลาด และการควบคุมระบบงาน
2. ความสมเหตุสมผลของขั้นตอนการประมวลผล และการควบคุมการสร้างและปรับปรุงแก้ไขข้อมูลในแฟ้มข้อมูลหลัก
3. ความถูกต้องในการทำงานของโปรแกรมการคำนวณต่าง ๆ เช่น ดอกเบี้ย ค่าใช้จ่าย ค่าเสื่อมราคา
4. การบันทึกการเปลี่ยนแปลงแก้ไขโปรแกรม

3. ขั้นตอนการจัดทำ Test Data และตัวอย่าง

3.1 ขั้นตอนการจัดทำ Test Data

1. กำหนดวัตถุประสงค์หรือเป้าหมายของการทดสอบในแต่ละเรื่องของกิจกรรม ที่พิจารณาว่าอาจก่อให้เกิดความเสี่ยง
2. กำหนดจำนวนรอบเวลาบัญชีหรือข้อมูล (Cycle) ที่จะใช้ในการทดสอบให้สอดคล้องกับเป้าหมายของการทดสอบที่กำหนดไว้
3. สร้างเงื่อนไขหรือประเภทของรายการที่จะทดสอบให้สัมพันธ์กับเป้าหมาย ให้สามารถคาดคะเนผลลัพธ์ที่จะออกมาได้
4. จัดเตรียมข้อมูลที่จะทดสอบตามเงื่อนไขที่ได้สร้างไว้ และจำแนกตามรอบเวลา (Cycle) ที่ได้กำหนดไว้
5. คำนวณผลลัพธ์ที่คาดว่าจะได้รับด้วย Manual (ขั้นตอนนี้จะเป็นการฝึกฝนและเพิ่มพูนความเข้าใจของผู้ตรวจสอบ ต่อระบบงานที่ตรวจสอบได้โดยละเอียด)
6. ประมวลผลข้อมูลทดสอบที่ได้เตรียมไว้ ตามกระบวนการที่กำหนดไว้ในการประมวลงานตามปกติ
7. ตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ โดยนำไปเปรียบเทียบกับผลลัพธ์ที่คาดว่าจะได้รับตามที่คำนวณได้ด้วย Manual
8. สรุปผลการทดสอบและระบุจุดอ่อนที่พบ ซึ่งผู้ตรวจสอบจะต้องระบุสาเหตุของจุดอ่อนแต่ละประเด็น และให้คำแนะนำในการปรับปรุงแก้ไข

3.2 ตัวอย่างขั้นตอนการจัดทำ Test Data ในระบบ On-line

เป็นตัวอย่างการปฏิบัติงานตรวจสอบระบบเงินฝากของธนาคารพาณิชย์โดยทั่ว ๆ ไป ซึ่งการปฏิบัติงานจริงในแต่ละธนาคารอาจมีรายละเอียดบางอย่างแตกต่างกันไปบ้าง

3.2.1 การเตรียมการก่อนการทดสอบ

1. ต้องศึกษาและทำความเข้าใจในระบบการปฏิบัติงานของธนาคารก่อนลงมือทดสอบในแต่ละระบบอย่างละเอียด
2. ต้องศึกษาและทำความเข้าใจใน Format และ Transaction Code ต่าง ๆ
3. ทำความเข้าใจในระบบการจัดเก็บ File และ Program ของระบบงานต่าง ๆ
4. ทำความเข้าใจในการทำ Copy ข้อมูลและโปรแกรมที่จะนำมาใช้ในการทดสอบ
5. ทำความเข้าใจและเจรจากับหัวหน้าศูนย์คอมพิวเตอร์ของธนาคารในเรื่องต่อไปนี้
 - 5.1 เวลาที่จะเริ่มทำการทดสอบ
 - 5.2 ระยะเวลาที่จะใช้สำหรับการทดสอบ
 - 5.3 ชื่อ Report ที่จะขอให้ธนาคารพิมพ์มีทั้งสิ้นเท่าใด
 - 5.4 Printer และ Keyboard ที่จะใช้สำหรับการทดสอบมีจำนวนเท่าใด
 - 5.5 เจ้าหน้าที่ผู้ประสานงานของธนาคารมีกี่คน และใครบ้าง
 - 5.6 Passbook หรือ Slip ต่าง ๆ ที่จะใช้สำหรับการทดสอบ จะต้องเตรียมการไว้ให้พร้อม เช่น Debit Slip, Credit Slip และ Transfer Slip รวมทั้งแบบพิมพ์อื่น ๆ ที่เกี่ยวข้อง
 - 5.7 ในกรณีที่ธนาคารมีเครื่องคอมพิวเตอร์จำกัด ก็จะต้องทราบว่าหลังจากเสร็จสิ้นงาน On-line แล้ว จะต้องทำงาน Batch อีกนานเท่าใด จึงสามารถเริ่มต้นให้เวลาสำหรับการ Test Data การออก Report และการ Load ข้อมูลกลับเข้าไปในเครื่อง เพื่อทำงานปกติของธนาคารต่อไปได้
 - 5.8 ให้ธนาคารเตรียม PASS-WORD และ USER-ID กับกุญแจเครื่องของเจ้าหน้าที่ระดับ Authorized แล้วจะเปลี่ยนแปลงใหม่ เมื่อการทดสอบข้อมูลเสร็จสิ้นลงแล้ว
6. สร้าง Logic และข้อมูลต่าง ๆ เพื่อใช้สำหรับการทดสอบ การสร้างข้อมูลนี้จะต้องคำนึงถึงความสะดวกและจุดมุ่งหมาย ในการทดสอบด้วย คือ
 - 6.1 สร้างข้อมูลขึ้นมาใหม่ทั้งหมด วิธีนี้จะต้องเปิดบัญชีขึ้นมาใหม่ สร้างรายการทั้งที่เกี่ยวกับตัวเลขและประวัติที่อยู่ของลูกค้าขึ้นมาใหม่ทั้งหมด คงจะเสียเวลาไปบ้างแต่จะได้ประโยชน์สำหรับการทำงานของเครื่อง คือใช้เวลาในการ Sort และการออก Report สั้นและเร็ว เพราะมีจำนวน Data เฉพาะส่วนที่ Key เข้าไปเท่านั้น
 - 6.2 ใช้ข้อมูลหรือบัญชีเดิมของธนาคารมาทำรายการต่อไป เช่น ยอดคงเหลือวงเงินต่าง ๆ Clearing Cheque จะมีการเปิดบัญชีและเพิ่มเติมข้อมูลใหม่เข้าไปบ้าง แต่จะน้อยกว่าการสร้างบัญชีขึ้นมาใหม่ วิธีการนี้จะทำให้ใช้เวลาสำหรับการ Key สั้นลง เพราะมีข้อมูลอยู่ใน File แล้วจำนวนหนึ่ง แต่จะมีข้อเสียคือ ใช้เวลา

ในการทำงานของเครื่องมาก เพราะการ Sort การออก Report จะใช้เวลา
นานเนื่องจากมีจำนวน Data อยู่ใน File มาก

ในเรื่องนี้ ผู้ตรวจสอบจะต้องตัดสินใจให้ได้ก่อน แล้วจึงแจ้งแก่ธนาคารให้เตรียมการล่วงหน้าก่อนการทดสอบ เพราะมีบางครั้งที่ธนาคารไม่สามารถจะสนองความต้องการของผู้ตรวจสอบได้ เช่น ธนาคารนัดให้ทำการทดสอบแล้ว แต่พอถึงเวลาจริงธนาคารไม่สามารถจะหา Tape ม้วนที่ Copy ไว้ได้ หรือการทำ Copy Data File ผิดพลาดจึงต้องเปลี่ยนเวลาในการทำ Test Data ออกไปใหม่อีก

7. ผู้ตรวจสอบจะต้องแบ่งงานการทดสอบออกเป็นระบบงาน และแยกความรับผิดชอบเป็นรายบุคคล เพื่อไม่ให้เกิดความยุ่งยากสับสนและอาจทำให้ล่าช้าลงได้
8. ต้องพยายามแบ่งงานการ Key ให้เสร็จไปพร้อม ๆ กันทุกงานโดยเฉพาะการปลด Lock cheque ควรจะทำไปในเวลาพร้อม ๆ กัน หรือใกล้เคียงกัน เพื่อบริหารเวลาให้สูญเสียให้น้อยที่สุด เพราะหากงานหนึ่งเสร็จก่อน แต่จะทำรายการต่อไปไม่ได้ ต้องรอให้ปลด Lock cheque ก่อน ในขณะที่เดียวกันงานอื่นยังไม่สามารถให้ทำรายการปลด Lock cheque ได้ จึงทำให้งานที่ทำเสร็จก่อนต้องเสียเวลารอคอย

3.2.2 ระหว่างการ Key ข้อมูล

1. ต้องแจ้งให้ธนาคารทราบว่าเป็นวันที่ในระบบงานที่กำหนดให้ทำ Test Data เป็นวันเดือนปีใด Yesterday และ Next day เป็นวันที่เท่าใด Clearing Hold ก็วันทั้งนี้เพื่อใช้สำหรับการออกวันที่ใน Report และการคิดดอกเบี้ย ฯลฯ
2. ผู้ตรวจสอบควรจะต้องมีโจทย์ไว้ 2 ชุด คือ ชุดรูปถ่ายที่ไม่มีผลที่คาดว่าจะเกิดขึ้น มอบให้แก่ Operator 1 ชุด เพื่อใช้สำหรับ Key ได้อย่างรวดเร็ว ส่วนอีกชุดหนึ่งมีผลที่คาดว่าจะเกิดขึ้น (Expectation) ผู้ตรวจสอบจะต้องถือไว้คอยกำกับการ Key และจด Output หรือ Response ที่เครื่องแสดงออกมา
3. ในระหว่างที่ Operator ทำการ Key แล้ว แจ้งแก่ผู้ตรวจสอบว่าอาจจะ Key ไม่ได้หรือขัดข้องน่าจะขอข้ามไปหรือแก้ไขโจทย์ได้หรือไม่
ผู้ตรวจสอบจะต้องเข้าใจว่าเป็นการทดสอบข้อมูล จึงไม่ควรที่จะยินยอมให้ข้ามไป หรือแก้ไขโจทย์ ควรจะให้ลองทำดูแล้วจดผลลัพธ์ที่ได้ก่อน แล้วจึงทำ Step ต่อไป
4. ก่อนการปลด Lock cheque clearing อย่าลืมให้ Operator ผู้รับผิดชอบทำรายการ Key รายละเอียดเช็คฉบับที่คืน (Return Cheque) เสียก่อนหากไม่ทำ Step นี้ โดยปลด Lock เช็คแล้วจะถือว่าทั้งหมดผ่านการ Clearing

3.2.3 เมื่อเสร็จสิ้นการ Key

1. เมื่อเสร็จสิ้นการ Key ข้อมูลแล้ว ควรจะให้มีการพิมพ์รายละเอียดและยอดรวมของ Teller ทุกคน
2. ขอให้ออก Journal Rool จากเครื่อง Printer และเก็บajoทย์ที่มอบให้แก่ Operater กลับคืนโดยครบถ้วน
3. ก่อนจะปิดเครื่อง ตรวจสอบ PASS-BOOK และ SLIP ต่าง ๆ ว่าได้รับคืนมาครบถ้วนหรือไม่ เพราะบางธนาคารหากปิดเครื่องไปแล้วจะให้เปิดและทำรายการใหม่ไม่ได้
4. ตรวจสอบ Report ที่ได้รับว่าครบถ้วนตามที่ต้องการหรือไม่

4. ข้อควรพิจารณาในการจัดทำ Test Data

1. ความถี่ในการใช้ Test Data ทดสอบโปรแกรมขึ้นอยู่กับ การเปลี่ยนแปลงแก้ไขโปรแกรม เนื่องจากเทคนิคนี้ใช้ในการประเมินการควบคุมและความถูกต้องเหมาะสมของโปรแกรมได้เฉพาะช่วงเวลาที่ทดสอบเท่านั้น
2. ผู้ตรวจสอบต้องศึกษากระบวนการให้เข้าใจโดยละเอียด เพื่อเป็นแนวทางในการกำหนดวัตถุประสงค์และประเด็นที่จะทดสอบได้อย่างมีประสิทธิภาพและครอบคลุมถึงการควบคุมที่สำคัญได้ครบถ้วน
3. ระบบงาน On-line ขนาดใหญ่ที่ยุ่งยากซับซ้อน การใช้เทคนิค Test Data จะทำได้ยากในทางปฏิบัติ เนื่องจากจะมีอุปสรรคในการจัดเตรียมอุปกรณ์คอมพิวเตอร์ และแฟ้มข้อมูลสำหรับการทดสอบประกอบกับผู้ตรวจสอบจะต้องเสียเวลามากในการศึกษากระบวนการให้เข้าใจโดยละเอียด
4. ต้องแน่ใจว่าโปรแกรมที่จะนำมาประมวลผลต้องเป็นโปรแกรมเดียวกับที่ใช้ในการปฏิบัติงานจริง โดยเปรียบเทียบชื่อและเลขที่โปรแกรมที่นำมาใช้ กับที่บันทึกไว้ในทะเบียนการนำมาใช้การประมวลผลงานตามปกติครั้งล่าสุด
5. ควรใช้โปรแกรมที่ได้แปลงรหัสแล้วพร้อมที่จะนำมาประมวลผลได้ทันที ไม่ควรใช้โปรแกรมที่ได้จากการนำ Source Program มาแปลงรหัสใหม่เมื่อนำมาประมวลผลข้อมูลทดสอบโดยเฉพาะ
6. แฟ้มข้อมูลและรายการทดสอบต้องไม่ปะปนกับข้อมูลจริงที่องค์การใช้งานอยู่ ควรป้องกันมิให้ข้อมูลที่ใช้งานอยู่มีข้อผิดพลาด
7. ควรกำหนดให้มีจำนวน cycle มากพอที่จะทดสอบได้ครอบคลุมทุกเงื่อนไขและสามารถทดสอบรายการที่ได้ป้อนข้อมูลผิดพลาดไปแล้วเมื่อ cycle ก่อน ๆ ได้
8. ควรพยายามจำกัดปริมาณข้อมูลทดสอบไม่ให้มีมากนัก เพื่อให้ผู้ตรวจสอบจะได้มีเวลาในการเตรียมข้อมูลวิเคราะห์ผลลัพธ์ และเวลาในการทำงานของเครื่องคอมพิวเตอร์ให้น้อยที่สุด
9. ควรจำกัดบุคคลที่จะได้รับอนุญาตให้ดูผลการทดสอบเฉพาะแต่เพียงผู้ตรวจสอบเท่านั้น ไม่ควรเปิดโอกาสให้บุคคลอื่นได้พบเห็น

5. ข้อดี ข้อเสีย ของการ Test Data มาใช้งาน

ข้อดี

1. ไม่จำเป็นต้องใช้บุคลากรที่มีความรู้ความชำนาญสูงในการเตรียมข้อมูลทดสอบ
2. การใช้ Test Data เป็นการรวมรายการธุรกิจ ตลอดจนรายการผิดปกติประเภทต่าง ๆ ไว้ด้วยกัน ทำให้ผู้ตรวจสอบสามารถพบข้อผิดพลาด/บกพร่องในโปรแกรมได้ง่ายกว่าที่จะตรวจสอบผลลัพธ์จากการประมวลผลโดยปกติ ซึ่งอาจจะต้องตรวจสอบนับพันรายการ จึงจะสามารถครอบคลุมรายการผิดปกติทั้งสิ้น เนื่องจากรายการเหล่านี้ อาจมีโอกาสดำเนินขึ้นจริงน้อยมาก
3. ในกรณีที่มีการแก้ไขโปรแกรมภายหลังจากที่ทำการตรวจสอบไปแล้ว ผู้ตรวจสอบสามารถทดสอบโปรแกรมได้ใหม่โดยใช้ Test Data ชุดเดิม โดยอาจเพียงแต่เพิ่มรายการทดสอบบางรายการ เพื่อให้ครอบคลุมถึงประเด็นเพิ่มเติมที่ต้องการทดสอบ แทนการสร้างข้อมูลทดสอบใหม่ทั้งหมด
โดยทั่วไปองค์กรจะไม่เปลี่ยนแปลงระบบงานโดยสิ้นเชิงในช่วงระยะเวลาอันสั้น ดังนั้น เมื่อผู้ตรวจสอบได้จัดเตรียม Test Data ในครั้งแรกแล้ว จะสามารถใช้ Test Data ชุดเดิมทำการทดสอบโปรแกรมได้ไม่จำกัดจำนวนครั้ง ซึ่งต่างจากการตรวจสอบ Source Program Listing ที่ต้องตรวจสอบใหม่โดยละเอียดทุกครั้งเมื่อมีการแก้ไขโปรแกรม เพราะการแก้ไขจุดใดจุดหนึ่งอาจกระทบถึงส่วนอื่น ๆ ของโปรแกรมด้วย
4. ผู้ตรวจสอบสามารถใช้ผลลัพธ์จากการทดสอบเป็นหลักฐานในการปฏิบัติงานตรวจสอบของตน
5. ในการเตรียมข้อมูล Test Data และคำนวณผลลัพธ์ที่คาดหวังไว้ล่วงหน้าตรวจสอบไม่จำเป็นต้องเกี่ยวข้องกับขั้นตอนการประมวลผลข้อมูลด้วยคอมพิวเตอร์มากนัก

