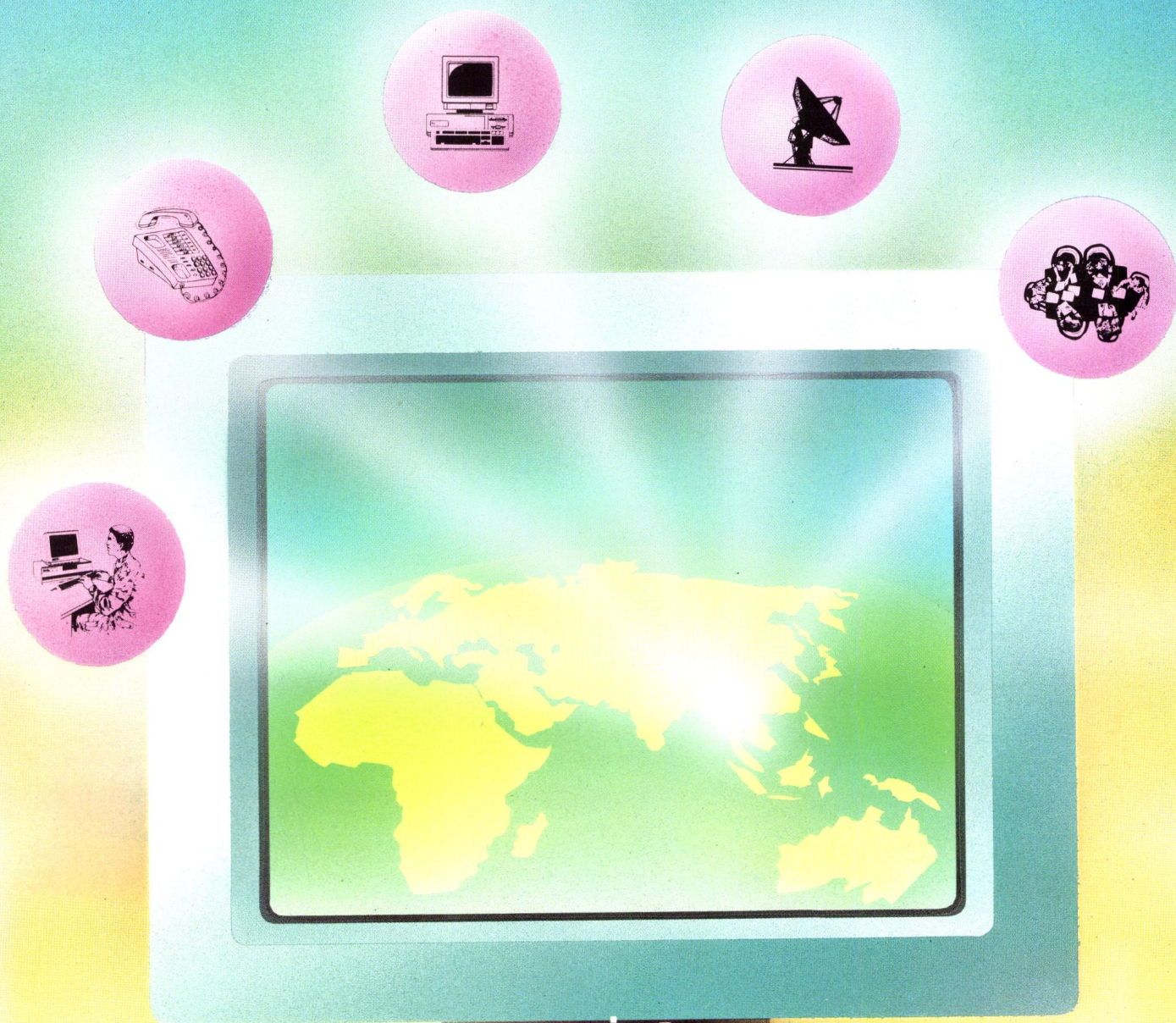


การดำเนินงาน และ การตรวจสอบสถาบันการเงิน ด้านคอมพิวเตอร์



เล่มที่ 4

คอมพิวเตอร์กับแผนฉุกเฉิน
(และการฝึกอบรม)

ISBN 974-89418-1-7

เมธา สุวรรณสาร

**การดำเนินงาน
และ
การตรวจสอบสถาบันการเงิน
ด้านคอมพิวเตอร์**

เล่ม 4

เมธา สุวรรณสาร

คำนำ

1. หนังสือเรื่อง “การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์” ทั้ง 4 เล่มนี้จะสมบูรณ์ไปไม่ได้ ถ้าไม่มีเรื่องแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan) เพราะการดำเนินงานขององค์กรที่ใช้คอมพิวเตอร์ โดยเฉพาะอย่างยิ่งสถาบันการเงินต่าง ๆ อาจหยุดชะงักการให้บริการได้ ถ้าไม่มี Contingency Plan ตามที่มีรายละเอียดในหนังสือเล่มนี้

ตัวอย่างในเรื่องนี้มีมาครั้ง โดยเฉพาะที่เกิดในประเทศไทยของเราเอง แต่ส่วนใหญ่ไม่ได้เป็นข่าวใหญ่มากนัก ทั้ง ๆ ที่การหยุดชะงักการให้บริการของสถาบันการเงินมีลักษณะเหมือนหนึ่งสถาบันการเงินขาดสภาพคล่อง ซึ่งเป็นเรื่องที่สำคัญมาก ทั้ง ๆ ที่องค์กรมิได้มีปัญหานี้แต่อย่างใด เมื่อปลายเดือนพฤษภาคม 2540 ก็เกิดปัญหาเครื่องคอมพิวเตอร์ขององค์กรที่สำคัญแห่งหนึ่งที่กรุงเทพฯ เกิดขัดข้องและหยุดการดำเนินการเกือบทั้งวัน ทั้ง ๆ ที่องค์กรนั้นมี second site back up ในระดับหนึ่งที่มีความสามารถในการ back up อย่างจำกัด ซึ่งก่อให้เกิดความเดือดร้อนและมีปัญหาตามมาหลายประการต่อประชาชนผู้ที่ต้องใช้บริการจากองค์กรนั้นจำนวนมาก

2. มีถ้อยคำที่ท่านผู้อ่านควรทำความเข้าใจอยู่ 3 คำด้วยกันคือ แผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan) หมายถึง แผนงานที่จัดทำไว้เพื่อใช้เป็นแนวทางในการกำหนดมาตรการรักษาความปลอดภัยและป้องกันความเสียหายจากเหตุฉุกเฉินหรือภัยพิบัติต่าง ๆ ที่อาจมีผลกระทบต่อการดำเนินงานและการให้บริการตามปกติขององค์กรที่ใช้คอมพิวเตอร์ รวมทั้งแผนปฏิบัติงานและปรับปรุงแก้ไขหรือกำหนดวิธีการอื่นใดที่จะทดแทนการหยุดทำงานของระบบงานคอมพิวเตอร์ เพื่อให้องค์กรที่ใช้คอมพิวเตอร์สามารถดำเนินการและให้บริการได้อย่างต่อเนื่องตามปกติ ซึ่งประกอบด้วยแผนย่อย ดังนี้

2.1 แผนปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน (Emergency Plan)

หมายถึง แผนการรักษาความปลอดภัยและขั้นตอนปฏิบัติงานเมื่อเกิดเหตุฉุกเฉินหรือภัยพิบัติต่าง ๆ เพื่อป้องกันความเสียหายที่อาจมีผลกระทบต่อการดำเนินงานและการให้บริการด้วยระบบงานคอมพิวเตอร์ตามปกติของสถาบันการเงินหรือองค์กรที่ใช้คอมพิวเตอร์

2.2 แผนปรับปรุงแก้ไขระบบงานคอมพิวเตอร์ (Recovery and Disaster Plan)

หมายถึง แผนปฏิบัติงานสำหรับใช้ดำเนินการแก้ไขระบบงานคอมพิวเตอร์ของสถาบันการเงินหรือองค์กรที่ใช้คอมพิวเตอร์ที่ขัดข้องหรือเสียหายไม่สามารถใช้งานได้ ให้กลับสภาวะปกติในเวลาอันควร รวมทั้งกำหนดวิธีการอื่นที่ใช้ทดแทนการหยุดทำงานของระบบงานคอมพิวเตอร์

2.3 ระบบคอมพิวเตอร์สำรอง (Back up)

หมายถึง การจัด หรือจัดทำระบบสำรองของเครื่องคอมพิวเตอร์อุปกรณ์ประกอบระบบคอมพิวเตอร์ และระบบงานคอมพิวเตอร์ เพื่อใช้ทดแทนการทำงานเมื่อระบบคอมพิวเตอร์ที่ใช้งานตามปกติขัดข้องหรือเสียหายใช้การไม่ได้

3. การรวบรวมและเรียบเรียงหนังสือทั้ง 4 เล่ม ใช้เวลาไม่น้อย ทั้ง ๆ ที่หนังสือดังกล่าวเกิดจากการรวบรวมเรื่องราวที่ผมได้แจกเป็นเอกสารประกอบการบรรยาย และจากการศึกษาให้กับสถาบันต่าง ๆ ในอดีต ตามที่กล่าวไว้แล้วในเล่มก่อน ๆ อย่างไรก็ดี การพิมพ์ใหม่ทำให้ต้องใช้เวลารวบรวม รวมทั้งเขียนเรื่องเพิ่มเติมโดยเฉพาะในเล่มที่ 3 ค่อนข้างมาก และเล่มที่ 4 ซึ่งเป็นเล่มที่ผมพิจารณาว่าน่าจะเป็นประโยชน์ต่อผู้ที่สนใจไม่ว่าจะเป็นผู้บริหาร ผู้พัฒนาระบบงาน และผู้ตรวจสอบทุกประเภท เพราะส่วนใหญ่ในเรื่องที่เกี่ยวกับตัวอย่างจุดอ่อนในระบบงานด้านคอมพิวเตอร์ไม่ได้เกิดจากการแปลหรือเรียบเรียงจากหนังสือต่างประเทศตามปกติเท่านั้น แต่ได้ผสมผสานแง่คิดหลาย ๆ ประการทั้งในภาคสนามและประสบการณ์ที่ ผู้ที่เกี่ยวข้องสามารถประยุกต์ใช้เป็นแนวทางป้องกันจุดอ่อน รวมทั้งการทุจริตได้ล่วงหน้าก่อนปัญหาจะเกิดขึ้นจริง ดังที่เคยกล่าวแล้วว่า “Point to the problem before it points to us” นั่นคือผู้บริหารควรเข้าใจและรู้ถึงประเด็นปัญหาที่อาจเกิดขึ้นกับองค์กรแล้วหาทางแก้ไข ก่อนที่ปัญหานั้นจะกลับมาทำความเสียหายให้องค์กรของตนเอง

4. หนังสือเล่มแรก ๆ ที่ได้แจกจ่ายไปนั้นมีผู้สนใจหลายรายได้อ่านแล้วโทรศัพท์มาสอบถาม และขอแลกเปลี่ยนทัศนะกับผมด้วย รวมทั้งขอให้ผมลงประวัติของตัวเองไว้ให้ผู้อ่านได้ทราบพื้นฐาน เพื่อจะได้ใช้ประโยชน์ในการศึกษาและแลกเปลี่ยนข้อมูลที่น่าสนใจจากการปฏิบัติงานภาคสนาม ซึ่งผมก็ได้ทำตามคำแนะนำของท่านผู้อ่านแล้ว ดังปรากฏข้อมูลในตอนท้ายของเล่มนี้แล้ว

5. หนังสือเรื่องนี้ทั้ง 4 เล่ม อาจสรุปให้ชัดเจนได้ไม่มากนัก เพราะขึ้นกับว่าท่านอยู่ในฐานะอย่างไรในองค์กร กล่าวคือท่านเป็นผู้บริหาร หรือผู้พัฒนาระบบงานหรือผู้ตรวจสอบ และเป็นผู้ตรวจประเภทใด ดังนั้นพื้นฐานก็คงจะอยู่กับตัวแปรดังกล่าวเป็นสำคัญ รวมทั้งมาตรฐานขององค์กรที่เกี่ยวข้องด้วย เพราะในทางปฏิบัติมีแนวการพิจารณาในเรื่องนี้แตกต่างกันมากในแต่ละองค์กรหรือแม้แต่องค์กรเดียวกันในแต่ละหน่วยงานที่เกี่ยวข้อง แต่สิ่งหนึ่งที่ควรจะเหมือนกันหรือคล้ายกันก็คือ ความรู้ ความตั้งใจจริง และความเข้าใจ ในแนวทางปฏิบัติของผู้บริหารในสภาวะแวดล้อมขององค์กรที่ใช้คอมพิวเตอร์ที่ได้เปลี่ยนแปลงไปมากมายจากการพัฒนาเทคโนโลยีที่ไม่หยุดยั้ง และมีผลกระทบต่อความเสี่ยง วิธีการควบคุม วิธีการตรวจสอบ และทักษะของผู้ตรวจสอบที่เกี่ยวข้องอยู่ตลอดเวลา และที่สำคัญที่สุดก็คือการที่คอมพิวเตอร์มีผลกระทบต่อแนวทางการตรวจสอบ หลักฐานการตรวจสอบ ฯลฯ และความน่าเชื่อถือได้ของข้อมูลทางการเงินที่ใช้ในการตรวจสอบฐานะที่แท้จริงของสถาบันการเงินที่ผู้บริหารในองค์กรที่ใช้คอมพิวเตอร์ทุกแห่งควรให้ความสนใจ

6. หนังสือชุดนี้เป็นส่วนหนึ่งของการดำเนินงานที่เป็นผลจากการวิเคราะห์จุดอ่อน จุดแข็ง โอกาสและอุปสรรค (SWOT) ของการปฏิบัติงานโดยธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ หนังสือทั้ง 4 เล่มจึงเป็น Action Plan แผนหนึ่งจาก 19 แผนงานของสาขาภาคฯ ซึ่งเกิดจากการตั้งเป้าหมายที่จะพัฒนาความรู้ในด้านการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ให้กับผู้ตรวจสอบของส่วนกำกับสถาบันการเงิน และธนาคารพาณิชย์รวมทั้งสถาบันการเงินอื่น ๆ ที่อยู่ภายใต้การดูแลของธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือโดยรวม และพิจารณาเป็นส่วนหนึ่งของการเสวนาเชิงปฏิบัติการระหว่างหน่วยงานทั้ง 2 ด้วย

การดำเนินการของธนาคารแห่งประเทศไทยดังกล่าว เป็นการป้องกันปัญหาล่วงหน้าที่อาจเกิดขึ้นกับสถาบันการเงิน ดังรายละเอียดปรากฏในหนังสือชุดนี้แล้ว

7. จากการที่ผ่านมามีโอกาสเป็นผู้แทนของไทยไปร่วมการประชุมที่องค์กรสหประชาชาติ (UN) ที่ New York ในปี 2532 เรื่อง Draft Model Law on International Credit Transfers ซึ่งเดิมใช้ชื่อว่า Model Rules on Electronic Funds Transfer การเปลี่ยนแปลงชื่อเรื่องดังกล่าวก็เพื่อให้ครอบคลุมร่างกฎหมายการโอนเงินทั้งทางอิเล็กทรอนิกส์และการโอนเงินแบบธรรมดา (ถ้ามี) ได้ หนังสือเล่ม 4 นี้จึงมีภาคผนวกที่เกี่ยวข้องรวบรวมไว้ให้ท่านผู้อ่านได้อ่านในเรื่องนี้โดยสังเขป

8. ในภาคผนวกของเล่มนี้ ได้เรียบเรียงความเห็นเกี่ยวกับการร่างแนวทางกฎหมายการโอนเงินทางอิเล็กทรอนิกส์ในช่วงที่ผมและคณะได้ศึกษากันมานานพอสมควร รวมทั้งความเป็นมาของการประชุมร่างกฎหมายดังกล่าวและการศึกษาการหักกลบลบหนี้ (Netting) ระหว่างประเทศ ที่น่าสนใจในยุคปัจจุบันอยู่ด้วย

9. หนังสือเล่ม 4 นี้ ได้ทำกรณีศึกษาการตรวจสอบ Data Center (General Controls) และการตรวจสอบ “งาน” (Application Controls) เพียงบางกรณี พร้อมแนวคำตอบจากการจัดทำกรณีศึกษาภาคสนามให้ท่านผู้สนใจได้ทบทวนอีกครั้ง โดยเฉพาะอย่างยิ่งผู้ตรวจสอบด้านคอมพิวเตอร์ (IS Auditor) รวมทั้งผู้ตรวจสอบโดยทั่วไป

10. ในที่สุดหนังสือชุดนี้ก็จัดทำรวมแล้วเป็น 4 เล่ม เพราะเนื้อหาเป็นเรื่องต่าง ๆ ที่อธิบายและบรรยายมีมากกว่าที่ประมาณการไว้มาก และอาจมีถึง 5 เล่ม หากผมมีเวลาพอโดยเฉพาะตัวอย่างรวมทั้งกรณีสร้าง Test Data เพื่อวัดประสิทธิภาพและประสิทธิผลของการควบคุมภายในและความน่าเชื่อถือของข้อมูลทางการเงินที่เป็นรายละเอียดในภาคปฏิบัติ การแยกเล่มเพิ่มเติมก็เพื่อให้การจัดพิมพ์หนังสือแต่ละเล่มมีความหนาและแยกเป็นเรื่อง ๆ ที่เหมาะสม หนังสือทั้ง 4 เล่ม ได้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อให้เกิดการเรียนรู้ในวงจำกัดต่อผู้ตรวจสอบ ในส่วนกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ และสถาบันการเงินอื่น ๆ เพื่อการศึกษา การพัฒนา การบริหารงาน และการตรวจสอบสถาบันการเงิน ด้านคอมพิวเตอร์หรือองค์กรที่ใช้คอมพิวเตอร์ ซึ่งจะช่วยให้สถาบันการเงินภายใต้การดูแลของธนาคารแห่งประเทศไทยมีความมั่นคงได้อีกทางหนึ่ง และจะเป็นการพัฒนาบุคลากรที่เกี่ยวข้องเรื่องนี้ให้ก้าวทันกับเทคโนโลยีทางคอมพิวเตอร์ที่มีผลกระทบต่อความเสี่ยงใหม่ ๆ ซึ่งต้องการการควบคุมรวมทั้งวิธีการตรวจสอบใหม่ ๆ ให้สอดคล้องกับวิธีการประมวลผลโดยใช้คอมพิวเตอร์ที่ทันสมัยเหล่านั้น

11. มีความเป็นไปได้ที่ธนาคารแห่งประเทศไทยจะให้สถาบันการเงินที่ใช้คอมพิวเตอร์ รวมทั้งผู้สอบบัญชี (External auditor) และผู้สอบบัญชีภายใน (Internal auditor) ของสถาบันการเงินมีความรับผิดชอบในการเป็นผู้ดูแลการบริหารงานและการตรวจสอบงานด้านคอมพิวเตอร์แทนการตรวจสอบงานด้านนี้ของธนาคารแห่งประเทศไทยมากขึ้น โดยธนาคารแห่งประเทศไทยเองอาจต้องให้ความสำคัญทางด้านฐานะของความมั่นคง การบริหารตลอดจนการจัดการความเสี่ยงทางด้าน Liquidity Risk, Market Risk, Credit Risk, Legal Risk, Operational Risk Systemic Risk, Settlement Risk ฯลฯ นอกเหนือจากการตรวจสอบคุณภาพของสินทรัพย์ และการบริหารงานด้านอื่น ๆ ที่เป็นความเสี่ยงในรูปแบบใหม่ ๆ จากนวัตกรรมทางการเงินที่อาจปรากฏได้ทั้งในรูปแบบข้อมูลทางการเงินใน Balance Sheet และ Off-Balance Sheet มากขึ้น ดังนั้นหนังสือเล่มทั้ง 4 เล่มชุดนี้จึงเป็นแนวทางที่ผู้ตรวจสอบจากธนาคารแห่งประเทศไทยและผู้ตรวจสอบที่เกี่ยวข้องกับสถาบันการเงินอาจนำไปใช้ศึกษาได้ตามวัตถุประสงค์ของการจัดทำหนังสือชุดนี้โดยธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ

12. ในปัจจุบันนี้ การบริหารความเสี่ยง (Risk Management) ในสถาบันการเงินมีความหลากหลาย การเข้าใจและวิเคราะห์ความเสี่ยง ตลอดจนการบริหารความเสี่ยงในรูปแบบต่าง ๆ จึงมีความสำคัญมาก ถึงแม้จะมี ตราสารอนุพันธ์ซึ่งเป็นเครื่องมือสำคัญของสถาบันการเงินต่าง ๆ ใช้ในการบริหารความเสี่ยงก็ตาม การลงทุนใน สัญญาตราสารอนุพันธ์ก็มีปัญหาเช่นเดียวกับการลงทุนในตราสารการเงิน นั่นคือ ยังมีความเสี่ยงสูงที่ทำนายผู้บริหาร ในสถาบันต่าง ๆ เป็นอย่างยิ่ง และความเข้าใจในเรื่องการบริหารความเสี่ยงในสถาบันต่าง ๆ ก็มีระดับความแตกต่างกันมาก หน่วยงานที่ทำหน้าที่กำกับดูแลสถาบันการเงินโดยเฉพาะผู้บริหารและผู้ตรวจสอบควรจะให้ความสนใจและ พัฒนาความเข้าใจในวิธีการบริหารความเสี่ยงมากขึ้น ผู้ตรวจสอบทุกประเภทจะต้องเข้าใจถึง nature ของ "ความเสี่ยง" การควบคุมความเสี่ยง และวิธีการตรวจสอบที่วัดผลความเสี่ยงด้านต่าง ๆ (Risk Modelling) ได้อย่างเป็นรูปธรรม แล้วพิจารณาหามาตรการการกำกับและดูแลความเสี่ยงที่อาจเกิดขึ้นก่อนที่ความเสียหายจะติดตามมา

13. การดำเนินงาน การบริหารงานและการตรวจสอบงานด้านคอมพิวเตอร์ก็เป็นอีกรูปแบบหนึ่งของงานที่มีความเสี่ยง ตามที่ผมได้กล่าวไว้แล้วในหนังสือชุดนี้ และเมื่อวันที่ 23 เมษายน 2540 ผมก็ได้รับข่าวสารทาง E-mail จาก Mr.David G. Rowley ซึ่งเป็นทั้งผู้ตรวจสอบและผู้บริหารอาวุโสทางด้าน IS examination จาก Federal Reserve Bank of Minneapolis, Minnesota ประเทศสหรัฐอเมริกา ขอให้จัดส่งแนวทางการจัดการและการบริหารการตรวจสอบ ตลอดจนการควบคุมของทางการ ทางด้านคอมพิวเตอร์ของประเทศไทยในปัจจุบันและในปี ค.ศ. 2000 หรือ IT 2000 ไปให้ทราบเพื่อใช้ประกอบการบรรยายเรื่องนี้ในประเทศสหรัฐอเมริกาด้วย ในเดือนมิถุนายน 2540 เพราะ Mr.David ได้รับมอบหมายให้บรรยายให้กับผู้บริหารของ FFIEC ซึ่งประกอบไปด้วย FRB, FDIC และ OCC รวมทั้งสมาคม ผู้ตรวจสอบงานคอมพิวเตอร์ (ISACA) ภาคพื้นกรุงเทพฯ ก็จะจัดให้มีการอภิปรายในหัวข้อทำนองเดียวกันนี้ในวันที่ 27 มิถุนายน 2540 ด้วย ทำให้ผมไม่แน่ใจว่าทางการในประเทศไทยยังจะควรมีบทบาทในการควบคุม กำกับ ดูแล สถาบันการเงินทางด้านคอมพิวเตอร์มากนักน้อย หรือควรลดลงอย่างไร เพราะขณะที่ทางการของประเทศสหรัฐอเมริกา และประเทศที่พัฒนาแล้วยังให้ความสนใจในการดำเนินงานด้านคอมพิวเตอร์ของสถาบันการเงินต่าง ๆ แต่สำหรับ ธนาคารแห่งประเทศไทยอาจมีแนวโน้มที่จะสนใจทางด้านความเสี่ยงใหม่ ๆ ที่มีผลกระทบต่อเสถียรภาพของสถาบัน การเงินอย่างอื่นที่มีความสำคัญมากกว่า อย่างไรก็ดี ผู้บริหารองค์กรที่ใช้คอมพิวเตอร์ทุกแห่งก็ควรให้ความสำคัญใน เรื่องการควบคุมความเสี่ยงโดยการพัฒนา IS Audit ต่อไปอย่างไม่หยุดยั้ง

14. จากการที่ได้ใช้เวลาในการจัดทำหนังสือชุดนี้ ที่ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่นเป็นเวลาประมาณ 2 ปี ก่อนที่ผมจะย้ายกลับไปทำงานที่สำนักงานใหญ่กรุงเทพ ในเดือนตุลาคม 2540 นี้ .ผมใช้การทำงานนอกเวลาทำงานตามปกติเป็นส่วนมาก ส่วนใหญ่ในหนังสือชุดนี้ทั้ง 4 เล่ม เป็นการรวบรวมโดย เขียนเพิ่มเติมประมาณ 20% จากเอกสารประกอบการบรรยายเรื่อง IS Audit ของผม ในชื่อต่างกันให้กับองค์กร ต่าง ๆ ในอดีต ส่วนที่ได้เพิ่มเติมมาใหม่ ส่วนใหญ่เป็นเรื่องคอมพิวเตอร์กับการทุจริตและภาคผนวกต่าง ๆ และยังมี อีกบางเรื่องที่ผมหาไม่พบจึงไม่มีโอกาสนำมาเผยแพร่ได้

ผมขอภัยในความผิดพลาดของตัวอักษร ทั้งภาษาไทยและภาษาอังกฤษ ที่ผมมักจะพบในภายหลัง จากการพิมพ์และเย็บเล่มเรียบร้อยแล้ว โดยเฉพาะเล่ม 1 ที่มีคำผิดพลาดในการพิมพ์มาก ซึ่งอาจจะเกิดจากการ แก้ไขแล้วไม่ได้ save ข้อมูลหลังจากแก้ไขเสร็จหรือผู้พิมพ์อาจหยิบแผ่น diskette สับสน ทำให้ผ่านขั้นตอนตรวจ

ทานไปได้เพราะได้พิสูจน์ตัวอักษรว่าถูกต้องแล้ว แต่เมื่อพิมพ์จริงและเย็บเล่มก็ปรากฏข้อผิดพลาดเดิม ๆ อยู่อีก ซึ่งเมื่อถึงขั้นตอนนี้ก็จะแก้ไขไม่ได้ดีเท่าที่ควร จึงขอภัยท่านผู้อ่านไว้ ณ ที่นี้อีกครั้ง และผมขอเน้นอีกครั้งว่า ความพยายามทั้งหมดในการจัดทำหนังสือชุดนี้ก็เพื่อผลประโยชน์ในการปฏิบัติงานของธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ ในการกำกับและดูแลสถาบันการเงินอีกมุมหนึ่งเป็นสำคัญ

15. สำหรับผู้ตรวจการธนาคารพาณิชย์ ส่วนกำกับสถาบันการเงินธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือรุ่นต่อ ๆ ไป ที่จะนำหนังสือชุดนี้ใช้ในการอบรมหรือพัฒนาผู้ตรวจสอบ โดยเฉพาะอย่างยิ่ง การอบรมการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ รวมทั้งการตรวจสอบฐานะการเงิน ความมั่นคงและการดำเนินงานโดยทั่วไป ควรพิจารณาเรื่องที่เกี่ยวข้องและสัมพันธ์กันที่อาจปรากฏอยู่ในเล่มต่าง ๆ มาใช้ในคราวเดียวกันด้วย ทั้งนี้ เพราะหนังสือชุดนี้ ได้มีการทบทวนเรื่องที่เกี่ยวข้องเพื่อให้ผู้ตรวจสอบได้ติดตามในรูปแบบที่ใช้การอธิบายที่แตกต่างกันออกไป แต่โดยรวมเรื่องเหล่านี้จะทำให้ผู้ตรวจสอบเข้าใจงานตรวจสอบทางด้าน IS Audit และ Financial Audit ได้ดีขึ้น

16. ขอขอบคุณบรรดาเพื่อนร่วมงานในอดีตทุกท่าน โดยเฉพาะรุ่นบุกเบิกการตรวจสอบงานด้านคอมพิวเตอร์ ได้แก่ คุณสุขุม ดันตราจิณ คุณสรสิทธิ์ สุนทรเทศ คุณปรีชา พรมาพจน์ คุณสมศักดิ์ มหินธิชัยชาญ คุณสุภัคดี ภูยานนทชัย คุณวุฒิพงศ์ สมนึก คุณชาตรี วรวิษขานันท์ และคุณพงศ์เทพ ชินพัฒน์ และเพื่อนร่วมงานรุ่นใหม่ ที่เข้ามาเสริมทีมงานในภายหลังที่ไม่อาจจะบอชื่อได้ทั้งหมด ซึ่งมีส่วนสำคัญในการช่วยเรียบเรียงเอกสารประกอบการบรรยายในอดีตในหลาย ๆ เรื่อง และทำให้งานตรวจสอบด้านคอมพิวเตอร์แพร่หลายมากขึ้นในปัจจุบัน ขอขอบคุณอีกครั้งสำหรับการมีส่วนร่วมใด ๆ ที่ผ่านมากในกิจกรรมเผยแพร่เอกสารการดำเนินงานการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ ขอขอบคุณเพื่อนร่วมงานในหน่วยวิชาการ ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือในปัจจุบันที่ช่วยตรวจทานความถูกต้องในการพิมพ์เล่มนี้

เมธา สุวรรณสาร

ผู้อำนวยการ

ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ

30 มิถุนายน 2540

สารบัญ

	หน้า
บทที่ 1 กลยุทธ์ในการเผชิญและการแก้ไขปัญหาเมื่อเกิดเหตุฉุกเฉิน	3
❑ บทนำ	3
❑ ความจำเป็นในการจัดทำแผนฉุกเฉินและระบบคอมพิวเตอร์สำรอง	3
❑ กฎหมายที่ออกบังคับใช้เกี่ยวกับการจัดตั้งแผนฉุกเฉินในสหรัฐอเมริกา	4
❑ ระยะเวลาในการอยู่รอดของธุรกิจหลังจากระบบคอมพิวเตอร์เสียหาย	5
❑ การวางแผนและกลยุทธ์ในการแก้ไขปัญหาเมื่อเกิดเหตุฉุกเฉิน	5
❑ ความสำเร็จของการแก้ไขปัญหาเมื่อเกิดเหตุฉุกเฉิน	8
❑ สรุป	9
บทที่ 2 ยุทธวิธีในการจัดทำแผนฉุกเฉิน	11
❑ บทนำ	13
❑ สาเหตุของปัญหาในการจัดทำแผนฉุกเฉิน	13
❑ แนวทางในการวางแผนฉุกเฉิน	14
❑ ขั้นตอนในการจัดทำแผน	15
บทที่ 3 มาตรการและเหตุผลในการกำหนดให้ธนาคารพาณิชย์จัดทำแผนฉุกเฉิน และมีระบบคอมพิวเตอร์สำรอง	19
❑ แผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน	23
- วัตถุประสงค์	23
- เหตุผลและความจำเป็น	23
❑ แนวทางการจัดทำแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน	24
- การกำหนดสิ่งจำเป็นในการพัฒนาแผน	24
- การพัฒนาจัดทำแผน	24
- การแปลงระบบและนำแผนออกใช้งาน	37
- การบำรุงรักษาและปรับปรุงแผน	37
❑ (ตัวอย่าง) แบบสำรวจข้อมูลสิ่งจำเป็นในการปฏิบัติงานประมวลผลระบบงานคอมพิวเตอร์	38
- วัตถุประสงค์	38
- วิธีการใช้	38
❑ (ตัวอย่าง) แบบสอบถามข้อมูล สถานการณ์ปฏิบัติงานสำรองชุดที่ใช้ปฏิบัติงานปัจจุบัน	44
- วัตถุประสงค์	44

	หน้า
☐ (ตัวอย่าง) แบบสำรวจข้อมูล ลำดับความสำคัญของระบบงานคอมพิวเตอร์	46
- วัตถุประสงค์	46
- การใช้ประโยชน์	46
บทที่ 4 แนวทางการพิจารณาเพื่อจัดหาและทำสัญญากับบุคคลภายนอกเพื่อใช้บริการประมวลผลข้อมูล หรือใช้เป็นระบบคอมพิวเตอร์สำรองเมื่อเกิดเหตุฉุกเฉิน	49
☐ วัตถุประสงค์	51
☐ การคัดเลือกศูนย์บริการคอมพิวเตอร์	51
☐ การทำสัญญาระหว่างธนาคารพาณิชย์กับศูนย์บริการคอมพิวเตอร์	54
☐ การกำหนดหน้าที่ความรับผิดชอบภายในของธนาคารพาณิชย์	55
บทที่ 5 กรณีศึกษา : แผนฉุกเฉิน	57
☐ บทเรียนที่ธนาคาร GRINDLAY ได้รับจากการจราจล	59
บทที่ 6 กรณีศึกษาการตรวจ Data Center (General Controls) และ Applications	61
☐ โดยประยุกต์ประเด็นที่ให้ศึกษาเป็นแนวคำถามและให้แนวคำตอบจากการปฏิบัติภาคสนาม	63
case1 ✓ ☐ กรณีศึกษา 1	64
case2 ✓ ☐ กรณีศึกษา 2	65
case3 ✓ ☐ กรณีศึกษา 3	66
case4 ✓ ☐ กรณีศึกษา 4	67
case5 ✓ ☐ กรณีศึกษา 5	68
case6 ✓ ☐ กรณีศึกษา 6	70
☐ กรณีศึกษา 7	71
- การตรวจสอบศูนย์ประมวลผลข้อมูล (Data Center)	71
☐ กรณีศึกษา 7 บริษัท เอส.เอ. อินเทอร์เน็ต จำกัด ภาค 1	71
☐ กรณีศึกษา 7 บริษัท เอส.เอ. อินเทอร์เน็ต จำกัด ภาค 2	80
- ระบบงานขายและรับเงิน	82
- ระบบงานซื้อและจ่ายเงิน	83
- ระบบงานผลิต	83
- ระบบงานเงินเดือน	84
☐ กรณีศึกษา 8 Data Center	92
- บริษัท ชี้อตรง จำกัด	92

	หน้า
☐ กรณีศึกษา 9	93
- บริษัท ภาพสวย จำกัด	93
- ขั้นตอนในการปฏิบัติงาน	93
case 7 ✓ ☐ กรณีศึกษา 10	95
- การรักษาความปลอดภัยห้องคอมพิวเตอร์	95
case 8 ✓ ☐ กรณีศึกษา 11	97
- บริษัท เทคโนโลยีทันสมัย จำกัด	97
case 9 ✓ ☐ กรณีศึกษา 12	97
case 10 ✓ ☐ กรณีศึกษา 13	98
- บริษัท วินิจฉัยโรค จำกัด	98
☐ กรณีศึกษา 14 Application	99
- บริษัท สายการบินปลอดภัย จำกัด	99
☐ กรณีศึกษา 15	103
- บริษัท เหล็กกล้า จำกัด	103
บทที่ 7 แนวคำตอบกรณีศึกษาต่าง ๆ (จากกรณีศึกษาที่ 1-15)	105
☐ แนวคำตอบกรณีศึกษา 1	107
☐ แนวคำตอบกรณีศึกษา 2	109
☐ แนวคำตอบกรณีศึกษา 3	110
- ทบทวนการวิเคราะห์จุดอ่อนขั้นพื้นฐาน	110
- จุดอ่อนที่สำคัญ	110
- ข้อเสนอแนะในการควบคุม	110
☐ แนวคำตอบกรณีศึกษา 4	111
☐ แนวคำตอบกรณีศึกษา 5	113
☐ แนวคำตอบกรณีศึกษา 6	115
☐ แนวคำตอบกรณีศึกษา 7	116
- การตรวจสอบศูนย์ประมวลผล บริษัท เอส.เอ.อินเตอร์เทรด จำกัด ภาค 1	116
- จุดอ่อนด้านการจัดการ	116
- จุดอ่อนด้านระบบงานและโปรแกรม	119
- จุดอ่อนด้านความน่าเชื่อถือของข้อมูล	123
- จุดอ่อนด้านการปฏิบัติงานคอมพิวเตอร์	124

☐	แนวคำตอบกรณีศึกษา 7	127
-	บริษัท เอส.เอ.อินเตอร์เทรด จำกัด ภาค 2 (การตรวจสอบระบบงาน Application)	127
-	ระบบงานขายและรับเงิน	127
-	ระบบงานซื้อและจ่ายเงิน	128
☐	แนวคำตอบกรณีศึกษา 8 - Data Center	129
-	บริษัท ซีอีตรง จำกัด	129
☐	แนวคำตอบกรณีศึกษา 9	131
☐	แนวคำตอบกรณีศึกษา 10	136
-	การรักษาความปลอดภัยห้องคอมพิวเตอร์ บริษัท ABC จำกัด	136
☐	แนวคำตอบกรณีศึกษา 11	137
-	บริษัท เทคโนโลยีทันสมัย จำกัด	137
☐	แนวคำตอบกรณีศึกษา 12	138
☐	แนวคำตอบกรณีศึกษา 13	139
-	บริษัท วินิจไฮเทค จำกัด	139
☐	แนวคำตอบกรณีศึกษา 14	142
-	บริษัท สายการบินปลอดภัย จำกัด	142
☐	แนวคำตอบกรณีศึกษา 15	145
บทที่ 8	การทดสอบความเข้าใจในการตรวจสอบงานด้านคอมพิวเตอร์บางประการ	147
☐	เรื่องที่ 1 การทดสอบแบบใดที่ผู้สอบบัญชีจะให้ความสนใจในการทดสอบความถูกต้องของรายการทางการเงิน (substantive test) เมื่อตรวจสอบโปรแกรมคอมพิวเตอร์	149
☐	เรื่องที่ 2 ท่านได้รับมอบหมายให้ตรวจสอบบัญชีลูกหนี้ซึ่งมีจำนวนเงินค่อนข้างสูง เมื่อเทียบกับสินทรัพย์ของบริษัทขนาดใหญ่แห่งหนึ่ง ท่านคิดจะใช้คอมพิวเตอร์ในการตรวจสอบแต่ท่านประสบเหตุการณ์ในแต่ละแบบ	149
☐	เรื่องที่ 3 เทคนิค 2 ประการในการตรวจสอบโปรแกรมโดยใช้ข้อมูลจริงอันได้แก่การประมวลผลภายใต้การควบคุมของผู้สอบบัญชี (controlled processing) และการประมวลผลใหม่ภายใต้การควบคุมของผู้สอบบัญชี (controlled reprocessing) ผู้สอบบัญชีจะเลือกใช้เมื่อใด	149
☐	เรื่องที่ 4 ผู้สอบบัญชีสามารถใช้ generalized computer audit program ตรวจสอบความถูกต้อง	150

❑ เรื่องที่ 5	การใช้ generalized computer programs มีวัตถุประสงค์หลักเพื่อทดสอบและวิเคราะห์	150
❑ เรื่องที่ 6	งานขั้นต่ำที่ผู้สอบบัญชีสามารถใช้ generalized computer-audit program จัดทำ	150
❑ เรื่องที่ 7	ผู้สอบบัญชีได้รับเทปแม่เหล็กที่บรรจุข้อมูลรายการสินค้าคงเหลือทั้งหมดและจำนวนเงินเรียงตาม style number และข้อมูลที่อยู่ในเทปไม่เรียงลำดับกัน (no particular sequence) ผู้สอบบัญชีสามารถตรวจหาสินค้าฝากขาย (consigned merchandise) จากข้อมูลในเทปดังกล่าว	150
❑ เรื่องที่ 8	โปรแกรมที่ใช้เรียงลำดับข้อมูล และโปรแกรมที่ใช้รวมข้อมูลหลายชุดเข้าด้วยกัน (sorting and merging) เป็นโปรแกรมที่ผู้สอบบัญชีมักจะใช้บ่อยในการตรวจสอบ โปรแกรมเหล่านี้ศูนย์ประมวลผลก็มีใช้เช่นกัน	151
❑ เรื่องที่ 9	วัตถุประสงค์หลักของ generalized computer audit program	151
❑ เรื่องที่ 10	การประมวลข้อมูลจริงผ่านโปรแกรมที่ใช้ปฏิบัติงานตามปกติและโปรแกรมของผู้สอบบัญชี (parallel simulation) เพื่อทดสอบการประมวลผล	151
❑ เรื่องที่ 11	ผู้สอบบัญชีสามารถใช้การเปรียบเทียบโปรแกรม (program comparison)	152
❑ เรื่องที่ 12	ในกรณีที่ผู้สอบบัญชีประมวลผลข้อมูลจริงเพื่อรวบรวมยอดคงเหลือจากบัญชีแยกประเภทเองในรอบระยะเวลาบัญชีที่ตรวจสอบโดยใช้โปรแกรมต่างหาก (computer audit program)	152
❑ เรื่องที่ 13	ในการตรวจสอบงบการเงิน ผู้สอบบัญชีอาจใช้โปรแกรมชุดที่เหมือนกับที่ใช้ปฏิบัติงานมาทำการประมวลข้อมูลจริงภายใต้การควบคุมของผู้สอบบัญชี	152
❑ เรื่องที่ 14	พนักงาน operator ผลักกลางคืนมีความรู้ในการเขียนโปรแกรม โดยที่คนทั่วไปไม่ทราบได้ใช้ความรู้ที่นั้นแก้ไขโปรแกรมการจ่ายเงินเดือนผ่านเครื่องควบคุมการทำงาน (Console) โดยแก้อัตราเงินเดือนให้พรรคพวกในหน่วยงานนั้น การทุจริตถูกพบโดยบังเอิญหลังจากนั้นหลายเดือน	152

	หน้า
☐ เรื่องที่ 15 ข้อใดที่ไม่ใช่ปัญหาในการใช้ test-deck ในการตรวจสอบ ด้านคอมพิวเตอร์	153
บทที่ 9 แนวคำตอบการทดสอบความเข้าใจ (เรื่องที่ 1-15)	155
☐ แนวคำตอบเรื่องที่ 1	157
☐ แนวคำตอบเรื่องที่ 2	158
☐ แนวคำตอบเรื่องที่ 3	158
☐ แนวคำตอบเรื่องที่ 4	158
☐ แนวคำตอบเรื่องที่ 5	158
☐ แนวคำตอบเรื่องที่ 6	158
☐ แนวคำตอบเรื่องที่ 7	158
☐ แนวคำตอบเรื่องที่ 8	159
☐ แนวคำตอบเรื่องที่ 9	159
☐ แนวคำตอบเรื่องที่ 10	159
☐ แนวคำตอบเรื่องที่ 11	159
☐ แนวคำตอบเรื่องที่ 12	159
☐ แนวคำตอบเรื่องที่ 13	159
☐ แนวคำตอบเรื่องที่ 14	159
☐ แนวคำตอบเรื่องที่ 15	159
ภาคผนวก ก	161
☐ ความเห็นเกี่ยวกับร่างแนวทางกฎหมายการโอนเงินทางอิเล็กทรอนิกส์	161
ภาคผนวก ข	173
☐ ความเป็นมาของการประชุมร่างแนวทางกฎหมายการโอนเงินทางอิเล็กทรอนิกส์โดย UNCITRAL	173
- การประชุมกลุ่มทำงานว่าด้วยการชำระหนี้ระหว่างประเทศ	174
- ข้อคิดเห็นจากการประชุมว่าด้วยการชำระหนี้ระหว่างประเทศ	174
ภาคผนวก ค	175
☐ แนวความคิดของกฎหมาย เพื่อการโอนเงินทางอิเล็กทรอนิกส์	175
- บทนำ	175
- ขอบเขตของกฎหมายการโอนเงินทางอิเล็กทรอนิกส์	175
- ความจำเป็นที่ต้องมีกฎหมาย	176

	หน้า
- สาเหตุที่ทำให้เกิดช่องว่างทางกฎหมาย	177
- ปัญหาบางประการอันเกิดจากการโอนเงินทางอิเล็กทรอนิกส์	178
- แนวความคิดทางกฎหมายการโอนเงินทางอิเล็กทรอนิกส์ในต่างประเทศ	180
- ลักษณะของแนวทางด้านกฎหมายที่จำเป็น	184
- ที่มาและข้อมูลที่น่าสนใจบางประการของพระราชบัญญัติการโอนเงินทางอิเล็กทรอนิกส์	185
❑ การโอนเงินที่มีการตกลงไว้ล่วงหน้า	190
❑ ข้อมูลที่น่าสนใจบางประการ (Data Protection Act 1984)	200
- ภาคที่ 1 ข้อความเบื้องต้น	200
- ภาคที่ 2 การจดทะเบียนและการควบคุมผู้ใช้ข้อมูลและ ผู้ใช้บริการข้อมูลคอมพิวเตอร์	202
- การกำกับควบคุม	205
- การอุทธรณ์	208
- บทเบ็ดเตล็ดและบทเสริม	209
- ภาคที่ 3 สิทธิของเจ้าของข้อมูล	211
ภาคผนวก ง	215
❑ การศึกษาการหักกลบลบหนี้ระหว่างประเทศ	215
❑ รายงานโครงการเรื่องการหักกลบลบหนี้	215
- คำนำ	215
- ความนำ	216
- บทสรุปและข้อสังเกตต่าง ๆ	217
- ประเภทของความเสี่ยงทางการเงิน	220
- ตลาดสำหรับข้อตกลงในการหักกลบลบหนี้	221
- รูปแบบตามกฎหมายของการหักกลบลบหนี้	222
- รูปแบบต่าง ๆ ที่จัดสร้างขึ้นจากการศึกษาเรื่องการหักกลบและความเสี่ยง	223
- ภาพทั้งหมดของความเสี่ยงเกี่ยวกับสภาพคล่อง	225
❑ คำอธิบายศัพท์	229
ภาคผนวก จ	231
❑ การตรวจสอบคอมพิวเตอร์ของหน่วยงานของรัฐในประเทศสหรัฐอเมริกา	231
- การตรวจสอบคอมพิวเตอร์ของ FDIC	231
- การตรวจสอบคอมพิวเตอร์ของ OCC (Office of the Comptroller of the Currency)	237
- การพัฒนาการตรวจสอบคอมพิวเตอร์ของ FDIC (Washington D.C.)	245

	หน้า
ภาคผนวก จ	251
❑ Role of the Bank of Thailand in Banking Computerization	253
❑ Appendix	277
- Electronic Banking and its impact on CAMEL	277
- How to Examine Computerized Commercial Banks	278
- Computer System Development Cycle	279
Project Development	280
Implementation	281
Maintenance	282
- Project Development	283
- Implementation	286
- Maintenance	287
ภาคผนวก ช	289
❑ การพิสูจน์โปรแกรมระบบงานที่สถาบันการเงินให้ใช้ทดสอบ ว่าเป็นโปรแกรมระบบงานชุดเดียวกับที่ใช้ปฏิบัติงานจริง	289
ภาคผนวก ซ	293
❑ วัตถุประสงค์ในการขอ ดู Source Program Listing	293

บทที่ 1

กลยุทธ์ในการเผชิญและแก้ไขปัญหา
เมื่อเกิดเหตุฉุกเฉิน

กลยุทธ์ในการเผชิญและแก้ไขปัญหาเมื่อเกิดเหตุฉุกเฉิน

1. บทนำ

ปัญหาสำคัญในการดำเนินงานด้านคอมพิวเตอร์ของธนาคารพาณิชย์และสถาบันการเงิน คือ การป้องกันความเสียหายที่อาจกระทบต่อการดำเนินงานและฐานะความมั่นคงของธนาคารพาณิชย์และสถาบันการเงิน อันเนื่องจากระบบคอมพิวเตอร์ล้มเหลวหรือหยุดทำงาน ซึ่งมีสาเหตุจากภัยพิบัติต่าง ๆ โดยที่ธนาคารพาณิชย์ส่วนใหญ่ ยังไม่มีการปฏิบัติในเรื่องเกี่ยวกับการจัดทำแผนฉุกเฉิน และการจัดตั้งระบบคอมพิวเตอร์สำรองอย่างจริงจัง เพื่อช่วยให้สามารถดำเนินงานและให้บริการแก่ประชาชนได้อย่างต่อเนื่อง ก็อาจสร้างปัญหาให้กับธนาคารพาณิชย์และผู้ที่เกี่ยวข้องทุกฝ่ายในภายหน้าได้อย่างมาก

ธนาคารแห่งประเทศไทยจึงได้เห็นความสำคัญของปัญหานี้ และได้ค้นคว้าหามาตรการต่าง ๆ เพื่อป้องกันและแก้ไขตลอดมา นอกจากการตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์โดยได้ให้ข้อสังเกตและข้อเสนอแนะใน รายงานการตรวจสอบ เพื่อเสนอแนะแนวทางที่เหมาะสมในการแก้ไขปัญหาและจุดอ่อนให้แก่ธนาคารพาณิชย์ แล้ว ยังได้กำหนดเงื่อนไขเกี่ยวกับระบบรักษาความปลอดภัยให้ธนาคารพาณิชย์มีแผนฉุกเฉินและระบบคอมพิวเตอร์สำรอง

ผลจากการดำเนินการดังกล่าว ได้ผลักดันให้ธนาคารพาณิชย์เพิ่มความสนใจและค้นคว้าเพื่อจัดทำแผนฉุกเฉิน และจัดตั้งระบบคอมพิวเตอร์สำรองขึ้น แต่ปัญหาส่วนใหญ่อยู่ที่เงินลงทุนและค่าใช้จ่ายในการจัดตั้งระบบคอมพิวเตอร์สำรอง ซึ่งเป็นจำนวนเงินที่ค่อนข้างสูง อย่างไรก็ตามผู้บริหารงานด้านคอมพิวเตอร์ของธนาคารพาณิชย์ไทย ได้ร่วมกันศึกษาและสัมมนาในเรื่องความร่วมมือระหว่างธนาคารพาณิชย์ในประเทศไทย เพื่อจัดตั้งบริษัทกลางซึ่งให้บริการระบบคอมพิวเตอร์สำรองแก่ธนาคารสมาชิก โดยมีลักษณะเป็น Common Back up ทั้งนี้เพื่อประหยัดเงินลงทุน และค่าใช้จ่ายของธนาคารสมาชิกลงได้เป็นจำนวนมาก ในเรื่องนี้ธนาคารแห่งประเทศไทยก็ได้เข้าร่วมศึกษาค้นคว้าเช่นกัน และให้ความสนับสนุนและส่งเสริมให้การดำเนินการบรรลุผลตามความเหมาะสมด้วย

หากหันมาพิจารณาปัญหาในการดำเนินงานด้านคอมพิวเตอร์ และแนวคิดในการแก้ไขปัญหาของสถาบันต่าง ๆ และผู้เชี่ยวชาญทางด้านการจัดทำแผนฉุกเฉินในประเทศสหรัฐอเมริกา จะพบว่ามีลักษณะคล้ายคลึงกับในประเทศไทย แต่ได้มีการค้นคิดเทคนิคใหม่ ๆ ขึ้นมาใช้ในการแก้ไขปัญหา ซึ่งอาจนำมาประยุกต์ใช้ในบ้านเราได้ แนวความคิดที่จะกล่าวต่อไปนี้จะได้ชี้และเน้นให้เห็นว่า แผนฉุกเฉินเพียงอย่างเดียวนั้นยังไม่เพียงพอ ควรมีการ ทบทวนและปรับปรุงแผนฉุกเฉินอยู่เป็นระยะ ๆ เพื่อให้มีประสิทธิภาพและสามารถใช้ได้ผลจริงเมื่อเกิดเหตุฉุกเฉินขึ้น

2. ความจำเป็นในการจัดทำแผนฉุกเฉินและระบบคอมพิวเตอร์สำรอง

เนื่องจากปัจจุบันศูนย์คอมพิวเตอร์ไม่ได้เป็นเอกเทศ แต่กลายเป็นเครื่องมือหรือเป็นระบบสำคัญ ที่เข้ามามีส่วนร่วมภายในองค์กร ดังนั้น ฝ่ายบริหารของธนาคารพาณิชย์และองค์กรที่ต้องทำงานอย่างต่อเนื่องจึงควร วิเคราะห์และประเมินความเสี่ยงที่จะเกิดความล้มเหลวต่อระบบงาน หรือเกิดภัยพิบัติอย่างอื่นที่ทำให้ธนาคารพาณิชย์ได้ รับความเสียหายอย่างรุนแรง แต่ถ้าโชคร้ายก็อาจจะทำให้ธุรกิจต้องหยุดชะงักหรือไม่สามารถดำเนินการต่อไปเลยทีเดียว

ผู้บริหารศูนย์คอมพิวเตอร์จะต้องประเมินผลจากภัยพิบัติที่จะกระทบต่อการปฏิบัติงานอย่างต่อเนื่องของธุรกิจโดยรวม ซึ่งในหลาย ๆ กรณีค่าใช้จ่ายในการออกแบบและบำรุงรักษาแผนปฏิบัติงาน และแก้ไขเหตุฉุกเฉินที่เพียงพอ จะต่ำกว่าเมื่อเทียบกับความเสียหายที่เกิดจากธุรกิจที่หยุดชะงัก ตลอดจนผลทางด้านกฎหมายและกฎเกณฑ์ต่าง ๆ ที่ตามมา

ในสหรัฐอเมริกา Federal regulators ได้พิจารณาปัญหาอย่างจริงจัง และได้ออกกฎเกณฑ์ขั้นต่ำเพื่อให้องค์กรต่าง ๆ มีการวางแผนที่เป็นมาตรฐาน เพื่อรับมือกับภัยพิบัติที่อาจเกิดขึ้น ซึ่งเป็นแรงผลักดันสำคัญที่ทำให้สถาบันการเงินในสหรัฐอเมริกาทำการพัฒนาแผนฉุกเฉินในเรื่องต่าง ๆ อย่างกว้างขวาง

3. กฎหมายที่ออกบังคับใช้เกี่ยวกับการจัดตั้งแผนฉุกเฉินในสหรัฐอเมริกา

3.1 The Foreign Corrupt Practices Act ค.ศ.1977 ปรับปรุงเมื่อ ค.ศ.1983
กฎหมายฉบับนี้แต่เดิมมีจุดมุ่งหมายที่จะกำหนดแนวทางให้ธนาคารที่ทำธุรกิจต่างประเทศปฏิบัติตาม อย่างไรก็ตามเมื่อไม่นานมานี้ก็ได้นำมาใช้บังคับกับธนาคารที่ทำธุรกิจเกี่ยวกับบ้านพักอาศัยด้วย ถือได้ว่าเป็นกฎหมายฉบับแรกที่กำหนดให้ธนาคารต้องมีการวางแผนฉุกเฉิน และต้องมีการรักษาความปลอดภัยให้กับทรัพย์สินของตนอย่างเพียงพอ ทั้งนี้รวมถึงองค์กรใดๆ ที่เกี่ยวข้องกับการค้าหลักทรัพย์ ทั้งที่ถูกควบคุมโดยรัฐบาล หรือที่มีข้อมูลมั่วต่อกับรัฐบาล การฝ่าฝืนกฎหมายมาตรานี้มีโทษปรับไม่เกิน 1 ล้านดอลลาร์ สรอ. ด้วย

3.2 The Office of the Comptroller of the Currency Banking Circular 177 ค.ศ.1978 แก้ไขเพิ่มเติม ค.ศ.1983 ออกเป็นหนังสือเวียนเพื่อกำหนดให้ธนาคารพาณิชย์ทุกธนาคารต้องพัฒนามาตรการเพื่อลดผลกระทบและ/หรือความเสี่ยงจากการสูญเสียข้อมูล กฎหมายมาตรานี้ให้อำนาจแก่รัฐบาลในการเข้าตรวจสอบแผนงานและเข้าจัดการถ้ารู้สึกว่แผนงานไม่มีประสิทธิภาพเพียงพอ จึงมีผลให้คณะกรรมการของธนาคารพาณิชย์ต้องรับผิดชอบในการทบทวนแผนฉุกเฉินของธนาคาร และบันทึกไว้ในรายงานการประชุมเป็นประจำทุกปี

3.3 Federal Home Loan Bank Board Memorandum R 67 ลงวันที่ 4 กันยายน ค.ศ.1986 กฎหมายฉบับนี้กำหนดมาตรฐานขั้นต่ำของการแก้ไขสถานการณ์เมื่อเกิดเหตุฉุกเฉิน ซึ่งสถาบันประกันเงินฝาก (Federally insured thrifts) ต้องปฏิบัติตามแนวทางเกี่ยวกับแผนฉุกเฉินตามที่กำหนดในมาตรานี้ และให้อำนาจแก่ FHLBB ในการบังคับให้ธนาคารที่มีข้อบกพร่องทำการแก้ไขแผนฉุกเฉินให้เหมาะสม

อย่างไรก็ดีกฎหมายต่าง ๆ ดังกล่าว ก็ไม่ได้ช่วยแก้ไขปัญหที่เกิดขึ้นกับฝ่ายบริหาร ซึ่งวางแผนเพียงเพื่อให้เป็นไปตามกฎเกณฑ์ โดยไม่คำนึงถึงความเหมาะสมในการปฏิบัติตามแผนเมื่อเกิดเหตุฉุกเฉินขึ้นจริง ๆ เพราะขาดแนวทางและประสบการณ์ในการจัดทำแผนดังกล่าว

4. ระยะเวลาในการอยู่รอดของธุรกิจหลังจากระบบคอมพิวเตอร์เสียหาย

มหาวิทยาลัย Minnesota ในประเทศสหรัฐอเมริกา ได้ทำการศึกษาเรื่องระยะเวลาที่กิจการพอจะดำเนินการต่อไปได้หลังจากเกิดเหตุฉุกเฉินขึ้นกับศูนย์คอมพิวเตอร์ ซึ่งปรากฏว่ากิจการธนาคารพาณิชย์และสถาบันการเงินจะอยู่รอดไปได้อีก 1 ถึง 2 วันเท่านั้น บริษัทขายสินค้าจะอยู่รอดได้อีกประมาณ 2 วัน บริษัทที่ทำการผลิตประมาณ 5 วัน และบริษัทประกันภัยประมาณ 5 ถึง 6 วัน

5. การวางแผนและกลยุทธ์ในการแก้ไขปัญหาเมื่อเกิดเหตุฉุกเฉิน

5.1 การวางแผนเพื่อแก้ไขสถานการณ์เมื่อเกิดเหตุฉุกเฉิน จะต้องเริ่มต้นจากการประเมินความเสี่ยงหรือปัญหา และกำหนดวิธีการแก้อ่อนหรือปัญหาพร้อมกันไป ซึ่งผู้บริหารระดับสูงส่วนใหญ่เห็นพ้องกันว่า การออกแบบและพัฒนาแผนการแก้ไขดังกล่าวมีความสำคัญมาก และควรได้รับคำแนะนำจากผู้ชำนาญการของบริษัทที่ปรึกษาทางด้านนี้โดยตรงโดยเฉพาะอย่างยิ่งธนาคารพาณิชย์หรือสถาบันการเงิน หากหยุดการให้บริการในเวลาเพียง 2-3 ชั่วโมง ก็อาจทำให้ธุรกิจบรรลุผลสำเร็จหรือล้มเหลวได้ต่างกันมาก

สิ่งสำคัญประการแรกของแผนฉุกเฉิน คือ การออกแบบยุทธวิธีในการแก้ไขและพัฒนาแผนสำหรับฟื้นฟูข้อมูลขึ้นมาใหม่ ซึ่งต้องวิเคราะห์จัดลำดับความสำคัญของข้อมูลด้วยว่าจำเป็นต้องแก้ไขเพื่อฟื้นฟูข้อมูลทั้งหมดโดยทันทีหรือไม่ หรือมีข้อมูลใดที่พอจะเก็บไว้แก้ไขในวันอื่นได้บ้าง และต้องทราบถึงความต้องการในการแก้ไขปัญหาด้วย ถ้ากิจการมีการให้บริการแบบ On-line เพียงอย่างเดียว ความเสียหายที่ได้รับใน 2-3 ชั่วโมงแรกที่ระบบหยุดชะงักจะเป็นปัญหาต่อความอยู่รอดของกิจการหรือไม่ หรือกิจการพอจะดำเนินการต่อไปได้อีก 2-3 วัน หรือสัปดาห์ ธุรกิจที่ต่างชนิดกันจะมีเป้าหมายในการแก้ไขสถานการณ์เมื่อเกิดเหตุฉุกเฉินต่างกัน ยุทธวิธีแก้ปัญหาดังกล่าวควรได้รับข้อมูลและความเห็นชอบจากทั้งผู้ใช้ระบบ (user) และผู้บริหารระดับสูง รวมทั้งคณะกรรมการบริหารของธนาคารพาณิชย์ โดยควรพิจารณาถึงการจัดลำดับความสำคัญของแต่ละงานและแต่ละขั้นตอนด้วย

5.2 การนำแผนงานมาเขียนเป็นแนวทางปฏิบัติงานเพื่อใช้เมื่อเกิดเหตุฉุกเฉิน แนวทางเหล่านี้จะระบุขั้นตอนการปฏิบัติงานที่เป็นมาตรฐานสำหรับความเสี่ยงประเภทต่าง ๆ หรือปัญหาต่าง ๆ ที่อาจเกิดขึ้น ซึ่งสิ่งหนึ่งที่ต้องกำหนดอยู่ในแผนงานด้วยก็คือ การเลือกใช้สถานที่ปฏิบัติงานสำรอง (Back up Site) ว่าจะเป็นแบบ Hot Site, Cold Site, Mobile Computer Trailer หรือวิธีอื่น ๆ

(1) Hot Site :

ในธุรกิจธนาคารพาณิชย์และธุรกิจหลักทรัพย์ ซึ่งจะเกิดภาวะวิกฤตทันทีถ้าระบบคอมพิวเตอร์ใช้การไม่ได้เพียง 2-3 ชั่วโมง ในสหรัฐอเมริกาธุรกิจเหล่านี้ส่วนใหญ่จะเลือกใช้ Hot Site ซึ่งเป็นบริการของบริษัทผู้ให้บริการแก้ไขเหตุฉุกเฉิน (Disaster service recovery vendor) สถานที่ปฏิบัติงานสำรองเหล่านี้มักจะมีอุปกรณ์ที่จำเป็น เช่น ตู้ Disk ตู้ Tape เครื่องพิมพ์ และอุปกรณ์สื่อสารติดตั้งอยู่แล้ว พร้อมสำหรับการเริ่มปฏิบัติงานได้ใหม่ โดยต้องการเพียงข้อมูลชุดสำรองและพนักงานควบคุมระบบ (Operator) เท่านั้น ซึ่งอาจต้องใช้งานไปจนกว่าศูนย์คอมพิวเตอร์ถาวรจะซ่อมแซมเสร็จ

(2) Cold Site :

จะมีลักษณะเป็นห้องคอมพิวเตอร์ว่าง ๆ ซึ่งเตรียมสถานที่และอุปกรณ์สื่อสารไว้แล้ว เมื่อเกิดเหตุฉุกเฉินจึงย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ที่จำเป็นต่าง ๆ รวมทั้งโปรแกรมและบุคลากรเข้ามาปฏิบัติงาน ซึ่งต้องเสียเวลา 24-48 ชั่วโมงในการติดตั้งอุปกรณ์ต่าง ๆ ให้พร้อมที่จะใช้งาน ทั้งนี้บริษัทผู้ขายเครื่องคอมพิวเตอร์ในสหรัฐอเมริกาจะต้องมีเครื่องและอุปกรณ์คอมพิวเตอร์ที่พร้อมจะใช้แทนกันได้ทันที ด้วยเหตุนี้บริษัทการเงินหลาย ๆ แห่งจึงไม่เลือกใช้วิธีนี้

(3) Mobile Computer Trailer :

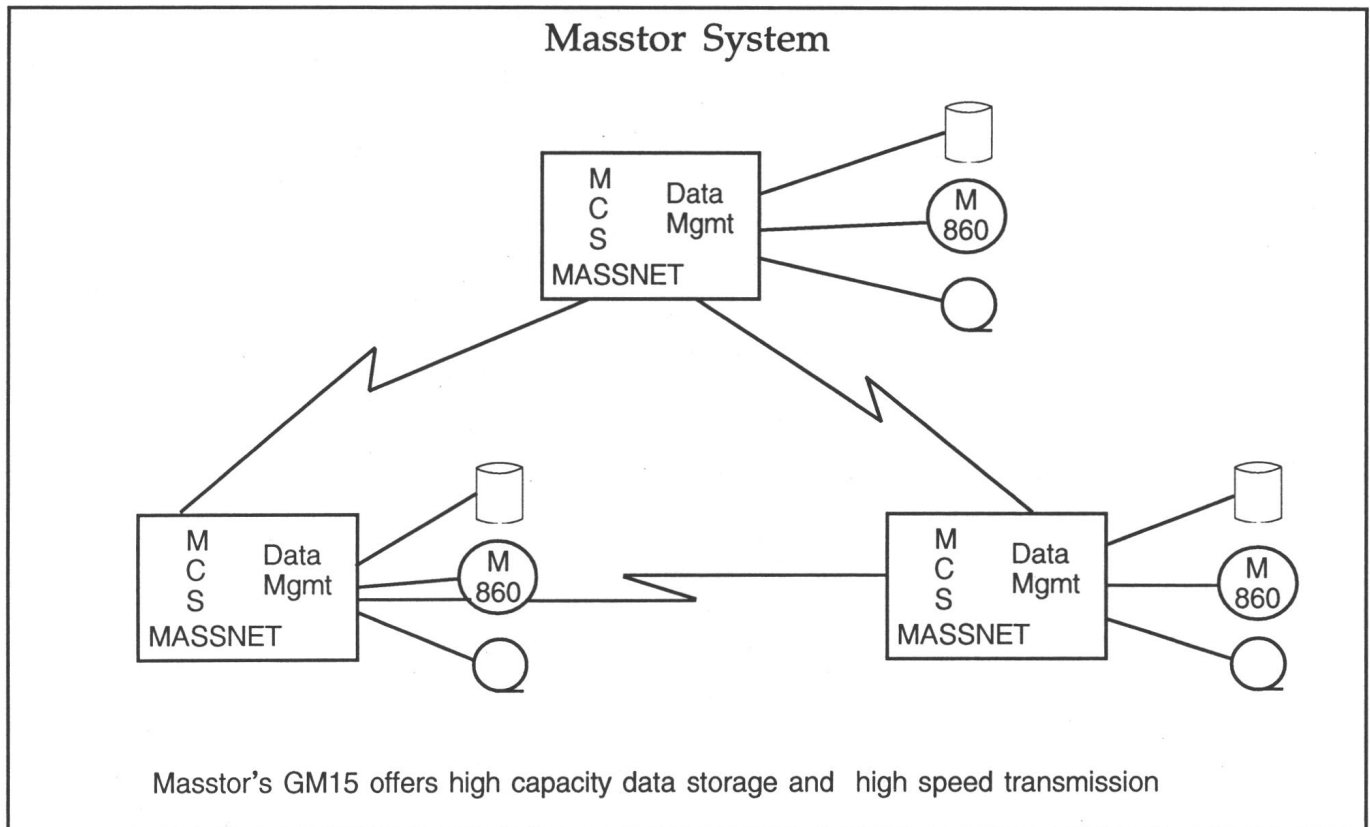
อีกวิธีหนึ่งซึ่งถูกคิดค้นขึ้นมาใหม่ คือ ศูนย์คอมพิวเตอร์เคลื่อนที่ ซึ่งติดตั้งอยู่ในรถพร้อมที่จะไปให้บริการแก่ลูกค้าถึงที่ จึงไม่ต้องย้ายบุคลากรหรืออุปกรณ์ต่าง ๆ ไปยังศูนย์คอมพิวเตอร์สำรองเลย

(4) ทำข้อตกลงแลกเปลี่ยนซึ่งกันและกัน

ทางเลือกอีกวิธีหนึ่งคือ การตกลงให้ความช่วยเหลือซึ่งกันและกันระหว่างธนาคารพาณิชย์หรือบริษัท เมื่อฝ่ายใดฝ่ายหนึ่งเกิดเหตุฉุกเฉิน ซึ่งเป็นทางเลือกที่ประหยัดกว่าทางเลือกอื่น ๆ แต่วิธีนี้จะไม่รองรับกรณีที่เกิดเหตุฉุกเฉินกับบริษัทคู่สัญญาพร้อม ๆ กัน หรือบริษัทคู่สัญญาอาจจัดลำดับความสำคัญของงานที่มาจากอีกบริษัทหนึ่งไว้รั้งท้ายก็ได้ อย่างไรก็ตามวิธีนี้ก็จะเป็นทางเลือกที่เหมาะสมสำหรับกิจการหรือบริษัทขนาดเล็กที่มีทุนน้อย

5.3 การตัดสินใจเรื่องการบำรุงรักษาศูนย์คอมพิวเตอร์สำรอง ซึ่งมีส่วนประกอบเช่นเดียวกับระบบที่ใช้งานประจำ ทำให้ค่าใช้จ่ายสูงเกินไปสำหรับบริษัทส่วนใหญ่ ทั้งนี้รวมทั้งขั้นตอนในการจัดเก็บและหมุนเวียนใช้ Tape ซึ่งต้องทำเป็นลายลักษณ์อักษร และมีการติดตามอย่างใกล้ชิด การดูแล Tape มีทางเลือกอยู่หลายวิธี ขึ้นอยู่กับความต้องการใช้งานและลำดับความสำคัญของงาน บางบริษัทเก็บ Tape ข้อมูลสำรองไว้ที่ศูนย์คอมพิวเตอร์สำรอง บริษัทผู้ให้บริการระบบคอมพิวเตอร์สำรองเพื่อแก้ไขเหตุฉุกเฉินบางแห่งทั้งที่เป็นแบบ Hot Site และ Cold Site ได้รวมการเก็บรักษาข้อมูลไว้ในบริการด้วย บางบริษัทก็ให้บริการเก็บรักษาข้อมูลสำรองด้วยระบบอิเล็กทรอนิกส์ โดยผู้ให้บริการสามารถ Update ข้อมูลผ่านทางสายสื่อสารมายังบริษัทผู้ให้บริการเก็บข้อมูลสำรองได้เสมือนกับการ Back up ที่ทำตามปกติ

บริษัท Tandem และบริษัท Masstor System เป็นผู้ให้บริการเก็บรักษาข้อมูลสำรองในลักษณะนี้ โดย Tandem จะเรียกบริการนี้ว่า RDF (Remote Duplicate Database Facility) ซึ่งสามารถลดเวลาในการเริ่มต้นระบบคอมพิวเตอร์ขึ้นมาใหม่ จาก 24 ชั่วโมง ลงเหลือไม่เกิน 1 ชั่วโมง ส่วน Masstor System จะให้บริการ On-line อัดโนมิตีด้วยหน่วยเก็บข้อมูลความจุสูง (high-capacity data storage) และเชื่อมต่อด้วยเครื่องคอมพิวเตอร์ขนาดใหญ่ที่มีความเร็วสูงระหว่างภูมิภาคต่าง ๆ ซึ่งประกอบด้วยระบบ MB180 และ GIMS (Global Information Management System) ดังรูป



บริษัท Masstor มีความชำนาญเป็นพิเศษในการให้บริการแก่ลูกค้า ซึ่งมีความเสี่ยงในการดำเนินงานสูง และอาจทำให้ระบบงานเสียหายได้ ระบบนี้มีตลาดอยู่ทั่วยุโรป และมีลูกค้าเป็นจำนวนมากแล้ว

5.4 การวางแผนฉุกเฉินที่สมบูรณ์อาจใช้เวลาติดต่อกันเป็นปี เมื่อได้จัดทำแผนงานที่เหมาะสมเป็นลายลักษณ์อักษรแล้ว ขั้นตอนต่อไปคือ การทดสอบและบำรุงรักษา ซึ่งหลังจากองค์ประกอบทั้งหมดในแผนการเข้ารूपเข้ารอยแล้ว ยังจำเป็นต้องทำการทดสอบระบบรวมเพื่อประเมินประสิทธิภาพของแผนทั้งหมด

5.5 เมื่อทดลองสร้างสถานการณ์ฉุกเฉิน มักจะพบปัญหาที่คาดไม่ถึงเกิดขึ้นในแผนเสมอ ดังนั้นจึงควรทำการทดสอบให้ทั่วถึงทุกองค์ประกอบในแผน และบุคลากรในแต่ละส่วนที่เกี่ยวข้องตั้งแต่ผู้ใช้งานจนถึงระดับบริหาร ซึ่งมีหน้าที่ในการเข้าร่วมทดสอบด้วย

5.6 ความซับซ้อนของขั้นตอนการทดสอบ จะขึ้นอยู่กับปริมาณการปฏิบัติงานของบริษัทที่ถูกกำหนดให้ดำเนินการที่สถานที่ปฏิบัติงานสำรองเมื่อเกิดเหตุฉุกเฉินขึ้น ตัวอย่างเช่น บริษัท Fidelity Investments ซึ่งมีสำนักงานใหญ่อยู่ที่ Boston ได้จัดให้มีการทดสอบในวันหยุดสุดสัปดาห์ปีละหลายครั้ง โดยใช้สถานที่ปฏิบัติงานสำรองใน Philadelphia ซึ่งเช่าจากบริษัท Sunguard Recovery Services ทีมงานที่ได้รับการแต่งตั้งจะนำ Tape ข้อมูลสำรองประจำวันไปยังสถานที่ปฏิบัติงานสำรอง ซึ่งเป็นแบบ Hot Site เพื่อเริ่มต้นการปฏิบัติงาน และตัวแทนของบริษัท Fidelity ทั่วประเทศจะสร้างรายการประจำวันป้อนเข้าสู่ระบบ การปฏิบัติงานสำรองมีเป้าหมายที่จะดำเนินงานเพื่อให้บริการแก่ผู้ใช้งานได้อย่างต่อเนื่องและไม่มีอุปสรรค การทดสอบระบบจะถูกประเมินผลในรูปของรายงานที่แสดงถึงความถูกต้องและความละเอียดทั่วถึงในการจัดการกับรายการที่ทดสอบ

5.7 หลังจากการทดสอบสิ้นสุดลง ยังต้องทำการทบทวนและปรับปรุงแผนฉุกเฉินเป็นครั้งคราว เพื่อให้แผนงานมีประสิทธิภาพและใช้ได้ผลต่อไป หลายบริษัทต้องเสียเวลาและค่าใช้จ่ายไปมากกับการวางแผน แต่กลับพบว่าแผนฉุกเฉินนั้นไม่มีประสิทธิภาพ ทั้งนี้เพราะขาดการปรับปรุงให้ทันต่อเหตุการณ์นั่นเอง

จากการสำรวจของบริษัท Data Processing Security พบว่าบริษัทที่ถูกสำรวจ ซึ่งกล่าวได้ว่ามีแผนฉุกเฉินที่สมบูรณ์แล้ว แต่เมื่อเกิดเหตุฉุกเฉินขึ้นจริง และได้ปฏิบัติตามแผน กลับใช้ได้ผลเพียง 5% เท่านั้น บริษัทส่วนใหญ่ลงความเห็นว่าความผิดพลาดนั้นเกิดจากแผนฉุกเฉินที่ล้าสมัย และไม่เข้ากับลำดับความสำคัญและความต้องการที่เป็นอยู่ในปัจจุบัน ดังนั้นการปรับปรุงแผนจึงต้องมีการทบทวนและปรับให้เข้ากับการเปลี่ยนแปลงของกลยุทธ์ และลำดับความสำคัญในหน่วยงานอยู่เสมอ

5.8 ฝ่ายบริหารของธนาคารพาณิชย์ต้องตระหนักว่า การหยุดชะงักของการประมวลผลจะมีผลกระทบไปทั่วทุกส่วนงาน เพราะระบบงานที่อาศัยคอมพิวเตอร์จำเป็นต้องได้รับการสนับสนุนให้การปฏิบัติงานทำได้อย่างต่อเนื่อง มากกว่าที่จะมาแก้ไขปัญหาเฉพาะหน้าเป็นครั้งคราว ดังนั้นการกำหนดกลยุทธ์ในการดำเนินงานและการปฏิบัติงานของส่วนงานจะต้องคำนึงถึงแผนฉุกเฉินควบคู่กันไปด้วย

6. ความสำเร็จของการแก้ไขปัญหาเมื่อเกิดเหตุฉุกเฉิน

ตัวอย่างของการวางแผนฉุกเฉินที่ประสบผลสำเร็จ คือ บริษัท Steinberg ในเมือง Montreal ประเทศแคนาดา ซึ่งมีทรัพย์สินถึง 4.5 พันล้านดอลลาร์ สรอ. ในธุรกิจ Supermarket ภัตตาคาร และร้านค้าปลีกหลายร้อยแห่ง เมื่อวันที่ 26 ตุลาคม ค.ศ.1986 สำนักงานใหญ่ของธุรกิจหลายพันล้านนี้ถูกเพลิงไหม้ไปหมด มีผลให้การดำเนินงานที่ใช้คอมพิวเตอร์ทั้งหมดของกิจการในเครือข่ายของ Steinberg ใช้การไม่ได้ ในเช้าวันรุ่งขึ้นบริษัท Comdisco Disaster Recovery Services ซึ่งเป็นผู้ให้บริการศูนย์คอมพิวเตอร์สำรองแบบ Hot Site แก่ Steinberg ได้รับแจ้งถึงเหตุฉุกเฉินนี้ ทีมงานแก้ไขเหตุฉุกเฉินจำนวน 25 คน ก็ได้เดินทางมายังเมือง Carlstadt รัฐ New Jersey โดยทันที เพื่อช่วยกันเตรียมการแก้ไขและดำเนินงานกู้ระบบขึ้นมาใหม่ Tape จำนวนหมื่นม้วนซึ่งบันทึกข้อมูลในการดำเนินงานของบริษัท Steinberg ได้ถูกขนส่งข้ามประเทศมายังบริษัท Comdisco อย่างรวดเร็ว และหลังจากนั้นเพียงไม่กี่ชั่วโมงต่อมาระบบงานหลายระบบก็สามารถดำเนินงานต่อไปได้

หลังจากเพลิงไหม้ 2 วัน ระบบที่สำคัญ ๆ ก็สามารถให้บริการได้ และภายในวันที่ 3 ทุกอย่างก็ดำเนินไปได้เหมือนปกติ

เหตุการณ์ที่เกิดขึ้นนี้แสดงให้เห็นถึงความสำคัญของการมีแผนฉุกเฉินที่สามารถใช้งานได้ผลจริง ซึ่ง Steinberg ได้เตรียมไว้ แผนฉุกเฉินนี้ได้ผ่านการพิจารณาจากคณะกรรมการบริหารอย่างถี่ถ้วน และนอกจากจะเป็นแผนการที่ดีพอแล้ว ยังได้มีการทดสอบก่อนเกิดเหตุเพียงไม่กี่สัปดาห์ด้วย จึงสรุปได้ว่าการเตรียมพร้อมอยู่เสมอก็เป็นปัจจัยสำคัญในการต่อสู้กับภัยพิบัติเพื่อความอยู่รอดของกิจการเช่นกัน

7. สรุป

แนวความคิดและสถานการณ์ข้างต้น ได้สะท้อนให้เห็นถึงความสำคัญของแผนฉุกเฉิน ซึ่งธนาคารพาณิชย์ควรนำมาพิจารณาประกอบในการพัฒนาและจัดทำแผนฉุกเฉิน กล่าวคือ การมีแผนฉุกเฉินที่สมบูรณ์แบบจะต้องได้รับความสนใจและเอาใจใส่จากฝ่ายบริหาร รวมทั้งคณะกรรมการบริหารของธนาคารพาณิชย์ด้วย และควรขอคำแนะนำหรือคำปรึกษาจากผู้ชำนาญการในการวางแผนฉุกเฉิน เพื่อสามารถเลือกใช้กลยุทธ์ที่เหมาะสมในการรับมือกับภัยพิบัติประเภทต่าง ๆ ทั้งนี้จะต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นกับการดำเนินงานโดยส่วนรวมของธนาคารพาณิชย์เองและระบบการธนาคารเป็นหลัก แผนฉุกเฉินที่สามารถจะนำมาใช้ได้อย่างมีประสิทธิภาพจะต้องมีการทดสอบการปฏิบัติตามแผนนั้นเป็นประจำ เพื่อให้เกิดความพร้อมหากมีภัยพิบัติเกิดขึ้นจริง และจะต้องมีการทบทวนปรับปรุงแผนฉุกเฉินให้เหมาะสมและสอดคล้องกับความเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับธนาคารพาณิชย์อยู่เสมอด้วย



บทที่ ๒

ยุทธวิธีในการจัดทำแผนฉุกเฉิน

ยุทธวิธีในการจัดทำแผนฉุกเฉิน

1. บทนำ

การสร้างหรือจัดทำแผนฉุกเฉิน หากได้ทำอย่างรอบคอบและเหมาะสมตั้งแต่แรกแล้ว ก็เชื่อได้ว่าแผนฉุกเฉินนั้นประสบความสำเร็จไปครึ่งทางแล้ว ที่เหลือคงต้องจัดให้มีการดูแลและบำรุงรักษาแผนให้สอดคล้องกับการเปลี่ยนแปลงขององค์กร และสภาพแวดล้อมที่เปลี่ยนแปลงไป และสิ่งสำคัญที่จะต้องปฏิบัติอยู่เป็นประจำก็คือ การทดสอบแผนฉุกเฉินเพื่อประเมินประสิทธิภาพและความสำเร็จของแผน ทั้งหมดนั้นหากไม่ได้รับการสนับสนุนอย่างเพียงพอจากคณะกรรมการบริหารของธนาคารแล้ว ก็เป็นจุดบอดที่สำคัญของแผนฉุกเฉินที่จะจัดทำหรือได้จัดทำไปแล้วก็ตาม

ที่กล่าวข้างต้นนั้นเป็นปัญหาที่ทุกฝ่ายที่เกี่ยวข้องได้ตระหนกอยู่แล้ว แต่ทำอย่างไรที่จะทำให้แผนฉุกเฉินมีประสิทธิภาพ สามารถใช้ปฏิบัติงานได้จริง ช่วยลดและป้องกันความเสียหายที่จะเกิดขึ้นให้เหลือน้อยที่สุด

ดังนั้น การค้นหายุทธวิธีในการจัดทำแผนฉุกเฉินจึงเป็นสิ่งที่ควรนำมาใช้วิเคราะห์ และพิจารณาประกอบควบคู่ไปด้วย โดยเฉพาะกิจการหรือธุรกิจของธนาคารพาณิชย์ที่มีผลกระทบต่อความปลอดภัยหรือผาสกแห่งสาธารณชน ซึ่งต้องการความละเอียดอ่อนและรอบคอบด้วยแล้ว การค้นหานหายุทธวิธีออกจะสำคัญและขาดเสียมิได้ บทความนี้จึงได้สรุปและเรียบเรียงยุทธวิธีในการจัดทำแผนฉุกเฉินจากผู้เชี่ยวชาญและมีประสบการณ์ทางด้านนี้ เพื่อใช้เป็นแนวทางในการพัฒนาและควบคุมการจัดทำแผนฉุกเฉินของธนาคารพาณิชย์ให้บรรลุเป้าหมาย โดยเน้นให้เห็นถึงสาเหตุที่อาจทำให้แผนล้มเหลวหรือสร้างความเสียหายมากขึ้น

หัวใจของระบบการจัดทำแผนฉุกเฉินคือ คู่มือปฏิบัติงานในภาวะฉุกเฉินที่อธิบายวิธีการแก้ไขปัญหาแต่ละลักษณะ และแนวทางปฏิบัติของผู้ที่เกี่ยวข้องไว้อย่างชัดเจน เนื่องจากในช่วงวิกฤตจะไม่มีผู้ใดมีเวลาตัดสินใจสั่งการได้อย่างมีประสิทธิภาพ

2. สาเหตุของปัญหาในการจัดทำแผนฉุกเฉิน

สาเหตุใหญ่ที่อาจทำให้แผนฉุกเฉินไม่สามารถใช้แก้ไขหรือบรรเทาภัยพิบัติ อาจแบ่งออกได้ดังต่อไปนี้

2.1 กำหนดมาตรการป้องกันความเสี่ยงเพียงบางส่วน ผู้พัฒนาแผนฉุกเฉินจำเป็นต้องวิเคราะห์ความเสี่ยงทุกรูปแบบที่อาจเกิดขึ้นในทุก ๆ ฝ่าย ทั้งนี้เพื่อช่วยให้สามารถมองเห็นความล่อแหลมต่อภัยอันตรายแต่ละลักษณะ และตัดสินใจว่าจำเป็นต้องมีแผนฉุกเฉินเฉพาะฝ่ายใดบ้าง จุดอ่อนที่พบเสมอได้แก่ ผู้วางแผนให้ความสำคัญเฉพาะด้านใดด้านหนึ่ง หรือมองข้ามจุดอ่อนบางจุดไป เช่น กำหนดและประมวลผลข้อมูลสำรอง โดยถือว่าระบบคอมพิวเตอร์เป็นศูนย์กลางของทุกสิ่งทุกอย่างของธนาคาร ซึ่งแม้ในข้อเท็จจริงจะเป็นเช่นนั้น แต่ผู้วางแผนจะต้องระลึกอยู่เสมอว่าธุรกิจของธนาคารมิใช่มีเพียงการประมวลผลข้อมูลเท่านั้น ยิ่งกว่านั้นแม้ในธนาคารที่ใช้คอมพิวเตอร์มากที่สุด ก็ยังมีส่วนงานบางส่วนที่มีได้นำเข้าศูนย์คอมพิวเตอร์ใหญ่ เช่น ใช้ Micro Computer สำหรับบริการบางด้าน เช่น Letter of Credit, เงินให้กู้ยืมบางประเภท หรือบริการชำระค่าสาธารณูปโภค และงานบางส่วนก็ทำด้วยมือ

2.2 ขาดแผนงานสำคัญบางส่วน เช่น

- 2.2.1 มิได้วิเคราะห์ปรับปรุงวิธีการควบคุมขั้นตอนการปฏิบัติต่าง ๆ เพื่อบรรเทาผลเสียหายจากภัยที่อาจเกิดขึ้น
- 2.2.2 มิได้เผื่อทางเลือกสำหรับการประมวลผลงานที่มีความสำคัญและจำเป็นไว้ในกรณีที่ไม่สามารถใช้คอมพิวเตอร์เป็นเวลานาน
- 2.2.3 มิได้กำหนดแนวทางในการฟื้นฟูชุดข้อมูลที่สำคัญและจำเป็นไว้โดยครบถ้วน

2.3 ตั้งข้อสมมติฐานผิดพลาด แผนฉุกเฉินได้จากการตั้งข้อสมมติฐานว่าภัยพิบัติลักษณะหนึ่ง ๆ จะเกิดขึ้น ณ ส่วนใดของธนาคาร มีระดับความรุนแรงเพียงใด และในเวลาใด เป็นต้น บางครั้งผู้วางแผนอาจจะเลยสิ่งต่าง ๆ ดังต่อไปนี้

- 2.3.1 ข้อตกลงใช้ระบบสำรองร่วมกับกิจการอื่นไม่สามารถใช้ได้ทางปฏิบัติ เนื่องจากศูนย์คอมพิวเตอร์ของคู่สัญญาไม่สามารถแบ่งเวลาให้ได้เมื่อเกิดเหตุฉุกเฉิน
- 2.3.2 ศูนย์บริการประมวลผลภายนอกที่ธนาคารมีข้อตกลงสำรองเวลาไว้ไม่สามารถให้บริการได้
- 2.3.3 พนักงานที่รับผิดชอบในการแก้ไขเหตุฉุกเฉินขาดความเข้าใจและความชำนาญในการทำหน้าที่เมื่อเกิดปัญหา ทำให้ปฏิบัติงานผิดพลาด
- 2.3.4 หน่วยงานที่รับผิดชอบฟื้นฟูความเสียหายถูกลดบทบาทหรือความสำคัญลง การตัดสินใจเกี่ยวกับการแก้ไขปัญหาและฟื้นฟูระบบต้องอาศัยบุคคลผู้มีประสบการณ์ และมีอำนาจบางอย่างเพียงพอ เพื่อให้ทุกอย่างเป็นไปตามแผนที่กำหนดไว้

2.4 แผนล้าสมัย แผนฉุกเฉินที่พัฒนาไว้เป็นเวลานานเกินสมควร อาจไม่สามารถนำมาใช้ให้บรรลุเป้าหมายได้ เนื่องจากเหตุดังต่อไปนี้

- 2.4.1 ปัจจัยแวดล้อมเปลี่ยนแปลงไปจากเดิม เช่น ธนาคารคิดค้นเสนอบริการประเภทใหม่ ๆ หรือลดบริการบางประเภท กระบวนการปฏิบัติงานได้รับการปรับปรุงให้แตกต่างจากที่เคยปฏิบัติ ในขณะที่มีการพัฒนาแผน ทำให้แผนไม่เพียงพอและไม่เหมาะสมในการนำออกปฏิบัติ
- 2.4.2 ขาดคนสนใจ เนื่องจากเวลาผ่านไปนาน หากไม่มีการปรับปรุงหรือทดสอบการปฏิบัติตามแผนก็อาจทำให้พนักงานเจ้าหน้าที่หลงลืมไปว่ายังมีแผนฉุกเฉินอยู่ในธนาคาร

3. แนวทางในการวางแผนฉุกเฉิน

การพัฒนาแผนฉุกเฉินเริ่มจากการจัดทำตารางโครงการ เพื่อมิให้ผู้ปฏิบัติงานเกิดการสับสน และสามารถติดตามความก้าวหน้าได้โดยสะดวก ตารางนี้ควรจำแนกงานที่ทำออกเป็นงานหลักและงานย่อยที่ประกอบขึ้นเป็นแผนรวม

กลุ่มเจ้าหน้าที่ซึ่งรับผิดชอบพัฒนาแผน ควรแบ่งออกเป็นคณะทำงานต่าง ๆ จำนวนคณะทำงานขึ้นอยู่กับขนาดของแผนว่าครอบคลุมงานด้านใดบ้าง และเพื่อให้ผู้ปฏิบัติมีเป้าหมายที่ชัดเจน ธนาคารควรตั้งคณะกรรมการเฉพาะกิจเพื่อควบคุมการพัฒนาโดยเฉพาะ คณะกรรมการนี้ควรมีผู้บริหารสูงสุดของธนาคารเป็นประธาน โดยมีเจ้าหน้าที่ระดับรองลงมาช่วยด้วย การควบคุมงานของคณะทำงานต่าง ๆ ควรใช้คณะทำงานกลาง (central project team) เป็นแกนกลางรวบรวมและรายงานต่อคณะกรรมการตามรอบระยะเวลาที่กำหนด รวมทั้งจัดทำคู่มือต่าง ๆ ด้วย คณะทำงานของฝ่ายต่าง ๆ ควรคัดเลือกจากพนักงานภายในฝ่ายต่าง ๆ และควรกำหนดให้รายงานต่อคณะทำงานกลางอย่างสม่ำเสมอ

4. ขั้นตอนในการจัดทำแผน

การจัดทำแผนฉุกเฉิน เป็นการศึกษาและจัดทำแนวทางในการแก้ไขภัยพิบัติลักษณะต่าง ๆ ไว้ล่วงหน้า แล้วจัดทำเป็นคู่มืออธิบายวิธีการแก้ไขเหตุดังกล่าวไว้ การจัดทำคู่มือมีขั้นตอนที่สำคัญดังต่อไปนี้

4.1 ระบุประเภทของความเสี่ยงที่อาจเกิดขึ้น คณะทำงานกลางมีหน้าที่วิเคราะห์ และระบุประเภทความเสี่ยงหรือล่อแหลมต่อความเสียหายที่อาจเกิดขึ้น โดยผ่านความเห็นชอบจากคณะกรรมการ ซึ่งจะใช้เป็นเครื่องกำหนดขอบเขตของแผนฉุกเฉินในขั้นต่อไป

ในการวิเคราะห์ความเสี่ยง คณะทำงานกลางควรพิจารณาถึงสถานที่ตั้งและสภาพแวดล้อมทางภูมิศาสตร์ของธนาคารหรือสำนักงานสาขาต่าง ๆ ที่อยู่ในข่ายการจัดให้มีแผนฉุกเฉินด้วย เนื่องจากสถานที่หรือสภาพแวดล้อมทางภูมิศาสตร์ที่แตกต่างกัน จะก่อให้เกิดความเสี่ยงแตกต่างกันออกไป เช่น สาขานาคารที่อยู่ทางภาคใต้ของประเทศอาจมีปัญหาดูแลติดต่อกับสำนักงานใหญ่หรือสาขาอื่นทางโทรศัพท์ในฤดูฝน เนื่องจากภัยธรรมชาติ เป็นต้น นอกจากนี้ควรคำนึงถึงภัยที่เกิดจากการกระทำของคน เช่น การทุจริต การก่อวินาศกรรม หรือการลักขโมย ถิ่นเทข้อมูล เป็นต้น

4.2 เค้าโครงของคู่มือ หลังจากคณะทำงานกลางวิเคราะห์และระบุความเสี่ยงออกมาแล้ว ขั้นตอนต่อมาเป็นการจัดทำเค้าโครงของคู่มือ ซึ่งควรมีรายละเอียดเกี่ยวกับประเภทของความเสี่ยงหรือภัยพิบัติแต่ละประเภท เจ้าหน้าที่ผู้รับผิดชอบในการเผชิญปัญหาและแก้ไขเหตุร้ายนั้น ๆ กลยุทธ์ในการแก้ไขปัญหา ฯลฯ และแผนการฟื้นฟูทรัพย์สินหรือระบบคอมพิวเตอร์ให้กลับใช้งานได้โดยเร็วที่สุด ทั้งนี้ควรมีขั้นตอน ระยะเวลา ที่ชัดเจน

4.3 แผนฉุกเฉินแม่บท เป็นแผนปฏิบัติสำหรับพนักงานธนาคารทุกคน แผนนี้ควรระบุให้ทราบวิธีการเคลื่อนย้ายทรัพย์สินและบุคลากรจากที่เกิดเหตุ รวมทั้งวิธีการแจ้งให้ทราบว่ามีเหตุร้ายเกิดขึ้น การจัดทำแผนแม่บทนี้นอกจากรวบรวมข้อมูลภายในธนาคารแล้ว ยังต้องอาศัยการสำรวจข้อมูลประกอบจากภายนอกด้วย เช่น สถานีตำรวจท้องที่ กองดับเพลิง โรงพยาบาล บริษัทประกันภัย เครือข่ายสื่อสาร การไฟฟ้า การโทรศัพท์ เป็นต้น

4.4 แผนเฉพาะฝ่าย เป็นแผนที่มีรายละเอียดมากที่สุด คณะทำงานของแต่ละฝ่ายเป็นผู้รับผิดชอบจัดทำ โดยอยู่ภายใต้การกำกับของคณะกรรมการกลาง แผนสำหรับฝ่ายปฏิบัติการ (line) ต่าง ๆ เช่น ฝ่ายสินเชื่อ ฝ่ายการธนาคารในประเทศ หรือฝ่ายการธนาคารต่างประเทศ จะต้องศึกษาและวิเคราะห์กระบวนการปฏิบัติงานและ

วิธีการปฏิบัติทางบัญชี เพื่อนำมาจัดทำคู่มือโดยละเอียด โดยเฉพาะขั้นตอนการประมวลผลข้อมูลที่มีความสำคัญ เอกสารและบันทึกต่าง ๆ ที่เกี่ยวข้อง แผนเฉพาะฝ่ายควรวิเคราะห์และจัดลำดับความเสี่ยงในระดับที่สามารถยอมรับได้ และที่ต้องจัดทำมาตรการป้องกันไว้ล่วงหน้า การวิเคราะห์อาจอาศัยประสบการณ์หรือคำนวณมูลค่าความเสียหาย โดยใช้หลักความน่าจะเป็น โดยมีคณะทำงานกลางร่วมตัดสินใจ

4.5 การทบทวนและทดสอบแผน ขั้นตอนนี้มีจุดประสงค์เพื่อตัดขั้นตอนที่ไม่จำเป็นหรือไม่ก่อให้เกิดประโยชน์ในแผนออกไป และปรับปรุงให้แผนมีความเหมาะสมกับสภาวะการณ์ สามารถนำออกใช้ในเหตุการณ์ได้ทุกขณะ

การทบทวนอาจทำได้หลายวิธี เช่น วิธีแรกคือมอบหมายให้คณะทำงานกลางตรวจทานร่างแผนฉุกเฉิน โดยอาจแบ่งออกเป็นส่วนตัว ๆ ให้เจ้าหน้าที่แต่ละคนตรวจทานโดยละเอียด ทั้งนี้ควรวิเคราะห์ส่วนอื่น ๆ ของแผนร่วมกันไปพร้อมกับส่วนของแต่ละคนด้วย วิธีนี้มีจุดอ่อนบางประการ กล่าวคือ หากผู้วิเคราะห์ตั้งสมมติฐานผิดพลาด การวิเคราะห์จะผิดแนวทางที่ผู้จัดทำแผนกำหนดไว้ได้ นอกจากนั้นอาจมีแรงกดดันจากบางสิ่งบางอย่างให้มีการแก้ไขแผนจนบิดเบือนไปได้ด้วย

วิธีที่สองคือ ให้บุคคลที่สามซึ่งมิได้เกี่ยวข้องกับคณะทำงานพัฒนาแผนเป็นผู้ทบทวนวิเคราะห์ เช่น ผู้ตรวจสอบภายใน หรือบริษัทที่ปรึกษา ปัญหาในการให้ผู้ตรวจสอบภายในทำการทบทวน คือ ธนาครอาจไม่มีผู้ตรวจสอบที่มีคุณสมบัติเหมาะสมในการทำหน้าที่นี้ สำหรับการให้บริการของบริษัทที่ปรึกษา โดยทั่วไปจะมีข้อได้เปรียบกว่าวิธีแรกในด้านการให้คำแนะนำและความคิดเห็นที่เป็นประโยชน์ ทั้งนี้ขึ้นอยู่กับประสบการณ์และชื่อเสียงของบริษัท นอกจากนั้นข้อแนะนำที่ได้รับจะมีความเป็นกลางมากกว่าการใช้บุคลากรภายในธนาคร เนื่องจากบริษัทภายนอกปลอดจากแรงกดดันภายในองค์กรของธนาคร

การแก้ไขข้อบกพร่องของแผนอีกวิธีหนึ่งคือ การทดสอบ อย่างไรก็ตามธนาครต้องตระหนักว่ากระบวนการทดสอบไม่สามารถจำลองสถานการณ์จริงได้โดยครบถ้วน โดยเฉพาะในส่วนที่เกี่ยวกับองค์การภายนอก ทำให้จำเป็นต้องมีการสมมุติสถานการณ์บางอย่างประกอบด้วย เช่น การทดสอบการปฏิบัติงาน ณ ศูนย์คอมพิวเตอร์สำรองภายนอกธนาคร การสนับสนุนจากผู้ขาย หรือการเคลื่อนย้ายทรัพย์สินบางอย่าง เป็นต้น

แผนที่แก้ไขแล้วควรผ่านการพิจารณาอนุมัติโดยคณะทำงาน เช่นเดียวกับการจัดทำในครั้งแรก หลังจากนั้นควรมีการทดสอบอีกครั้งหนึ่งก่อนการประกาศให้ใช้

4.6 การฝึกอบรม การประกาศใช้แผน และการทดสอบอย่างต่อเนื่อง ขั้นตอนสุดท้ายในกระบวนการพัฒนาแผนฉุกเฉิน คือ การประกาศใช้แผน ซึ่งเป็นขั้นตอนที่มีความสำคัญที่สุด เนื่องจากการที่จะให้ผู้ที่เกี่ยวข้องกับเหตุการณ์และมีส่วนร่วมในการแก้ไขปัญหาตระหนักถึงความสำคัญของแผน และการฝึกอบรมในเรื่องที่มีโอกาสเกิดขึ้นได้น้อยนั้น เป็นงานที่ทำหายและมีความยากลำบากกว่างานอื่น เพื่อให้แผนฉุกเฉินได้รับการปรับปรุงให้สอดคล้องกับความเปลี่ยนแปลงต่าง ๆ และพนักงานเกิดความชำนาญในการปฏิบัติ ไม่สับสนในยามฉุกเฉิน ธนาครควรกำหนดให้มีการทดสอบและฝึกซ้อมแผนทุกปี อย่างน้อยปีละครั้ง เฉพาะจุดที่มีความล่อแหลมสูงควรทดสอบและฝึกซ้อมให้บ่อยครั้งกว่าปกติ

แผนฉุกเฉินทุกแผนจะสามารถนำมาใช้อย่างมีประสิทธิภาพได้ในเวลาหนึ่ง ทั้งนี้ขึ้นอยู่กับอัตราการเปลี่ยนแปลงของสิ่งต่าง ๆ ที่กระทบต่อแผน โดยทั่วไปแผนที่ได้รับการพัฒนา วิเคราะห์ แก้ไข และทดสอบอย่างต่อเนื่อง จะใช้ได้ประมาณ 5 ปี หลังจากนั้นธนาคารจำเป็นต้องอาศัยแผนที่พัฒนาขึ้นใหม่ทดแทนต่อไป



บทที่ 3

มาตรการและเหตุผลในการกำหนดให้
ธนาคารพาณิชย์จัดทำแผนฉุกเฉิน
และมีระบบคอมพิวเตอร์สำรอง

มาตรการและเหตุผลในการกำหนดให้ธนาคารพาณิชย์จัดทำแผนฉุกเฉิน และมีระบบคอมพิวเตอร์สำรอง

มาตรการที่กำหนด	เหตุผล
1. กำหนดให้ทุกธนาคารจัดทำแผนฉุกเฉิน และมีระบบคอมพิวเตอร์สำรองนอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักของธนาคารให้เสร็จสิ้นและใช้งานได้ในปี พ.ศ.2532 2. การหยุดให้บริการทุกประเภทของธนาคาร อันมีสาเหตุจากระบบคอมพิวเตอร์ขัดข้องหรือเสียหายจะหยุดเกิน 1 วันทำการไม่ได้เว้นแต่จะมีเหตุผลและความจำเป็นอื่นที่พิจารณาได้ว่าเป็นเหตุอันควรที่ต้องหยุดให้บริการเกินกว่าเวลาที่กำหนดไว้ข้างต้น	1. เพื่อให้ธนาคารพาณิชย์ทุกธนาคารมีระบบการป้องกันและแก้ไขเมื่อระบบคอมพิวเตอร์ของธนาคารล้มเหลว หรือขัดข้องหยุดการทำงานเนื่องจากภัยพิบัติต่าง ๆ มาตรการที่กำหนดนี้จะช่วยให้ธนาคารพาณิชย์สามารถให้บริการแก่ประชาชนได้อย่างต่อเนื่องโดยไม่หยุดชะงัก เสร็จสิ้นและใช้งานได้ในปี เป็นการป้องกันมิให้เกิดความเสียหายแก่ประชาชน และช่วยรักษาเสถียรภาพของระบบธนาคารพาณิชย์ การที่กำหนดระยะเวลาให้ทุกธนาคารดำเนินการให้แล้วเสร็จในปี พ.ศ.2532 เนื่องจากจำเป็นต้องให้เวลาแก่ธนาคารในการเตรียมจัดทำแผนฉุกเฉิน และศึกษาหาาระบบคอมพิวเตอร์สำรองที่เหมาะสม ตลอดจนต้องให้เวลาจัดหา ติดตั้ง และทดสอบการปฏิบัติงานของระบบคอมพิวเตอร์สำรองตามแผนฉุกเฉินด้วย 2. การกำหนดระยะเวลามีให้หยุดบริการเกินกว่า 1 วัน ซึ่งเป็นช่วงเวลาสั้น เพื่อเป็นการกระตุ้นให้ธนาคารพาณิชย์กระตือรือร้นในการเตรียมการต่าง ๆ ให้พร้อมตลอดเวลา และรีบเร่งแก้ไขปัญหาที่เกิดขึ้นกับการให้บริการประเภทที่สำคัญของธนาคาร โดยเฉพาะการฝากถอนและโอนเงิน เพื่อให้ประชาชน ผู้ฝากเงินและผู้ใช้บริการของธนาคารได้รับความเดือดร้อนและเสียหายจากการหยุดให้บริการเป็นเวลานานเกินไป มาตรการนี้จึงเป็นการกำหนดขึ้นเพื่อพิทักษ์รักษาประโยชน์ของประชาชนโดยตรง

มาตรการที่กำหนด	เหตุผล
3. กรณีที่ธนาคารไม่อาจดำเนินการให้มีแผนฉุกเฉินและระบบคอมพิวเตอร์สำรองด้วยตนเองได้ ให้ธนาคารเลือกวิธีปฏิบัติได้ คือ ก. ขอร่วมใช้บริการจากธนาคารอื่น หรือ มีข้อแลกเปลี่ยนหรือสัญญาข้อตกลงใช้บริการคอมพิวเตอร์สำรองร่วมกัน ข. ร่วมกับธนาคารพาณิชย์อื่นจัดตั้งเป็น กลุ่มหรือตั้งเป็นบริษัทกลาง หรือองค์กรอิสระเพื่อ ให้บริการคอมพิวเตอร์สำรองร่วมกัน ค. ใช้บริการจากบริษัทหรือเอกชนภายนอกธนาคารหรือองค์กรอื่นที่ให้บริการคอมพิวเตอร์ สำรองกับธนาคารได้	3. มาตรการนี้เป็นทางเลือกสำหรับธนาคาร-พาณิชย์ขนาดเล็ก ซึ่งไม่สามารถลงทุนจัดหาระบบคอมพิวเตอร์สำรองเป็นของตนเองได้ ธนาคารนั้นก็ยังต้องจัดทำแผนฉุกเฉินเช่นเดียวกัน ส่วนการจัดหาระบบคอมพิวเตอร์สำรองนั้น ธนาคารอาจเลือกปฏิบัติตามที่มาตรการนี้กำหนดได้ตามข้อ ก.-ค. ได้ ในกรณีนี้จะนำมาตรการเกี่ยวกับเรื่องเวลาที่กำหนดในข้อ 1 และข้อ 2 มาใช้บังคับด้วย กล่าวคือ ธนาคารจะต้องดำเนินการให้แล้วเสร็จในปี พ.ศ.2532 และเมื่อระบบคอมพิวเตอร์เกิดปัญหาขึ้น ธนาคารจะหยุดให้บริการเกินกว่า 1 วันทำการไม่ได้เช่นกัน

แผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan)

วัตถุประสงค์

เพื่อป้องกัน ลดความเสี่ยงภัย และความเสียหายจากภัยพิบัติอันใดก็ตามที่ทำให้การปฏิบัติงานคอมพิวเตอร์ของธนาคารต้องหยุดชะงัก ในกรณีที่มียาอาจหลีกเลี่ยงได้ ก็พร้อมที่จะปฏิบัติงานทดแทนและแก้ไขเหตุการณ์ให้กลับคืนสู่สภาพปกติโดยเร็วที่สุด

เหตุผลและความจำเป็น

ธนาคารพาณิชย์ได้เริ่มนำระบบงานคอมพิวเตอร์มาใช้สนับสนุนการดำเนินงานและการให้บริการกับลูกค้าและประชาชนที่เกี่ยวข้องอย่างกว้างขวาง ขอบเขตและปริมาณการใช้งานเพิ่มมากขึ้นเป็นลำดับ ข้อมูลการเงินและระบบงานที่สำคัญต่าง ๆ ของธนาคารถูกประมวลผลด้วยระบบงานคอมพิวเตอร์ และมีการขยายขอบเขตงานเชื่อมโยงกับต่างประเทศทั่วโลก ซึ่งทำให้การปฏิบัติงานสะดวก รวดเร็ว ลดขั้นตอนที่ไม่จำเป็นให้มีประสิทธิภาพ อีกทั้งช่วยเสริมสร้างภาพพจน์ที่ทันสมัย และเป็นการสร้างให้เกิดบริการใหม่อีกด้วย

ระบบงานคอมพิวเตอร์จึงกลายเป็นสิ่งจำเป็น และมีบทบาทสำคัญในการดำเนินงานของธนาคารพาณิชย์มากขึ้น นอกจากระบบงานคอมพิวเตอร์จะอำนวยความสะดวกและให้ความสะดวกในการปฏิบัติงานอย่างมากมาแล้ว ยังอาจก่อให้เกิดปัญหาและความเสี่ยงภัยในรูปแบบใหม่ ๆ ติดตามมาด้วย เช่น อาชญากรรมทางคอมพิวเตอร์ และความเสียหาย อันเนื่องจากระบบงานคอมพิวเตอร์หยุดชะงัก ถึงแม้จะเป็นเพียงช่วงระยะเวลาอันสั้น ก็อาจก่อให้เกิดความเสียหาย และผลกระทบต่าง ๆ เช่น เกิดความล่าช้าในการปฏิบัติงาน ไม่สามารถให้บริการแก่ลูกค้า ค่าใช้จ่ายเพิ่มขึ้น สูญเสียรายได้ ประชาชนและผู้ถือหุ้นขาดความไว้วางใจ ซึ่งอาจมีความรุนแรงจนมีผลให้การดำเนินงานของธนาคารต้องหยุดชะงัก และไม่สามารถดำเนินงานต่อไปอีกได้ ซึ่งจะกระทบฐานะและความมั่นคงของธนาคารพาณิชย์และลูกค้าประชาชนที่เกี่ยวข้อง ตลอดจนระบบเศรษฐกิจของประเทศได้ในที่สุด

ดังนั้น ธนาคารพาณิชย์จึงควรตระหนักถึงภัยพิบัติต่าง ๆ อันเนื่องมาจากภัยธรรมชาติ อุบัติเหตุ ภัยที่เกิดจากเจตนาและไม่มีเจตนากระทำของบุคคล หรือภัยใด ๆ ก็ตามที่จะเกิดขึ้นกับการดำเนินงานด้านคอมพิวเตอร์ เพื่อจัดทำและสร้างมาตรการป้องกันภัยนั้น ๆ และลดความเสี่ยงภัยที่นำความเสียหายหรือผลกระทบที่อาจเกิดขึ้น ดังกล่าวซึ่งสามารถจัดทำได้หลายวิธี วิธีที่เป็นที่นิยมจัดทำและเป็นที่ยอมรับแล้วในต่างประเทศ ได้แก่ การจัดสร้างแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan) แผนดังกล่าวนี้พัฒนาสืบเนื่องมาจากระบบการควบคุมภายในและรักษาความปลอดภัยทางกายภาพของธนาคารพาณิชย์ โดยมีวัตถุประสงค์เพื่อสนับสนุนการดำเนินงานของธนาคารให้เป็นไปอย่างต่อเนื่องโดยไม่หยุดชะงัก แม้ว่าจะเกิดภัยอันตรายใด ๆ ต่อศูนย์และการประมวลผลงานคอมพิวเตอร์ก็ตาม

ทั้งนี้ แผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉินจะมีประสิทธิภาพต้องเริ่มจากผู้บริหารยอมรับและตระหนักถึงความสำคัญดังกล่าว โดยกำหนดเป็นนโยบายให้มีแผนดังกล่าวและถือปฏิบัติอย่างเคร่งครัด รวมทั้งควบคุมติดตามการพัฒนาจัดทำ ซึ่งอาจพัฒนาขึ้นเอง หรือใช้บริการจากบุคคลภายนอกที่มีความชำนาญพิเศษ แต่ทั้งนี้ต้องแน่ใจว่าวัตถุประสงค์และขอบเขตของแผนครอบคลุมถึงการป้องกันรักษาความปลอดภัยเพื่อลดความเสี่ยงภัย และระงับภัยที่อาจเกิดขึ้น พร้อมทั้งการเตรียมพร้อมที่จะปฏิบัติงานในภาวะฉุกเฉินเมื่อประสบภัย รวมทั้งการปฏิบัติงานปรับปรุงแก้ไขเหตุฉุกเฉิน และการกำหนดวิธีการปฏิบัติสำรองทดแทนการหยุดทำงานของระบบงานคอมพิวเตอร์ ณ สถานที่ปฏิบัติงานสำรองนอกสถานที่ เพื่อให้ธนาคารพาณิชย์สามารถดำเนินการและให้บริการได้อย่างต่อเนื่อง โดยมีต้นทุนค่าใช้จ่ายในการจัดทำที่เหมาะสม ไม่กระทบต่อฐานะความมั่นคงและความสามารถในการดำเนินงานของธนาคารพาณิชย์เป็นสำคัญ

แนวทางการจัดทำแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan)

ขั้นตอนและวิธีการจัดทำ Contingency Plan อาจพิจารณาแบ่งได้เป็น 4 ขั้นตอน ดังนี้

1. การกำหนดสิ่งจำเป็นในการพัฒนาแผน
2. การพัฒนาจัดทำแผน
3. การแปลงระบบและนำแผนออกใช้งาน
4. การบำรุงรักษาและปรับปรุงแผน

1. การกำหนดสิ่งจำเป็นในการพัฒนาแผน

1.1 คณะทำงาน

จัดตั้งคณะทำงานพร้อมทั้งระบุอำนาจหน้าที่ความรับผิดชอบ ควรประกอบด้วยเจ้าหน้าที่จากส่วนงานคอมพิวเตอร์ และผู้ใช้ระบบงาน (users) ที่มีความรู้ความชำนาญในการประมวลผลข้อมูลด้วยคอมพิวเตอร์

1.2 งบประมาณ

จัดทำงบประมาณในการพัฒนาจัดทำแผน

2. การพัฒนาจัดทำแผน

การพัฒนาจัดทำแผนควรมีขั้นตอนตามลำดับ ดังนี้

2.1 ดำรวจข้อมูลเกี่ยวกับระบบงานคอมพิวเตอร์ชุดปัจจุบัน

วัตถุประสงค์

เพื่อทราบสถานะการปฏิบัติงานชุดที่ใช้ในการประมวลผลงานปกติ และลำดับความสำคัญของระบบงานคอมพิวเตอร์ต่าง ๆ ขั้นตอนการปฏิบัติการ และสภาพแวดล้อมโดยทั่วไป ซึ่งอาจจัดทำได้โดยใช้แบบสำรวจข้อมูลดังต่อไปนี้

- (1) ขั้นตอนและวิธีการปฏิบัติงาน
- (2) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ
- (3) โปรแกรมควบคุมระบบงาน
- (4) ระบบงาน โปรแกรม รวมทั้งระบบงานสำคัญที่กำลังพัฒนาอยู่
- (5) ระบบสื่อสารข้อมูล
- (6) อุปกรณ์อำนวยความสะดวก
- (7) วัสดุอุปกรณ์
- (8) บุคลากร เจ้าหน้าที่รับผิดชอบ รวมทั้งผู้ใช้ระบบงาน
- (9) ปริมาณงานที่ใช้ประมวลผล

2.2 ดำรวจข้อมูลเกี่ยวกับระบบคอมพิวเตอร์สำรอง (Back up) ชุดปัจจุบัน

วัตถุประสงค์

เพื่อประเมินความเหมาะสมเพียงพอของระบบคอมพิวเตอร์สำรองชุดที่ใช้ปฏิบัติงานปัจจุบัน โดยอาจใช้แบบ

สำรวจข้อมูล

- (1) ขั้นตอนและวิธีการปฏิบัติงานสำรอง รวมทั้งการจัดทำข้อมูลชุดสำรอง
- (2) ระยะเวลาและความถี่ในการจัดทำข้อมูลชุดสำรอง
- (3) สถานที่ปฏิบัติงานสำรอง และสถานที่จัดเก็บข้อมูลชุดสำรอง
- (4) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบชุดสำรอง
- (5) โปรแกรมควบคุมระบบงานสำรอง
- (6) ระบบงานและโปรแกรมชุดสำรอง
- (7) อุปกรณ์อำนวยความสะดวกชุดใช้งานในการปฏิบัติงานสำรอง
- (8) วัสดุอุปกรณ์สำรอง
- (9) เอกสารประกอบระบบงานสำรอง
- (10) บุคลากร เจ้าหน้าที่รับผิดชอบในการปฏิบัติงานสำรอง
- (11) การคมนาคมขนส่งสู่สถานที่ปฏิบัติงานสำรอง

2.3 การวิเคราะห์ความเสี่ยงภัย (Risk Analysis)

วัตถุประสงค์

เพื่อให้ทราบว่าการประมวลผลงานและระบบงานคอมพิวเตอร์มีบริเวณหรือจุดเสี่ยงภัยและโอกาสที่จะเกิดภัย
มากน้อยเพียงใด และเพื่อจัดสร้างมาตรการป้องกันและระงับภัยดังกล่าว

แนวทางการจัดทำ

(1) การวิเคราะห์ภัย (Threat)

การวิเคราะห์ภัย (Threat) รวมถึงข้อผิดพลาดต่าง ๆ อันอาจเกิดขึ้นได้ในระบบงานคอมพิวเตอร์ ซึ่งอาจจำแนกได้เป็น 4 ประเภท ดังนี้

- (1.1) ภัยธรรมชาติ เช่น น้ำท่วม ไฟป่า พายุ
- (1.2) ภัยอันเกิดจากไม่มีเจตนากระทำหรืออุบัติเหตุ เช่น อัคคีภัย กระแสไฟฟ้าดับหรือขัดข้อง
- (1.3) ภัยอันเกิดจากเจตนากระทำการหรืออาชญากรรมทางคอมพิวเตอร์ เช่น การขโมยและการเปิดเผยข้อมูล การเปลี่ยนแปลงข้อมูล การก่อการร้าย
- (1.4) ภัยอันเกิดจากความเสียหายหรือความล้มเหลวของอุปกรณ์คอมพิวเตอร์ ระบบ การสื่อสาร ข้อมูล อุปกรณ์อำนวยความสะดวก ข้อผิดพลาดของโปรแกรม และพนักงาน

(2) การวิเคราะห์อัตราความเสี่ยงภัย

วิเคราะห์ว่าในแต่ละระบบงานมีโอกาสเกิดภัยต่าง ๆ ที่สำรวจไว้ ณ จุดใดมากน้อยเพียงไร โดยพิจารณาจากองค์ประกอบต่าง ๆ เช่น ขั้นตอนและวิธีการปฏิบัติงาน สภาพแวดล้อมในการปฏิบัติงาน อุปกรณ์คอมพิวเตอร์และอุปกรณ์ประกอบ เครื่องอำนวยความสะดวก มาตราการควบคุมภายในและป้องกันภัยที่ใช้บังคับอยู่ในปัจจุบัน เจ้าหน้าที่ปฏิบัติงานและผู้ที่เกี่ยวข้อง ซึ่งอาจพิจารณาจุดเสี่ยงภัยในขั้นตอนการปฏิบัติงานต่าง ๆ เช่น

- (2.1) การจัดสร้างข้อมูลขั้นต้น
- (2.2) การนำข้อมูลเข้าสู่ระบบ
- (2.3) การสื่อสารข้อมูล
- (2.4) การประมวลผลข้อมูล
- (2.5) การจัดส่งข้อมูลผลลัพธ์
- (2.6) การเก็บรักษาข้อมูล
- (2.7) การทำลายข้อมูลที่เลิกใช้งาน

2.4 กำหนดและลำดับความสำคัญของระบบงาน

วัตถุประสงค์

เพื่อให้ทราบลำดับความสำคัญของระบบงานคอมพิวเตอร์ของธนาคาร และประเมินค่าความเสียหายความล่าช้าในการประมวลผลงาน ผลกระทบอันเกิดจากภัยพิบัติ และจัดสร้างระบบงานสำรองที่เหมาะสม

จากข้อมูลที่รวบรวมมาแล้วข้างต้น นำมาประกอบในการพิจารณาลำดับความสำคัญของระบบงานโดยคำนึงถึงความถี่และเวลาที่ใช้ในการประมวลผล อุปกรณ์คอมพิวเตอร์โปรแกรมระบบงาน ความซับซ้อนของการประมวลผล รวมทั้งจำนวนเงินของความเสียหาย ผลกระทบในการดำเนินงาน ค่าใช้จ่ายเพิ่มเติม การสูญเสียรายได้ ผลกระทบทางกฎหมาย ตลอดจนการขาดความเชื่อถือจากลูกค้า และการเสียชื่อเสียง โดยอาจจัดทำแบบสำรวจข้อมูล

2.5 กำหนดระยะเวลาที่แต่ละระบบงานสามารถหยุดให้บริการ อันมีสาเหตุจากระบบคอมพิวเตอร์ขัดข้องหรือเสียหาย

วัตถุประสงค์

เพื่อให้ทราบระยะเวลาที่แต่ละระบบงานสามารถหยุดให้บริการ และจัดสร้างมาตรการปรับปรุงแก้ไข เหตุฉุกเฉินให้สามารถปฏิบัติงานได้ทันเวลา รวมทั้งจัดการปฏิบัติงานทดแทนระบบงานที่หยุดชะงัก เพื่อบรรเทา ความเสียหายที่อาจเกิดขึ้นให้มากที่สุด

ระยะเวลาที่ต้องสามารถแก้ไขเหตุฉุกเฉินนี้ สามารถพิจารณาพร้อมกับลำดับความสำคัญของระบบงาน โดยปกติระบบงานที่มีความสำคัญจะมีความเสียหายเกิดขึ้นสูง ฉะนั้นจึงจำเป็นต้องแก้ไขเหตุการณ์ให้สามารถปฏิบัติงาน ทดแทนได้โดยเร็วที่สุด

2.6 กำหนดรูปแบบและวิธีการปฏิบัติงานคอมพิวเตอร์สำรอง

เมื่อทราบลำดับความสำคัญของระบบงานและระยะเวลาที่แต่ละระบบงาน สามารถหยุดให้บริการ อันเนื่องมาจากระบบคอมพิวเตอร์ขัดข้องหรือเสียหาย นำมาเป็นองค์ประกอบในการพิจารณา กำหนดรูปแบบและวิธีการ ปฏิบัติงานคอมพิวเตอร์สำรอง

(1) รูปแบบการปฏิบัติงานสำรองอาจจัดทำได้หลายรูปแบบ ดังนี้

(1.1) ใช้บริการ Service Bureaus

ใช้บริการจากสำนักงานที่รับประมวลผลงานคอมพิวเตอร์ให้แก่ผู้อื่น โดยคิดค่าบริการ และจัดทำสัญญาตกลงไว้ล่วงหน้า

(1.2) ใช้บริการ Contingency Center หรือ Hot Sites

ใช้บริการจากสำนักงานที่รับประมวลระบบงานคอมพิวเตอร์สำรองเมื่อเกิดเหตุฉุกเฉินโดย เฉพาะ

(1.3) Empty Shells หรือ Cold Sites

จัดหรือสร้างสถานที่ไว้สำหรับปฏิบัติงานสำรอง ซึ่งอาจตกแต่งภายในไว้เรียบร้อยแล้ว แต่ ไม่มีอุปกรณ์คอมพิวเตอร์ ซึ่งจะนำมาติดตั้งเมื่อเกิดเหตุฉุกเฉินหรือปฏิบัติงานสำรอง

(1.4) Time Brokers

ใช้บริการจากสำนักงานหรือบริษัทที่ทำหน้าที่เป็นนายหน้ารับจัดหาเวลาประมวลผลงาน คอมพิวเตอร์ (Processing time) ณ ศูนย์คอมพิวเตอร์ของผู้อื่นที่มีประสิทธิภาพทัดเทียมกันเมื่อเกิดเหตุฉุกเฉิน

(1.5) Membership in Shared Contingencies Facilities

องค์การหรือสถาบันหลายแห่งร่วมกันลงทุนและบริหารงาน เพื่อปฏิบัติงานสำรองสำหรับ สมาชิกในกรณีฉุกเฉิน

(1.6) Redundant Facilities

ระบบงานคอมพิวเตอร์สำรองที่จะจัดสร้างขึ้นเหมือนกับระบบงานจริง

(1.7) Reciprocal Agreement

การทำสัญญาระหว่างองค์การหรือสถาบันตั้งแต่ 2 องค์การขึ้นไป เพื่อตกลงยินยอมใช้ อุปกรณ์คอมพิวเตอร์ของกันและกัน ในกรณีผู้หนึ่งผู้ใดประสบภัย

(1.8) Manual Processing

การปฏิบัติงานสำรองด้วยมือ

(2) วิธีการปฏิบัติงานคอมพิวเตอร์สำรอง

(2.1) การประมวลผลงานแบบ Batch

(2.2) การประมวลผลงานแบบ On-line

(2.3) การประมวลผลงานด้วยมือ

(3) องค์ประกอบการพิจารณากำหนดรูปแบบและวิธีการในการปฏิบัติงานคอมพิวเตอร์สำรอง

การพิจารณากำหนดรูปแบบในการปฏิบัติงานสำรองควรคำนึงถึง

(3.1) **ขีดความสามารถของระบบคอมพิวเตอร์เท่าเทียมกัน (Compatibility)** โดยเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบสามารถทำงานทดแทนได้ โดยไม่ต้องดัดแปลงแก้ไขโปรแกรม หรือการทำงานได้ถูกต้องเหมือนเดิม ซึ่งอาจพิจารณาจากองค์ประกอบดังนี้

(3.1.1) ส่วนประกอบเครื่องคอมพิวเตอร์ (Hardware Configuration)

(3.1.2) อุปกรณ์ประกอบ (Peripherals)

(3.1.3) หน่วยความจำหลัก (Core Memory)

(3.1.4) หน่วยความจำสำรองทั้งหมด (Mass Storage)

(3.1.5) รุ่นและการนำออกใช้งานของโปรแกรมควบคุมระบบงาน (Software version and release)

(3.1.6) อุปกรณ์และโปรแกรมระบบสื่อสารข้อมูล (Communications hardware and software)

(3.1.7) วัสดุอุปกรณ์และเอกสาร

(3.1.8) มาตรการรักษาความปลอดภัยของระบบงานและโปรแกรม (Application Controls)

(3.1.9) มาตรการรักษาความปลอดภัยทางกายภาพ

(3.2) **ความพร้อมในการปฏิบัติงาน (Reliability)** หมายถึง ความพร้อมในการปฏิบัติงานในเวลาที่ต้องการ และมีช่วงระยะเวลาประมวลผลเพียงพอสำหรับประมวลผลงานสำรองดังกล่าว

(3.3) **ความสามารถของระบบงาน (Capacity)** หมายถึง ความสามารถของระบบงานในการประมวลผลงานที่มีปริมาณรายการเพิ่มขึ้นมากกว่าภาวะปกติ

(3.4) **ระยะเวลาเตรียมพร้อมในการปฏิบัติงานสำรอง (Preparation time)** ควรคำนึงถึง

(3.4.1) เวลาเปิดหรือจัดสร้างระบบงานให้พร้อมที่จะปฏิบัติงาน (Regenerate system) เช่น การ Boot ระบบงาน

(3.4.2) เวลาที่ใช้ในการบรรจุข้อมูลลงแฟ้มข้อมูล (Reload Data Base Files)

(3.4.3) เวลาที่ใช้ในการแปลโปรแกรมภาษาระดับสูงให้เป็นโปรแกรมภาษาเครื่อง (Recompile Programs)

(3.4.4) เวลาที่ใช้ในการแปลงข้อมูลเพื่อนำเข้าสู่ระบบ (Convert input)

(3.4.5) เวลาที่ใช้จัดสร้างระบบสื่อสารข้อมูล

(3.4.6) เวลาทดสอบระบบงานก่อนใช้งาน

(3.4.7) เวลาสั่งซื้อ จัดส่ง อุปกรณ์และวัสดุที่ต้องใช้ในการปฏิบัติงานสำรอง ข้อตกลงกับร้านค้า

(3.5) **ต้นทุน** ต้นทุนในการจัดสร้างระบบคอมพิวเตอร์สำรอง และค่าใช้จ่ายในการปฏิบัติงานสำรอง

2.7 กำหนดสิ่งจำเป็นในการจัดสร้างแผน

(1) สถานที่ปฏิบัติงานสำรอง

การพิจารณากำหนดสถานที่ปฏิบัติงานสำรอง ควรคำนึงถึงองค์ประกอบขั้นต่ำ ดังนี้

(1.1) สภาพแวดล้อมบริเวณที่ตั้ง

(1.1.1) สถานที่ตั้งห่างจากศูนย์ปฏิบัติงานเดิมโดยไม่ได้รับผลกระทบจากภัยพิบัติเดียวกัน

(1.1.2) การคมนาคมสะดวก

(1.1.3) ตั้งอยู่ในชุมชนที่มีบริการสาธารณูปโภคเพียงพอ เช่น ไฟฟ้า ประปา โทรศัพท์ การสื่อสาร สถานีดับเพลิง สถานีตำรวจ

(1.2) ลักษณะการก่อสร้างของอาคาร

(1.2.1) อาคาร พื้น และผนัง มีความแข็งแรงเพียงพอเพื่อรองรับน้ำหนักของอุปกรณ์ต่าง ๆ

- (1.2.2) เพดานของแต่ละชั้นอาคารมีความสูงเพียงพอให้อากาศถ่ายเทความร้อนจากเครื่องคอมพิวเตอร์และอุปกรณ์
- (1.2.3) ทางเข้าออกของอาคารมีความกว้างเพียงพอที่จะเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์และวัสดุต่าง ๆ ได้สะดวก

(1.3) ลักษณะภายในบริเวณที่ตั้งศูนย์คอมพิวเตอร์

- (1.3.1) ตั้งอยู่ในชั้นที่ไม่สูงเกินไป ในกรณีที่เกิดภัยสามารถเคลื่อนย้ายได้สะดวก หรือไม่ตั้งอยู่ในชั้นที่ต่ำเกินไป เพื่อป้องกันผู้บุกรุก หรือหลีกเลี่ยงภัยธรรมชาติ เช่น น้ำท่วม เป็นต้น
- (1.3.2) ทางเข้าออกศูนย์ตั้งอยู่ในตำแหน่งที่เหมาะสม และมีการรักษาความปลอดภัยเพียงพอ เพื่อป้องกันผู้บุกรุกรวมทั้งมีบริเวณกว้างเพียงพอที่จะเคลื่อนย้ายอุปกรณ์ต่าง ๆ
- (1.3.3) ลักษณะการดำเนินงานหรือธุรกิจของผู้ที่อยู่ในบริเวณรอบ ๆ ศูนย์ไม่ก่อให้เกิดความเสี่ยงภัยต่าง ๆ เพิ่มขึ้น เช่น ผู้เช่าอาคารใช้ชั้นเดียวกับศูนย์ทำธุรกิจขายน้ำยาเคมีซึ่งเป็นวัสดุไวไฟ เป็นต้น
- (1.3.4) บริเวณที่ตั้งอุปกรณ์อำนวยความสะดวกตั้งอยู่ในตำแหน่งหลีกเลี่ยงเพดานห้องคอมพิวเตอร์ เพื่อป้องกันความเสี่ยงภัยอันเกิดจากน้ำ หรือน้ำยาเคมีรั่วลงบนเครื่องคอมพิวเตอร์และอุปกรณ์
- (1.3.5) สถานที่เก็บอุปกรณ์เคมีและวัสดุไวไฟตั้งอยู่ห่างไกลจากศูนย์ เพื่อป้องกันความเสี่ยงจากอัคคีภัย

(1.4) การรักษาความปลอดภัยและการบำรุงรักษาสถานที่

- (1.4.1) การรักษาความปลอดภัยบริเวณอาคารและศูนย์คอมพิวเตอร์เพียงพอและเหมาะสม
- (1.4.2) การดูแลรักษาความสะอาดอาคารและศูนย์คอมพิวเตอร์เพียงพอและเหมาะสม
- (1.4.3) มีมาตรการตรวจจับและป้องกันไฟ ความชื้น ความร้อน และผู้บุกรุก

(2) อุปกรณ์ที่จำเป็นต้องใช้ในการปฏิบัติงานสำรอง

นำข้อมูลเกี่ยวกับรายละเอียดลำดับความสำคัญของระบบงานและสิ่งจำเป็นต้องใช้ในการปฏิบัติงานในสภาวะปกติที่รวบรวมไว้แล้วดังกล่าวข้างต้นมาวิเคราะห์เพิ่มเติมให้สมบูรณ์ รวมทั้งข้อมูลเกี่ยวกับการประมวลผลงานที่เกี่ยวข้องหรือการให้บริการแก่สถาบันอื่น เช่น ระบบงาน ATM, POS เป็นต้น และกำหนดสิ่งจำเป็นต้องใช้ในการปฏิบัติงานสำรอง ซึ่งอาจประกอบด้วย

- (2.1) คอมพิวเตอร์ อุปกรณ์ประกอบ ไมโครคอมพิวเตอร์ และอุปกรณ์พิเศษอื่น ๆ
- (2.2) โปรแกรมควบคุมระบบงาน โปรแกรมระบบงาน และโปรแกรมพิเศษ เช่น Encryption

- (2.3) เพิ่มข้อมูล
- (2.4) ระบบการสื่อสารข้อมูลและสายสื่อสาร
- (2.5) เอกสารประกอบระบบงาน
- (2.6) วัสดุอุปกรณ์
- (2.7) เครื่องอุปกรณ์อำนวยความสะดวก
- (2.8) การคมนาคมไปยังสถานที่ปฏิบัติงานสำรองเมื่อเกิดเหตุฉุกเฉิน

(3) เจ้าหน้าที่ปฏิบัติงานสำรอง

กำหนดคณะเจ้าหน้าที่ปฏิบัติงานสำรอง พร้อมทั้งระบุหน้าที่ความรับผิดชอบให้เหมาะสมกับความสามารถ และสอดคล้องกับหน้าที่ที่รับผิดชอบในภาวะปกติเป็นลายลักษณ์อักษร เพื่อให้เจ้าหน้าที่ปฏิบัติงานด้วยความชำนาญ ถูกต้อง และรวดเร็ว จำนวนเจ้าหน้าที่ปฏิบัติงานสำรองขึ้นอยู่กับขนาดของธนาคาร และขั้นตอนวิธีการปฏิบัติงาน คณะเจ้าหน้าที่อาจประกอบด้วยบุคคลจากหน่วยงานต่าง ๆ ดังนี้

- ผู้บริหาร
- เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์
- เจ้าหน้าที่พัฒนาระบบงาน
- เจ้าหน้าที่วิเคราะห์ระบบงาน
- เจ้าหน้าที่แปลรหัส
- เจ้าหน้าที่จากบริษัทผู้ขายเครื่องอุปกรณ์คอมพิวเตอร์
- ผู้ตรวจสอบภายใน
- ผู้ใช้ระบบงาน
- เจ้าหน้าที่รักษาความปลอดภัย เป็นต้น

2.8 ขอบเขตของแผน

ขอบเขตของแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan) ควรครอบคลุมถึงมาตรการต่าง ๆ ดังนี้คือ

(1) มาตรการป้องกันและรักษาความปลอดภัย

วัตถุประสงค์

เพื่อป้องกันและลดความเสียหายที่นำความเสียหาย หรือผลกระทบที่อาจมีผลให้การดำเนินงานและการให้บริการลูกค้าด้วยคอมพิวเตอร์หยุดชะงัก ให้มีโอกาสดำเนินการขึ้นน้อยที่สุด มาตรการดังกล่าวจึงมีลักษณะเป็นเอกเทศที่มีนัยสำคัญเกี่ยวข้องกับการดำเนินงานด้านคอมพิวเตอร์ และเป็นส่วนหนึ่งของมาตรการป้องกันและรักษาความปลอดภัยของธนาคารหรือองค์กร จึงต้องประกาศให้ถือปฏิบัติโดยเคร่งครัด

แนวทางการจัดสร้าง

- (1.1) พิจารณาผลการวิเคราะห์อัตราความเสี่ยงภัย (Risk Analysis) จะทราบว่าในการปฏิบัติงานคอมพิวเตอร์และระบบงานมีโอกาสเกิดภัย ณ บริเวณใด มากหรือน้อยเพียงใดแล้วนั้น และประเมินความเพียงพอของมาตรการป้องกันรักษาความปลอดภัยและระเบียบการควบคุมภายในที่ถือปฏิบัติอยู่ในปัจจุบันที่ป้องกัน และลดความเสี่ยงภัยดังกล่าว
- (1.2) ปรับปรุงแก้ไขหรือเพิ่มเติมมาตรการรักษาความปลอดภัยและการควบคุมภายใน ให้รัดกุม
- (1.3) ประกาศและให้ถือปฏิบัติตามมาตรการหรือระเบียบการรักษาความปลอดภัยเป็นลายลักษณ์อักษร
- (1.4) จัดทำการประกันภัยด้านคอมพิวเตอร์ เพื่อลดภาระความเสี่ยงภัยหรือความเสียหายต่าง ๆ

(2) มาตรการเตรียมพร้อมและแก้ไขเหตุฉุกเฉิน

วัตถุประสงค์

เพื่อเตรียมพร้อมที่จะแก้ไขสถานการณ์ ระวังภัยพิบัติที่มีอาจหลีกเลี่ยงได้ให้ทันเวลา และดำเนินการแก้ไขการปฏิบัติงานคอมพิวเตอร์ที่ประสบภัยให้กลับคืนสู่สภาวะปกติภายในเวลาที่เร็วที่สุด รวมทั้งกำหนดวิธีปฏิบัติงานสำรองทดแทนระบบงานคอมพิวเตอร์ที่หยุดชะงักให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง ซึ่งประกอบด้วยแผนย่อยดังนี้

- (2.1) แผนปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน (Emergency Plan)
- (2.2) แผนปรับปรุงแก้ไขระบบงานคอมพิวเตอร์ (Recovery Plan)
- (2.3) แผนปฏิบัติงานของระบบคอมพิวเตอร์สำรอง (Back up Plan)

(2.1) แผนปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน (Emergency Plan)

หมายถึง แผนที่ใช้เป็นแนวทางในการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉินหรือภัยพิบัติที่มีอาจหลีกเลี่ยงได้ เพื่อป้องกันและบรรเทาความเสียหายให้เหลือน้อยที่สุด

(2.1.1) วิธีการปฏิบัติเมื่อได้รับสัญญาณเตือนภัย พนักงานควรได้รับการอบรมให้รู้จักวิธีปฏิบัติ และสัญญาณเตือนภัยทุกประเภท เช่น สัญญาณเตือนไฟ ไฟดับ น้ำท่วม สัญญาณกันขโมยหรือผู้บุกรุก ข้อผิดพลาดโปรแกรมและระบบงานต่าง ๆ สัญญาณเตือนความล้มเหลวของอุปกรณ์ เป็นต้น รวมทั้งวิธีการใช้สัญญาณดังกล่าว

(2.1.2) ขั้นตอนปฏิบัติขั้นต้นเมื่อรับทราบแน่ชัดว่าเกิดภัยพิบัติต่าง ๆ เช่น

(2.1.2.1) การรักษาความปลอดภัยและการปฐมพยาบาลแก่เจ้าหน้าที่

(2.1.2.2) การแจ้งเหตุฉุกเฉิน (Notification System) กำหนดขั้นตอนและวิธีการแจ้งเหตุฉุกเฉินแก่เจ้าหน้าที่ปฏิบัติงาน ผู้บริหาร และผู้ที่เกี่ยวข้องตามลำดับ ควรประกอบด้วย รายชื่อเจ้าหน้าที่ สถานที่ทำงาน หมายเลขโทรศัพท์บ้านพักและหมายเลขโทรศัพท์หรือสถานที่ที่ติดต่อได้ รวมทั้งระบุรายชื่อผู้ที่ปฏิบัติงานแทนหากมีอาจติดต่อได้ พร้อมทั้งจัดมอบสำเนารายชื่อดังกล่าวให้กับพนักงานผู้ที่มีส่วนเกี่ยวข้องกับหน้าที่รับผิดชอบนั้นและรายชื่อพนักงานนี้เป็นเอกสารประกอบของแผนฉุกเฉิน

(2.1.2.3) ระวังภัยขั้นต้นแล้วแต่กรณี

(2.1.2.4) ป้องกันและรักษาเครื่องมืออุปกรณ์ระบบงาน เพิ่มข้อมูล โดยพยายามปิดระบบงานตามลำดับขั้นตอนที่เหมาะสม เก็บรักษาเคลื่อนย้ายเพิ่มข้อมูลที่สำคัญ และเอกสารประกอบระบบงานต่าง ๆ ปิดคลุมอุปกรณ์ต่าง ๆ

(2.2) แผนปรับปรุงแก้ไขระบบงานคอมพิวเตอร์ (Recovery Plan)

หมายถึง แผนปฏิบัติงานที่ใช้เป็นแนวทางในการแก้ไขระบบงานคอมพิวเตอร์ที่ประสบภัยให้กลับคืนสู่สภาพปกติโดยเร็วที่สุดอาจจัดทำตามขั้นตอนต่อไปนี้

(2.2.1) ประเมินความเสียหายและผลกระทบ โดยพิจารณาต้นเหตุที่ทำให้เกิดภัยและความเสียหายที่เกิดขึ้น และดำเนินการแก้ไขตามขั้นตอน และวิธีการที่กำหนดไว้ ซึ่งอาจแบ่งได้เป็นกรณี ต่าง ๆ ตัวอย่างเช่น

- ความเสียหายเล็กน้อย ระยะเวลาที่ระบบงานคอมพิวเตอร์หยุดชะงัก และสามารถแก้ไขได้ภายใน 2 ชั่วโมง
- ความเสียหายปานกลาง ระบบงานหยุดชะงักและสามารถแก้ไขได้ภายในเวลา 6 ชั่วโมง
- ความเสียหายรุนแรง ระบบงานหยุดชะงัก ต้องใช้เวลาแก้ไขมากกว่า 6 ชั่วโมงขึ้นไป