ข้อเสีย

1. วิธีนี้จะทำการทดสอบได้เฉพาะบางจุดของโปรแกรม ได้แก่ การควบคุมที่กำหนดและการคำนวณเท่านั้น ไม่สามารถตรวจสอบโปรแกรมได้โดยละเอียดทุกขั้นตอน จึงไม่สามารถตรวจพบการทุจริตประเภท Trojan Horse (เป็นการแทรกคำสั่งที่ต้องการเพื่อการทุจริตแฝงอยู่ในโปรแกรมการทำงานปกติขององค์กร) ได้
ดังนั้น ผู้ตรวจสอบควรตรวจสอบ Source Program Listing ควบคู่ไปด้วย โดยเน้นเฉพาะการค้นหาคำสั่งผิดปกติที่ประมวลผลรายการใดรายการหนึ่งเป็นกรณีพิเศษ
2. ผู้ตรวจสอบต้องเสียเวลามากในการจัดเตรียม Test Data และคำนวณผลลัพธ์ที่คาดหวังไว้ล่วงหน้า
3. การใช้ Test Data บางครั้งอาจจะต้องใช้เวลาการทำงานของเครื่องคอมพิวเตอร์ในการประมวลผลเป็นเวลานาน ซึ่งทำให้ต้องเสียค่าใช้จ่ายสูง
4. ประสิทธิภาพและประสิทธิผลที่จะได้รับ ขึ้นอยู่กับความสามารถของผู้ตรวจสอบแต่ละคน ผู้ตรวจสอบอาจมองข้ามประเด็นสำคัญที่ควรทดสอบไปได้

6. ตัวอย่างการจัดทำ Test Data อย่างง่าย ๆ

ในระบบงานเงินฝากของธนาคารพาณิชย์ การจัดทำ Test Data อาจจำแนกตาม จำนวน Cycle ที่จัดทำได้ดังนี้

6.1 Test Data 1 Cycle

ตัวอย่างที่ 1

วัตถุประสงค์ : ทดสอบการควบคุมเลขที่บัญชี
เงื่อนไข : ฝากหรือถอนโดยใช้เลขที่บัญชีที่ปิดไปแล้ว
ข้อมูลทดสอบ : บัญชีเงินฝากประจำ 12 เดือน มีข้อมูลทดสอบดังนี้

วัน/เดือน/ปี	รายการ	จำนวนเงิน
15/02/86	เปิดบัญชีโดยเงินสด	50,000
15/02/87	ดอกเบี้ย (สุทธิจากภาษี)	3,000
16/02/87	ปิดบัญชี - ถอนเงินสด	53,000
=====> 20/02/87	ฝากเงินสด	70,000

ผลที่คาดหวัง : ปฏิเสธ

ผลจากการทดสอบ : ถ้าปฏิเสธ-----> ระบบงานมีการควบคุมแล้ว
ยอมรับ -----> ระบบงานไม่มีการควบคุม เป็นช่องทางให้ทุจริตได้
โดยเอาเลขที่บัญชีที่ปิดแล้วไปใช้อีก

ตัวอย่างที่ 2

วัตถุประสงค์ : ทดสอบการควบคุมการนำเช็คมาถอนเงินสด
เงื่อนไข : ถอนเงินสด 2 ครั้ง โดยใช้เช็คเลขที่เดียวกัน
ข้อมูลทดสอบ : บัญชีเงินฝากกระแสรายวัน มีข้อมูลทดสอบดังนี้

วัน/เดือน/ปี	รายการ	เลขที่เช็ค	จำนวนเงิน
23/08/88	ถอนเงินสด	1234567	50,000
27/08/88	"	1234568	20,000
=====> 09/09/88	"	1234567	70,000

ผลที่คาดหวัง : ปฏิเสธ

ผลจากการทดสอบ : ถ้าปฏิเสธ-----> ระบบงานมีการควบคุมแล้ว
ยอมรับ -----> อาจก่อให้เกิดการทุจริตทางคอมพิวเตอร์
โดยจัดทำเช็คปลอมด้วยเช็คเลขที่ที่เคยนำมา
ถอนเงินแล้ว นำมาขึ้นเงินสดอีกครั้งหนึ่ง

ตัวอย่างที่ 3

วัตถุประสงค์ : ทดสอบการจำกัดจำนวนเงินการบันทึกรายการของ
Teller/Authorized

เงื่อนไข : ฝากหรือถอนเกินวงเงินที่กำหนดไว้ของ Teller/Authorized

ข้อมูลทดสอบ : วงเงินของ Teller ในการบันทึกรายการฝาก = 200,000
-----"----- = 100,000

บัญชีเงินฝากออมทรัพย์มีข้อมูลทดสอบ ดังนี้

	วัน/เดือน/ปี	รายการ	จำนวนเงิน
=====>	25/09/88	ฝากเงินสด	700,000
=====>	03/10/88	ถอนเงินสด	153,700

ผลที่คาดหวัง : ต้องผ่านอนุมัติจาก รับมอบอำนาจ

ผลจากการทดสอบ : ถ้าปฏิเสธ-----> ระบบงานมีการควบคุมที่เข้มงวดจนเกินไปไม่มี
ความคล่องตัวในการปฏิบัติงาน

ยอมรับ -----> ขาดการควบคุมภายในที่ดี เป็นช่องทางให้ Teller
ทุจริตได้ เช่น บ่อนรายการฝาก/ถอนด้วยจำนวน
เงินสูง ๆ แล้วลักลอบเงินจำนวนนั้นไป

ต้องผ่านการอนุมัติ -----> มีการควบคุมภายในที่ดีและมีความคล่องตัว
ในการปฏิบัติงาน



ตัวอย่างที่ 4

วัตถุประสงค์ : ทดสอบการควบคุมการบันทึกรายการแก้ไข

เงื่อนไข : ฝากเช็คเคลียร์แล้วแก้ไขรายการฝากนั้น

ข้อมูลทดสอบ : บัญชีเงินฝากประจำ มียอดคงเหลือยกมาและข้อมูลทดสอบดังนี้

วัน/เดือน/ปี	รายการ	จำนวนเงิน	จำนวนเงิน
24/07/88	ยกมา	-	74,932
24/07/88	ฝากเช็คเคลียร์	25,000	99,932
=====> 24/07/88	แก้ไขรายการฝากเช็คเคลียร์	35,000	64,932

ผลที่คาดหวัง : ปฏิเสธ

ผลจากการทดสอบ : ถ้า 1) ยอมรับ-----> ระบบงานไม่มีการตรวจสอบรายการเบื้องต้น
(Original Transaction) ก่อนการแก้ไขรายการ

จากการตรวจสอบ report หัก

(1.1) ยอดคงเหลือเท่ากับ 64,932 แสดงว่าการคำนวณตัวเลขหลังจากแก้ไขถูกต้อง

(1.2) " ไม่เท่ากับ 64,932 " ไม่ถูกต้อง

2) ปฏิเสธ-----> ระบบงานมีการตรวจสอบรายการเบื้องต้น
(Original Transaction) ก่อนการแก้ไข
รายการเพราะฉะนั้นมีการควบคุมดีแล้ว



ตัวอย่างที่ 5

วัตถุประสงค์ : ทดสอบความถูกต้องของการแก้ไขรายการ

เงื่อนไข : ถอนเงินสดแล้วแก้ไขรายการถอนนั้น

ข้อมูลทดสอบ : บัญชีเงินฝากออมทรัพย์ มียอดคงเหลือยกมา และข้อมูลทดสอบดังนี้

วัน/เดือน/ปี	รายการ	จำนวนเงิน	จำนวนเงิน
04/09/88	ยอดยกมา	—	350,000
04/09/88	ถอนเงินสด	45,000	305,000
=====> 04/09/88	แก้ไขรายการถอนเงินสด	45,000	350,000

ผลที่คาดว่าจะได้ : 1. ยอมรับ
2. ยอดคงเหลือ = 350,000

ผลจากการทดสอบ : ถ้ายอมรับ ----> ระบบงานยินยอมให้มีการแก้ไขข้อผิดพลาด
ของการบันทึกรายการ แต่ไม่ได้หมายความว่า
การแก้ไขนั้นจะเชื่อถือได้ว่าถูกต้อง

เพราะฉะนั้น ต้องตรวจสอบ report ว่ายอดคงเหลือ = 350,000 จึงจะเชื่อถือได้ว่าถูกต้อง



ตัวอย่างที่ 6

วัตถุประสงค์ : ทดสอบความถูกต้องของการแก้ไขรายการ
เงื่อนไข : ถอนเงินสดโดยใช้เลขที่เช็คเดียวกับเลขที่เช็คที่เคยใช้และได้แก้ไขรายการแล้ว
ข้อมูลทดสอบ : บัญชีเงินฝากกระแสรายวัน มีข้อมูลทดสอบดังนี้

วัน/เดือน/ปี	รายการ	เลขที่เช็ค	จำนวนเงิน
04/09/88	ถอนเงินสด	475932	100,000
04/09/88	แก้ไขรายการถอนเงินสด	475932	100,000
=====> 04/09/88	ถอนเงินสด	475932	100,000

ผลที่คาดหวัง : ยอมรับ

ผลจากการทดสอบ : ถ้ายอมรับ ---->

รหัสประเภทรายการแก้ไขรายการ
ทำงานได้ถูกต้อง

ปฏิเสธ ---->

รหัสประเภทรายการแก้ไขรายการ
ทำงานไม่ถูกต้อง

การแก้ไขรายการไม่ได้ล้างข้อมูลของรายการเดิมออกทั้งหมด

หมายเหตุ : การสร้างข้อมูลทดสอบชุดนี้ ควรทำหลังจากได้ทดสอบแล้วว่า ระบบงานมีการควบคุม
เลขที่เช็คนำมาใช้ถอนเงิน



6.2 การ Test Data 2 Cycles

ตัวอย่างที่ 1

วัตถุประสงค์ : ทดสอบความถูกต้องของการบันทึกรายการเช็คคืน
เงื่อนไข : บันทึกรายการเช็คคืนโดยไม่มีรายการนำฝากเช็คเคลียร์วันก่อน
ข้อมูลทดสอบ : บัญชีเงินฝากประจำ 12 เดือน มีข้อมูลทดสอบดังนี้

วัน/เดือน/ปี	รายการ	จำนวนเงิน	ยอดคงเหลือ
13/02/89	ยอดยกมา	-	70,000
13/02/89 (C.1)	ฝากเงินสด	3,000	73,000
=====> 14/02/89 (C.1)	เช็คคืน	3,000	

ผลที่คาดหวัง : ปฏิเสธ

ผลจากการทดสอบ : ถ้าปฏิเสธ ----> ระบบงานมีการควบคุมและตรวจสอบแล้วว่า
ต้องมีเช็คนำฝากในวันก่อนวันบันทึกรายการ
เช็คคืน
ยอมรับ ----> ระบบงานไม่มีการควบคุมดังกล่าว ทำให้ลูกค้า
อาจได้รับความเสียหาย หากพนักงาน
บันทึกรายการเช็คคืนให้ลูกค้าผิดรายการหรือใช้
รหัสประเภทรายการผิดพลาด



ตัวอย่างที่ 2

วัตถุประสงค์ : ทดสอบความถูกต้องของการบันทึกรายการเช็คคืน

เงื่อนไข : บันทึกรายการเช็คคืนด้วยจำนวนเงินมากกว่าเช็คนำเข้าเมื่อวาน

ข้อมูลทดสอบ : บัญชีเงินฝากออมทรัพย์ มีข้อมูลทดสอบดังนี้

วัน/เดือน/ปี	รายการ	จำนวนเงิน
25/03/88 (C.1)	ฝากเช็ค	10,000
25/03/88 (C.1)	ฝากเงินสด	3,000
=====> 26/03/88 (C.2)	เช็คคืน	13,000

ผลที่คาดหวัง : ปฏิเสธ

ผลจากการทดสอบ : ถ้าปฏิเสธ ----> ระบบงานมีการควบคุมแล้ว
ยอมรับ ----> ระบบงานไม่มีการควบคุม ทำให้การคำนวณ
ดอกเบี้ยและยอดคงเหลือผิดพลาด



ตัวอย่างที่ 3

วัตถุประสงค์ : ทดสอบการคำนวณดอกเบี้ยกรณีเช็คคืน
เงื่อนไข : เลือกบัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถาม (C/A) ที่มียอดสุทธิเป็นเงินเบิกเกินบัญชี (ตัวแดง) เพื่อฝากเช็ค CL เข้า ทำให้ยอดสุทธิเป็นยอดคงเหลือ (ตัวดำ) แล้วมีเช็คคืนในวันถัดไป

ข้อมูลทดสอบ : บัญชีเงินฝากที่ต้องจ่ายคืนเมื่อทวงถามและเงินเบิกเกินบัญชี (C/A) มีข้อมูลทดสอบดังนี้

CYCLE 1 : ฝากเช็ค CL จนทำให้ Bal. เป็นตัวดำ

CYCLE 2 : เช็คคืนด้วยจำนวนเงินเท่ากับเช็คที่ฝากเข้าเมื่อ Cycle 1

วัน/เดือน/ปี	รายการ	จำนวนเงิน	ยอดคงเหลือ
01/03/89 (C.1)	ยอดยกมา		- 4,900
30/03/89 (C.1)	ฝากเช็ค CL	7,000	2,100
=====> 31/03/89 (C.2)	เช็คคืน	7,000	- 4,900

ผลที่คาดว่าจะได้ : - ยอมรับ
- สมมติว่าอัตราดอกเบี้ย = 15% ระบบงานได้คำนวณดอกเบี้ยถึงสิ้นวันที่ 28/02/89 และบันทึกตัดบัญชีเงินฝากของลูกค้าในวันเดียวกันและลูกค้าไม่ได้เดินรายการมาตั้งแต่ 01/03/89

- เพราะฉะนั้นดอกเบี้ยที่คำนวณถึงสิ้นวันที่ 31/03/89 ควรเท่ากับ

$$4,900 * \frac{15}{100} * \frac{31}{365} = 62.42$$

ผลลัพธ์ที่ได้ : - ควรจะยอมรับ หากปฏิเสธให้ดูข้อความที่แสดงบนจอ Terminal
- ตรวจสอบการคำนวณดอกเบี้ยจากรายงานที่ได้รับหลังจากการประมวลผลเพื่อคำนวณดอกเบี้ยถึงสิ้นวันที่ 31/03/89 ว่าจำนวนดอกเบี้ยตรงกับที่คำนวณไว้หรือไม่
- ถ้าตรงกัน --> ระบบงานคำนวณดอกเบี้ยกรณีเช็คคืน ถูกต้องแล้ว
- ถ้าไม่ตรงกัน --> -----"----- ไม่ถูกต้อง
ซึ่งอาจเกิดจากไม่ได้คำนวณย้อนกลับไป 1 วัน หรือโปรแกรมคำนวณดอกเบี้ยผิดพลาดหรือใช้อัตราดอกเบี้ยไม่ถูกต้องติดตามหาสาเหตุต่อไป

ตัวอย่างที่ 4

วัตถุประสงค์ : การป้องกันการถอนเงินยอดฝากเช็คที่ยังไม่ทราบผลการเรียกเก็บ
เงื่อนไข : ถอนเงินจากยอดฝากด้วยเช็ค Clearing ที่ยังไม่ทราบผลการเรียกเก็บ
ข้อมูลทดสอบ : บัญชีเงินฝากออมทรัพย์ มีข้อมูลทดสอบดังนี้
CYCLE 1 : ฝากเช็ค CL 7,000
CYCLE 2 : ก่อนทราบผลการเรียกเก็บเงินตามเช็ค
ถอนเงินสดลํ้าส่วนของยอดฝากด้วยเช็คที่ยังไม่ทราบผลการเรียกเก็บ

วัน/เดือน/ปี	รายการ	จำนวนเงิน	ยอดคงเหลือ	AV.Bal
01/03/89	ยอดยกมา	—	20,000	20,000
01/03/89 (C.1)	ฝากเช็ค CL	7,000	27,000	20,000
=====> 02/03/89 (C.1)	ถอนเงินสด	25,000		

ผลที่คาดหวัง : ปฏิเสธ

ผลจากการทดสอบ : ถ้าปฏิเสธ ----> ระบบงานมีการควบคุมป้องกันการถอนเงินจาก
ยอดฝากเช็คที่ยังไม่ทราบผลการเรียกเก็บ
ยอมรับ ----> ระบบงานไม่มีการควบคุมดังกล่าว หากธนาคาร
เรียกเก็บเงินตามเช็คไม่ได้ภายหลังจากที่จ่ายเงิน
ไปแล้ว ธนาคารจะได้รับความเสียหายและการ
แสดงยอดคงเหลือไม่ถูกต้องด้วย