(2.2.2) รายงานความเสียหาย รายงานความเสียหายที่ทำให้ระบบงานคอมพิวเตอร์ต้องหยุดชะงัก และหรือเวลาที่ใช้ในการแก้ไขให้กลับคืนสู่สภาวะปกติ ต่อผู้บริหารตามลำดับ เพื่ออนุมัติและดำเนินการแก้ไขเหตุการณ์ตามขั้นตอนที่กำหนดไว้ ซึ่งรวมถึงการปฏิบัติงานสำรองทดแทน ณ ศูนย์คอมพิวเตอร์สำรองตามแผนปฏิบัติงานสำรอง (Back up Plan) ที่จัดทำไว้

(2.2.3) วิธีการปรับปรุงแก้ไขระบบงานคอมพิวเตอร์ที่ใช้ปฏิบัติงานจริงให้กลับคืนสู่สภาพปกติ ควรจัดทำแนวทางการแก้ไขระบบงานไว้ล่วงหน้า เพื่อให้การปฏิบัติงานเป็นไปอย่างถูกต้องและรวดเร็ว นอกจากนั้นยังเป็นแนวทางช่วยให้ผู้บริหารตัดสินใจเลือกวิธีการแก้ไขเหตุฉุกเฉินที่เหมาะสมในเวลาวิกฤต ควรประกอบด้วยขั้นตอนที่สำคัญดังนี้

(2.2.3.1) เตรียมการกู้ระบบงาน โดยติดต่อแจ้งเจ้าหน้าที่และผู้ที่เกี่ยวข้อง เช่น ผู้ใช้ระบบงานคอมพิวเตอร์ที่ได้รับความเสียหายจากภัยพิบัติ ติดต่อบริษัทประกันภัยเพื่อแจ้งเหตุฉุกเฉินตามเงื่อนไขกรมธรรม์ประกันภัยที่จัดทำไว้

(2.2.3.2) สำรวจความเสียหาย โดยสามารถเปรียบเทียบจากทะเบียนอุปกรณ์ และสิ่งที่ใช้ในการประมวลผลระบบงาน และแผนผังแสดงที่ตั้งอุปกรณ์และสภาพแวดล้อมที่รวบรวมไว้แล้วข้างต้น ระบบงานและโปรแกรมข้อมูล และอุปกรณ์ที่ชำรุดเสียหาย เพื่อซ่อมแซมแก้ไขหรือจัดซื้อมาทดแทน

(2.2.3.3) ประเมินค่าความเสียหายที่เกิดขึ้น

(2.2.3.4) พิจารณาวิธีการปรับปรุงแก้ไขหรือกู้ระบบงาน โดยคำนึงถึงความเหมาะสมของต้นทุนค่าใช้จ่าย และระยะเวลาที่ใช้ในการแก้ไขให้กลับคืนสู่สภาพปกติ เช่น การซ่อมแซม เปลี่ยนชิ้นส่วนอุปกรณ์ หรือใช้อุปกรณ์ ทดแทนที่สำรองไว้ เช่าหรือซื้ออุปกรณ์ต่าง ๆ ดังนั้น จึงจำเป็นต้องมีข้อมูลเกี่ยวกับสิ่งจำเป็นต้องใช้ในการปฏิบัติงาน รวมทั้งขั้นตอนการจัดหาอุปกรณ์ดังกล่าว ซึ่งอาจจัดแบ่งได้เป็นประเภทใหญ่ ๆ ดังนี้

- สถานที่ปฏิบัติงาน
- เครื่องตกแต่งสำนักงาน
- เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ
- อุปกรณ์สื่อสาร
- วัสดุต่าง ๆ
- พนักงาน
- ระบบงานและโปรแกรม
- ข้อมูล ฐานข้อมูล หรือข้อมูลที่สำคัญอื่น ๆ
- อุปกรณ์อำนวยความสะดวก
- เอกสารประกอบระบบงาน

(2.2.3.5) การเริ่มปฏิบัติงานตามภาวะปกติ ก่อนที่จะเริ่มกลับมาปฏิบัติงานตามภาวะปกตินั้น ควรมีการทดสอบระบบงานก่อนใช้งาน เพื่อให้แน่ใจว่าระบบงานปฏิบัติงานถูกต้อง เช่น

- การปฏิบัติงานเชื่อมโยงระหว่างระบบงาน อุปกรณ์ประกอบและอุปกรณ์สื่อสาร
- คุณภาพของสายสื่อสารข้อมูล
- ความสามารถของระบบงานในการประมวลผลปริมาณงานสูง
- การปฏิบัติงานของอุปกรณ์พิเศษต่าง ๆ

- ทดสอบมาตรการรักษาความปลอดภัยของระบบงาน เพื่อให้แน่ใจว่าระบบงานเป็นระบบงานชุดที่ใช้ปฏิบัติงานอยู่เดิม ไม่มีการแก้ไขหรือเปลี่ยนแปลงระหว่างเกิดเหตุฉุกเฉินโดยไม่ได้รับอนุญาต เช่น รหัสประจำตัวผู้ใช้ระบบงาน (User ID) รหัสลับ (Password) หมายเลขงานที่ประมวลผล (Job Number) การแปลงรหัสรับส่งข้อมูล (Encryption) ฯลฯ

(2.2.3.6) ยกเลิกการปฏิบัติงานสำรอง ก่อนที่จะยกเลิกการปฏิบัติงานสำรอง ธนาคารอาจปฏิบัติงานระบบงานจริงที่แก้ไขแล้วควบคู่ไปกับระบบสำรอง (Parallel Processing) ภายในระยะเวลาที่เหมาะสมจนกว่าจะแน่ใจว่าระบบงานสามารถปฏิบัติงานได้อย่างถูกต้อง

(2.3) แผนปฏิบัติงานระบบคอมพิวเตอร์สำรอง (Back up Plan)

หมายถึง แนวทางที่ใช้ในการปฏิบัติงานคอมพิวเตอร์สำรองเพื่อทดแทนระบบงานคอมพิวเตอร์ที่ใช้ในการประมวลผลงานปกติเมื่อประสบภัย และให้ธนาคารสามารถประกอบธุรกิจ ตลอดจนให้บริการแก่ลูกค้าได้อย่างต่อเนื่อง ควรประกอบด้วยขั้นตอนที่จำเป็นดังนี้

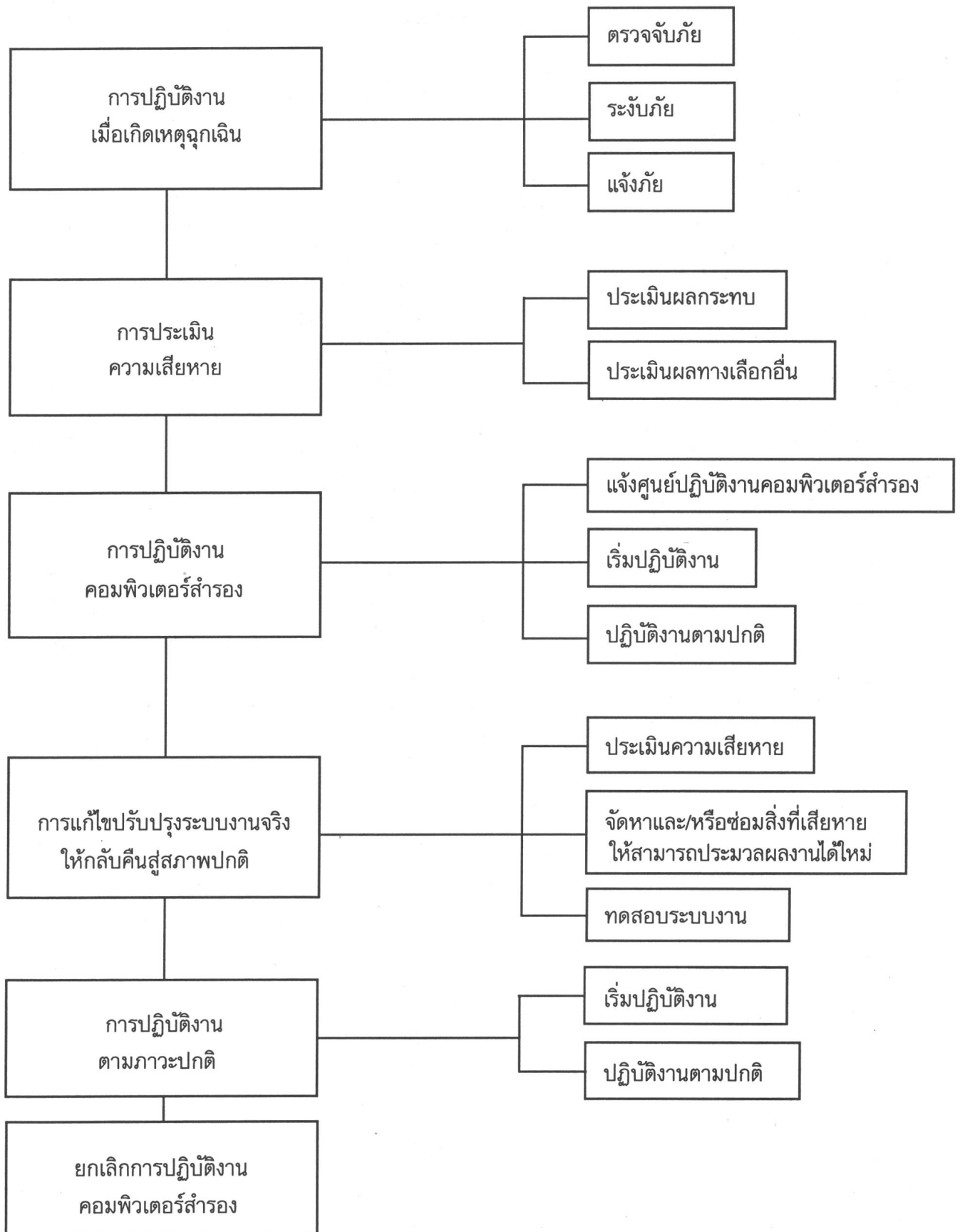
(2.3.1) การแจ้งเหตุฉุกเฉิน แจ้งเหตุฉุกเฉินให้แก่พนักงานและผู้ที่เกี่ยวข้องที่มีหน้าที่รับผิดชอบในการปฏิบัติงานสำรอง (Back up) รวมทั้งแจ้งการปฏิบัติงานไปยังสถานที่ปฏิบัติงานสำรอง (Back up Site)

(2.3.2) การเตรียมการปฏิบัติงานสำรอง เช่น จัดหาหรือเตรียมพาหนะเพื่อเดินทางไปยังสถานที่ปฏิบัติงานสำรอง ขนย้ายแฟ้มข้อมูล โปรแกรมระบบงาน เอกสาร และสิ่งจำเป็นต้องใช้ในการปฏิบัติงาน จัดเตรียมเครื่องคอมพิวเตอร์สำรองและอุปกรณ์ประกอบ ระบบสื่อสารข้อมูล อุปกรณ์อำนวยความสะดวก ตลอดจนจัดให้มีมาตรการป้องกันและรักษาความปลอดภัย ณ สถานที่ปฏิบัติงานสำรองอีกด้วย

(2.3.3) การปฏิบัติงานสำรอง เช่น เปิดระบบงาน บรรจุโปรแกรมและแฟ้มข้อมูล เปลี่ยนหรือใส่รหัสประจำตัวผู้ใช้ระบบงานสำรอง ทดสอบระบบงานก่อนปฏิบัติงาน ปฏิบัติงานตามขั้นตอนและตารางการปฏิบัติงาน ซึ่งครอบคลุมถึงการนำข้อมูลเข้าสู่ระบบ การประมวลผลงาน การจัดเตรียมและจัดส่งข้อมูลผลลัพธ์



ขั้นตอนการปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน
(Contingency Activities)



3. การแปลงระบบและนำแผนออกใช้งาน

มีขั้นตอนดังนี้

- 3.1 จัดเตรียมอุปกรณ์และระบบสำรอง ณ สถานที่ปฏิบัติการสำรองให้พร้อม เพื่อให้แน่ใจว่าสามารถปฏิบัติงานสำรองได้ทันที
- 3.2 อบรมฝึกหัดเจ้าหน้าที่ปฏิบัติงานและผู้เกี่ยวข้องให้ทราบถึงหน้าที่และความรับผิดชอบ
- 3.3 ทดสอบการปฏิบัติตามแผนที่กำหนด และประเมินผลการทดสอบ เพื่อปรับปรุงแก้ไขจุดบกพร่องให้สมบูรณ์
- 3.4 เสนอผู้บริหารอนุมัติ เพื่อประกาศให้ผู้ที่เกี่ยวข้องทราบและถือปฏิบัติต่อไป

4. การบำรุงรักษาและปรับปรุงแผน

มีวัตถุประสงค์เพื่อรักษาประสิทธิภาพของระบบงานสำรองให้พร้อมที่จะใช้งานได้ตลอดเวลา ซึ่งมี

ขั้นตอนดังนี้

- 4.1 ปรับปรุงระบบการแจ้งภัยให้แก่ผู้เกี่ยวข้องให้เป็นปัจจุบัน
- 4.2 อบรมเจ้าหน้าที่ให้มีความรู้ความชำนาญในหน้าที่
- 4.3 ดูแลและบำรุงรักษาอุปกรณ์สำรองต่าง ๆ
- 4.4 ควบคุมดูแลวัสดุอุปกรณ์
- 4.5 ดูแลปรับปรุงวิธีการคมนาคมขนส่ง
- 4.6 ปรับปรุงเอกสารประกอบระบบงานชุดสำรองให้เป็นปัจจุบัน
- 4.7 ให้มีการตรวจสอบสถานที่ปฏิบัติงานสำรอง
- 4.8 ทดสอบแผนฉุกเฉินเป็นระยะ ๆ ตามเวลาที่เหมาะสม
- 4.9 มีการจัดทำทดสอบแผนฉุกเฉินทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน หรือในจุดที่สำคัญ

รายการแนบ 1

(ตัวอย่าง)
แบบสำรวจข้อมูล
สิ่งจำเป็นในการปฏิบัติงานประมวลผลระบบงานคอมพิวเตอร์

วัตถุประสงค์

เพื่อให้ทราบข้อมูลเกี่ยวกับสิ่งจำเป็นในการประมวลผลงานด้วยคอมพิวเตอร์ ขั้นตอนการทำงาน และสภาพแวดล้อมในการปฏิบัติงาน

วิธีการใช้

แบบสำรวจข้อมูลแบ่งได้เป็น 5 ประเภท ดังนี้

1. โปรแกรมและระบบงาน

โปรแกรมควบคุมระบบงาน

โปรแกรมระบบงาน

โปรแกรมพิเศษ

ขั้นตอนการปฏิบัติงาน

2. เครื่องคอมพิวเตอร์

เครื่องคอมพิวเตอร์ Mainframe

Microcomputer

อุปกรณ์พิเศษ

3. ระบบสื่อสารข้อมูล

ระบบ Shared Network

ระบบ Online

ระบบ Dailups

4. อุปกรณ์ประกอบ

5. ข้อมูล แบบฟอร์ม และวัสดุ

แบบสำรวจข้อมูลอุปกรณ์คอมพิวเตอร์

ประเภทอุปกรณ์	หน้าที่/วิธีการปฏิบัติ/รหัสประจำตัวเครื่อง (Serial Number)	สถานที่ติดตั้ง	จำนวนที่มีอยู่	ประเมินการจัดหาทดแทน	
				เวลา	ค่าใช้จ่าย

แบบสำรวจข้อมูลอุปกรณ์ประกอบต่าง ๆ

รายการ	ตำแหน่งที่ตั้ง	ปริมาณที่มีอยู่	ประเมินการจัดหาทดแทน	
			เวลา	ค่าใช้จ่าย

แบบสำรวจข้อมูล ทางเดินของข้อมูล แบบฟอร์มและเอกสารที่เกี่ยวข้อง

รายการ/ประเภท	แหล่งที่มาเอกสารข้อมูล			โปรแกรม/ งานเลขที่	สื่อเก็บข้อมูล			ระยะเวลาเก็บ	ความถี่การจัดทำชุดสำรอง	สถานที่เก็บข้อมูลชุดสำรอง
	เอกสาร	ผู้จัดทำ	วิธีการเตรียม		ประเภท	เนื้อที่ DISK	จำนวนเทป			

(ตัวอย่าง)
แบบสอบถามข้อมูล
สถานการณ์ปฏิบัติงานสำรองชุดที่ใช้ปฏิบัติงานปัจจุบัน

วัตถุประสงค์

เพื่อประเมินความเหมาะสมเพียงพอของขั้นตอนการจัดทำระบบงานสำรองชุดที่ใช้ปฏิบัติงานในปัจจุบัน และปรับปรุงแก้ไขในการจัดทำ Contingency Plan ต่อไป

1. ในปัจจุบันการจัดสร้างระบบงานสำรองเพื่อประมวลผลระบบงานสำคัญ ณ สถานที่อื่นหากมีโปรด
ตอบคำถามดังต่อไปนี้

	มี	ไม่มี
1.1 การปฏิบัติงานสำรองสนับสนุนการประมวลผลงานลักษณะพิเศษเฉพาะ เช่น Microcomputer, Mainframe		
1.2 การปฏิบัติงานสำรองจัดทำเป็นทางการมีเอกสารเป็นลายลักษณ์อักษร มีผลผูกพันตามกฎหมาย		
1.3 สถานที่ปฏิบัติงานสำรองตั้งอยู่ห่างไกลจากศูนย์ปฏิบัติงานจริง และ ไม่ได้รับความเสียหายจากภัยพิบัติเดียวกัน		
1.4 มีการทดสอบเป็นระยะ ๆ เพื่อให้แน่ใจว่าระบบงานสามารถปฏิบัติทดแทนกันได้		
1.5 การปฏิบัติงานสำรองจัดเตรียมระบบสื่อสารข้อมูลสำหรับการประมวลผลงาน Online และแผนโครงข่ายสื่อสาร		
1.6 ระบบงานสำรองมีวิธีการหรืออุปกรณ์พิเศษดังที่ใช้อยู่ที่ชุดปฏิบัติงานจริง เช่น Encryption, RACF		
1.7 มีความมั่นใจหรือไม่ว่าระบบงานสำรองพร้อมที่จะปฏิบัติงานได้ภายในเวลาที่ยอมรับได้เมื่อเกิดเหตุฉุกเฉิน ทำให้ต้องเปลี่ยนแปลงวิธีการประมวลผลจากวิธีการปกติ		
1.8 มีอุปกรณ์ แบบฟอร์ม วัสดุ ระบบงาน และโปรแกรมที่จำเป็นต้องใช้ในการประมวลผลเก็บไว้ที่สถานที่ปฏิบัติงานสำรอง หรือสถานที่อื่นนอกสถานที่ที่มีการขนส่งสะดวก ไปยังที่ปฏิบัติงานสำรอง		
1.9 มีการมอบหมายหน้าที่ให้เจ้าหน้าที่ปฏิบัติงานสำรองเป็นทางการ		
1.10 สถานที่ปฏิบัติงานสำรองมีแผน Contingency Plan ชุดปัจจุบันเก็บไว้		

ต่อไปนี

2. ปัจจุบันมีขั้นตอนจัดทำข้อมูลชุดสำรองและดูแลรักษา Software หรือไม่ หากมีโปรดตอบคำถาม

	มี	ไม่มี
2.1 มีการกำหนดความถี่ในการจัดทำข้อมูลชุดสำรองหรือไม่		
2.2 มีการกำหนดวิธีการจัดทำข้อมูลชุดสำรองหรือไม่		
2.3 มีการจัดทำและจัดเก็บข้อมูลชุดสำรองโดยวิธี Grandfather-Father-Son หรือไม่		
2.4 ระยะเวลา ความถี่ และวิธีการจัดทำข้อมูลสำหรับระบบงานสำคัญ ได้มีการกำหนดตามความต้องการหรือเห็นชอบโดยผู้ใช้ระบบงานหรือไม่		
2.5 มีการกำหนดประเภทของข้อมูลสำรองเพื่อแยกจัดเก็บหรือไม่ (เช่น เพิ่มข้อมูลที่ใช้งานประจำ เพิ่มข้อมูลสำรองชุดก่อน)		
2.6 มีการผลิตเปลี่ยนอุปกรณ์สำรองที่ off site หรือไม่		
2.7 มีวิธีการควบคุมคุณภาพข้อมูลและโปรแกรมสำรองหรือไม่		
2.8 มีการทดสอบสื่ออุปกรณ์สำรองเป็นระยะ ๆ เพื่อให้แน่ใจว่าสามารถใช้งานได้หรือไม่		
2.9 หากมีการนำ Tape กลับไปยัง primary site โดยเหตุผลอันใดก็ตาม นอกเหนือจากการปรับปรุงข้อมูลให้เป็นปัจจุบันตามขั้นตอนปกติ มีมาตรการควบคุมการปฏิบัติดังกล่าวเพื่อให้แน่ใจว่าได้มีการนำ Tape นั้นคืนสู่ back up site ทันทีเมื่อเสร็จงานหรือไม่		
2.10 มีเอกสารระบุอุปกรณ์สิ่งจำเป็นต้องใช้ในการปฏิบัติงานสำรอง และเอกสารดังกล่าวระบุสถานที่เก็บตัวอย่างแน่ชัด		
2.11 มีการจัดเตรียมคำสั่งวิธีการปฏิบัติการแก้ไขเพิ่มข้อมูลและหรือข้อมูลให้กลับคืนสู่สภาพปกติ		
2.12 สถานที่ปฏิบัติงานสำรองมีความปลอดภัยหรือไม่		
2.13 ที่เก็บอุปกรณ์สำรองต่าง ๆ มีแผน Contingency ที่เป็นชุดปัจจุบัน		
2.14 Back up Site ตั้งอยู่ ณ ที่มีการคมนาคมเข้าออกสะดวก		
2.15 มีการกำหนดการจัดทำและจัดเก็บ diskette ชุดสำรอง		

3. โปรดระบุข้อคิดเห็นเกี่ยวกับการจัดทำระบบงานสำรองปัจจุบันที่คิดว่าจะเป็นประโยชน์ในการจัดทำ Contingency Plan

ข้อคิดเห็น.....
.....
.....

(ตัวอย่าง)
แบบสำรวจข้อมูล
ลำดับความสำคัญของระบบงานคอมพิวเตอร์

วัตถุประสงค์

รวบรวมข้อมูลเพื่อวิเคราะห์ความสำคัญของระบบงาน ความเสียหาย และผลกระทบจากภัยพิบัติ เพื่อใช้ในการพัฒนาระบบงานสำรองที่เหมาะสม

การใช้ประโยชน์

1. แบบสอบถามสามารถใช้ในการสอบถามหาข้อมูลเกี่ยวกับระบบงานคอมพิวเตอร์ได้ทุกระยะ กล่าวคือ ระบบงานใหม่ ระบบงานที่ใช้งานอยู่ปัจจุบัน ระบบงานที่กำลังปรับปรุงหรือแก้ไข
2. ข้อมูลที่รวบรวมจากการสำรวจระบบงาน (Inventory Forms) ใช้พิจารณาประกอบในการสัมภาษณ์เพื่อตอบแบบสอบถาม

-
1. ชื่อระบบงาน.....
 2. รหัส.....
-

3. ความสำคัญของระบบงาน

- 3.1 จำเป็นต้องมี Back up ☐ จำเป็น ☐ ไม่จำเป็น
- 3.2 ความล่าช้า (Delay) ที่สามารถรอนานที่สุด.....ชั่วโมง
- 3.3 ทางเลือกที่สนับสนุนการ Back up

- ☐ ปฏิบัติงานแบบ Manual ได้
- ☐ หยุดการประมวลผลได้ระยะหนึ่ง

3.4 มีการประมวลผลลักษณะพิเศษหรือการสื่อสารข้อมูลที่เป็นต้องมีในระบบงานนี้

- ☐ มี ☐ ไม่มี

ถ้ามี ระบุ.....

3.5 มีองค์กรอื่นเชื่อมโยงหรือเกี่ยวข้องกับระบบงานนี้ ☐ มี ☐ ไม่มี

ถ้ามี ระบุความสำคัญ.....

- 3.6 มีระบบงานอื่นที่รับหรือส่งข้อมูลให้กับระบบงาน ☐ มี ☐ ไม่มี
ถ้ามี ระบุความสำคัญ.....
- 3.7 การประมวลผลระบบงานมีบางช่วงเวลาที่ปริมาณรายการสูงกว่าปกติ และหรือ
ต้องให้ความสำคัญเป็นเวลาพิเศษ ☐ มี ☐ ไม่มี
ถ้ามี เวลา.....
- 3.8 มีอุปกรณ์พิเศษที่ต้องใช้ในการประมวลผล ☐ มี ☐ ไม่มี
ถ้ามี ระบุ.....
-

4. ความสำคัญของข้อมูล

- 4.1 ข้อมูลหรือโปรแกรมต้องเป็นความลับหรือสำคัญ ☐ มี ☐ ไม่มี
- 4.2 ต้องมีการรักษาความปลอดภัยพิเศษ ☐ มี ☐ ไม่มี
-

5. ผลกระทบจากภัยพิบัติ

รวบรวมรายละเอียดเกี่ยวกับข้อมูลต่อไปนี้

- 5.1 ผลกระทบทางด้านการปฏิบัติงาน (Operation).....
.....
- 5.2 ความเสียหายของธุรกิจ (Business Loss).....
.....
- 5.3 ความรับผิดชอบทางด้านกฎหมาย.....
.....
- 5.4 ผลกระทบกับความเชื่อถือของประชาชน.....
.....

บทที่ 4

แนวทางการพิจารณาเพื่อจัดหาและ
ทำสัญญากับบุคคลภายนอกเพื่อให้บริการ
ประมวลข้อมูล หรือใช้เป็นระบบคอมพิวเตอร์
สำรองเมื่อเกิดเหตุฉุกเฉิน

แนวทางการพิจารณาเพื่อจัดหาและทำสัญญากับบุคคลภายนอก เพื่อให้บริการประมวลผลข้อมูล หรือใช้เป็นแบบคอมพิวเตอร์สำรองเมื่อเกิดเหตุฉุกเฉิน

ในกรณีที่ธนาคารพาณิชย์เลือกใช้บริการประมวลผลข้อมูล หรือใช้เป็นระบบคอมพิวเตอร์สำรองเมื่อเกิดเหตุฉุกเฉิน ของศูนย์บริการคอมพิวเตอร์ (Service Bureau) โดยองค์กรอื่นภายนอกธนาคาร ซึ่งเจ้าหน้าที่ผู้ปฏิบัติงานมิได้เป็นพนักงาน และมีได้อยู่ภายใต้การควบคุมดูแลของธนาคารพาณิชย์ ดังนั้นเพื่อให้การใช้ระบบคอมพิวเตอร์สำรองดำเนินการต่อไปด้วยความมั่นใจและเชื่อได้ของทุกฝ่ายที่เกี่ยวข้อง จึงควรกำหนดหน้าที่และความรับผิดชอบบางประการไว้ในสัญญาการใช้บริการ และควรร่วมกันหาวิธีและมาตรการรักษาความปลอดภัยและการควบคุมภายในที่เหมาะสม

1. วัตถุประสงค์

เพื่อชี้ประเด็นที่ควรพิจารณาในการจัดหาและทำสัญญากับบุคคลภายนอกในลักษณะที่จะเป็นประโยชน์ และให้ความคุ้มครองอย่างเพียงพอแก่ธนาคารพาณิชย์และลูกค้าประชาชนผู้ใช้บริการ ในอันที่จะมั่นใจได้ว่าจะมีการปฏิบัติตามสัญญาที่ได้ตกลงกันไว้ และไม่ส่งผลกระทบต่อการทำงานและการให้บริการของธนาคารพาณิชย์

2. การคัดเลือกศูนย์บริการคอมพิวเตอร์ (Service Bureau)

การพิจารณาคัดเลือกศูนย์บริการคอมพิวเตอร์ ควรพิจารณาประเด็นที่สำคัญ ดังนี้

(1) ฐานะและการดำเนินงานของศูนย์บริการคอมพิวเตอร์

(1.1) ควรพิจารณาศูนย์บริการคอมพิวเตอร์ที่มีฐานะทางการเงินที่มั่นคง เพื่อให้บริการแก่ธนาคารพาณิชย์ได้อย่างมั่นคง ปลอดภัย และต่อเนื่อง ไม่ส่งผลกระทบต่อการทำงานตามแผนฉุกเฉิน และการใช้ระบบคอมพิวเตอร์สำรองของธนาคารพาณิชย์

(1.2) ผู้บริหารและเจ้าหน้าที่ปฏิบัติงานของศูนย์บริการคอมพิวเตอร์ ควรประกอบด้วยผู้ที่มีความรู้ความชำนาญทางด้านคอมพิวเตอร์ และเข้าใจในธุรกิจการธนาคารพาณิชย์

(1.3) มีมาตรการรักษาความปลอดภัยที่รัดกุมเหมาะสม

(1.4) แผนปฏิบัติงานและการปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan) ของศูนย์บริการคอมพิวเตอร์ มีขอบเขตเพียงพอและเหมาะสม รวมทั้งสอดคล้องกับแผนดังกล่าวของธนาคารพาณิชย์เอง เพื่อพร้อมที่จะปฏิบัติงานเมื่อเกิดเหตุฉุกเฉินที่อาจเกิดขึ้นกับธนาคารพาณิชย์ได้อย่างมีประสิทธิภาพ

(1.5) มีอัตราและวิธีการคิดค่าบริการที่เหมาะสมและยุติธรรม

(1.6) มีการประกันภัยที่ให้ความคุ้มครองความเสียหายต่าง ๆ อย่างเพียงพอ

(2) สภาพแวดล้อมโดยทั่วไปของศูนย์บริการคอมพิวเตอร์

(2.1) สถานที่ตั้งของศูนย์บริการคอมพิวเตอร์ตั้งอยู่ในที่เหมาะสม ไม่ตั้งอยู่ใกล้ในบริเวณเดียวกับที่ตั้งศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ เพราะอาจได้รับผลกระทบจากภัยพิบัติประเภทเดียวกัน และไม่ตั้งอยู่ห่างไกลจากธนาคารพาณิชย์เกินไป เพื่อความสะดวกและประหยัดค่าใช้จ่ายในการคมนาคมและติดต่อสื่อสาร

(2.2) ลักษณะการก่อสร้างอาคารมีความแข็งแรงเพียงพอที่จะรองรับน้ำหนักของอุปกรณ์ต่าง ๆ มีความสูงของเพดานอาคารแต่ละชั้นเพียงพอให้อากาศถ่ายเทความร้อนจากอุปกรณ์คอมพิวเตอร์ได้ดี

(2.3) ลักษณะภายในอาคารและบริเวณที่ตั้งของศูนย์คอมพิวเตอร์ตั้งอยู่ในชั้นที่ไม่สูงและต่ำเกินไป เพื่อหลีกเลี่ยงผู้บุกรุกและภัยต่าง ๆ และมีทางเข้าออกสู่ศูนย์คอมพิวเตอร์ที่เหมาะสมสอดคล้องกับมาตรการรักษาความปลอดภัย

(2.4) ลักษณะการดำเนินงานหรือธุรกิจของผู้ที่อยู่ในบริเวณรอบ ๆ ศูนย์บริการคอมพิวเตอร์ ไม่ก่อให้เกิดความเสี่ยงภัยต่าง ๆ

(2.5) บริเวณที่ตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบต่าง ๆ เหมาะสม

(2.6) การรักษาความปลอดภัยและบำรุงรักษาสถานที่เพียงพอและเหมาะสม

(3) สภาพแวดล้อมในการปฏิบัติงานของศูนย์บริการคอมพิวเตอร์

(3.1) ชีตความสามารถระบบงานคอมพิวเตอร์ของศูนย์บริการคอมพิวเตอร์เท่าเทียมกับระบบงานคอมพิวเตอร์ของธนาคารพาณิชย์ และสามารถปฏิบัติงานทดแทนกันได้

(3.2) ความพร้อมที่จะปฏิบัติงานในเวลาที่ต้องการ และจัดหาช่วงระยะเวลาประมวลผลงานให้แก่ธนาคารพาณิชย์ได้เพียงพอ

(3.3) ความสามารถของระบบงานในการประมวลผลงานที่มีปริมาณรายการเพิ่มขึ้นมากกว่าภาวะปกติ

(3.4) ระยะเวลาเตรียมพร้อมในการปฏิบัติงานหรือประมวลผลสำรองให้แก่ธนาคารพาณิชย์เมื่อได้รับแจ้งเหตุฉุกเฉิน สามารถดำเนินการได้อย่างเหมาะสมและมีประสิทธิภาพ

(4) การควบคุมการปฏิบัติงานของศูนย์บริการคอมพิวเตอร์

เมื่อธนาคารพาณิชย์เลือกใช้บริการด้านคอมพิวเตอร์จากบุคคลภายนอกเพื่อประมวลผลงานหรือเป็นระบบงานสำรองเมื่อเกิดเหตุฉุกเฉิน ศูนย์บริการคอมพิวเตอร์จะทำหน้าที่ควบคุมการปฏิบัติงานแทนธนาคารพาณิชย์ ดังนั้นธนาคารพาณิชย์จึงควรมีการติดตามและควบคุมการปฏิบัติงานของศูนย์บริการคอมพิวเตอร์อย่างใกล้ชิด และร่วมกันหาวิธีการควบคุมที่เหมาะสม โดยมีหลักการดังนี้

(4.1) การแบ่งแยกหน้าที่

การแบ่งแยกหน้าที่เป็นการควบคุมขั้นพื้นฐาน เพื่อป้องกันการทุจริตที่อาจเกิดขึ้นจากเจ้าหน้าที่ผู้ปฏิบัติงาน ตัวอย่างในการแบ่งแยกหน้าที่ได้แก่

- กำหนดไม่ให้เจ้าหน้าที่คนใดคนหนึ่งมีอำนาจอนุมัติแต่เพียงผู้เดียว หรือทำงานคนเดียวทุกขั้นตอน
- สลับเปลี่ยนหน้าที่ของเจ้าหน้าที่ผู้ปฏิบัติงานหมุนเวียนกันไปเป็นประจำ และกำหนดให้เจ้าหน้าที่ในแต่ละหน้าที่ลาหยุดพักผ่อนเป็นระยะ ๆ
- ควรใช้วิธีการคุมซ้อน (dual control) เช่นเดียวกับที่ใช้ในการทำงานตามระบบเดิม

(4.2) การควบคุมภายใน

การควบคุมภายในอาจจำแนกได้เป็น 3 ประเภท คือ

- การควบคุมด้านการบริหารงาน ได้แก่ การตรวจตราดูแลการปฏิบัติงานประจำวัน และรายงานที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ เพื่อให้เกิดประสิทธิภาพในการปฏิบัติงานโดยอาศัย Exception Report ต่าง ๆ
- การควบคุมด้านการเงิน เพื่อให้แน่ใจว่ารายการด้านการเงินที่เกิดขึ้นมีการอนุมัติตามขั้นตอนที่กำหนดไว้ เช่น มีการควบคุมทั้งก่อนและหลังการประมวลผล มีระเบียบการจัดส่งรายงาน การแก้ไขข้อมูล และการควบคุมการใช้ Exception Report ต่าง ๆ
- การควบคุมด้านอื่น ๆ ที่ไม่เกี่ยวกับการเงิน เช่น ชื่อที่อยู่ลูกค้า โดยควบคุมและตรวจสอบจนแน่ใจว่าข้อมูลเหล่านี้ถูกต้องพร้อมที่จะใช้งาน

(4.3) การสื่อสารข้อมูล

การสื่อสารข้อมูลในระบบงาน On-line ระหว่างศูนย์บริการคอมพิวเตอร์กับธนาคารพาณิชย์ ควรจัดให้มีการควบคุมตามความเหมาะสม เช่น

- การควบคุมโดยวิธีกำหนดตัวผู้ปฏิบัติงาน การควบคุมตามวิธีนี้จะอนุญาตให้พนักงานที่ได้รับมอบหมายเท่านั้นที่จะใช้ระบบคอมพิวเตอร์ได้ โดยกำหนดตัวพนักงาน และเครื่อง Terminal ที่จะใช้ ด้วยการให้ผู้ปฏิบัติงานมีกุญแจสำหรับเปิดปิดเครื่อง มีบัตรอนุญาต (machine readable badge) หรือมีรหัสลับประจำตัวผู้ที่ได้รับมอบอำนาจให้ใช้เครื่อง (password) ฯลฯ
- การควบคุมการใช้ข้อมูล คือ การกำหนดให้ผู้ปฏิบัติงานใช้ข้อมูลเฉพาะส่วนที่ตนมีหน้าที่เกี่ยวข้องเท่านั้น

- การควบคุมโดยการจำกัดอำนาจในการบันทึกรายการ (Restricted Transaction) สำหรับรายการที่มีความสำคัญเป็นพิเศษ ควรกำหนดให้พนักงานชั้นบริหารเป็นผู้บันทึกรายการด้วยตนเอง ตัวอย่างเช่น การล้างรายการ การแก้ไขจำนวนเงินในบัญชีของลูกค้า หรือการออกยอดงบการเงินประจำวัน เป็นต้น
- การติดตามควบคุมการปฏิบัติงานด้านสื่อสารข้อมูล เช่น การใช้อุปกรณ์พิเศษ และการใช้ Exception Report ต่าง ๆ
- การรักษาความปลอดภัยทางกายภาพของระบบสื่อสาร

(4.4) การตรวจสอบภายใน

ศูนย์บริการคอมพิวเตอร์ควรจัดให้มีการตรวจสอบภายในด้านคอมพิวเตอร์ทุกระยะโดยอาจจัดตั้งผู้ตรวจสอบภายในของตนเอง หรือให้ผู้ตรวจสอบจากภายนอกเพื่อป้องกันความเสียหายที่อาจเกิดจากการควบคุม และวิธีการปฏิบัติงานที่ขาดประสิทธิภาพ การปฏิบัติงานที่ผิดพลาดไม่ถูกต้องตามระเบียบ และการทุจริตของพนักงาน รวมทั้งควรกำหนดและยินยอมให้ผู้ตรวจสอบของธนาคารพาณิชย์ และเจ้าหน้าที่ผู้ตรวจสอบของธนาคารแห่งประเทศไทย ที่มีหน้าที่กำกับและตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์ เข้ามาตรวจสอบการปฏิบัติงานของศูนย์บริการคอมพิวเตอร์

นอกจากนี้ธนาคารพาณิชย์ควรเข้าชมการปฏิบัติงานของศูนย์บริการคอมพิวเตอร์ เพื่อดูการปฏิบัติงานทั่ว ๆ ไป ประกอบการพิจารณา และซักถามเพิ่มเติมจนเป็นที่พอใจ เพื่อให้แน่ใจว่าศูนย์บริการคอมพิวเตอร์จะสามารถให้บริการต่อไปได้ แม้จะเกิดภาวะผันแปรทางเศรษฐกิจ และควรติดต่อสอบถามบรรดาลูกค้าของศูนย์บริการคอมพิวเตอร์นั้น ๆ ในเรื่องความถูกต้องของงาน การตรงต่อเวลา และการให้ความร่วมมือ เพื่อเป็นการยืนยันคุณภาพในการปฏิบัติงาน

3. การทำสัญญาระหว่างธนาคารพาณิชย์กับศูนย์บริการคอมพิวเตอร์

ในการทำสัญญาระหว่างธนาคารพาณิชย์กับศูนย์บริการคอมพิวเตอร์ จะต้องระบุความรับผิดชอบของทั้งสองฝ่ายเกี่ยวกับการให้บริการด้านคอมพิวเตอร์ให้ครบถ้วน เพื่อป้องกันปัญหาที่อาจเกิดขึ้นภายหลัง โดยควรระบุเรื่องที่สำคัญไว้ในสัญญา ดังนี้

- (1) ระบุงานที่ธนาคารใช้บริการ ระยะเวลาในการประมวลผล และข้อมูลที่ปรากฏในรายงานต่าง ๆ
- (2) หลักเกณฑ์ในการคำนวณค่าบริการและค่าใช้จ่ายต่าง ๆ
- (3) กำหนดเวลาในการรับส่งงาน ระหว่างศูนย์บริการคอมพิวเตอร์กับธนาคารพาณิชย์
- (4) กำหนดความรับผิดชอบในการตรวจสอบ รวมทั้งสิทธิของธนาคารพาณิชย์และธนาคารแห่งประเทศไทย ซึ่งมีหน้าที่กำกับและตรวจสอบธนาคารพาณิชย์ ในการส่งตัวแทนเข้าไปตรวจสอบการทำงานของศูนย์บริการคอมพิวเตอร์ ฐานะของกิจการ และการดำเนินงานที่จำเป็น
- (5) การจัดมาตรการและอุปกรณ์ที่จำเป็นในการปฏิบัติงาน และการป้องกันข้อมูลที่อาจเสียหาย เพื่อให้แน่ใจว่าศูนย์บริการคอมพิวเตอร์สามารถประมวลผลได้ทันที่ตามกำหนด แม้จะมีเหตุฉุกเฉินเกิดขึ้นเมื่อใดก็ตาม

(6) ความรับผิดชอบในการขนส่งเอกสารข้อมูลต่าง ๆ ระหว่างธนาคารพาณิชย์กับศูนย์บริการคอมพิวเตอร์ ถ้าศูนย์บริการคอมพิวเตอร์เป็นผู้รับผิดชอบ ศูนย์บริการคอมพิวเตอร์จะต้องทำการประกันภัยให้คุ้มกับค่าเสียหายที่อาจเกิดขึ้นด้วย

(7) ควรประกันภัยข้อมูลที่อาจสูญหายเนื่องจากเจ้าหน้าที่ปฏิบัติงานผิดพลาด และบกพร่องละเลย ไม่ปฏิบัติตามหน้าที่ด้วย

(8) การรักษาความลับของข้อมูล

(9) กรรมสิทธิ์ในโปรแกรมและเอกสารที่ใช้ปฏิบัติงานที่เกี่ยวข้อง

(10) กรรมสิทธิ์ในแฟ้มข้อมูล (data files)

(11) การป้องกันและเก็บรักษาข้อมูล แฟ้มข้อมูล โปรแกรม เอกสารต่าง ๆ

(12) การจัดลำดับความสำคัญและขั้นตอนในการปฏิบัติงาน

(13) การยินยอมให้มีการเปลี่ยนแปลงระบบงานและขั้นตอนการปฏิบัติงานในกรณีที่ธนาคารพาณิชย์มีการปรับปรุงแก้ไขระบบงาน รวมทั้งระยะเวลาที่ใช้ในการเปลี่ยนแปลงดังกล่าว

(14) การกำหนดให้ศูนย์บริการคอมพิวเตอร์แจ้งการเปลี่ยนแปลงระบบงานใด ๆ หรืออื่น ๆ ที่จะมีผลกระทบต่อขั้นตอนและวิธีการปฏิบัติงาน ให้ธนาคารพาณิชย์ทราบก่อนล่วงหน้าในเวลาที่เหมาะสม

(15) การเปลี่ยนแปลงราคาค่าบริการหรือค่าใช้จ่ายต่าง ๆ

(16) การกำหนดวิธีการยกเลิกสัญญา เช่น กำหนดให้ศูนย์บริการคอมพิวเตอร์แจ้งล่วงหน้า 60-120 วันก่อนจะครบกำหนดสัญญา

(17) การกำหนดให้ธนาคารพาณิชย์สามารถทำการทดสอบแผนปฏิบัติงาน และปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉินได้ในระยะเวลาที่เหมาะสม

(18) กำหนดให้ศูนย์บริการคอมพิวเตอร์ส่งงบการเงินของตนไปให้ธนาคารพาณิชย์ทุกงวดการบัญชีเพื่อวิเคราะห์ฐานะทางการเงินของศูนย์บริการคอมพิวเตอร์

4. การกำหนดหน้าที่ความรับผิดชอบภายในของธนาคารพาณิชย์

ธนาคารพาณิชย์ควรกำหนดหน้าที่ความรับผิดชอบในระดับต่าง ๆ ที่เกี่ยวข้องกับการให้บริการด้านคอมพิวเตอร์ภายนอกธนาคาร ดังนี้

(1) ฝ่ายจัดการ ควรมีหน้าที่และความรับผิดชอบในการพิจารณา

- ขั้นตอนการจัดทำข้อตกลงและข้อสนับสนุนต่าง ๆ เป็นไปตามรูปแบบของสัญญา
- แต่งตั้งหรือกำหนดบุคคลใดบุคคลหนึ่งเป็นตัวแทนที่มีอำนาจหน้าที่ในการอนุมัติการจัดทำสัญญาที่จัดทำขึ้นเพื่อสนับสนุนแผนปฏิบัติงาน และปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan) ของธนาคารพาณิชย์ นอกจากนี้ควรกำหนดเจ้าหน้าที่ปฏิบัติงานด้านต่าง ๆ ให้เหมาะสมด้วย
- อนุมัติการจัดทำสัญญากับศูนย์บริการคอมพิวเตอร์

- (2) ฝ่ายควบคุมและตรวจสอบกิจการ/ธุรกิจ/การจัดทำสัญญา ควรรับผิดชอบ
- ตรวจสอบว่าข้อกำหนดตามแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน ได้ระบุไว้โดยครบถ้วนในสัญญาที่ทำไว้กับศูนย์บริการคอมพิวเตอร์ ก่อนที่จะมีการใช้บริการ หรือรับความสนับสนุนใด ๆ
 - ตรวจสอบกิจกรรมที่ศูนย์บริการคอมพิวเตอร์กระทำ ว่าสอดคล้องหรือเป็นไปตามแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉินของธนาคารพาณิชย์ด้วย เช่น การจัดทำข้อมูลชุดสำรอง การปรับปรุงข้อมูลให้เป็นปัจจุบันเมื่อมีการเปลี่ยนแปลงเกิดขึ้น รวมทั้งประสานงานกับฝ่ายกฎหมายในการพิจารณาจัดทำสัญญา
 - สอบทานแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉินของศูนย์บริการคอมพิวเตอร์ มีความเหมาะสมและสอดคล้องกับแผนปฏิบัติงานดังกล่าวของธนาคารพาณิชย์
- (3) ฝ่ายกฎหมาย ควรรับผิดชอบ
- พิจารณาลดความในสัญญา มีความสมบูรณ์ถูกต้อง ครบถ้วน และเป็นไปตามข้อกำหนดที่ต้องการตามแผนปฏิบัติงาน และปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉินของธนาคารพาณิชย์
 - มีการระบุโทษในกรณีที่ไม่ปฏิบัติตามสัญญาโดยชัดเจน
 - ให้คำแนะนำฝ่ายจัดการในการดำเนินการตามกฎหมายเพื่อเรียกร้องค่าเสียหายถ้าจำเป็น
- (4) เจ้าหน้าที่ปฏิบัติงาน ควรรับผิดชอบ
- ปฏิบัติงานตามขั้นตอนการปฏิบัติงานที่กำหนดไว้ในแผนปฏิบัติงาน และปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน
 - ทดสอบแผนปฏิบัติงานดังกล่าวเป็นระยะ ๆ ตามความเหมาะสม และเมื่อมีการปรับปรุงแก้ไขระบบงาน
 - ประสานงานกับศูนย์บริการคอมพิวเตอร์ในการปฏิบัติงานสำรอง หรือประมวลผลงานตามแผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน



บทที่ 5

กรณีศึกษา : แผนฉุกเฉิน

กรณีศึกษา : แผนฉุกเฉิน บทเรียนที่ธนาคาร GRINDLAY ได้รับจากการจลาจล

วันอังคารที่ 17 เมษายน พ.ศ.2527 การปฏิบัติงานประมวลผลงาน BATCH ประจำวันที่ส่งมาจากสำนักงานสาขาต่าง ๆ ในเมือง LONDON ของพนักงานศูนย์คอมพิวเตอร์ ธนาคาร GRINDLAY สาขาจตรัส ST. JAMES ต้องชะงักลงเมื่อเวลา 11.00 นาฬิกา เนื่องจากการประท้วงของนักศึกษาที่อยู่ภายนอกอาคารสำนักงานประชาชนชาวลิเบียทวีความรุนแรงขึ้นถึงกับมีการเสียชีวิตและมีผู้ได้รับบาดเจ็บหลายคน

เจ้าหน้าที่ตำรวจได้เข้าดำเนินการปราบปรามอย่างรวดเร็ว จตรัสถูกปิดล้อมไว้พนักงาน 140 คนของธนาคารได้รับการคุ้มกันและถูกกักบริเวณให้อยู่ภายในอาคาร ประตูด้านหน้าของธนาคารถูกปิดห้ามผ่านเข้าออก จนถึงเวลาเย็นพนักงานจึงถูกปล่อยให้กลับบ้านทางประตูหลังด้าน ORMOND YARD

วันต่อมาเจ้าหน้าที่ตำรวจยังคงล้อมบริเวณจตรัส และห้ามผ่านเข้าออกอาคารที่อยู่ใกล้เคียงกับบริเวณนั้นโดยเด็ดขาด แต่ในที่สุดก็ยินยอมให้พนักงานธนาคารผ่านเข้าออกได้วันละ 2 ครั้ง คือ เวลาเช้าและเลิกงาน และผลจากการต่อรองอีกครั้ง ธนาคารก็ได้รับอนุญาตให้ขนส่งเอกสารได้วันละ 6 ครั้ง การปฏิบัติงานเริ่มดำเนินไปอย่างเร่งรีบ มีการปฏิบัติงานนอกเวลาถึง 4 วัน งานของศูนย์คอมพิวเตอร์จึงแล้วเสร็จทันเวลา

ธนาคารมีแผนการปฏิบัติงานกรณีฉุกเฉิน (Emergency plan) แต่เป็นการปฏิบัติโยกย้ายหลบหนีจากอาคาร อันเนื่องมาจากการฉีกน้ำท่วมจากแม่น้ำ Thames โดยไม่ได้คำนึงถึงเหตุการณ์จลาจลเช่นนี้ แต่ก็สามารถแก้ไขสถานการณ์ได้โดยปรับปรุงแผนการให้เหมาะสม ดังนี้

1. โยกย้ายพนักงานจากอาคาร เหลือเพียงกลุ่มน้อยที่จะปฏิบัติงานคอมพิวเตอร์
2. ย้ายการปฏิบัติงานศูนย์คอมพิวเตอร์ทั้งหมดไปปฏิบัติที่แห่งอื่น

การจลาจลในครั้งนี้ยืดเยื้อเป็นเวลาถึง 14 วัน จึงยุติ สามารถประกอบธุรกิจได้ตามปกติ ธนาคารได้รับบทเรียนในการบริหารงาน แก่ไขวิกฤตการณ์ดังนี้

1. เทคนิคการปฏิบัติงานของศูนย์คอมพิวเตอร์มีขอบเขตจำกัดมากเกินไป หากสถานการณ์ร้ายแรงกว่านี้อาจต้องปิดศูนย์คอมพิวเตอร์
2. วิกฤตการณ์ครั้งนี้มีผลกระทบด้านพนักงานมากกว่าด้านอื่น เพราะพนักงานเป็นผู้ปฏิบัติการใช้เครื่องคอมพิวเตอร์ ซึ่งมีความสำคัญต่อการประมวลผล
3. เหตุการณ์เช่นนี้ควรเป็นหน้าที่ของผู้จัดการสาขาแห่งนั้น ที่จะต้องดำเนินการแก้ปัญหาเฉพาะหน้ามิใช่หน้าที่ของผู้บริหารอาวุโสจากสำนักงานใหญ่ เพราะผู้ที่อยู่ในเหตุการณ์ย่อมจะรู้รายละเอียดต่าง ๆ ดีกว่าผู้ที่อยู่ห่างไกล
4. ผู้บริหารควรแจ้งให้พนักงานทราบถึงเหตุการณ์ที่เกิดขึ้นในขณะนั้น และแผนการแก้ไขสถานการณ์ที่กำลังเผชิญอยู่

5. ถึงแม้ว่าการปฏิบัติงานร่วมกันของหน่วยงานในองค์การที่มีโครงสร้างและการบริหารที่ดีย่อมมีประสิทธิภาพ เพราะมีการประสานงานสอดคล้องกัน แต่ในขณะเดียวกันความเป็นอิสระและความรอบคอบในการปฏิบัติงานของหน่วยงานก็มีประสิทธิภาพดีเช่นกัน การปฏิบัติงานร่วมกันอาจมีข้อขัดแย้งมากขึ้น เพราะต่างฝ่ายมีวิธีแก้ปัญหาอันเดียวกันนั้นได้หลายวิธี สำหรับในกรณีนี้ผู้บริหารต้องมีความสามารถปฏิบัติงานได้อย่างอิสระและทันทั่วทั้งที่

6. การปฏิบัติงานแต่ละวันให้สำเร็จลุล่วงย่อมเต็มไปด้วยความยากลำบาก ผู้บริหารต้องใช้ความพยายามและความสามารถผลักดันผู้ใต้บังคับบัญชาให้มีความตั้งใจปฏิบัติงาน

7. ถึงแม้เหตุการณ์จะผ่านไปแล้ว สามารถพูดได้ว่า “เรารอดมาได้และสามารถเผชิญกับมันได้อย่างเต็มที่” แต่ควรจะมีการพิจารณาวางแผนการแก้ปัญหาเหตุการณ์เฉพาะหน้า และตัดสินใจอย่างแน่วแน่ที่จะจัดให้มีการทดสอบหรือทดลองปฏิบัติงานตามแผนการที่กำหนดไว้เป็นครั้งคราว ก่อนที่จะรอให้ปัญหาเกิดขึ้นเสียก่อน



บทที่ 6

**กรณีศึกษาการตรวจ Data Center
(General Controls) และ Applications**



กรณีศึกษาการตรวจ Data Center (General Controls)

และ Applications

โดยประยุกต์ประเด็นที่ให้ศึกษาเป็นแนวคำถามและ
ให้แนวคำตอบจากการปฏิบัติภาคสนาม

กรณีศึกษาการตรวจองค์กรที่ใช้คอมพิวเตอร์ในบทนี้เป็นการทบทวนและฝึกซ้อมความเข้าใจที่เน้นหนักไปในการตรวจสอบด้านคอมพิวเตอร์ (Computer Audit หรือ IS Audit) ในส่วนที่เป็น Data Center หรือการตรวจ General Controls และการตรวจสอบระบบงานต่าง ๆ (Application Controls หรือ Application Audit) ทั้งนี้โดยตั้งแนวคำถามที่ประยุกต์มาจากประสบการณ์การตรวจสอบด้านคอมพิวเตอร์ภาคสนาม (field works) ในช่วงเวลาที่ผมทำหน้าที่ดูแลรับผิดชอบ การตรวจสอบสถาบันการเงินต่าง ๆ ทางด้านคอมพิวเตอร์

การตั้งกรณีศึกษาในบทนี้ เป็นการตั้งคำถามหรือคำถามอย่างง่าย ๆ เพียงเพื่อให้ท่านผู้อ่านได้ทบทวนความเข้าใจถึงการปฏิบัติงานและเข้าใจการตรวจสอบด้านคอมพิวเตอร์จริง ๆ ได้มากขึ้น ทั้งนี้ขอให้ท่านได้โปรดดูบทที่เกี่ยวกับการตรวจสอบต่าง ๆ ที่เกี่ยวข้องรวมทั้งบทที่ได้รับประสบการณ์จากประเทศต่าง ๆ ซึ่งเป็นเรื่องที่เกิดขึ้นจริง ๆ ที่ได้กล่าวถึงจุดอ่อน ความเสียหาย และการทุจริตที่เกี่ยวข้อง

หากท่านได้เพียงได้อ่านเรื่องดังกล่าวโดยไม่ได้เป็นผู้ตรวจสอบหรือต้องรับผิดชอบในด้านการบริหารที่เกี่ยวข้องด้วย ท่านก็อาจคิดเพียงว่าบางเรื่องแทบไม่น่าเป็นไปได้โดยเฉพาะกรณีศึกษาต่าง ๆ ด้าน Applications แต่ถ้าท่านเป็นผู้บริหารหรือผู้ตรวจสอบที่เกี่ยวข้องกับการตรวจสอบโดยตรง ท่านต้องสนใจเพิ่มขึ้นอีกระดับหนึ่งว่า จุดอ่อน ความเสียหายและการทุจริตที่อาจเกิดขึ้นได้ จะตรวจสอบโดยเชิงป้องกันปัญหาก่อนที่จะเกิดขึ้นได้อย่างไรแล้ว กรณีศึกษาทั้ง 2 บทนี้จะเป็นเรื่องที่น่าสนใจมากสำหรับท่านที่สนใจ

อย่างไรก็ดี แนวคำตอบจากกรณีศึกษาต่าง ๆ ในบทนี้ก็ไม่ได้กล่าวถึงวิธีการตรวจสอบจนพบประเด็นต่าง ๆ อย่างไร กรณีนี้ท่านสามารถนำบทต่าง ๆ ที่มีสรุปการตรวจสอบที่เกี่ยวข้องนำมาประยุกต์ใช้ได้

ผมใคร่ขอแนะนำว่าเมื่อท่านได้อ่านกรณีศึกษาแล้ว ขอท่านได้โปรดวิเคราะห์การเน้นถึงคำตอบเป็นขั้นเป็นตอน และใช้ดุลยพินิจของท่านจนได้คำตอบระดับหนึ่งก่อน แล้วจึงไปดูแนวคำตอบที่ได้ให้แนวทางไว้ในแต่ละกรณีแล้ว จะทำให้การศึกษาเปรียบเทียบได้ผลดีมากขึ้น อีกทั้งเป็นการทบทวนว่าท่านมีความเข้าใจในระดับใดได้ด้วย



กรณีศึกษา 1

บริษัทแห่งหนึ่งมีสาขาทั้งในกรุงเทพฯ และจังหวัดใกล้เคียงประมาณ 15 สาขา ได้ประสบปัญหาเรื่องการบันทึกข้อมูลทางการเงินไม่ทันเวลา และก่อให้เกิดความเสียหายต่อบริษัทอย่างมาก เพราะธุรกิจของบริษัทจะต้องใช้ข้อมูลที่ถูกต้องตลอดเวลาทำการ ดังนั้น จึงได้จัดตั้งศูนย์คอมพิวเตอร์ขึ้น และได้ซื้อโปรแกรมระบบงานสำเร็จรูปจากบุคคลภายนอกที่มีประสิทธิภาพสูงมาใช้ประมวลผลข้อมูลในเวลาทำการด้วยระบบ On-line โดยให้สาขาของบริษัททุกสาขาส่งข้อมูลผ่านเครื่องเทอร์มินอล และหลังเวลาทำการจะประมวลผลด้วยระบบ Batch

ในระหว่างเวลาทำการที่ศูนย์คอมพิวเตอร์จะมีเจ้าหน้าที่ควบคุมการทำงานของระบบคอมพิวเตอร์อยู่เมื่อหยุดการประมวลผลในระบบ On-line ในเวลา 18.30 น. แล้ว เจ้าหน้าที่ควบคุมการทำงานของระบบคอมพิวเตอร์จะจัดเตรียมโปรแกรมและอุปกรณ์ต่าง ๆ ที่ต้องใช้ในการประมวลผลในระบบ Batch แล้วปล่อยให้ระบบคอมพิวเตอร์ทำงานโดยอัตโนมัติ ซึ่งจะใช้เวลาในการประมวลผลประมาณ 7 ชั่วโมง และได้กำชับยามรักษาการณ์ว่า ถ้าไฟฟ้าดับก่อน 02.00 น. ของวันใหม่ ให้โทรศัพท์ไปบอกด้วย

ถ้าไม่มีปัญหา เจ้าหน้าที่ควบคุมระบบคอมพิวเตอร์จะมาทำข้อมูลชุด Back up และจัดแยกรายงานของหน่วยงานต่าง ๆ ในวันรุ่งขึ้น หลังจากนั้น ก็จะเตรียมระบบคอมพิวเตอร์และโปรแกรมเพื่อใช้ประมวลผลในระบบ On-line ซึ่งจะใช้เวลาประมาณ 1 ชั่วโมง และจะต้องให้เสร็จพร้อมใช้งานได้ภายในเวลา 8.30 น.

ให้ท่าน ระบุความเสี่ยง ความเสียหาย ข้อเสนอแนะในการควบคุม และการตรวจสอบที่เหมาะสมด้วย



กรณีศึกษา 2

จากการตรวจสอบศูนย์คอมพิวเตอร์แห่งหนึ่งเกี่ยวกับการส่งมอบรายงานให้แก่ผู้ใช้รายงาน พบว่าพนักงานประจำศูนย์คอมพิวเตอร์แยกรายงานตามสาขาแล้วไปไว้ตามช่องเก็บรายงานของแต่ละสาขา ซึ่งพนักงานรับ-ส่งเอกสารจะมาหยิบรายงานของสาขาตนไป แล้วลงชื่อผู้รับรายงาน และกรอกวันและเวลาที่รับตามแบบฟอร์มที่กำหนด

จากตัวอย่างแบบฟอร์มการรับรายงานข้างล่างนี้ ให้ท่านระบุความเสี่ยง ความเสียหาย และการควบคุมที่เหมาะสมด้วย

แบบฟอร์มการรับรายงานของวันที่ 8 พ.ค. 31

ชื่อสาขา	ลายมือชื่อผู้รับ รายงาน	วันเดือนปี รายงาน	เวลาที่รับ (น.)
ก	แดง	9 พ.ค.31	07.00
ข	แดง	9 พ.ค.31	07.00
ค	ดำ	9 พ.ค.31	03.00
ง			
จ	ดำ	9 พ.ค.31	10.10



กรณีศึกษา 3

ฝ่ายสินเชื่อของธนาคาร เอื้องฟ้า จำกัด ได้นำคอมพิวเตอร์มาใช้งานรับฝากหลักประกันเพื่อเป็นประกันหนี้ของลูกค้า กระบวนการรับฝากมีดังนี้

เจ้าหน้าที่สินเชื่อจะจัดเตรียมแบบฟอร์มที่มีหมายเลขกำหนดไว้ล่วงหน้า สำหรับใช้ในการบันทึกรายละเอียดของหลักประกัน และใช้เป็นใบรับด้วย แบบฟอร์มพร้อมสำเนา มี 4 ใบ คือ

- ใบที่ 1 สีมชมพู เป็นต้นฉบับ สำหรับมอบเป็นใบรับให้กับลูกค้า
- ใบที่ 2 สีขาว เป็นสำเนา ส่งให้กับเสมียนที่ทำหน้าที่จดบันทึกหลักประกันโดยตรง
- ใบที่ 3 สีฟ้า เป็นสำเนาที่เจ้าหน้าที่สินเชื่อจะส่งให้กับเจ้าหน้าที่รักษาตู้নির্যায়พร้อมกับตัวหลักประกัน
- ใบที่ 4 สีเหลือง เป็นสำเนา เก็บเข้าแฟ้มไว้อ้างอิง

เมื่อเจ้าหน้าที่ดูแลตู้নির্যায়ได้รับเอกสารแล้ว จะเปรียบเทียบใบสีฟ้า กับหลักประกันที่ได้รับ ถ้าถูกต้องตรงกันก็จะลงนามในใบสีฟ้า และบันทึกข้อความติดป้ายไว้กับหลักประกัน แล้วนำส่งหลักประกันพร้อมกับสำเนาใบสีฟ้า ให้พนักงานประจำตู้নির্যায় พนักงานประจำตู้নির্যายจะตรวจสอบข้อความในป้ายกับสำเนาใบสีฟ้า ถ้าข้อความถูกต้องตรงกันก็จะเปิดตู้নির্যายพร้อมกับเจ้าหน้าที่ที่นำมาให้ แล้วนำหลักประกันนั้นเก็บเข้าไปไว้ในตู้নির্যาย บันทึกเลขที่ลงในสำเนาสีฟ้า พร้อมทั้งลงนามไว้ แล้วส่งไปให้เสมียนที่ทำหน้าที่บันทึกหลักประกัน

เสมียนจะเก็บสำเนาสีขาวไว้เรียงตามเลขที่ จนกว่าจะได้รับสำเนาสีฟ้า นำมาเปรียบเทียบถ้าตรงกัน เสมียนก็จะ Key ข้อมูลบันทึกหลักประกันเข้าไว้ในระบบคอมพิวเตอร์เรียงตามเลขที่เสร็จแล้วฉีกสำเนาสีขาวทิ้งไป แล้วจึงเก็บสำเนาสีฟ้าไว้ในแฟ้มถาวร เรียงตามตัวอักษรชื่อลูกค้า หากมีข้อแตกต่าง ผู้ช่วยของเจ้าหน้าที่สินเชื่อจะเป็นผู้แก้ไขปัญหาเองทั้งหมด

ให้ท่าน ระบุจุดอ่อนที่สำคัญ และเสนอแนะการควบคุมที่เหมาะสมมาเป็นข้อ ๆ



กรณีศึกษา 4

หน่วยงานทางด้านคอมพิวเตอร์ของบริษัท จักรวาล จำกัด มีบุคลากรที่สำคัญอยู่ 3 คน คือ E D P Department Manager , Programmer / Operator และ Part - time Night Operator

- E D P Department Manager ทำหน้าที่เป็น System Analyst และหัวหน้า Programmer
- Programmer / Operator เป็นผู้จัดตารางการปฏิบัติงาน และเป็น Operator ในช่วงเวลากลางวัน
- Part - time Night Operator ทำงานคืนละ 4 ชั่วโมง เขาเป็นนักศึกษา วิชาเอกคอมพิวเตอร์ ในมหาวิทยาลัยแห่งหนึ่ง

ฝ่ายบริหารของบริษัทยืนยันว่า การจัดองค์กรและแบ่งแยกหน้าที่ของบุคลากรทางด้านคอมพิวเตอร์เหมาะสมดีแล้ว เพราะบริษัทซื้อโปรแกรมสำเร็จรูปมาใช้งานเป็นส่วนใหญ่ ซึ่งบริษัทผู้ขายก็ได้มอบเอกสารประกอบระบบงานให้ด้วย แล้ว บริษัทเพียงแต่ปรับปรุงโปรแกรมสำเร็จรูปที่ซื้อมาเพียงเล็กน้อยก็สามารถนำไปใช้งานได้ ประกอบกับในระหว่างวัน Operator ก็ไม่มีงานอะไรมากนัก เนื่องจากบริษัทประมวลผลด้วยวิธี On-line real-time Part-time Night Operator ทำหน้าที่ประมวลผลงานสิ้นวัน (Batch Processing) และทดสอบการทำงานของเครื่องคอมพิวเตอร์ในตอนเย็นด้วย

นอกจากนี้ฝ่ายบริหารเห็นว่าไม่จำเป็นต้องมี Tape librarian เนื่องจากในระหว่างวันม้วนเทปทั้งหลายก็ถูกนำมาใช้งานอยู่แล้ว ในเวลากลางคืนจึงจะเก็บไว้ในตู้สำหรับใส่ม้วนเทปโดยเฉพาะซึ่งตั้งอยู่ในห้องคอมพิวเตอร์นั่นเอง Part-time Night Operator จึงสามารถหยิบเอาม้วนที่ต้องการไปใช้งานได้ทันที และนำไปเก็บไว้ในตู้เมื่อใช้งานเสร็จแล้ว ตลอดเวลาที่ผ่านมาก็เกือบ 5 ปี บริษัทก็ไม่เคยประสบปัญหาใด ๆ เกี่ยวกับงานด้านคอมพิวเตอร์เลย

ในฐานะที่ท่านเป็นผู้ตรวจสอบด้านคอมพิวเตอร์ ท่านมีความเห็นและขอแนะนำแก่บริษัทนี้อย่างไรบ้างในเรื่องที่เกี่ยวข้องกับความเสี่ยง ความเสียหาย และการควบคุม



กรณีศึกษา 5

1. ธนาคารท่าพระจันทร์ จำกัด เป็นธนาคารขนาดกลาง มีสาขาทั้งในกรุงเทพฯ และต่างจังหวัดที่นำเครื่องคอมพิวเตอร์มาใช้ในการประมวลผลงานต่าง ๆ งานแรกที่ธนาคารนำเครื่องคอมพิวเตอร์มาใช้ในการประมวล คือ ระบบงานเงินฝากทั้ง 3 ประเภท ได้แก่ เงินฝากกระแสรายวัน เงินฝากออมทรัพย์ และเงินฝากประจำ พร้อมทั้งนำเครื่อง ATM มาให้บริการแก่ลูกค้าด้วย รูปแบบในการประมวลผลเป็นแบบ Centralized on-line ลูกค้าสามารถใช้บริการต่างสาขาได้สำหรับเงินฝากประจำ ธนาคารจะไม่จ่ายดอกเบี้ยให้กับเงินฝากที่มีระยะเวลาฝากไม่ถึง 3 เดือน เงินฝากออมทรัพย์จ่ายดอกเบี้ยให้ลูกค้าทุก 6 เดือน (วันที่ 30 มิถุนายน และ 31 ธันวาคม ของทุกปี) ซึ่งเครื่องจะบันทึกการรายการนี้ให้อัตโนมัติ หากลูกค้าปิดบัญชีระหว่างงวด พนักงานต้องคำนวณดอกเบี้ยจ่ายตั้งแต่งวดสุดท้ายจนถึงวันปิดบัญชีด้วยมือ (manual) แล้วบันทึกการจ่ายดอกเบี้ยผ่านทางเครื่อง terminal นอกจากนี้ ระเบียบปฏิบัติและขั้นตอนในการประมวลผลต่าง ๆ ก็จะคล้ายคลึงกับธนาคารพาณิชย์ทั่ว ๆ ไป เช่น ลูกค้าจะถอนเงินเกินยอดเงินคงเหลือที่มีสิทธิถอน (Available balance) ไม่ได้ ถึงแม้ยอดเงินที่ปรากฏในบัญชี (balance) จะมีมากกว่าก็ตาม หรือในทำนองตรงกันข้ามหาก Balance มีต่ำกว่า แต่มี Available balance สูงกว่า ผู้ฝากหรือเจ้าของบัญชีอาจถอนเงินได้มากกว่า Balance ก็ได้ เช่น บัญชีที่มีวงเงินเบิกเกินบัญชี เป็นต้น นอกจากนี้ การฝากเช็คติด clearing ซึ่งหมายถึง การฝากเช็คที่ยังไม่รู้ผลว่าเช็คใบนั้นจะถูกส่งคืนมาหรือไม่ จำเป็นที่ผู้รับหรือลูกค้าต้องทราบผลการเรียกเก็บเงินก่อน ซึ่งปกติใช้เวลาอย่างน้อย 1 วัน จึงจะมีสิทธิถอนเงินได้

ผู้ตรวจสอบด้านคอมพิวเตอร์ เข้าตรวจสอบศูนย์คอมพิวเตอร์และระบบงานต่าง ๆ ที่ประมวลผลด้านคอมพิวเตอร์ของธนาคาร โดยมีนายชาติชาย เป็นผู้รับผิดชอบตรวจสอบระบบงานเงินฝาก และ ATM หลังจากการตรวจสอบผ่านไปประมาณ 1 เดือน นายชาติชายพอจะทราบขั้นตอนการทำงานของโปรแกรมรหัสต่าง ๆ และแฟ้มข้อมูลที่ใช้บ้าง แต่ยังไม่ละเอียดนัก นายชาติชาย จึงตัดสินใจใช้เทคนิคการตรวจสอบที่เรียกว่า Test Data มาช่วยในครั้งนี้ด้วย โดยสร้างข้อมูลทดสอบขึ้นมาจำนวนหนึ่ง และจากข้อมูลทดสอบในแต่ละชุดที่ได้สร้างไว้ ขอให้ท่านกำหนดหรือระบุถึง

1. วัตถุประสงค์ในการตรวจสอบ
2. ผลลัพธ์ที่คาดว่าจะได้ (ระบุว่า ระบบงานจะ “ยอมรับ” หรือ “ปฏิเสธ” รายการ)
3. ความเสี่ยงและผลเสียหาย และการควบคุมที่ควรมี หากผลจากการทดสอบ ไม่เป็นไปตามผลลัพธ์ที่

คาดไว้

ชุดที่ 1 บัญชีเงินฝากประจำ 12 เดือน มี Test Data และข้อมูลปรากฏตามลำดับ ดังนี้

วัน / เดือน / ปี	รายการ	จำนวนเงิน
15/02/92	ฝากเงินสดเปิดบัญชี	50,000
15/02/93	ดอกเบี้ย (สุทธิจากภาษี)	3,000
15/02/93	ถอนเงินสดปิดบัญชี	53,000
20/03/93	ฝากเงินสด	70,000

ชุดที่ 2 บัญชีเงินฝากกระแสรายวัน มี Test Data และข้อมูลปรากฏตามลำดับ ดังนี้

วัน / เดือน / ปี	รายการ	จำนวนเงิน
25/02/93	ฝากเช็คเคลียร์	10,000
25/02/93	ฝากเงินสด	3,000
26/02/93	เช็คคืน	13,000

ชุดที่ 3 บัญชีเงินฝากออมทรัพย์ มียอดคงเหลือ (Available balance)
ยกมา 300 บาท เมื่อวันที่ 25/10/92 แล้วมี Test Data ตามลำดับดังนี้

วัน/ เดือน/ ปี	รายการ	จำนวนเงิน
25/10/92	ฝากเช็คเคลียร์	2,000
25/10/92	ถอนเงินสด	1,700

ชุดที่ 4 บัญชีเงินฝากประจำ (สามารถทำการถอนอายุได้บางส่วนได้)
มี Test Data และข้อมูลปรากฏตามลำดับดังนี้

วัน / เดือน / ปี	รายการ	จำนวนเงิน
13/03/92	ฝากเงินสดเปิดบัญชี	300,000
21/03/92	อายุเงินฝาก	200,000
25/03/92	เพิกถอนการอายุเงินฝาก	50,000
20/04/92	ถอนเงินสด	250,000

ชุดที่ 5 ธนาคารได้กำหนดอัตราดอกเบี้ยสำหรับเงินฝากประจำ ประเภท 12 เดือน และ 6 เดือน
ไว้เท่ากับ 7% และ 6.5% ต่อปีตามลำดับ โดยคอมพิวเตอร์จะบันทึกการจ่ายดอกเบี้ย
ให้แก่ลูกค้าที่ฝากจนครบกำหนดโดยอัตโนมัติ และ Teller จะเป็นผู้ key อัตราดอกเบี้ย
พร้อมกับข้อมูลอื่น ๆ ทุกครั้งที่รับฝากมี Test Data และข้อมูลปรากฏตามลำดับดังนี้

วัน / เดือน / ปี	รายการ	จำนวนเงิน
01/08/91	ฝากเงินสด (12 เดือน)	100,000
07/09/91	ฝากเงินสด (6 เดือน)	50,000
01/08/92	ดอกเบี้ย (ไม่คำนึงถึงภาษี)	7,000
07/03/92	ดอกเบี้ย (ไม่คำนึงถึงภาษี)	1,625
12/08/92	ถอนเงินสด (ยอดรวมพร้อม- ดอกเบี้ย)	107,000

กรณีศึกษา 6

โปรดเติมข้อมูลเป็นจำนวนเงินในช่องผลลัพธ์ที่คาดว่าจะได้รับ ทั้งในช่อง balance และ Available balance และ/หรือให้เติมข้อมูลอื่นในช่องผลลัพธ์ เช่น “ปฏิเสธ” ถ้าท่านคาดว่าผลลัพธ์เป็นปฏิเสธด้วย

เมื่อวันที่ 15/10/87 มี Balance 90,000.- บาท มี Available balance 290,000.- บาท (มีวงเงิน O/D 200,000.- บาท) มี Test Data และข้อมูลปรากฏตามลำดับดังนี้

วัน / เดือน / ปี	รายการ	จำนวนเงิน	ผลลัพธ์ที่คาดว่าจะได้รับ
20/11/87	ฝากเงินสด	100,000	- Balance.....
			- Available
			- อื่น ๆ
	ฝากเช็คที่ยังติดเคลียร์	5,000	- Balance
			- Available
			- อื่น ๆ
22/11/87	ถอนเงินสด	200,000	- Balance
			- Available
			- อื่น ๆ
23/11/87	ถอนเงินสด	195,000	- Balance
			- Available
			- อื่น ๆ
24/11/87	ถอนเงินสดผ่าน ATM	1,000	- Balance
			- Available
			- อื่น ๆ
25/11/87	ฝากเช็คที่ยังติดเคลียร์	30,000	- Balance
			- Available
			- อื่น ๆ

กรณีศึกษา 7

การตรวจสอบศูนย์ประมวลผลข้อมูล (Data Center)

วัตถุประสงค์ : เพื่อใช้ฝึกหัดการวิเคราะห์ความเสี่ยงหรือการหาจุดอ่อนในการตรวจสอบคอมพิวเตอร์ด้านการตรวจสอบศูนย์คอมพิวเตอร์ (Data Center) และการตรวจสอบระบบงาน (Applications)

กรณีศึกษานี้ต้องการให้เห็นภาพรวม จึงพยายามสมมติให้ครอบคลุมเรื่องราวต่าง ๆ เกือบทุกเรื่อง จึงไม่อาจเน้นลงลึกไปในรายละเอียดของเรื่องต่าง ๆ ได้ทั้งหมดแต่จะเน้นเพียงบางประเด็นที่คิดว่าสนใจเท่านั้น อย่างไรก็ตาม เนื่องจากกรณีศึกษานี้เขียนขึ้นอย่างค่อนข้างชัดเจนและไม่ซับซ้อนแต่อย่างใด การวิเคราะห์จึงทำได้ค่อนข้างง่าย เพื่อให้เข้าใจการวิเคราะห์ความเสี่ยงและการหาจุดอ่อนเพื่อประเมินผลการควบคุมระบบงานที่ใช้คอมพิวเตอร์กรณีที่มีจุดอ่อนน้อยจุดก็อาจมีความร้ายแรงมากกว่าการมีจุดอ่อนที่ไม่ร้ายแรงหลาย ๆ จุดก็ได้ ทั้งนี้ ท่านต้องพยายามประยุกต์ และดัดแปลงนำความรู้ที่ได้รับไปใช้ให้เป็นประโยชน์ต่อไป

ในการฝึกหัดวิเคราะห์จุดอ่อนต่าง ๆ ควรระบุถึงความเสี่ยงภัยที่คาดว่าจะเกิดขึ้นจากจุดอ่อนต่าง ๆ เหล่านั้นด้วย และควรเสนอแนะแนวทางหรือวิธีการแก้ไขจุดอ่อนดังกล่าวอีกด้วยจึงจะได้ประโยชน์สมบูรณ์ตามเจตนารมณ์ของกรณีศึกษาชุดนี้

กรณีศึกษา 7

บริษัท เอส.เอ. อินเทอร์เน็ต จำกัด

ภาค 1

บริษัท เอส.เอ. อินเทอร์เน็ต จำกัด ก่อตั้งขึ้นเมื่อปี พ.ศ.2530 เป็นบริษัทที่ผลิตสินค้าอุปโภคบริโภคขนาดนับชนิด มีโรงงานถึง 5 แห่ง ตั้งอยู่ทั้งในกรุงเทพและต่างจังหวัด นอกจากผลิตเพื่อจำหน่ายในประเทศแล้วยังทำการส่งออก บริษัทได้ใช้ระบบคอมพิวเตอร์ช่วยในการควบคุม การผลิตในโรงงานและการประมวลผลข้อมูลในการดำเนินงาน และช่วยในการบริหารงานขายและสินค้าคงคลังของบริษัทย่อยซึ่งจัดตั้งในรูปของห้างสรรพสินค้าซึ่งมีอยู่ 2 แห่ง

บริษัทได้เลือกใช้เครื่องคอมพิวเตอร์ IBM 9370 ซึ่งเป็นเครื่องคอมพิวเตอร์ขนาดมินิและมีการนำ Micro computer มาใช้อีกจำนวนหนึ่ง สำหรับโปรแกรมคำสั่งงานได้ใช้วิธีสั่งซื้อโปรแกรมสำเร็จรูปมาดัดแปลงใช้ให้เข้ากับงานที่ต้องการ และพัฒนาโปรแกรมส่วนหนึ่งขึ้นใช้เอง

งานด้านคอมพิวเตอร์จะอยู่ในความรับผิดชอบของศูนย์คอมพิวเตอร์ ซึ่งขึ้นอยู่กับผู้จัดการฝ่ายการเงิน (ดูผังโครงสร้างการจัดองค์กร รูป 1) และภายในศูนย์คอมพิวเตอร์มีการจัดโครงสร้างการบริหารภายในตามที่แสดงในรูปที่ 2 หัวหน้าศูนย์คอมพิวเตอร์คือ คุณพิกุลทอง ซึ่งเป็นน้องสาวของ คุณปรีชา ซึ่งเป็นรองประธานบริษัทฝ่ายการตลาด คุณพิกุลทองสำเร็จการศึกษาชั้นปริญญาตรีทางสถิติและปริญญาโททางคอมพิวเตอร์จากประเทศสหรัฐอเมริกา สำหรับ

โปรแกรมเมอร์ทั้ง 2 คน คือ คุณчим และ คุณพินท์ทั้งสองสำเร็จการศึกษาทางสถิติศาสตร์และมีประสบการณ์การทำงานในฐานะโปรแกรมเมอร์มาหลายปีสำหรับพนักงานป้อนข้อมูลเข้ามีเพียง 2 คน ก็เพราะงานส่วนใหญ่ผู้ใช้ฝ่ายต่าง ๆ เป็นผู้ป้อนข้อมูลเก็บไว้ในแผ่น Diskette ด้วยตนเองแล้วส่งเข้าประมวลผลผ่านเครื่องไมโครคอมพิวเตอร์ ซึ่งต่อเชื่อมกับเครื่อง IBM 9370 สำหรับพนักงานปฏิบัติการนั้นมีอยู่ด้วยกัน 3 คน สับเปลี่ยนเวรกันเป็นกะตามตารางการปฏิบัติงานที่กำหนดไว้

เนื่องจากงานด้านคอมพิวเตอร์เป็นเรื่องของเทคโนโลยีสมัยใหม่ ผู้บริหารระดับสูงส่วนใหญ่ไม่มีประสบการณ์ในด้านนี้ ดังนั้นการจัดการต่าง ๆ ในด้านนี้จึงเป็นหน้าที่ของคุณพิกุลทอง ที่จะเสนอเรื่องราวความต้องการต่าง ๆ ขึ้นไป และผู้บริหารระดับสูงก็มักจะอนุมัติตามที่ขอ จะพิจารณาและได้ถามเฉพาะกรณีที่ซึ่งงบประมาณจำนวนสูง เมื่อเริ่มจัดตั้งศูนย์คอมพิวเตอร์ใหม่ ๆ นั้น คุณพิกุลทองต้องยุ่งกับงานตลอดเวลาจนกระทั่งไม่มีเวลามานั่งวางแผนเป็นลายลักษณ์อักษรอย่างละเอียด และแผนลักษณะงาน (Job Description) ก็บอกแต่โดยคร่าว ๆ ว่าแต่ละคนจะต้องทำอะไรบ้าง โดยไม่ได้กำหนดรายละเอียดขอบเขตอำนาจหน้าที่ความรับผิดชอบอย่างชัดเจนและเพียงพอ และข้อห้ามปฏิบัติสำหรับแต่ละตำแหน่งงาน อย่างไรก็ตามเรื่องต่าง ๆ เหล่านี้ ไม่ได้ถูกตั้งข้อสังเกตจากฝ่ายตรวจสอบภายในแต่อย่างใด เป็นเพราะฝ่ายตรวจสอบภายในไม่เคยเข้าตรวจการดำเนินงานของศูนย์คอมพิวเตอร์ ทั้งนี้ฝ่ายตรวจสอบภายในอ้างว่าไม่มีบุคลากรที่มีความสามารถในด้านการตรวจสอบคอมพิวเตอร์อย่างเพียงพอ เท่าที่เป็นอยู่พนักงานจากฝ่ายตรวจสอบภายในจะใช้วิธีตรวจ Input กับ Report และเมื่อมีปัญหา ก็จะสอบถามจากโปรแกรมเมอร์ ซึ่งโปรแกรมเมอร์ทั้ง 2 คน พยายามชี้แจงอย่างตึงตังใจ แต่พนักงานฝ่ายตรวจสอบก็ไม่เข้าใจอย่างลึกซึ้งนัก ดังนั้นจึงไม่พยายามถามถ้าไม่จำเป็น การติดต่องานระหว่างทั้งสองฝ่ายจึงมีน้อยมาก ประกอบกับคุณพิกุลทองซึ่งเป็นคนที่ค่อนข้างเข้มงวดเคยตำหนิฝ่ายตรวจสอบที่ครั้งหนึ่งเคยตั้งข้อสังเกตข้อผิดพลาดในรายงานโดยที่ฝ่ายตรวจสอบเข้าใจผิดเอง ดังนั้นฝ่ายตรวจสอบจึงไม่พยายามตั้งข้อสังเกตนับจากนั้นมา

อย่างไรก็ดี ผู้สอบบัญชีภายนอกเคยตั้งข้อสังเกตว่า บริษัทไม่มีการวิเคราะห์ความเสี่ยงภัย และนำเทคนิคการบริหารงานอื่น ๆ มาใช้กำหนดประเภทการประกันภัยและวงเงินประกันภัยคอมพิวเตอร์ ทำให้การประกันภัยต่ำกว่ามูลค่าจริง และไม่มีการจัดทำแผนฉุกเฉินและแผนการรักษาความปลอดภัยเสนอต่อคณะกรรมการของบริษัท ซึ่งคุณพิกุลทองก็ชี้แจงกับฝ่ายบริหารเป็นการภายในว่า ถ้าจะวิเคราะห์ความเสี่ยงก็ต้องจ้างบริษัทผู้สอบบัญชีภายนอกมาประเมิน ลั่นเปลื้องค่าใช้จ่ายสูงและเธอก็คิดว่าประโยชน์ที่ได้ไม่คุ้มค่า เพราะระบบงานไม่ได้ซับซ้อนหรือเป็นระบบใหญ่โตเกินไป ความเสี่ยงที่มีอยู่ก็เป็นที่ยอมรับกันดีอยู่แล้ว สำหรับการประกันภัยคอมพิวเตอร์นั้นมีอุปกรณ์คอมพิวเตอร์ล้ำสมัยอย่างรวดเร็วและมูลค่าลดลงเร็วมาก จึงไม่ควรทำประกันภัยไว้ และยังแผนฉุกเฉินนั้นเธอก็คิดว่าไม่จำเป็นเพราะพนักงานที่ปฏิบัติงานในศูนย์คอมพิวเตอร์มีไม่กี่คน และเนื่องจากเป็นศูนย์คอมพิวเตอร์ขนาดเล็ก ทุกคนทราบหน้าที่ของตนดีอยู่แล้ว การซักซ้อมด้วยวาจาก็เป็นการเพียงพอ และที่สำคัญคือโอกาสที่จะเกิดความเสี่ยงที่ทำให้ศูนย์คอมพิวเตอร์ได้รับความเสียหายก็มีน้อยมากเพราะเมืองไทยไม่มีใครมีการจราจรหรือขว้างปาระเบิด จะมีก็แต่ปัญหาน้ำท่วม ซึ่งศูนย์คอมพิวเตอร์ก็ตั้งอยู่ที่ชั้น 3 ซึ่งไม่มีปัญหาข้อนี้อยู่แล้ว ภัยพิบัติทางธรรมชาติอื่น ๆ ประเทศเราก็ไม่มีจึงไม่น่าเป็นห่วงแต่อย่างไร

และด้วยความรำคาญที่จะต้องตอบคำถามต่าง ๆ ที่คุณพิกุลทองคิดว่าไม่น่าจะถาม ทำให้คุณพิกุลทองเรียนรู้ที่จะทำรายงานเสนอต่อผู้บริหารระดับสูงในลักษณะที่จะเสนอแต่งงานและความคืบหน้าตลอดจนความสำเร็จที่เกิดขึ้นแล้วโดยไม่พยายามอิงเปรียบเทียบกับแผนระยะสั้นปีต่อปีที่เธอวางไว้ เพราะมักจะไม่สอดคล้องกันอยู่เสมอ โดยเฉพาะงบประมาณที่มักบานปลายซึ่งจุดนี้เธอไม่สามารถหลีกเลี่ยงได้ แต่เธอก็มักมีเหตุผลที่ฟังดูสมเหตุสมผลมากกล่าวอ้างกับผู้บริหารระดับสูงได้เสมอ

ในด้านการบริหารภายในศูนย์คอมพิวเตอร์ คุณพิกุลทองก็ไม่มีใครมีเวลาอยู่ในศูนย์คอมพิวเตอร์นักเพราะต้องออกไปติดต่อธุรกิจวันอยู่ข้างนอกทุกวัน ดังนั้นเธอจึงขอเลขานุการประจำตัวหนึ่งคน ได้แก่ คุณเพ็ญพร ซึ่งคอยทำหน้าที่ต่าง ๆ เวลาเธอไม่อยู่ และเนื่องจากคุณพิกุลทองเป็นคนหัวใหม่และเชื่อมั่นว่าผู้ได้บังคับบัญชาเป็นพวกทฤษฎี Y คือ รู้จักรับผิดชอบในตัวเองและยินดีที่จะทำงานอย่างอิสระไม่ต้องการการควบคุมที่เข้มงวด โดยเฉพาะพวกโปรแกรมเมอร์ ดังนั้นเธอจึงไม่ใคร่จะกำหนดระเบียบ ข้อบังคับ หรือข้อกำหนดอะไรมากนัก โดยเธอยึดหลักความยืดหยุ่นและให้ความเป็นอิสระ และเธอเองไม่ชอบงานเอกสารที่ยุ่งยากเสียเวลา เธอจึงนิยมให้รายงานเป็นวาจาและติดต่อด้วยวาจามากกว่าเสนอรายงานหรือเอกสาร ซึ่งเธอคิดว่าไม่คล่องตัวและรวดเร็วพอ ดังนั้นลักษณะการทำงานในศูนย์คอมพิวเตอร์จึงค่อนข้างเป็นอิสระเสรี ไม่มีระเบียบหรือกฎเกณฑ์หยาบหยาบ เช่น การกำหนดระเบียบในการออกแบบระบบงาน และพัฒนาระบบงาน ระเบียบการคัดเลือกโปรแกรมสำเร็จรูป ระเบียบการจัดทำโปรแกรม หรือ ระเบียบการจัดทำเอกสารประกอบระบบงานและโปรแกรม แต่โปรแกรมเมอร์ทั้ง 2 คนก็ตกลงพูดคุยกันด้วยวาจา และเข้าใจกันดีว่าจะทำแบบไหนอย่างไรก็ดี เอกสารระบบงานและโปรแกรมก็มักจะใช้เวลาานกว่าจะทำเสร็จ ซึ่งก็เป็นธรรมดาไม่ว่าที่ไหน เพราะบรรดาโปรแกรมเมอร์ชอบหรือถนัดเขียนโปรแกรมมากกว่าคำพรรณนา นอกจากนี้ เป็นเพราะมีระบบงานที่ต้องพัฒนาให้กับคอมพิวเตอร์หลายระบบงาน โปรแกรมเมอร์จึงไม่มีใครมีเวลาแม้แต่จะทบทวนระบบงานใหม่ที่น่าออกใช้จริงแล้ว จะมีก็แต่กรณี User ประสบปัญหาและต้องการแก้ไขโปรแกรม ก็ทำเรื่องเสนอมาทางศูนย์คอมพิวเตอร์ เมื่อมีงานยุ่ง โปรแกรมเมอร์จึงเก็บเอกสารที่เกี่ยวข้องไว้และยังไม่ได้ Update เอกสารประกอบระบบงานและโปรแกรมในทันทีหลังจากที่แก้ไขโปรแกรมเสร็จแล้ว

ถึงแม้ว่าคุณพิกุลทองจะไม่ได้กำหนดระเบียบหยาบหยาบมากมาย แต่ระเบียบสำคัญที่เธอห้ามเด็ดขาดคือห้ามโปรแกรมเมอร์ไปยุ่งกับแฟ้มข้อมูลจริง แต่เธอไม่ได้ห้ามโปรแกรมเมอร์ไปยุ่งกับโปรแกรมจริงที่นำออกใช้งานแล้ว เพราะอาจต้องมีการแก้ไขโปรแกรม ซึ่งเธอไม่ได้กำหนดระเบียบไว้ตายตัว แต่กำหนดว่าต้องผ่านการอนุมัติจากเธอก่อน อย่างไรก็ตาม เนื่องจากเธอมีงานยุ่งมากจึงไม่ได้ตามไปกำกับดูแลอย่างจริงจังจึงจะมีการแก้ไขตามเอกสารหลักฐานที่แนบให้เธอเซ็นอนุมัติหรือไม่

สำหรับพวกเอกสารประกอบระบบงานและโปรแกรมทั้งที่ใช้งานจริงแล้ว และกำลังอยู่ในระหว่างการพัฒนาตลอดจนเอกสารประกอบ Operating System คุณพิกุลทองกำชับให้โปรแกรมเมอร์ถือกฎและไม่ให้พนักงานปฏิบัติการหรือพนักงานป้อนข้อมูลเข้าถึงได้

ดังที่ได้กล่าวแล้วว่าคุณพิกุลทองเธอมีฐานะมาก และไม่มีใครอยู่ในศูนย์คอมพิวเตอร์งานส่วนใหญ่เธอได้มอบให้คุณเพ็ญพรซึ่งเป็นเลขารับผิดชอบ ซึ่งคุณเพ็ญพรเองไม่ได้จบการศึกษาทางด้านเลขานุการโดยเฉพาะเธอไม่มีความรู้

ด้านคอมพิวเตอร์ การควบคุมงานภายในศูนย์เธอก็ทำไม่ได้ มีก็แต่รับการติดต่อจากภายนอก รับหนังสือเข้าออกและเสนอเจ้านายของเธอ ผลคือการควบคุมบางด้านก็หย่อนลง เช่น การจัดทำรายงานและส่งรายงานให้ผู้ใช้อ้างอิงข้อมูลล่าช้าไม่เป็นไปตามตารางเวลาที่กำหนดให้ออกรายงานแก่ผู้ใช้ ซึ่งนาน ๆ ที่เมื่อผู้ใช้นั้นมามาก ๆ คุณพิกุลทองเธอก็จะชำระความทีหนึ่งและกำชับผู้ใต้บังคับบัญชาของเธอเป็นคราว ๆ ไป สำหรับการตรวจสอบ Console log เธอก็ไม่ว่าจะทำและจะมอบให้โปรแกรมเมอร์ช่วยทำก็เป็นไปไม่ได้ เพราะโปรแกรมเมอร์มีงานยุ่งอยู่แล้ว จะให้คนอื่นดูแลก็ไม่มีใครรู้เรื่อง ผลก็คือไม่เคยมีใครตรวจดู Console log เลย

อยู่มาวันหนึ่ง คุณพิกุลทองก็ได้พาแขกของบริษัทเข้าเยี่ยมชมการดำเนินงานของศูนย์คอมพิวเตอร์ ซึ่งต้องยื่นรอลิฟท์อยู่นานเนื่องจากลูกค้าของบริษัทมีมากและไม่ว่าชั้น 1 ชั้น 2 ชั้น 4 ชั้น 5 เป็นชั้นที่เปิดรับลูกค้า และมีคนพลุกพล่านเสมอ ศูนย์คอมพิวเตอร์ของเธออยู่ชั้น 3 จึงต้องพลอยติดขัดเรื่องการจราจรระยะไกลไปด้วย เมื่อลิฟท์เปิดออกที่ชั้น 3 ก็มองเห็นป้ายตัวโตสีดำตัดทองสวยงามว่า ศูนย์คอมพิวเตอร์ และมองเห็นทะเลประดูและผนังห้องที่เป็นกระจกในและเห็นห้องกระจกชั้นในซึ่งเป็นที่ตั้งของเครื่องคอมพิวเตอร์ คุณพิกุลทองเธอก็ต้องพาแขกเบียดเสียดลูกค้าในลิฟท์ออกมา ยามซึ่งยืนเฝ้า Floor ทั้งชั้นซึ่งเป็นของศูนย์คอมพิวเตอร์ ซึ่งเข้าเวรทีละคนก็รีบทำความเคารพ แล้วเดินวนกลับไปอีกทางหนึ่งซึ่งเป็นห้องน้ำ คุณพิกุลทองยิ้มและอธิบายแนะนำสถานที่กับแขก เธอหยิบบัตรออกมาเสียบที่ประตู และกล่าวว่าศูนย์คอมพิวเตอร์ของบริษัทได้ใช้ระบบรักษาความปลอดภัยเป็นอย่างดีมีการใช้บัตรแสดงตัว ซึ่งในบัตรมีข้อมูลระบุตัวผู้ถือบัตรเฉพาะจึงจะมีสิทธิเข้าไปในห้องคอมพิวเตอร์ได้หากเอาบัตรที่มีแถบแม่เหล็กทั่วไปมาใช้ เช่น บัตร ATM ก็ไม่สามารถใช้ได้ คุณพิกุลทองได้เดินนำเข้าไป โดยจับประตูไว้ให้แขกเข้าตามมา ขณะที่ประตูกำลังจะปิดอย่างเชื่องช้านั้น ก็มีแขกคนหนึ่งซึ่งมัวแต่หันไปมองวิวที่เป็นสระว่ายน้ำของโรงแรมที่อยู่ข้าง ๆ ลืมเดินตามเข้ามารีบคว้าประตูไว้แล้วผลุบตามมาโดยไม่พยายามทำเสียงดังให้ใครหันมา เพราะเกิดความเขิน ซึ่งก็ไม่มีใครสังเกตเห็นความผิดปกตินั้นคุณพิกุลทองได้อธิบายต่ออีกว่าศูนย์คอมพิวเตอร์โดยทั่วไปต้องจ้างพนักงานเฝ้าที่เคาน์เตอร์ทางเข้าคอยลงสมุดบันทึกว่าใครเข้ามาเวลานั้นและลงลายมือชื่อ แต่ที่นี่ไม่จำเป็นเพราะเมื่อเสียบบัตรที่ประตู ระบบจะบันทึกทันทีว่าใครเข้ามาเวลาใดประหยัดพนักงานได้ 1 คน

เมื่อเห็นคุณพิกุลทองพาแขกเดินเข้ามาหลายคน คุณเพ็ญพรซึ่งเป็นเลขานุการก็รีบกระวีกระวาดออกมาต้อนรับ คุณพิกุลทองก็สั่งให้เอาน้ำชากาแฟและของว่างมาต้อนรับ คุณเพ็ญพรรับคำสั่งแล้วก็รีบผลุนผลันไปทันที เพราะเผอิญเพิ่งจะนึกได้ว่ากาแฟเหลืออยู่พอซังเพียงแก้วเดียว คุณเพ็ญพรรีบเดินกึ่งวิ่งผลุนผลายออกไปทางห้องน้ำซึ่งเปิดออกสู่ข้างนอกตะโกนเรียกยามให้ไปบอกแม่บ้านขอพวกของว่างที่เป็นขนมหรือผลไม้ แล้วเธอก็ผลุบกลับเข้ามาและตรงไปที่ห้องเล็ก ๆ ทำห้องกระจกซึ่งกันแบ่งห้องเล็ก ๆ เก็บพวกชากาแฟและน้ำร้อนน้ำเย็นเพื่อสำรวจดูว่าน้ำร้อนมีพร้อมหรือยัง อารามรีบเก็บทำให้เธอสะดุดหกล้มกับกองกระดาษที่สูงเป็นภูเขาย่อม ๆ มีทั้งเอกสาร แบบฟอร์มเปล่า รายงานต่าง ๆ เธอบ่นพึมพำหลังจากที่ใจหายไปแวบหนึ่ง พลังนึกในใจว่าถ้าไฟจะไหม้ก็คงเป็นเพราะเจ้ากองกระดาษเหล่านี้ เมื่อตรวจดูว่าน้ำร้อนเรียบร้อยแล้ว เธอก็รีบสาวเท้าลงบันไดข้างหลังไปยังชั้นสองเพื่อขอยืมกาแฟจากเพื่อนสาว

ทางฝ่ายคุณพิกุลทองเมื่อนำแขกเข้ามาในศูนย์คอมพิวเตอร์แล้วก็พาแขกตรงไปที่ห้องทำงานของเธอแล้วบรรจงหยิบสมุดเล่มสวยให้แขกลงนามว่าได้เข้าเยี่ยมชมศูนย์คอมพิวเตอร์เมื่อใด หลังจากนั้นก็พาแขกออกชมภายในบริเวณศูนย์คอมพิวเตอร์แบ่งเป็นส่วน ๆ (ดูรูปที่ 3 Lay out ภายในศูนย์คอมพิวเตอร์) เธอไม่พยายามเดินพาแขกไปท้ายของ

ศูนย์คอมพิวเตอร์ เพราะมีเอกสารกองอยู่อย่างไม่เป็นระเบียบ เมื่อออกจากห้องของเธอ เธอจึงพาแขกที่ชมภายในห้องกระจกที่ตั้งเครื่องคอมพิวเตอร์ ที่ประตูทางเข้าไม่มีพนักงานเฝ้าและไม่ต้องเสียบบัตรผ่าน ไม่มีทะเบียนบันทึกชื่อผู้เข้าออก มีแต่ตารางเวรว่าพนักงานปฏิบัติงานใดต้องอยู่เวร เมื่อคุณพิกุลทองดูรายชื่อ ซึ่งได้แก่ นายสมชาย และนายสมปอง แต่คุณพิกุลทองกลับเห็นนายสมชายกับนายพินิจ และเห็นโปรแกรมเมอร์คือคุณชิมอยู่ในห้องนั้นด้วย ซึ่งคุณพิกุลทองก็ขมวดคิ้วแต่ก็ไม่พูดว่าอะไร เธอถามนายสมชายว่านายสมปองไปไหน นายสมชายตอบว่า นายสมปองแลกเวรกับนายพินิจ คุณพิกุลทองก็ไม่ได้ว่าอะไรและหันไปอธิบายกับแขก คุณชิมเดินเข้ามาต้อนรับ คุณพิกุลทอง จึงแนะนำแล้วถามพลางเล็กคิ้วว่าคุณชิมทำอะไรอยู่ คุณชิมบอกว่าเขามาตรวจดูโปรแกรม คุณพิกุลทองจึงถามว่า เครื่องเทอร์มินัลที่ห้องโปรแกรมเมอร์เสียหรือ คุณชิมตอบว่าไม่ แต่มาขอให้พนักงานปฏิบัติการ Load โปรแกรมให้ คุณพิกุลทองก็ไม่ว่าอะไร เมื่อเดินไปที่ห้องเก็บสื่อ (Media) เธอก็ต้องขมวดคิ้วเมื่อเห็นประตูเปิดอยู่ สำหรับห้องนี้เธอไม่ได้พาแขกเข้า คงให้ยืนดูอยู่ที่ประตู เมื่อมองเข้าไปเธอก็เห็นพวกเทปต่าง ๆ วางระเกะระกะอยู่ และบางม้วนก็ไม่มีป้ายชื่อกำกับ บางม้วนป้ายก็หลุดห้อยแขวนอยู่ มีแขกคนหนึ่งถามว่า Media พวกนี้มีการตรวจนับบ้างหรือไม่ คุณพิกุลทองยกไหล่อย่างเฉลือดัว ตอบพลางยิ้มหวานว่า ไม่จำเป็นต้องมีการตรวจนับ เพราะไม่มีใครจะหยิบเทปพวกนี้ออกไปได้เพราะเธอเก็บกุญแจห้องเก็บเทปไว้เอง มีแขกอีกคนหนึ่งถามว่าหากมีปัญหาเกิดขึ้นกับพวกข้อมูลโปรแกรม หรือแม้แต่ตัวคอมพิวเตอร์จะทำอย่างไร คุณพิกุลทองก็ยิ้มพลางตอบว่าที่ศูนย์คอมพิวเตอร์มีการ Back up ข้อมูลโปรแกรมไว้อีกชุดหนึ่งที่เก็บไว้ทุกวัน และสามารถหยิบใช้ได้ทันที สำหรับเครื่องคอมพิวเตอร์ถ้ามีปัญหา บริษัท IBM สามารถเข้ามาแก้ไขได้ทันที กรณีไฟดับก็มี UPS (Uninterrupted Power System) ภายในห้องคอมพิวเตอร์การยกพื้นอยู่แล้วเมื่อมีปัญหาไฟไหม้ก็มีน้ำยาดับเพลิงโดยเฉพาะ ว่าพลางก็ชี้ให้ดูเครื่องดับเพลิง และยังชี้ให้ดูเครื่องวัดอุณหภูมิและความชื้น และก้มลงชี้ที่พื้นขณะที่ดวงตาอันคมกริบของคุณพิกุลทองก็เลื้อยไปเห็นเศษบุหรี่ยี่สิบซองที่ซอกขาโต๊ะและเห็นคราบเป็นดวงราวกับน้ำชาหกหน้าที่ยืมแยมของเธอจึงเปลี่ยนไป ขณะที่กำลังจะออกจากห้องก็มีแขกคนหนึ่งถามว่าทำไมต้องมีไฟฉายไว้ในห้องคอมพิวเตอร์ คุณพิกุลทองเองก็ลงไปชั่วคราว เธอหันไปถามพนักงาน ปฏิบัติการ ซึ่งก็ตอบว่าเอาไว้เผื่อไฟดับ

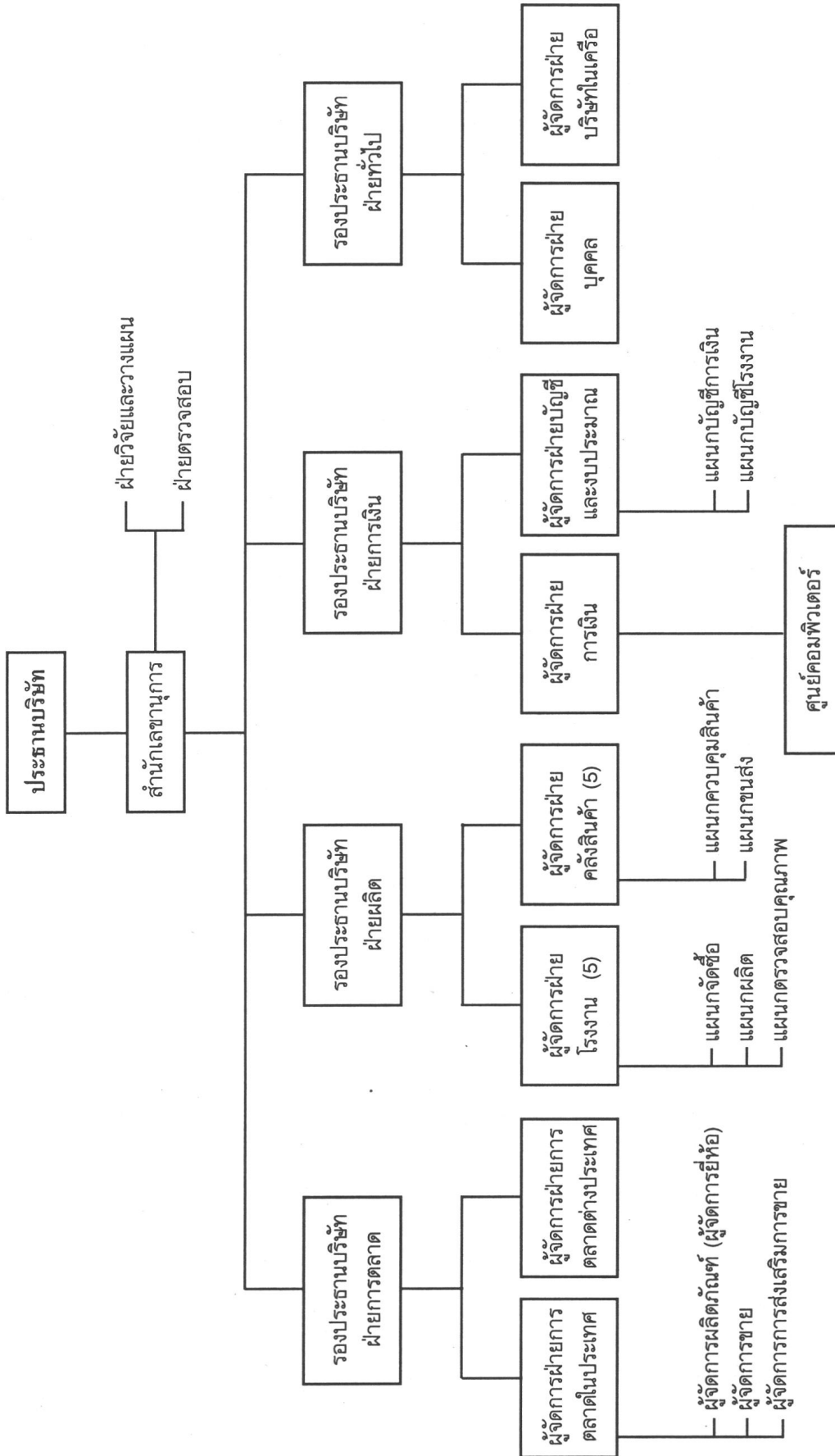
เมื่อออกจากห้องคอมพิวเตอร์ เธอก็พาแขกไปดูห้องเตรียมข้อมูลแล้วก็นำไปนั่งที่ห้องประชุมระหว่างเดินผ่านห้องคอมพิวเตอร์ชั้นในเธอก็เห็นเจ้าหน้าที่ของ IBM กำลัง่วนอยู่กับเครื่อง แยกที่เดิมตามมาก็ถามว่าเครื่องขัดข้องหรือ คุณพิกุลทองจึงสอบถามกับคุณเพ็ญพร ซึ่งเดินมากระซิบน้าชากาแฟและของว่างเตรียมเสร็จแล้ว ก็เชิญคุณพิกุลทองกับแขกไปรับประทานได้ คุณเพ็ญพรจึงตอบว่าเจ้าหน้าที่ของ IBM มาทำ PM (Preventive Maintenance) คุณพิกุลทองจึงถามด้วยความสงสัยว่าทำไมมาเวลานี้ เธอจำได้ว่าตามตารางเวลาที่ตกลงกันไม่ใช่เวลานี้ คุณเพ็ญพรจึงตอบเจ้าหน้าที่ IBM มาไม่แน่นอนบางทีก็ช้าเป็นเดือน คุณพิกุลทองจึงบอกว่าถ้าแขกกลับแล้วให้เอาทะเบียนบันทึกการทำ PM และการแก้ไขกรณีเครื่องขัดข้องมาให้เธอดู ซึ่งคุณเพ็ญพรก็รับคำ

หลังจากที่แขกพากันกลับไปหมดแล้ว คุณพิกุลทองตรวจดูทะเบียนทั้งสอง ซึ่งเธอก็พบว่าเป็นอย่างที่เลขาของเธอแจ้งให้ทราบ และการบันทึกการแก้ไขกรณีเครื่องขัดข้องก็ไม่มีใครเป็นระเบียบนัก ไม่มีการบอกรายละเอียดว่าเสียนานเพียงใดถี่ห่างแค่ไหน และมีสาเหตุเพราะอะไรตลอดจนทำการแก้ไขอย่างไร โดยใครและใครรับผิดชอบดูแลระหว่างที่เจ้าหน้าที่ของ IBM มาทำการแก้ไขข้อขัดข้อง บางหน้าก็บอกแต่ไม่ครบถ้วน ขณะที่อ่านอยู่เธอก็นึกถึงเรื่องหนึ่งขึ้นมาได้ เธอจึงหันไปถามเลขาว่ากุญแจห้องเก็บสื่อที่เธอสั่งให้เก็บไว้อยู่ไหน คุณเพ็ญพรก็ยิ้มพลางตอบว่าได้มอบให้พนักงานปฏิบัติ

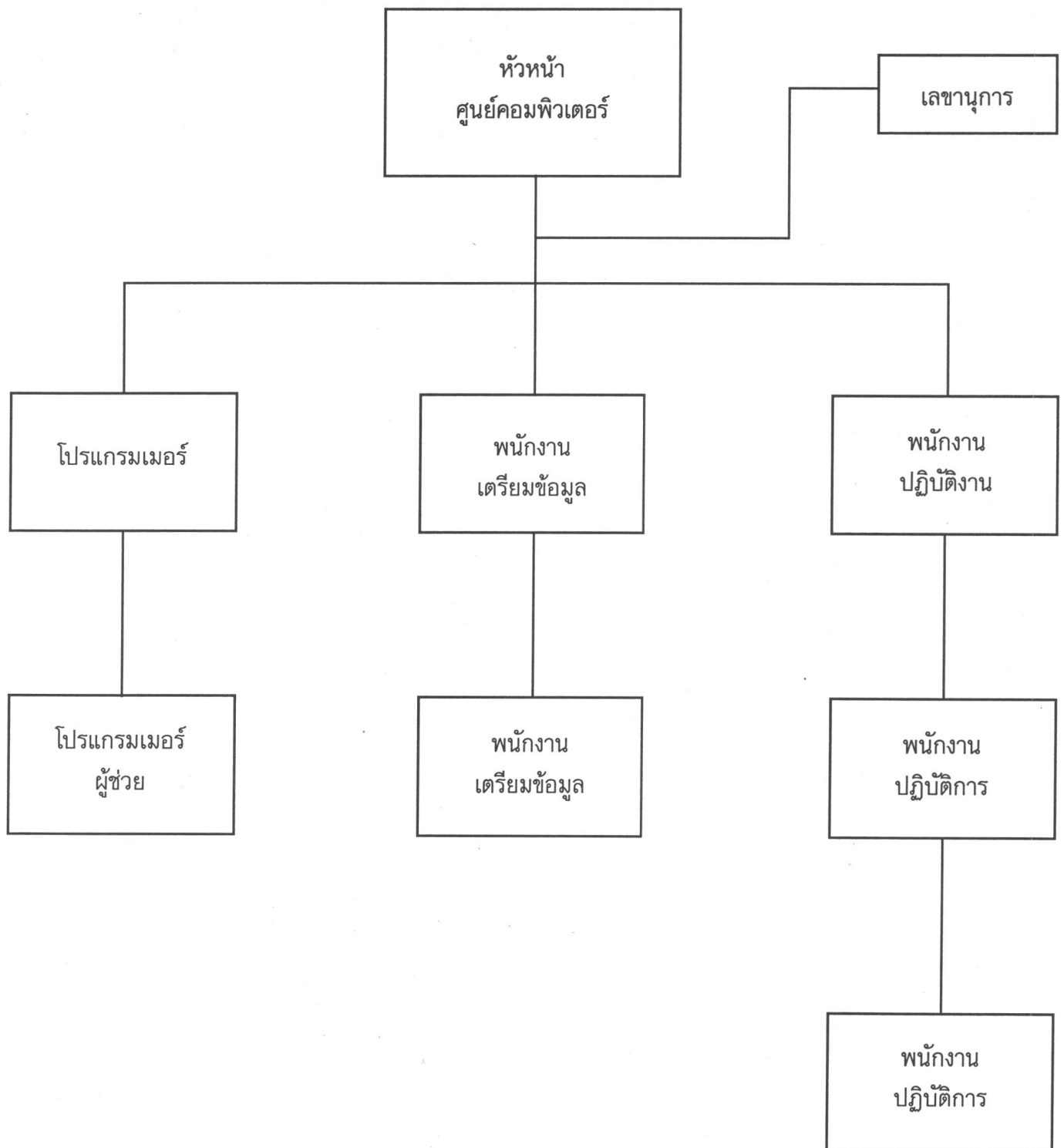
การนำไปใช้ คุณพิกุลทองจึงถามว่าคุณเพชรตามไปดูหรือไม่ว่าพนักงานปฏิบัติการหยิบแฟ้มข้อมูลใดมาใช้บ้าง คุณเพชรก็ตอบว่าไม่ได้ดูเพราะเธอทำตามที่คุณพิกุลทองปฏิบัติอยู่ เพราะคุณพิกุลทองเองก็ใช้วิธีให้กุญแจพนักงานปฏิบัติการไปเปิดหยิบแฟ้มข้อมูลเอง แล้วเธอก็ทำสีหน้าหงายสงสัยและถามว่าเธอทำอะไรผิดหรือไม่ คุณพิกุลทองก็ถอนใจเฮือก แล้วก็บอกให้เธอไปนั่งที่ ในทันใดนั้นเธอก็ถามคำถามออกมาว่าแล้วกุญแจห้องเก็บเอกสารและกุญแจตู้เก็บเอกสารสำคัญ ซึ่งเก็บพวก Program listing และพวกข้อมูล Back up ต่าง ๆ และโปรแกรมสำรอง คุณเพชรก็ตอบว่าก็ให้พวกพนักงานปฏิบัติการใช้เปิดห้องและเปิดตู้เพื่อเก็บพวก Back up เหล่านั้นทุกวัน เธอให้กุญแจไปทั้งชุด แต่ไม่ได้ให้โปรแกรมเมอร์เลยตามที่คุณพิกุลทองเคยกำชับไว้

คุณพิกุลทองนั่งหลับตาลงอย่างเหนื่อยอ่อน เธอรู้สึกว่ปัญหาบางอย่างเริ่มก้าวเข้ามาหาเธอแล้ว

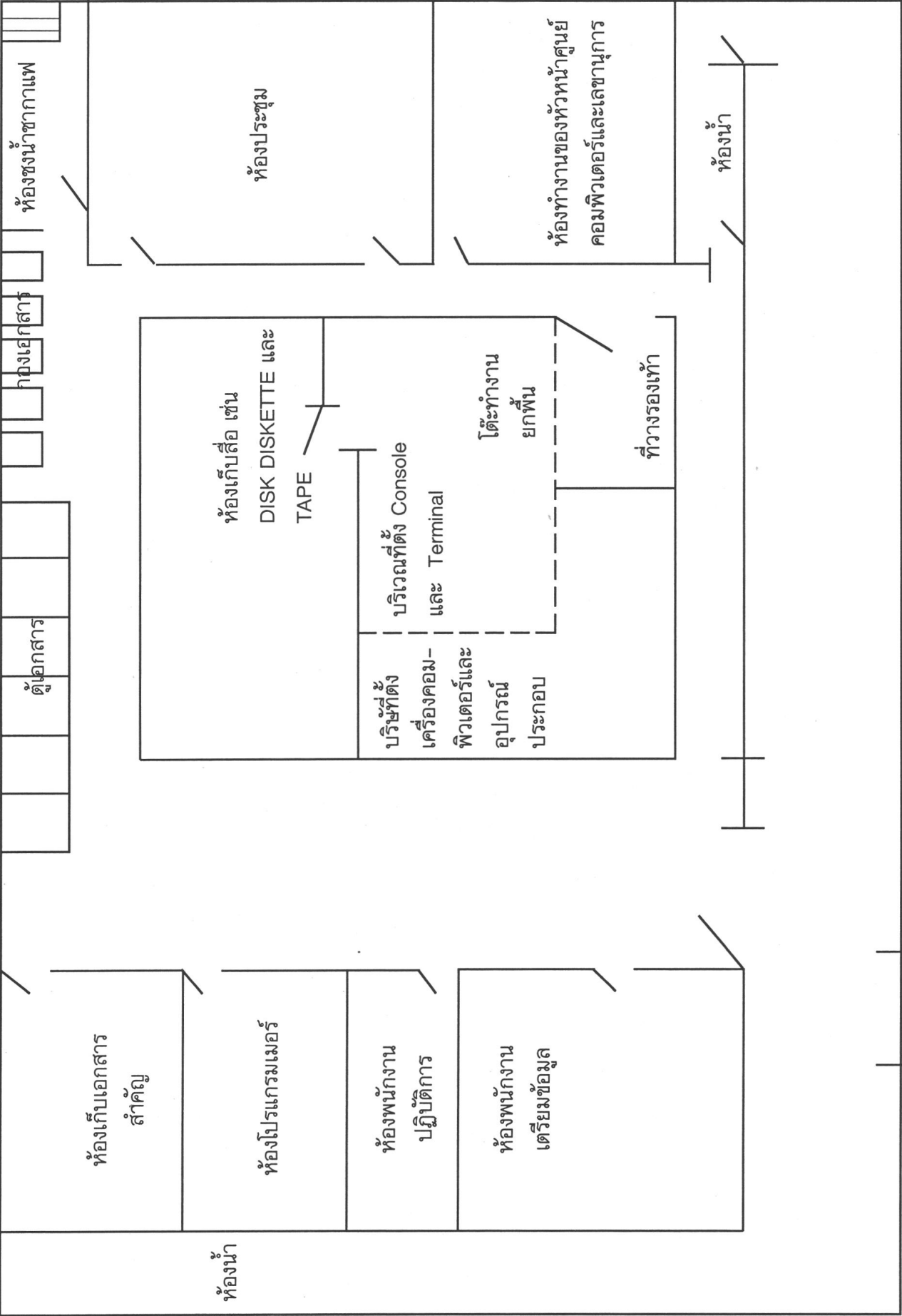




รูป 1 โครงสร้างการจัดองค์การ



รูป 2 โครงสร้างภายในของศูนย์คอมพิวเตอร์



รูป 3 Layout ภายในศูนย์คอมพิวเตอร์

ลิฟท์

กรณีศึกษา 7

บริษัท เอส.เอ.อินเตอร์เทรด จำกัด

ภาค 2

ขณะที่คุณพิกุลทองนั่งพักหลับตาได้ชั่วครู่ ก็มีโทรศัพท์ดังขึ้น คุณเพ็ญพรเลขาคนสวยรีบตรงเข้าไป และกล่าวว่าผู้จัดการฝ่ายตรวจสอบภายในขอพูดสายด้วย คุณพิกุลทองจึงคว้าโทรศัพท์ขึ้นรับอย่างว่องไว

“ฮัลโล..สวัสดีค่ะ..ดิฉันพิกุลทองค่ะ....อ้อ....หรือค่ะ....พวกผู้สอบบัญชีภายนอกเขาจะขอเข้าตรวจด้านคอมพิวเตอร์อย่างละเอียดในคราวนี้ด้วยหรือค่ะ...ทั้งตรวจสอบศูนย์คอมพิวเตอร์และระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ หรือค่ะ...ค่ะ...เอ๊ะ แล้วจะเข้าตรวจเมื่อไรค่ะ...อ้อ...อีกสองวันหรือค่ะ..ก็เป็น วันพฤหัสบดีค่ะ จะต้องมีการบรรยายสรุปเกี่ยวกับระบบงานที่ใช้คอมพิวเตอร์ประมวลผลให้พวกเขาฟังด้วยหรือค่ะ...ได้ซิค่ะ ดิฉันคิดว่าดิฉันจะให้โปรแกรมเมอร์ที่เตรียมสรุปเรื่องที่จะต้องฟรีเซ็นท์ให้ผู้สอบบัญชีฟัง และตัวดิฉันเองจะขอนำเรื่องด้วยการพูดถึงการนำคอมพิวเตอร์เข้ามาใช้เมื่อเริ่มแรกและพูดถึงเรื่องทั่ว ๆ ไป...ค่ะ...ขอบพระคุณมากนะคะที่กรุณาแจ้งให้ทราบล่วงหน้าจะได้ทันเตรียมตัว...ค่ะ...สวัสดีค่ะ”

เมื่อวางโทรศัพท์ลงแล้ว คุณพิกุลทองก็รีบสั่งให้เลขาไปตามตัวคุณчимและคุณพินท์มาด่วน เพื่อมอบหมายให้เตรียมตัวในการบรรยายสรุปให้บรรดาผู้สอบบัญชีภายนอกฟังภายในสองวันข้างหน้า

ภายในห้องประชุมมีบุคคลหลากหลายตานั่งเรียงรายกันอยู่ ผู้จัดการฝ่ายตรวจสอบนั่งเป็นประธานอยู่กลางโต๊ะ และเริ่มแนะนำบุคคลต่าง ๆ เริ่มจากทางขวามือของตน แต่ก่อนที่จะแนะนำผู้อื่น ผู้จัดการฝ่ายตรวจสอบก็เอ่ยแนะนำตัวเองก่อน ด้วยการโน้มศีรษะลงและเอ่ยด้วยเสียงดังกังวาน

“สวัสดีครับทุกท่าน วันนี้กระผมในฐานะตัวแทนบริษัท ใคร่ขอกล่าวต้อนรับบรรดาคณะผู้สอบบัญชี ซึ่งก็ได้กลับมาเยี่ยมเยียนเราอีกครั้งเป็นประจำแบบนี้ทุกปี ผมชื่อ ณรงค์ หากมีอะไรให้ผมรับใช้เชิญได้เสมอไม่ต้องเกรงใจ ถัดจากผมไปนะครับคือ ผู้ช่วยผู้จัดการฝ่ายตรวจสอบ คุณอัศวิน ถัดไปนะครับคือคุณฤชา และคุณพิทยา ซึ่งเป็นหัวหน้าหน่วยตรวจสอบทั้งสองหน่วยที่เรา มี และตัวแทนซึ่งเป็นสุภาพสตรีคนเดียวของเราในที่นี้คือ คุณพิกุลทอง หัวหน้าศูนย์คอมพิวเตอร์ และโปรแกรมเมอร์ทั้งสองของเราคือคุณчимและคุณพินท์ครับ คราวนี้คงต้องขอเชิญคุณศุภศิริ หัวหน้าผู้สอบบัญชีแนะนำทุกท่านในที่นี้ละนะครับเชิญครับคุณศุภศิริ”

“ครับขอบคุณครับ กระผมในนามของทีมตรวจสอบรู้สึกมีความยินดีที่ได้พบปะและรู้จักทุกท่าน ซึ่งคงต้องอาศัยทุกท่านในการให้ความร่วมมือ สำหรับทีมงานของกระผมนี้ได้แก่ คุณสุปรีย์ คุณภาคนิย และคุณธนียะครับ พวกกระผมทั้งหมดจะทำการตรวจสอบในด้านที่เน้นไปทางระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ ซึ่งต้องเรียนขอความกรุณาท่านผู้จัดการฝ่ายตรวจสอบและท่านหัวหน้าศูนย์คอมพิวเตอร์ บรรยายสรุปเรื่องระบบงานต่าง ๆ ที่ประมวลผลด้วยคอมพิวเตอร์ และการนำคอมพิวเตอร์เข้ามาใช้ของบริษัทด้วยนะครับ”

“ครับ...เรื่องนี้ทางเราได้รับทราบความประสงค์ของท่านผู้สอบบัญชีทั้งหลาย และทางคุณพิกุลทองจะได้บรรยายสรุปในเรื่องดังกล่าวให้ได้ทราบต่อไป เชิญคุณพิกุลทองครับ”

“สวัสดีค่ะ ทุกท่าน ดิฉันรู้สึกเป็นเกียรติและมีความยินดีที่จะได้ให้ความร่วมมือแก่ทุกท่านในเรื่องที่ดิฉันรับผิดชอบอยู่ ในการนำคอมพิวเตอร์มาใช้ของบริษัทนั้น เริ่มตั้งแต่เมื่อเริ่มตั้งบริษัทในปี 2530 เราใช้เครื่อง IBM รุ่น 9370 และมีการนำ Micro Computer เข้ามาใช้บางส่วน เรามีโครงการว่าจะเชื่อมต่อไมโครคอมพิวเตอร์ในลักษณะของ LAN (Local Area Network) เอาละค่ะ ดิฉันคิดว่าได้เสนอเรื่องราวความเป็นมาและการนำระบบคอมพิวเตอร์เข้ามาใช้พอสมควรแล้วนะคะ ต่อไปคุณชมและคุณพินท์จะได้มาเล่าให้เราฟังถึงรายละเอียดในด้านระบบงาน เชิญคุณชมค่ะ”

“สวัสดีครับ ในเรื่องของระบบงานนั้น เรานำคอมพิวเตอร์มาใช้กับหลายระบบงานก่อนอื่นผมของสรุปภาพรวมให้เห็นว่าเรามีการใช้คอมพิวเตอร์กับระบบงานใดบ้าง ดังที่ทุกท่านได้ทราบกันดีอยู่แล้วว่าบริษัทของเรามีการผลิตสินค้าอุปโภคบริโภคมากมายหลายชนิด และยังทำหน้าที่จำหน่ายเองทั้งในด้านตลาดภายในประเทศและตลาดต่างประเทศ โรงงานเพื่อการผลิตมีทั้งที่อยู่ในเขตกรุงเทพฯ และต่างจังหวัด นอกจากนี้ เรายังมีบริษัทในเครือซึ่งเป็นห้างสรรพสินค้า และคอมพิวเตอร์ที่เราได้ใช้เพื่อบริการกับบริษัทในเครือด้วย ดังนั้น ในการพัฒนาระบบงานได้พยายามให้เป็นประโยชน์แก่ทุก ๆ ฝ่าย และเป็นไปโดยมีประสิทธิภาพ และประสิทธิผล ระบบงานที่ได้พัฒนามาใช้ระบบคอมพิวเตอร์แล้วคือ ระบบงานขาย ระบบงานซื้อ ระบบงานผลิต เป็นระบบงานในลักษณะ ON LINE IN HOUSE และระบบงานจ่ายเงิน ระบบงานเงินเดือน เป็นระบบงาน BATCH”

แล้วคุณชมก็ได้นำเสนอรายละเอียดของแต่ละระบบงานโดยคร่าว ๆ ซึ่งก็เป็นไปตาม Flow chart แนบทั้งนี้ เพื่อช่วยให้ผู้สอบบัญชีเข้าใจโดยง่าย การฟรีเซ็นท์ในวันนั้นได้รับความสำเร็จโดยดี และผู้สอบบัญชีก็รู้สึกพอใจที่ได้ทราบข้อมูลเบื้องต้นที่จำเป็นเพื่อใช้ในการดำเนินการตรวจสอบต่อไป และได้ยื่นแบบรายการขอเอกสารที่จะใช้ในการตรวจสอบ ปรากฏว่ามีเอกสารบางรายการที่ศูนย์คอมพิวเตอร์ไม่อาจจัดให้ได้ เนื่องจากไม่เรียบร้อย และบางรายการก็ไม่ได้ทำไว้เลยอย่างไรก็ดี คุณศุภศิริได้ขอเอกสารเท่าที่มี เพื่อจะได้สามารถดำเนินการตรวจสอบต่อไปได้ โดยไม่เสียเวลารอ และได้เกริ่นการจะขอเข้าเยี่ยมชมและตรวจสอบศูนย์คอมพิวเตอร์อีกด้วยรวมถึงการใช้เทคนิคการตรวจสอบโดยอาศัยคอมพิวเตอร์เข้าช่วย ซึ่งอาจต้องรบกวนเวลาทำงานเครื่องคอมพิวเตอร์ของทางบริษัท เอส.เอ.อินเตอร์เทรด และอาจต้องขอให้เจ้าหน้าที่ของศูนย์คอมพิวเตอร์ช่วยเหลือในการดังกล่าวด้วย

รุ่งเช้าวันต่อมา ทีมผู้สอบบัญชีภายนอกก็ได้เข้าปฏิบัติงานตรวจสอบในรายละเอียด คุณศุภศิริได้มอบหมายให้คุณสุปรีย์ รับผิดชอบในการตรวจสอบระบบงานขายและรับเงิน คุณภาคนิษฐ์รับผิดชอบในการตรวจสอบระบบงานซื้อและจ่ายเงิน และคุณธนียะรับผิดชอบระบบงานผลิตและช่วยในการตรวจสอบศูนย์คอมพิวเตอร์ ซึ่งคุณศุภศิริเป็นผู้รับผิดชอบ

ผลจากการตรวจสอบพบว่า

ระบบงานขายและรับเงิน

1. เพื่อความสะดวกได้อนุญาตให้พนักงานขายทุกคนสามารถรับคำสั่งซื้อและป้อนข้อมูลได้เลยโดยตรง ทั้งนี้ มีการแจ้ง Password ให้พนักงานขายทราบ มีระเบียบแจ้งให้มีการเปลี่ยน Password เป็นระยะ ๆ แต่ส่วนใหญ่ไม่มีใครต้องการเปลี่ยนเพราะคุ้นเคยและจำ Password เก่าจนขึ้นใจอยู่แล้ว และจากการทำ Test Data พบว่าระบบจะฟ้องเมื่อมีการเปลี่ยน Password มาเหมือนกัน โดยขึ้นเป็นข้อความเตือน และยังสามารถใช้ Password ดังกล่าวได้ต่อไป
2. ในการอนุมัติเครดิตในการขายนั้น ได้กำหนดไว้ในโปรแกรมให้เช็คสอพบเพิ่มข้อมูลลูกค้าว่ามีการให้วงเงินเครดิตไว้เท่าใด และให้ไปแล้วเท่าใด สำหรับในกรณีที่มีการซื้อเกินจำนวนวงเงินเครดิตและผู้จัดการขายเห็นสมควรผู้จัดการขายก็อาจใช้ Password ของตนเองอนุมัติให้พนักงานขายทำการได้
3. จากการตรวจสอบในรายละเอียดพบว่า มีการป้อนหน่วยของสินค้าผิดพลาดเสมอ ๆ เนื่องจากบริษัทมีการขายให้ลูกค้าทั้งรายเล็กและรายใหญ่ ทั้งตลาดในประเทศและต่างประเทศจึงทำให้เกิดความสับสนในเรื่องของหน่วยของปริมาณการสั่งซื้อของลูกค้า และในกรณีการป้อนราคาต่อหน่วยก็เช่นกัน
4. เนื่องจากบริษัทมีสินค้าอยู่มากมายหลายชนิด ดังนั้น การเปลี่ยนแปลงด้านราคาขายจึงเกิดขึ้นอยู่เสมอ ๆ เมื่อมีการเปลี่ยนแปลงราคาขาย จะมีผู้มีอำนาจทำการอนุมัติ และต้องมีการใช้ Password ของผู้มีอำนาจในการทำรายการ ผลจากการทำ Test Data พบว่า โปรแกรมมีการเช็คสอพบรหัสสินค้าใน Master file ให้ตรงกับหมายเลขของสินค้าที่ต้องการเปลี่ยนราคาขาย และยังเช็คสอพบราคาเก่าว่าถูกต้องตรงกันอีกด้วย รวมทั้งวันที่จะให้มีผลบังคับใช้ นอกจากนี้ มีการออกรายงานแสดงการเปลี่ยนแปลงราคาของสินค้าเหล่านั้นให้ทราบ เพื่อทำการตรวจทานอีกด้วย
5. บัญชีลูกหนี้ มีการกำหนดหมายเลขประจำตัว ซึ่งมีการใช้ Check digit ในแบบของ Modulus 10 และมีการใช้ตัวถ่วงน้ำหนักตัวท้ายเป็น 5
6. เมื่อมีการจัดส่งของให้แก่ลูกค้า แผนกส่งของจะส่งใบส่งของให้แก่แผนกขายเพื่อป้อนข้อมูลเข้าสู่คอมพิวเตอร์ กรณีที่มีการเปลี่ยนแปลงจำนวนของที่จัดส่งไปยังลูกค้า ไม่ว่าจะส่งมากหรือน้อยกว่าที่ลูกค้าต้องการ ก็จะทราบได้ในทันที (ใบส่งของมีการ Running number ไว้ล่วงหน้า)
7. จากการตรวจสอบรายงานที่สั่งพิมพ์เพื่อแสดงรายละเอียดในแฟ้มข้อมูลรายการสั่งซื้อ พบว่ามีรายการสั่งซื้อจากลูกค้าที่ค้างอยู่เป็นเวลานานหลายรายการ ซึ่งจากการสอบถามพบว่าบางรายการเป็นเพราะไม่มีของ แต่อีกหลายรายการไม่สามารถชี้แจงเหตุผล
8. สำหรับการขายของห้างสรรพสินค้า 2 แห่ง ซึ่งเป็นบริษัทในเครือกัน พบว่าเนื่องจากมีสินค้ามากมายหลากหลายชนิด ปัญหาที่มักเกิดขึ้นคือ การป้อนข้อมูลรายละเอียดของสินค้าผิดพลาด และสร้างปัญหาให้ ผู้ตรวจสอบภายในซึ่งมักตรวจพบว่ามีสินค้าไม่ตรงกับตามที่บันทึกไว้ในบัญชี

9. มีการจำหน่ายบัญชีลูกหนี้ที่ค้างอยู่และไม่เคลื่อนไหวเป็นเวลานาน โดยผ่านการเห็นชอบจากคณะกรรมการที่เกี่ยวข้องและมีหลักฐานการอนุมัติโดยแนชด์ กรณีที่มีการเรียกเก็บได้ในภายหลัง ได้มีการติดตามเพื่อบันทึกเป็นรายได้โดยครบถ้วน สำหรับบัญชีลูกหนี้ที่เริ่มไม่เคลื่อนไหวเป็นระยะเวลาหนึ่ง โปรแกรมจะทำการล๊อคไว้ เมื่อจะทำรายการใด ๆ ต้องใช้ Password จากผู้มีอำนาจผ่านรายการ

10. กรณีที่มีการรับคืนสินค้าจะมีการบันทึกแบบฟอร์มเอกสารที่มีการลงหมายเลขสำคัญล่วงหน้า และมีรายละเอียดการคืนประกอบ และมีทะเบียนควบคุมรายการ

11. ในการทำ Batch total เอกสารการรับชำระหนี้ มีการพิจารณายอดรวมจำนวนรายการและยอดรวมจำนวนเงิน ซึ่งในบางครั้งพบว่ารายละเอียดไม่ถูกต้อง แต่หักกลบลบกันได้ถูกต้องตรงกับยอดรวมที่ใช้สอบยันกัน และผลจากการส่งยืนยันยอดลูกหนี้ มีลูกหนี้ตอบมาว่ายอดหนี้คงค้างไม่ถูกต้องหลายราย

ระบบงานซื้อและจ่ายเงิน

1. การปรับปรุงเพิ่มข้อมูลผู้ขายไม่มีใครเป็นปัจจุบัน เนื่องจากพนักงานระดับล่างมีงานในมือหลายอย่างทำให้ไม่มีเวลาปรับปรุงทันทีที่มีการเปลี่ยนแปลงข้อมูลเกี่ยวกับผู้ขาย

2. มีปรากฏอยู่บ่อยครั้งว่า รายการของที่ได้รับมาซึ่งตรงกับรายละเอียดใบสั่งซื้อแต่กลับไม่ตรงกับของที่จำเป็นต้องใช้และขาดอยู่ ซึ่งปรากฏอยู่ในรายงานสินค้าที่ต้องสั่งซื้อ

3. มีรายการสั่งซื้อจำนวนไม่น้อย ซึ่งยังไม่ได้รับของและค้างพัสดุอยู่ในแฟ้มข้อมูลเป็นเวลานานทีเดียว ซึ่งทางแผนกคลังสินค้ามักทวงถามมายังแผนกจัดซื้อเสมอ ซึ่งแผนกจัดซื้อก็มักต้องถามกลับไปยังแผนกคลังสินค้าเสมอว่าเป็นรายการสั่งซื้อสินค้าอะไร ซึ่งทำให้แผนกคลังสินค้าไม่ใคร่พอใจในประสิทธิภาพการทำงานของแผนกจัดซื้อนัก

4. พนักงานรับของพบว่าตนได้ตรวจนับและรับของจากผู้ขายถูกต้องตรงกับใบสั่งซื้อของเสมอ แต่เมื่อส่งให้แผนกคลังสินค้าแล้วพบว่า ถูกแผนกคลังสินค้าทวงกลับมาบ่อยครั้งว่าไม่ตรงกับความต้องการที่ร้องขอไป

5. เมื่อมีการพิมพ์เช็คจ่ายแล้ว จะส่งให้แก่ผู้รักษาเงินเพื่อเตรียมชำระให้แก่เจ้าหนี้ผู้ขายต่อไปผลจากการยืนยันยอดเจ้าหนี้พบว่า เจ้าหนี้บางรายตอบว่ายอดหนี้คงค้างมีสูงกว่าที่ปรากฏในจดหมายยืนยันยอด และเจ้าหนี้บางรายตอบว่ามียอดหนี้คงค้างน้อยกว่าที่ปรากฏในจดหมาย

ระบบงานผลิต

1. จากการสุ่มตรวจนับสินค้า ตามรายงานซึ่งให้ส่งถึงรายการสินค้า ซึ่งระบุตามสถานที่จัดเก็บปรากฏว่า ยอดจำนวนสินค้าที่ได้จากการตรวจนับไม่ตรงกับที่บันทึกไว้ในบัญชีหลายรายการ

2. แผนกคลังสินค้ามีปัญหาเรื่องการจัดเก็บค่อนข้างมาก เพราะมีเนื้อที่จัดเก็บไม่ค่อยจะเพียงพออยู่ตลอดเวลา มีพนักงานบ่นว่ามีวัตถุดิบและสินค้าหลายชนิดที่ค้างอยู่ไม่มีการเบิกจ่ายเป็นเวลานาน ๆ แต่ก็มีการจัดเก็บเป็นจำนวนมาก และไม่มีใครคิดจะจัดการหรือปรับปรุงอย่างใด

3. ในการควบคุมต้นทุนด้านการผลิต ระบบคอมพิวเตอร์มีการจัดพิมพ์รายงานแสดงต้นทุนการผลิตที่ต่างจากที่ประมาณการไว้ แต่ปรากฏว่าแผนกวางแผนการผลิตซึ่งรับรายงานดังกล่าวไปก็ไม่ได้ใส่ใจเท่าที่ควร เนื่องจากรายงานมีความสลับซับซ้อน ดูแลทำความเข้าใจยาก ต้องเสียเวลาเป็นอันมาก

4. ในกรณีที่มีการเปลี่ยนแปลงรายละเอียดข้อมูลในแฟ้มข้อมูลวัตถุดิบ วัสดุ แฟ้มข้อมูลต้นทุนมาตรฐาน แฟ้มข้อมูลสินค้า แฟ้มข้อมูลงานระหว่างทำ (ซึ่งไม่ใช่กรณีการโอนตัดหรือเพิ่มรายการอัตโนมัติ เมื่อมีการ Transfer รายการตามที่ตั้งไว้ในโปรแกรม) ได้มีการกำหนดให้ผ่านการอนุมัติจากผู้มีอำนาจในระดับที่สมควร และมีการสอบทานรายงานการเปลี่ยนแปลงดังกล่าวโดยรัดกุม