21

การป้องกัน ดีกว่าการแก้ไข

การป้องกันดีกว่าการแก้ไข

สัญญาณการทุจริตหรือจุดอ่อนบางประการในองค์การที่ใช้คอมพิวเตอร์^{1/}

มีสัญญาณการทุจริตหรือจุดอ่อนในระบบงานโดยทั่ว ๆ ไป ซึ่งจะชี้ให้ฝ่ายจัดการรู้ล่วงหน้าได้ถ้าฝ่ายจัดการมีความเอาใจใส่ในการบริหารงานอย่างใกล้ชิดและมีประสิทธิภาพ และมีสัญญาณของนักบริหารที่จะรู้ถึงปัญหาหรือภัยที่เกิดจากการทุจริตในองค์การของตนได้ล่วงหน้าซึ่งสามารถป้องกันปัญหาได้ก่อนที่จะต้องสูญเสียและต้องแก้ไขปัญหากันในภายหลัง

สัญญาณนี้ก็ไม่จำเป็นต้องใช้ความรู้ทางเทคนิคหรือการฝึกฝนแต่อย่างไร อย่างไรก็ตามหากผู้ตรวจสอบภายในหรือผู้สอบบัญชีภายนอกสามารถแจกแจงสัญญาณเตือนภัยเหล่านี้ได้ จะช่วยให้ฝ่ายจัดการขององค์การสามารถทำหน้าที่ที่สำคัญในการป้องกันการทุจริตหรือทราบจุดอ่อนในระบบงานด้านคอมพิวเตอร์ขององค์การได้อย่างมีประสิทธิภาพเพิ่มขึ้น

ตัวอย่างสัญญาณการทุจริตหรือจุดอ่อนในระบบงานดังกล่าว ได้แก่

- พนักงานให้คำอธิบายอย่างพิรุธต่อการหายไปของอุปกรณ์ ทรัพย์สิน หรือเงิน
- บันทึกข้อมูลถูกเขียนใหม่โดยไม่มีเหตุผลอันควร
- บันทึกข้อมูล (Record) ถูกแก้ไขเปลี่ยนแปลง เพิ่มเติม ลบล้าง หรือทำลาย โดยผิดขั้นตอนหรือไม่ปฏิบัติตามขั้นตอนที่กำหนดไว้
- ลายมือบนเอกสารสำคัญถูกปลอมแปลง
- บันทึกข้อมูลที่มีอยู่ปรากฏว่าเป็นของปลอม
- สินค้าคงคลังมักขาดจำนวน
- พนักงานในระบบงานสำคัญมีการทำงานล่วงเวลาบ่อย ๆ
- บันทึกข้อมูลไม่มีการปรับปรุงให้ทันเวลา
- บุคลากรในแผนกที่สำคัญรู้สึกลังเลในการให้ความร่วมมือต่อการควบคุมการบันทึกข้อมูลหรือลังเลใจในการให้ความร่วมมือต่อการถูกตรวจสอบไม่ว่าจากการตรวจสอบภายในหรือจากบุคคลที่สาม
- พนักงานในศูนย์คอมพิวเตอร์หรือผู้ที่เกี่ยวข้องแสดงความสนใจระวังตัวต่อคำถามทั่ว ๆ ไปมากเกินไปพิเศษ
- คำร้องเรียนของลูกค้า ผู้ขาย ผู้ซื้อ และบัญชีอื่น ๆ มีลักษณะยืดเยื้อ
- คำร้องเรียนของพนักงานในส่วนที่เกี่ยวข้องกันมีจำนวนมากเกินสมควร
- คำร้องเรียนเกี่ยวกับพฤติกรรมทุจริตถูกละเลยไม่สนใจ
- การกระทำที่ไม่ถูกต้องไม่เป็นไปตามระเบียบและขาดศักยภาพถูกซ่อนเร้นไว้
- พนักงานในระบบงานสำคัญปฏิเสธการเลื่อนตำแหน่งหรือการหยุดพักผ่อน

^{1/} สรุปรจากหนังสือ How to prevent Computer crime, A Guide for Managers
โดย August Beguai

- พนักงานมักจะเกลียดออกไปนอกแผนกของตนเอง
- ข้อมูลทางการเงินที่เป็นความลับมักจะถูกนำมาใช้เพื่อผลประโยชน์ทางการเงินส่วนตัว
- ข้อมูลภายในรั่วไหลสู่เพื่อนหรือญาติโดยบุคคลภายใน เพื่อผลประโยชน์ด้านการลงทุน
- ความลับทางการค้าถูกลักลอบนำไปขายแก่กิจการที่เป็นคู่แข่ง
- ขบวนการในการตัดสินใจถูกนำออกเผยแพร่แก่บุคคลภายนอกที่ไม่มีหน้าที่เกี่ยวข้อง
- โปรแกรมถูกลักลอบถ่ายสำเนาและนำออกขายแก่บุคคลภายนอก
- รายชื่อลูกค้าถูกถ่ายสำเนาและขายโดยพนักงาน
- ไม่มีเอกสารประกอบระบบงาน และคู่มือที่เพียงพอ และทันกาล ในการปฏิบัติงานด้านคอมพิวเตอร์
- ไม่มีการทดสอบและประเมินงาน ควบคุมภายในโดยบุคคลภายนอกองค์การที่มีประสิทธิภาพ
- มีการกระทำผิดระเบียบอื่น ๆ

การหลีกเลี่ยงและการป้องกันการกระทำผิดเกี่ยวกับคอมพิวเตอร์เป็นสิ่งที่ทุกองค์การจะต้องเกี่ยวข้อง จึงเป็นสิ่งที่หลีกเลี่ยงเสียมิได้ที่ฝ่ายจัดการจะต้องเข้าใจสภาพแวดล้อมที่จะก่อให้เกิดมีการกระทำผิดหรือมีจุดอ่อนดังกล่าว ผู้บริหารในปัจจุบันจึงต้องได้รับการศึกษาและอบรมทั้งในด้านความสามารถในการบ่งชี้ปัญหาและการแก้ปัญหาดังกล่าว แต่ไม่ถึงกับต้องเป็นผู้ชำนาญในด้านคอมพิวเตอร์ อย่างไรก็ดี นับว่าเป็นโชคร้ายที่องค์การจำนวนมากเข้าใจว่าถ้าเขาปิดตาเสียบ้างปัญหาดังกล่าวจะไม่เกิดขึ้น ซึ่งที่จริงกลับเป็นสิ่งที่อำนวยความสะดวกให้เกิดการทุจริตหรือจุดอ่อนที่อาจเป็นปัญหาร้ายแรงตามมาได้

ท่านเห็นด้วยหรือไม่กับคำกล่าวที่ว่า "การป้องกันดีกว่าการแก้ไข" หากท่านเห็นด้วยท่านได้ทราบและติดตามการแก้ไขปัญหามาจากสัญญาณเตือนภัยดังกล่าวอย่างไร และพอเพียงหรือไม่?





ความสูญเสียของสถาบันการเงิน
ที่มีเหตุมาจากโปรแกรม
คอมพิวเตอร์ผิดพลาด

**“เหตุมาจากโปรแกรมคอมพิวเตอร์ผิดพลาด
ทำให้เกิดเป็นลูกหนี้ 32 พันล้านเหรียญสหรัฐอเมริกา”
SOFTWARE FAILURE CAUSES
US \$ 32 BILLION OVERDRAFT
(EDPACS, JAN 1986)**

บทนำ

ธนาคารแห่งนิวยอร์ก (The Bank of New York) ซึ่งเป็นธนาคารใหญ่ลำดับที่ 18 ของสหรัฐอเมริกา ปรากฏว่าวันที่ 21 พฤศจิกายน 2528 ธนาคารได้ตกเป็นลูกหนี้เบิกเกินบัญชี (overdraft) เป็นจำนวนสูงถึง 32 พันล้านเหรียญสหรัฐ ต่อ Federal Reserve Bank ทั้ง ๆ ที่ โดยข้อเท็จจริงแล้วธนาคารมิได้มีปัญหาทางการเงินแต่อย่างใด หากเกิดจากการทำงานล้มเหลวของโปรแกรมระบบงานคอมพิวเตอร์ ที่ทำหน้าที่ประมวลผลงานซื้อขายหลักทรัพย์รัฐบาล (Government Securities) ของธนาคารแห่งนิวยอร์กนั่นเอง

ประวัติการทำงานของธนาคารโดยย่อ

ธนาคารแห่งนิวยอร์กนอกจากเป็นธนาคารพาณิชย์แล้ว ยังเป็นธนาคารที่ทำหน้าที่ชำระบัญชี (Clearing Bank) และเป็นนายหน้าขายหลักทรัพย์ของรัฐบาลรายใหญ่แห่งหนึ่ง ดำเนินธุรกิจประสบความสำเร็จมานานจนได้รับการยกย่องให้เป็นธนาคารที่มีระบบงานตัวอย่างของ Federal Reserve Bank มีปริมาณงานเฉลี่ย 27,000 รายการต่อวัน เป็นมูลค่า 200 พันล้านเหรียญ เฉลี่ยมูลค่ารายการละ 7.5 ล้านเหรียญ และในเดือนมีนาคม 2528 ธนาคารได้ปรับปรุงเพิ่มประสิทธิภาพของระบบงานคอมพิวเตอร์ ให้สามารถรับปริมาณธุรกิจได้ 36,000 รายการต่อวันอีกด้วย

ตัวอย่างการดำเนินธุรกิจการซื้อขายหลักทรัพย์รัฐบาล

1. ผู้ขายส่ง (dealer) X ต้องการซื้อหลักทรัพย์รัฐบาลผ่านธนาคารแห่งนิวยอร์ก เมื่อ Federal Reserve Bank ได้รับแจ้งจากธนาคารแห่งนิวยอร์ก จะเพิ่ม (credit) บัญชีหลักทรัพย์รัฐบาล และหัก (debit) บัญชีเงินสดของธนาคารแห่งนิวยอร์ก จากนั้นธนาคารแห่งนิวยอร์กจะติดต่อกับผู้ขายส่งต่อไป

2. ในทำนองเดียวกัน ผู้ขายส่ง Z ขายหลักทรัพย์รัฐบาลผ่านธนาคารแห่งนิวยอร์ก เมื่อ Federal Reserve Bank ได้รับแจ้ง จะหัก (debit) บัญชีหลักทรัพย์รัฐบาล และเพิ่ม (credit) บัญชีเงินสดของธนาคารแห่งนิวยอร์ก

จากที่กล่าว สรุปได้ว่า เมื่อเกิดธุรกิจการซื้อขายหลักทรัพย์ Federal Reserve Bank จะหัก (debit) บัญชีเงินสดของธนาคารแห่งนิวยอร์ก และเมื่อมีการขายหลักทรัพย์ก็จะเพิ่ม (credit) บัญชีเงินสดของธนาคารแห่งนิวยอร์ก หากธนาคารแห่งนิวยอร์กไม่สามารถรายงานการซื้อขายต่อ Federal Reserve Bank บัญชีเงินสดของธนาคารแห่งนิวยอร์ก ณ Federal Reserve Bank จะถูกหัก (debit) โดยไม่มีการเพิ่ม (credit)

สาเหตุของข้อผิดพลาด

ในวันพุธที่ 20 พฤศจิกายน 2528

การซื้อขายหลักทรัพย์รัฐบาลมีปริมาณสูงกว่าปกติ ตามทฤษฎี ระบบงานสามารถรับงานได้ถึง 36,000 ราย แต่ในวันเกิดเหตุ เมื่อปริมาณงานเพิ่มมากกว่า 32,000 รายการ การทำงานของแฟ้มข้อมูลระบบคอมพิวเตอร์ก็เริ่มขัดข้อง เมื่อขายหลักทรัพย์ ธนาคารแห่งนิวยอร์กไม่สามารถแจ้ง Federal Reserve Bank ส่งหลักทรัพย์ให้ลูกค้าของตนได้ Federal Reserve Bank จึงไม่สามารถจ่ายเงินให้กับธนาคารแห่งนิวยอร์ก เมื่อลูกค้าธนาคารแห่งนิวยอร์กต้องการซื้อหลักทรัพย์ Federal Reserve Bank โอนให้แก่ลูกค้าและหักบัญชีเงินสดของธนาคารแห่งนิวยอร์ก

วันพฤหัสบดีที่ 21 พฤศจิกายน 2528

ระบบงานคอมพิวเตอร์ยังคงขัดข้อง ธนาคารแบ่งเจ้าหน้าที่เขียนโปรแกรมเป็น 2 กลุ่มกลุ่มละ 50 คน กลุ่มหนึ่งทำหน้าที่แก้ไขโปรแกรม (patching) เพื่อให้สามารถกลับทำงานได้ตามปกติ และอีกกลุ่มหนึ่งแก้ไขโปรแกรม 700 โปรแกรมให้รับงานได้มากกว่า 32,000 รายการ

ผลจากเหตุการณ์ครั้งนี้ทำให้เจ้าหน้าที่ธนาคารอื่นและตัวแทนซื้อขาย (dealer) หลายร้อยคนต้องทำงานตลอดวันและคืน เพื่อแก้ไขปัญหาที่เกี่ยวข้องกับตนด้วย ในวันที่สองปริมาณงานน้อยกว่าปกติ ณ เวลาปิดการซื้อขาย ธนาคารแห่งนิวยอร์กตกเป็นลูกหนี้เบิกเกินบัญชีของ New York Federal Reserve Bank ถึง 32 พันล้านเหรียญ ในที่สุดเจ้าหน้าที่แก้ไขโปรแกรมได้สำเร็จ ธนาคารเริ่มปฏิบัติการและหักชำระบัญชีได้ 7.7 ล้านเหรียญ แต่เมื่อเวลาประมาณเที่ยงคืนเศษ ระบบงานก็ล้มเหลวอีกครั้งที่สอง ทำให้ธนาคารแห่งนิวยอร์ก จำต้องยื่นหลักทรัพย์ทั้งหมดของธนาคารและของลูกค้าที่ได้รับการยินยอมเพื่อเป็นหลักประกันกู้ยืมเงินจากธนาคารอื่นเป็นจำนวน 700 ล้านเหรียญ และ 23.6 พันล้านเหรียญ จาก New York Federal Reserve Bank เพื่อชำระหนี้ครั้งนี้

วันศุกร์ที่ 22 พฤศจิกายน 2528

Federal Reserve Bank ยังคงเปิดบริการชำระเงินโดยระบบคอมพิวเตอร์ (Wire Clearing System) ทั่วประเทศอยู่ ส่วนเจ้าหน้าที่เขียนโปรแกรมธนาคารแห่งนิวยอร์กสามารถแก้ไขงานจนสำเร็จ ทำให้ธนาคารเริ่มประกอบธุรกิจเมื่อเวลา 5.00 นาฬิกา โดยนำรายการของวันพุธที่ 20 และพฤหัสบดีที่ 21 มาประมวลผลย้อนหลัง และปฏิบัติงานของวันศุกร์ที่ 22 เพื่อให้งานเป็นปัจจุบัน แต่อย่างไรก็ตาม การซื้อขายหลักทรัพย์ยังคงดำเนินอยู่ทำให้ธนาคารแห่งนิวยอร์กยังประสบปัญหาเบิกเกินบัญชีอยู่เช่นเดิม Federal Reserve Bank จึงประกาศระงับรายการที่เกี่ยวข้องกับธนาคารแห่งนิวยอร์กทั้งหมดเป็นการชั่วคราว เพื่อลดภาวะความตึงเครียดในตลาดซื้อขายหลักทรัพย์ บางรายไม่ยอมรับและยกเลิกรายการที่เกี่ยวข้องกับธนาคารแห่งนิวยอร์ก เมื่อเวลาประมาณ 12.00 นาฬิกาเศษ ธนาคารก็สามารถปฏิบัติงานแล้วเสร็จเป็นปัจจุบัน ซึ่งใช้เวลาไม่ถึง 24 ชั่วโมง แก้ไขสถานการณ์ครั้งนี้

ภายหลังเหตุการณ์

ธนาคารแห่งนิวยอร์กต้องจ่ายดอกเบี้ยเงินเบิกเกินบัญชี 5 ล้านดอลลาร์ ซึ่งก็คงจะหักจากกำไร 70 ล้านดอลลาร์ ที่ประกาศผลการดำเนินงานสำหรับ 9 เดือนแรกของปี 2528

คณะอนุกรรมการกำหนดนโยบายการเงินของท้องถิ่น (The US House Subcommittee on Domestic Monetary Policy) เรียกประชุมสืบสวนเหตุการณ์ที่เกิดขึ้น ผู้เข้าร่วมประชุมได้ให้ความคิดเห็นหลายคน สรุปได้คือ เหตุการณ์ครั้งนี้เป็นบทเรียนอย่างดี จำเป็นต้องให้ความสำคัญแก่ความปลอดภัย มั่นคงและประสิทธิภาพของระบบชำระเงิน พร้อมทั้งจัดให้มีระบบสำรอง (Backup) ที่ดีกว่านี้ มีผู้เสนอให้มีการทำโทษโดยปรับเป็นอัตราดอกเบี้ยในการกู้ยืมเมื่อมีการผิดพลาดเกิดขึ้น ประธานกรรมการของธนาคารแห่งนิวยอร์ก กล่าวว่า "ดอกเบี้ย 5 ล้านดอลลาร์ที่ธนาคารจ่าย ก็เสมือนค่าปรับมากเพียงพอสำหรับ ผู้ถือหุ้น เจ้าหน้าที่ และลูกจ้างธนาคารอยู่แล้ว"