ระบบงานเงินเดือน

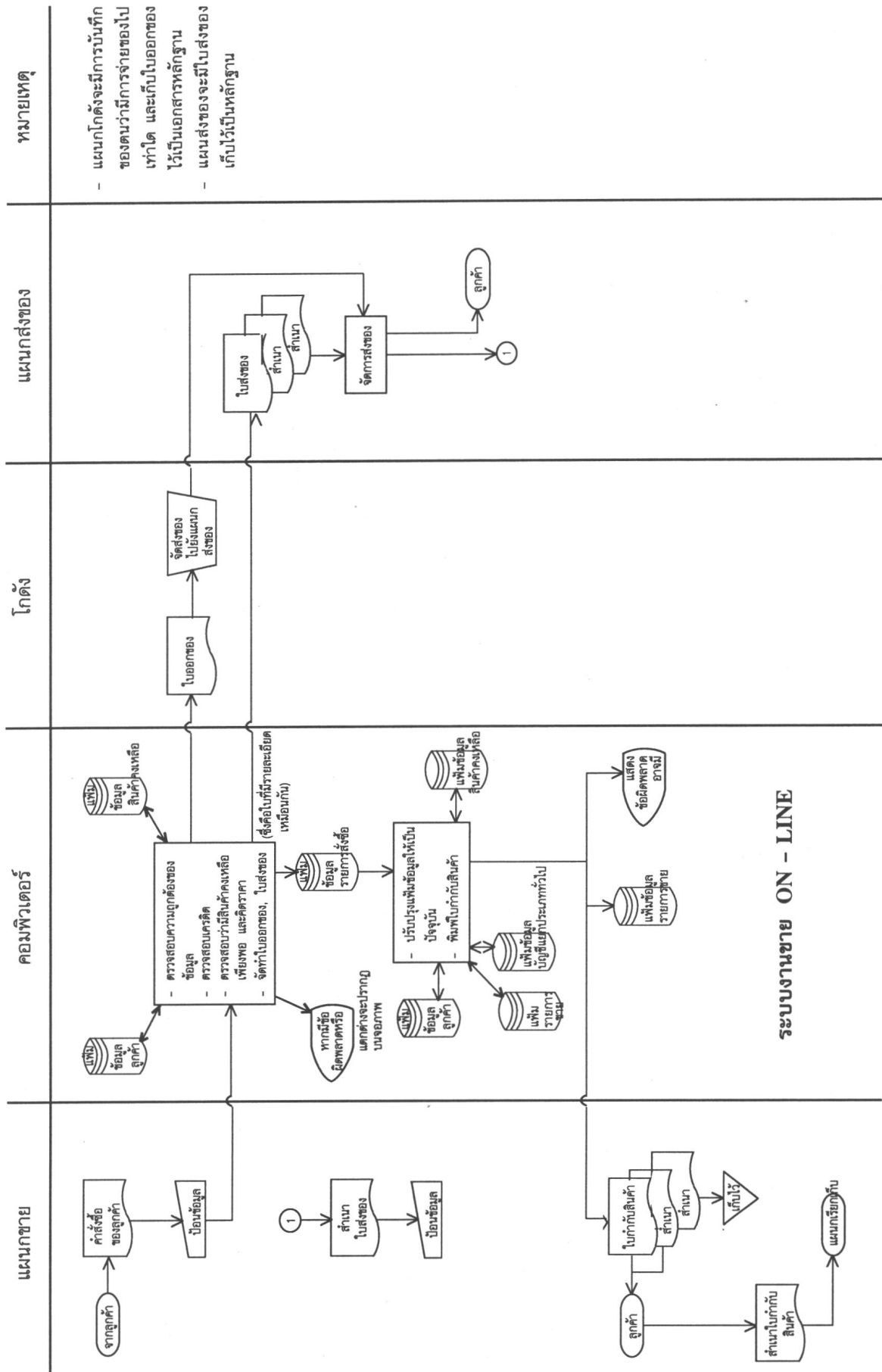
1. พบว่ามีการทวงตังจากพนักงานและลูกจ้างอยู่บ่อยครั้งถึงยอดเงินเดือนจ่ายซึ่งผิดพลาด แต่เมื่อตรวจสอบกับยอดคุมตาม Batch total พบว่ายอดรวมถูกต้อง

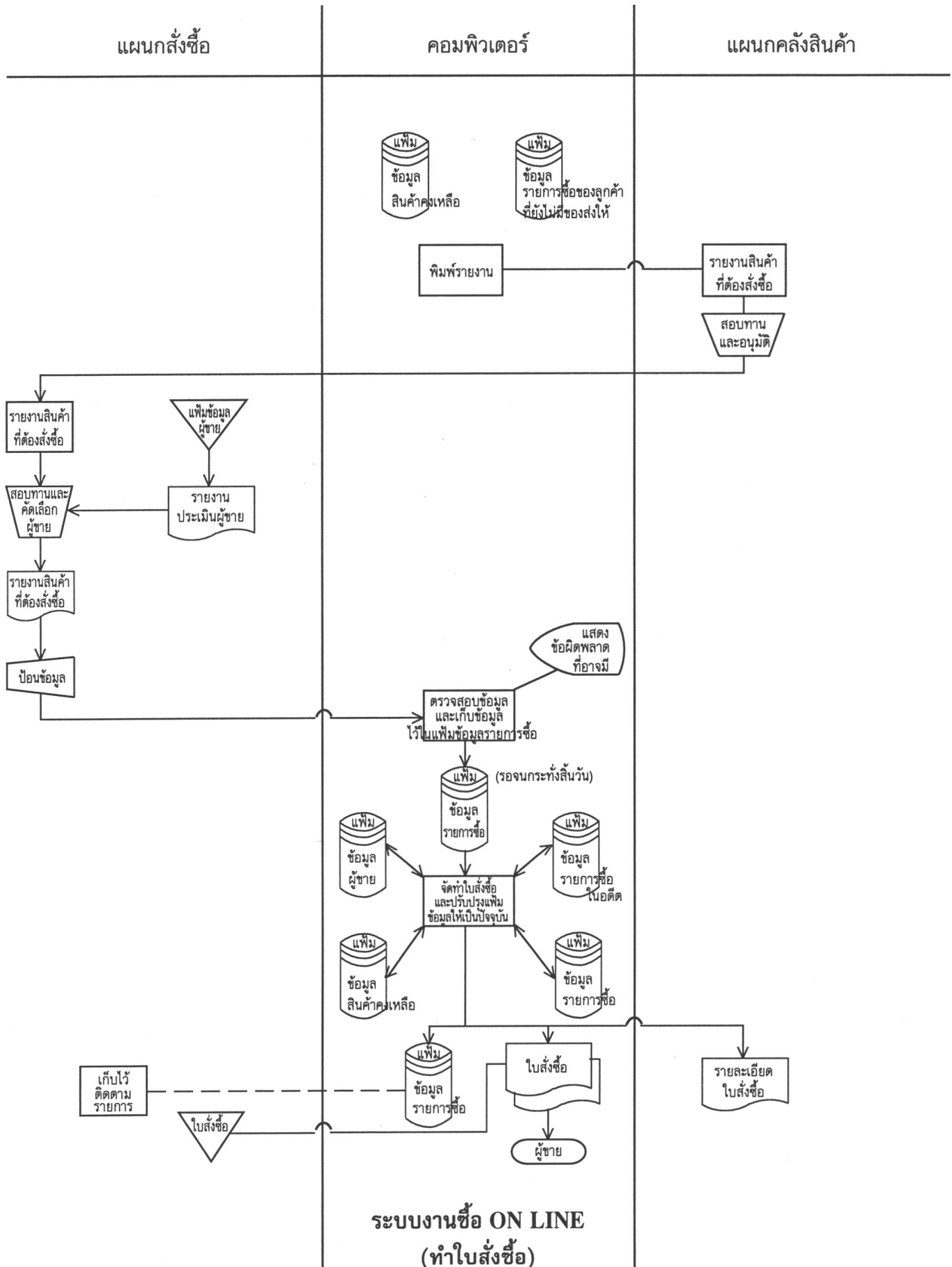
2. ในการเปลี่ยนแปลงอัตราค่าแรง จะต้องใช้ Password ของผู้มีอำนาจ และมีการออกรายงานเพื่อตรวจสอบอีกครั้งว่า การเปลี่ยนแปลงอัตราค่าแรงดังกล่าวเป็นไปตามที่ต้องการและที่อนุมัติ

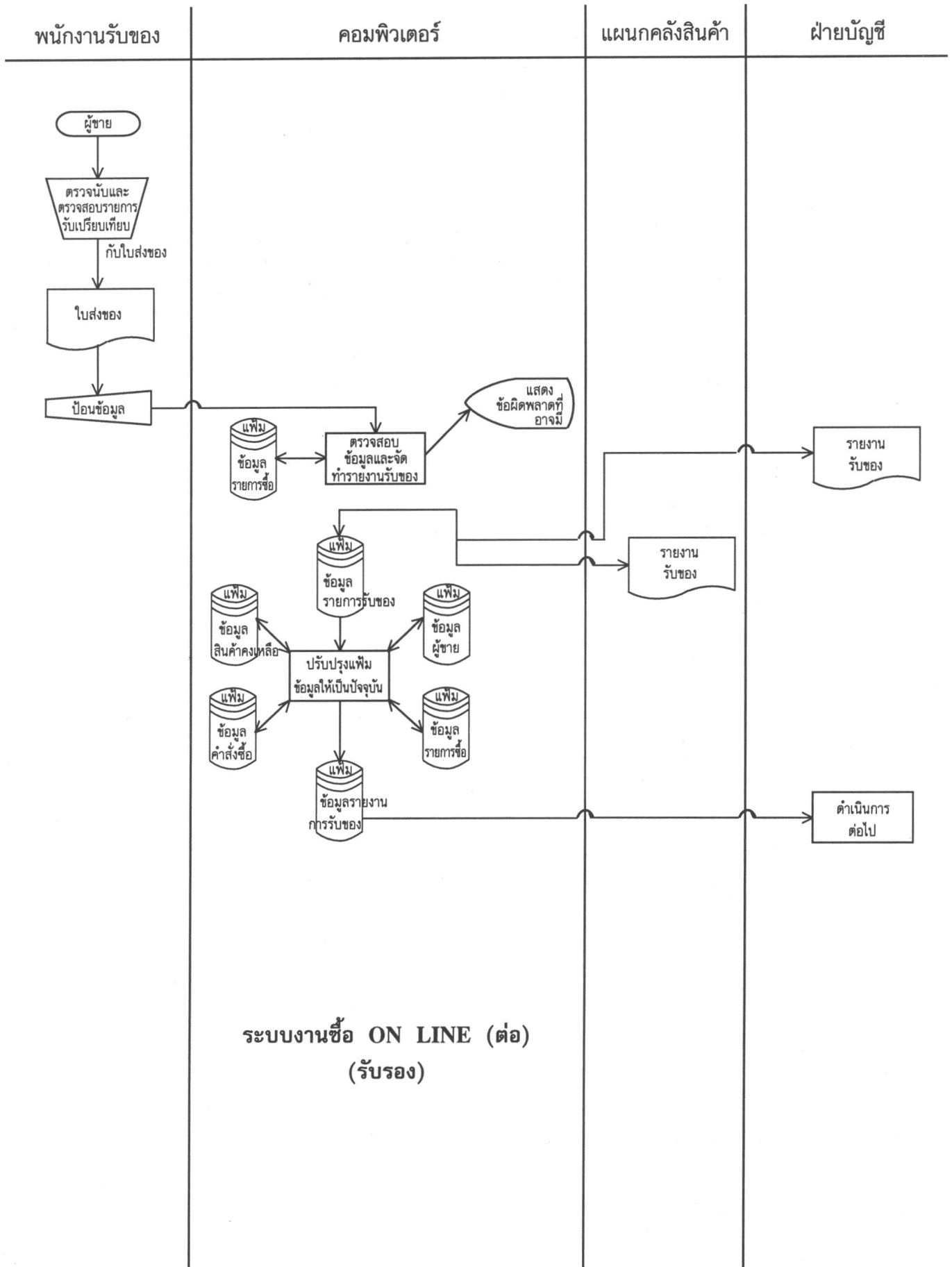
3. ใบบันทึกเงินเดือนมีรายละเอียดค่อนข้างน้อย กล่าวคือ ออกเพียงยอดเงินเดือนรวมและภาษีและยอดเงินเดือนสุทธิ

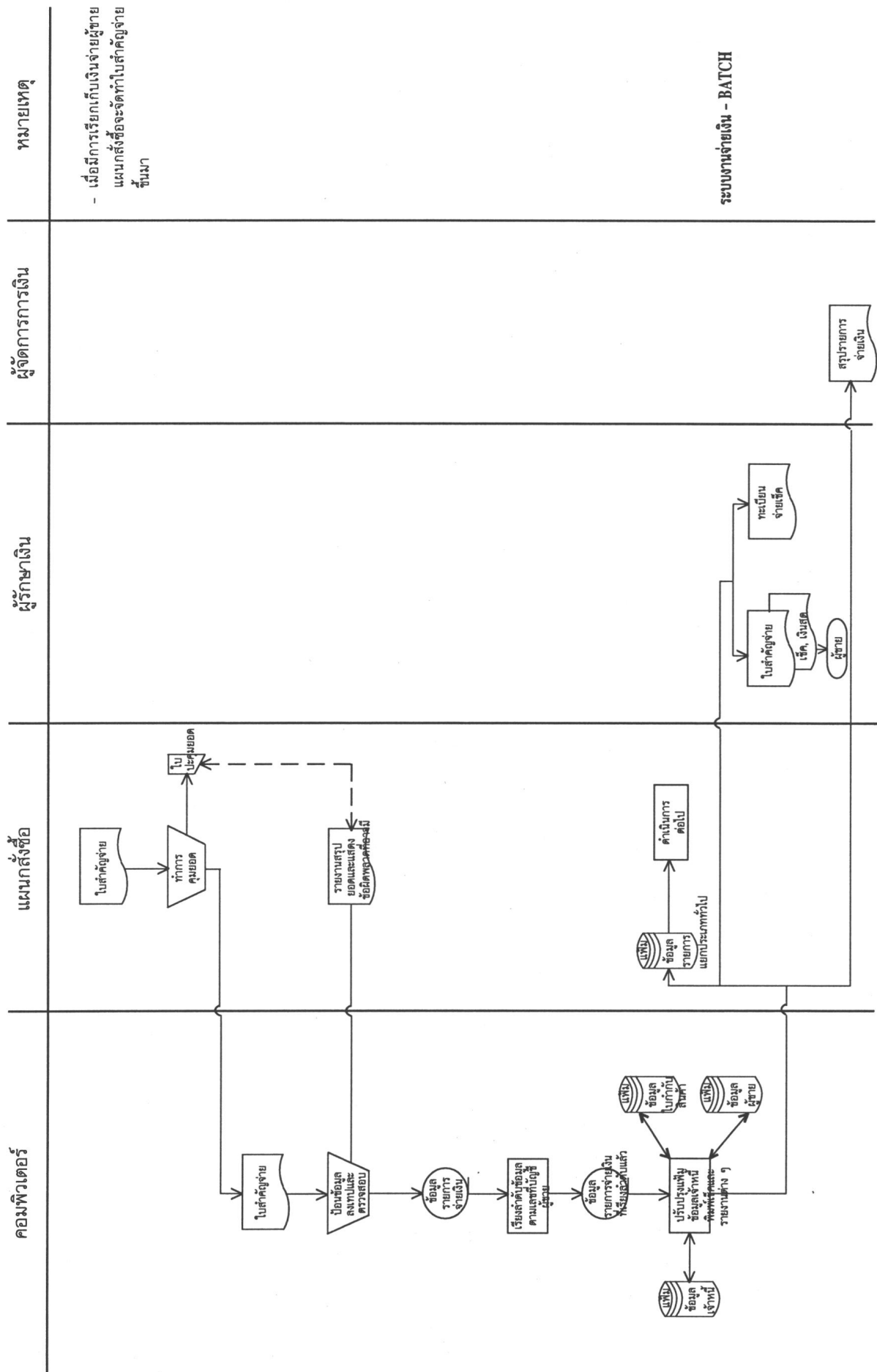
วัตถุประสงค์ : เพื่อใช้ฝึกหัดวิเคราะห์จุดอ่อนต่าง ๆ หรือความเสี่ยง โดยให้ระบุถึงความเสี่ยงที่คาดว่าจะอาจเกิดขึ้นจากจุดอ่อนต่าง ๆ เหล่านั้น และควรเสนอแนะแนวทางแก้ไขจุดอ่อนดังกล่าวด้วย

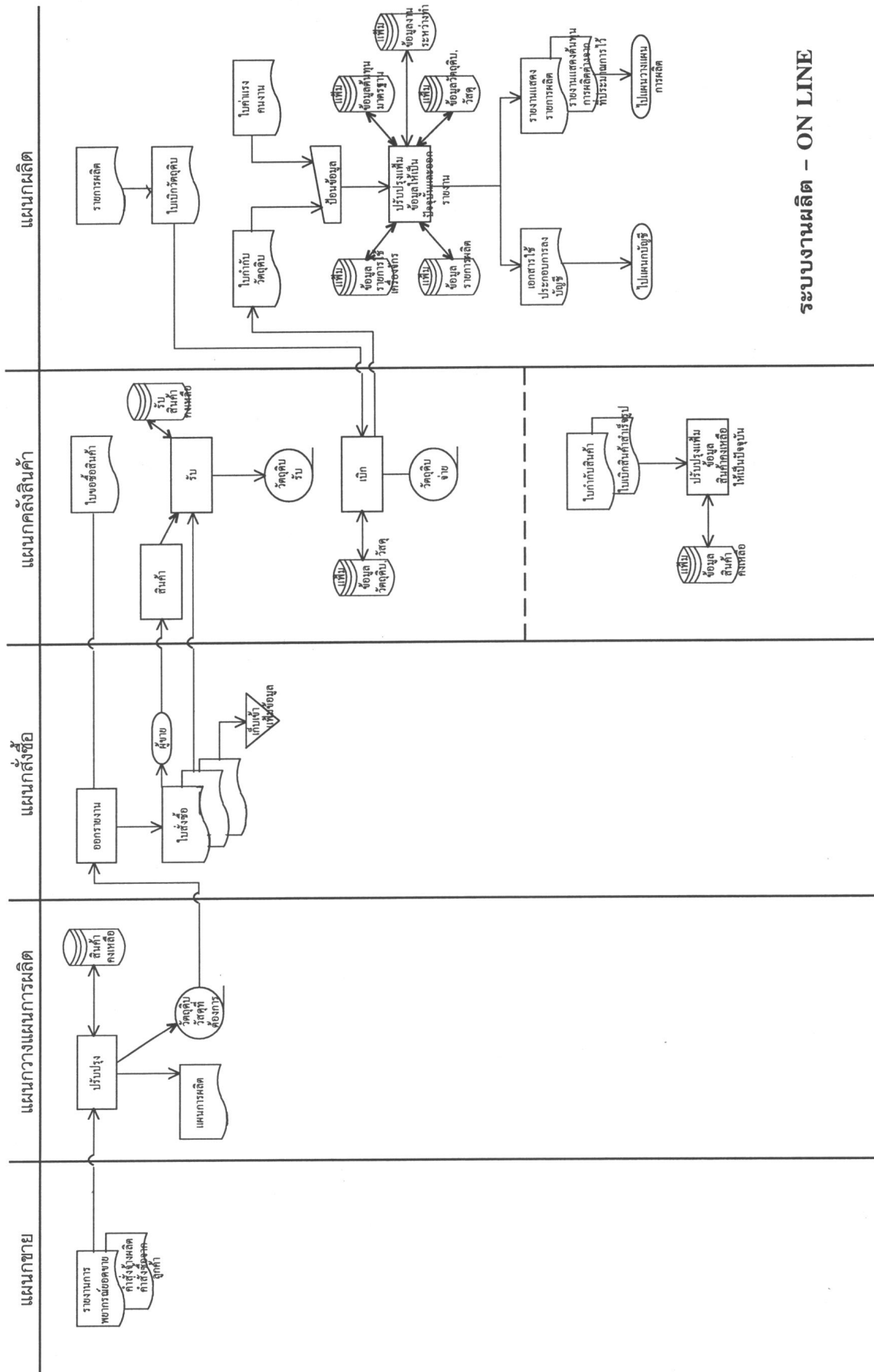


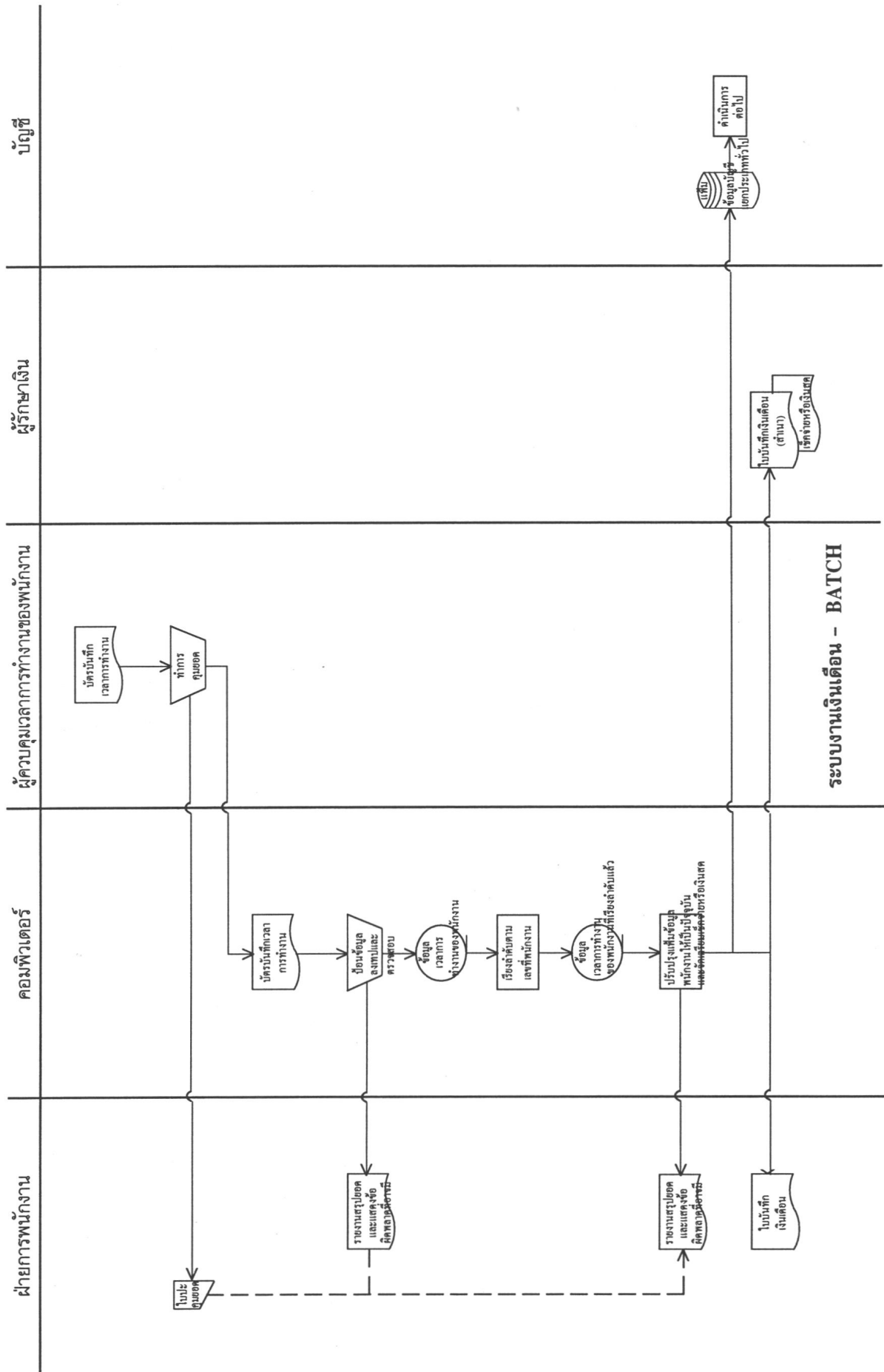












กรณีศึกษา 8 - Data Center

บริษัท ชื่อดัง จำกัด

บริษัท ชื่อดัง จำกัด เป็นบริษัทขนาดกลางค่อนข้างเล็ก มีทำการอยู่ร่วมกับอาคารบ้านพักอาศัยของเจ้าของกิจการ บริษัทนำเครื่องคอมพิวเตอร์มาใช้ในการประมวลผลงาน ซึ่งติดตั้งอยู่ในห้องหนึ่งต่างหากมีขนาดใหญ่โตนัก และจัดให้มีพนักงานประจำทั้งเจ้าหน้าที่เกี่ยวข้องโดยเฉพาะ

วันนี้เจ้าของกิจการนัดกับ นายชาญชัย เพื่อนสนิทไว้ว่าจะพาชมห้องคอมพิวเตอร์ เมื่อถึงเวลาที่นัดหมาย นายชาญชัยก็มาถึงพอดี หลังจากที่นั่งพักคุยกันที่ห้องรับแขกสักครู่ เจ้าของจึงพาไปที่ห้องคอมพิวเตอร์

ที่ประตูทางเข้า นายชาญชัย สังเกตเห็นเครื่องเสียบบัตรติดอยู่ ซึ่งเจ้าของอธิบายว่าใช้สำหรับตรวจสอบบัตรของผู้ที่ได้รับอนุญาตให้เข้ามาในห้อง แทนการใช้กุญแจเปิดประตู นายชาญชัย นึกขึ้นมาได้ว่าตนเองมีบัตร ATM ติดกระเป๋าไปด้วย จึงอยากจะนำมาทดลองใช้ดู แต่บังเอิญเหลือบไปเห็นประตูห้องเปิดอยู่แล้ว โดยมีเครื่องดับเพลิงขนาดเล็กค้ำอยู่ เลยได้แต่นึกเสียดายอยู่ในใจที่ไม่ได้ทดลองใช้บัตร ATM ระหว่างที่เดินเข้าไปภายในห้องได้เหลือบไปเห็นเครื่องดับเพลิงอีกอันหนึ่งขนาดใหญ่กว่าอันแรก ติดอยู่กับฝาผนังข้างหลังตู้ขนาดใหญ่ เนื่องจากนายชาญชัยเป็นพนักงานขายของตัวเองแทนจำหน่ายเครื่องดับเพลิง จึงอยากรบว่าเพื่อนใช้หรืออะไร ทำให้ต้องเรียกคนงานมาช่วยยับยั้งกระเถิบออกมาซึ่งต้องใช้เวลาอยู่หลายนาที และพบว่าที่เครื่องดับเพลิงมีกระดานแผ่นหนึ่งมีข้อความว่าได้ทดสอบแล้ว เมื่อเดือนมิถุนายน พ.ศ. 2520

หลังจากนั้น นายชาญชัย เดินไปที่ท้ายห้อง พบว่ามีหน้าต่างบานใหญ่เปิดอยู่ มองออกไปข้างนอกเป็นทางเดินแคบ ๆ เสียบบังไม่มีผู้คนพลุกพล่าน ลมพัดเย็นสบาย เจ้าของกิจการเล่าให้ฟังว่าเปิดไว้ระบายอากาศและควันจากห้องครัวที่อยู่ติดกัน ส่วนอีกด้านหนึ่งของห้องเป็นประตูเปิดไปสู่ห้องเก็บอุปกรณ์ และเอกสารต่าง ๆ ที่เปิดไว้อยู่ตลอดเวลา นายชาญชัยจึงเดินเข้าไปดู เห็นบรรณารักษ์นั่งหันหลังอยู่ในห้องหนึ่งคน เขาไม่ทันเห็นเจ้าของและนายชาญชัย และไม่สนใจว่าจะมีใครเดินเข้า-ออกบ้างระหว่างนั้น พนักงานห้องเครื่องเดินมาหยิบเทปข้อมูล 2 ม้วน จากกองม้วนเทปที่มุมพื้นห้อง ซึ่งล้วนแต่เป็นเทปข้อมูลชุดสำรองของสัปดาห์ที่แล้ว นายชาญชัยสังเกตเห็นสมุดเซ็นรับม้วนเทปที่นำไปใช้งานวางอยู่บนโต๊ะ เมื่อเปิดดูพบว่ารายการสุดท้ายลงวันที่เมื่อต้นสัปดาห์ก่อนหลังจากนั้นได้เดินกลับไปที่ห้องเครื่องคอมพิวเตอร์อีกครั้งหนึ่ง พบว่าที่ผนังห้องมีกระดานแผ่นใหญ่แขวนอยู่จดข้อความต่าง ๆ ไว้มากมาย ได้แก่ ตารางการประมวลงาน ชื่อพนักงานอยู่เวร รหัสลับ (Password) สำหรับเข้าถึงระบบงาน และหมายกำหนดการประชุม เป็นต้น

เมื่อเยี่ยมชมห้องคอมพิวเตอร์จนทั่วแล้ว เจ้าของกิจการถามนายชาญชัยว่า ห้องคอมพิวเตอร์เป็นอย่างไรบ้าง ใช้ได้ไหม

ให้ท่านช่วยนายชาญชัย ระบุดูอ่อนของการควบคุมภายใน ความเสียหายที่อาจเกิดขึ้นและเสนอแนะการควบคุมที่เหมาะสมมาเป็นข้อ ๆ

กรณีศึกษา 9

บริษัท ภาพสวย จำกัด

บริษัท ภาพสวย จำกัด ตั้งอยู่ที่อำเภอเมือง จังหวัดเชียงใหม่ เป็นบริษัทจำหน่ายภาพทั้งแบบป๊อปปี้และส่งด้วยเงินเชื่อ โดยให้ลูกค้าสั่งซื้อทางไปรษณีย์ มีคุณโสภเป็นพนักงานต้อนรับ คุณวิไลเป็นพนักงานบัญชี และคุณตริงตราทำหน้าที่รับ-จ่ายเงิน (Cashier) และเป็นเลขานุการด้วย

บริษัทนำเครื่องคอมพิวเตอร์มาใช้ในการบันทึกจำนวนสินค้า การขาย และการรับชำระค่าสินค้า ซึ่งเครื่อง terminal ทุกเครื่องจะใช้แฟ้มข้อมูลและ CPU ร่วมกัน

ขั้นตอนในการปฏิบัติงาน มีดังนี้

1) ลูกค้าจะมีคำสั่งซื้อเข้ามาทางไปรษณีย์ประมาณ 15-20 รายต่อวัน คุณโสภจะเป็นผู้เปิดซองคำสั่งซื้อซึ่งเป็นแบบฟอร์มของบริษัท แล้วส่งต่อให้คุณวิไล

2) คุณวิไล จะจัดทำใบกำกับสินค้า (Sale Invoice) ขึ้นมา 4 ชุด เพื่อจัดส่งและเก็บที่หน่วยงานต่าง ๆ ดังนี้

- | | |
|----------------|--|
| ชุดที่ 1 | เก็บไว้ที่แผนกบัญชี จัดเรียงตามลำดับอักษรชื่อลูกค้า |
| ชุดที่ 2 และ 3 | ส่งไปยังแผนกรับ-ส่งสินค้า |
| ชุดที่ 4 | ส่งไปยังห้องเก็บสินค้า และถือเป็นใบอนุมัติการจ่ายสินค้าออกจากแผนก เมื่อห้องเก็บสินค้าได้รับแล้ว จะจัดส่งสินค้าพร้อมกับใบกำกับสินค้าชุดที่ 4 นี้ ไปยังแผนกรับ-ส่งสินค้า |

แผนกรับ-ส่งสินค้า จะบันทึกการตัดยอดสินค้าจาก Stock ผ่านทางเครื่อง terminal ของแผนก เมื่อได้จัดส่งสินค้าไปให้ลูกค้า และในทำนองเดียวกันเมื่อได้รับสินค้าจากการสั่งซื้อ ก็จะทำบันทึกการเพิ่มยอดสินค้าใน Stock เช่นกัน การบันทึกจะบันทึกรหัสประเภทสินค้า และจำนวนหน่วย หากไม่ Key วันที่ระบบงานจะถือว่าวันที่ในระบบงาน (System Date) เป็นวันที่กำเนิดรายการ

3) เมื่อแผนกรับ-ส่งสินค้าได้รับใบกำกับสินค้าชุดที่ 2 และ 3 จะเก็บไว้รอจนกว่าจะได้รับสินค้าและใบกำกับสินค้าชุดที่ 4 จากห้องเก็บสินค้า ทางแผนกจัดส่งสินค้าจะสอบยันความถูกต้องตรงกันของใบกำกับสินค้าชุดที่ 2, 3 กับชุดที่ 4 แล้วจัดส่งสินค้าให้ลูกค้า พร้อมทั้งแนบใบกำกับสินค้าชุดที่ 3 ลงไปด้วย แล้วจึงประทับตรา “ส่งสินค้าแล้ว” ในใบกำกับสินค้า ก่อนส่งชุดที่ 2 กลับคืนไปให้คุณวิไล ส่วนใบกำกับสินค้าชุดที่ 4 จะเก็บไว้ที่แผนกเรียงตามหมายเลขของเอกสาร

4) คุณวิไล จะตรวจสอบความถูกต้องของใบกำกับสินค้าชุดที่ 1 และ 2 แล้วบันทึกการขายผ่านเครื่อง terminal ของแผนก ซึ่งจะผ่านเข้าบัญชีแยกประเภทที่เกี่ยวข้องโดยอัตโนมัติแล้วเก็บใบกำกับสินค้าชุดที่ 1 ไว้ ส่วน

ใบกำกับสินค้าชุดที่ 2 ส่งไปให้ห้องเก็บสินค้ารวบรวมไว้แล้วจัดทำใบเรียกเก็บเงินขึ้น 3 ชุด ชุดที่ 1 และ 3 ส่งไปเรียกเก็บเงินจากลูกค้า ส่วนชุดที่ 2 เก็บไว้เป็นสำเนา

5) การรับชำระหนี้ เมื่อลูกค้าได้รับใบเรียกเก็บเงินแล้ว จะต้องจ่ายชำระค่าสินค้าด้วยเช็ค (Cheque) เท่านั้น โดยต้องแนบใบเรียกเก็บเงินชุดที่ 3 มาด้วย

เมื่อบริษัทฯ ได้รับเช็คและใบเรียกเก็บเงินชุดที่ 3 จากลูกค้า คุณโสภา (พนักงานต้อนรับ) จะเป็นผู้เปิดซองแล้วส่งให้คุณวิไล

คุณวิไลจะตรวจสอบความถูกต้องเรียบร้อยของเช็ค แล้วบันทึกรายการรับชำระหนี้จากลูกค้าด้วยเครื่อง terminal เดียวกันกับที่บันทึกบัญชีลูกค้าไว้ แล้วจึงส่งเช็คไปให้คุณตริงตรา (Cashier) นำฝากธนาคาร และคุณตริงตราจะส่งสำเนาใบรับฝากกลับคืนมาให้คุณวิไลเก็บไว้

การชำระหนี้ต้องชำระให้หมดในคราวเดียว สำหรับการสั่งซื้อแต่ละครั้งจะชำระเป็นงวด ๆ ไม่ได้

รายการที่บันทึกผ่านทางเครื่อง terminal ดังกล่าว จะแสดงในรายงานประจำวัน (Daily Report) ทุกรายการ ซึ่งแต่ละแผนกที่เป็นผู้ป้อนข้อมูลเข้าจะได้รับและเก็บไว้เรียงตามวันที่เกิดรายการ

การบันทึกการขายและการรับชำระหนี้ จะต้องป้อนข้อมูลดังนี้

- หมายเลขประจำตัวลูกค้า xxxxx
- รหัสรายการ xx
- จำนวนเงิน xxxxxxx.xx
- วันที่ xx/xx/xx อาจไม่ต้องป้อนข้อมูลก็ได้ หากไม่ได้ป้อนระบบงานจะ

ถือว่า วันที่ในระบบงาน (System Date) เป็นวันที่กำเนิดรายการ

ให้ทำ :

1) วาดผังระบบงานของบริษัท ภาพสวย จำกัด ตามที่มีข้อมูล โดยใช้สัญลักษณ์ให้ถูกต้องทั้งนี้ ไม่ต้องคำนึงถึงการส่งคืนสินค้า ให้จำแนกเป็นการขายสินค้าและการรับชำระค่าสินค้า

- 2) ให้ระบุ
- จุดอ่อนในการควบคุมและข้อแนะนำ
 - จุดที่โปรแกรมการทำงานในเครื่องคอมพิวเตอร์ควรมีการเช็คสอบในการบันทึกการขายแต่ละประเภท คือ การบันทึกจำนวนสินค้า การบันทึก รายการขายและการรับชำระหนี้

กรณีศึกษา 10

การรักษาความปลอดภัยห้องคอมพิวเตอร์

บริษัท ABC จำกัด ประกอบธุรกิจส่งออกเสื้อผ้าสำเร็จรูป ตั้งอยู่ย่านหัวหมากใกล้มหาวิทยาลัยรามคำแหง บริษัทได้จ้างสำนักงานสอบบัญชีแห่งหนึ่งให้ประเมินระบบรักษาความปลอดภัยศูนย์คอมพิวเตอร์ของบริษัท ซึ่งได้ย้ายจากชั้นที่ 2 ลงมาอยู่ชั้นล่างติดกับลานจอดรถด้านหน้าบริษัท นายโชคชัยซึ่งได้รับมอบหมายจากสำนักงานสอบบัญชีให้มาประเมินระบบรักษาความปลอดภัยศูนย์คอมพิวเตอร์ มาติดต่อนายสำราญหัวหน้าศูนย์คอมพิวเตอร์ของบริษัทเพื่อขอทราบนโยบายเกี่ยวกับการรักษาความปลอดภัยและขอระเบียบต่าง ๆ ที่เกี่ยวข้อง ซึ่งนายโชคชัยได้สรุปมาตรการเกี่ยวกับการรักษาความปลอดภัยศูนย์คอมพิวเตอร์ของบริษัทไว้ดังนี้

- ผู้มาติดต่อทุกคนต้องเซ็นชื่อเข้า-ออก ลงเวลา และระบุว่ามาติดต่อใครในทะเบียน
- ผู้มาติดต่อจะต้องติดบัตรแสดงตนตลอดเวลาที่อยู่ในศูนย์คอมพิวเตอร์
- ผู้บริหารและพนักงานของศูนย์คอมพิวเตอร์มีสิทธิเข้า-ออกห้องคอมพิวเตอร์ได้โดยใช้บัตรพลาสติกมีแถบแม่เหล็กกับรหัสประจำตัว ตรงประตูทางเข้าห้องคอมพิวเตอร์ และมีการบันทึกรหัสเจ้าของบัตรที่เข้าออกไว้โดยคอมพิวเตอร์
- มีพนักงานรักษาความปลอดภัยหน้าห้องคอมพิวเตอร์ตลอดเวลา
- ห้ามเก็บกระดาษาหรือวัสดุไวไฟไว้ในห้องคอมพิวเตอร์และห้ามสูบบุหรี่
- พนักงาน librarian เป็นผู้ควบคุมเทปทั้งหมด การเบิกจ่ายเทปต้องบันทึกในทะเบียนทุกครั้ง
- พนักงาน librarian เท่านั้นที่มีอำนาจลบข้อมูลในม้วนเทปได้

เมื่อระเบียบและเอกสารต่าง ๆ เกี่ยวกับการรักษาความปลอดภัยจนพอใจแล้ว นายโชคชัยต้องการชมศูนย์คอมพิวเตอร์ของบริษัท เพื่อดูว่าการควบคุมต่าง ๆ เป็นไปตามที่ระบุไว้หรือไม่ นายโชคชัยจึงนัดนายสำราญให้พาเขาไปชมศูนย์คอมพิวเตอร์ในตอนเช้าวันรุ่งขึ้น

เช้าวันรุ่งขึ้นนายสำราญพานายโชคชัยไปที่ศูนย์คอมพิวเตอร์ ซึ่งตั้งอยู่ชั้นล่างของบริษัทติดกับลานจอดรถ นายโชคชัยเดินตรงไปที่โต๊ะพนักงานรักษาความปลอดภัยหน้าประตูทางเข้าเพื่อเซ็นชื่อในทะเบียนผู้มาติดต่อ แต่นายสำราญบอกว่าไม่จำเป็นเพราะมากับเขา เมื่อทั้งสองเดินมาถึงประตูทางเข้านายสำราญก็นึกขึ้นมาได้ว่าเขาลืมบัตรพลาสติก ไว้ที่ห้องทำงาน แต่เขารู้สึกว่าเขาโชคดีประตูไม่ได้ล็อกไว้

ภายในห้องคอมพิวเตอร์ นายโชคชัยเห็นพนักงาน operator จำนวน 5 คน จับกลุ่มคุยกัน นายสำราญบอกกับเขาว่า พวกพนักงาน operator กำลังตกลงกันว่าวันนี้ใครจะทำอะไร

ด้านหลังห้องคอมพิวเตอร์เป็นที่ตั้งตู้เทป นายโชคชัยบังเอิญเดินไปชนพนักงาน operator ซึ่งกำลัง load เทปอยู่จนเทปหลุดมือตกลงที่พื้นห้อง นายโชคชัยถามว่า เทปจะเสียหายไหม พนักงาน operator บอกไม่เป็นไรและหยิบเทปม้วนนั้นขึ้นมา load ต่อ นายโชคชัยถามต่อว่าเป็นเทปข้อมูลเกี่ยวกับอะไร พนักงาน operator ตอบว่าไม่ทราบเพราะไม่มี label ติดไว้ นายโชคชัยเห็นแผ่นกระดาษต่อเนื่องพิมพ์ข้อความขนาดใหญ่ว่า “Happy

birthday Somsram) แขนงอยู่บนเพดานระหว่างเครื่องตรวจจับความร้อนกับหัวท่อแก๊ส Halon นายสำราญอธิบายว่า ที่ศูนย์คอมพิวเตอร์มีโปรแกรมพิมพ์ข้อความขนาดใหญ่ และบรรดาพนักงานเขียนโปรแกรมและพนักงาน operator มักจะพิมพ์ข้อความขนาดใหญ่แบบนี้ออกมาในช่วงที่ไม่ค่อยมีงาน ซึ่งทำให้พวกเขาไม่รู้สึกรำคาญหรือเคร่งเครียดกับงานจนเกินไป

นายโชคชัยกล่าวกับนายสำราญว่า ห้องคอมพิวเตอร์ของบริษัทสะอาดดีมาก ไม่วางสิ่งของเกะกะเลย นายสำราญจึงคุยว่าบริษัทกำหนดให้พนักงานทำความสะอาดทำความสะอาดห้องคอมพิวเตอร์เป็นประจำทุกวันอาทิตย์ ซึ่งเป็นวันที่ไม่มีพนักงานของศูนย์คอมพิวเตอร์อยู่เลย และพนักงานซ่อมบำรุงของบริษัทผู้ขายเครื่องคอมพิวเตอร์ก็จะมาตรวจสอบสภาพเครื่องคอมพิวเตอร์ในวันอาทิตย์เช่นกัน

หลังจากที่ชมอุปกรณ์คอมพิวเตอร์จนพอใจแล้ว นายโชคชัยจึงขอเข้าห้องเก็บเทปต่อไป ภายในห้องเก็บเทปนายโชคชัยเห็นเทปวางซ้อนกันกองโตบนโต๊ะของพนักงาน librarian นายสำราญบอกว่าเทปเหล่านั้นเป็นเทปซึ่งหมดอายุการใช้งานรอการทำลาย แต่ในช่วงนี้พนักงาน librarian ไม่มีเวลาว่างพอที่จะจัดการให้เรียบร้อยในช่วงเวลาดังกล่าว นายทินกร พนักงานเขียนโปรแกรมเดินเข้ามาหยิบเทปไปม้วนหนึ่ง นายทินกร มีที่ทำสนิทสนมกับนายสำราญเป็นอย่างดีซึ่งต่อมานายโชคชัยทราบว่า นายทินกรเป็นพนักงานเขียนโปรแกรมคนแรกของบริษัท ภรรยา นายทินกร เสียชีวิตไปเมื่อ 5 ปีก่อน ทำให้นายทินกรมุ่งทำแต่งานไม่ค่อยลาหยุดเลยตั้งแต่นั้น

จึงให้ข้อสังเกตเกี่ยวกับการรักษาความปลอดภัยห้องคอมพิวเตอร์ของบริษัท ABC จำกัด ตามข้อมูล ที่นายโชคชัยพบ



กรณีศึกษา 11

บริษัท เทคโนโลยีทันสมัย จำกัด

คุณขวัญตา เป็นนักบัญชีต้นทุนของบริษัทเทคโนโลยีทันสมัย จำกัด เธอมีหน้าที่รับผิดชอบในการตรวจสอบต้นทุนในการพัฒนาและในด้านการตลาดของผลิตภัณฑ์ใหม่ ข้อมูลเกี่ยวกับบริษัทข้อมูลด้วยรูปแบบฐานข้อมูล (Data - Base) โดยผู้ใช้สามารถสอบถามได้ในระบบ On - line ส่วนฝ่ายการบัญชีของบริษัทมี terminal อยู่หลายเครื่องทุกเครื่องสามารถสอบถามหรือบันทึกข้อมูลเข้าเครื่องคอมพิวเตอร์ได้ตามต้องการ

ให้ทำ : ระบุการรักษาความปลอดภัย และการควบคุมทั่วไปที่จะช่วยให้มั่นใจได้ว่า

- 1) ข้อมูลต้นทุนดังกล่าวเป็นข้อมูลเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น
- 2) ข้อมูลดังกล่าวสามารถเรียกใช้งานโดยผ่านระบบ On - line ได้ตลอดเวลา
- 3) ข้อมูลต้นทุนมีความน่าเชื่อถือได้



กรณีศึกษา 12

โปรตระกูล ความเสี่ยง ความเสียหายที่อาจเกิดขึ้น การควบคุมที่เหมาะสม และแนวการตรวจสอบในกิจกรรมต่อไป

โปรแกรมในระบบการเงินของธุรกิจการเงินแห่งหนึ่งได้มีการควบคุมการจัดทำรายการทั้งด้านการเงินและไม่ใช้ด้านการเงินด้วยโปรแกรมระบบงานคอมพิวเตอร์ โดยจะปรากฏ Menu ที่จอเทอร์มินอลทุกจอที่ใช้อยู่ได้เหมือนกันหมด ซึ่งผู้พัฒนาระบบได้บอกถึงประโยชน์ที่จัดทำโปรแกรมในรูปแบบที่กล่าว เพราะจะไม่ว่าเครื่องใดเครื่องหนึ่งเสียก็สามารถไปใช้เครื่องอื่นทำงานต่อไปแต่การเลือกใช้ Menu ใดได้บ้างนั้นจะขึ้นอยู่กับ Password ของพนักงานแต่ละคน และบาง Menu พนักงานในระดับที่ต่ำกว่าทำรายการได้เพียงบางส่วนเท่านั้น ถ้าเกินอำนาจของตนก็ต้องให้พนักงานในระดับที่สูงกว่ามาป้อน Password ที่จอของพนักงานระดับที่ต่ำกว่า เพื่อเป็นการอนุมัติรายการนั้น

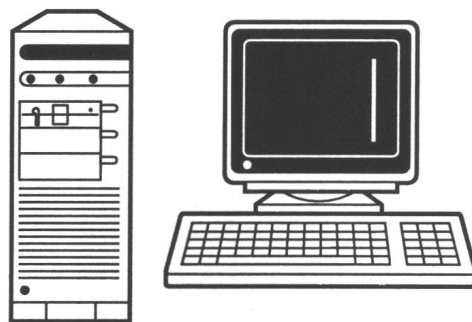
กรณีศึกษา 13

บริษัท วินิจไฮเทค จำกัด

เดิมบริษัท วินิจไฮเทค จำกัด ใช้ชื่อว่า บริษัท วินิจ จำกัด และเป็นบริษัทที่ไม่ใคร่จะทันสมัย ต่อมา มีการปรับปรุงทีมผู้บริหาร และมีการนำเทคโนโลยีคอมพิวเตอร์อันทันสมัยเข้ามาช่วยในการดำเนินงาน และเปลี่ยนชื่อ เป็นบริษัท วินิจไฮเทค จำกัด

บริษัทมีการผลิตในลักษณะของการประกอบชิ้นส่วนทางอิเล็กทรอนิกส์ และมีคนงานอยู่เป็นจำนวนมาก และในบางครั้งก็มีการทำงานล่วงเวลา คนงานมีอยู่หลายผลัด มีทั้งคนงานประจำและจ้างรายวัน ซึ่งมีทักษะต่าง ๆ กัน อัตราค่าแรงจึงแตกต่างกันไป ในแต่ละเดือนมีปัญหาในการคิดค่าแรง หรือค่าจ้างเงินเดือนมาก (ในระบบแบบเดิม) ซึ่งใช้บัตรบันทึกค่าแรงและการคำนวณด้วยมือในระบบแบบใหม่ มีการนำบัตรซึ่งมีแถบแม่เหล็กมาใช้ บนแถบแม่เหล็ก มีข้อมูลเกี่ยวกับตัวพนักงานผู้ถือบัตร และเมื่อเข้าทำงานก็จะรูดบัตรบนเครื่องอ่าน ซึ่งจะบันทึกเวลาการทำงานโดยอัตโนมัติและเมื่อเลิกงาน ก็รูดบัตรอีกครั้ง ระบบงานคอมพิวเตอร์จะทำการคำนวณค่าจ้างและเงินเดือนให้โดยอัตโนมัติ และมีการหักค่าใช้จ่ายตลอด

ขอให้ท่านประเมินความเสี่ยงจากการนำเอาระบบคอมพิวเตอร์เข้ามาใช้ในด้านของการคำนวณเงินเดือนจ่าย และระบุจุดควบคุม



กรณีศึกษา 14 - Application

บริษัท สายการบินปลอดภ้ย จำกัด

บริษัทสายการบินปลอดภ้ย จำกัด เป็นสายการบินภายในประเทศ ผู้โดยสารสามารถโทรศัพท์สำรองที่นั่งได้ที่สำนักงานใหญ่ หรือ สาขา ซึ่งมีอยู่ 40 แห่งทั่วประเทศ เที่ยวบินจะมีบริการทุกวันเหมือนกันวันละ 10 เที่ยวบิน มีรหัสดังนี้ M1 M2 M3 M4 M5 A1 A2 A3 A4 และ A5 โดยจองล่วงหน้าไมต่ำกว่า 3 วัน ก่อนวันเดินทาง และไม่เกิน 15 วัน ถ้าที่นั่งเต็ม บริษัทจะเสนอเที่ยวบินที่ว่างถัดไปให้แก่ลูกค้า

บริษัทใช้เครื่องคอมพิวเตอร์ในการประมวลผลงานสำรองที่นั่งนี้ โดยมีศูนย์ประมวลผลกลางอยู่ที่สำนักงานใหญ่ กรุงเทพฯ เชื่อมโยงกับ Terminal ทั้ง 41 เครื่อง ที่ติดตั้งอยู่ตามแต่ละสาขาและสำนักงานใหญ่ การประมวลผลเป็นแบบ Centralized On-line Processing มีโปรแกรมที่สำนักงานใหญ่ กรุงเทพฯ เป็นตัวจัดการเพื่อตอบรับหรือปฏิเสธ คำสำรองที่นั่งของลูกค้าแต่ละราย และเสนอเที่ยวบินใหม่ให้แก่ลูกค้าที่ถูกปฏิเสธ

จอภาพ ขั้นตอนการทำงาน และรายงานสิ้นวันที่ได้รับ มีรายละเอียดดังนี้

- 1) Terminal ของจองที่นั่ง 41 เครื่อง มีจอภาพรับข้อมูลดังนี้

ชื่อ	:	_____
วันที่	:	_____
เที่ยวบิน	:	_____
คำตอบ	:	_____

(รูปที่ 1)

เมื่อสำนักงานใหญ่ หรือ สาขา ได้รับคำสั่งจอง ก็จะ Key ข้อมูลเข้าตามจอภาพ

ชื่อ หมายถึง ชื่อ และ นามสกุล ของลูกค้า

วันที่ หมายถึง วันที่ ที่จะเดินทาง (DD/MM/YY)

เที่ยวบิน หมายถึง เที่ยวบินที่ต้องการเดินทางในวันที่ข้างต้น

ข้อมูลเหล่านี้ จะถูกส่งไปที่สำนักงานใหญ่ เพื่อตรวจสอบว่ามีที่นั่งว่างหรือไม่ แล้วสำนักงานใหญ่จะส่งคำตอบกลับมาปรากฏที่จอภาพนี้ คำตอบอาจเป็น “OK” (คือ มีที่นั่งให้ และรับจองแล้ว) หรือ “NO” DD/MM/YY : XX (คือ ที่นั่งเต็ม ขอเสนอเที่ยวบินใหม่ เดินทางวันที่_____และเที่ยวบินที่.... ตามข้อความที่ปรากฏต่อท้ายคำว่า “NO”)

แต่ละสาขาและสำนักงานใหญ่ จะมีพนักงานที่ได้รับอนุญาตให้ Key ข้อมูลได้ 3 คน โดยระบุชื่อไว้ชัดเจนว่าเป็นใครบ้าง บุคคลอื่นนอกเหนือจากที่กำหนดไว้ไม่มีสิทธิ Key ข้อมูล

ในกรณีที่คำตอบเป็น “OK” พนักงานสาขาจะแจ้งให้ลูกค้าทราบและถือเป็นการยืนยันตอบรับการจอง ถ้าคำตอบเป็น “NO” ก็จะถามว่าลูกค้าต้องการเปลี่ยนเที่ยวบินใหม่หรือไม่ถ้าต้องการ พนักงานต้องบันทึกรายการขอจองเป็นรายการใหม่ ซึ่งอาจจะตรงกับที่เสนอมาหรือไม่ก็ได้ ถ้าไม่ต้องการ สาขา也不需要ทำอะไรต่อไป

ระหว่างวัน เครื่องคอมพิวเตอร์ที่สาขาจะพิมพ์รายงานแสดงการบันทึกรายการที่ Key ข้อมูลเข้า มีรายละเอียดดังนี้

รายงานการขอสำรองที่นั่ง			
วันที่/เดือน/ปี			
ลำดับที่	ชื่อลูกค้า	วันที่	เที่ยวบิน
"	"	"	"
"	"	"	"
"	"	"	"
รวมทั้งสิ้น		ราย	

(รูปที่ 2)

คำอธิบาย

วันที่/เดือน/ปี	หมายถึง	วันที่ วันที่ ในระบบงาน
ลำดับที่	"	ลำดับที่การจอง เรียงตามลำดับ ก่อน-หลัง ที่ Key ข้อมูลเข้า
วันที่	"	วันที่ ที่ต้องการเดินทาง
เที่ยวบิน	"	เที่ยวบินที่ต้องการเดินทาง ในวันที่ข้างต้น
ยอดรวม	จำนวนขายจะเท่ากับลำดับที่สุดท้าย	

2) Terminal บันทึกการจองที่สำนักงานใหญ่ มีจอภาพรับข้อมูล ดังนี้

สาขา	:	_____
ชื่อ	:	_____
วันที่	:	_____
เที่ยวบิน	:	_____
รหัสผู้อนุมัติ	:	_____

(รูปที่ 3)

Terminal นี้เป็นคนละ Terminal กับ Terminal ของจองตามสาขา บริษัทมอบหมายให้พนักงานเฉพาะ 4 คนที่กำหนดให้ Key ข้อมูลได้ (ซึ่งเป็นคนละชุดกับพนักงาน Key ข้อมูลของจอง) และต้องมีผู้อนุมัติคนใดคนหนึ่ง ใน 2 คนที่บริษัทแต่งตั้ง Key รหัสลับของตนเพื่ออนุมัติรายการที่หน้าจอข้างต้นรายการดังกล่าวจึงจะผ่านเข้าไปประมวลผลได้ และเช่นเดียวกับการที่ของจอง ระหว่างเครื่องคอมพิวเตอร์จะพิมพ์รายงาน แสดงการบันทึกรายการรับจองที่ Key ข้อมูลเข้า มีรายละเอียดดังนี้

รายงาน การรับสำรองที่นั่ง				
วันที่/เดือน/ปี				
ลำดับที่	สาขา	ชื่อลูกค้า	วันที่	เที่ยวบิน
"	"	"	"	"
"	"	"	"	"
รวมทั้งสิ้น _____ ราย				

(รูปที่ 4)

นอกจากนี้สิ้นวัน ยังมีการประมวลผลงาน Batch เพื่อออกรายงานสรุป การสำรองที่นั่งแสดงข้อมูลจำแนกตามวันที่เดินทาง และเที่ยวบิน ดังนี้

รายงานสรุปสิ้นวัน				
วันที่/เดือน/ปี				
วันที่/เดือน/ปี	เที่ยวบิน	ชื่อลูกค้า	สาขา	จำนวนที่นั่ง
	M1	:	:	:
		รวม	ราย	
	M2			
	:			
	A5			
วันที่/เดือน/ปี		:		

(รูปที่ 5)

ให้ท่าน :

1. แสดงความเห็นเกี่ยวกับความเหมาะสมและความเพียงพอข้อมูลที่แสดงในรูปที่ 1 และรูปที่ 2
2. ข้อมูลแต่ละ field ที่ปรากฏบนจอภาพตามรูปที่ 3 โปรแกรมควรมีจุดควบคุมโดยการตรวจสอบ

อะไรบ้าง

(ตัวอย่าง ชื่อ : ต้องเป็นตัวอักษรเท่านั้น มีความยาวไม่เกิน 35 ตัวอักษร)

3. ให้ความเห็น และ ข้อเสนอแนะ เกี่ยวกับข้อมูลที่แสดงในรูปที่ 3 และ 4 ที่จะเป็นประโยชน์ต่อ บริษัทในด้านการลดความเสียหายที่อาจเกิดขึ้น
4. พิจารณาว่าจะใช้ประโยชน์จากข้อมูลในรายงานสิ้นวัน (รูปที่ 5) ช่วยในการควบคุม และตรวจสอบ ได้อย่างไร และควรจะแสดงข้อมูลใดเพิ่มเติมบ้าง
5. ให้คำแนะนำแก่บริษัทฯ ควรจะจัดทำเอกสารอะไรในขั้นตอนใดเพิ่มเติมเพื่อใช้เป็น audit trail ในการตรวจสอบความถูกต้อง ครบถ้วนของข้อมูล หรือเพื่อใช้ติดตามรายการที่มีข้อสงสัย/ปัญหาที่อาจมีขึ้นในภายหลัง



กรณีศึกษา 15

บริษัทเหล็กกล้า จำกัด นำเครื่องคอมพิวเตอร์ขนาดเล็กมาใช้ประมวลระบบงานเงินเดือนของบริษัทเมื่อ
สัปดาห์แรกของเดือนกุมภาพันธ์ บริษัทได้บันทึกข้อมูลไว้ดังนี้

หมายเลขประจำตัว ลูกจ้าง	ชื่อลูกจ้าง	หมายเลขแผนก ของลูกจ้าง	จำนวนชั่วโมง
13251	นายสุดหล่อ	1	40
13620	น.ส.สุดสวย	1	40
13543	นางแพรวดา	1	48
13658	นางใจดี	1	40
13752	น.ส.พริ้งเพรา	2	42
24313	นายขยัน	2	44
25001	นายอดทน	2	84

หมายเลขประจำตัวลูกจ้างจะมี 5 หลัก แต่ละหลักมีความหมายดังนี้

หลักแรก x หมายถึง หมายเลขแผนกที่ลูกจ้างสังกัด

หลักที่ 2-4 xxx “ running no. ของลูกจ้าง

หลักที่ 5 x “ check digit ที่ไม่เป็น 0

- ให้ทำ :
1. ระบุประเภทและอธิบาย Batch control total เท่าที่ทราบอย่างย่อ ๆ พร้อมทั้งคำนวณยอดรวมของแต่ละประเภทด้วย
 2. ระบุข้อผิดพลาดของข้อมูล และการตรวจสอบในโปรแกรม (program check) ที่จะป้องกันข้อผิดพลาดดังกล่าว

บทที่ ๗

แนวคำตอบบกรณีสึกษาต่าง ๆ
(จากกรณีสึกษาที่ 1-15)

แนวคำตอบกรณีศึกษาต่าง ๆ

(จากกรณีศึกษาที่ 1-15)

แนวคำตอบ กรณีศึกษา 1

กรณีมีความเสี่ยง ความเสียหาย ซึ่งมีข้อเสนอแนะในการควบคุม และการตรวจสอบดังนี้

- | | | |
|----------------|---|--|
| (1) ความเสี่ยง | - | ระบบงานสำเร็จรูปอาจไม่ตรงความต้องการ (application) ของบริษัท |
| ความเสียหาย | - | อาจทำให้ข้อมูลทางการเงินผิดพลาด หรือไม่ตรงกับความต้องการของผู้ใช้ |
| การควบคุม | - | ควรมีการศึกษาและให้บริษัทผู้จำหน่ายให้คำแนะนำหรืออธิบายโปรแกรมให้ละเอียด หรืออาจ train คนขึ้นมารับผิดชอบงาน software นั้น ๆ |
| การตรวจสอบ | - | ควรมีการทำ Test Data เพื่อสอบทานดูว่าผลลัพธ์ที่ออกมาตรงตามที่เราต้องการหรือไม่ |
| | | |
| (2) ความเสี่ยง | - | การป้อนข้อมูลของเจ้าหน้าที่แต่ละสาขาผิดพลาด |
| ความเสียหาย | - | ทำให้ยอดข้อมูลทางการเงินของสาขาและทั้งบริษัทผิดพลาดไปทั้งระบบ |
| การควบคุม | - | ควรมีการจัดทำ Preventive Control ต่าง ๆ เช่น มีการทำ Preprinted form, Default Option และควรมี Detective Control ได้แก่ Visual Verification, Check digit, Limit check, Validity check ทั้งนี้เพื่อให้ผู้ป้อนข้อมูลสามารถสอบทานความถูกต้องของการป้อนข้อมูลของแต่ละสาขาได้ก่อนที่จะประมวลผลหลังเวลาทำการ โดยเฉพาะอย่างยิ่งการมี Audit Trail ซึ่งจะช่วยให้สามารถติดตามแก้ไขข้อผิดพลาดได้ |
| การตรวจสอบ | - | ควรจัดให้มี Console log และทำการตรวจสอบรายการที่มีการประมวลผลเป็นช่วงเวลา ๆ ไปด้วยข้อมูลต่าง ๆ ที่ป้อนเข้าเครื่องถูกต้องหรือไม่ |
| | | |
| (3) ความเสี่ยง | - | การประมวลผลไม่สมบูรณ์หรือไม่อาจประมวลผลได้ หากไฟฟ้าดับ |
| ความเสียหาย | - | ข้อมูลของแต่ละสาขาจะผิดพลาดหมด และกว่าจะจัดทำผลการประมวลผลได้ใหม่ อาจไม่ทันแก่ความต้องการของแต่ละสาขา |
| การควบคุม | - | ควรจัดให้มีระบบไฟสำรองเมื่อกรณีไฟฟ้าดับลงระหว่างทำการประมวลผล ควรให้เจ้าหน้าที่อยู่ดูแลไปจนกว่าการประมวลผลจะสิ้นสุด เพื่อป้องกันความผิดพลาดในระหว่างการประมวลผล โดยมีการลงเวลาทำงานและเวลากลับไว้ในสมุดบันทึกเวลาทำงาน |
| การตรวจสอบ | - | ควรมีการทดสอบข้อมูลที่ได้รับหลังการประมวลผลว่าถูกต้องตรงตามที่ควรจะเป็นหรือไม่ |
| | - | ควรมีการทดสอบวิธีการทำงานของพนักงานควบคุมเครื่องด้วยว่า ทำงานจริงตามเวลาหรือไม่ |

- (4) ความเสี่ยง
ความเสียหาย
การควบคุม
การตรวจสอบ
- ข้อมูลสูญหาย และไม่สามารถ Recovery ได้
 - บริษัทไม่มีข้อมูลในการตัดสินใจในวันรุ่งขึ้น
 - ควรมีการจัดทำ Back up ไว้ด้วยขณะที่ทำการประมวลผล เช่น อาจมี Transaction File อีก 1 file เพื่อ record รายการต่าง ๆ ไว้ด้วย
 - ควรมีการทดสอบการ Recovery file ว่าจะสามารถจัดทำได้หรือไม่
 - ควรมีการตรวจสอบการทำงานของเจ้าหน้าที่ควบคุมเครื่องด้วย
- (5) ความเสี่ยง
ความเสียหาย
การควบคุม
การตรวจสอบ
- การจัดส่งรายงานผิดพลาด เนื่องจากเวลาการแยกรายงานและจัดเตรียมข้อมูลสำหรับวันใหม่มีแค่ 1 ชั่วโมง
 - สาขาอาจได้รับข้อมูลที่ไม่ถูกต้องมาใช้ในการตัดสินใจในวันรุ่งขึ้น
 - ระบบ Computer อาจไม่พร้อมสำหรับการประมวลผลในระบบ On-line ในวันรุ่งขึ้น ซึ่งทำให้เกิดความล่าช้าไปทั้งระบบ
 - ควรจัดแยกรายงานทันทีเมื่อประมวลผลเสร็จ และให้พนักงานผู้รับผิดชอบของสาขาต่าง ๆ มารับรายงานและตรวจสอบ output ไปด้วยเลย
 - ควรมีการจัดแบ่งเวลาการทำงานให้ชัดเจนและแน่นอน
 - รายงานควรพิมพ์ชื่อรายงาน ชื่อสาขา ไว้ให้ชัดเจน
 - ควรมีการทดสอบข้อมูล (Test Data) ด้วยว่า Input ที่ป้อนเข้าไปควรได้ output ดังที่แสดงในรายงานหรือไม่



แนวคำตอบ กรณีศึกษา 2

จากตัวอย่างแบบฟอร์มการรับรายงานและวิธีการส่งมอบรายงานตามที่กล่าว จะพบว่าระบบงานดังกล่าวมีความเสี่ยง ความเสียหาย และวิธีการควบคุมที่เหมาะสมดังนี้

ความเสี่ยง / ความเสียหาย	การควบคุม
(1.1) ความเสี่ยง - มีการรับข้อมูลแทนกันเช่น กรณีสาขา ก. และ ข. ความเสียหาย - ข้อมูลบางอย่างอาจเป็นความลับของสาขา ซึ่งอาจเป็นเหตุให้ความลับรั่วไหลได้ เช่น ข้อมูลเกี่ยวกับเงินเดือน เป็นต้น	(1.1) - ควรกำหนดระเบียบขึ้นมาให้พนักงานที่มีการมอบหมายหน้าที่เป็นการเฉพาะจากแต่ละสาขาเป็นผู้มารับรายงานด้วยตนเอง โดยบันทึกรายละเอียดในแบบฟอร์มดังกล่าว
(1.2) ความเสี่ยง - รายงานอาจเกิดการสูญหายในระหว่างที่รอให้พนักงานรับ-ส่ง มา รับรายงานจากช่องเก็บไป ความเสียหาย - ข้อมูลบางอย่างอาจเป็นความลับของบริษัท อาจรั่วไหลสู่บุคคลภายนอกได้ อาจทำให้เกิดความเสียหายต่อสาขาต่าง ๆ เนื่องจากจากไม่มีข้อมูลมาใช้ในการตัดสินใจหรืออาจได้รับล่าช้า เนื่องจากต้อง run ใหม่อีก	(1.2) - ควรมีการจัดเก็บรายงานของแต่ละสาขาไว้ที่ศูนย์อย่างมิดชิด และเวลาพนักงานมารับเอกสารควรลงทะเบียนรับหรือแสดงบัตรของสาขาแล้วจึงจะหยิบรายงานของแต่ละสาขาให้กับพนักงานรับ-ส่งแต่ละสาขา - ควรมีซองใส่รายงานและ Seal ไว้ด้วย เพื่อป้องกันความลับรั่วไหล
(1.3) ความเสี่ยง - พนักงานรับ-ส่งเอกสารอาจมารับล่าช้าหรืออาจไม่มารับ ความเสียหาย - อาจทำให้สาขาเกิดความเสียหายจากการไม่มีข้อมูลเพื่อใช้ตัดสินใจทันแก่ความต้องการ (กรณีของสาขา ง. เป็นต้น)	(1.3) - ควรมีการแบ่งแยกความสำคัญหรือตามความเร่งด่วน หากมีความเร่งด่วน ควรจัดส่งให้แต่ละสาขาเอง - ควรมีการบันทึกเวลารับเอกสารและเวลาที่เอกสารมาถึงสาขาเพื่อควบคุมให้พนักงานรับ-ส่งดำเนินการให้เหมาะสมแก่เวลา ไม่ใช่ไปและทานกาแฟกลางทาง เป็นต้น
(1.4) ความเสี่ยง - อาจมีการจ่ายรายงานใส่ช่องของสาขา สลับกัน ความเสียหาย - สาขาอาจใช้ข้อมูลผิดพลาด ทำให้การตัดสินใจและข้อมูลอื่น ๆ ผิดพลาดตามไปด้วย	

แนวคำตอบ กรณีศึกษา 3

ทบทวนการวิเคราะห์จุดอ่อนขั้นพื้นฐาน

จุดอ่อนที่สำคัญ คือ

- 1) พนักงานควบคุมตู้নির্যয় ไม่มีสำเนาเอกสารของการบันทึกรายละเอียดของหลักประกัน เก็บไว้เพื่อเป็นหลักฐานในการรับฝากหลักประกัน
- 2) เสมียนฉีกสำเนาใบสীখা ซึ่งเป็นเอกสารสำคัญทิ้งไป ทำให้เกิดจุดอ่อน คือ เสมียนอาจจะฉีกสำเนาสীখাทิ้งไปเอง โดยไม่มีสำเนาสำเนาที่พอได้ หรือเป็นช่องทางให้เกิดการร่วมมือยกยอกหลักประกันระหว่างเสมียนกับเจ้าหน้าที่ / พนักงานประจำตู้নির্যয়ได้ หรือ ทำให้ขาดการบันทึกหลักประกันบางรายการไว้ในระบบ Computer
- 3) กรณีเกิดข้อแตกต่างหรือปัญหาใด ๆ ผู้ช่วยของเจ้าหน้าที่สินเชื่อเป็นผู้แก้ปัญหาเองทั้งหมด ซึ่งอาจเกิดการทุจริตหรือข้อผิดพลาดได้

ข้อเสนอแนะในการควบคุม

- 1) หน่วยงานที่รับผิดชอบตู้নির্যয় ควรจัดทำทะเบียนบันทึกการรับฝากหลักประกัน สมุดลงนามรับ-ส่งหลักประกัน สำหรับให้ผู้ที่น่าส่ง / บิล หลักประกันลงนาม พร้อมทั้งวันที่และเวลาไว้เป็นหลักฐาน
- 2) ควรจัดให้มีเจ้าหน้าที่ตรวจสอบความถูกต้องของข้อมูลที่เสมียน Key บันทึกหลักประกันไว้ในระบบ Computer ว่าถูกต้องตรงกับข้อความในสำเนาสীখาที่ส่งมาจากหน่วยงานด้านตู้নির্যয়หรือไม่ โดยให้มี report หรือ log ที่พิมพ์จากเครื่อง Computer แล้วนำมาตรวจสอบกับเอกสารสำเนาดังกล่าว
- 3) ควรแบ่งระดับของเจ้าหน้าที่ผู้มีอำนาจในการแก้ไขข้อแตกต่างตามประเภทและความสำคัญ ในกรณีที่เป็นเรื่องสำคัญควรกำหนดระดับการอนุมัติก่อนที่จะทำการแก้ไขและมีการตรวจสอบความถูกต้องของรายการแก้ไขในภายหลัง
- 4) ฝ่ายสินเชื่อควรจัดทำทะเบียนการรับหลักประกันจากลูกค้า และการส่งหลักประกันไปให้เจ้าหน้าที่ตู้নির্যয় เพื่อไว้สอบยันกับทะเบียนของทางตู้নির্যয়
- 5) ควรให้ลูกค้าลงนามรับสำเนาสীখা เพื่อเก็บไว้เป็นหลักฐานในการรับหลักประกันจากลูกค้า
- 6) ควรส่งสำเนาสীখาไปพร้อมกับสীখาและหลักประกันให้กับเจ้าหน้าที่ตู้নির্যয় และให้เซ็นรับและส่งสำเนาสীখาให้ฝ่ายสินเชื่อเก็บไว้เป็นหลักฐาน
- 7) สำเนาสীখาไม่ควรฉีกทิ้ง ควรเย็บติดกับสำเนาสীখาที่ได้รับคืน เก็บไว้เป็นหลักฐานว่าทางตู้নির্যয়ได้รับหลักประกันไปแล้ว

แนวคำตอบ กรณีศึกษา 4

ความเห็นในเรื่อง ความเสี่ยง ความเสียหาย และข้อเสนอแนะในการควบคุม คือ

1) การแบ่งแยกหน้าที่ภายในหน่วยงานด้านคอมพิวเตอร์

- **ความเสี่ยง** บริษัทมอบหมายให้บุคคลคนเดียวกันทำหน้าที่ทางด้าน System Analyst และ Programmer, Programmer และ Operator
- **ความเสียหาย** เป็นการเปิดโอกาสให้ Programmer ซึ่งรู้ logic และจุดควบคุม / จุดเช็คสอปในโปรแกรม ทำการแก้ไข Program เพื่อการทุจริตได้ ส่วน System Analyst และ Programmer นั้น หากสามารถมอบหมายให้บุคคลแยกกันได้ก็จะเป็นการช่วยเช็คสอปการออกแบบและการแก้ไขโปรแกรมอีกชั้นหนึ่ง ถ้าไม่สามารถแบ่งแยกได้ ก็ไม่ถือว่าเป็นจุดอ่อนที่สำคัญนัก
- **การควบคุม** ภายใต้ข้อจำกัดของจำนวนบุคลากรที่กำหนด บริษัทอาจไม่จำเป็นต้องมี System Analyst เพราะใช้โปรแกรมสำเร็จรูปและงานไม่ซับซ้อนมากนัก และแบ่งหน้าที่ให้แต่ละบุคคล ดังนี้
 - 1) ทำหน้าที่รับผิดชอบทางด้าน Programming
 - 2) ทำหน้าที่เกี่ยวกับงาน Operation

ถ้าจำเป็นต้องมี Operator ทำตลอด 24 ชั่วโมง ก็อาจกำหนดให้พนักงาน Full-time ทำหน้าที่ที่สำคัญ เช่น การทดสอบการทำงานของเครื่อง การประมวลผลงาน Batch เนื่องจาก output ที่ได้จะมีข้อมูลที่สำคัญหรือ ความลับของบริษัทรวมอยู่ด้วย และมอบหมายงานประจำตัวไปให้แก่พนักงาน full-time อีกคนหนึ่งที่ทำหน้าที่อื่นที่ไม่มีผลกระทบต่องานด้านคอมพิวเตอร์ปฏิบัติงานควบคู่ไปด้วย หรือพนักงาน part-time ตามแต่จะเหมาะสม

2) การควบคุมม้วนเทป

- **ความเสี่ยง** ไม่มีกุญแจล็อกตู้ใส่ม้วนเทป และไม่มีทะเบียนคุมการเบิก-ใช้ม้วนเทป
- **ความเสียหาย** ม้วนเทปซึ่งเก็บข้อมูลสำคัญอาจสูญหาย ถูกนำไปใช้โดยไม่ผ่านการอนุมัติ
- **การควบคุม** ควรจัดให้มีกุญแจล็อกตู้ใส่ม้วนเทป มีทะเบียนควบคุมการเบิกใช้ และส่งคืน พร้อมทั้งกำหนดว่าใครมีสิทธิใช้ม้วนไหนได้บ้าง และมอบหมายให้มีบุคคลคนหนึ่งรับผิดชอบดูแลตู้ม้วนเทปนี้โดยเฉพาะ ซึ่งอาจไม่ใช่บุคลากรของหน่วยงานด้านคอมพิวเตอร์ในกรณีที่ไม่สามารถว่าจ้าง Librarian โดยเฉพาะก็ได้

3) การจัดทำข้อมูลสำรอง

- **ความเสี่ยง** ไม่มีม้วนเทปชุด Copy ไว้เป็น backup และตู้ที่เก็บม้วนเทปก็อยู่ในห้องคอมพิวเตอร์นั้นด้วย
- **ความเสียหาย** ข้อมูลอาจสูญหายหรือถูกทำลาย และไม่สามารถปฏิบัติงานต่อเนื่องได้ ถ้าเกิดม้วนเทปสูญหาย หรือถูกทำลายไป
- **การควบคุม** ควรมีม้วนเทปชุด copy ไว้อีกชุดหนึ่ง เก็บรักษาไว้อย่างปลอดภัยแยกคนละสถานที่กับม้วนเทปชุดที่ใช้งานจริง และมีการ update ข้อมูลในชุด copy เป็นระยะ ๆ ตามความเหมาะสม



แนวคำตอบ กรณีศึกษา 5

- ชุดที่ 1**
- มีวัตถุประสงค์เพื่อที่จะทดสอบว่า บัญชีที่ปิดไปแล้วมีการ delete ข้อมูลของลูกค้ารายนั้น ๆ ออกหรือไม่
 - ผลลัพธ์คือ เครื่องควรวัดและปฏิเสธรายการเงินฝาก จำนวน 70,000 บาท
 - หากการทดสอบไม่เป็นไปตามที่คาดไว้ จะทำให้มีความเสี่ยง คือ อาจมีการบันทึกรายการผิดพลาด ความเสียหายจะเกิดกับทั้งธนาคารและเจ้าของเงินฝากซึ่งมีบัญชีเลขที่อื่น แต่เงินฝากของตนไปปรากฏในบัญชีอื่น ควรควบคุมโดย ควรมีการ delete ข้อมูลบัญชีที่ปิดไปแล้วทิ้ง
- ชุดที่ 2**
- มีวัตถุประสงค์เพื่อทดสอบว่า cheque ที่ไม่ผ่าน clearing จะมีการล้งยอด Balance ออกถูกต้องหรือไม่
 - ผลลัพธ์ เครื่องควรวัดและปฏิเสธรายการ cheque คืนที่มีจำนวนเงินผิดพลาดนี้
 - หากไม่เป็นดังนี้ ความเสี่ยงคือ อาจมีการลดยอดเงินในบัญชีผิดพลาด ซึ่งทำให้เกิดความเสียหายคือยอดคงเหลือในบัญชีไม่ถูกต้อง วิธีการควบคุมควรมีการ match เลขที่ cheque กับ Amount ที่ถูกต้องก่อน adjust Balance
- ชุดที่ 3**
- มีวัตถุประสงค์เพื่อทดสอบว่า โปรแกรมมีการ delay รายการ cheque ที่ติด clearing ไว้เพื่อขอผ่านบัญชีก่อนที่จะ adjust ยอด available balance หรือไม่
 - ผลลัพธ์ เครื่องควรวัดและปฏิเสธการจ่ายเงิน
 - หากไม่เป็นดังนี้ ความเสี่ยงคือ อาจมีการถอนเงินไปโดยที่ cheque ยังไม่ผ่านบัญชี ซึ่งจะก่อให้เกิดความเสียหายแก่ธนาคารได้ การควบคุมควรมีการ set ไว้ในโปรแกรมว่า ถ้ามีการฝาก cheque ให้ delay การ adjust ยอด available balance ไว้อีก 1 วัน เพื่อให้มีการ clearing ไปก่อน
- ชุดที่ 4**
- มีวัตถุประสงค์เพื่อทดสอบโปรแกรมการอายัดบัญชีและการยกเลิกการอายัดว่า สมบูรณ์หรือไม่
 - ผลลัพธ์ เครื่องควรวัดและปฏิเสธการจ่ายเงิน
 - หากไม่เป็นดังนี้ ความเสี่ยงคือ อาจมีการถอนเงินที่ธนาคารยอมให้ถอนเงินได้ การควบคุมควรมีการ adjust ยอด available balance ก่อนที่จะอนุมัติการจ่ายเงิน

- ชุดที่ 5** - มีวัตถุประสงค์เพื่อทดสอบการคำนวณดอกเบี้ยและการอนุมัติการจ่ายเงินจาก available balance
- ผลลัพธ์ เครื่องควรจะปฏิเสธจำนวนดอกเบี้ยที่ป้อนข้อมูลเข้าไป แต่ขณะเดียวกันการถอนเงินสด 107,000 ควรจะจ่ายได้ เพราะเครื่องจะมียอด available balance จากการคำนวณของตนจากอัตราดอกเบี้ย 7% และ 6.5% อยู่แล้ว (เนื่องจาก available balance เฉพาะเงินฝากก็เท่ากับ 150,000 บาทแล้ว ทั้ง ๆ ที่ยังไม่รวมดอกเบี้ย)
 - หากไม่เป็นดังนี้ ความเสี่ยงคือ ถ้าอัตราดอกเบี้ยขึ้นอยู่กับ key ของ teller จะมีผลให้ยอด balance ผิดพลาด เช่น อาจ key ดอกเบี้ย 100% ก็ได้ ซึ่งการควบคุมควรที่จะให้เครื่องคิดดอกเบี้ยจาก rate ที่ set ไว้ และมียอดคงเหลือแสดงขณะที่ Teller จะคำนวณดอกเบี้ยเข้าไป adjust ด้วย



แนวคำตอบ กรณีศึกษา 6

วัน / เดือน / ปี	รายการ	จำนวนเงิน	ผลลัพธ์ที่คาดว่าจะได้รับ
20/11/87	ฝากเงินสด	100,000	- Balance.....190,000.- - Available.....390,000.-..... - อื่น ๆ
	ฝากเช็คที่ยังติดเคลียร์	5,000	- Balance.....195,000.-..... - Available..... 390,000.-..... - อื่น ๆ
22/11/87	ถอนเงินสด	200,000	- Balance.....-5,000.-..... - Available..... 195,000.-..... - อื่น ๆ
23/11/87	ถอนเงินสด	195,000	- Balance.....-200,000.-..... - Available.....@..... - อื่น ๆ
24/11/87	ถอนเงินสดผ่าน ATM	1,000	- Balance.....-200,000.-..... - Available.....@..... - อื่น ๆ เครื่องปฎิเสธการจ่ายเงิน
25/11/87	ฝากเช็คที่ยังติดเคลียร์	30,000	- Balance.....-170,000.-..... - Available.....-..... - อื่น ๆ



แนวคำตอบ กรณีศึกษา 7
การตรวจสอบศูนย์ประมวลผล
บริษัท เอส.เอ.อินเตอร์เทรด จำกัด
ภาค 1

จุดอ่อนด้านการจัดการ (ข้อ 1-8)

1. จากผังโครงสร้างการจ้างองค์การ ปรากฏว่าศูนย์คอมพิวเตอร์ไปขึ้นกับผู้จัดการฝ่ายการเงินแทนที่จะเป็นสำนักเลขานุการ ผลคือ

- ไม่เป็นอิสระเท่าที่ควรจะเป็น
- อาจไม่ Service หน่วยงานอื่นเท่าที่ควร

ดังนั้น จึงควรให้ศูนย์คอมพิวเตอร์ขึ้นกับสำนักเลขานุการจะเหมาะสมกว่า

2. ไม่ได้มีการกำหนดแผนงานในระยะยาว ไม่มีทีมผู้บริหารระดับสูงหรือคณะกรรมการร่วมพิจารณา ทุกอย่างอยู่ในการพิจารณาตัดสินใจเสนอเรื่องโดยหัวหน้าศูนย์คอมพิวเตอร์ ผลคือ

อาจไม่เกิดประโยชน์สูงสุดแก่องค์การหรือตามที่ต้องการอย่างแท้จริง ผู้บริหารระดับสูงของธนาคารหรือคณะกรรมการที่มีหน้าที่เกี่ยวข้องกับงานคอมพิวเตอร์ควรเป็นผู้พิจารณาและให้ความเห็นชอบในเรื่อง

- นโยบายการใช้คอมพิวเตอร์
- มาตรการจัดสรรทรัพยากรให้แก่โครงการต่าง ๆ
- มาตรการที่ใช้ในการรักษาความปลอดภัยและการควบคุมภายใน
- การวิจัยและการศึกษาเพื่อพัฒนางานคอมพิวเตอร์
- งบประมาณคอมพิวเตอร์
- การจัดลำดับความสำคัญในการใช้คอมพิวเตอร์
- การเปลี่ยนแปลงระบบงาน การจ้างองค์การ และเครื่องจักรหรืออุปกรณ์คอมพิวเตอร์
- สถานะของโครงการและผลการดำเนินงานตามเป้าหมายที่กำหนดไว้
- แผนงานคอมพิวเตอร์ในระยะยาว

3. ไม่มีการกำหนดรายละเอียดเกี่ยวกับตำแหน่งงานและขอบเขตหน้าที่ความรับผิดชอบของพนักงานในหน่วยงานคอมพิวเตอร์อย่างชัดเจนและเพียงพอ (ที่กำหนดไว้นั้นหยابเกินไป) ผลคือ

การทำงานอาจไม่มีประสิทธิภาพ หรือตรงตามความต้องการเท่าที่ควร อาจมีการทำงานซ้ำซ้อนหรือตกหล่นในบางเรื่อง และอาจมีการทำงานผิดพลาดหรือนอกเหนือจากความต้องการได้

ควรมีการกำหนดรายละเอียดเกี่ยวกับตำแหน่งงาน และขอบเขตอำนาจหน้าที่ความรับผิดชอบของพนักงานในหน่วยงานคอมพิวเตอร์อย่างชัดเจนและเพียงพอ

4. ไม่มีการตรวจสอบภายในด้านคอมพิวเตอร์ มีแต่การตรวจสอบโดยใช้ข้อมูลจาก Report เปรียบเทียบกับข้อมูลเข้า (Input) ผลคือ

อาจมีการเปิดช่องโหว่ในระบบงานคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนที่อาจก่อให้เกิดความเสียหายได้ถึงขั้นร้ายแรง และการตรวจสอบเพียงดูจากข้อมูลที่ Input และข้อมูลจากรายงานเป็นสิ่งที่ไม่พอเพียง

ควรจัดให้มีการตรวจสอบภายในด้านคอมพิวเตอร์ ทั้งนี้ มีประเด็นที่ควรพิจารณาดังนี้

4.1 ธุรกิจต้องมอบอำนาจให้ผู้ตรวจสอบภายใน

- เพียงพอที่จะทำให้งานตรวจสอบมีประสิทธิภาพ
- สามารถกำหนดวิธีการควบคุมภายใน และจัดให้มีข้อมูลสำหรับใช้เป็นหลักฐานในการควบคุมและตรวจสอบได้อย่างเพียงพอทุกระบบงาน

4.2 มีการจัดสรรงบประมาณสำหรับการตรวจสอบคอมพิวเตอร์

4.3 มีคณะกรรมการ

- เป็นผู้พิจารณาแผนงานและเป้าหมายการตรวจสอบประจำปี
- ติดตามผลการปฏิบัติงานของผู้ตรวจสอบภายใน โดยเปรียบเทียบผลการปฏิบัติงานจริงกับแผนงานและเป้าหมายการตรวจสอบประจำปี
- เป็นผู้พิจารณาหลักเกณฑ์ที่ใช้ในการคัดเลือกงานตรวจสอบ
- รับทราบผลการตรวจสอบคอมพิวเตอร์

4.4 ผู้ตรวจสอบภายใน ต้อง

- เข้าร่วมประชุมพิจารณาจัดหาเครื่องคอมพิวเตอร์ และ / หรือระบบงานและโปรแกรม
- เข้าร่วมพัฒนาระบบงานและโปรแกรม
- มีหน้าที่ตรวจสอบศูนย์คอมพิวเตอร์และระบบงานที่ประมวลผลด้วยคอมพิวเตอร์และเสนอรายงานการตรวจสอบต่อคณะกรรมการ

4.5 ต้องมีการกำหนดคุณสมบัติของผู้ตรวจสอบภายในด้านคอมพิวเตอร์อย่างเหมาะสม

4.6 ควรมีการประเมินความเสี่ยงและจัดทำแผนการตรวจสอบ

4.7 ควรมีการจัดทำคู่มือตรวจสอบ ซึ่งอธิบาย

- วิธีตรวจสอบการดำเนินงานคอมพิวเตอร์
- วิธีตรวจสอบระบบงานคอมพิวเตอร์
- วิธีพิจารณาทบทวนระบบงานใหม่ก่อนอนุญาตให้นำออกใช้ประมวลผลข้อมูลจริง
- มีรูปแบบของรายงานการตรวจสอบแสดงไว้เป็นตัวอย่าง
- มีข้อสังเกตและคำแนะนำของผู้ตรวจสอบภายในแสดงไว้เป็นแนวทาง
- รวบรวมจุดอ่อน สาเหตุที่เกิดข้อผิดพลาด และวิธีแก้ไขข้อผิดพลาดแสดงไว้โดยละเอียด

4.8 มีระเบียบการติดตามผลการตรวจสอบ

- มีการกำหนดระยะเวลาให้หน่วยงานที่ถูกตรวจสอบตอบชี้แจง
- มีหลักเกณฑ์ในการกำหนดระยะเวลาการตรวจสอบเพื่อติดตามผล

4.9 มีคู่มือจัดทำกระดานทำการอธิบาย

- วิธีจัดทำเอกสารหลักฐานและการจัดเก็บเอกสารเข้าแฟ้มเพื่อความสะดวกในการค้นหา
- วัตถุประสงค์การตรวจสอบ
- รายละเอียดของงานที่ตรวจสอบ รวมทั้งระเบียบการปฏิบัติงาน และวิธีการควบคุมภายในที่ใช้ในงานที่ตรวจสอบ
- วิธีทบทวนกระดานทำการเก่าที่เกี่ยวข้องกับคำแนะนำหรือข้อสังเกตในการตรวจสอบครั้งก่อน
- การปฏิบัติงานตามนโยบายและการปฏิบัติตามระเบียบของบริษัท

4.10 มีการจัดให้มีการตรวจสอบในเรื่องดังต่อไปนี้

- การกระทบบยอดข้อมูล
- การเตรียมข้อมูล
- การปฏิบัติงานคอมพิวเตอร์
- ระบบงานและโปรแกรม
- การประมวลผลโดยอาศัยระบบสื่อสาร
- โปรแกรมที่ใช้กับงานที่มีความสำคัญ
- เอกสารระบบงานและโปรแกรม
- การควบคุมภายในหน่วยงานผู้ใช้ข้อมูล

5. ไม่มีการวิเคราะห์ความเสี่ยงภัยและนำเทคนิคการบริหารงานอื่น ๆ มาใช้กำหนดประเภทการประกัน และวงเงินประกันภัยคอมพิวเตอร์ ทำให้การประกันภัยต่ำกว่ามูลค่าจริง ผลคือหากเกิดภัยพิบัติขึ้น หรือคอมพิวเตอร์ได้รับความเสียหาย อาจทำให้บริษัทสูญเสียมากกว่าที่จำเป็นบริษัทควรมีการวิเคราะห์ความเสี่ยงภัย และจัดทำวงเงินประกันภัยคอมพิวเตอร์อย่างเหมาะสม

6. ไม่มีการจัดทำแผนฉุกเฉินและแผนการรักษาความปลอดภัยเสนอต่อคณะกรรมการ ผลคือ

เมื่อเกิดเหตุฉุกเฉินขึ้น อาจเกิดความสับสนและความโกลาหล ทำอะไรไม่ถูก ทำให้บริษัทได้รับความเสียหาย มากกว่าที่ควรจะเป็นหากได้มีการเตรียมพร้อม โดยมีการจัดทำแผนฉุกเฉินและได้มีการซ้อมอย่างน้อยปีละครั้ง

บริษัทควรจัดให้มีแผนฉุกเฉินและแผนการรักษาความปลอดภัยและมีการซ้อมอย่างน้อยปีละครั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นดังกล่าวด้วย

แผนปฏิบัติงานและปรับปรุงแก้ไขเมื่อเกิดเหตุฉุกเฉิน (Contingency Plan) หมายถึง แผนงานที่จัดทำไว้เพื่อใช้เป็นแนวทางในการกำหนดมาตรการรักษาความปลอดภัยและป้องกันความเสียหายจากเหตุฉุกเฉินหรือภัยพิบัติ

ต่าง ๆ ที่อาจมีผลกระทบต่อการดำเนินงาน และการให้บริการตามปกติของธนาคารพาณิชย์หยุดชะงัก รวมทั้งแผนปฏิบัติงานและปรับปรุงแก้ไขหรือกำหนดวิธีการอื่นใดที่จะทดแทนการหยุดทำงานของระบบคอมพิวเตอร์ เพื่อให้องค์กรสามารถดำเนินการและให้บริการได้อย่างต่อเนื่องตามปกติ ซึ่งประกอบด้วยแผนย่อยดังนี้

6.1 แผนปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน (Emergency Plan) หมายถึง แผนการรักษาความปลอดภัย และขั้นตอนปฏิบัติงานเมื่อเกิดเหตุฉุกเฉินหรือภัยพิบัติต่าง ๆ เพื่อป้องกันความเสียหายที่อาจมีผลกระทบต่อการดำเนินงานและการให้บริการด้วยระบบงานคอมพิวเตอร์ตามปกติขององค์กรให้เกิดขึ้นน้อยที่สุด

6.2 แผนปรับปรุงแก้ไขระบบงานคอมพิวเตอร์ (Recovery and Disaster Plan) หมายถึง แผนปฏิบัติงานสำหรับใช้ดำเนินการแก้ไขระบบงานคอมพิวเตอร์ขององค์กรที่ขัดข้องหรือเสียหายไม่สามารถใช้งานได้ ให้กลับสู่สภาวะปกติในเวลาอันสมควร รวมทั้งกำหนดวิธีการอื่นที่ใช้ทดแทนการหยุดทำงานของระบบงานคอมพิวเตอร์

6.3 ระบบคอมพิวเตอร์สำรอง (Back up) หมายถึง การจัดหรือจัดทำระบบสำรองของเครื่องคอมพิวเตอร์ อุปกรณ์ประกอบระบบคอมพิวเตอร์ และระบบงานคอมพิวเตอร์เพื่อใช้ทดแทนการทำงานเมื่อระบบคอมพิวเตอร์ที่ใช้งานตามปกติขัดข้องหรือเสียหายใช้การไม่ได้

7. ไม่มีระบบการรายงานการปฏิบัติงานที่ดีและมีประสิทธิภาพ เพื่อให้พนักงานชั้นบริหารระดับสูงของธนาคารใช้ในการควบคุมดูแลและติดตามการปฏิบัติงานของหน่วยงานคอมพิวเตอร์ มีแต่การแจ้งว่าทำอะไรบ้างและก้าวหน้าแค่ไหน โดยไม่อ้างอิงงานที่ทำไม่ได้ตามแผนหรือไม่เป็นไปตามแผน และอุปสรรคปัญหาที่เกิดขึ้น ผลคือ

ผู้บริหารระดับสูงไม่ทราบสาเหตุแห่งความล้มเหลวและไม่อาจแก้ไขได้ทันการ และไม่ทราบว่าการปฏิบัติงานของหน่วยงานคอมพิวเตอร์เป็นไปในลักษณะที่ก่อให้เกิดประโยชน์สูงสุดแก่องค์กรหรือไม่

บริษัทควรจัดให้มีระบบการรายงานผลการปฏิบัติงานที่ดีและมีประสิทธิภาพ เพื่อให้พนักงานชั้นบริหารระดับสูงของบริษัทใช้ในการควบคุมดูแลและติดตามการปฏิบัติของหน่วยงานคอมพิวเตอร์

8. ค่าใช้จ่ายของศูนย์คอมพิวเตอร์ไม่เป็นไปตามงบประมาณที่วางไว้ ผลคืออาจเป็นไปได้ที่มีการใช้จ่ายเกินความจำเป็น และไม่มีการควบคุมค่าใช้จ่ายอย่างดีพอหรืออาจเป็นเพราะงบประมาณที่วางไว้ไม่เหมาะสมพอ

บริษัทควรมีการสอบทานเพื่อหาสาเหตุที่แท้จริงของค่าใช้จ่ายจริงที่คลาดเคลื่อนจากงบประมาณที่วางไว้ ทั้งนี้ เพื่อให้การควบคุมค่าใช้จ่ายของศูนย์คอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ทั้งนี้ โดยสัมฤทธิ์ผลตามที่ต้องการ

จุดอ่อนด้านระบบงานและโปรแกรม (ข้อ 9-17)

9. ไม่มีการกำหนดระเบียบในการออกแบบระบบงานและการพัฒนาระบบงานอย่างเป็นทางการหรือเป็นลายลักษณ์อักษรอย่างเพียงพอ มีแต่การบอกเล่าด้วยวาจา โดยถือว่ามีผู้ร่วมปฏิบัติงานไม่กี่คนผลคือ

ขาดความเป็นมาตรฐานและความเป็นระบบงานและการพัฒนาระบบงานขาดเครื่องมือที่จะใช้ในการควบคุมและติดตามในการออกแบบระบบงานและการพัฒนาระบบงานอีกด้วย

บริษัทควรกำหนดระเบียบในการออกแบบระบบงานและการพัฒนาระบบงานอย่างเป็นทางการและเป็นลายลักษณ์อักษรอย่างเพียงพอเพื่อควบคุมติดตามให้มีการปฏิบัติตามอย่างถูกต้องโดยกำหนดให้มี

- 9.1 การศึกษาความเหมาะสมของโครงการ
- 9.2 การวิเคราะห์ต้นทุนและผลตอบแทนที่ได้รับจากโครงการ
- 9.3 การรายงานผลความก้าวหน้าของการพัฒนาระบบงาน
- 9.4 การพิจารณาทบทวนและให้ความเห็นชอบในการออกแบบระบบงานทุกขั้นตอน
- 9.5 การขอความเห็นชอบในการออกแบบระบบงานจากผู้ใช้อีกก่อนจัดทำโปรแกรม
- 9.6 การทดสอบระบบงานโดยผู้ใช้อีกและผู้ปฏิบัติงานคอมพิวเตอร์
- 9.7 การขอหนังสือรับรองระบบงานหรือหนังสือรับรองระบบงานจากผู้ใช้อีก
- 9.8 การพิจารณาทบทวนผลการปฏิบัติงานภายหลังจากที่ได้นำระบบงานใหม่ออกใช้งานจริง

10. ไม่มีระเบียบในการคัดเลือกโปรแกรมสำเร็จรูป มีแต่การพูดคุยตกลงเห็นชอบกัน ผลคือ

ขาดความเป็นมาตรฐานและความเป็นระบบระเบียบในการคัดเลือกโปรแกรมสำเร็จรูป และขาดเครื่องมือที่จะใช้ในการควบคุมในการคัดเลือกโปรแกรมสำเร็จรูป

บริษัทควรมีการกำหนดระเบียบในการออกแบบระบบงานและการพัฒนาระบบงานอย่างเป็นทางการและเป็นลายลักษณ์อักษรอย่างเพียงพอ โดยกำหนดให้มี

- 10.1 การวิเคราะห์โปรแกรมสำเร็จรูปของผู้ผลิตหรือผู้ขายแต่ละรายที่มีลักษณะการทำงานคล้ายกันหรือใช้ทดแทนกันได้โดยละเอียด
- 10.2 การวิเคราะห์ต้นทุนและผลตอบแทนที่ได้รับจากการใช้โปรแกรมสำเร็จรูปของผู้ผลิตหรือผู้ขายแต่ละราย

11. ไม่มีระเบียบในการจัดทำโปรแกรม ผลคือขาดความเป็นมาตรฐานและความเป็นระบบระเบียบในการจัดทำโปรแกรมและขาดเครื่องมือที่จะใช้ในการควบคุมการจัดทำโปรแกรม

บริษัทควรมีการกำหนดระเบียบในการจัดทำโปรแกรม โดยกำหนดให้มี

- 11.1 โปรแกรมตรวจสอบความถูกต้องของข้อมูลนำเข้าก่อนนำไปใช้ประมวลผลในขั้นตอนต่อไป
- 11.2 การใช้ File Label พิสูจน์ความถูกต้องในการใช้แฟ้มข้อมูล
- 11.3 กำหนดจุดตรวจสอบความถูกต้องในการประมวลผลข้อมูลให้มากที่สุดเท่าที่จะปรับได้ซึ่งจุดตรวจสอบเหล่านี้สามารถใช้เป็นจุดตั้งต้นประมวลผลข้อมูลในขั้นตอนต่อไปได้โดยไม่จำเป็นต้องย้อนกลับไปประมวลผลใหม่ตั้งแต่เริ่มแรก
- 11.4 การบันทึกการรายการไว้ในระบบสำหรับใช้เป็นหลักฐานในการควบคุมและตรวจสอบ
- 11.5 การใช้โปรแกรมมาตรฐาน (Standardized Routine) ให้มากที่สุดเท่าที่จะเป็นไปได้
- 11.6 การจัดทำรายงานแสดงที่ผิดปกติในการประมวลผลข้อมูล

12. ไม่มีการกำหนดระเบียบในการจัดทำเอกสารประกอบระบบงานและโปรแกรม มีแต่การตกลงด้วยวาจา และการจัดทำเอกสารประกอบระบบงาน และโปรแกรมหักล้างมักล่าช้าอยู่เสมอและไม่ทันกาล ผลคือ

ขาดความเป็นมาตรฐานและความเป็นระบบระเบียบในการจัดทำเอกสารประกอบระบบงานและโปรแกรม และขาดเครื่องมือที่จะใช้ในการควบคุมการจัดทำเอกสารประกอบระบบงาน และโปรแกรมสำหรับกรณีที่ไม่มีการกำหนด ระเบียบในเรื่องดังกล่าว และเป็นสาเหตุส่วนหนึ่งที่ทำให้การจัดทำเอกสารประกอบระบบงานและโปรแกรมมีความล่าช้าอยู่เสมอและไม่ทันการ ทำให้เกิดความไม่สะดวกในการติดตามตรวจสอบหรือการแก้ไขในจุดใดจุดหนึ่ง

บริษัทควรกำหนดให้มีระเบียบในการจัดทำเอกสารประกอบระบบงานและโปรแกรมเป็นลายลักษณ์อักษร ทั้งนี้ โดยกำหนดรวมอยู่ในระเบียบปฏิบัติก่อนนำระบบงานใหม่ออกใช้งานจริงดังนี้

12.1 การตรวจรับระบบงานอย่างเป็นทางการโดยผู้ใช้อุปกรณ์และผู้ปฏิบัติงานคอมพิวเตอร์

12.2 การจัดตั้งคู่มือปฏิบัติงานชุดล่าสุดให้ผู้ใช้อุปกรณ์และผู้ปฏิบัติงานคอมพิวเตอร์

12.3 การฝึกอบรมผู้ใช้อุปกรณ์ให้เสร็จเรียบร้อย

12.4 การจัดทำเอกสารระบบงานและโปรแกรมให้เสร็จสมบูรณ์

สำหรับในระเบียบการจัดทำเอกสารระบบงานและโปรแกรม ควรกำหนดให้มี

- คำอธิบายระบบงาน
- ผังแสดงทางเดินของระบบงาน
- คำอธิบายโปรแกรม
- ผังแสดงรูปแบบการบันทึกข้อมูล และผังแสดงรูปแบบข้อมูลที่ได้จากการประมวลผล
- คำอธิบายวิธีการตรวจสอบความถูกต้องของข้อมูลนำเข้า และวิธีการควบคุมที่นำไปใช้ใน แต่ละโปรแกรม
- Source Listing ชุดปัจจุบัน
- คำสั่งที่ใช้ในการปฏิบัติงานสำหรับพนักงานในห้องคอมพิวเตอร์
- คู่มือปฏิบัติงานสำหรับผู้ใช้อุปกรณ์
- การบันทึกประวัติการแก้ไขโปรแกรม

13. ไม่มีการพิจารณาทบทวนภายหลังจากการนำระบบงานใหม่ออกใช้งานจริง ผลคือ

อาจมีการใช้งบประมาณ ระยะเวลา มากเกินความจำเป็น และผลที่ได้ไม่คุ้มค่าและไม่ทราบถึงปัญหา ที่อาจมีได้ในการปฏิบัติงานในระบบงานใหม่และไม่ได้ปรับปรุงให้ดีขึ้น

บริษัทควรกำหนดให้มีการพิจารณาทบทวนผลการปฏิบัติงานภายหลังจากที่ได้นำระบบงานออกใช้งานจริง ทั้งนี้ โดยครอบคลุมเรื่องดังต่อไปนี้

13.1 การวิเคราะห์ค่าใช้จ่ายในการพัฒนาระบบงานที่กำหนดไว้ในแผนงาน

13.2 การเปรียบเทียบค่าใช้จ่ายที่จะประหยัดได้ตามที่กำหนดไว้ในแผนงานกับค่าใช้จ่ายที่ประหยัดได้จริง

13.3 การเปรียบเทียบผลตอบแทนที่คาดว่าจะได้รับจากระบบงานใหม่กับผลตอบแทนที่ได้รับจริง

13.4 ปัญหาการปฏิบัติงานในระบบงานใหม่และการปรับปรุงแก้ไขให้ดีขึ้น

14. ไม่มีการจัดเอกสารให้เป็นปัจจุบัน (Up date) ทันทีที่มีการแก้ไขโปรแกรม ผลคือ

ทำให้ยากแก่การติดตามตรวจสอบและแก้ไขในครั้งต่อ ๆ ไป หรือในกรณีที่มีปัญหาต้องการใช้อ้างอิงก็อาจได้ข้อมูลที่ไม่เป็นปัจจุบันและมีการเปลี่ยนแปลงแก้ไขไปแล้ว ซึ่งอาจก่อให้เกิดความเสียหายได้

บริษัทควรจัดให้มีระเบียบการแก้ไขเอกสารระบบงานและโปรแกรมภายหลังการแก้ไขโปรแกรม โดยทันที และควรกำหนดให้มีการจัดเก็บรายละเอียดการแก้ไขโปรแกรมของแต่ละระบบงานไว้ทุกครั้งตามลำดับก่อนหลัง

15. ไม่มีการกำหนดระเบียบห้ามว่าโปรแกรมเมอร์ทำอะไรได้บ้างหรือห้ามทำอะไรบ้างโดยละเอียด เช่น การห้ามโปรแกรมเมอร์ใช้ข้อมูลจริงและโปรแกรมจริงที่อนุมัติให้ใช้งานแล้ว ตลอดจนการใช้เอกสาร Operating System ผลคือ

โปรแกรมเมอร์อาจกระทำการทุจริตในอันที่จะก่อให้เกิดประโยชน์แก่ตัวเองโดยง่ายเพราะเป็นผู้เชี่ยวชาญการใช้โปรแกรมอยู่แล้ว หากมีโอกาสเข้าถึงข้อมูลจริงย่อมสามารถทำการทุจริตได้ง่ายขึ้นและการเข้าถึง Operating System อันเป็นโปรแกรมควบคุมระบบนั้นนับว่าเป็นจุดอ่อนสำคัญ หากโปรแกรมเมอร์ผู้นั้นมีความรู้ความสามารถเพียงพอที่จะแก้ไขหรือทำให้ตนเองผ่านจุดควบคุมบางประการที่ Operating System ได้สร้างไว้เพื่อป้องกันผู้บุกรุกและผู้ไม่มีอำนาจไปได้

บริษัทควรกำหนดเป็นระเบียบห้าม Programmer ทุกคนใช้แฟ้มข้อมูลจริง และห้ามใช้เอกสาร Operating System และโปรแกรมที่ได้รับอนุมัติให้ใช้งานจริง ยกเว้นในกรณีจำเป็นต้องใช้ก็ให้อยู่ในการควบคุมและขออนุมัติจากหัวหน้าศูนย์คอมพิวเตอร์

16. ไม่มีการกำหนดระเบียบในการขอแก้ไขโปรแกรมอย่างเพียงพอและเป็นลายลักษณ์อักษรผลคือ

อาจมีช่องโหว่ที่เป็นจุดอ่อนที่ก่อให้เกิดความเสียหายในกรณีที่มีผู้เจตนาทุจริตทำการเปลี่ยนแปลงแก้ไขโปรแกรมโดยไม่ผ่านการอนุมัติ หรือข้ามขั้นตอนการควบคุมบางประการ

บริษัทควรกำหนดระเบียบในการขอแก้ไขโปรแกรมอย่างเพียงพอและเป็นลายลักษณ์อักษรและควรมีระเบียบกำหนดให้มีการตรวจสอบและมีการพิจารณาอนุมัติโปรแกรมที่มีการปรับปรุงหรือดัดแปลงให้ดีขึ้น ก่อนนำไปใช้งาน เช่นเดียวกับกรณีที่มีการแก้ไขโปรแกรม ระเบียบที่ว่าต้องเริ่มตั้งแต่

16.1 ระเบียบการทำหนังสือขออนุมัติแก้ไขโปรแกรม

16.2 ระเบียบการแก้ไขโปรแกรม ซึ่งกำหนดให้มี

- การให้หมายเลขหรือเลขลำดับลงในใบขออนุมัติแก้ไขโปรแกรมไว้ล่วงหน้า
- การชี้แจงปัญหาหรือเหตุผลในการแก้ไขโปรแกรมไว้ในใบขออนุมัติโดยละเอียด
- การขอความเห็นชอบจากผู้ที่ได้รับผลกระทบจากการแก้ไขโปรแกรมหรือผู้ที่เกี่ยวข้องทุกฝ่าย
- การระบุชื่อผู้ขอแก้ไขโปรแกรมไว้ในใบขออนุมัติแก้ไขโปรแกรม
- พนักงานชั้นบริหารควบคุมดูแลการแก้ไขโปรแกรม และลงนามให้ความเห็นชอบกำกับใบขออนุมัติ
- การส่งสำเนาใบขออนุมัติแก้ไขโปรแกรมให้ผู้ตรวจสอบภายในให้ครบถ้วนทุกครั้ง

16.3 มีระเบียบกำหนดให้หน่วยงานที่มีหน้าที่จัดทำโปรแกรมต้องพิจารณาทบทวนความเหมาะสมในการแก้ไขโปรแกรมก่อนรับไปดำเนินการ

16.4 ระเบียบการพิจารณาคำขอแก้ไขโปรแกรม ซึ่งมีข้อกำหนดเกี่ยวกับ

- วิธีการที่จะเลือกใช้ในการแก้ไขโปรแกรม
- ค่าใช้จ่ายในการแก้ไขโปรแกรม
- ระยะเวลาที่จำเป็นต้องใช้ในการแก้ไขโปรแกรม

17. มีการเก็บเอกสารประกอบระบบงานและโปรแกรมทั้งที่ใช้งานจริงแล้วและกำลังอยู่ในระหว่างการพัฒนา ตลอดจนเอกสารประกอบ Operating System ไว้ในที่เดียวกันและโปรแกรมเมอร์เข้าถึง ผลคือ

(เหมือนข้อ 15)

จุดอ่อนด้านความน่าเชื่อถือของข้อมูล (ข้อ 18 -19)

18. ไม่มีการควบคุมการจัดทำรายงานและการจัดส่งรายงานให้ผู้ใช้อข้อมูลให้เป็นไปตามตารางเวลาที่กำหนดให้ออกรายงาน ทำให้มีความล่าช้าอยู่เสมอ ผลคือ

ทำให้การทำงานของผู้ใช้ไม่คล่องตัว และอาจลดประสิทธิภาพลง ในกรณีที่เป็นข้อมูลสำคัญอาจกระทบกระเทือนต่อธุรกิจ

ควรมีการควบคุมการจัดทำรายงานและการจัดส่งรายงานให้ผู้ใช้อข้อมูลให้เป็นไปตามตารางเวลาที่กำหนด นอกจากนี้ ต้องมีการจัดส่งข้อมูลให้ถูกตัวผู้ใช้อข้อมูลและมีการควบคุมข้อมูลของลูกค้ำที่ปรากฏอยู่ในรายงานคอมพิวเตอร์ด้วยวิธีการที่เหมาะสม

สำหรับในกรณีที่มียาการที่นำเข้าประมวลผลไม่ได้ไม่ว่าด้วยสาเหตุใด จะต้องมียาการคอมพิวเตอร์แสดงรายละเอียดของรายการเหล่านั้นและใช้ควบคุมในการนำข้อมูลเหล่านั้นมาประมวลผลใหม่อีกครั้ง และต้องมีการกระทบยอดรายการที่คอมพิวเตอร์ไม่ยอมรับ กับรายงานแสดงรายละเอียดของข้อมูลทุกรายการที่ส่งเข้าประมวลผล และมีการสอบยันยอดที่ผู้ใช้อข้อมูลจัดทำด้วยมือกับยอดที่ได้จากการประมวลผล ตลอดจนมีการจัดส่งรายงานแสดงรายการที่คอมพิวเตอร์ไม่ยอมรับ และข้อมูลที่คอมพิวเตอร์บันทึกรายการไม่ได้กลับไปให้ผู้ใช้อข้อมูล

นอกจากนี้ จะต้องมียาการชั้นบริหารอนุมัติการปรับปรุงแก้ไขข้อมูลนำเข้าในกรณีที่มิ

- รายการที่หน่วยงานคอมพิวเตอร์รับมาจากผู้ใช้อข้อมูลแต่ไม่ได้เข้าประมวลผล
- รายการที่หน่วยงานคอมพิวเตอร์จัดทำแทนผู้ใช้อข้อมูลหรือจัดทำเพิ่มเติมจากรายการที่ผู้ใช้อข้อมูลจัดส่งมาให้

19. ไม่มีการตรวจสอบ Console log ผลคือ

อาจทำให้ไม่ทราบว่ามีสิ่งผิดปกติเกิดขึ้นในการประมวลผล เช่น มีการแอบเอารายงานอื่นมาประมวลผล ซึ่งเป็นการขโมยเวลาเครื่อง หรือมีการใช้โปรแกรมไม่ถูกต้อง หรือใช้เวลาในการประมวลผลนานผิดปกติ หรือมีการประมวลผลข้ามขั้นตอนงานบางอย่าง หรือมีปัญหาข้อขัดข้องบางอย่างในการประมวลผล เป็นต้น

ควรมีการตรวจสอบ Console log เป็นครั้งคราวตามสมควร

จุดอ่อนด้านการปฏิบัติงานคอมพิวเตอร์ (ข้อ 20 - 34)

20. ที่ตั้งศูนย์คอมพิวเตอร์ ตั้งอยู่ในชั้น 3 ซึ่ง ชั้น 1, 2, 4 และ 5 เป็นชั้นที่เปิดรับลูกค้า จึงมีคนพลุกพล่านอยู่เสมอ ซึ่งไม่เหมาะสม เพราะมีการเข้าถึงได้ง่าย และป้องกันลำบาก

บริษัทควรเลือกที่ตั้งของศูนย์คอมพิวเตอร์ที่ไม่มีคนพลุกพล่านจนเกินไป อย่างไรก็ตามหากมีการตั้งศูนย์คอมพิวเตอร์ไปแล้ว และการโยกย้ายต้องสิ้นเปลืองสูง ก็ควรทำให้มิดชิดและมีการควบคุมเพื่อป้องกันการเข้าถึงโดยรัศุม และเข้มแข็ง

21. มีการแสดงศูนย์คอมพิวเตอร์ในลักษณะที่เด่นจนเกินไป นับตั้งแต่ป้ายตัวโตระบุว่าเป็นห้องคอมพิวเตอร์ และมีการใช้ผาผนังห้องเป็นกระจกใสที่มองเห็นทะลุถึงทั้งใน ซึ่งเป็นการโจ่งแจ้งมากเกินไป และทำให้ผู้มีเจตนาไม่สุจริต หรือมีเจตนาร้ายสามารถเข้าถึงได้โดยง่าย

บริษัทไม่ควรแสดงศูนย์คอมพิวเตอร์ให้โจ่งแจ้งจนเกินไป และไม่ควรติดป้ายตัวโต หรือทำผนังห้องเป็นกระจกใส ถ้าไม่จำเป็นก็ไม่ควรติดป้ายบอกเลยว่าเป็นศูนย์คอมพิวเตอร์ สำหรับผาผนังที่เป็นกระจกใสควรติดฟิล์มเสีย หรือใช้กระจกสีขุ่น หรือใช้ม่านปิด

22. ทั้งชั้นที่เป็นที่ตั้งของศูนย์คอมพิวเตอร์มียามเฝ้าอยู่คนเดียว และเมื่อยามเดินกลับไปเข้าห้องน้ำก็จะไม่มีใครเฝ้าอยู่ที่บริเวณหน้าประตูศูนย์เลย และประตูศูนย์คอมพิวเตอร์เองปิดช้า ชนิดที่ถ้ามีคนผลุบตามคนหน้าที่มีบัตรเสียบบประตูผ่านได้ ก็จะไม่มีความผิดปกติเกิดขึ้นเลย ซึ่งถึงแม้ประตูจะใช้ระบบบัตรเสียบบเพื่อพิสูจน์ตัวผู้มีสิทธิเข้าออกศูนย์คอมพิวเตอร์แล้วโดยรัศุม และเปิดประตูเพียงบานเดิมให้เข้าออกทีละคนก็ตาม

ควรมีการจัดเวลาที่เคาน์เตอร์ประตูทางเข้าศูนย์ เมื่อผ่านประตูเข้ามาแล้วต้องลงนามในทะเบียนเป็นครั้งคราวว่ามีการมอบบัตรเสียบบประตูเพื่อผ่านเข้าออกให้ผู้อื่นใช้แทนหรือไม่ เพราะเมื่อเสียบบัตรระบบจะบันทึกว่าเป็นบัตรของใครใช้ผ่านเข้าออกเวลาใด นอกจากนี้ควรแก้ไขให้ประตูปิดเร็วขึ้นหรือใช้กลไกล็อคให้เข้าได้ทีละคนเท่านั้นเมื่อประตูเปิด

23. ทางเข้าออกศูนย์คอมพิวเตอร์มีมากจนเกินไป ซึ่งมีความเสี่ยงต่อการเข้าถึงโดยง่ายและทำให้การป้องกันการเข้าถึงมีความลำบากมากขึ้น

ควรจัดให้มีช่องทางเข้าออกศูนย์คอมพิวเตอร์น้อยทางที่สุดเท่าที่จำเป็น การมีช่องทางเข้าออกถึง 2 ช่องทางก็นับว่ามากแล้ว ถ้าช่องทางเดียวก็จะควบคุมได้ง่ายขึ้น แต่ทั้งนี้ช่องทางดังกล่าวต้องกว้างพอให้เข้าออกได้โดยง่ายกรณีเกิดเหตุฉุกเฉิน

24. มีการวางกองกระดาษรายงานจำนวนมากไว้ในศูนย์คอมพิวเตอร์ซึ่งเป็นเชื้อไฟได้โดยง่าย ควรเคลื่อนย้ายเอกสารที่ไม่จำเป็นนำไปเก็บไว้ที่อื่น

ควรเคลื่อนย้ายเอกสารที่ไม่จำเป็นไปเก็บไว้ที่อื่น

25. ภายในห้องเครื่องชั้นในของศูนย์คอมพิวเตอร์ ไม่มีการควบคุมการเข้าออกโดยรัศุมไม่มีการบันทึกทะเบียนผู้เข้าออก ไม่มีการใช้บัตรเสียบบประตูเพื่อผ่าน ไม่มีพนักงานเฝ้าตรงทางเข้าออกโดยเฉพาะซึ่งห้องเครื่องชั้นในนั้นเป็นจุดที่ Sensitive มากที่สุดเพราะเป็นที่ตั้งอุปกรณ์คอมพิวเตอร์และเป็นที่เก็บสื่อข้อมูลต่าง ๆ หากสามารถเข้าถึงส่วนนี้ได้ก็มีโอกาสเข้าสู่ระบบได้ง่ายขึ้น

ควรมีการควบคุมการเข้าออกห้องเครื่องชั้นในของศูนย์คอมพิวเตอร์โดยรัดกุม และมีการบันทึกผู้ผ่านเข้าออกด้วยเพื่อสามารถใช้เป็นหลักฐานในการติดตามตรวจสอบได้ต่อไปกรณีที่เกิดปัญหา

26. มีการกำหนดตารางการปฏิบัติงานคอมพิวเตอร์และมอบหมายผู้รับผิดชอบ แต่ในทางปฏิบัติมีการฝกงานกันและสับเปลี่ยนเวรกันอย่างไม่เป็นทางการ และไม่เป็นไปตามระเบียบ นอกจากนี้ยังไม่มี การบันทึกการเข้ารับช่วงงานในเวลาต่าง ๆ และลงลายมือชื่อไว้อีกด้วย ผลคือ

ในกรณีที่มีปัญหาเกิดขึ้นจะทำให้ติดตามหาตัวผู้รับผิดชอบลำบากและอาจเกิดความสับสน ทำให้เกิดการสวมรอยขึ้นได้โดยง่าย

ควรมีการกวดขันให้มีการปฏิบัติตามระเบียบและตารางการปฏิบัติงาน ในกรณีที่บุคคลที่รับผิดชอบไม่สามารถมาปฏิบัติหน้าที่ได้ ต้องมีการกำหนดผู้รับผิดชอบแทน และต้องมีการบันทึกลายมือชื่อแสดงความรับผิดชอบในช่วงเวลาที่เข้าทำหน้าที่แทน ในกรณีที่ปฏิบัติงานตามปกติต้องลงลายมือชื่อแสดงความรับผิดชอบในช่วงเวลานั้น ๆ เสมอ

27. โปรแกรมเมอร์สามารถเข้าห้องเครื่องได้ โดยมีเหตุผลที่ไม่สมควร ซึ่งการที่โปรแกรมเมอร์เข้าไปภายในห้องเครื่องได้ ย่อมเป็นไปได้ว่าโปรแกรมเมอร์มีโอกาสที่จะเข้าถึงแฟ้มข้อมูลจริงและโปรแกรมที่นำออกใช้งานจริงแล้วได้โดยง่าย ซึ่งอาจเป็นอันตรายอย่างยิ่ง

ควรมีระเบียบห้ามเด็ดขาด ไม่ให้โปรแกรมเมอร์เข้าไปภายในห้องเครื่องคอมพิวเตอร์และที่เก็บสื่อแม่เหล็กซึ่งมีแฟ้มข้อมูลจริงบรรจุอยู่

28. ไม่มีการกำหนดตัวบุคคลที่มีสิทธิเข้าไปในห้องเก็บเทปและจานแม่เหล็กโดยเฉพาะ แต่ใช้วิธีอนุญาตให้พนักงานปฏิบัติการเข้าไปหยิบได้เอง โดยขอกุญแจจากหัวหน้าศูนย์ หรือเลขานุการทุกครั้งที่ต้องการ และการจัดเก็บเทปและจานแม่เหล็กไม่มีใครเป็นระเบียบเรียบร้อย และป้ายชื่อเทปบางม้วนก็หลุดห้อยอยู่ ผลคือ

ระเบียบเรียบร้อย และป้ายชื่อที่หลุดม้วนอยู่ อาจทำให้เกิดการหยิบ File ผิดและเกิดความเสียหายรุนแรงได้

29. ไม่มีระเบียบกำหนดและไม่เคยมีการปฏิบัติในการตรวจนับสื่อต่าง ๆ เลย ผลคือ

สื่อแม่เหล็กที่เก็บข้อมูลสำคัญอาจสูญหายได้โดยที่ไม่ทราบ เพราะนานครั้งจึงหยิบใช้ครั้งหนึ่งและสื่อเปล่าก็อาจถูกขโมยออกไปเพื่อหาประโยชน์ได้

บริษัทควรกำหนดให้มีระเบียบและมีการปฏิบัติในการตรวจนับสื่อต่าง ๆ เป็นระยะ ๆ ตามเหมาะสม ซึ่งควรจะเป็นหน้าที่ของผู้ตรวจสอบภายใน

30. ไม่มีการ Back up ข้อมูล โปรแกรม เอกสารระบบงานและโปรแกรม (ทั้ง Application programme, O/S และ Utility programme) ไว้ภายนอกศูนย์ หรือที่สถานที่อื่นนอกอาคารหรือบริเวณนั้น มีแต่การ Back up ข้อมูลและโปรแกรมไว้ในศูนย์คอมพิวเตอร์เอง ผลคือ

ถ้าเกิดภัยพิบัติขึ้น ไม่ว่าโดยธรรมชาติหรือโดยการกระทำของมนุษย์ และมีผลให้ศูนย์คอมพิวเตอร์เสียหายใช้งานไม่ได้ หรือทั้งอาคารประกันภัยแล้ว บริษัทจะไม่สามารถหาแฟ้มข้อมูลและโปรแกรมที่จะนำมาประมวลผล

ได้อย่างทันท่วงที และอาจต้องใช้เวลาานมากกว่าจะกู้สถานะได้และอาจต้องหยุดการดำเนินงานไป ซึ่งหมายถึงการหยุดชะงักของธุรกิจด้วย เนื่องจากข้อมูลสำคัญส่วนใหญ่ถูกทำลายลง ซึ่งผลเสียหายอาจมากมายจนประเมินไม่ถูก

บริษัทควรมีการ Back up ข้อมูลและโปรแกรมรวมทั้งเอกสารระบบงานและโปรแกรมไว้ภายนอกศูนย์คอมพิวเตอร์ หรือนอกอาคารดังกล่าว โดยเก็บรักษาไว้ในสถานที่ที่มั่นคงปลอดภัย และมีการป้องกันการเข้าถึงอย่างเข้มงวดและรัดกุม และเมื่อเกิดเหตุฉุกเฉินสามารถนำมาใช้ได้ทันทีโดยไม่มีปัญหา

31. และ 32. มีร่องรอยของการไม่ปฏิบัติตามระเบียบที่ห้ามรับประทานอาหารหรือเครื่องดื่มและสูบบุหรี่ในห้องเครื่องคอมพิวเตอร์ และมีการนำไฟฉาย ซึ่งอาจมีส่วนประกอบที่เป็นสารแม่เหล็กและเกิดอันตรายต่อแฟ้มข้อมูลได้

ควรมีการกวดขันและเข้มงวดในการให้พนักงานปฏิบัติตามการทำตามระเบียบที่วางไว้ และกำหนดโทษหากมีการฝ่าฝืน และกวดขันให้มีการรักษาความสะอาดให้เข้มงวด

33. การซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ (Preventive Maintenance) ไม่เป็นไปตามเวลาที่กำหนด ผลคืออาจมีบางชิ้นส่วนเสื่อมสภาพหรือมีปัญหา แต่ยังไม่มีผลกระทบทั้งระบบถ้าได้พบเสียก่อนและเปลี่ยนกันตามตารางเวลาที่กำหนดให้มีการซ่อมบำรุง และเมื่อพบชำรุดเกินไป อาจทำให้กระทบกระเทือนทั้งระบบแล้วก็ได้ หรือถ้ามีการทำ PM ตามระยะเวลาที่กำหนด ก็จะช่วยให้อุปกรณ์คอมพิวเตอร์ทำงานได้อย่างไม่มีปัญหาและมีอายุยาวนานขึ้น แต่การทำ PM ลำช้า อาจทำให้อุปกรณ์คอมพิวเตอร์ได้รับการทำนุบำรุงโดยเหมาะสมกับชั่วโมงการใช้งานอุปกรณ์เหล่านั้นอาจล้าและเกิดความบกพร่องได้ง่าย

ควรมีการเจรจากับทางบริษัทผู้ขายที่ทำหน้าที่ซ่อมบำรุงให้มีการปฏิบัติตามตารางเวลาการทำ PM ที่ตกลงกันไว้อย่างเคร่งครัด

34. กรณีที่อุปกรณ์คอมพิวเตอร์และเครื่องคอมพิวเตอร์เกิดขัดข้องเสียหายมีการบันทึกทะเบียนไว้แต่ไม่ละเอียดเท่าที่ควร เช่น ไม่มีการบันทึกว่าเสียหายนานเท่าใด ถี่ห่าง บ่อยครั้ง แคไหน มีสาเหตุเพราะอะไร ตลอดจนทำการแก้ไขอย่างไร โดยใคร และใครรับผิดชอบดูแลระหว่างเจ้าหน้าที่ประเมินไม่ได้หรือไม่ทราบ ว่า เหตุขัดข้องที่เกิดขึ้นส่วนใหญ่มาจากอะไร แก้ไขเหมาะสมหรือไม่ หรือควรดำเนินมาตรการอย่างไร เพื่อลดข้อบกพร่องหรือข้อขัดข้องดังกล่าว และแต่ละครั้งที่เกิดขัดข้องสร้างความเสียหายมากน้อยเพียงใด และควรดำเนินการต่อไปอย่างไรหรือไม่ เป็นต้น นอกจากนี้ไม่ทราบว่าผู้รับผิดชอบในกรณีที่มีการแก้ไขข้อขัดข้องแต่ละครั้งคือใคร หากมีปัญหาก่อขึ้นในภายหลังจะติดตามตัวและหาผู้รับผิดชอบไม่ได้

ควรกำหนดระเบียบให้มีการบันทึกทะเบียนการแก้ไขข้อขัดข้องที่เกิดขึ้นกับระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ทั้งหลายโดยละเอียดครบถ้วน เพื่อประโยชน์ในการติดตามและดำเนินการต่อไป

แนวคำตอบ กรณีศึกษา 7
บริษัท เอส.เอ.อินเตอร์เทรด จำกัด
ภาค 2
(การตรวจสอบระบบงาน - Application)

ระบบงานขายและรับเงิน

1. การให้พนักงานทุกคนรับคำสั่งซื้อและป้อนข้อมูลได้โดยตรง ไม่เป็นการดีนักทั้งนี้ เพราะอาจเกิดข้อผิดพลาดและปฏิบัติไม่เป็นระเบียบ รายการตกหล่นขาดหาย หรือมีการป้อนข้อมูลซ้ำซ้อน มีผลกระทบต่อการควบคุมความครบถ้วนถูกต้องของรายการขอซื้อของลูกค้า เช่น กรณีมีรายการขอซื้อทั้งจากเคาน์เตอร์ขาย จากทางไปรษณีย์ หรือจากทางโทรศัพท์ ดังนั้น ควรมอบหมายให้ผู้หนึ่งผู้ใดจัดการควบคุมรายการขอซื้อทั้งหมด โดยรับเข้ามาและ Running number เอกสารการขอซื้อเหล่านั้นเป็นหลักฐาน

การไม่เปลี่ยนแปลง Password เป็นระยะ ๆ จะทำให้ผู้อื่นสังเกตเห็นได้ง่ายและอาจมีการแอบเอาไปใช้โดยเจ้าของ Password ไม่ทราบ

การที่ระบบฟ้องเมื่อมีการเปลี่ยน Password มาเหมือนกัน โดยขึ้นเป็นข้อความเตือนนั้นเป็นการดีแต่การที่ระบบยังยินยอมให้ใช้ Password ที่ซ้ำนั้นต่อไปได้ เป็นเรื่องที่ไม่ใครจะสมควร เพราะอาจเกิดกรณีที่ นาย ข บังเอิญเปลี่ยน Password ไปซ้ำกับนาย ก. นาย ข. จึงขอเปลี่ยนกลับ แล้วแอบใช้ Password ของนาย ก. โดยนาย ข. เองก็อาจไม่ทราบว่า Password ของใคร เพียงแต่รู้ว่าสามารถใช้เพื่อเข้าถึงระบบได้

2. การอนุมัติเครดิตจะขึ้นกับผู้จัดการขายไม่ได้ เป็นจุดอ่อนที่อันตราย การอนุมัติเครดิตเป็นเรื่องของผู้จัดการสินเชื่อที่จะพิจารณา ซึ่งจะต้องไม่ใช่ฝ่ายขาย หรือฝ่ายบัญชีลูกหนี้

3. ควรมีการกำชับให้ผู้ป้อนรายการใช้ความระมัดระวังให้มาก และในด้านการจัดทำเอกสารเองต้องพยายามเขียนให้ชัดเจน อ่านง่าย เพื่อความสะดวกในการดูแลโอกาสที่จะผิดพลาด

นอกจากนี้ อาจกำหนดในโปรแกรมให้มีการเช็คสอบความถูกต้องของหน่วยขายโดยถามย้ำอีกครั้งว่าหน่วยอะไร เพื่อผู้ป้องกันจะได้ป้อนซ้ำเป็นการ Verify อีกครั้ง

4. รัดกุมดีอยู่แล้ว

5. การใช้ Check digit ในแบบ Modulus 10 และมีการใช้ตัวถ่วงน้ำหนัก ตัวท้ายเป็น 5 จะทำให้ Check digit ของหมายเลขประจำตัวบัญชีลูกหนี้ที่ต่างกันมีค่า Check digit ซ้ำกันหรือเหมือนกัน เพิ่มโอกาสที่จะป้อนเลขที่บัญชีผิดและผ่านการตรวจสอบ Check digit ไปได้โดยง่าย

6. รัดกุมดีอยู่แล้ว

7. ควรมีการติดตามรายการสั่งซื้อที่ยังไม่ได้จัดส่งของไปให้ลูกค้าอยู่เสมอ และถ้ารายการใดเป็นรายการที่ไม่มีของจะส่งให้ เมื่อมีของก็ต้องรีบจัดส่งโดยเร็ว ไม่ควรทิ้งให้ค้างอยู่

8. เนื่องจากสินค้าส่วนใหญ่เป็นสินค้าที่มีการใช้ Bar code อยู่ข้างกล่อง หรือภาชนะบรรจุ ดังนั้นจึงน่าจะสะดวกมากกว่าหากจะใช้ OCR (Optical Character Reader) เพราะเมื่อรูดสินค้าโดยหันด้านที่มี Bar code ผ่านเครื่องอ่าน OCR ระบบจะทำการบันทึกรายการขาย ตัดสต็อกสินค้า และเพิ่มรายการเงินสดรับหรือลูกหนี้ทันที ซึ่งช่วยอำนวยความสะดวกและลดโอกาสผิดพลาดในการป้อนข้อมูลได้มาก

9. รัดกุมดีอยู่แล้ว

10. ควรมีการเทียบยอดลูกหนี้รายตัวกับบัญชีคุมยอดเป็นระยะ อย่างน้อยทุกเดือน

ระบบงานซื้อและจ่ายเงิน

1. การปรับปรุงเพิ่มข้อมูลผู้ขาย ไม่ควรให้พนักงานระดับล่างรับผิดชอบ เพราะเป็นเรื่องที่สำคัญควรมอบให้พนักงานระดับผู้มีอำนาจอนุมัติ รับผิดชอบในการแก้ไข นอกจากนี้การที่เพิ่มข้อมูลผู้ขายไม่มีใครเป็นปัจจุบัน อาจทำให้บริษัทเสียประโยชน์ส่วนที่พึงได้ ในขบวนการสอบทานและคัดเลือกผู้ขายก็ได้

2. ในช่วงของการป้อนข้อมูลรายการสั่งซื้อ จากรายงานสินค้าที่ต้องสั่งซื้อซึ่งผ่านการสอบทานและอนุมัติจากแผนกคลังสินค้าแล้วนั้น ไม่ได้มีการตรวจสอบรายงานดังกล่าวกับใบสั่งซื้อที่จัดพิมพ์ขึ้น ทำให้เกิดข้อผิดพลาดดังกล่าว

3. เพื่อความสะดวกในกรณีที่ส่งของไปแล้ว และเกิน 2 สัปดาห์แล้วยังไม่ได้รับของควรให้คอมพิวเตอร์พิมพ์รายงาน Exceptional Report แสดงรายละเอียดรายการสั่งซื้อเหล่านั้น เพื่อจะได้ติดตามเร่งรัดผู้ขายต่อไปอย่างมีประสิทธิภาพ

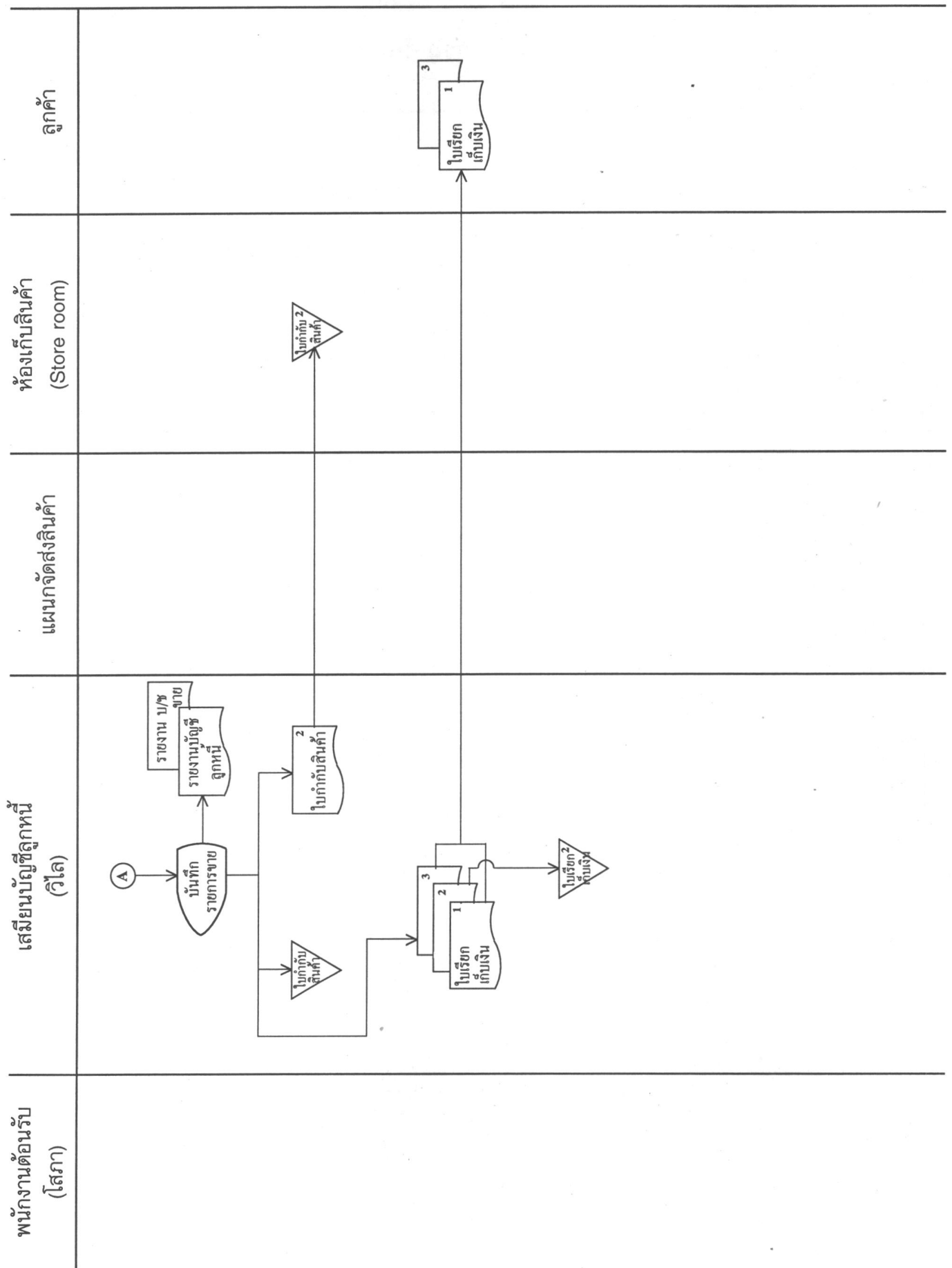
4. มีจุดอ่อนใน Flowchart ระบบงานซื้อ ON LINE แผ่นที่ 2 (การรับของ) กล่าวคือไม่มีการตรวจสอบของที่รับและใบส่งของ กับใบสั่งซื้อเลยนั่นเอง และเมื่อมีการป้อนข้อมูลเข้าสู่คอมพิวเตอร์ ก็ไม่มีการฟ้องในจุดดังกล่าวนี้ ซึ่งการแก้ไขจะต้องกระทำโดยกำหนดให้มีการตรวจสอบของที่รับกับรายละเอียดในใบส่งของและในใบสั่งซื้อด้วย และโปรแกรมควรเช็คสอบ และฟ้องให้ทราบเมื่อรายการรับของแตกต่างจากรายการสั่งซื้อสำหรับสินค้าหรือวัตถุดิบรายการนั้น ๆ

5. ถ้าหน่วยคอมพิวเตอร์มีหน้าที่ในการพิมพ์เช็ค ซึ่งจะส่งไปชำระหนี้อย่างน้อยต้องมีการควบคุมเพื่อป้องกันมิให้มีการชำระหนี้ ซึ่งเข้าช้อนหรือจ่ายเงินให้เจ้าหนี้ผิดราย แผนกบัญชีเจ้าหนี้ควรจะเป็นผู้กำหนดหมายเลขบัญชีเจ้าหนี้รายตัวและมีการตรวจสอบหมายเลขเหล่านี้เป็นครั้งคราว เพื่อป้องกันการจ่ายเงินที่ไม่เหมาะสมหรือจ่ายเงินให้เจ้าหนี้ผิดราย ก่อนที่จะส่งเช็คที่พิมพ์แล้วไปยังเจ้าหนี้ ควรจะต้องส่งกลับไปตรวจสอบความถูกต้องยังแผนกบัญชีเจ้าหนี้อีกครั้งหนึ่ง