ข้อคิดเห็น

1. การวิเคราะห์ปัญหา

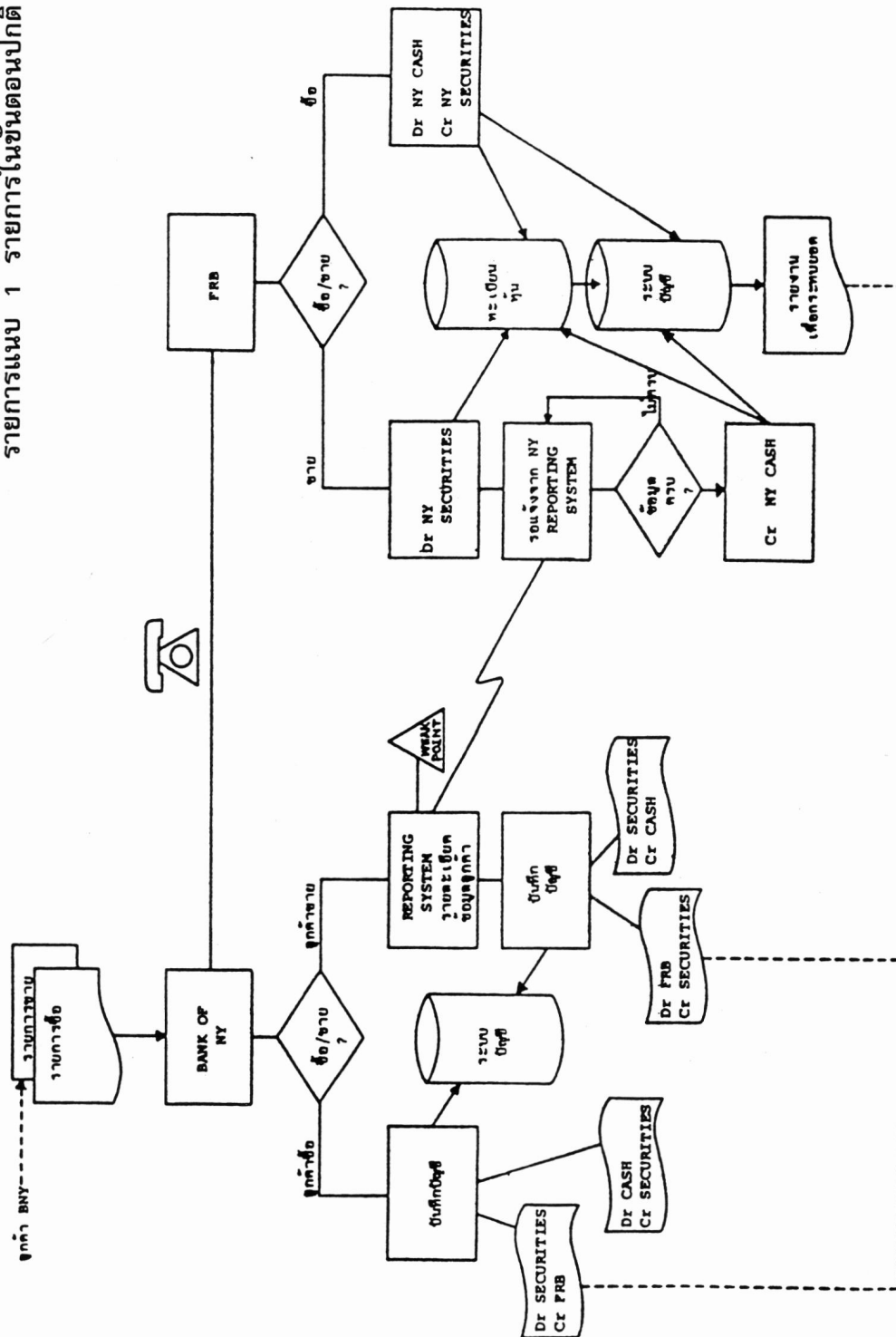
ในการวิเคราะห์ปัญหากรณีธนาคารแห่งนิวยอร์ก จำเป็นต้องศึกษารายละเอียดเกี่ยวกับข้อมูล ดังนี้

- 1.1 ระบบการบันทึกบัญชี (Accounting System)
- 1.2 ระบบการติดต่องาน (Communication System)
- 1.3 ขั้นตอนการทำงาน (Job Flow)

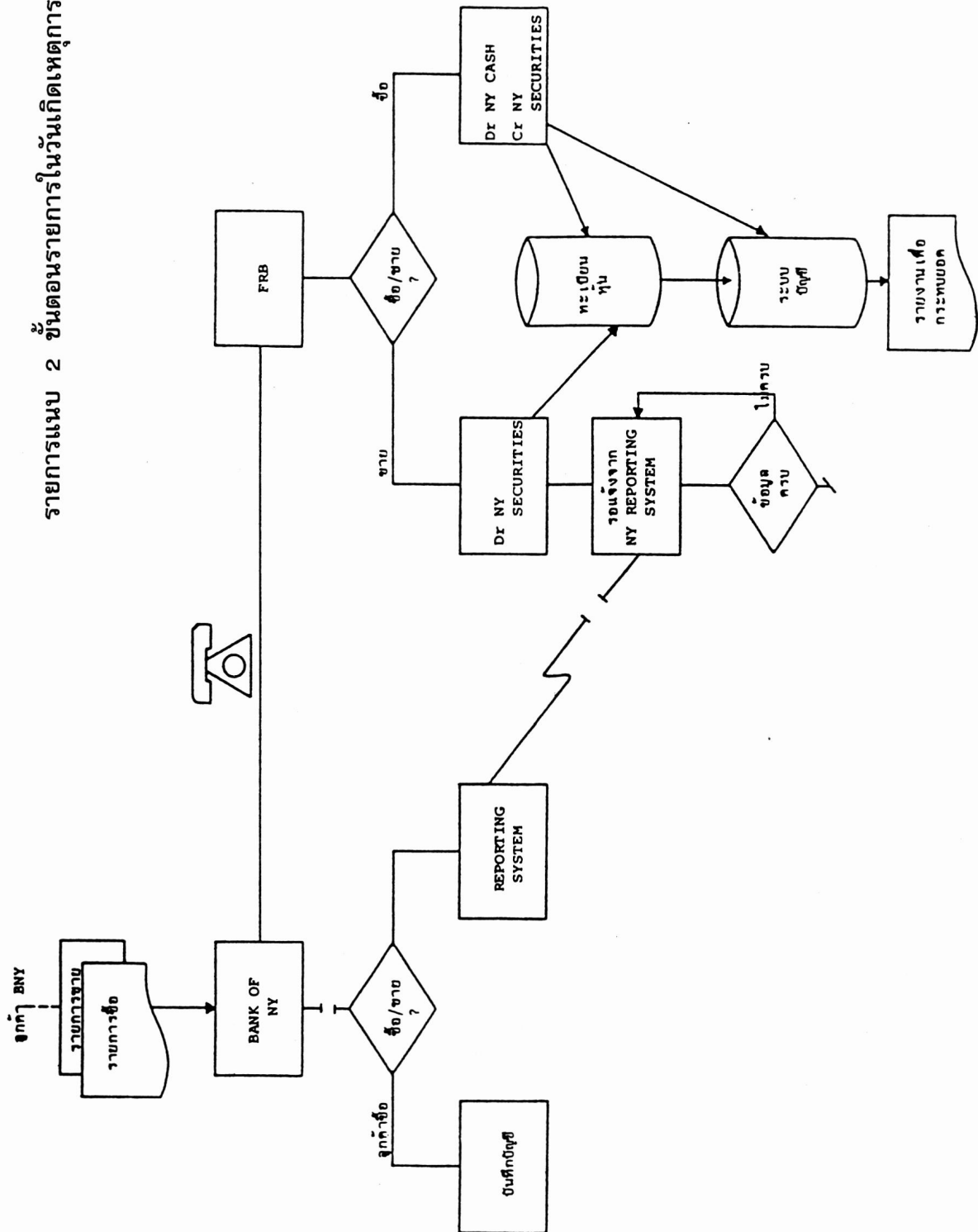
จากเหตุการณ์ครั้งนี้ สามารถรวบรวมข้อมูลและบันทึกเป็นผังการปฏิบัติงาน (Flow) ได้ตามรายการแนบ 1 และ 2



รายการแนบ 1 รายการในชั้นตอนปกติ



รายการแนบ 2 ขั้นตอนรายการในวันเกิดเหตุการณ์



2. สรุปผลการวิเคราะห์ปัญหา

ในธุรกิจเกือบทุกประเภทนำเครื่องอุปกรณ์คอมพิวเตอร์มาใช้ เพื่ออำนวยความสะดวกรวดเร็ว และเพิ่มประสิทธิภาพในการทำงาน แต่เมื่อมีเหตุการณ์กรณีธนาคารแห่งนิวยอร์กเกิดขึ้นจะเห็นว่าความล้มเหลวของระบบคอมพิวเตอร์ในช่วงระยะเวลาอันสั้นก็ให้โทษมากมายเช่นกัน ซึ่งนอกจากจะเสียหายเป็นเงินและเวลาแล้ว ยังมีสิ่งอื่นติดตามมาอีกด้วย เช่น การเสียชื่อเสียง การสูญเสียลูกค้า ผู้ถือหุ้นขาดความเชื่อถือ และผลทางกฎหมาย

ดังนั้น ระบบงานที่มีประสิทธิภาพ มั่นคง และปลอดภัย ต้องเริ่มมาจากการวางแผน การจัดการ การปฏิบัติงาน การควบคุม การรักษาความปลอดภัย และการตรวจสอบที่ดีและรอบคอบ ทั้งนี้ รวมถึงการมีบุคลากรที่มีความรู้ความชำนาญในการทำงานเพียงพออีกด้วย จากเหตุการณ์ธนาคารแห่งนิวยอร์กนี้ ธนาคารอาจมีจุดอ่อนหรือข้อบกพร่องพอสรุปได้ตามหัวข้อดังต่อไปนี้

2.1 การจัดการ

- (1) การแบ่งหน้าที่ความรับผิดชอบ ธนาคารควรพิจารณามอบหน้าที่ให้กับบุคคลที่มีคุณสมบัติเหมาะสมกับงาน มีความรู้ความเข้าใจในระบบงาน (Application) และประสิทธิภาพของเครื่องอุปกรณ์ต่าง ๆ (Hardware)
- (2) เมื่อมีการนำระบบงานใหม่มาใช้ หรือมีการแก้ไขปรับปรุงระบบงานธนาคารควรจัดให้มีการวางแผน วิเคราะห์โครงการอย่างรอบคอบ และผ่านการทดสอบอย่างเพียงพอ

2.2 การควบคุม

- (1) ธนาคารควรจัดให้มีผู้ตรวจสอบภายในตรวจสอบระบบงานคอมพิวเตอร์ เพื่อตรวจสอบระบบงานให้ได้มาตรฐานและประสิทธิภาพตามนโยบายที่กำหนด
- (2) ควรให้ผู้ตรวจสอบภายในเข้าร่วมพัฒนาหรือปรับปรุงแก้ไขระบบงาน เพื่อให้การควบคุมภายในมีประสิทธิภาพตั้งแต่แรกเริ่ม
- (3) ควรให้ผู้ตรวจสอบภายใน ทดสอบและตรวจรับระบบงานก่อนนำออกใช้งานจริง

2.3 การปฏิบัติงาน

- (1) จัดให้มีการควบคุมการใช้เครื่องอุปกรณ์คอมพิวเตอร์ให้เป็นไปอย่างถูกต้องและปลอดภัย
- (2) ให้มีการบำรุงรักษาเครื่องอุปกรณ์คอมพิวเตอร์สม่ำเสมอ เพื่อป้องกันไม่ให้เกิดความล้มเหลวของอุปกรณ์เครื่องมือต่าง ๆ
- (3) ธนาคารควรจัดให้มีอุปกรณ์ชุดสำรอง ทั้งโปรแกรมระบบงาน (Software) เครื่องอุปกรณ์คอมพิวเตอร์ (Hardware) และเอกสารสนับสนุนการปฏิบัติงานที่จำเป็นสำหรับการประมวลผล

- (4) ธนาคารควรจัดให้มีแผนการป้องกันภัยและมาตรการการปรับปรุงแก้ไข (Contingency and Recovery Plan) ที่รอบคอบและมีประสิทธิภาพ เพื่อป้องกันและบรรเทาภัยใด ๆ อันอาจเกิดขึ้น ซึ่งรวมถึงความล้มเหลวของระบบงาน และสามารถปฏิบัติงานให้กลับสู่สภาพปกติโดยเร็วที่สุด ในกรณีการแก้ไขโปรแกรม (Patching) ถึงสองครั้ง เจ้าหน้าที่อาจวิเคราะห์ปัญหาไม่ถูกต้อง และหรืออาจเป็นเพราะจัดลำดับขั้นตอนการทำงานที่ต้องปรับปรุงแก้ไขไม่ถูกต้อง หากมีแผนการแก้ไขที่รอบคอบ (Recovery Plan) ธนาคารอาจใช้เวลาแก้ไขงานน้อยกว่า หรือลดความเสียหายที่เกิดขึ้นครั้งนี้ได้
- (5) ให้มีการประกันภัยเพื่อป้องกันการเสี่ยงภัยอันอาจเกิดขึ้นในกรณีต่าง ๆ เช่น ความล้มเหลวของอุปกรณ์ต่าง ๆ ความซื่อสัตย์ของพนักงาน ข้อผิดพลาดและบกพร่องจากการปฏิบัติงาน การสูญหายของข้อมูล การหยุดชะงักของธุรกิจ เป็นต้น



ภาคผนวก



ประกาศอธิบดีกรมสรรพากร

เกี่ยวกับภาษีมูลค่าเพิ่ม (ฉบับที่ 63)

เรื่อง กำหนดแบบ หลักเกณฑ์ วิธีการ และเงื่อนไขเกี่ยวกับการจัดทำรายงาน การลงรายการในรายงาน การเก็บใบกำกับภาษีและเอกสารหลักฐานอื่นที่ใช้ประกอบการลงรายงานตามมาตรา 87 และมาตรา 87/3 วรรคสอง แห่งประมวลรัษฎากร

อาศัยอำนาจตามความในมาตรา 87 และมาตรา 87/3 วรรคสอง แห่งประมวลรัษฎากร ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 30) พ.ศ. 2534 อธิบดีกรมสรรพากรกำหนดแบบ หลักเกณฑ์ วิธีการ และเงื่อนไขเกี่ยวกับการจัดทำรายงานการลงรายการในรายงานการเก็บใบกำกับภาษีและเอกสารหลักฐานอื่นที่ใช้ประกอบการลงรายงานภาษีซื้อ ดังต่อไปนี้

ข้อ 1 ให้ยกเลิกความในข้อ 5 แห่งประกาศอธิบดีกรมสรรพากรเกี่ยวกับภาษีมูลค่าเพิ่ม (ฉบับที่ 22) เรื่อง กำหนดแบบหลักเกณฑ์ วิธีการ และเงื่อนไขเกี่ยวกับการจัดทำรายงาน การลงรายการในรายงาน การเก็บใบกำกับภาษีและเอกสารหลักฐานอื่นที่ใช้ประกอบการลงรายงานภาษีซื้อ ตามมาตรา 87 และมาตรา 87/3 วรรคสอง แห่งประมวลรัษฎากร ลงวันที่ 27 ธันวาคม พ.ศ. 2534 ซึ่งแก้ไขเพิ่มเติมโดยข้อ 1 แห่งประกาศอธิบดีกรมสรรพากรเกี่ยวกับภาษีมูลค่าเพิ่ม (ฉบับที่ 41) เรื่อง กำหนดแบบ หลักเกณฑ์ วิธีการ และเงื่อนไขเกี่ยวกับการจัดทำรายงาน การลงรายการในรายงาน การเก็บใบกำกับภาษีและเอกสารหลักฐานอื่นที่ใช้ประกอบการลงรายงานภาษีซื้อ ตามมาตรา 87 และมาตรา 87/3 วรรคสอง แห่งประมวลรัษฎากร ลงวันที่ 25 สิงหาคม พ.ศ. 2535 และให้ใช้ความต่อไปนี้แทน

ข้อ 5 การลงรายการในรายงานภาษีขาย รายงานภาษีซื้อ รายงานสินค้าและวัตถุดิบ และรายงานมูลค่าของฐานภาษี ตามมาตรา 87 แห่งประมวลรัษฎากร ให้เขียนด้วยหมึก หรือพิมพ์ดีด หรือสิพิมพ์ หรือพิมพ์ด้วยเครื่องคอมพิวเตอร์ และจะลงรายการเป็นภาษาไทยหรือภาษาอังกฤษก็ได้

หากผู้ประกอบการจดทะเบียนใช้เครื่องคอมพิวเตอร์จัดทำรายงานตามวรรคหนึ่ง คุณสมบัติของซอฟต์แวร์ระบบการลงรายการในรายงานดังกล่าวจะต้องเป็นไปตามมาตรฐานซอฟต์แวร์ของกรมสรรพากรชนิดหนึ่งชนิดใด ดังต่อไปนี้

ชนิด ก.