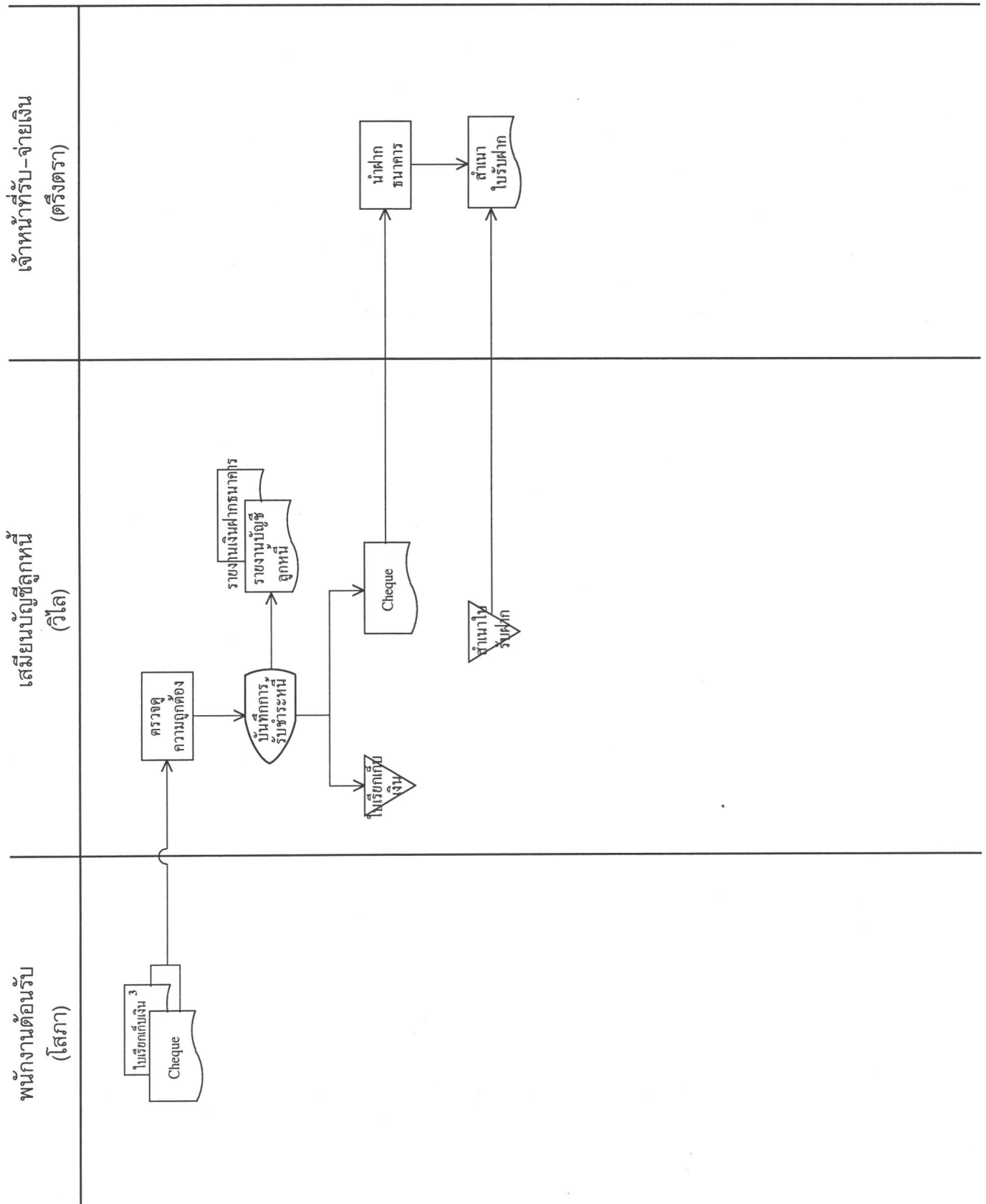
แนวคำตอบ กรณีศึกษา 8 - Data Center
บริษัท ชีอตรง จำกัด

ลำดับ	จุดอ่อนของการควบคุมใน	ความเสียหายที่อาจเกิดขึ้น	ข้อเสนอแนะการควบคุม
1.	ที่ประตูทางเข้าไม่มีพนักงานรักษาความปลอดภัยเฝ้าอยู่ใช้แต่เครื่องอ่านบัตรตรวจสอบผู้ที่เข้าไปในศูนย์คอมพิวเตอร์แต่เพียงอย่างเดียว	อาจมีบุคคลอื่นถือโอกาสเดินตามคนที่มึ่บัตรเข้าไปก่อนที่จะประตูจะปิดได้	ควรจัดให้มีพนักงานรักษาความปลอดภัยเฝ้าอยู่หน้าประตู และมีสมุดจดบันทึกรายละเอียดของผู้ที่เข้าไปในศูนย์โดยไม่มีบัตร เช่น มาติดต่อธุระ ซ่อมเครื่อง
2.	ประตูห้องเปิดอยู่ตลอดเวลาโดยมีอุปกรณ์ดับเพลิงขนาดเล็กค้างอยู่	เปิดโอกาสให้บุคคลที่ไม่ได้รับอนุญาตเข้าไปภายในศูนย์คอมพิวเตอร์ได้ โดยไม่มีผู้ใดทราบ	ควรย้ายอุปกรณ์ดับเพลิงออกไปติดตั้งไว้ที่ ๆ หยิบใช้ได้สะดวกและให้ประตูปิดสนิทตลอดเวลาจะเปิดต่อเมื่อมีบัตรที่ถูกต้องเสียบเข้าที่เครื่องอ่านบัตรเท่านั้น
3.	อุปกรณ์ดับเพลิงขนาดใหญ่ติดอยู่กับฝาผนังข้างหลังตู้ขนาดใหญ่ต้องใช้เวลาานกว่าจะนำออกมาใช้งานได้	ถ้าเกิดเพลิงไหม้จะไม่สามารถนำอุปกรณ์ดับเพลิงมาใช้งานได้ทันที อาจทำให้สูญเสียอุปกรณ์คอมพิวเตอร์ แฟ้มข้อมูล ฯลฯ ซึ่งอาจก่อให้เกิดความเสียหายทางธุรกิจ กระทบต่อฐานะการเงินและการทำกำไร	ควรติดตั้งอุปกรณ์ดับเพลิงไว้ในที่ ๆ หยิบใช้ได้สะดวก ทันท่วงที
4.	ไม่มีการทดสอบการทำงานของอุปกรณ์ดับเพลิงเป็นเวลานานถึง 12 ปี	น้ำยาดับเพลิงอาจหมดอายุไม่สามารถดับเพลิงได้ เมื่อเกิดเพลิงไหม้ และอาจก่อให้เกิดความเสียหายเช่นเดียวกับข้อ 3	ควรมีการทดสอบการทำงานของอุปกรณ์เป็นระยะ ๆ เช่น ทุก 6 เดือน หรือทุกปี
5.	มีหน้าต่าง ประตูไปสู่ห้องเก็บสื่อและเอกสารต่าง ๆ เปิดอยู่ตลอดเวลา	เปิดโอกาสให้บุคคลที่ไม่ได้รับอนุญาตเข้าไปในห้องคอมพิวเตอร์ได้ โดยไม่ต้องผ่านการตรวจสอบก่อน	ห้องคอมพิวเตอร์ควรเป็นห้องปิดมิดชิด ไม่มีหน้าต่าง (ควรโอบกปูนเป็นกำแพง) และมีประตูเข้า-ออกทางเดียว

ลำดับ	จุดอ่อนของการควบคุมใน	ความเสียหายที่อาจเกิดขึ้น	ข้อเสนอแนะการควบคุม
6.	ห้องคอมพิวเตอร์อยู่ติดกับห้องครัว	อาจเกิดเพลิงไหม้ได้ง่าย และเขม่า คว้น ฝุ่นละอองจากห้องครัว อาจทำให้เครื่องคอมพิวเตอร์เสียหายได้ ความร้อนอาจจะทำลายข้อมูลเสียหายได้	ควรย้ายห้องครัวไปไว้ที่ส่วนอื่นของอาคารให้ห่างไกลจากห้องคอมพิวเตอร์
7.	บรรณารักษ์ไม่ควบคุมทรัพย์สินและปล่อยให้พนักงานห้องเครื่องหยิบเทปข้อมูลได้เอง	ม้วนเทปที่เก็บข้อมูลที่เป็นความลับของกิจการ หรือข้อมูลที่ต้องใช้ อาจถูกขโมยหรือทำให้เสียหายได้	ควรกำชับให้บรรณารักษ์ควบคุมการใช้ทรัพย์สิน จัดให้มีสมุดลงนามยืม-คืนเทปข้อมูลหรือเอกสาร และมีให้ผู้ที่ไม่มีกิจธุระเข้ามาหยิบสิ่งของได้
8.	ม้วนเทปข้อมูลชุดสำรองกองไว้ที่พื้นห้อง	ม้วนเทปอาจสูญหาย หรือถูกทำลาย หรือถูกนำไปใช้โดยไม่ได้รับอนุญาตข้อมูลที่เป็นความลับอาจถูกเปิดเผยหรือมีการแก้ไขข้อมูล	ควรจัดเก็บม้วนเทปไว้ในตู้มีป้าย (label) ปิดบอกรายละเอียดไว้ และจัดทำทะเบียนการยืม-คืน พร้อมทั้งให้บรรณารักษ์ตรวจนับเป็นครั้งคราว
9.	จากการที่สมุดเซ็นรับม้วนเทปลงวันที่เมื่อสัปดาห์ก่อนแสดงว่าไม่มีการควบคุมให้มีการเซ็นรับ-ส่งม้วนเทปทุกครั้งที่น่าออกไปจากห้อง	ขาดเครื่องมือในการควบคุมม้วนเทป เนื่องจากไม่ได้ใช้สมุดเซ็นรับ-ส่ง เมื่อมีคนมาหยิบม้วนเทปไปใช้โดยเคร่งครัด	กำหนดเป็นระเบียบให้บรรณารักษ์ถือปฏิบัติโดยเคร่งครัด ในการใช้สมุดเซ็นรับ-ส่ง ควบคุมการนำม้วนเทปออกไปจากห้อง
10.	จดรหัสลับ (Password) ไว้บนกระดานแขวนที่ผนังห้องเป็นการเปิดเผย	รหัสลับจะไม่เป็นความลับ ทำให้การเข้าถึงระบบคอมพิวเตอร์เป็นสาธารณะ ไม่เป็นส่วนบุคคลเฉพาะที่ได้รับอนุญาต	มีการควบคุมให้แน่ใจว่า Password เป็นความลับจริง ๆ และมีการดูแลรักษาความปลอดภัยอยู่ตลอดเวลา



2. การรับชำระค่าสินค้า



จุดอ่อนในการควบคุมและข้อแนะนำ

1. ควรมีการกำหนดเลขที่ของเอกสารไว้ล่วงหน้า เพื่อควบคุมความครบถ้วนของเอกสารได้แก่ ใบกำกับสินค้า ใบเรียกเก็บเงิน
2. เอกสารควรมีการออกแบบให้ครอบคลุมประเภทของข้อมูลที่ต้องการ เช่น วันที่สั่งซื้อวันที่ต้องการสินค้า ชื่อลูกค้า ฯลฯ ทั้งนี้ เพื่อสะดวกในการบันทึกการขายและการควบคุม
3. ควรมีการตรวจสอบความถูกต้องของข้อมูลในเอกสารต่าง ๆ ก่อนที่จะบันทึกข้อมูลเข้าเครื่องคอมพิวเตอร์ และก่อนจะส่งเอกสารไปให้ลูกค้า
4. ห้องเก็บสินค้าควรมีใบกำกับสินค้าเป็นสำเนาเก็บไว้หลังจากส่งสินค้าให้แก่แผนกรับ-ส่งสินค้า มิใช่ส่งมาให้ในภายหลัง
5. การรับชำระค่าสินค้า หลังจากตรวจสอบความถูกต้องของเช็คแล้ว ควรมีสมาชิกทะเบียนบันทึกการรับเช็ค ก่อนส่งเช็คให้คุณดรีงตรา (Cashier) นำฝากธนาคาร แล้วจึงนำสำเนาใบรับฝากมาตรวจสอบกับสมาชิกทะเบียนบันทึกการรับเช็ค รอจนกว่าเช็คผ่านการเรียกเก็บแล้วจึงบันทึกการขายการรับชำระค่าสินค้าทาง terminal
6. ผู้ที่บันทึกการขายและรายการรับชำระหนี้ ควรจะเป็นคนละคน (โดยกำหนดแยก password ที่จะเข้าถึง menu หรือการอนุมัติรายการ)
7. ไม่ควรให้คุณโสภะซึ่งเป็นพนักงานต้อนรับ เข้ามามีส่วนเกี่ยวข้องกับเอกสารด้านการสั่งซื้อ และเอกสารการเงิน

จุดที่โปรแกรมควรมีการเช็คสอบ

- 1) การบันทึกเพิ่ม/ตัดยอดสินค้า โปรแกรมการทำงานควรมีจุดตรวจสอบดังนี้
 - 1.1) มีการแสดงยอดคงเหลือของสินค้าก่อนที่จะ Key ข้อมูลเพื่อบันทึกการขายเพิ่ม/ตัดยอดสินค้า
 - 1.2) ในกรณีป้อนจำนวนสินค้าที่จะตัดยอดสินค้ามีมากกว่ายอดคงเหลือต้องมี message เตือนให้ผู้ป้อนข้อมูลทราบ
 - 1.3) ควรจำกัด limit ในการ Key ตัดยอดสินค้าแต่ละครั้งและแต่ละวัน
- 2) การบันทึกการขาย โปรแกรมการทำงานควรมีจุดตรวจสอบหรือจุดควบคุมดังนี้
 - 2.1) กำหนดวงเงิน (limit) ของลูกค้าที่จะซื้อสินค้า กล่าวคือ ลูกค้าแต่ละรายจะมี limit ได้ไม่เท่ากัน ทั้งนี้ ในโปรแกรมการจะจำแนกระดับของ limit ได้จากรหัส 2 หลักแรกของหมายเลขประจำตัวลูกค้า
 - 2.2) กำหนดจำนวนเงินสูงสุดที่ลูกค้าจะสั่งซื้อได้ในแต่ละวัน หากเกินจะต้องให้ผู้มีอำนาจอนุมัติรายการ

- 3) การรับชำระหนี้ โปรแกรมการทำงานควรมีจุดตรวจสอบหรือจุดควบคุมดังนี้
- 3.1) ตรวจสอบหมายเลขประจำตัวลูกค้าว่า เคยมีการบันทึกรายการขาย สำหรับลูกค้ารายนี้มาก่อนหรือไม่
 - 3.2) ตรวจสอบจำนวนเงินที่รับชำระหนี้ (ที่ป้อนเข้าไป) ว่าตรงกับจำนวนเงินการขายสินค้าของลูกค้า รายนี้หรือไม่
 - 3.3) ตรวจสอบวันที่ในการรับชำระหนี้ จะต้องเป็นวันที่หลังจากวันสั่งซื้อ

การบันทึกรายการแต่ละประเภท

- 1) การป้อนข้อมูลนำเข้า ควรมีการกำหนดให้ป้อนเลขที่ของเอกสารที่เกี่ยวข้อง เช่น เมื่อบันทึกการขาย ควรกำหนดให้ป้อนเลขที่ใบกำกับสินค้า หรือเมื่อบันทึกการขายรับชำระหนี้ควรกำหนดให้บันทึกเลขที่เช็คเป็นต้น
- 2) สิ้นวัน ระบบงานควรกำหนดให้มีการออกยอด batch total เพื่อตรวจสอบความถูกต้องและครบถ้วนของรายการที่บันทึกเข้าเครื่องคอมพิวเตอร์ นอกจากนี้ ควรมี edit check โดยทั่ว ๆ ไป เช่น
- ข้อมูลที่ป้อนต้องไม่เกินจำนวนหลักที่กำหนดไว้
 - รหัสรายการ เป็นไปตามที่ได้กำหนดไว้เท่านั้นแนวคำตอบ กรณีศึกษา 10



แนวคำตอบ กรณีศึกษา 10

การรักษาความปลอดภัยห้องคอมพิวเตอร์ บริษัท ABC จำกัด

สรุปข้อสังเกตตามกรณีศึกษา เรื่อง การรักษาความปลอดภัยห้องคอมพิวเตอร์ บริษัท ABC จำกัด

1. ห้องคอมพิวเตอร์ตั้งอยู่ชั้นล่างสุดของบริษัท อาจไม่ปลอดภัยจากน้ำท่วมเพราะย่านหัวหมากน้ำท่วมบ่อยและเครื่องคอมพิวเตอร์ของมหาวิทยาลัยรามคำแหงก็เคยเสียหายเพราะน้ำท่วมมาแล้ว
2. ไม่ควรละเว้นการเซ็นชื่อเข้า-ออกห้องคอมพิวเตอร์ เพราะขัดกับมาตรการรักษาความปลอดภัยที่กำหนดไว้
3. ควรถือคูปองทางเข้าห้องคอมพิวเตอร์ไว้ตลอดเวลา บุคคลผู้เข้า-ออกต้องใช้บัตรพลาสติกกับรหัสในการเปิดประตูทุกครั้ง
4. ควรจัดตารางการปฏิบัติงานของพนักงาน operator ไว้ล่วงหน้า
5. เมื่อสงสัยว่าม้วนเทปอาจจะเสียหายควรให้พนักงาน librarian ตรวจสอบก่อนที่จะ load ประมวลผล
6. ควรติด label บอกชื่อ file และรายละเอียดต่าง ๆ ที่จำเป็นเพื่อป้องกันการใช้ File ผิด และการนำเทปออกจากห้องเก็บเทปควรลงทะเบียนด้วยทุกครั้ง
7. ไม่ควรนำวัสดุใด ๆ ไปปิดกั้นเครื่องตรวจจับความร้อน เพราะอาจจะทำให้การทำงานของระบบดับเพลิงผิดพลาดได้
8. ไม่ควรให้พนักงานทำความสะอาดหรือพนักงานซ่อมบำรุงของบริษัทผู้ขายเครื่องคอมพิวเตอร์อยู่ในห้องคอมพิวเตอร์ตามลำพัง โดยไม่มีพนักงานของศูนย์คอมพิวเตอร์คอยควบคุมดูแล
9. ควรจัดให้พนักงานทุกคนในศูนย์คอมพิวเตอร์ได้ลาหยุดพักผ่อนบ้างเพื่อจะได้ให้พนักงานคนอื่นมาปฏิบัติหน้าที่แทน เพื่อป้องกันพนักงานทุจริต



แนวคำตอบ กรณีศึกษา 11

บริษัท เทคโนโลยีทันสมัย จำกัด

การรักษาความปลอดภัยและการควบคุมภายในทั่วไปที่จะช่วยให้มั่นใจได้ว่า :

- 1) เป็นข้อมูลลับเฉพาะ คือ
 - (1) กำหนดรหัสลับ (Password) ให้แก่ คุณขวัญตา และผู้จัดการใหญ่อีก 2 คน ในการเข้าถึงข้อมูลต้นทุบลับเฉพาะ
 - (2) ใส่กุญแจล็อค terminal ทุกตัว ของฝ่ายการบัญชี ทุกสิ้นวันทำการ
 - (3) กำหนดให้เครื่อง Terminal ของฝ่ายบัญชีเท่านั้น ที่จะเข้าถึงข้อมูลต้นทุบลับได้
 - (4) จัดให้มีทะเบียนบันทึกการพยายามเข้าถึงระบบ และกำหนดให้ Terminal ปิดตัวเองโดยอัตโนมัติ หลังจากที่มีผู้พยายามเข้าถึงข้อมูล 3 ครั้งติดต่อกันและไม่สำเร็จ
 - (5) วางนโยบายห้ามผู้เขียนโปรแกรมและบุคลากรที่ไม่ได้อยู่ในฝ่ายการบัญชีไปใช้เครื่อง Terminal ของฝ่ายการบัญชี นั่นคือ จัดเครื่อง Terminal ไว้ในที่ที่มีการรักษาความปลอดภัย
 - (6) จัดเก็บข้อมูลต้นทุบลับในรูปแบบที่แปลงรหัสแล้ว (Encoded Form)
 - (7) ทำลายรายงานต่าง ๆ ที่พิมพ์ข้อมูลต้นทุบลับหลังจากใช้เสร็จแล้ว
- 2) มีข้อมูลต้นทุบลับที่สามารถเรียกใช้งานได้ตลอดเวลา คือ
 - (1) มีการถ่ายเทข้อมูลต้นทุบลับจากแฟ้มข้อมูลที่ให้อยู่ในงาน On-line ไปบันทึกไว้ในเทปอย่างน้อยวันละครั้ง
 - (2) จัดให้มีทะเบียนบันทึกรายการข้อมูลต้นทุบลับทุกรายการ (รวมทั้งรายการประเภทอื่นด้วย) และบันทึกสถานะของต้นทุบลับทั้งก่อนและหลังการเปลี่ยนแปลง
 - (3) จัดเก็บเทปที่บันทึกข้อมูลสำรอง และทะเบียนบันทึกรายการไว้ในสถานที่แยกต่างหากจากสำนักงานใหญ่ของกิจการ
 - (4) จัดให้มีการป้องกันความเสียหายของอุปกรณ์คอมพิวเตอร์ ทางด้านไฟไหม้ น้ำท่วม ไฟฟ้าดับ ฯลฯ
- 3) ข้อมูลมีความเชื่อถือได้ คือ
 - (1) จัดให้มีการรวบรวมรายชื่อผู้ที่ได้รับอนุมัติให้เปลี่ยนแปลงข้อมูลได้ โดยจัดให้มีโปรแกรมสำเร็จรูปเพื่อตรวจสอบว่าบุคคลที่เข้าถึงข้อมูลเป็นบุคคลที่ได้รับอนุมัติให้ทำการเปลี่ยนแปลงข้อมูลได้
 - (2) ใช้โปรแกรมตรวจสอบ (edit program) เพื่อตรวจสอบความถูกต้องของข้อมูล
 - (3) ว่าจ้างผู้ตรวจสอบให้ตรวจทานการควบคุมระบบอย่างต่อเนื่องอย่างสม่ำเสมอ

แนวคำตอบ กรณีศึกษา 12

ในการควบคุมการจัดทำรายการด้วยโปรแกรมระบบงาน Computer ดังกล่าว มีความเสี่ยงความเสียหายที่อาจเกิดขึ้น และมีการควบคุมและแนวทางการตรวจสอบดังนี้

- ความเสี่ยง** - กรณีที่รายการที่เกินอำนาจของพนักงานระดับต่ำกว่า แล้วต้องให้พนักงานระดับที่สูงกว่ามาป้อน Password ที่จอเครื่องเดียวกันเพื่ออนุมัติรายการ อาจทำให้พนักงานระดับต่ำกว่านั้นสามารถจำ Password ดังกล่าวได้
- ความเสียหาย** - รายการบางรายการอาจไม่ผ่านการอนุมัติจากผู้ที่มีอำนาจหน้าที่รับผิดชอบ ซึ่งอาจเกิดความเสียหายในแง่ของการที่ข้อมูลไม่ถูกต้องหรืออาจมีการแก้ไขจำนวนเงิน หรืออื่น ๆ ในรายการที่มีใช้ตัวเงิน
- การควบคุม** - ควรมีเครื่อง Terminal ที่เป็นเครื่องเฉพาะสำหรับพนักงานในระดับสูง เพื่อสามารถอนุมัติรายการได้โดยไม่ต้องไป Key ที่เครื่องของ Operator ในระดับต่ำกว่า
- การตรวจสอบ** - ควรมี Console log เพื่อให้พนักงานระดับสูงมีการสอบทานว่า มีรายการที่เกินวงเงินแล้ว ตัวเองมิได้อนุมัติรายการผ่านเข้าไปบ้างหรือไม่



แนวคำตอบ
กรณีศึกษา 13
บริษัท วิจิไฮเทค จำกัด

ความเสี่ยง	จุดควบคุม
1. ข้อมูลเปลี่ยนสภาพไปอยู่ในรูปของสื่อแม่เหล็กซึ่งมองด้วยตาเปล่าไม่เห็น และการเปลี่ยนแปลงแก้ไขกระทำได้โดยไม่ทิ้งร่องรอยและทำได้อย่างรวดเร็วมาก ข้อมูลที่อาจมีการเจตนาเปลี่ยนแปลงแก้ไขได้แก่ จำนวนชั่วโมงการทำงาน และอัตราค่าแรงเป็นต้น 2. อาจมีความเป็นไปได้ค่อนข้างมาก คือ พนักงานอาจไหว้วานให้เพื่อนพนักงานช่วยрутบัตรแทนให้ และแม้วันทั้งวันนั้นพนักงานผู้นั้นไม่ได้มาทำงาน แต่ก็มีการบันทึกเวลาทำงานเสมือนมาทำงาน ซึ่งในเรื่องเดียวกันนี้เอง อาจเป็นไปได้ว่ามีบุคคลภายในกระทำการทุจริตปลอมแปลงบัตรหรือใช้บัตรซึ่งพนักงานดังกล่าวลาออกไปแล้ว มาหาประโยชน์	1. ป้องกันมิให้มีการเข้าถึงและเปลี่ยนแปลงเพิ่มข้อมูลได้โดยง่าย ทั้งนี้ อาจกระทำได้โดยใช้การควบคุมการเข้าถึงทางกายภาพ (Physical access control) และการควบคุมทางด้านโปรแกรมและเพิ่มข้อมูล ในกรณีที่มีการเปลี่ยนแปลงอัตราค่าแรงต้องผ่านการอนุมัติจากผู้มีอำนาจ และต้องใช้ Password ของผู้มีอำนาจในการผ่านรายการ และต้องมีการออกรายงานมาเช็คสอบว่ามีการเปลี่ยนแปลง อัตราค่าแรงให้เป็นไปดังที่ต้องการ 2. มีวิธีป้องกันที่อาจไม่ได้ผลนักคือ ให้ลงชื่อกำกับในสมุดทะเบียน แต่อาจมีคนใช้วิธีปลอมลายมือชื่อแทนกัน มีอีกวิธีหนึ่งซึ่งรัดกุมกว่า แต่ก็ต้องเสียค่าใช้จ่ายเพิ่มคือ จ้างคนมานั่งเฝ้าเครื่อง 1 คน คอยดูว่ามีการрутบัตร 1 คน ต่อ 1 ครั้งหรือไม่และเป็นพนักงานตัวจริง กรณีป้องกันการปลอมแปลงบัตร คือ ต้องวางระบบการจัดทำบัตรให้รัดกุม มิให้คนที่ไม่เกี่ยวข้องเข้าถึงได้โดยง่ายและข้อมูลบนบัตรควรอยู่ในรูปของการใส่รหัส ผู้ที่มีเครื่องอ่านบัตรก็จะไม่สามารถเข้าใจว่ารหัสดังกล่าวหมายถึงอะไร เพราะโปรแกรมในระบบงานจะไปถอดความหมายของรหัสเหล่านั้นเอง

ความเสี่ยง	จุดควบคุม
3. มีโอกาสที่จะป้อนข้อมูลรายตัวพนักงานผิดพลาดเนื่องจากมีพนักงานจำนวนมาก ข้อมูลในแฟ้มข้อมูลอาจผิดพลาด และข้อมูลในบัตรแม่เหล็กก็อาจผิดพลาด 4. มีโอกาสที่โปรแกรมในการคำนวณค่าจ้าง ภาษี และรายการหักต่าง ๆ มีความผิดพลาดหรือเช็คเงื่อนไขต่าง ๆ ไม่ครบถ้วน 5. อาจเป็นไปได้ว่า พนักงานทำบัตรหาย หรือ ขำรุดจนไม่สามารถใช้การได้ 6. กรณีเครื่องขัดข้องหรือใช้งานไม่ได้ หรือ เครื่องหาย	นอกจากนี้ กรณีที่มีพนักงานลาออก ต้องมีการควบคุมบัตรของพนักงานเหล่านั้นโดยรัดกุม เช่น อาจมีการเรียกคืน และทำลายทิ้งเสีย ไม่สามารถนำไปใช้ใหม่ได้ 3. เมื่อมีการป้อนข้อมูลรายตัวดังกล่าวของพนักงาน ต้องมีการออกรายงานออกมาเช็คสอบอีกครั้ง 4. ต้องมีการสุ่มตรวจโปรแกรม เช่น Test data โดยกำหนดเงื่อนไขต่าง ๆ ที่ควรจะเป็นไปได้ และเป็นจุดเช็คสอบความรัดกุม นอกจากนี้ ต้องมีการควบคุมเพื่อป้องกัน การเปลี่ยนแปลงโปรแกรม โดยไม่ได้รับอนุญาต และในกรณีที่มีการเปลี่ยนแปลงโปรแกรม โดยผ่านการอนุมัติแล้ว ก็ต้องมีการตรวจสอบว่า การเปลี่ยนแปลงดังกล่าวเป็นไปตามที่ต้องการจริง ๆ ทั้งนี้ ควรผ่านการสอบทานจากต้นสังกัดที่ต้องการเปลี่ยนแปลง ข้อมูลดังกล่าว นอกจากนี้ต้องกำหนดวันที่ที่การเปลี่ยนแปลงดังกล่าวจะมีผลบังคับใช้ด้วย 5. ในกรณีนี้ ควรทำสมุดทะเบียนลงเวลาแทน และบันทึกเวลาต่อหน้าพนักงานเฝ้าเครื่อง (พนักงานผู้นี้ควรสับเปลี่ยนเวียนคนมาบ้าง อย่าให้ผู้หนึ่งใดอยู่ประจำเป็นเวลานาน ๆ) เมื่อทำงาน Batch ก็ป้อนรายการปรับปรุงในภายหลัง 6. ควรควบคุมให้มีการทำ Preventive Maintenance เครื่อง ตามระยะเวลาที่กำหนดเพื่อยืดอายุการใช้งาน และบรรเทาปัญหาที่จะเกิดขึ้นกับเครื่อง ให้น้อยที่สุด ซึ่งวิธีนี้เป็น การป้องกัน

ความเสี่ยง	จุดควบคุม
7. กรณีระบบคอมพิวเตอร์ของบริษัทเกิดขัดข้องใช้งานไม่ได้ ซึ่งอาจเนื่องมาจากระบบเกิดความล้มเหลวขึ้นเอง หรือไฟดับหรือจากภัยอื่น ๆ 8. อาจมีความผิดพลาดขึ้นได้ในการทำรายการปรับปรุงเพิ่มข้อมูล เช่น ในกรณีที่พนักงานทำผิดหรือทำของเสียหาย ต้องการลงโทษโดยการตัดเงินเดือนหรือตรงข้ามกรณีพนักงานปฏิบัติงานได้ดีเยี่ยมต้องการให้รางวัล	สำหรับในกรณีที่เครื่องขัดข้องหรือใช้งานไม่ได้แล้ว หรือเครื่องหาย ควรมีการทำสัญญาล่วงหน้ากับบริษัท สามารถนำเครื่องมาให้ใช้ทดแทนได้ทันที หรือสามารถซ่อมแซมให้กลับคืนสู่สภาพเดิมในเวลาเท่าใด เป็นต้น ซึ่งควรกำหนดไว้เป็นส่วนหนึ่งของแผนฉุกเฉินรวมทางด้านคอมพิวเตอร์ของบริษัท นอกจากนี้ หากราคาเครื่องดังกล่าวมีราคาแพง ควรมีการประกันภัยไว้ด้วย 7. บริษัทควรมีการวางแผนฉุกเฉินไว้ล่วงหน้า ในกรณีที่อาจเกิดเหตุการณ์ต่าง ๆ ที่มีผลทำให้ระบบคอมพิวเตอร์ไม่สามารถดำเนินการประมวลผลต่อไปได้ เช่น ในกรณีไฟฟ้ามดับอาจมีการใช้ตัว Generator บันทึกลงใช้ชั่วคราว หรือมีการใช้ UPS (Uninterrupted Power Supply) เป็นต้น ในกรณีระบบคอมพิวเตอร์ขัดข้อง อาจมีการทำสัญญากับผู้ขายให้หาเครื่องมาทดแทนให้ หรือทำสัญญากับผู้อื่น เพื่อขอใช้คอมพิวเตอร์เป็นการชั่วคราว เป็นต้น ทั้งนี้ ควรมีการวางแผนและทำสัญญาไว้ล่วงหน้า 8. กรณีที่มีการทำรายการปรับปรุงต้องมีการควบคุม ให้ผ่านการอนุมัติจากผู้มีอำนาจเท่านั้น และต้องใช้ Password ของผู้มีอำนาจในการทำรายการดังกล่าว และควรมีทางออก Exceptional Report เพื่อสอบถามรายการดังกล่าวว่ามีการปรับปรุงให้เป็นไปตามความต้องการหรือไม่

แนวคำตอบ กรณีศึกษา 14
บริษัท สายการบินปลอดภัย จำกัด
(Application controls)

(1) ความเสี่ยง

รูปที่ 1

- 1) ไม่มี field ให้ป้อนข้อมูลของจำนวนที่นั่งที่ลูกค้าแต่ละรายต้องการจอง ถ้าระบบงานถือว่า 1 รายการ = 1 ที่นั่ง ในกรณีที่ลูกค้าต้องการจองมากกว่า 1 ที่นั่ง ก็จะไม่สะดวกและอาจเกิดความผิดพลาดได้ง่าย
- 2) ไม่มี field รับข้อมูล “USER ID” ให้ user key หมายเลขประจำตัวของงาน เนื่องจากมี user ที่ได้รับอนุญาตให้ key ข้อมูลได้มากกว่า 1 คน และอาจมีเจ้าหน้าที่/พนักงานคนอื่นที่ไม่ได้รับอนุญาตทำงานอยู่ในแต่ละสาขาได้ ทำให้ไม่สามารถทราบได้ว่าใครเป็นผู้บันทึกการกรณนั้น ๆ
- 3) ไม่มีการถามเพื่อให้ลูกค้ายืนยันความต้องการในการจองที่นั่งอีกครั้งหนึ่ง หลังจากได้รับคำตอบจากสำนักงานใหญ่ว่า “OK” (เพราะถ้าคำตอบเป็น “NO” ก็ไม่ต้องยืนยันจะจองไม่ได้อยู่แล้ว) ทำให้มีปัญหาเมื่อลูกค้าเพียงแต่ประสงค์จะสอบถามข้อมูล ยังไม่ต้องการจอง

รูปที่ 2

- 1) ในรายงานไม่ได้ระบุว่าเป็นของสาขาใด ในกรณีที่ปัญหาและส่งให้สำนักงานใหญ่ดูจะไม่ทราบว่า เป็นรายงานของสาขาใด
- 2) ไม่ได้แสดงเกี่ยวกับจำนวนที่นั่ง และ User Id เนื่องจากไม่มีการ key ข้อมูลเข้าทำให้ข้อมูลที่ได้ไม่สามารถนำไปใช้ประโยชน์ได้เท่าที่ควร
- 3) เนื่องจากไม่ได้บันทึกข้อมูลเกี่ยวกับจำนวนที่นั่งของการจองแต่ละครั้ง ถ้าระบบงานถือว่าการจองแต่ละรายการ = จอง 1 ที่นั่ง จำนวนรวมทั้งสิ้นท้ายรายงานจะเป็นจำนวนที่นั่งที่จอง ไม่ใช่จำนวนรายของลูกค้า ซึ่งอาจทำให้ผู้ใช้รายงานสับสนได้ แต่ถ้าเป็นการรวมจำนวนรายของลูกค้า ซึ่งอาจทำให้ผู้ใช้รายงานสับสนได้ แต่ถ้าเป็นการรวมจำนวนรายของลูกค้า ตัวเลขที่ได้ก็จะไม่ถูกต้อง
- 4) รายงานนี้แสดงข้อมูลของลูกค้าทั้งรายที่ได้รับคำตอบเป็น “OK” และ “NO” ปะปนกันอยู่อาจทำให้การใช้ข้อมูลจากรายงานสับสน และไม่สะดวก และไม่ทราบว่าข้อมูลแต่ละบรรทัดมีคำตอบเป็นอะไร ไม่สามารถสอบยืนยันความถูกต้องกับสำนักงานใหญ่ได้

ข้อเสนอแนะ

รูปที่ 1

- 1) ควรมี field รับข้อมูล “จำนวนที่นั่ง” เพื่อความสะดวกในกรณีที่ลูกค้าต้องการจองมากกว่า 1 ที่นั่ง เพราะเป็นการช่วยป้องกันการ key ข้อมูลผิดพลาดได้ในเบื้องต้น
- 2) ควรมี field รับข้อมูล User Id/Password เพื่อเป็นหลักฐานว่าใครเป็นผู้ key รายการนั้น เนื่องจาก มี terminal เครื่องเดียว แต่มีพนักงานที่ได้รับอนุญาตถึง 3 คน
- 3) ปรับปรุงโปรแกรมให้มีการยืนยันความต้องการในการจองที่นั่ง ในกรณีที่คำตอบจากสำนักงานใหญ่เป็น “OK” เพื่อจะได้ใช้ประโยชน์ในการ inquiry ข้อมูลได้ด้วย หรือกรณี key ข้อมูลผิดต้องการแก้ไขข้อมูลใหม่

รูปที่ 2

- 1) รายงานควรแสดงข้อมูลเพิ่มเติม ดังนี้
 - ชื่อสาขา จะได้ทราบว่าเป็นรายงานของสาขาใด
 - จำนวนที่นั่ง และ User Id ตามที่ key เข้ามา
 - คำตอบที่ได้รับว่าเป็น “NO” หรือ “OK” เพื่อจะได้ทราบว่ารายใดที่ได้รับการจองแล้ว
 - 2) การออกยอดรวม ควรรวมจำนวนที่นั่งที่จองได้แล้ว คือ เฉพาะที่มีคำตอบเป็น “OK” เท่านั้น
- (2) ข้อมูลแต่ละ field ตามรูปที่ 3 โปรแกรมควรมีจุดควบคุมโดยการตรวจสอบในเรื่องดังนี้
- 1) สาขา จะต้องเป็นรหัสสาขาตามที่กำหนดไว้เท่านั้น
 - 2) วันที่ จะต้อง
 - เป็นตัวเลขเท่านั้น สอดคล้องกับเดือน 6 ปี เดือนต้องเป็นเลข 01-12 เท่านั้น
 - ต้องเป็นวันที่หลังจากวันนี้ไม่น้อยกว่า 3 วัน และไม่เกิน 15 วัน
 - 3) เทียบบิน จะต้องมียุทธเป็น M1 M2 M3 M4 M5 A1 A2 A3 A4 A5 อย่างใดอย่างหนึ่ง
 - 4) รหัสผู้อนุมัติจะต้องเป็นรหัสที่กำหนดไว้เท่านั้น และไม่ปรากฏให้เห็นบนจอ terminal

เท่านั้น

(3) (คล้ายกับ ข้อ (1))

รูปที่ 3

- 1) สาขา ชื่อ วันที่ เทียบบิน ควรจะเป็นข้อมูลที่ปรากฏขึ้นมาบนจอภาพให้เลย โดยดึงมาจากแฟ้มข้อมูล หลังจากที่เราตรวจสอบแล้วว่าที่นั่งว่าง และทางสาขายืนยันการจองมาแล้ว
- 2) การ key รหัสผู้อนุมัติไม่ควร key ที่ terminal นี้ ควร key ที่เครื่องอื่นหรือใช้ card รูด โดยเก็บรักษา card ไว้ให้ดี

- 3) หน้าจอควรดึงข้อมูลของจำนวนที่นำมาแสดงด้วย
- 4) ควรให้ key User Id

รูปที่ 4

- 1) ควรแสดงจำนวนที่นำ และ User Id/Password ไว้ในรายงานด้วย

(4) ข้อมูลในรายงานสิ้นวัน (รูปที่ 5) จะใช้ประโยชน์ในการควบคุมและตรวจสอบได้ ดังนี้

- 1) ใช้ในการสอบยัน (reconcile) กับรายงานของสาขา โดยส่งไปให้ทุกสาขาสอบความถูกต้อง
- 2) ส่งให้แผนกควบคุมการบิน ไว้คอยตรวจสอบผู้โดยสาร ณ วันเดินทาง
- 3) ช่วยทางด้านการบริหารและการตลาด ผู้บริหารสามารถนำไปใช้พิจารณาได้ว่าในแต่ละวันเที่ยวบินใดที่ลูกค้ามีความต้องการมากที่สุด เที่ยวบินใดมีความต้องการน้อย

ข้อมูลที่ควรแสดงเพิ่มเติม ดังนี้

- 1) จำนวนที่นั่งของลูกค้าแต่ละราย
- 2) User Id/Password ของผู้บันทึกและอนุมัติรายการจองที่นั่ง
- 3) จำนวนที่นั่งที่เหลืออยู่ของแต่ละเที่ยวบิน จนถึง ณ วันที่ออกรายงาน

(5) เอกสารที่ควรจัดทำเพิ่มเติม ได้แก่

- 1) ควรจัดทำรายงานที่แสดงข้อมูลของลูกค้าที่ถูกปฏิเสธการจอง โดยจำแนกเป็นรายเที่ยวบินของแต่ละวัน เพื่อช่วยฝ่ายบริหารในการพิจารณาความต้องการของลูกค้า
- 2) ควรจัดทำรายงานเกี่ยวกับการยกเลิกการจอง ที่แสดงข้อมูลเกี่ยวกับการจองที่ถูกยกเลิก เพื่อนำไปใช้ตรวจสอบจำนวนที่นั่งที่ยังว่างอยู่ของแต่ละเที่ยวบิน
- 3) สำนักงานใหญ่ ควรจัดทำรายงานส่งให้แต่ละสาขา แสดงข้อมูลการรับจองจำแนกตามวันที่และเที่ยวบิน เพื่อให้สาขาสอบยันความถูกต้องกับรายงานของตนอีกครั้งหนึ่งในวันรุ่งขึ้น
- 4) ควรจัดทำบันทึกการรับจองทางโทรศัพท์ เนื่องจากพนักงานรับโทรศัพท์จะเป็นใครก็ได้ทั้งนี้เพื่อนำไปตรวจสอบกับรายงานรูปที่ 2 ว่าได้มีการบันทึกข้อมูลการจองของลูกค้าครบถ้วนหรือไม่

แนวคำตอบ กรณีศึกษา 15

(I) Batch Control total ที่สามารถนำมาใช้ได้ในการนี้ข้อมูลดังกล่าวได้แก่

- (1) **ยอดคุดจำนวนรายการ** - เป็นการรวมยอดของจำนวนรายการที่ส่งเข้าประมวลผลในแต่ละชุด เช่น กรณีของ บ.เหล็กกล้า สำหรับข้อมูลในการประมวลผลเงินเดือน ช่วงสัปดาห์แรกของเดือนกุมภาพันธ์ จะมียอดรวมของจำนวนรายการเท่ากับ 7 (Document Control total)
- (2) **Hash Total** - เป็นการจัดทำยอดคุดที่ไม่เกี่ยวกับจำนวนเงิน เช่น การทำยอดรวมของหมายเลขประจำตัวลูกจ้างซึ่งเท่ากับ 117138 เป็นต้น
- (3) **Batch Total** - เป็นการจัดทำยอดคุดจำนวนรายการบัญชีใดบัญชีหนึ่ง ในกรณีนี้ ได้แก่ การจัดทำยอดคุดหมายเลขแผนกของลูกจ้างซึ่งเท่ากับ 10 หรือยอดคุดจำนวนชั่วโมงการทำงาน ซึ่งเท่ากับ 338

(II) ในกรณีดังกล่าวจะพบว่า นายอดทน เลขประจำตัว 25001 มีชั่วโมงการทำงานถึง 84 ชั่วโมง ในสัปดาห์เดียว ซึ่งไม่ถูกต้องเนื่องจากถ้าคิดว่าทำงานวันละ 8 ชั่วโมง จะได้ 10.5 ซึ่งเป็นไปไม่ได้ หรือถ้าคิดว่าทำงาน 7 วัน จะได้วันละ 12 ชั่วโมง ซึ่งก็เป็นไปไม่ได้อีก ในกรณีเช่นนี้ ควรมีการตรวจสอบในโปรแกรม (Programme Check) โดย

- (1) **Limit Check** - โดยควรมีการ set ไว้ในโปรแกรมด้วยว่า เมื่ออ่านข้อมูลชั่วโมงทำงานของแต่ละ record เข้าไปแล้ว จำนวนชั่วโมงทำงานไม่ควรเกิน 48 ชั่วโมง (หรือที่จะกำหนดไว้) ซึ่งถ้าเกินควร reject ออกมาหรือ list ออกมาให้ทราบ (Exception Report)
- (2) **validity Check** - กรณีที่ Check digit กำหนดว่าไม่เป็น กรณีนี้มีข้อมูลผิดพลาดคือของ น.ส.สุดสวย เลขประจำตัว 13820 ซึ่งกรณีที่จริงแล้วเครื่องควรจะไม่ยอมรับ ดังนี้ โปรแกรมควรมีการคำนวณ check digit และยังควรมีการกำหนดไว้ด้วยว่า field สุดท้ายของเลขประจำตัวจะไม่มีค่า ซึ่งถ้า key 13620 เข้าไปแล้ว เครื่องควรจะ reject ออกมาและพิมพ์ออกมาใน exception report ด้วย

บทที่ 8

การทดสอบความเข้าใจ
ในการตรวจสอบงานด้านคอมพิวเตอร์
บางประการ

การทดสอบความเข้าใจในการ ตรวจสอบงานด้านคอมพิวเตอร์บางประการ

เรื่องที่ 1 : การทดสอบแบบใดที่ผู้สอบบัญชีจะให้ความสนใจในการทดสอบความถูกต้องของรายการทางการเงิน (substantive test) เมื่อตรวจสอบโปรแกรมคอมพิวเตอร์

เรื่องที่ 2 : ท่านได้รับมอบหมายให้ตรวจสอบบัญชีลูกหนี้ซึ่งมีจำนวนเงินค่อนข้างสูงเมื่อเทียบกับสินทรัพย์ของบริษัทขนาดใหญ่แห่งหนึ่ง ท่านคิดจะใช้คอมพิวเตอร์ในการตรวจสอบแต่ท่านประสบเหตุการณ์ในแต่ละแบบดังนี้

1) ผู้จัดการหน่วย OPERATION ชี้แจงว่าเครื่องคอมพิวเตอร์ถูกกำหนดตารางการทำงานไว้ล่วงหน้าหมดแล้ว จึงไม่สามารถให้ผู้สอบบัญชีไปปฏิบัติงานได้

2) ผู้จัดการด้าน SCHEDULING แนะนำให้ท่าน CATALOGUE โปรแกรมของท่านรอไว้ใน disk เพื่อประมวลผลตอนที่เครื่องคอมพิวเตอร์ว่าง

3) ท่านถูกห้ามเข้าห้องคอมพิวเตอร์

4) ผู้จัดการด้านระบบงาน (system manager) แจ้งว่า การปรับโปรแกรมของท่าน (computer audit program) ให้ทำงานได้กับระบบควบคุมการทำงาน (operating system) ของเครื่องคอมพิวเตอร์จะเสียเวลามากเกินไป น่าจะให้พนักงานเขียนโปรแกรมที่จำเป็นต้องใช้ในการตรวจสอบให้จะสะดวกกว่า

ในสถานการณ์แต่ละแบบข้างต้น ผู้สอบบัญชีจะกระทำอย่างไรเพื่อทำการตรวจสอบบัญชีลูกหนี้ของบริษัทดังกล่าว

มีผู้ต้องการปกปิดบัญชีลูกหนี้ที่ไม่มีตัวตน (falsified account receivable) การใช้โปรแกรมตรวจสอบของผู้สอบบัญชีจะทำให้ปฏิบัติงานตรวจสอบให้ลุล่วงไปโดยรวดเร็ว และไม่ก่อให้เกิดการเข้าใจผิดเกี่ยวกับระบบงานที่ตรวจสอบ

เรื่องที่ 3 : เทคนิค 2 ประการในการตรวจสอบโปรแกรมโดยใช้ข้อมูลจริงอันได้แก่ การประมวลผลภายใต้การควบคุมของผู้สอบบัญชี (controlled processing) และการประมวลผลใหม่ภายใต้การควบคุมของผู้สอบบัญชี (controlled reprocessing) ผู้สอบบัญชีจะเลือกใช้เมื่อใด

เรื่องที่ 4 : ผู้สอบบัญชีสามารถใช้ generalized computer audit program ตรวจสอบความถูกต้องของ

- ก. การควบคุมการประมวลผล (data processing controls)
- ข. การประมาณการทางบัญชี (accounting estimates)
- ค. ยอดรวมทั้งหมดและยอดรวมย่อย (totals and sub-totals)
- ง. การจำแนกประเภทบัญชี (account classifications)

เรื่องที่ 5 : การใช้ generalized computer programs มีวัตถุประสงค์หลักเพื่อทดสอบและวิเคราะห์

- ก. ระบบคอมพิวเตอร์ (system)
- ข. อุปกรณ์คอมพิวเตอร์ (equipment)
- ค. ข้อมูลที่เก็บอยู่ในระบบคอมพิวเตอร์ (records)
- ง. ตรรกของการประมวลผล (processing logic)

เรื่องที่ 6 : งานขั้นต่ำที่ผู้สอบบัญชีสามารถใช้ generalized computer-audit program จัดทำคือ

- ก. คัดเลือกบัญชีลูกหนี้และพิมพ์ใบขอยืนยันยอดหนี้ (confirmations)
- ข. พิมพ์รายชื่อลูกหนี้ที่น่าสังเกต (account receivable confirmation exceptions) เพื่อตรวจสอบ
- ค. เปรียบเทียบยอดบัญชีลูกหนี้รายตัว (subsidiary files) กับยอดในบัญชีแยกประเภททั่วไป (general ledger)
- ง. ตรวจสอบรายการผิดปกติหรือน่าสังเกต (exceptions) กับลูกหนี้ที่ส่งใบยืนยันยอด (accounts receivable confirmations)

เรื่องที่ 7 : ผู้สอบบัญชีได้รับเทปแม่เหล็กที่บรรจุข้อมูลรายการสินค้าคงเหลือทั้งหมดและจำนวนเงินเรียงตาม STYLE NUMBER และข้อมูลที่อยู่ในเทปไม่เรียงลำดับกัน (NO PARTICULAR SEQUENCE) ผู้สอบบัญชีสามารถตรวจหาสินค้าฝากขาย (CONSIGNED MERCHANDISE) จากข้อมูลในเทปดังกล่าว โดยโปรแกรมที่ใช้ตรวจสอบซึ่งสามารถ

- ก. เลือกกลุ่มตัวอย่างรายการสินค้าตามจำนวนเงินโดยวิธีทางสถิติ
- ข. แยกเฉพาะ STYLE NUMBER ของสินค้าที่ฝากขายออกมา
- ค. คำนวณหาปริมาณสินค้าแต่ละชนิดจากราคาต่อหน่วย
- ง. พิมพ์ข้อมูลรายการสินค้าในเทปออกมา

เรื่องที่ 8 : โปรแกรมที่ใช้เรียงลำดับข้อมูล และโปรแกรมที่ใช้รวมข้อมูลหลายชุดเข้าด้วยกัน (SORTING AND MERGING) เป็นโปรแกรมที่ผู้สอบบัญชีมักจะใช้บ่อยในการตรวจสอบ โปรแกรมเหล่านี้ ศูนย์ประมวลผลก็มีใช้เช่นกัน เรียกว่า

- ก. โปรแกรมที่พัฒนาขึ้นเอง (USER PROGRAM)
- ข. โปรแกรมที่ใช้แปลงโปรแกรมที่เขียนให้เป็นภาษาเครื่อง (compiler program)
- ค. โปรแกรมที่ใช้ควบคุมการปฏิบัติงานของเครื่องคอมพิวเตอร์ (supervisory program)
- ง. โปรแกรมอรรถประโยชน์ (utility program)

เรื่องที่ 9 : วัตถุประสงค์หลักของ generalized computer audit program คือช่วยให้ผู้สอบบัญชี

- ก. สามารถใช้พนักงานของบริษัทที่ตรวจสอบทำการตรวจสอบ (audit routine check) ข้อมูลที่ประมวลผลแทนผู้สอบบัญชี
- ข. ทดสอบตรรก (logic) ของโปรแกรมที่ใช้ประมวลผล
- ค. คัดเลือกตัวอย่างได้ครอบคลุมมากกว่าปกติ (larger samples)
- ง. ประมวลผลข้อมูลจริงได้เองโดยอิสระ

เรื่องที่ 10 : การประมวลข้อมูลจริงผ่านโปรแกรมที่ใช้ปฏิบัติงานตามปกติและโปรแกรมของผู้สอบบัญชี (parallel simulation) เพื่อทดสอบการประมวลผล

- ก. ต้องจำลองการทำงานของโปรแกรมที่ใช้ในการปฏิบัติงานครบทุกลักษณะ (functions)
- ข. ไม่สามารถนำ generalized audit software มาช่วยได้
- ค. สามารถใช้ได้ทั้งข้อมูลจริงหรือข้อมูลทดสอบ (test data)
- ง. ผู้สอบบัญชีไม่ต้องมีความรู้ด้านคอมพิวเตอร์ลึกซึ้ง (advanced EDP knowledge)
- จ. ไม่มีข้อใดถูก

เรื่องที่ 11 : ผู้สอบบัญชีสามารถใช้ในการเปรียบเทียบโปรแกรม (program comparison) เพื่อ

- ก. ตรวจสอบว่าโปรแกรมที่ตรวจสอบสามารถปฏิบัติงานได้ตามที่กำหนดไว้ (required function)
- ข. ทดสอบประสิทธิภาพของการเขียนโปรแกรม (program codings)
- ค. ค้นหาการแก้ไขโปรแกรมโดยไม่ผ่านการอนุมัติ (unauthorized changes)
- ง. ดูว่าข้อมูลที่ผ่านการประมวลผลจากโปรแกรกดังกล่าวเชื่อถือได้เพียงใด
- จ. ถูกข้อมูล

เรื่องที่ 12 : ในกรณีที่ผู้สอบบัญชีประมวลผลข้อมูลจริงเพื่อรวบรวมยอดคงเหลือจากบัญชีแยกประเภทเองในรอบระยะเวลาบัญชีที่ตรวจสอบโดยใช้โปรแกรมต่างหาก (computer audit program) วิธีนี้จะใช้แทน

- ก. การตรวจสอบโดยการสุ่มตัวอย่างทางสถิติจากเอกสารขั้นต้น
- ข. การประเมินการควบคุมแฟ้มข้อมูลหลัก (master file) ที่ใช้แสดงยอดบัญชีแยกประเภท
- ค. การตรวจการผ่านบัญชี (posting) และการรวมยอด (footing) ด้วยมือ
- ง. ถูกทุกข้อ
- จ. ถูกเฉพาะข้อ ก. และ ค.

เรื่องที่ 13 : ในการตรวจสอบงบการเงิน ผู้สอบบัญชีอาจใช้โปรแกรมชุดที่เหมือนกับที่ใช้ปฏิบัติงานมาทำการประมวลผลข้อมูลจริงภายใต้การควบคุมของผู้สอบบัญชี วิธีนี้อาจใช้เพื่อ

- ก. ทำการสุ่มตรวจสอบเอกสารหลักฐานขั้นต้น
- ข. สอบทานการควบคุมการประมวล
- ค. สอบทานผังการทำงานของประมวล (data processing flowcharts)
- ง. ใช้ข้อมูลทดสอบ (Test data deck) ทดสอบการทำงานของโปรแกรม

เรื่องที่ 14 : พนักงาน operator ผิดกลางคืนมีความรู้ในการเขียนโปรแกรมโดยที่คนทั่วไปไม่ทราบได้ใช้ความรู้ที่นั้นแก้ไขโปรแกรมการจ่ายเงินเดือนผ่านเครื่องควบคุมการทำงาน (Console) โดยแก้อัตราเงินเดือนให้พรรคพวกในหน่วยงานนั้น การทุจริตถูกพบโดยบังเอิญหลังจากนั้นหลายเดือน ในกรณีนี้วิธีการควบคุมที่ดีที่สุดคือ

- ก. ตรวจสอบรายงานจาก Console log เพื่อดูรายการที่ไม่ได้รับการอนุมัติ (unauthorized intervention)
- ข. สอบทานระบบเงินเดือนและควบคุมการแจกจ่ายรายงานต่าง ๆ (distribution controls)
- ค. ตรวจสอบรายงานการจ่ายเงินเดือน (payroll journal output)
- ง. สอบทานการออกยอดรวมต่าง ๆ (control total review)

เรื่องที่ 15 : ข้อใดที่ไม่ใช่ปัญหาในการใช้ test-deck ในการตรวจสอบด้านคอมพิวเตอร์

- ก. การตรวจสอบแบบ through the computer ค่อนข้างจะยุ่งยากกว่าการตรวจสอบแบบ around the computer
- ข. เป็นการยากที่จะกำหนดข้อมูลใน test deck ให้ครอบคลุมรายการทุกประเภท ทุกสถานการณ์
- ค. ข้อมูลที่ใช้ทดสอบอาจเข้าไปปะปนกับข้อมูลจริงก่อให้เกิดปัญหาในการปฏิบัติงานตามปกติ
- ง. โปรแกรมที่ทำการทดสอบไม่ใช่ชุดที่ใช้ปฏิบัติงานจริง



บทที่ 9

แนวคำตอบการทดสอบ

ความเข้าใจ

(เรื่องที่ 1-15)

แนวคำตอบ

เรื่องที่ 1 :

มีการทดสอบ 2 ชนิดที่ผู้สอบบัญชีใช้ในการทดสอบความถูกต้องของยอดคงเหลือทางบัญชี (test of account balances) โดยแบบแรกเป็นการทดสอบเพื่อดูว่าโปรแกรมคำนวณผลลัพธ์ทางคณิตศาสตร์ได้ถูกต้อง (arithmetically accurate) แบบที่สองเป็นการทดสอบเพื่อดูทางเดินของข้อมูล (trace the flow of information) ภายใต้การทำงานของโปรแกรมว่ามีการแยกประเภทและผ่านรายการถูกต้องหรือไม่ ทั้งนี้ในการทดสอบความถูกต้องของรายการทางการเงินเพิ่มเติม นอกเหนือจากการตรวจสอบโปรแกรมจะกระทำกับแฟ้มข้อมูล (computer files) ข้อ 12-10 การใช้วิธีตรวจสอบโดยไม่ต้องประมวลผล (nonprocessing of data) วิธีตรวจสอบโดยประมวลผลข้อมูลจริง (processing of actual data) และวิธีตรวจสอบโดยประมวลผลข้อมูลตามที่ได้กำหนดไว้ (processing of simulated data) ในการทดสอบความถูกต้องของรายการทางการเงิน (substantive test) แตกต่างไปจากการตรวจสอบระบบการควบคุม (compliance testing) อย่างไร

ต่างกันตรงวัตถุประสงค์ในการตรวจสอบ การทดสอบความถูกต้องของรายการทางการเงิน (substantive test) มีวัตถุประสงค์เพื่อหาข้อผิดพลาดที่เป็นจำนวนเงินที่เกิดขึ้น (the amount of monetary error) การตรวจสอบระบบการควบคุม (compliance testing) มีวัตถุประสงค์เพื่อดูว่ามีการควบคุมตามที่ได้กำหนดไว้หรือไม่โดยไม่คำนึงถึงว่าข้อผิดพลาดที่เกิดขึ้นเป็นจำนวนเงินเท่าไร โดยเน้นที่อัตราเกิดข้อผิดพลาดว่ามีมากน้อยเพียงใด

การใช้วิธีตรวจสอบโดยไม่ต้องประมวลผล (non-processing of data) ในการทดสอบความถูกต้องของรายการทางการเงิน (substantive testing) เพื่อดูความถูกต้องแม่นยำ (accuracy) ของการประมวลผล แต่เมื่อใช้วิธีในการตรวจสอบระบบการควบคุม (compliance testing) ผู้สอบบัญชีใช้เพื่อดูว่าการควบคุมที่กำหนดอยู่ในโปรแกรมจะค้นพบข้อผิดพลาดและไม่ยอมประมวลผลรายการที่ผิดพลาดนั้น

ในการใช้วิธีการตรวจสอบโดยประมวลผลข้อมูลจริง (processing of actual data) และวิธีการตรวจสอบโดยประมวลผลข้อมูลตามที่ได้กำหนดไว้ (processing of simulated data) ก็จะพบข้อแตกต่างเช่นเดียวกับที่กล่าวข้างต้น คือเมื่อใช้วิธีการเหล่านี้ในการทดสอบความถูกต้องของรายการทางการเงิน (substantive testing) ผู้สอบบัญชีจะดูเฉพาะความถูกต้องในการประมวลผลเป็นสำคัญ เช่น มีข้อผิดพลาดเกี่ยวกับรายการทางการเงิน (monetary errors) เกิดขึ้นเมื่อใช้โปรแกรมนี้นั้น ในการตรวจสอบระบบการควบคุม (compliance testing) ด้วยวิธีการเหล่านี้ ผู้สอบบัญชีจะดูว่ามีการควบคุมด้านการนำข้อมูลเข้า (input) การประมวล (processing) และรายงาน (output) ตามที่กำหนดไว้หรือไม่

เรื่องที่ 2 :

1) ในสถานการณ์ที่ได้รับแจ้งว่าเครื่องคอมพิวเตอร์มีงานเต็มไม่มีเวลาให้ผู้สอบบัญชีประมวลผลได้ ผู้สอบบัญชีควรติดต่อกับผู้มีอำนาจของบริษัท (proper official) เพื่อขอเข้าใช้เครื่องคอมพิวเตอร์ และควรแนะนำว่าในคู่มือปฏิบัติงานกล่าวไว้ชัดเจนว่ายอมให้มีการตรวจสอบข้อมูลและใช้คอมพิวเตอร์ในการตรวจสอบได้ (computer use and access for audits)

2) ในสถานการณ์ที่ขอให้ผู้สอบบัญชี catalogue โปรแกรมรอไว้เพื่อประมวลผลนั้น ผู้สอบบัญชีไม่ควรยินยอมเพราะโปรแกรมอาจถูกแก้ไขโดยผู้สอบบัญชีไม่ทราบได้

3) ในกรณีที่ถูกห้ามเข้าห้องคอมพิวเตอร์ ผู้สอบบัญชีควรอ้างว่าตามข้อตกลงเกี่ยวกับการสอบบัญชี (charter) ระบุไว้ชัดเจนว่า ผู้สอบบัญชีสามารถเข้าถึงข้อมูลทั้งหมดขององค์กรนั้นได้ทุกแห่ง

4) ในกรณีที่ถูกร้องไม่ให้ใช้โปรแกรมตรวจสอบของผู้สอบบัญชีโดยให้พนักงานในศูนย์คอมพิวเตอร์เขียนโปรแกรมให้ใหม่ ผู้สอบบัญชีควรยืนยันที่จะใช้โปรแกรมของตนเองเพราะอาจ

เรื่องที่ 3 :

การประมวลผลภายใต้การควบคุมของผู้สอบบัญชี (controlled processing) จะใช้เมื่อ

1) ผู้สอบบัญชีรู้ว่าโปรแกรมที่นำมาประมวลผลนั้นเป็นชุดเดียวกับที่ใช้ปฏิบัติงานตามปกติ

2) ผู้สอบบัญชีสามารถสังเกตการประมวลผลได้ตลอดทุกขั้นตอนว่าเหมาะสมหรือไม่ ไม่ควรปล่อยให้มีการใด ๆ ที่ผู้สอบบัญชีไม่ทันสังเกตหรือไม่เข้าใจเกิดขึ้นในขณะที่ประมวลผล

3) ผู้สอบบัญชีสามารถควบคุมการประมวลผลได้โดยไม่เป็นอุปสรรคหรือทำให้การประมวลผลตามปกติต้องหยุดชะงัก ข้อมูลที่ประมวลผลต้องครอบคลุมรายการทุกแบบที่เกิดขึ้นจากการปฏิบัติงานตามปกติ

การประมวลผลใหม่ภายใต้การควบคุมของผู้สอบบัญชี (controlled reprocessing) จะใช้เมื่อ

1) ผู้สอบบัญชีรู้ว่าโปรแกรมที่นำมาประมวลผลข้อมูลเดิมอีกครั้งเป็นโปรแกรมชุดเดียวกับที่ใช้ปฏิบัติงานตามปกติ

2) ผู้สอบบัญชีสามารถสังเกตการประมวลผลใหม่ได้ตลอดทุกขั้นตอนว่าเหมาะสมหรือไม่

เรื่องที่ 4 : (เฉลย ข้อ ค.)

เรื่องที่ 5 : (เฉลย ข้อ ค.)

เรื่องที่ 6 : (เฉลย ข้อ ง.)

เรื่องที่ 7 : (เฉลย ข้อ ข.)

เรื่องที่ 8 : (เฉลย ข้อ ง.)

เรื่องที่ 9 : (เฉลย ข้อ ง.)

เรื่องที่ 10 : (เฉลย ข้อ ค.)

เรื่องที่ 11 : (เฉลย ข้อ ค.)

เรื่องที่ 12 : (เฉลย ข้อ ค.)

เรื่องที่ 13 : (เฉลย ข้อ ง.)

เรื่องที่ 14 : (เฉลย ข้อ ข.)

เรื่องที่ 15 : (เฉลย ข้อ ก.)