- (1) เป็นโปรแกรมที่เมื่อบันทึกข้อมูล (Data Entry) และโอนเข้าบัญชีแยกประเภท (Post) แล้ว จะแก้ไขรายการนั้น ๆ โดยไร้ร่องรอยไม่ได้ ถ้าจะแก้ไขต้องทำการปรับปรุงตามหลักบัญชี
- (2) เป็นโปรแกรมที่ช่วยไม่ให้เกิดความเสี่ยงภาษี ถ้าเป็นโปรแกรมที่ใช้กับ PC ผู้ขายซอฟต์แวร์ไม่ได้ให้ Source Code ไปกับซอฟต์แวร์นั้น
- (3) เป็นโปรแกรมที่มีระบบรักษาความปลอดภัย เพื่อควบคุมการเข้าถึงข้อมูลได้ โดยต้องระบุระดับเจ้าหน้าที่ที่สามารถบันทึก อ่าน หรือแก้ไขข้อมูลได้
- (4) เป็นโปรแกรมที่การบัญชีเป็นไปตามหลักบัญชีคู่ (Double Entry Accounting)

ชนิด ข.

- (1) เป็นโปรแกรมที่เมื่อบันทึกข้อมูล (Data Entry) และโอนเข้าบัญชีแยกประเภท (Post) แล้ว จะแก้ไขรายการนั้น ๆ โดยไร้ร่องรอยไม่ได้ ถ้าจะแก้ไขก็ต้องทำการปรับปรุงตามหลักบัญชี
- (2) เป็นโปรแกรมที่ช่วยไม่ให้เกิดความเสี่ยงภาษี ถ้าเป็นโปรแกรมที่ใช้กับ PC ผู้ขายซอฟต์แวร์ไม่ได้ให้ Source Code ไปกับซอฟต์แวร์นั้น
- (3) เป็นโปรแกรมที่มีระบบรักษาความปลอดภัย เพื่อควบคุมการเข้าถึงข้อมูลได้ โดยต้องระบุระดับเจ้าหน้าที่ที่สามารถบันทึก อ่าน หรือแก้ไขข้อมูลได้
- (4) เป็นโปรแกรมที่การบันทึกบัญชีเป็นไปตามหลักบัญชีคู่ (Double Entry Accounting)
- (5) เป็นโปรแกรมที่ถ้ามีระบบซอฟต์แวร์ในระบบงานใด ระบบซอฟต์แวร์นั้นทุกระบบ เช่น ระบบขาย ระบบพัสดุฯ บันทึกเข้าระบบบัญชีแยกประเภทโดยอัตโนมัติและแก้ไขโดยไร้ร่องรอยไม่ได้

ชนิด ค.

- (1) เป็นโปรแกรมที่เมื่อบันทึกข้อมูล (Data Entry) และโอนเข้าบัญชีแยกประเภท (Post) แล้ว จะแก้ไขรายการนั้น ๆ โดยไร้ร่องรอยไม่ได้ ถ้าจะแก้ไขก็ต้องทำการปรับปรุงตามหลักบัญชี
- (2) เป็นโปรแกรมที่ช่วยไม่ให้เกิดความเสี่ยงภาษี ถ้าเป็นโปรแกรมที่ใช้กับ PC ผู้ขายซอฟต์แวร์ไม่ได้ให้ Source Code ไปกับซอฟต์แวร์นั้น
- (3) เป็นโปรแกรมที่มีระบบรักษาความปลอดภัย เพื่อควบคุมการเข้าถึงข้อมูลได้โดยต้องระบุระดับเจ้าหน้าที่ที่สามารถบันทึก อ่าน หรือแก้ไขข้อมูลได้
- (4) เป็นโปรแกรมที่การบันทึกบัญชีเป็นไปตามหลักบัญชีคู่ (Double Entry Accounting)
- (5) เป็นโปรแกรมที่ระบบงานทุกระบบใช้คอมพิวเตอร์ และลงบัญชีแยกประเภทโดยอัตโนมัติและแก้ไขโดยไร้ร่องรอยไม่ได้

ชนิด ง.

- (1) เป็นโปรแกรมที่เมื่อบันทึกข้อมูล (Data Entry) และโอนเข้าบัญชีแยกประเภท (Post) แล้ว จะแก้ไขรายการนั้น ๆ โดยไร้ร่องรอยไม่ได้ ถ้าจะแก้ไขก็ต้องทำการปรับปรุงตามหลักบัญชี
- (2) เป็นโปรแกรมที่ช่วยไม่ให้หลีกเลี่ยงภาษี ถ้าเป็นโปรแกรมที่ใช้กับ PC ผู้ขายซอฟต์แวร์ไม่ได้ให้ Source Code ไปกับซอฟต์แวร์นั้น
- (3) เป็นโปรแกรมที่มีระบบรักษาความปลอดภัย เพื่อควบคุมการเข้าถึงข้อมูลได้ โดยต้องระบุระดับเจ้าหน้าที่ที่สามารถบันทึก อ่าน หรือแก้ไขข้อมูลได้
- (4) เป็นโปรแกรมที่การบันทึกบัญชีเป็นไปตามหลักบัญชีคู่ (Double Entry Accounting)
- (5) เป็นโปรแกรมที่ระบบงานทุกระบบใช้คอมพิวเตอร์ และลงบัญชีแยกประเภทโดยอัตโนมัติและแก้ไขโดยไร้ร่องรอยไม่ได้

(6) มีรหัสที่แจ้งไว้ที่กรมสรรพากรซึ่งทำให้สามารถผ่านรหัส Security ต่าง ๆ ทั้งสิ้นได้ ใส่ของปิดผนึก ซึ่งกรมสรรพากรจะไม่เปิด ยกเว้นต่อหน้าผู้ประกอบการ

ทั้งนี้ ผู้จำหน่ายซอฟต์แวร์ได้ระบุไว้ที่หน้าจอเดียวกับชื่อโปรแกรมและได้ระบุไว้บนภาชนะบรรจุซอฟต์แวร์ดังกล่าว ซึ่งข้อความดังต่อไปนี้

"ซอฟต์แวร์นี้เขียนขึ้นโดย.....ซึ่งมีเลขประจำตัวซอฟต์แวร์เข้าสู่เลขที่.....เป็นซอฟต์แวร์เลขที่.....และเป็นซอฟต์แวร์ตามมาตรฐานซอฟต์แวร์เพื่อภาษีสรรพากรของกรมสรรพากรชนิด.....กล่าวคือ.....(ระบุคุณสมบัติข้างต้น)....."

หรือในกรณีผู้ประกอบการจดทะเบียนเขียนซอฟต์แวร์ขึ้นเองได้ระบุไว้ที่หน้าจอเดียวกับชื่อโปรแกรมซึ่งข้อความดังต่อไปนี้

"ซอฟต์แวร์นี้เขียนขึ้นโดย.....และเป็นซอฟต์แวร์ตามมาตรฐานซอฟต์แวร์เพื่อภาษีสรรพากรของกรมสรรพากรชนิด.....กล่าวคือ.....(ระบุคุณสมบัติข้างต้น)....."

ความใน (1) ถึง (3) ของมาตรฐานซอฟต์แวร์ชนิด ก ชนิด ข ชนิด ค หรือชนิด ง ข้างต้น มีดังต่อไปนี้

(1) เป็นโปรแกรมที่เมื่อบันทึกข้อมูล (Data Entry) และโอนเข้าบัญชีแยกประเภท (Post) แล้ว จะแก้ไขรายการนั้น ๆ โดยไร้ร่องรอยไม่ได้ ถ้าจะแก้ไขก็ต้องทำการปรับปรุงตามหลักบัญชี หมายความว่า

(ก) เมื่อบันทึกข้อมูลแล้ว จะต้องโอนรายการเข้าบัญชีแยกประเภทด้วย และสามารถพิมพ์รายงานจากบัญชีแยกประเภทเพื่อการตรวจสอบได้

(ข) การแก้ไขรายการไม่ให้วิธีลบทิ้งหรือล้างรายการออก แต่ให้วิธีบันทึกการปรับปรุงเพิ่มเติมเข้าไป เพื่อแสดงรายการก่อนปรับปรุงและหลังปรับปรุงให้เห็น

(ค) สามารถแสดงรายงานการแก้ไขปรับปรุงรายการ (Audit Trail) โดยอัตโนมัติ ซึ่งต้องระบุต้นตอของเอกสาร เช่น Document Number หรือ Reference Number พร้อมทั้งแสดงวันที่ เวลาที่เกิดรายการ รหัสประจำตัวของผู้ทำรายการแต่ละรายการ และจำนวนรายการที่มีการแก้ไขปรับปรุงด้วย และ

(ง) ปฏิเสธการทำรายการปกปิดหรือซ่อนรายการรายงานการแก้ไขปรับปรุงรายการ (Hide Audit Trail) ไม่ว่าทั้งหมดหรือบางส่วน

- (2) เป็นโปรแกรมที่ช่วยไม่ให้หลักเสียภาษี หมายความว่า เป็นโปรแกรมที่
- (ก) เขียนขึ้นตามเงื่อนไขกฎหมายและระเบียบวิธีปฏิบัติที่กำหนดตามประมวลรัษฎากร
 - (ข) ไม่สามารถกำหนดหรือเลือกวิธีการประมวลผลข้อมูล เช่น การกำหนดเงื่อนไขให้ยอดขายสินค้าชนิดเดียวกันบางรายการนำไปเสียภาษีมูลค่าเพิ่ม บางรายการไม่ต้องนำไปเสียภาษีมูลค่าเพิ่ม
 - (ค) สามารถแสดงยอดรวมและเปรียบเทียบยอด เพื่อตรวจนับความครบถ้วนของข้อมูลขณะทำการประมวลผล
 - (ง) สามารถตรวจนับจำนวนรายการ (Transaction) ที่มีอยู่ในแฟ้มข้อมูล (File) ว่าอยู่ครบหรือไม่ และสามารถสอบยันกับจำนวนรายการที่นำเข้าว่าตรงกันหรือไม่
 - (จ) กรณีงบการเงินมีงบประกอบหรืองบย่อย ต้องสามารถแสดงรายละเอียดของงบประกอบหรืองบย่อยซึ่งเป็นที่มาของงบการเงินรวม (consolidate) เป็นรายงานด้วย
 - (ฉ) สามารถบวกลบรายการท้ายงบการเงินเพื่อการคำนวณกำไรสุทธิที่ต้องเสียภาษี และมีรายงานซึ่งระบุที่มาของรายการ เช่น Document Number ด้วย และ
 - (ช) ไม่สามารถ Post Sale ได้โดยไม่ Post ภาษีมูลค่าเพิ่มพร้อมกัน
- (3) เป็นโปรแกรมที่มีระบบรักษาความปลอดภัย เพื่อควบคุมการเข้าถึงข้อมูลได้ โดยต้องระบุระดับเจ้าหน้าที่ที่สามารถบันทึก อ่าน หรือแก้ไขข้อมูลได้ หมายความว่า
- (ก) สามารถแสดงภาพการทำงานรวมของระบบ (System Flowchart)
 - (ข) ให้แสดงระดับการปฏิบัติงานของเจ้าหน้าที่ที่หน้าจอ โดยระบุ จำนวน และระดับเจ้าหน้าที่ที่สามารถบันทึก อ่าน หรือแก้ไขข้อมูลได้
 - (ค) โปรแกรมและแฟ้มข้อมูลมีการควบคุมโดยใช้รหัสผ่าน (Password) และการตั้งรหัสผ่านสำหรับผู้แก้ไขต้องตั้งเพิ่มแยกต่างหากจากส่วนอื่น
 - (ง) มีรายงานบันทึกการใช้รหัสผ่าน (Password) ในการทำงานโดยระบุให้ทราบถึง รหัสประจำตัวของผู้ปฏิบัติงาน งานที่ทำ และวันเวลาที่ปฏิบัติงาน สำหรับรายงานการแก้ไข ต้องระบุให้ทราบถึงรหัสประจำตัวของผู้ปฏิบัติ จำนวนและรายละเอียดของรายการที่มีการแก้ไขปรับปรุง และ
 - (จ) ถ้าแฟ้มข้อมูลมีการควบคุมโดยการ Encryption เพื่อป้องกันการเข้าถึงข้อมูล ถ้ามีการทำ Decrypting ต้องบันทึกหลักฐานไว้ทุกครั้ง เพื่อทำรายงานได้"

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ 1 มกราคม 2539 เป็นต้นไป

ประกาศ ณ วันที่ 1 สิงหาคม พ.ศ. 2538

จตุมงคล โสณกุล

(ม.ร.ว.จตุมงคล โสณกุล)

อธิบดีกรมสรรพากร

**EDP Supervision
of Financial Institutions**

***SEACEN* Course on**
Computer Audit (Advanced Level)
Bangkok,

1 November - 3 December 1993

EDP Supervision of Financial Institutions

November 2, 1993

MR. METHA SUVANASARN
DIRECTOR
NORTH EASTERN REGION BRANCH
BANK OF THAILAND

	Page
1. Introduction	313 - 314
2. Historical Development of Computerized Banks in Thailand	315
2.1 ATM	315 - 317
2.2 Electronic Funds Transfer	317 - 318
2.3 Electronic Banking	318
2.4 Other Services	319
2.5 New Payment System	320 - 321
3. Electronic Banking Measures, Rules and Regulations	322
3.1 EDP Examination	323 - 324
3.2 Electronic Banking Permission	325
3.3 Security Requirement for Commercial Bank Operating the Electronic Machine Services	325 - 329
3.4 EDP Audit Requirement	330 - 331
3.5 Revision of Banking Act and Other Regulations	332
3.6 Expansion of Customer Services	332 - 334
3.7 Contingency Plan	335 - 336
3.8 External Auditor	336
3.9 Minimum Standard of Information	337
3.10 Data Processing by Third Party	337

	Page
4. EDP Examination	338
4.1 Objectives	338
4.2 Scope of Examination	338
1) Data Center Operations	339 - 342
- Management	
- System Programming and Documentation	
- Computer Operation & Security	
- Computer Audit	
2) Application Systems	342 - 343
- Data Input	
- Data Processing	
- Data Output	
4.3 Examination Findings	343 - 352
1) Data Center	
2) Applications	
3) ATM	
4) SWIFT	
5. Computer Assited Audit Techniques	353 - 354
6. Conclusion	355

7. Appendixes

Appendix 1 : The historical development of electronic banking in Thailand	356
Appendix 2 : Conditions in granting permission to commercial banks in providing ATM services within bank premises exceeding working hours	357 - 359
Appendix 3 : Conditions in granting permission to commercial banks in providing the electronic machines services off bank premises.	360 - 363
Appendix 4 : Chronological records of electronic banking measures.	364 - 367

1. Introduction

Due to the rapid development of the Electronic Data Processing (EDP) technology, computers are now widely and intensively used in many fields, especially in banking and finance industry. The accuracy and the ability to accomplish volumes of transactions at economical cost together with the advanced communication technology contribute to the development of new customer services, collectively called "Electronic Banking". These new services can provide the better and more efficient services to customers.

However, the computerization of banking activities has altered the traditional control mechanism relating to accounting and reporting system. For example, the normal ledger card system is now replaced by computer files residing in magnetic storage media, such as disk packs and magnetic tapes. The traditional notion of separation of duties--such as separate individuals should be responsible for initiating transactions and recording transactions--does not always apply. Adequate documents and records that are necessary to provide the audit trail of activities within the system may not be used to support the initiation, execution, and recording of some transactions. Moreover, some transactions may be activated automatically by a computer system. Thus, no visible audit or management trail may be available to trace the transaction. In addition, computer control technology is more complex than manual system control technology. Consequently, it is more difficult to understand controls and to collect evidence on the reliability of controls.

From the supervisory agency's point of view, the new services concerning electronic banking facilities, the inherent risks of computerization, and the complex computer controls contribute to the development of EDP supervision.

The aim of EDP supervision is basically still the same as any form of supervision of financial institutions, i.e.,

- to protect the interest of the depositors,
- to ascertain whether the financial institution is complying with applicable laws and regulations,
- to appraise the financial conditions and operation including systems and control of the financial institutions.

However, in the case of EDP supervision, the supervisory agency would also have to ensure that there is a high level of public confidence in the electronic banking services provided by the banks, such as the safety of customers using the ATM, the continuation of operation, the security measures, etc. As mentioned earlier, traditional control has taken a new form and audit trails also changed significantly. Thus, the supervisory agency needs to enhance its capacity to identify risks associated with electronic banking and needs to provide its examiners with new set of skills and techniques to cope with EDP operations.

2. HISTORICAL DEVELOPMENT OF COMPUTERIZED BANKS

Electronic Banking has been offered to customers since 1970 (See Appendix I), the Bangkok Bank Ltd. implemented its first Online Deposit System at its head office. With further development by 1975 the new banking concept had facilitated the process of funds transfer within the Bangkok Metropolitan area.

A few years later, many other banks had been computerized and had implemented their computer networks. By 1980, a number of decentralized computer centers were installed in the major provinces nationwide.

2.1 ATM

By January 1983, the Electronic Banking evolution in Thailand had been recognized when the first full function of the Online Automatic Teller Machine (ATM) was first introduced by the Siam Commercial Bank Ltd. The customers' response and acceptance of the services were beyond expectation. Within a year, the Siam Commercial Bank has experienced an increase of customers by 30%.

Consequently, this service innovation has created an intense competition among banks. Some banks feel obligated to invest in the new services in order to keep up with their competitors.

During the year 1983-1984, the ATM program rapidly gained acceptance from the commercial banks as well as the customers. A total number of 515 ATMs had been ordered into the country, of which 107 machines were in operation. Two of them were located in a regional area with over 300,000 cardholders.

In December 1984, the Bank of Thailand issued a major guideline on electronic banking development, by requiring banks to offer shared ATM services within one year if they wish to operate the services exceeding working hours. Each shared service or "pool" must be comprised of at least 3 banks.

In response to the Bank of Thailand guidelines, the first ATM pool was established in February 1985. Within one year three additional pools were set up.

However, the ATM programs still played an important role in the year 1985. There were 12 local banks offering services with a total of 431 machine installations, serving approximately 1.8 million cardholders.

Early in 1986, Two local banks implemented their ATM services. The Shared ATM concept has shown some degree of success, since two pools comprising 7 local banks have agreed to merge. The services have been made available throughout the Metropolitan area and expanded to all countrywide regions.

As for the year 1987, Two ATM pools have jointly signed an agreement on the operation of the sharing through the switching center. Banks have also introduced new ATM products to customers by interchanging services with international credit card companies. This enables their customers to withdraw cash from corresponding ATMs worldwide and vice versa. Another feature of the ATM is that the Thai Farmers Bank Ltd. was the first to offer Mobile ATM services.

At the end of July 1993, commercial banks offered ATM services through 1642 ATM points, serving over 10 million cardholders. All local commercial banks agreed to establish "National ATM Pool" in September 1993.

2.2 Electronic Funds Transfer

Another step forward was taken in electronic banking development when an "Electronic Funds Transfer at Point of Sale" service (POS) was first offered by the Bangkok Bank Ltd. in May 1985, this was followed by the Siam Commercial Bank Ltd.

and the Thai Farmers Banks Ltd. In October, the three banks reached their agreement on a Shared-POS terminals at 38 different retail outlets. Later on in December, The Thai Military Bank Ltd. joined the Shared network.

The Bank of Thailand and eleven local banks have taken full advantage of the electronic funds transfer system. They became members of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) Organization, which began its operation in September 1985. The regional center was located at the Bangkok Bank Ltd.'s head office. It was linked to the primary center in Virginia, USA. This service allows the transferring of funds and information with fast speed and security among their members worldwide.

2.3 Electronic Banking

In term of new service competition, more of the new products that have been offered in 1985 included: Tele-Banking, Office Banking, Video Banking, Information Banking, Cash Management, Credit Card Authorization (Verifone), and Badge card reader (BCR)/Pin Pad services.

Furthermore, the first full array of self-service banking was introduced by the Siam Commercial Bank Ltd., called "The Computer Branch" service. The services are offered by placing all of their self-service facilities in the branch lobby including the Personal Banking, Current Account Statement Inquiry, ATM, Tele-Banking, Info Banking, Graphic Banking, and Videotext Banking.

2.4 Other Services

In September 1988, the Bank of Ayudthaya was the first to launch Disaster Recovery Services to the customers with two service options. One is data depository service and the other is computer backup service. The data depository service is available for any institutions. Meanwhile, the computer disaster recovery service is available only for IBM 4381 mainframes and the IBM System 36. The number of customers for this service is limited to only five for each system. In case of the disaster affecting the computer system, the bank can restore the data and provide their services within 24 hours.

The new service concept is now being developed. The Thai Bankers Association, together with the Board of Trade and the Federation of Thai Industries have jointly formed a non-profit organization to set up a computer center that provides a database for all necessary financial and business information. This computerized trade data center was first discussed two years ago, with costs estimated at around 70-80 million baht. They also hope to store business and financial data from overseas sources in the future.

2.5 New Payment System

Rapid growth of financial activities and the trend of more transaction volume of paper notes, large value funds transfer, retail funds transfer, and the global trends toward computerization of the payment system contribute to the development of new Thai Payment System. The Master Plan has been developed in accordance with the acquired information from the Bank of Thailand, commercial banks, and other concerned parties. The overall goals of new payment system are summarized as follows:

- lessening cash and paper notes dependency rates
- low dishonored cheque rate
- higher usage of electronic funds transfer system throughout the country

In response to the overall goals, a system development plan, consisting of three phases, is established. In Phase I, the main tasks are to construct a sound and computerized financial system in the Bangkok Metropolitan Area in order to better perform cheque clearing, large value funds transfer, and off-line retail funds transfer. Online retail funds transfer will be improved by commercial banks meanwhile.

The second phase focuses on extending the service area, providing more services, and increasing the functions of the system. As a result, the large value funds transfer will be available in the areas outside of Bangkok and the clearing and settlement of both government and Bank of Thailand's bond will be in service. Finally, the use of on-line file transfer for large volume of low value transactions will also become part of the system functions.

In the third phase, the payment system is looking to integrate such independent financial systems like Financial Information System and Credit Information System.

However, prior to introducing the new payment system, four major tasks deserve contemplation: operational preparation for the new system, establishment new rules and regulations, establishment of rule book, and manpower development. Furthermore, relevant banking rules and regulations which are made in reference to contemporary ones in the major leading countries would need to be established before the system is actually implemented.

3. Electronic Banking Measures,
Rules and Regulations

The rapid development of computerized banking and communication technology has an impact on the supervisory role of the Bank of Thailand in the following manners:

- the examiner is no longer able to trace transactions because of the elimination of audit trails.
- new characteristics of the internal control are required to ensure sound EDP practices.
- the existing laws and regulations do not clearly cover the EDP operation of computerized banks.
- EDP technology also introduced new risks that may not be recognized by bankers and regulators.

From those reasons and necessities, the Bank of Thailand had reviewed and modified former rules and regulations to oversee the electronic banking activities as follows:-

3.1 EDP Examination

During the past year 1970-1981, commercial bank examination has always been concentrated on the financial examination by way of evaluating the documents, reports and financial statements that were produced by the computer. Only with the commercial banks provision of informations, verification of data accuracy and reliability had been limited. There had been a gradual increase in the examiner's concern on how to maintain their role and capability toward banking examination in the most effective and appropriate manner. Until 1972, the Bank of Thailand had set up a working group of the examiner to study the feasibility and guideline on the electronic data processing examination.

Sequences of EDP examination development :

- 1) The manual or guidelines on how to use commercial bank computerized report, had been developed in order to support the financial examination that include :

- 1.1) Summaries of reports to be used in the examination on each Application System such as Deposit Accounts, Loans, Customer Account Informations, Classified Debt, etc.

- 1.2) Reports and Transactions Code definition.
 - 1.3) Report frequency such as daily, weekly, monthly, semi-annually including the reports and file retention period.
 - 1.4) Reconcilement of report total and control account.
-
- 2) In 1981, the EDP examination section was established with the primary duty and responsibility for examining the commercial banks computer system.
 - 3) In 1982, the Minimum Standard Requirement on computer system development and operation was issued with the objective of providing commercial bank guidelines on the EDP operation and the EDP examination scope.
 - 4) The commercial bank EDP examination was first conducted in 1983.

3.2 Electronic Banking Permission

ATM has been playing the important role in Banking business in Thailand since 1983, so a lot of electronic machines have been imported to install nationwide. Therefore, at the beginning the Bank of Thailand had to establish the rules and conditions in granting permission of ATM services (see appendix 2 and 3). Due to the policy of deregulation, finally in October 1992, ATM services have no longer been to obtain an approval from the Bank of Thailand but the commercial bank have to notify Bank of Thailand at least 7 days prior to beginning and stopping of services. However all commercial banks operating electronic machine services are still required to have security system and EDP audit coverage.

3.3 Security Requirement for Commercial Bank Operating the Electronic Machine Services

The minimum standard requirement on security procedures.

1) Segregation of duties and responsibilities in the following functions.

- System Development
- System Maintenance
- Equipment Maintenance
- Customer card generation
- Customer PIN generation
- ATM cash handling
- Network management and control

- 2) Adequate documentation must be maintained and shall include the following standards and guidelines.

2.1) System Manual

- General system and network description
- Computer equipments currently in use and backup equipments.
- Data management and backup data file
- Interrelationship of all application systems and control function
- Output report description of all applications

2.2) Program Description Manual

- Detail description of the individual program includes the objective, function processing instruction and the inter-relationship to the other program.
- Program listing
- Editing and control procedures
- Record of all program changes and system modification

2.3) User Manuals

- Description of function and their responsibilities.
- User operation instruction
- Error and problem resolution procedure

2.4) Electronic funds transfer system documentation.

- Equipment description
- Customer card
- Customer personal identification number
- Program messages
- ATM Cash Handling
- Data Communication command and messages
- Receipt of Fund Transfer Transaction
- Mechanism of cash dispensing devices
- Deposit and payment handling
- Transaction Logging

3) Data communication control and security

3.1) Access control over communication lines and devices.

3.2) Data communication backup system

3.3) Log all transactions to includes

- Location or devices identification code
- Date and time of transaction
- Type of transaction
- Customer card and account number
- Transaction amount

4) Customer Security

- Must have written notice to educate the customers on usage and safeguarding of the ATM card and PIN including warnings and precautionary measures for any possible loss.
- Must have written contract agreement stating the liabilities of commercial bank, customers, and all relevant parties. Advanced notification must be given to the customers if there are any changes in terms and conditions.
- Must not disclose customers' information.
- Must provide warning message or protective device to prevent the customers' failure to retain their card and receipt of transaction after the completion of transaction.

5) Site Location Security

- The terminal devices must be situated publicly in an open area with sufficient lighting for illumination.
- Must install alarm system or other security device.

- 6) Insurance coverage that provides adequate protection for financial losses or other disastrous consequences.
- 7) Must have an effective contingency plan that includes the following measures.
 - 7.1) Physical Protection and Emergency Plan to minimize exposure or probability of threats to the computer operation such as fire, flood, natural hazard and equipment failure, etc.
 - 7.2) Recovery Plan that clearly defined methods and procedures for system recovery.
 - 7.3) Backup Plan that provides minimum requirement as follows:
 - Must provide a backup capability for data facility.
 - Backup procedures and operational instructions including the use of alarm or security device to prevent and detect possible threats to the system.
 - All security plans must be maintained and tested periodically.
 - Designating contingency personnel and their responsibilities.
 - Determining criticality function in order to define backup processing requirement.

3.4 EDP Audit Requirement

Commercial banks must perform a computer audit at least once a year within 12 months comprising a minimum audit scope as follows:-

1) Computer Audit Coverage:

1.1) Electronic Data Processing Operation

- Organization Data Center audited
- Applications and Programs
- Data Management and Controls
- Computer Operations
- Data Communication System
- Electronic Funds Transfer System
- EDP services provided by other organization or Service Bureau

1.2) Computer Application

- Documentation
- System Test
- Application and Program Maintenance
- Data Access Control
- Data Files and Programs Control
- Backup System

1.3) Financial loss caused by computer operation or computer internal control weakness of following cases.

- Failure or destruction of the computer system, equipment, peripheral, Application Systems, and Data Communication System.
- Fraud, theft or any loss which caused by bank employee or outsider.

2) Audit Information

2.1) Name, Location and opening date of the Data Center audited.

2.2) Date and Time of Audit

2.3) Sequence of the audit and date of the last audit

2.4) Auditor's name

2.5) Details of audit findings and recommendations

2.6) Description of financial loss resulting from computer abuse or computer internal control weakness includes:

- Definition of error or loss
- Cause of error or loss
- Amount of loss
- Preventive measure implemented

2.7) Application System Audit Documentation.

- Organization of the Department audited.
- Detailed Description of Equipment and program change.

3.5 Revision of Banking Act and Other Regulations

Banking Act

In May 1985, the Bank of Thailand formalized the enforcement policy to amend the law on commercial banking. Regarding the electronic banking examination practice, revision had been made on section 35, to empower the examiner to examine banks' electronic data processing system and/or their EDP servicers.

Performance Report

To monitor and review commercial banks performance, on July 30, 1986, the Bank of Thailand has requested banks to submit their Statistical Service Performance Report on the electronic banking products include the information such as the total volume of transactions per day and per month, total number of cardholders or customers, and the volume of other banks' customer transactions. In addition, on April 17, 1987, the Bank of Thailand required that performance reports shall be submitted semi-annually.

3.6 Expansion of Customer Services

Focusing more on the deregulation aspect, the Bank of Thailand has allowed commercial banks to offer Financial Information services such as inquiry of the Security Exchange,

Interest Rate , Exchange Rate and other Financial Information daily for 24 hours without requiring permission. However, banks must notify the Bank of Thailand 7 days in advance before the scheduled opening day.

Toward the end of the year 1987, on Nov 3, the Bank of Thailand has announced major deregulation measures designed to enable banks to adjust their operations in order to cope with changing economic situations, to make them more flexible and to help them to expand their customer services by allowing banks to operate more businesses. Banks are allowed to do the following businesses.

1) Selling their developed computer programs including their application program development, under the following conditions:

- (1) The Sale must not be performed as part of normal business.
- (2) The Application programs must be in connection with financial services.
- (3) The provision of the services, must be developed in such a manner that they will increase the utilization of existing resources.

2) Providing the Security Exchange service by allowing the customer to buy and sell securities through the bank communication network.

The following conditions must be complied with :

- (1) The provision of the services must be operated by utilizing more of existing computer resources.
- (2) Banks must allow any security company to become a subscriber for the service, and they shall not adopt protectionism against any trade or business.
- (3) Banks are allowed to offer only the security informations and the funds transfer services, but are not allowed to perform any activities which may be defined as a security business.
- (4) In the primary stage, banks shall not provide such business within bank premises. The customers can only operate the facility at their houses or offices.

3.7 Contingency Plan

On December 24, 1987 the Bank of Thailand has invited commercial banks to attend meeting on the subject of the development of an Emergency Plan and the computer backup system. The meeting was held on January 14, 1988. The Bank of Thailand has alerted commercial banks to the importance of a Contingency Plan for electronic data processing support which is one of the methods used in the EDP industry to reduce the potential impact of the loss of the EDP service. Banks should develop an effective Contingency Plan that includes provisions for off-site backup of critical data files, software, hardware, documentation, form, and supplies as well as alternate means of processing transactions electronically or manually. Bank management should review and employ the most appropriate method for its organization.

Concentrating the security system enforcement the Bank of Thailand has issued its latest guideline on June 23, 1988, requiring banks who offer electronic machine services, to develop an effective contingency plan with the following conditions:

- 1) Commercial banks must develop a contingency plan that provides an alternative backup system off-premises and shall be completed within the year 1989 unless permission is granted 45 days before the scheduled date.

2) Starting from 1990, banking service disruption due to the failure of computer processing support, may not exceed 1 working day or 24 hours unless permission is granted.

3) To minimize cost and fully utilize resources, commercial banks are suggested to select the following appropriate methods:

3.1) Banks may enter into agreements with other banks or institutions to provide each other with equipment backup, or

3.2) In cooperation with other banks or institutions to form a group or organization to own and operate the facility.

3.8 External Auditor

According to the Auditing standard no.28 and 29 issued by the Auditing Standard Board in March 1990, the chartered accountants in Thailand are required to evaluate internal controls in the EDP environment system and are insisted to use computer as an audit tools. And prior to the appointment, commercial bank & financial institution's auditors have to submit their audit programs to the Bank of Thailand for approval.

3.9 Minimum Standard of Information

In April 1991, minimum standard of information was set as the guidance for designing and keeping of data processing records required to expedite supervisory examinations.

3.10 Data Processing by Third Party

Commercial banks and /or financial institutions may have their data processed by the data processing servicers or third parties. When EDP is performed off premises (local or abroad), the processing integrity and controls similar to those of in-house data processing must be maintained. So, it is necessary for the commercial banks and/or the financial institutions to obtain the permission from the Bank of Thailand. In granting of that permission, the Bank of Thailand established the conditions that they have to make the agreement with the servicers or third parties to allow the Bank of Thailand's examiners to perform the EDP examination at the data center of the servicers or third parties.

4. EDP Examination

4.1 Objectives

The aim of EDP examination is to evaluate the risks and controls which affect the accuracy of financial data and the continuity of operation. In a computer system many different controls are used to maintain data integrity and continuity of operation. The major types of controls are general controls (or data center controls) and application system controls. All these controls will be discussed in details later in this course. In case that an inadequate control is identified, the supervisory agency should determine the areas where control is needed and the corrective action to be taken.

4.2 Scope of Examination

In discussing the scope of examination, let us divide an EDP examination into two basic areas: Data Center Operations and Application Systems.

1) Data Center Operations

- Management
- System Programing and Documentation
- Computer Operation and Security
- Computer Audit (Internal & External)

2) Application Systems

- Data Input
- Data Processing
- Data Output

1) Data Center Operations

In conducting EDP examination, examiners must first evaluate data center controls or general controls which govern the operation and management of computer processing activities. In other words, general controls are the organization, management and operation controls within data center.

Management

A data center may have the best controls ever designed, but if management is weak and unable to enforce them, then the set of controls might as well not exist. The most important responsibility of management involves formulating a set of organizational controls and the general security standards. Examiners should ensure that the basic security measures are set and put in place.

System Programming and Documentation

All programming functions, especially systems development and documentation, should be guided by written standards and procedures. A series of standard manuals should be written to cover :

- System design : To guide the creation of effective, efficient and control oriented application systems.
- Software analysis and selection : To ensure the purchase of quality software from vendors at the most reasonable price.

- Programming : To ensure that desired features and controls are included in application programs.
- Documentation : To record both the essential elements of the data processing application and the logic of the computer programs. Documentation is the basic source of information for those who audit, maintain, operate, and use the system.

Examiners should ensure that system development procedures are followed and closely monitored as written in standard manuals. Moreover, documentation should be complete and up to date.

Computer operation & security

Data center has responsibility for the daily running of hardware and software resources. Specifically, it performs several major functions :

- (a) operation of the hardware and software;
- (b) communications network control;
- (c) data preparation;
- (d) production workflow control;
- (e) control over the data, program, and file library;
- (f) control over the documentation library; etc.

While these functions appear somewhat routine and mundane, their proper performance is critical if effective controls are to be exercised over the operations. Examiners must ensure that methods and performance standards exist for

each function, high-quality personnel are hired to perform each function, personnel should not be assigned duties that will conflict with their responsibilities. For example, the computer operators should be restricted to the mechanical operation of the system, i.e., they should not be required or allowed to perform any input preparation, output reconciliation, financial accounting, programming or similar duties.

Besides evaluating computer operations, examiners need to evaluate security measures to ensure that it can prevent, detect and minimize loss from damage or unauthorized use of equipment, personnel, software or data. An overall security measures includes : physical protection of the data facility; emergency procedures; and a disaster recovery plan. Controls and procedures, such as backup, housekeeping, auditing and documentations, supplement the protection provided by security measures. These security measures are formulated to maintain data integrity and the ability of the system to survive hazards or to continue operation in case of disaster.

Moreover, computer security does not only involve protecting the data against unauthorized access, but also the computer center itself is well-protected. In evaluating physical security, examiners should pay special attention to the major types of threats that may compromise physical security in the computer center : fire, water or flood, energy variations, structural damage, pollution, and unauthorized intrusion.

Computer Audit (Internal & External)

To ensure that security measures and controls of EDP operations are adequately put in place, an independent audit must be performed. This audit should be performed by a qualified person, internal auditors or external auditors who are capable of evaluating EDP controls. Examiners should evaluate the performance of internal auditors or external auditors (EDP audit coverage) in the following manners :

- Qualifications and independence of auditors.
- Scope of the audit.
- Frequency of the audit.
- Techniques to be used.
- Audit findings.

2) Application Systems

Besides evaluating data center controls or general controls, examiners must evaluate application controls embedded in some significant application systems. Application controls are the specific controls included in the computer programs or manual procedures of an application. Examiners need to identify significant application controls and determine how controls operate by conducting detailed examinations of documentation, interviewing EDP and user department personnel, and observing operation of application controls. And then the examiners should perform compliance test where they consider necessary.

In evaluating application controls, examiners should emphasis on three areas below :

- Data Input - To ensure whether controls prevent or detect loss, errors or omissions in recording, preparing, and entering data for processing.
- Data Processing - To ensure whether correct files and programs are used in processing.
- Data Output - To ensure whether preparation and issuance of output, and reports are properly controlled.

4.3 Examination Findings

Some of the problems confronting us during the auditing period are related to data center and application system, mangement and controls.

1) Data Center

- Contingency plan is either insufficient or not up to date.
- Lack of segregation of duties and inadequate measures on physical security.

- System documents are not updated periodically.
- Backup files are not kept separately from regular files.
- Physical and logical access controls to computer center, system and data are not sufficient and enforced.
- Inadequate control on a program modification.
- Insurance policies are inadequate and do not cover all computer losses.
- Inadequate preventive measures and controls on computer operation such as using of no internal file label, if an operator picks up wrong files, it would cause a serious damage.
- Improper project management, no feasibility study and no system development and system operation performance evaluation, these may lead to over expenditure or project failure.
- Lack of internal audit, especially computer center audit.

- Lack of consistent reviewing computer activity logs.
- Inconsistent preventive maintenance of computer hardware.
- Prompt implementation of developed programs without adequate program testing.
- Inadequate control over utility programs
- Internal auditors do not involve during the system development cycle, so some critical internal control may not be set.
- No errors and problems reporting from users.
- No system and program development standard.
- Lack of emergency warning system and fire-distinguisher in the computer room.
- Incomplete log for computer system and computer room.
- No operator in the computer room when a vendor system engineer comes to repair computer hardware.

2) Applications

Input

- Check digit calculation module is not well developed, errors appear when issuing some account number to different branches in the on-line system.

- Open new account transaction can be performed inter-branches which is unsafe and can cause fraudulent.

- Cheque return transaction can be performed although no cheque has been deposited on the previous day.

- In the deposit program safeguards are inadequate in effect to ensure that access control for authorized personnel only.

- Program on-line interactive branches do not have an adequate procedure and control on interbranch correction transaction, will enable on-line terminal to delete financial information from master file.

- Back dated of withdrawn transaction can be performed in order to be pass the authorization in the case of overdrawn.

- Teller can perform a back date transaction to correct other transaction without any authorization from the supervisor which does not comply with a good internal control system that all correction transactions should be authorized.

- New interest rate is not correctly adjusted and it leads to an error in interest calculation.

- When performing a loan-offering transaction, programs do not check for the credit limit approved by an authorized officer.

Processing

- Close-system transaction, delete-master-file transaction and hold releasing transaction can be performed at the Bank Branch which is unsafe. It should be performed only at Head Office.

- Some transactions such as cash-withdrawal transaction, transfer withdrawal transaction, accumulated-interest adjustment transaction. O/D-limit addition and deletion transactions are actually performing at the bank which is not the account-owned branch. This is very unsafe and expose to a high risk.

- The program procedure on current deposit does not include control over the maximum amount of transfer-deposit transaction which should be set in order to limit a risk exposure in the case of fraud.

- O/D interest-calculation program logic is not flexible because it uses the maximum interest rate in stead of the specific rate of that O/D line credit set between the customer and the bank.

- A computerized branch did not delete conversion programs and the branch still kept them on files. With ineffective, preventive control, will lead to the fraud and illegitimate changes of fields in the master file.

- Over-limit withdrawal can be performed without any authorization

- Programs do not have control over the customer cheque number withdrawn, the already paid cheque may be repeatedly negotiated.

- No authorization on customer cheque number issued, then the program can not check whether the negotiated cheque had been already paid or not.

- Programs do not have cross check procedure transaction between the old and corrected one.

- When a cheque return transaction occurs, programs do not verify available balance. It calculated the interest for overdrawn even is not the case.

- No-book withdrawal transaction can be performed by a bank branch which is not the account-owned branch. This is very unsafe and expose to a high risk.

- Programs do not have control over deposit number for withdrawal correction and partially withdrawal correction transaction, the corrected transaction may not be complied with the original one.

- The system programs do not have control on bank code for a correction transaction of cashier order & cheque clearing deposits, so the corrected transaction will not be complied with the original one.

- When a no-book withdrawal correction transaction is performed, programs do not automatically decrease accumulated tax charged on interest, so the tax amount is overstatement.

- The system does not have procedure programs allowing print a no-book withdrawal correction transaction in a customer's passbook, and it shows incompletely all the transaction that have already been done.

- Insufficient field length may cause error if the deposit is more than 999 days because the field lenght was limited only to 3 characters.

Example 3 yrs. fixed deposit

3 yrs. = 365 x 3 = 1,095 days

1_0_9_5_

this field keeping
number of days used
in interest calculation
provides only 3
character space.

"1" will disappear when
character space is overflowed

When programs calculate interest amount, it uses 95 days
in stead of 1,095 days.

- Teller has never been told that partial withdrawal has
the same effect as releasing total hold amount of that deposit
number.

- Back date transaction can be performed exceeding the
account open date and the back date deposit can be performed
with highly amount without any authorization.

- Program do not have control over compliance between
withdrawn amounts and hold amounts.

- For the amount hold transaction, programs do not check
whether that account has any on-process collected clearing
cheque. If the cheque is returned for any purposes, it can
cause damage to the bank.

- When a cheque return transaction occurs, programs would calculate interest by using the date as an effective date instead of the cheque deposit date.

- Programs do not check an effective date in the case of interest rate change.

- Account-balance hold releasing transaction can be performed without any authorization.

Output

- Interbranch transactions report does not include in house branch report, leads to insufficient audit trails.

- No special report of master file data when added, deleted or modified.

3) ATM

- Inadequate controls over keys and passwords used for access to ATM machine and money cartridges inside.

- Lack of control on segregation of duties between ATM card keeper and PIN keeper.

- ATM application programmer knows both an A-key and E-PIN key (A-key used for decrypt E-Pin key by DES algorithm and acquire the top executives' pin) and can access to DES algorithm, cardholder file and PIN generated program module, so he can illegally produce all customer PINs by using the top executives' PIN and customer card number from cardholder file processing through DES algorithm and PIN generated program module.

4) SWIFT

- Authenticator key file used for network security is casually kept in the cabinet in the SWIFT terminal room.

- Inadequate control over log-in table which is used for access to SWIFT network, an unauthorized person who knows it and can access to the terminal is able to perform some transaction.

5. Computer Assisted Audit Techniques

Computer can be used as an audit tool for testing and collecting evidences on the examination of financial institutions. It can improve examination coverage and reduce the cost of testing and sampling which would otherwise be performed manually.

With software developed for audit purpose, examiners can use a computer to :

- Test footings and computations to verify the correctness of EDP outputs.
- Test records for completeness, logical consistency, validity of conditions and reasonableness of amounts.
- Summarize data and analyze performance.
- Select and print data by the use of statistical sampling techniques for confirmations, etc.
- Independently simulate processing of transactions to verify the correctness and consistency of computer programs.
- Generate audit trial balances and related reports.

Audit software may be developed by examiner or audit staff or offered by equipment manufacturers, audit firms, and independent software houses.

Bank of Thailand has been developing a tentative audit software that can prepare audit reports and test the accuracy of interest calculation of the promissory notes. However, this tentative audit software has its limitations

and is not flexible. It can not use with other applications that have diverse characteristics, different hardware and software environments, different data structures, different record formats, etc. And it is beyond our capacities to develop an audit software for every system that will extract, manipulate, and report data required for audit purposes. Therefore, the Bank of Thailand decided to purchase a generalized audit software package that can provide powerful data retrieval, data manipulation, and reporting capabilities, specifically oriented to the need of examiners. However, the effective and efficient use of the software requires an understanding of both its capabilities and limitations.

6. Conclusion

An EDP supervision does not only involve regulation which sets up the various guidelines that financial institutions have to follow, but also involves on-site examination which reveals whether financial institutions observe those rules and regulations and have safe and sound EDP operations. In an EDP examination, the role and the performance of examiners depend on their technical knowledge and skills, especially EDP audit techniques. Therefore, in the rest of this Course, we would be taking a closer look at EDP examination scope or different areas that examiners have to look into. As a result, we can determine what are key EDP issues and their related controls. Moreover, we will look at EDP audit tools and techniques and learn how to use them in such an effective manner.

Thank you.

Appendix 1

The Historical Development of Electronic Banking in Thailand

<u>Year</u>	<u>Services</u>	<u>Leader</u>
1970-1974	- In-house Deposit Application	Bangkok Bank Limited
1975-1979	- On-line Deposit Application in Bangkok	Bangkok Bank Limited
1980-1984	- On-line Deposit Application in Provinces	Bangkok Bank Limited
	- ATM	Siam Commercial Bank Limited (1983)
	- SWIFT	Bangkok Bank Limited (1984)
	- Tele-Banking	Siam Commercial Bank Limited (1984)
1985	- POS Pool	Bangkok Bank Limited
	- ATM Pool	4 Pools
	- BCR (Badge card reader)/Pin Pad	Bangkok Bank Limited
	- Office Banking/Video Banking/Info Banking/ Cash Card Authorization	Bangkok Bank Limited
	- Credit Card Authorization	Thai Farmers Bank Limited
1987	- Mobile ATM	Thai Farmers Bank Limited
	- Computer branch or Self-service electronic banking corner	Siam Commercial Bank Limited
1988	- Electronic mail	Bank of Ayudthaya Limited
	- Disaster recovery services	Bank of Ayudthaya Limited
	- Second site back up services	
	- Data Depository Services	
	- Security Exchange Information Services	Bangkok Bank Limited
	- Computer back up center	Bangkok Bank Limited and Thai Farmers Bank Limited
1989	- Clearing cheques	Some local commercial banks
1991	- Credit card information service bureau	Medium-sized local commercial banks
1993	- National ATM Pool	All local commercial banks
	- Worldwide ATM Service	Bangkok Bank Limited
	- Electronic cheque Clearing System (ECS)	
	- Off-line Retail Funds Transfer System	During implemented by Bank of Thailand
	- Inter-bank Funds Transfer System (Large Value)	

Appendix 2

Conditions in granting permission to commercial banks in providing ATM services within bank premises exceeding working hours:

Prior to rendering the services :

Prior to rendering the services, Commercial banks must inform the Bank of Thailand at least 7 days in advance with detail information as follows:

1. Name of the opening branch
2. Estimated customers per month
3. Service function provided
4. Total number of machine provided
5. Schedule opening date and time.
6. Installation layouts illustrating the location of the machine.
7. Day and hours of service provided
8. System specification including the machine model, vendor name, and machine rent or purchasing price.
9. Detail or draft of contract agreement between customer and bank.
10. Operation instructions and procedures.
11. Security System complying with the minimum security requirement as prescribed by the Bank of Thailand.

After rendering the service:

After service has been offered, commercial bank must comply with the following conditions:

1. From the first operating day, commercial banks must have at least two other banks jointly provide the services.
2. Electronic machine shall provide service function of cash withdrawals, cash or cheque deposits, transferring of funds, account balance inquiry and other services as prescribed by the Bank of Thailand.
3. Commercial banks must notice the service providing days and hours at the machine site location.
4. Commercial banks must notify the Bank of Thailand 3 days in advance before changing the service providing hours that have been permitted even still in the same period of time permitted.
5. Commercial banks must install the electronic machine in an area that are exclusive from the main office area.

6. Commercial banks must implement the security procedures as prescribed by the Bank of Thailand. Prior to modifying the computer application system or changing in term and conditions, commercial banks must obtain an approval from the Bank of Thailand provided with the explanation of reasons and its impact to the security and control systems.

7. Commercial banks must conduct a computer audit at least once a year, with a sufficient audit scope as prescribed by the Bank of Thailand. For each audit performed, a copy of audit reports, relevant instructions and recommendations must be submitted to the Bank of Thailand within 45 days from the audit date.

Appendix 3

Conditions in granting permission to commercial banks in providing the electronic machines services off bank premises.

Commercial banks that have been authorized to provide the electronic machine services, may submit the application to provide the electronic machine service off bank premises at all time, and must contain the following documents:

1. Business in the area or location where the electronic machines are installed, with a map illustrating the financial institutions within 500 metres.
2. Estimated transactions per month.
3. Service function provided.
4. Total number of machine provided.
5. Designated branch office that responsible for the installation operation.
6. A map illustrating the machine location.
7. Day and hours of service provided.
8. System specification including the machine model, vendor name, and machine rent or purchasing price.
9. Detail or draft of contract agreement between customer and bank.
10. Operation instruction.
11. Security system complying with the minimum security requirement as prescribed by the Bank of Thailand.

After the application has been approved, commercial banks must comply with the following conditions:

1. By virtue of the Commercial Banking Act, the electronic machine to be installed off bank premises, is considered as the establishment of a branch office. Therefore, commercial banks must comply with the regulations under the provision of the Banking Act. Except for the working days and hours to be opened for public which will be granted permission individually by the Bank of Thailand. Commercial banks must have a clear notice stating the service providing days and hours posted at each the machine site location.
2. Commercial banks must have 2 or more of other commercial banks jointly provide the services, otherwise permissions shall be revoked except authorizations are granted with conditions to be complied with.
3. Electronic machines shall only be used for withdrawing cash, accepting cash or cheque deposit, transferring of funds, account balance inquiry and other service functions as prescribed by the Bank of Thailand.

4. Commercial banks must provide the electronic machine services within 1 year after permission has been granted except authorizations are granted.
5. Commercial banks must notify name of the designated branch office for monitoring the electronic machine. Prior to changing the reported branch office, commercial banks must notify the Bank of Thailand at least 7 days in advance.
6. Commercial banks must submit a copy of the authorization letter empowering the branch office responsibilities of monitoring the electronic machine (if there is.....) including name, location, map and schedule opening date, 7 days in advance before schedule opening date.
7. Commercial banks must have a notice, stating name of other banks that jointly provide the services, posted distinctively at the installation site.
8. Commercial banks must implement the minimum security procedures as prescribed by the Bank of Thailand. And, prior to modifying the computer application system or changing in terms and conditions, banks must obtain an approval from the Bank of Thailand provided with the explanation of reasons and its impact to the security and control procedures.

9. Commercial banks must perform a computer audit at least once a year with sufficient audit scope as prescribed by the Bank of Thailand. For each audit performed, a copy of audit report, relevant instructions and recommendations, must be submitted to the Bank of Thailand within 45 days from the audit date.

Appendix 4
Chronological records of Electronic Banking Measures

	SUBJECT	OBJECTIVE
1	1983-1984 20/09/1983 Rules and conditions in granting permission to install the Automated Teller Machine.	Notification of Rules and conditions to install the ATM within and off-premises.
2	28/12/1984 Rules and conditions in granting permission to commercial banks providing ATM services exceeding banking hours.	Commercial banks shall offer the electronic machine services at bank premise and exceeding working hour up to a maximum of 50 units, and must seek an approval from the BOT prior to order the machine. Within 1 year, commercial banks must have at least 2 or more other banks jointly provide the services.
3	1985 02/05/1985 Provision of the electronic machine services for deposits and withdrawals by non-bank organizations.	The provision of any services connected with the bank computerized system is considered as the provision of the ATMs off premises.
4	28/05/1985 Provision of services in new technology by commercial banks.	Commercial banks wishing to import technology equipment in order to provide new services must seek an approval from BOT, and the provision of mentioned services off premise and/or exceeding bank working hours are required the approval of the Ministry of Finance or the BOT depending upon the situations.

		SUBJECT	OBJECTIVE
5	03/10/1985	Rules and conditions in granting permission to commercial bank providing services of electronic machine for deposits and withdrawals.	Revision of Rules and conditions in granting permission to commercial banks providing ATM service within bank premises, exceeding bank working hours and off bank premises.
6	09/10/1985	Feasibility Study on service provision of the electronic machine for deposits and withdrawals.	Seeking cooperation from Thai commercial banks wishing to install ATM and for POS service, to conduct the Feasibility Study on such services and submit the report to the Bank of Thailand.
7	21/11/1985	Revision of The Commercial Banking Acts.	Regarding to the commercial examination practice, revision of Section 35 had been made to empower the examiner to examine banks' computer system and/or their EDP services.
8	21/04/1986 1986	Granting permission to provide electronic machine services for deposits and withdrawals.	Revision of rules in granting permission to commercial banks providing ATM services exceeding bank working hours.
9	30/07/1986	Submission of computer audit report in accordance with rules and conditions prescribed to provide electronic machine services for deposits and withdrawals.	Informing of computer audit procedures to be complied with.

		SUBJECT	OBJECTIVE
10	30/07/1986	Request on performance Report of electronic machine services.	Request commercial banks to submit Past Performance Report of every electronic banking services to the Special Assignments Division by September 1986.
11	17/04/1987	Request on the Performance Report of the electronic banking services and local credit card services.	Requiring commercial banks to submit Performance Report on electronic machine service every 6 months.
12	08/05/1987	Importing of the electronic machine utilized for deposits and withdrawals.	Commercial banks may import quantity of ATM more than a total numbers of bank branches in Bangkok Metropolitan area with the approval from BOT depending on individual bank requirement and necessity.
13	18/08/1987	Provision on financial information services.	In provision of non-financial information activities, commercial banks are exempt from an approval from BOT but must inform the BOT within 7 days before rendering services.
14	3/11/1987	Extension of commercial banking business scope.	Commercial banks may sell their actual developed computer programs including the application programs development.
15	24/12/1987	Invitation to attend meeting on the development of Emergency Plan and the Computer Backup System.	

		SUBJECT	OBJECTIVE
16	1988 27/04/1988	Provision of Security Exchange service through the Office Banking Services.	Commercial Banks must seek an approval from the BOT before offering such services to their customers and BOT may prescribe conditions to be complied with.
17	09/05/1988	Revision of rules in granting permission to commercial banks providing the electronic machines for deposits and withdrawals.	Revision of rules and conditions in granting permission to commercial banks operating ATM services exceeding working hours, off premises, and temporary services.
18	23/06/1988	Development on the Emergency Plan and Computer Backup System of commercial Banks.	Guidelines on operation procedures of the Emergency Plan and Bank Computer backup system in order to provide services to customers timely.
19	1991 13/09/91	Minimum Standard of Information for bank examination purposes.	Guidelines on data processing records required to expedite supervisory examinations.

Note : Since October 1992, banks have not been required to get an approval of ATM services. However, they have to notify the Bank of Thailand 7 days prior to provide ATM services to customers.

บรรณานุกรม

1. EDP Examination Handbook โดย Federal Financial Institutions Examination Council (FFIEC)
2. Auditing EDP System โดย Donald A. watne and Peter BB Turney
3. Auditing Bank EDP System โดย Bank Adminstration Institute
4. EDP Risk Analysis and Controls Justification โดย William E. Perry and Javier F. Kuong
5. Risk Management and Insurance โดย C. Arthur Williams tr. and Richard M. Heins
6. Control of Electronic Fund Tremsfer System โดย Kevin J. Fitjgerald
7. Auditing Computer Application โดย Keagle W. Davis กับ William. Perry
8. EDP Auditing โดย Mc Graw Hill
9. Auditing and EDP โดย Gordon B. Davis, Donald L. Adams, Corol A. Schaller
10. มาตรฐานการสอบบัญชี โดย สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย
11. EDP Supervision of Financial Institutions โดย Metha Suvanasarn
12. AICPA Professional Standards
13. EDPACS

เพิ่มเติม/แก้ไขคำผิด *

	หน้า	ย่อหน้า	บรรทัด	คำผิด	แก้ไข
คำนำ :	1	แรก	5	ธนาคาร พาณิชย์	ธนาคารพาณิชย์
	1	แรก	5	สมาคมนักบัญชี และผู้สอบบัญชี	สมาคมนักบัญชีและผู้สอบบัญชี
	2	2	4	ผู้ฟัง	ผู้ฟัง
	3	2	3	ฐานะดำเนินงาน	ฐานะการดำเนินงาน
	4	แรก	2	หลักการการ	หลักการ
	5	แรก	4	ส่วนกำกับสถาบันการเงินธนาคาร แห่งประเทศไทย	ส่วนกำกับสถาบันการเงิน ธนาคาร แห่งประเทศไทย
สารบัญ :	3	-	21	การตรวจสอบการปฏิบัติงาน คอมพิวเตอร์	การตรวจสอบการปฏิบัติงานคอมพิวเตอร์ โดยผู้ตรวจการธนาคารพาณิชย์
	3	-	22	การจัดทำข้อมูลที่น่าเชื่อถือได้ โดย ผู้ตรวจการธนาคารพาณิชย์	การจัดทำข้อมูลที่น่าเชื่อถือได้
	5	-	13	การสอบทานการควบคุมเฉพาะระบบงาน	การสอบทานการควบคุมเฉพาะระบบ
	6	-	17	สาเหตุที่ใช้คอมพิวเตอร์ทำให้ ผู้ตรวจสอบต้องเปลี่ยนแปลงวิธีและ เทคนิคในการตรวจสอบ	สาเหตุที่คอมพิวเตอร์ทำให้ ผู้ตรวจสอบต้องเปลี่ยนแปลงวิธีและ เทคนิคในการตรวจสอบ
	8	-	2	การควบคุมภายใน	การควบคุมใน
	9	-	14	1222	222
	10	-	7	สถาบันการเงิน	สถาบันการเงินที่
	10	-	11	อาชญากรรมทางเทคโนโลยี	อาชญากรรมทางเทคโนโลยี (คอมพิวเตอร์)
	10	-	17	สามารถทุจริต	สามารถจะ
	10	-	23	ประเภทการตรวจสอบ	ประเภทการตรวจสอบ/ลักษณะการ ตรวจสอบ
	11	-	13	คู่มือการ	คู่มือ
	12	-	8	การทำ	การ
เนื้อเรื่อง :	7	-	สุดท้าย	-	เดิมข้อความ “ซึ่งผู้บริหาร ผู้ตรวจสอบ และผู้ปฏิบัติงานที่เกี่ยวข้องควรทำความเข้าใจการดำเนินงานด้านคอมพิวเตอร์ ในลักษณะของ Total System approach ทั้ง 3 ส่วน รวมทั้งความสัมพันธ์ที่ เกี่ยวข้องด้วย
	11	ข้อ 1	3	case	cash

* เนื่องจากต้องการความเร่งด่วนในการออกหนังสือให้ทันงานวันธนาคารภาคตะวันออกเฉียงเหนือประจำปี 2539 ที่จังหวัดร้อยเอ็ด
จึงขอภัยในข้อผิดพลาดมา ณ ที่นี้

	หน้า	ย่อหน้า	บรรทัด	คำผิด	แก้ไข
เนื้อเรื่อง :	13	ข้อ 8.1	4	(disk)	disk
	15	-	3	(Comarison of Old New Forms of Evidence)	(Comparison of Old and New Forms of Evidence)
	16	ข้อ 1)	2	ประมวลผลใช้	ประมวลผลโดยใช้
	23	ข้อ 1	3	ปฏิบัติงานการควบคุมภายใน	ปฏิบัติงาน การควบคุมภายใน
	37	สุดท้าย	1	เพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ	เพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ
	45	ข้อ 1.15	1	การประเมินงาน ตรวจสอบ	การประเมินงานตรวจสอบ
	47	สุดท้าย	1	ในภาพรวม	ในภาพรวม
	48	-	สุดท้าย	I/Q CONTROL AREA	I/O CONTROL AREA
	55	ข้อ 3.12	2	การปรับปรุง	การปรับปรุงโปรแกรม
	58	ข้อ 4.3.2	8	Schmeatics	schematics
	59	-	2	เพื่อให้	เพื่อให้
	61	ข้อ 4.7	1	การตรวจสอบ เอกสารสนับสนุนการปฏิบัติงาน	การตรวจสอบเอกสารสนับสนุนการปฏิบัติงาน
	63	ข้อ 5.9	1	การตรวจสอบ การปฏิบัติงานคอมพิวเตอร์ โดย	การตรวจสอบการปฏิบัติงานคอมพิวเตอร์โดย
	63	ข้อ 5.9	4	สถาบัน การเงิน	สถาบันการเงิน
	64	ข้อ 6.1	2	(Transaction Initiation and Data Entry) Q	(Transaction Initiation and Data Entry)
	65	สุดท้าย	4	บัญชีหัก	บัญชีหัก
	66	ข้อ 6.1.2	1	(Non-MICR Data Entry)	NON-MICR Data Entry
	68	ข้อ 6.4	5	รายการหัก	รายการหัก
	69	ข้อ 6.5	2	(ได้แก่ disk, tape, drum และ card)	ได้แก่ disk,tape, drum และ card
	69	ข้อ 6.5	3	การ เก็บอุปกรณ์	การเก็บอุปกรณ์
	69	ข้อ 6.5	7	เสียหาย	เสียหาย
	69	ข้อ 6.5	11	เบี่ยงหน้า ที่ใช้ดับเพลิง	เบี่ยงหน้าที่ใช้ดับเพลิง
	71	5	3	อยู่ท้ายfile	อยู่ท้าย file
	71	สุดท้าย	4	การทำงานทดลอง	การทำงานทดลอง
	72	ข้อ 6.6	8	การประมวล	การประมวลผล
	73	สุดท้าย	1	และงบทดลองที่ปรากฏในบัญชีแยกประเภททั่วไป	และบัญชีแยกประเภททั่วไปที่ปรากฏในงบทดลอง
	76	-	4	รักษาปลอดภัย	รักษาความปลอดภัย

หน้า	ย่อหน้า	บรรทัด	คำผิด	แก้ไข
82	สุดท้าย	1	ธนาคาร	สถาบันการเงิน
83	ข้อ 7.4	3	การทุจริตการจารกรรม	การทุจริต การจารกรรม
83	ข้อ 7.4	6	ทดแทน ได้อย่างรวดเร็ว	ทดแทนได้อย่างรวดเร็ว
83	ข้อ 7.5	4	หากเป็นบุคคล ภายนอก	หากเป็นบุคคลภายนอก
83	ข้อ 7.6	3	โปรแกรมเอกสารสนับสนุน	โปรแกรม เอกสารสนับสนุน
85	ข้อ 8.1	3	หน่วยประมวลผลกลางคืน	หน่วยประมวลผลกลาง คือ
88	ข้อ 8.2.7	2	inquiry/memo/post	memo-post
89	ข้อ 9	3	ภายนอกสถาบันการ	ภายนอกสถาบันการเงิน
90	ข้อ 9.2	10	ธนาคารพาณิชย์	สถาบันการเงิน
99	ข้อ 13	1	ฉบับที่ 29	ฉบับที่ 28
100	-	4	กรณีการใช้คอมพิวเตอร์	กรณีกิจการใช้คอมพิวเตอร์
101	ข้อ 5.1	9	ลดน้อยลง ได้กิจกรรม	ลดน้อยลงได้ กิจกรรม
113	ข้อ 9	11	5.6 ช่วยเวลา	9.6 ช่วงเวลา
114	ข้อ 11	3	วางแผนและ	วางแผน
115	ข้อ 14.4	4	แอปซีติก	แอปซีติก
115	ข้อ 15.2	2	ไม่ใช่	ไม่ใช่
120	ข้อ 31	2	31 ธันวาคม	31 ธันวาคม 2536
130	ข้อ 6.2.1	4	SAY	WAY
130	ข้อ 6.2.3	11	จุดอ่อน	จุดอ่อน
132	-	-	ประเมินประสิทธิภาพของ ระบบการควบคุม และ กระบวนการปฏิบัติงาน	ประเมินประสิทธิภาพของ ระบบการควบคุม และ กระบวนการปฏิบัติงาน
136	ข้อ 7.4	2	พิธีปฏิบัติ	วิธีปฏิบัติ
137	ข้อ 7.6	2	คณะกรรมการบริหาร	คณะกรรมการบริหาร
137	ข้อ 7.8	สุดท้าย	ตรวจสอบ	ตรวจสอบ
141	ขั้นตอนที่ 3	2	เหมาะสมแล้ว ทำรายงาน	เหมาะสม แล้วทำรายงาน
148	ข้อ 5	6	สามารถและค้นหา	สามารถค้นหา
154	ข้อ (1)	2	ละอาจ	และอาจ
157	-	12	Separation	Separation
170	ข้อ 6	2	เป็นสิ่งที่จำเป็น	เป็นสิ่งที่จำเป็น
171	ข้อ 4	2	ไม่ควรกระทำในทำนองเดียวกัน การ	ไม่ควรกระทำ ในทำนองเดียวกันการ
171	สุดท้าย	2	ขั้นสุดท้ายนั้น	ขั้นสุดท้ายนั้น
175	แรก	6	people	People
177	ข้อ 2.1	2	จำต้อง	จำเป็นต้อง

หน้า	ย่อหน้า	บรรทัด	คำผิด	แก้ไข
177	ข้อ 2.1	2	มัน อย่างไร	มันอย่างไร
178	ข้อ 2.3	3	สภาวะปกติได้แนวคิด	สภาวะปกติได้ แนวคิด
178	ข้อ 2.4	3	จึงเป็นจุด	จึงเป็นจุด
179	-	11	Password	Password
180	ข้อ จ.	4	(Password)	(Password)
181	ข้อ 2.5.5	6	มีการทุจริต	ให้มีการทุจริต
182	ข้อ 2.6	17	ผังแสดง	ผังแสดง
183	ข้อ 2.6.3	2	การประเมินควบคุมภายใน	การประเมินการควบคุมภายใน
193	-	8	ละควบคุม	และควบคุม
193	ข้อ 2.2	11	Docement	Document
195	ข้อ 4.1	4	ข้อบังคับ	บังคับ
196	ข้อ 4.5	10	ชักชวน	ชักชวน
196	ข้อ 4.6	6	ที่มีกิจการ	ที่กิจการ
211	ข้อ 5	2	คู่มือ	คู่มือ
214	ข้อ 9	3	ขอบเขต	ขอบเขต
221	ข้อ 1.8	1	Input	Input
221	ข้อ 1.10	2	Edp	EDP
223	ข้อ 4.16	1	file	File
237	ข้อ 4.6	3	คอม-พิวเตอร์	คอมพิวเตอร์
243	-	7	5.1.2.4	4.1.2.4
243	ข้อ 4.1.3	4	(ตามข้อ 5.2)	(ตามข้อ 4.1.2)
243	ข้อ 4.3	2	5.3.1	4.3.1
243	ข้อ 4.3	3	5.3.2	4.3.2
243	ข้อ 4.3	4	5.3.3	4.3.3
261	-	9	ดีขึ้น	ดีขึ้น
261	สุดท้าย	1	อัตรากรมวนเวียน	อัตรากรมวนเวียน
291	-	2	ทำให้ตกเป็นลูกหนี้	ทำให้ธนาคารตกเป็นลูกหนี้
บรรณานุกรม :	1 ข้อ 6	2	Tremster	Transfer

บันทึก

บันทึก

บันทึก