ภาคผนวก ก ^{1/}

ความเห็นเกี่ยวกับร่างแนวทางกฎหมายการโอนเงินทางอิเล็กทรอนิกส์ (ที่ UNCITRAL สอบถามประเทศต่าง ๆ)

Issue No.	ความเห็นของประเทศไทย
Issue No. 1 Are major changes in the law required by the development of electronic funds transfers? การพัฒนาระบบการชำระเงินด้วยเครื่องอิเล็กทรอนิกส์นั้น จำเป็นต้องมีการเปลี่ยนแปลงเนื้อหากฎหมายเพื่อรองรับหรือไม่	โดยวิธีการโอนเงินด้วยเครื่องอิเล็กทรอนิกส์นั้นมีระเบียบพิธีปฏิบัติแตกต่างไปจากวิธีการโอนเงินด้วยเอกสารหลักฐานอย่างสิ้นเชิง ดังนั้น กฎเกณฑ์ต่าง ๆ ที่ใช้บังคับจึงควรประยุกต์ให้เข้ากับระเบียบพิธีการที่เปลี่ยนไปนี้ จึงสมควรร่างกฎหมายที่เหมาะสมให้มีผลใช้บังคับเฉพาะเรื่องเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์
Issue No. 2 To what types of financial transactions should the law of funds transfers apply? กฎหมายเกี่ยวกับโอนเงินควรจะครอบคลุมธุรกรรมทางการเงินประเภทใดบ้าง	รายการโอนเงินทุกประเภทที่จะต้องการหักบัญชีผ่านระบบสถาบันการเงิน ควรจะรวมอยู่ในคำจำกัดความของการโอนเงิน ยกเว้นการโอนดังกล่าวเป็นข้อตกลงของบุคคลสองกลุ่มโดยมิได้กระทำผ่านสถาบันการเงิน
Issue No. 3 Should the law governing funds transfers recognize the increased role of the funds transfer system in individual inter-bank funds transfers? กฎหมายเกี่ยวกับการโอนเงินจำเป็นต้องคำนึงถึงบทบาทในการโอนเงินระหว่างธนาคารเป็นรายธนาคารหรือไม่	บทบาทของระบบการโอนเงินทางอิเล็กทรอนิกส์นั้นมีแนวโน้มที่จะขยายตัวขึ้นตลอดเวลา แต่ในขณะเดียวกันในแต่ละระบบก็มีเทคโนโลยีที่แตกต่างกัน ดังนั้น หากมีการดำเนินงานเป็นข่ายงานหรือเป็นการโอนเงินระหว่างประเทศแล้ว ก็ควรอยู่ภายใต้มาตรฐานและกฎเกณฑ์เดียวกัน
Issue No. 4 Should funds transfers between the transferor and transferee and the funds transfer transactions implementing the funds transfer be governed by the same rulers? If some of the rules might be different, should the differences be reflected in	ในเรื่องการโอนเงินของลูกค้าภายในธนาคารเดียวกันนั้น เงื่อนไขหรือพิธีปฏิบัติระหว่างผู้โอนกับผู้รับโอนอาจจะแตกต่างกันได้ ขึ้นอยู่กับระเบียบของแต่ละธนาคารซึ่งต้องแจ้งให้ลูกค้าทราบ แต่ถ้าการโอนดังกล่าวเป็นการโอนระหว่างธนาคาร ไม่ว่าผู้โอนหรือผู้รับโอนจะเป็นธนาคารหรือไม่ ระเบียบ

^{1/} หมายเหตุ : The United Nations Commission on International Trade Law หรือ UNCITRAL จาก UN ได้มีหนังสือผ่านกระทรวงการต่างประเทศมาให้ธนาคารแห่งประเทศไทย และธนาคารกลางประเทศต่างๆ ประมาณปี พ.ศ. 2524 เพื่อสอบถามความเห็นในเรื่องนี้ และส่วนตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์ ธนาคารแห่งประเทศไทย ก็ได้ดำเนินการประสานงานและตอบคำถามดังกล่าวไปยัง UN โดยผ่านกระทรวงต่างประเทศดังกล่าวข้างต้น

Issue No.	ความเห็นของประเทศไทย
the law or by inter-bank agreements? การโอนเงินระหว่างผู้โอนไปยังผู้รับโอน กับรายการโอนในระบบการโอนเงิน จำเป็นต้องอยู่ภายใต้กฎหมายเดียวกันหรือไม่ หากระเบียบต่าง ๆ แตกต่างกัน ควรจะตัดสินโดยกฎหมายหรือข้อตกลงระหว่างธนาคาร Issue No. 5 Should internationally agreed rules be prepared to govern international electronic funds transfers? ในการโอนเงินระหว่างประเทศ ควรจะต้องจัดทำข้อตกลงสากลหรือไม่ Issue No. 6 Should internationally agreed rules on conflicts of law be prepared for international electronic funds transfers? ในการโอนเงินระหว่างประเทศ หากกฎหมายของแต่ละประเทศขัดแย้งกัน ควรจะมีข้อตกลงสากลตัดสินหรือไม่ Issue No. 7 Do the rules of evidence give records of funds transfers kept in computer-readable form the same legal value as record kept in paper-based form? หลักฐานในการโอนเงินที่จัดทำเป็นเอกสารหลักฐานกับหลักฐานที่เก็บไว้โดยวิธีประมวลข้อมูลทางอิเล็กทรอนิกส์ ควรจะมีผลตามกฎหมายเช่นเดียวกันหรือไม่	ปฏิบัติควรจะเป็นมาตรฐานเดียวกัน โดยอยู่ในรูปข้อตกลงระหว่างธนาคาร เนื่องจากกฎหมายของแต่ละประเทศแตกต่างกันออกไป และระเบียบปฏิบัติของแต่ละหน่วยงานในปัจจุบัน ก็มีความแตกต่างกัน ดังนั้น เพื่อหลีกเลี่ยงปัญหาดังกล่าว ควรจะมีข้อตกลงในเรื่องระเบียบปฏิบัติที่เป็นสากล เพื่อให้เป็นหลักปฏิบัติทั่วไป ในกรณีที่มีการโอนเงินระหว่างประเทศ การโอนเงินทางอิเล็กทรอนิกส์นั้นเป็นเทคโนโลยีใหม่หลาย ๆ ประเทศ ซึ่งอาจจะยังไม่มีกฎหมายเฉพาะรองรับ ดังนั้น หากกฎหมายของแต่ละประเทศมีความขัดแย้งกัน ก็ควรมีกฎหมายสากลเป็นเครื่องตัดสิน อันที่จริงแล้ว การเก็บหลักฐานโดยเอกสารหรือโดยอุปกรณ์ทางอิเล็กทรอนิกส์ เช่น เทปแม่เหล็ก หรือจานแม่เหล็ก ควรมีผลบังคับทางกฎหมายเช่นเดียวกัน อย่างไรก็ดี เนื่องจากเทคโนโลยีในแต่ละประเทศมิได้มีความทัดเทียมกัน ดังนั้น หากเป็นการโอนเงินระหว่างประเทศแล้วเรื่องเอกสารหลักฐานทางกฎหมายควรจะต้องอิงกฎหมายของแต่ละประเทศเป็นหลัก ว่าจะถือว่าการเก็บข้อมูลด้วยอุปกรณ์อิเล็กทรอนิกส์มีผลทางกฎหมายหรือไม่

Issue No.	ความเห็นของประเทศไทย
Issue No. 8 Are changes in law required in order to permit the truncation of cheques, bill of exchange and other debit transfer instructions at the bank of deposit. ควรจะมีการเปลี่ยนแปลงกฎหมายเพื่อให้ธนาคารผู้รับฝาก เช็ค ตัวแลกเงิน มีอำนาจสั่งธนาคารผู้ออกเช็ค หรือตัวแลกเงิน ตัดบัญชี เช็คหรือตัวแลกเงิน จากบัญชีของลูกค้าในลักษณะคำสั่ง debit transfer หรือไม่ Issue No. 9 Does the development of electronic funds transfer technique require changes in the law governing bank secret? การนำวิธีการโอนเงินด้วยเครื่องอิเล็กทรอนิกส์มาใช้นี้ จำเป็นต้องเปลี่ยนแปลงกฎหมายที่เกี่ยวข้องกับการเก็บรักษาความลับหรือไม่ Issue 10 Should bank have written contracts with their customers covering rights and duties of the customers and the banks in respect of electronic funds transfers? สัญญาระหว่างลูกค้ากับธนาคารในเรื่องการให้บริการโอนเงินทางอิเล็กทรอนิกส์นั้น จำเป็นต้องทำสัญญาเป็นลายลักษณ์อักษรเพื่อระบุสิทธิและหน้าที่ของลูกค้าหรือไม่	โดยปกติแล้ว ธนาคารผู้รับเช็คจะเครดิตบัญชีผู้นำฝากเช็คในลักษณะการหักบัญชีเพื่อรอเรียกเก็บ การเครดิตจะสมบูรณ์ต่อเมื่อธนาคารผู้ออกเช็คยืนยันการตัดบัญชีผู้ออกเช็คตามเช็คนั้นแล้ว ดังนั้น ธนาคารผู้รับฝากเช็คจึงไม่ควรมีสิทธิสั่งให้ธนาคารผู้ออกเช็ค เดบิตบัญชีผู้ออกเช็คได้เนื่องจากธนาคารผู้รับฝากเช็คไม่สามารถจะพิสูจน์ความถูกต้องของเช็คที่ออกโดยธนาคารอื่น การรักษาความลับของลูกค้า โดยปกติก็มีกฎหมายบังคับไว้อยู่แล้ว ส่วนกรณีที่ธนาคารถูกลักลอบสืบความลับของลูกค้าโดยอาศัยเทคโนโลยีทางสื่อสารนั้น เป็นเงื่อนไขความปลอดภัยขั้นต่ำที่ต้องกำหนดให้ธนาคารจัดขึ้นไว้ในระบบเพื่อป้องกันกรณีดังกล่าว อย่างไรก็ดี กฎหมายก็ควรให้ธนาคารเปิดเผยความลับของลูกค้าแก่ธนาคารกลางหรือรัฐบาลได้โดยเฉพาะในเรื่องการโอนเงินระหว่างประเทศ เนื่องจากในบางประเทศที่ขาดแคลนเงินตราต่างประเทศ จำเป็นระมัดระวังเรื่องเงินตราต่างประเทศไหลออก การโอนเงินทางอิเล็กทรอนิกส์เป็นเทคโนโลยีใหม่ซึ่งมีหลักปฏิบัติแตกต่างไปจากเดิม และลูกค้าบางรายอาจจะยังไม่เข้าใจในเรื่องดังกล่าวดี ดังนั้น การให้บริการแก่ลูกค้าแต่ละราย ธนาคารจึงควรต้องทำสัญญาเป็นลายลักษณ์อักษรกับลูกค้าโดยระบุให้แน่ชัดถึงสิทธิที่สามารถคุ้มครองความเสียหายแก่ลูกค้า และข้อปฏิบัติของลูกค้า ในการใช้เครื่องอิเล็กทรอนิกส์ หรือกรณีเกิดความเสียหาย ทั้งนี้ เพื่อป้องกันข้อโต้แย้งในเรื่องความรับผิดชอบ หากมีกรณีสูญเสียเกิดขึ้น

Issue No.	ความเห็นของประเทศไทย
Issue No. 11 Should there be any restriction placed on standing authorizations to debit? คำสั่งให้ตัดบัญชีในลักษณะที่เป็น standing authorizations ควรจะมีข้อจำกัดใดหรือไม่	คำสั่งให้โอนเงินประเภทที่ให้อำนาจธนาคารโอนเงินตามเวลาที่ระบุไว้เป็นลักษณะประจำนั้นควรมีข้อกำหนดเรื่อง - จำนวนเงินขั้นสูงสุดที่จะใช้ standing authorization ได้ - กำหนดเวลาที่สามารถบอกเลิกหรือเปลี่ยนแปลง standing authorization - ผู้โอนไม่มีสิทธิที่จะให้ธนาคารล้างรายการหรือกลับรายการที่โอนไปแล้ว
Issue No. 12 Should there be an legal requirement as to the form of authentication necessary in an electronic funds transfer? ควรมีกฎหมายกำหนดรูปแบบของรหัสที่ใช้ในการสื่อสาร (authentication) ในระบบการโอนเงินทางอิเล็กทรอนิกส์หรือไม่	ปกติรูปแบบของรหัสทางการสื่อสารและการพิสูจน์รหัสนั้น เป็นเรื่องสำคัญที่สุดในระบบการโอนเงินในปัจจุบัน เนื่องจากข่าวสารที่ส่งระหว่างกันนั้นมิได้มีการแปลงสัญญาณ (encryption) ก่อนจึงต้องส่งเป็นรหัสลับ และต้องมีการพิสูจน์รหัสลับเพื่อยืนยันผู้ส่งและขอความให้ถูกต้องตรงกัน อย่างไรก็ตาม ในการสื่อสารด้วยเครื่องอิเล็กทรอนิกส์นั้น นอกจากจะต้องแจ้งรหัสลับ (PIN) และ password แล้ว การสื่อสารก็มักจะส่งผ่านเครื่องแปลงสัญญาณ (encryption) ในการส่งเสียก่อน โดยผู้รับก็จะมีเครื่องถอดสัญญาณ (decryption) ให้กลับเป็นข้อความที่เข้าใจได้ ซึ่งก็น่าจะให้ความปลอดภัยในการส่งข่าวสารเช่นเดียวกับการส่งข่าวสารด้วยรูปแบบของรหัส ดังนั้น จึงไม่มีความจำเป็นต้องมีกฎหมายบังคับให้การส่งข้อมูลต้องอยู่ในรูปแบบของรหัส
Issue No. 13 Should sending banks be required to adhere to standard formats when sending funds transfer instructions? ธนาคารผู้โอนจำเป็นต้องใช้ข้อความมาตรฐานในคำสั่งโอนเงินหรือไม่	เนื่องจากข่ายงานการสื่อสารระหว่างประเทศในปัจจุบันมีอยู่มากมาย แต่ละแห่งก็ใช้รูปแบบของข้อมูลแตกต่างกันไป และมักเกิดปัญหาเมื่อต้องมีการสื่อสารระหว่างข่ายงาน ดังนั้น รูปแบบข้อความทางการสื่อสารนั้นควรจะเป็นมาตรฐานเดียวทั่วโลก เพื่อให้ข่ายงานทุกแห่งสามารถติดต่อกันได้สะดวก และเพื่อหลีกเลี่ยงข้อโต้แย้งทางกฎหมายอันอาจเกิดขึ้นหากข้อความที่ใช้สื่อสารให้ความหมายต่างกัน

Issue No.	ความเห็นของประเทศไทย
Issue No. 14 Should a single electronic funds transfer format be required for all debit and credit cards in use in a country? ในประเทศเดียวกัน ข้อความที่ใช้ในระบบการเงินรูปแบบหนึ่ง ควรจะใช้ได้กับบัญชีทุกประเภททั้ง credit card และ debit card หรือไม่	ข้อความที่ใช้ในการสื่อสารทางอิเล็กทรอนิกส์นั้น ควรจะมีมาตรฐานเดียว ซึ่งสามารถใช้กับบัตรทุกประเภท ไม่ว่าจะเป็น debit card หรือ credit card เนื่องจากบัตรพลาสติกดังกล่าวใช้เพื่อวัตถุประสงค์เดียวกันคือการโอนเงิน อันจะเป็นประโยชน์แก่ผู้ถือบัตรต่างประเภทสามารถโอนเงินซึ่งกันและกันได้ นอกจากนี้ การมีระบบข้อความสื่อสารที่เป็นมาตรฐานเดียวกันจะอำนวยความสะดวกในการสร้างข่ายงานภายในประเทศด้วย
Issue No. 15 Where should customer accounts be considered to be located for the purposes of legal rules governing funds transfers? ตามกฎหมายแล้ว ควรจะถือว่าสถานที่ใดเป็นสถานที่เก็บรักษาบัญชีของลูกค้า	ในเรื่องบัญชีของลูกค้า ควรจะถือว่าอยู่ที่สถานที่ที่ลูกค้าเปิดบัญชี เนื่องจากสาขาที่รับเปิดบัญชีเป็นสถานที่เก็บเอกสารหลักฐานการเปิดบัญชีของลูกค้าไว้ และลูกค้าก็ใช้บริการในฐานะลูกค้าของสาขาแห่งนั้น ถึงแม้ว่าการบันทึกรายการทางบัญชีของลูกค้าจะเก็บไว้ที่ศูนย์ประมวลข้อมูลกลางก็ตาม
Issue No. 16 Should the duty of a transferor bank in a credit transfer be limited to sending a proper credit transfer instruction to a proper receiving bank or should the transferor bank's duty be to see that the transferor's instruction is carried out? ควรจะกำหนดขอบเขตหน้าที่ของธนาคารผู้โอนไว้เพียงดำเนินการโอนเงินของลูกค้าไปยังธนาคารผู้รับโอน หรือต้องรับผิดชอบจนกว่าการโอนนั้นจะได้ โอนเข้าบัญชีของผู้รับโอนเรียบร้อยแล้ว	ธนาคารผู้โอนนั้นไม่มีอำนาจที่จะสั่งให้ธนาคารผู้รับโอนโอนเงินเข้าบัญชีของผู้รับโอนได้ตามเวลาที่ต้องการ และธนาคารผู้โอนก็ไม่มีอำนาจที่จะสั่งให้ธนาคารผู้รับโอนโอนเงินออกจากบัญชีผู้รับโอนกลับคืนมาได้ ดังนั้นหน้าที่ของธนาคารผู้โอนจึงควรจำกัดเพียงโอนเงินให้แก่ธนาคารผู้รับโอน เพื่อให้เข้าบัญชีผู้รับโอนเท่านั้น ไม่จำเป็นต้องมีติดตามการโอนเงินของธนาคารผู้รับโอนไปเข้าบัญชีผู้รับโอนด้วย
Issue No. 17 Is the transferee bank responsible to the transferor, to the sending bank or to the transferee for the proper fulfilment of its obligations in regard to a credit transfer?	ปกติธนาคารผู้รับโอนมีภาระเพียงรับการโอนเงินจากธนาคารผู้โอน และดำเนินการโอนเงินไปให้บัญชีผู้รับโอนตามคำสั่งของผู้โอนเท่านั้น ดังนั้น ธนาคารผู้รับโอนไม่ควรจะมีภาระรับผิดชอบไปถึงผู้โอน หรือธนาคารผู้โอนแต่อย่างใด

Issue No.	ความเห็นของประเทศไทย
ธนาคารผู้รับโอนควรจะต้องรับผิดชอบต่อผู้โอน ธนาคารผู้โอน หรือผู้รับโอน แค่นั้นเพียงใด Issue No. 18 Should public telecommunications carriers, private data communications services, electronic funds transfer networks and electronic clearing-houses be responsible for losses arising out of errors or fraud in connection with a funds transfer instruction? หากมีความเสียหายเกิดขึ้น แต่มิได้เกิดจากข้อผิดพลาดหรือทุจริต ผู้ให้บริการสายโทรคมนาคมและช่วยงานการเงิน จำเป็นต้องรับผิดชอบหรือไม่ Issue No. 19 Should a bank be free from responsibility for errors or delayed funds transfers caused by failures in computer hardware or software? หากความล้มเหลวของเครื่องคอมพิวเตอร์หรือระบบก่อให้เกิดความผิดพลาดหรือล่าช้าธนาคารควรรับผิดชอบหรือไม่ Issue No. 20 Should a bank be liable to its customer for having entered a debit or credit to the account according to the account number indicated on the funds transfer instruction it has received if the name on that account does not correspond to the name given on the funds transfer instruction. หากชื่อบัญชีและเลขที่บัญชีที่ระบุไว้ในคำสั่งโอนเงินไม่ถูกต้องแล้ว ธนาคารได้ debit หรือ credit บัญชีของลูกค้า ธนาคารควรต้องรับผิดชอบหรือไม่	ความเสียหายที่อาจเกิดขึ้นนอกเหนือจากกรณีทุจริตหรือข้อผิดพลาด เช่น การส่งข่าวสารล่าช้าหรือข่าวสารถูกเปิดเผย หากธนาคารมีทางเลือกที่จะใช้สายโทรคมนาคมขององค์กรใดแล้ว ธนาคารควรจะต้องรับผิดชอบต่อความเสียหายนั้น แต่หากธนาคารไม่มีทางเลือกในการใช้สายโทรคมนาคม ผู้โอนก็ควรรับภาระความเสียหายนั้นไปเอง ทั้งตัวเครื่องคอมพิวเตอร์และโปรแกรมนั้นเป็นหน้าที่ของธนาคารจะต้องดูแลรักษาให้อยู่ในสภาพใช้งานได้ดี และถูกต้องอยู่เสมอ ดังนั้น หากความเสียหายแก่ลูกค้าเป็นผลมาจากการทำงานของเครื่องหรือระบบโปรแกรมล้มเหลว ธนาคารควรเป็นผู้รับผิดชอบต่อความเสียหายนั้น โดยปกติหากคำสั่งโอนที่ระบุชื่อบัญชี เลขที่บัญชีของผู้โอนหรือผู้รับโอน หรือรหัสลับใด ๆ อย่างใดอย่างหนึ่งไม่สอดคล้องตรงกันแล้ว ธนาคารก็จะไม่ดำเนินการให้ แต่หากธนาคารได้ผ่านบัญชีตามคำสั่งการโอนนั้นแล้ว ธนาคารที่ดำเนินการดังกล่าวก็ควรต้องรับผิดชอบต่อรายการโอนเงินนั้น

Issue No.	ความเห็นของประเทศไทย
Issue No. 21 Should the bank or the bank customer carry the burden of proof whether a debit to the transferor's account was authorized by him or occurred through his fault? ธนาคารหรือลูกค้าของธนาคารควรจะเป็นผู้รับภาระในการพิสูจน์ว่า การหักบัญชีของผู้โอนเงินนั้นได้รับอนุญาตจากตนหรือเกิดขึ้นโดยความผิดพลาดของตน Issue No. 22 Should the customer or the relevant banks carry the burden of proof as to the source to error or fraud causing loss in effecting a fund transfer? ลูกค้าหรือธนาคารที่เกี่ยวข้องควรจะเป็นผู้รับภาระในการพิสูจน์หาสาเหตุของความผิดพลาดหรือทุจริต ซึ่งก่อให้เกิดความเสียหายในการโอนเงิน Issue No. 23 Should the funds be required to be made available to the transferee within specific periods of time be determined? ควรจะมีการกำหนดระยะเวลาที่เงินโอนจะต้องไปถึงผู้รับหลังจากที่ธนาคารผู้โอนเงินได้รับคำสั่งให้โอนเครดิตนั้นหรือไม่ ถ้าควรกำหนดควระกำหนดได้อย่างไร	ในกรณีที่ลูกค้าใช้เครื่องมือสื่อสารโอนเงินได้เอง เช่น ผ่าน ATMS หรือ home banking แต่ธนาคารไม่มีหลักฐานรายการดังกล่าว หากลูกค้าไม่มีหลักฐานพิสูจน์ว่าได้มีการดำเนินการโอน ลูกค้าควรจะต้องรับภาระหาทางพิสูจน์ด้วยตนเอง ในกรณีที่คำสั่งโอนเงินนั้นได้สูญหายหรือเกิดความล่าช้า หรือมีข้อผิดพลาดเมื่อมีการโอนเงินนั้นไปถึงธนาคารผู้รับเงินโอน แต่สาเหตุที่ก่อให้เกิดปัญหานั้นไม่กระจ่างชัด ธนาคารผู้โอนเงินควรจะต้องรับภาระพิสูจน์หาสาเหตุที่เกิดความขัดข้องหรือการทุจริตด้วยตนเอง น่าจะไม่มี ความจำเป็นต้องกำหนดระยะเวลาที่ใช้ในการโอนเงินจากผู้โอนไปยังผู้รับโอนหลังจากที่ธนาคารผู้โอนได้รับคำสั่งให้โอนแล้ว เพราะอย่างน้อยการโอนเงินทางอิเล็กทรอนิกส์จะต้องเร็วกว่าการโอนเงินด้วยเอกสารตามปกติ

Issue No.	ความเห็นของประเทศไทย
Issue No. 24 How often should a bank be required to send its customers a statement of account activity? ควรจะกำหนดให้ธนาคารส่ง statement แสดงว่าความเคลื่อนไหวในบัญชีของลูกค้าไปให้ลูกค้าบ่อยครั้งแค่ไหน	statement ที่ธนาคารต้องส่งให้แก่ลูกค้าควรให้เป็นไปตามประเพณีที่ปฏิบัติกันในแต่ละประเทศ ไม่ควรถูกกำหนดเป็นกฎเกณฑ์ตายตัว แต่อย่างน้อยที่สุดไม่ควรต่ำกว่าเดือนละ 1 ครั้ง
Issue No. 25 How much time should bank customer have to notify his bank of improper entries to his account? ลูกค้ามีเวลาเท่าใดในการแจ้งให้ธนาคารทราบเกี่ยวกับการผ่านรายการผิดพลาดลงในบัญชีของตน	ควรจะให้เร็วที่สุดเท่าที่จะเป็นไปได้เมื่อลูกค้าได้รับ statement หรือรับข้อมูลจากธนาคารผ่านเครื่อง Terminal แต่การที่จะกำหนดเวลาที่สมควรใช้ในการแจ้งเป็นมาตรฐานเดียวกันทั้งหมดนั้นไม่น่าจะกระทำได้ ทั้งนี้ขึ้นอยู่กับสภาพแวดล้อมที่จะมีผลในทางปฏิบัติของแต่ละประเทศ
Issue No. 26 Should there be any articulated error resolution procedure? ควรจะมีการกำหนดกรรมวิธีในการแก้ไขข้อผิดพลาดไว้อย่างชัดเจนหรือไม่	ควรมีการกำหนดมาตรฐานขั้นต่ำของกรรมวิธีในการแก้ไขข้อผิดพลาดไว้อย่างชัดเจน
Issue No. 27 Should either the transferor or the transferee recover interest for a delay of a funds transfer? ผู้โอนเงินหรือผู้รับโอนควรจะต้องได้รับการชดเชยเป็นดอกเบี้ยหรือไม่ ถ้าการโอนเงินนั้นเกิดความล่าช้ากว่าที่ควรจะเป็น	ผู้รับโอนควรจะได้รับ การชดเชยเป็นดอกเบี้ย ถ้าการโอนเงินนั้นใช้เวลามากกว่าที่ควร ในกรณีที่บัญชีของผู้รับโอนนั้นเป็นบัญชีที่มีดอกเบี้ย โดยคิดตามจำนวนวันที่ล่าช้ากว่าที่ควรจะเป็นในทางปฏิบัติของแต่ละประเทศ
Issue No. 28 Should either the transferor or the transferee recover exchange losses for delay of a funds transfer? ผู้โอนเงินหรือผู้รับโอนควรจะต้องได้รับการชดเชยการ	ในกรณีที่เป็น การซื้อขายเงินตราต่างประเทศหรือการทำ hedging ในตลาดเงินตราต่างประเทศนั้น การโอนเงินจะต้องมีความถูกต้องรวดเร็ว เนื่องจากอัตราแลกเปลี่ยนเคลื่อนไหวอยู่ตลอดเวลา ดังนั้น หากเกิดความล่าช้าในการโอนขึ้น ความเสียหายจะเกิดขึ้นแก่ผู้โอนหรือ

Issue No.	ความเห็นของประเทศไทย
ขาดทุนในอัตราแลกเปลี่ยนเงินตรา สำหรับความล่าช้าในการโอนเงินหรือไม่ Issue No. 29 Under what circumstances should the bank be liable for consequential damages? ในสถานการณ์เช่นใดที่ธนาคารควรจะต้องรับผิดชอบต่อผลเสียหายที่ติดตามมา Issue No. 30 Should there be special rules governing the inter-bank liability for late reimbursement or for erroneous funds transfers? ควรจะมีกฎข้อบังคับเป็นพิเศษสำหรับใช้บังคับเรื่องความรับผิดชอบระหว่างธนาคาร ซึ่งเกิดจากได้รับเงินล่าช้า หรือการโอนเงินที่ผิดพลาด หรือไม่ Issue No. 31 What should be the consequences of a funds transfer or funds transfer transaction becoming final? หากกระบวนการโอนเงินได้เสร็จสิ้นโดยสมบูรณ์แล้ว ควรจะมีผลทางบัญชีต่อไปอย่างไร	ผู้รับโอน ซึ่งความเสียหายดังกล่าวมิใช่ความผิดของผู้โอนหรือผู้รับโอน ดังนั้น ผู้โอนหรือผู้รับโอนควรจะได้รับ การชดเชยจากความล่าช้าดังกล่าว ความเสียหายที่อาจจะเกิดติดตามมาเนื่องจากการโอนเงินล่าช้ากว่ากำหนดนั้น เช่น ผู้โอนเงินอาจถูกบอกเลิกสัญญา หรือถูกปรับ หรือหมดสิทธิบางประการ ถ้าความล่าช้านี้เกิดจากธนาคารผู้โอนเงิน ผู้โอนเงินควรจะได้รับ การชดเชยค่าเสียหายที่เกิดขึ้นนั้น ถ้าผู้โอนเงินได้แจ้งให้ธนาคารผู้โอนทราบถึงความสำคัญของระยะเวลาที่ต้องใช้ในการโอนแล้ว ธนาคารผู้โอนจะต้องรับผิดชอบต่อความเสียหายที่เกิดจากการโอนเงินล่าช้าผิดปกตินั้น โดยธนาคารดังกล่าวอาจจะคิดค่าธรรมเนียมเพิ่มขึ้นเป็นพิเศษก็ได้สำหรับการโอนเงินรายการนั้น ควรมีกฎข้อบังคับเป็นพิเศษสำหรับใช้บังคับเรื่องภาระหนี้ระหว่างธนาคาร ซึ่งเกิดจากการได้รับเงินล่าช้า หรือการโอนที่ผิดพลาด ในกรณีที่เป็น การโอนเงินระหว่างประเทศ เนื่องจากกฎหมายของแต่ละประเทศมีความแตกต่างกัน หรือบางประเทศก็ไม่มีกฎหมายบังคับในเรื่องนี้ จึงควรมีการออกกฎข้อบังคับสากลขึ้น เพื่อความยุติธรรมในการโอนเงินระหว่างประเทศ ส่วนการโอนเงินภายในประเทศ อาจไม่มีความจำเป็นต้องออกกฎเป็นพิเศษในกรณีที่ยังไม่มีกฎหมายใช้บังคับ เนื่องจากธนาคารควรจะ สามารถตกลงกันเองได้ หรือสมาคมธนาคารของแต่ละประเทศควรจะกำหนดมาตรฐานกันเองได้ ขึ้นอยู่กับว่า กระบวนการโอนเงินได้เสร็จสิ้นสมบูรณ์ ณ จุดใด แต่โดยทั่วไปแล้วกระบวนการโอนเงินควรถือว่าการสิ้นสุดลงเมื่อผู้รับโอนได้รับผ่านบัญชีแล้ว ไม่ควรจะเป็นการผ่านโดยเดบิตหรือเครดิต ดังนั้น ผลของความสมบูรณ์ในการโอนเงินจะทำให้ยอดคงเหลือในบัญชีของผู้รับโอนเปลี่ยนไป

Issue No.	ความเห็นของประเทศไทย
Issue No. 32 Should funds transfer be final for any or all purposes on the happening of a particular point of time? ความสำเร็จสิ้นสมบูรณ์ของการโอนเงินนั้นควรจะขึ้นอยู่กับกระบวนการโอนเงินหรือขึ้นอยู่กับขีดจำกัดของเวลา Issue No. 33 What should be the effect on a credit transfer between two customers that a funds transfer transaction between two banks has become final? หากกระบวนการโอนเงินระหว่างธนาคารได้เสร็จสิ้นโดยสมบูรณ์แล้ว การโอนเงินแบบ credit transfer จะมีผลต่อผู้โอนและผู้รับโอนอย่างไร Issue No. 34 Should the time of finality of a funds transfer be assested by a guarantee of honour of the funds transfer instruction by the transferor bank? Guarantee of honour จากธนาคารผู้โอนควรมีผลต่อความสำเร็จสิ้นสมบูรณ์ของกระบวนการโอนเงินหรือไม่ Issue No. 35 Should there be a specific rule as to whether a transferee bank to which funds have been sent for delivery to the transferee upon identification holds the funds for the transferor or for the transferee?	กระบวนการโอนเงินนั้นควรจะถือว่าสิ้นสุดลงเมื่อผู้รับโอนได้รับการเครดิตบัญชีจากธนาคารผู้รับโอนแล้ว อันหมายความว่า ธนาคารผู้รับโอนได้ตอบยืนยันการรับโอนและเครดิตบัญชีตามคำสั่งแล้วรายการโอนดังกล่าวจะไม่สามารถล้างรายการหรือกลับรายการได้ อย่างไรก็ดี ขีดความสามารถของเทคโนโลยีที่ใช้ในระบบการโอนเงินนั้นยังมีความแตกต่างกันหากยึดถือพิธีการโอนเป็นเกณฑ์ จะเกิดความได้เปรียบเสียเปรียบในเทคโนโลยีแต่ละประเภท ดังนั้น จึงควรใช้เกณฑ์เวลาเป็นเครื่องกำหนดความสำเร็จสิ้นสมบูรณ์ในการโอนเงิน หากการโอนสิ้นสุดแล้ว ผลของการโอนเงินควรจะทำให้ผู้รับโอนมีสิทธิที่จะถอนเงินออกจากบัญชีได้ ดังนั้น เมื่อการโอนสิ้นสุดลงแล้ว ผู้โอนหรือธนาคารผู้โอนก็ไม่มีสิทธิที่จะขอล้างรายการโอนหรือสั่งให้ธนาคารผู้รับโอน โอนเงินกลับไปได้ เนื่องจาก guarantee of honour ทำให้ผู้รับโอนไม่สามารถใช้เงินที่ได้รับโอนมาทันที แต่ guarantee of honour ก็จะเป็นเครื่องยืนยันในความสมบูรณ์ของการโอนว่าจะไม่มีการล้างรายการหากการโอนได้เสร็จสิ้นโดยสมบูรณ์แล้ว ดังนั้น หาก guarantee of honour จะเป็นผลให้ความสำเร็จสิ้นสมบูรณ์ของการโอนต้องเลื่อนออกไปอีกก็เป็นเรื่องที่น่าจะอนุโลมให้ได้ เมื่อธนาคารผู้รับโอนได้รับโอนเงินมาแล้วก็ไม่ควรถือไว้ในรายการพัก แต่ควรจะเครดิตบัญชีให้ผู้รับโอนในทันที ทั้งนี้ หลักเกณฑ์ดังกล่าวควรจะระบุให้แน่ชัดว่าธนาคารผู้รับโอนจะต้องเครดิตบัญชีให้แก่ผู้รับโอนในทันทีหลังจากได้รับคำสั่งโอนเงินดังกล่าว

Issue No.	ความเห็นของประเทศไทย
ควรจะมีกฎเกณฑ์ระบุโดยแน่ชัดหรือไม่ว่าธนาคารผู้รับโอนจะต้องผ่านบัญชีให้แก่ผู้รับโอนในทันที หลังจากที่ได้รับโอนเงินมาแล้ว หรือสามารถถือไว้ในบัญชีพักก่อนได้ Issue No. 36 Should the time when an underlying obligation is discharged by means of a funds transfer be dependent upon the means used by the banks to effect the funds transfer? Should the time of discharge be the same as the time when the funds transfer becomes final? การสิ้นสุดภาระในการโอนเงินควรขึ้นอยู่กับพิธีปฏิบัติและเครื่องมือที่ใช้ในระบบการโอนเงินหรือไม่ ภาระควรจะสิ้นสุดในเวลาเดียวกับกระบวนการโอนเงินได้เสร็จสิ้นโดยสมบูรณ์หรือไม่ Issue No. 37 Should the rules governing funds transfers take into consideration the possibility that a bank may fail to settle? ระเบียบในการโอนเงินนั้นจำเป็นต้องคำนึงถึงความเสี่ยงที่ธนาคารจะล้มเลิกการผ่านบัญชีหรือไม่	การสิ้นภาระจากการโอนเงินนั้นต้องขึ้นอยู่กับกระบวนการปฏิบัติในเรื่องการโอนเงินของแต่ละธนาคารด้วย เพราะแต่ละธนาคารก็มีพิธีปฏิบัติในการโอนเงินและเทคโนโลยีทางการสื่อสารแตกต่างกันไป ดังนั้น ภาระดังกล่าวก็น่าจะหมดลง หลังจากทีกระบวนการโอนเงินตามพิธีปฏิบัติของธนาคารได้จบสิ้นโดยสมบูรณ์แล้ว คือ ผู้รับโอนมีสิทธิที่จะใช้เงินที่ได้รับโอนแล้ว หากคำสั่งโอนมิได้ถูกดำเนินการแล้วจะก่อให้เกิดความเสียหายแก่ผู้โอนหรือผู้รับโอน โดยเฉพาะอย่างยิ่ง ถ้าเป็นการโอนเงินระหว่างประเทศความเสียหายจะมีมูลค่าสูง ถึงแม้ในปัจจุบันระบบการโอนเงินจะดำเนินงานด้วยเทคโนโลยีที่ทันสมัยก็ตาม แต่ความล้มเหลวของระบบอาจจะเกิดขึ้นเมื่อไรก็ได้ ดังนั้นระบบการโอนเงินจึงมีความเสี่ยงอยู่เสมอ ดังนั้น หากธนาคารไม่สามารถที่จะดำเนินการกระบวนการโอนเงินให้เสร็จสมบูรณ์ได้ ไม่ว่าจะกรณีใดก็ตาม ควรจะมีผู้รับผิดชอบในความเสียหายที่เกิดขึ้น และจำเป็นต้องมีกฎหมายระบุอย่างแน่ชัดในเรื่องผู้รับผิดชอบในกรณีที่ธนาคารใดธนาคารหนึ่งไม่สามารถจะดำเนินการโอนเงินตามคำสั่งให้เสร็จสมบูรณ์ได้

Issue No.	ความเห็นของประเทศไทย
Issue No. 38 Can a funds transfer bring final outside the normal working hours? กระบวนกรโอนเงินนั้นจะเสร็จสิ้นโดยสมบูรณ์นอกเวลาทำการปกติได้หรือไม่	โดยที่ระบบการเงินทางอิเล็กทรอนิกส์แบบ on-line นั้น ลูกค้าสามารถจะติดต่อกับธนาคารได้ตลอด 24 ชั่วโมง ดังนั้น หากยึดหลักเกณฑ์ที่ว่ากระบวนกรโอนเงินจะเสร็จสมบูรณ์ต่อเมื่อผู้รับโอนมีสิทธิที่จะถอนเงินที่ได้รับโอนออกไปใช้ได้แล้วความสมบูรณ์ของการโอนเงินก็เป็นไปตลอด 24 ชั่วโมงด้วยเช่นกัน นอกจากนี้ หากเป็นการโอนเงินระหว่างประเทศที่มีความแตกต่างกันเรื่องเวลานั้น ไม่สามารถจะระบุได้ว่าช่วงเวลาใดคือเวลาปฏิบัติงานปกติ เนื่องจากเวลาของแต่ละประเทศแตกต่างกัน ดังนั้น จึงต้องถือว่าความสมบูรณ์ของการโอนจะอยู่ในเวลาใดก็ได้ ไม่จำเป็นต้องภายในเวลาปฏิบัติงานปกติ
Issue No. 39 When should a debit or credit be considered to be entered to an account? ธนาคารจะสามารถเดบิตหรือเครดิตบัญชีลูกค้าเมื่อใด	หากธนาคารสามารถพิสูจน์ได้ว่า คำสั่งในการโอนนั้นเป็นคำสั่งที่ส่งโดยผู้ที่มีสิทธิตามกฎหมายเป็นไปโดยเจตนาสุจริต และบัญชีทั้งของผู้โอนและผู้รับโอนถูกต้องสอดคล้องตามคำสั่งนั้น ก็สามารถจะเดบิตหรือเครดิตบัญชีได้ทันที
Issue No. 40 In what order of priority should the various entries to an account be considered to have been made? ธนาคารควรมีหลักเกณฑ์ในการเรียงลำดับการผ่านรายการให้ลูกค้าอย่างไร	ลำดับในการลงรายการควรขึ้นอยู่กับเวลาที่ลูกค้ากระทำการรายการนั้น มิใช่ลำดับของพิธีการผ่านรายการของธนาคาร ไม่ว่าจะเป็นการผ่านรายการด้วยเอกสารหลักฐานงาน batch หรือ on-line ควรจะยึดถือ วัน เวลาที่ลูกค้าติดต่อเป็นเครื่องลำดับการผ่านรายการ
Issue No. 41 Should a bank have a right to recover an erroneous credit by reversing an entry to the account of credit party.? หากธนาคารผ่านรายการเครดิตไปให้ลูกค้าผิดบัญชีธนาคารมีสิทธิล้างรายการเครดิตดังกล่าวออก เพื่อผ่านรายการเครดิตให้แก่บัญชีที่ถูกต้องได้หรือไม่	หากเป็นการลงรายการผิดพลาด และธนาคารสามารถพิสูจน์ได้ว่าเป็นการผ่านรายการเครดิตผิดบัญชีธนาคารก็ควรมีสิทธิที่จะล้างรายการออกได้เพื่อเครดิตให้บัญชีที่ถูกต้องต่อไป ทั้งนี้ธนาคารต้องแจ้งให้ลูกค้าที่ธนาคารผ่านรายการเครดิตที่ผิดพลาดทราบในทันทีที่ได้ล้างรายการออกแล้ว

ภาคผนวก ข

ความเป็นมาของการประชุมร่างแนวทางกฎหมาย
การโอนเงินทางอิเล็กทรอนิกส์โดย UNCITRAL
(The United Nations Commission on International Trade Law)
โดยมีเป้าหมายเป็นการร่างรูปแบบกฎหมายการโอนเครดิตระหว่างประเทศ
(Draft Model Law on International Credit Transfers)

UNCITRAL มีเป้าหมายที่จะสนับสนุนส่งเสริมความก้าวหน้าในความสอดคล้องและเป็นอันหนึ่งอันเดียวกันของกฎหมายที่เกี่ยวกับการค้าระหว่างประเทศของทั่วโลก

ในปี พ.ศ. 2525 ได้เริ่มมีการศึกษาแนวร่างกฎหมายการโอนเงินทางอิเล็กทรอนิกส์ด้วยมีวัตถุประสงค์ที่จะให้แนวทางแก่ผู้ออกกฎหมายหรือนักกฎหมายในการออกกฎหมายดังกล่าว

ในปี พ.ศ. 2529 ได้มีการเสนอร่างกฎหมายหลายบทเข้าสู่การประชุมครั้งที่สิบเจ็ดของ The Commission

ในการประชุมครั้งที่ 18 ของ The Commission ที่กรุงเวียนนา ในระหว่างวันที่ 3-21 มิถุนายน 2529 ได้มีการเสนอให้ส่งแนวร่างกฎหมายดังกล่าวไปยังรัฐบาลของประเทศต่าง ๆ และองค์การระหว่างประเทศที่เกี่ยวข้องเพื่อสอบถามความคิดเห็นและขอข้อสังเกต และมีการทบทวนร่างดังกล่าวเพื่อเสนอเข้าพิจารณาในการประชุมครั้งต่อไป โดยธนาคารแห่งประเทศไทยได้ออกความเห็นในเรื่องที่กล่าวผ่านกระทรวงการต่างประเทศไปให้ UNCITRAL ตามรายละเอียดต่อจากเรื่องนี้

สำหรับสาเหตุที่ต้องการศึกษาในเรื่องดังกล่าว เพราะในปัจจุบันในประเทศต่าง ๆ ได้มีการนำเอาเทคโนโลยีทางด้านคอมพิวเตอร์และการสื่อสารเข้ามาใช้ในการโอนเงิน ทำให้รูปแบบของการโอนเงินในลักษณะที่ใช้เอกสารเป็นเครื่องมือ (Paper-based funds transfers) เปลี่ยนไป กลายเป็นการโอนเงินทางอิเล็กทรอนิกส์ (Electronic funds transfers) ซึ่งมีลักษณะเฉพาะและมีความแตกต่างจากการโอนเงินในรูปแบบเดิม ทำให้เกิดปัญหาในด้านกฎหมายที่จะใช้รองรับ โดยเฉพาะอย่างยิ่งในการโอนเงินระหว่างประเทศอันเนื่องมาจากการค้าระหว่างประเทศ หากมีความแตกต่างของกฎหมายและวิธีปฏิบัติแล้ว ย่อมเป็นอุปสรรคที่จะก่อให้เกิดความไม่สะดวกในการค้าระหว่างประเทศได้ การกำหนดมาตรฐานและรูปแบบของกฎหมายร่วมกันในระหว่างนานาประเทศจึงเป็นสิ่งจำเป็น นอกจากนี้ ยังเป็นประโยชน์ในการพัฒนากฎหมายการโอนเงินในประเทศให้สอดคล้องและเป็นอันหนึ่งอันเดียวกับมาตรฐานสากลอันเป็นที่ยอมรับกันทั่วไป ซึ่งจะเป็นการช่วยในการพัฒนาระบบการชำระเงินของประเทศอีกส่วนหนึ่งด้วย

หมายเหตุ : จากการเข้าร่วมประชุมที่สหประชาชาติ NYC ประเทศสหรัฐอเมริกาปี 2532 ทั้งนี้ไม่ได้นำรายละเอียดผลของการประชุมและร่างข้อตกลงเบื้องต้นมากล่าวในที่นี้

1. การประชุมกลุ่มทำงานว่าด้วยการชำระหนี้ระหว่างประเทศ

การร่างรูปแบบกฎหมายการโอนเครดิตระหว่างประเทศนี้เดิมใช้ชื่อว่ารูปแบบกฎเกณฑ์การโอนเงินทางอิเล็กทรอนิกส์ (Model Rules on Electronic Funds Transfer) ต่อมาที่ประชุมได้พิจารณาเปลี่ยนชื่อใหม่เป็น Draft Model Law on International Credit Transfers เพื่อให้ครอบคลุมการโอนเครดิตทุกประเภทที่ดำเนินการในแบบ Electronics และในแบบการโอนด้วยตราสารปกติ

2. ข้อคิดเห็นจากการประชุมว่าด้วยการชำระหนี้ระหว่างประเทศ

เนื่องจากการประชุมของ UNCITRAL มีวัตถุประสงค์เพื่อให้มีกฎหมายสากลสำหรับใช้ควบคุมการโอนเครดิตระหว่างประเทศ ซึ่งส่วนใหญ่เป็น Electronic Funds Transfer ใช้ยึดเป็นหลักปฏิบัติและยอมรับโดยทั่วไป โดยแต่ละประเทศอาจนำกฎหมายนี้ไปใช้หรือปรับใช้ในการออกกฎหมายหรือกฎเกณฑ์ควบคุมเกี่ยวกับเรื่องนี้ภายในประเทศของตนตามความเหมาะสม

อย่างไรก็ดี การพิจารณานำเอากฎหมายการโอนเครดิตระหว่างประเทศนี้มาปรับใช้ในการออกกฎหมายของแต่ละประเทศนั้น ควรที่จะพิจารณาความเห็นของคณะทำงานที่เกี่ยวข้องจากระบบการชำระเงินจากธนาคารกลางของประเทศกลุ่ม G-10 ซึ่งได้จัดให้มีการประชุมที่ Basel ในช่วงเวลากลางปี พ.ศ. 2531 โดยได้เริ่มศึกษาเกี่ยวกับข้อตกลงในการหักกลบลบหนี้ (Netting arrangement) หรือรายการที่เกี่ยวข้องกับการเงินระหว่างประเทศ ที่มีอยู่และที่จะเกิดขึ้นในอนาคตด้วยว่าจะมีส่วนช่วยสนับสนุนตลาดการเงินระหว่างประเทศ และระบบการชำระเงินระหว่างประเทศอย่างไร จะมีผลกระทบต่อความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องของคู่สัญญาและธนาคารอย่างไร โดยมีรายละเอียดในภาคผนวกเล่มนี้ด้วยแล้ว

การพิจารณาดังกล่าวจะช่วยทำให้การออกกฎหมายหรือกฎเกณฑ์ใด ๆ ที่เกี่ยวกับการโอนเครดิตระหว่างประเทศ มีความรอบคอบรัดกุมและครอบคลุมเรื่องที่สำคัญได้เป็นอย่างดี สำหรับประเทศไทยเราก็ได้มีการพัฒนาเทคโนโลยีด้านธุรกิจการธนาคารพาณิชย์อย่างรวดเร็วและอาจจำเป็นต้องมีกฎหมายการโอนเงินทางอิเล็กทรอนิกส์ หรือ EFT Acts ในประเทศและการโอนเงินเครดิตระหว่างประเทศในลักษณะ Electronic ต่อไปในอนาคต เพื่อรองรับความก้าวหน้าทางเทคโนโลยีที่เกี่ยวข้องกับการโอนเงินระหว่างประเทศจะแล้วเสร็จ (Draft Model Law on International Credit Transfers) ที่ประชุมที่ UN ได้ประมาณไว้ในปี พ.ศ. 2534 ทั้งนี้ เพื่อจะได้มีการศึกษาเตรียมการ และติดตามเรื่องราวที่เกี่ยวข้อง ซึ่งมีอยู่มากได้ทันการและเหมาะสม เช่น การศึกษา Netting arrangement ของกลุ่ม G-10 ประกอบกันไปกับการศึกษาการโอนเงินทางอิเล็กทรอนิกส์ และการโอนเครดิตทั้งในประเทศและระหว่างประเทศจาก EFT Act และจาก Draft Model Law on International Credit Transfers ตลอดจนการจัดทำร่างรูปแบบ กฎเกณฑ์การโอนเครดิตไว้ล่วงหน้า เพื่อใช้ศึกษาเปรียบเทียบ และรวบรวมประเด็นที่น่าจะหยิบยกหาหรือในการประชุม เพื่อให้ประเทศโดยมีกฎหมายที่เกี่ยวข้องในเรื่องนี้ทันเวลาที่เหมาะสม

ภาคผนวก ค

แนวความคิดของการออกกฎหมายเพื่อการโอนเงินทางอิเล็กทรอนิกส์

1. บทนำ

ปัจจุบันธนาคารพาณิชย์ทุกธนาคารให้บริการโอนเงินทางอิเล็กทรอนิกส์แก่ลูกค้า และมีแนวโน้มว่าวิธีการโอนเงินทางอิเล็กทรอนิกส์จะขยายตัวออกไปอีกอย่างไม่หยุดยั้งในสถาบันการเงินต่าง ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์เป็นวิธีการเฉพาะซึ่งแตกต่างจากวิธีการทางเอกสารอย่างสิ้นเชิงโดยเฉพาะในเรื่อง

1.1 อุปกรณ์ และวิธีการปฏิบัติงานทางอิเล็กทรอนิกส์ ล้วนเป็นเครื่องอัตโนมัติการบันทึกและเก็บข้อมูลใช้ระบบแม่เหล็กไฟฟ้าแทนระบบเอกสาร การสื่อสารระหว่างกันจะใช้ระบบโทรคมนาคม การตรวจสอบ การอนุมัติรายการ และการพิสูจน์สิทธิต่าง ๆ ใช้วิธีการของรหัสแทนลายเซ็น

1.2 เครื่องมือการชำระเงิน ได้เปลี่ยนจากตราสารมาเป็นบัตรพลาสติก เช่น บัตรเดบิต และบัตรเครดิต ซึ่งมีวิธีการปฏิบัติเฉพาะที่ส่งผลเป็นการชำระเงินเช่นเดียวกับตราสารแต่กลับปราศจากสถานะทางกฎหมาย

เมื่อวิธีการทางอิเล็กทรอนิกส์ถูกนำมาแทนที่วิธีการทางเอกสารแล้ว กฎเกณฑ์ต่าง ๆ ที่เคยยึดถือมาก่อนก็ไม่สามารถจะใช้ได้อีกต่อไป โดยเฉพาะอย่างยิ่งในเรื่องของการแสดงหลักฐานและการพิสูจน์หลักฐานของธุรกรรม จึงทำให้เกิดช่องว่างทางกฎหมายที่ไม่สามารถจะชี้ชัดตัดสินโดยชอบธรรมได้เมื่อเกิดปัญหาในการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งได้เคยเกิดขึ้นมาแล้วทั้งในประเทศและต่างประเทศ

ทางออกของธนาคารพาณิชย์ที่ปฏิบัติกันอยู่ในขณะนี้จึงใช้วิธีการของสัญญา การให้บริการระหว่างธนาคารกับลูกค้าผู้ใช้บริการ ซึ่งไม่เพียงแต่จะผูกมัดให้ผู้ใช้บริการต้องปฏิบัติตามกฎเกณฑ์ที่ธนาคารกำหนดไว้เท่านั้น ยังเป็นการผลักภาระความรับผิดชอบทั้งหลายให้แก่ผู้ใช้บริการ โดยไม่เปิดทางให้ผู้ใช้บริการสามารถยกขึ้นมาเป็นข้อเรียกร้องเมื่อเกิดความสูญเสียอีกด้วย วิธีการของสัญญาในลักษณะดังกล่าวจึงมิใช่ทางออกที่เป็นธรรม แต่เป็นเพียงการพยายามหลบเลี่ยงปัญหาด้วยชั้นเชิงทางกฎหมายเท่านั้น

วัตถุประสงค์ของภาคผนวกเรื่องนี้ก็เพื่อให้องค์กรทางการเงินและลูกค้าได้ทราบเรื่องราวที่ใกล้เคียงและอาจเป็นประโยชน์และเข้าใจเมื่อกฎหมายการโอนเงินทางอิเล็กทรอนิกส์มีใช้ในประเทศไทยในอนาคต

2. ขอบเขตของกฎหมายการโอนเงินทางอิเล็กทรอนิกส์ (EFT Acts)

เนื่องจากการโอนเงินทางอิเล็กทรอนิกส์เป็นเรื่องที่เกี่ยวข้องกับผลประโยชน์ของประชาชนจำนวนมาก ฉะนั้นจึงจำเป็นต้องมีกฎหมายที่ถาวรและมีผลบังคับใช้ได้ทั่วไป วิธีการที่ดีที่สุดคือการมีกฎหมายเฉพาะสำหรับการโอนเงินทางอิเล็กทรอนิกส์ โดยกฎหมายดังกล่าวควรมีลักษณะดังนี้

2.1 ให้การรับรองผลแห่งธุรกรรมการโอนเงินทางอิเล็กทรอนิกส์ว่าเป็นธุรกรรมตามกฎหมายพร้อมทั้งให้คำจำกัดความสมบูรณ์ในการโอนเงินทางอิเล็กทรอนิกส์และเงื่อนไขต่าง ๆ เมื่อจะเพิกถอนหรือยกเลิกการโอนเงิน

2.2 กำหนดเงื่อนไขในการแสดงหลักฐาน อันเกิดจากการบันทึกและการเก็บรักษาข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ พร้อมทั้งให้คำจำกัดความที่ชัดเจนในสถานภาพของบัตรเดบิตและบัตรเครดิต ซึ่งเป็นเครื่องมือทางการเงินตามวิธีการโอนเงินทางอิเล็กทรอนิกส์

2.3 กำหนดสิทธิ หน้าที่ ภาระ และความรับผิดชอบของฝ่ายต่าง ๆ ที่เกี่ยวข้องกับธุรกรรมการโอนเงินทางอิเล็กทรอนิกส์

3. ความจำเป็นที่ต้องมีกฎหมาย

เนื่องด้วยปัจจุบันธนาคารพาณิชย์เกือบทุกธนาคารได้หันมาเน้นความสำคัญของการทำธุรกิจด้านธนาคารอิเล็กทรอนิกส์เพิ่มขึ้นตามลำดับ วิธีการโอนเงินทางอิเล็กทรอนิกส์มีแนวโน้มจะมีวิวัฒนาการสูงขึ้นและกว้างขึ้นอย่างรวดเร็ว และเนื่องจากการโอนเงินทางอิเล็กทรอนิกส์ เป็นวิธีการชำระเงินที่มีกระบวนการปฏิบัติงานแตกต่างจากการชำระเงินโดยทางเอกสารอย่างสิ้นเชิงกล่าวคือ

2.1 มีความรวดเร็วสูงมาก การโอนเงินจะเกิดขึ้นทันทีที่ได้รับคำสั่งให้โอนเงินโดยไม่สามารถเพิกถอนหรือระงับคำสั่งนั้นได้

2.2 การบันทึกหลักฐานตามขั้นตอนต่าง ๆ ในการปฏิบัติงาน ตลอดจนข้อมูลที่เกี่ยวข้องจะอยู่ในรูปของคลื่นแม่เหล็กไฟฟ้า ไม่สามารถจะตรวจสอบติดตามหรือหยิบยกขึ้นมาแสดงให้เห็นได้ดังเช่นวิธีการทางเอกสาร

2.3 เครื่องมือที่ใช้สั่งให้มีการชำระเงินหรือโอนเงินได้เปลี่ยนแปลงไปจากเดิมที่เคยใช้ตราสารปกติมาเป็นบัตรพลาสติกที่ติดแถบแม่เหล็กหรือบรรจุวงจรอิเล็กทรอนิกส์ไว้ภายในแทน เช่น บัตรเดบิตและบัตรเครดิต เป็นต้น

ดังนั้น ขั้นตอนการปฏิบัติงานในวิธีการโอนเงิน จึงขาดความสอดคล้องกับกฎหมายที่มีอยู่ในปัจจุบัน ซึ่งถูกสร้างขึ้นเพื่อรองรับธุรกรรมจากเอกสารเท่านั้น กฎหมายดังกล่าวจึงไม่สามารถจะประยุกต์ใช้กับธุรกรรมการโอนเงินทางอิเล็กทรอนิกส์ได้ ธนาคารซึ่งให้บริการโอนเงินทางอิเล็กทรอนิกส์ในปัจจุบัน จึงอาศัยสัญญาการให้บริการระหว่างธนาคารกับลูกค้าเป็นเครื่องมือเพื่อหลีกเลี่ยงปัญหาทั้งปวงตลอดมา

ประเด็นสำคัญที่กฎหมายปัจจุบันไม่สามารถจะนำมาใช้กับวิธีการโอนเงินทางอิเล็กทรอนิกส์ได้คือ ประเด็นในเรื่องการแสดงหลักฐานและการพิสูจน์หลักฐาน เนื่องด้วยวิธีการทางอิเล็กทรอนิกส์เป็นกระบวนการประมวลผล และเก็บข้อมูลด้วยคลื่นแม่เหล็กไฟฟ้าเอาไว้ในเทปหรือแผ่นจานแม่เหล็ก การยอมรับหลักฐานในรูปแบบดังกล่าวยังไม่มีความชัดเจน นอกจากนี้นี้ยังขาดหลักเกณฑ์ในการกำหนดสิทธิ หน้าที่ และความรับผิดชอบของฝ่ายต่าง ๆ ที่เกี่ยวข้องในธุรกรรมดังกล่าว ดังนั้น เมื่อเกิดความเสียหายจากการโอนเงินทางอิเล็กทรอนิกส์ก็ไม่สามารถจะยึดถือเกณฑ์ตัดสินใจที่ให้ความยุติธรรมแก่ทุกฝ่ายได้ ดังนั้น การจัดสร้างกฎหมายเฉพาะขึ้นมาใช้รองรับธุรกรรมดังกล่าวอย่างเหมาะสม จึงเป็นเรื่องที่ต้องให้ความสนใจ

4. สาเหตุที่ทำให้เกิดช่องว่างทางกฎหมาย

4.1 สาเหตุจากอุปกรณ์การปฏิบัติงานและวิธีการปฏิบัติงานด้วยเครื่องอิเล็กทรอนิกส์

แม้ว่าอุปกรณ์อิเล็กทรอนิกส์จะถือเป็นเครื่องมือในการปฏิบัติงานชนิดหนึ่ง แต่การปฏิบัติงานด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น การประมวลผลด้วยเครื่องคอมพิวเตอร์ การบันทึกหรือเก็บข้อมูลด้วยเทปแม่เหล็กหรือแผ่นจานแม่เหล็ก การอนุมัติขั้นตอนการปฏิบัติงานด้วยรหัส และการสื่อสารข้อความด้วยระบบโทรคมนาคมมิใช่เป็นเพียงการใช้เครื่องมือเสริมหรือประกอบการปฏิบัติงานบางส่วนดังเช่นการใช้เครื่องจักรในอดีต แต่เป็นการนำกระบวนการประมวลผลในรูปแบบใหม่เข้ามาแทนที่กระบวนการปฏิบัติงานเดิมทั้งหมด อันได้แก่

4.1.1 วิธีการบันทึก ทำโดยกระบวนการของคลื่นแม่เหล็กไฟฟ้าในรูปของรหัสซึ่งเรียกว่าภาษาเครื่องจักร ข้อมูลจะถูกเก็บไว้ในแฟ้มข้อมูลซึ่งเป็นเทปแม่เหล็กหรือแผ่นจานแม่เหล็กซึ่งไม่สามารถนำมาอ่านหรือใช้อ้างอิงได้ทันที แต่จะต้องนำไปผ่านกระบวนการทางอิเล็กทรอนิกส์ เพื่อแปลงรหัสที่บันทึกไว้ออกมาให้อยู่ในรูปแบบของภาษาที่ใช้สื่อความหมายได้ แล้วจึงแสดงผลออกมาจอภาพหรือโดยการจัดพิมพ์ออกมาเป็นเอกสาร

การเก็บข้อมูลด้วยรหัสและแปลงรหัสออกมาเป็นเอกสารด้วยวิธีการที่กล่าวนั้นมีได้มีกฎหมายรองรับ และจะเป็นปัญหาเมื่อต้องมีการพิสูจน์หลักฐานต่าง ๆ ในการบันทึก

4.1.2 วิธีการอนุมัติและการแสดงสิทธิเพื่อสั่งการให้มีการโอนเงินทางอิเล็กทรอนิกส์ล้วนเป็นการใช้รหัส โดยจะมีกระบวนการเฉพาะทางอิเล็กทรอนิกส์ในการพิสูจน์ถึงสิทธิของผู้สั่งให้มีการโอนเงินก่อนที่เครื่องอิเล็กทรอนิกส์จะปฏิบัติการโอนเงินให้ กระบวนการทั้งหมดไม่สามารถจะมองเห็นหรือพิสูจน์หลักฐานใด ๆ จึงเกิดปัญหาเรื่องการแอบแฝงสิทธิในการสั่งโอนเงินโดยทุจริต เพราะไม่สามารถจะใช้กฎเกณฑ์ใดพิสูจน์ได้ว่า การปฏิบัติตามคำสั่งโอนเงินดังกล่าวเป็นการปฏิบัติตามคำสั่งโอนเงินของผู้ทรงสิทธิโดยชอบธรรมหรือไม่

4.1.3 การสื่อสารทางอิเล็กทรอนิกส์ เป็นการใช้กระบวนการของระบบโทรคมนาคมซึ่งมีความรวดเร็ว เมื่อสิ้นสุดคำสั่งแล้วก็ไม่สามารถจะรับหรือเพิกถอนการโอนได้ ในขณะเดียวกันก็ไม่มีหลักเกณฑ์ระบุลงไปแน่ชัดว่าความสมบูรณ์ในการโอนเงินเสร็จสิ้นลงเมื่อใด

4.1.4 การปฏิบัติงานกลไกทางอิเล็กทรอนิกส์ ตามคำสั่งการโอนเงินกรณีที่มีข้อบกพร่องเนื่องจากความผิดพลาดล้มเหลวของระบบต่าง ๆ ทำให้การโอนเงินผิดพลาดล่าช้า จนเป็นเหตุให้เกิดความเสียหายแก่ฝ่ายหนึ่งฝ่ายใดแล้ว ควรจะกำหนดความรับผิดชอบเช่นไร

4.2 สาเหตุจากเครื่องมือการชำระเงินตามวิธีการทางอิเล็กทรอนิกส์

ด้วยเหตุที่วิธีการทางอิเล็กทรอนิกส์เป็นการใช้อุปกรณ์เฉพาะเข้ามาแทนที่กระบวนการเดิมทั้งหมด เครื่องมือในการชำระเงินจึงต้องเปลี่ยนแปลงไปให้เหมาะสมกับอุปกรณ์ดังกล่าววิธีการทางอิเล็กทรอนิกส์เครื่องมือการชำระเงินคือ บัตรพลาสติกติดแถบแม่เหล็ก หรือบัตรพลาสติกซึ่งบรรจุแผงวงจรไฟฟ้าขนาดเล็กและหน่วยความจำไว้ภายในมีวิธีการปฏิบัติในการโอนเงินหรือชำระเงินแตกต่างออกไป แต่ก็ไม่สามารถระบุสถานะทางกฎหมายของเครื่องมือดังกล่าวได้ ทั้ง ๆ ที่เครื่องมือนี้ยังคงไว้ซึ่งวัตถุประสงค์เดิมคือ เพื่อสั่งให้มีการโอนเงินหรือการชำระเงิน กล่าวคือ

4.2.1 การชำระเงินด้วยตราสารปกติ จะมีผลบังคับทางกฎหมายเมื่อมีการส่งมอบตราสาร โดยผู้รับสามารถโอนหรือส่งมอบให้ผู้อื่นต่อไปก็ได้ แต่เมื่อเป็นการชำระเงินทางอิเล็กทรอนิกส์ การโอนจะกระทำโดยตรงให้ผู้รับเงินรายสุดท้ายทันที โดยผู้รับจะโอนหรือส่งมอบให้ผู้อื่นต่อไปอีกไม่ได้

4.2.2 ในการชำระเงินด้วยตราสารปกติ การพิสูจน์สิทธิของผู้ส่งจ่ายกระทำได้ด้วยการพิสูจน์ลายเซ็นบนตราสาร แต่การชำระเงินทางอิเล็กทรอนิกส์เป็นการสั่งให้ธนาคารจ่ายเงินโดยวิธีการโอนทันทีที่ผู้ส่งโอนจะต้องพิสูจน์สิทธิของตนเองด้วยรหัสประจำตัว แต่ทางผู้รับเงินไม่จำเป็นต้องมีหลักฐานใด ๆ แสดงสิทธิในการรับเงิน กระบวนการทั้งสิ้นปฏิบัติโดยอุปกรณ์อิเล็กทรอนิกส์ซึ่งถูกกำหนดขั้นตอนการปฏิบัติงานไว้ล่วงหน้าแล้ว จึงไม่สามารถตรวจสอบติดตามขั้นตอนต่าง ๆ ได้เช่นวิธีการของตราสารปกติธรรมดา

4.2.3 เมื่อตราสารการชำระเงินสูญหาย ขนาดความเสียหายของการชำระเงินด้วยตราสารจะไม่เกินมูลค่าการชำระเงินที่ระบุไว้บนตราสารนั้น และในบางครั้งก็สามารถระงับการจ่ายเงินตามตราสารได้ทันที ในกรณีที่มีการทุจริต เช่น การปลอมเอกสารหรือลายเซ็นเจ้าของบัญชีก็จำเป็นต้องรับผิดชอบต่อความเสียหายนั้นเลย

แต่กรณีที่เครื่องมือการชำระเงินเป็นบัตรพลาสติก บัตรดังกล่าวมีมูลค่าเท่ากับเงินทั้งหมดในบัญชี ดังนั้นเมื่อสูญหายหรือเกิดการทุจริต มูลค่าความเสียหายอาจจะสูงเท่ากับเงินทั้งหมดในบัญชี และเจ้าของบัญชีก็ยากที่จะพิสูจน์ความสุจริตของตน

5. ปัญหาบางประการอันเกิดจากการโอนเงินทางอิเล็กทรอนิกส์

เนื่องจากกฎหมายที่มีอยู่ขาดความเหมาะสม หรือไม่ก็ขาดความสอดคล้องกับวิธีการโอนเงินทางอิเล็กทรอนิกส์ เมื่อเกิดความเสียหายในการโอนเงิน กฎเกณฑ์ทางกฎหมายที่มีอยู่จึงไม่เพียงพอที่จะให้คำชี้ขาดได้โดยยุติธรรม ในต่างประเทศการโอนเงินระหว่างธนาคารทางอิเล็กทรอนิกส์ เช่น การโอนผ่าน CHIPS, CHAPS หรือ SWIFT จะมีข้อตกลงระหว่างธนาคารผู้โอนและผู้รับโอน เกี่ยวกับพิธีการปฏิบัติและหลักเกณฑ์ในการตัดสินธุรกรรมเหล่านั้นในการโอนเงินระหว่างลูกค้ากับธนาคารก็มักจะใช้สัญญาระหว่างลูกค้ากับธนาคารเป็นเกณฑ์ในการปฏิบัติ แต่ก็ไม่สามารถจะครอบคลุมได้ทุกกรณี ปัญหาซึ่งมักจะพบอยู่เสมอและหาข้อยุติไม่ได้ตัวอย่างเช่น

5.1 กรณีการโอนเงินด้วยระบบ on-line ผ่านข่ายงานหักบัญชีระหว่างธนาคารในนิวยอร์ก (CHIPS) ที่มีปัญหาคือกรณี Delbrueck ได้สั่งให้ธนาคาร Manufacturers Hanover โอนเงินผ่าน CHIPS เพื่อเข้าบัญชี Herstatt ที่ธนาคาร Chase Manhattan แต่หลังจากเสร็จสิ้นการโอนเงินเพียง 2-3 นาที Delbrueck ก็ขอให้ธนาคาร Manufacturers Hanover ล้างรายการโอนเนื่องจากทราบว่า Herstatt กำลังประสบภาวะวิกฤตทางการเงิน แต่ธนาคาร Manufacturers Hanover ไม่สามารถล้างรายการดังกล่าวได้ ทั้ง ๆ ที่ธนาคาร Chase Manhattan ยังมีได้เครดิตบัญชีให้ Herstatt Delbrueck จึงฟ้องธนาคาร Manufacturers Hanover เรียกร้องค่าเสียหาย 12.5 ล้านดอลลาร์สหรัฐ แต่ภายหลังศาลได้ตัดสินให้ธนาคาร Manufacturers Hanover ชนะคดี ดังนั้น ต่อมา CHIPS จึงได้กำหนดหลักเกณฑ์ใหม่ให้ผู้โอนสามารถบอกยกเลิกการโอนได้ก่อนธนาคารปิดทำการได้

5.2 กรณีการโอนเงินระหว่างธนาคารซึ่งเกิดขึ้นในลอนดอน และเป็นกรณีของ Herstatt เช่นกัน คือ มีการโอนเงินจากบัญชีของ Herstatt ไปเข้าบัญชีของ Momm ซึ่งต่างก็เป็นลูกค้าของธนาคาร Barclays ในลอนดอน โดยปกติธนาคารจะประมวลผลการโอนเงินเมื่อสิ้นวัน และเจ้าหน้าที่ของธนาคารจะเป็นผู้ตรวจสอบความถูกต้องในการโอนในวันรุ่งขึ้น จากการตรวจสอบพบว่า Herstatt มียอดคงเหลือในบัญชีเป็นลูกหนี้ธนาคาร ในขณะที่เดียวกันก็ทราบว่า Herstatt ถูกทางการเยอรมันสั่งปิดแล้ว จึงล้งรายการโอนออกในเช้าวันรุ่งขึ้นนั้น Momm ได้ฟ้องธนาคาร Barclays ที่ล้งรายการโอนออกทั้ง ๆ ที่การโอนดังกล่าวสิ้นสุดลงโดยสมบูรณ์แล้ว ศาลตัดสินให้ธนาคาร Barclays แพ้คดีเนื่องจากการล้งรายการมิได้กระทำภายในวันเดียวกัน

กรณีตัวอย่างทั้งสองข้างต้น เกิดขึ้นเนื่องจากไม่มีกฎหมายในการโอนเงินที่ชัดเจนเพียงพอ

5.3 เรื่องของการแสดงหลักฐาน เป็นเรื่องที่ถกเถียงกันมากที่สุด เพราะกฎหมายมิได้เปิดทางให้สามารถแสดงหลักฐานอันเกิดจากการบันทึกด้วยเครื่องคอมพิวเตอร์ได้ทุกกรณี เช่น

5.3.1 ในบางประเทศกฎหมายจะยอมรับการแสดงหลักฐานที่จัดพิมพ์จากเครื่องคอมพิวเตอร์ เฉพาะในธุรกรรมทางการค้าเท่านั้น

5.3.2 ขณะที่กฎหมายในบางประเทศจะยอมรับการแสดงหลักฐานที่จัดพิมพ์จากคอมพิวเตอร์ โดยจะต้องมีหลักฐานอื่นประกอบด้วยเท่านั้น ดังนั้น หลักฐานจากการโอนเงินทางอิเล็กทรอนิกส์ผ่านเครื่องฝากถอนเงินอัตโนมัติ และการโอนเงินทางอิเล็กทรอนิกส์ ณ จุดขายจึงไม่เข้าข่ายที่กล่าวเพราะมิใช่ธุรกรรมทางการค้า

5.4 วิธีการพิสูจน์และการกำหนดภาระการพิสูจน์ก็เป็นเรื่องสำคัญ

ในการโอนเงินด้วยเครื่องฝากถอนเงินอัตโนมัติและการโอนเงินทางอิเล็กทรอนิกส์ ณ จุดขายมี ปัญหาในเรื่องการพิสูจน์มากที่สุด เช่น ทำอย่างไรจะพิสูจน์ได้ว่าการสั่งให้เครื่องอัตโนมัติจ่ายเงินนั้นเป็นการสั่งโดยเจ้าของบัญชีที่แท้จริง ถึงแม้จะใช้รหัสรับได้ถูกต้องก็ตาม และเมื่อมีการถอนเงินด้วยเครื่องฝากถอนเงินอัตโนมัติไปโดยเจ้าของบัญชีไม่รู้เห็น ทำอย่างไรจะพิสูจน์ความสุจริตได้ โดยมีใครควรจะรับภาระในการพิสูจน์

5.5 ปัญหาการกำหนดความรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากกรณีการทุจริตหรือการโอนเงิน ผิดพลาด หรือเมื่อการปฏิบัติงานของเครื่องอิเล็กทรอนิกส์ล้มเหลวจนไม่สามารถจะโอนเงินได้สำเร็จ ซึ่งได้มีตัวอย่างเกิดขึ้นแล้ว เช่น

5.5.1 ผู้ใช้บริการเครื่องฝากถอนเงินอัตโนมัติอ้างว่า เงินถูกตัดบัญชีไปโดยตนมิได้เป็นผู้เบิกถอนปัญหานี้พบอยู่เสมอรวมทั้งในประเทศไทยด้วย

5.5.2 ลูกค้าสั่งให้ธนาคารโอนตัดบัญชีเพื่อชำระค่าสาธารณูปโภคไว้ล่วงหน้าเป็นประจำทุกเดือน แต่ธนาคารละเลยหรือตัดบัญชีล่าช้า เป็นเหตุให้ลูกค้าได้รับความเสียหายในภายหลัง

5.5.3 ลูกค้าสั่งให้ธนาคารโอนเงินไปเข้าบัญชีของบุคคลอื่นต่างธนาคารหลังจากที่ธนาคารผู้สั่ง ได้ตัดบัญชีของผู้สั่งโอนแล้ว แต่พอดีระบบอิเล็กทรอนิกส์ของธนาคารผู้รับโอนเกิดขัดข้องก่อนที่ธนาคารดังกล่าวจะโอนเงินเข้าบัญชีให้ผู้รับเงินตามคำสั่งการโอนได้ เป็นผลให้ผู้รับโอนไม่ได้รับเงินโอนทันเวลา

จากกรณีปัญหาต่าง ๆ ตามที่กล่าวข้างต้นนั้น ทำให้สถาบันที่มีบริการโอนเงินและมี
หน่วยงานซึ่งให้บริการโอนเงินแก่สถาบันต่าง ๆ ต้องมีสัญญาหรือข้อตกลงหรือกฎระเบียบไว้เป็นหลักปฏิบัติในการโอนเงิน
ระหว่างกัน แต่สัญญาหรือข้อตกลงต่าง ๆ ระหว่างธนาคารกับลูกค้ามักจะเป็นเรื่องของการกำหนดหน้าที่เงื่อนไขต่าง ๆ ใน
การให้บริการมากกว่าการกำหนดความรับผิดชอบโดยยุติธรรม และมักเป็นไปเพื่อหลีกเลี่ยงการพิสูจน์หลักฐานต่าง ๆ
โดยเฉพาะอย่างยิ่งสัญญาให้บริการเครื่องฝากถอนเงินอัตโนมัติระหว่างธนาคารกับลูกค้า ซึ่งมักจะเปิดโอกาสให้ลูกค้า
ยกขึ้นมาเป็นข้ออ้างเรียกร้องความรับผิดชอบได้เลย

การจัดทำสัญญาสำหรับบริการโอนเงินทางอิเล็กทรอนิกส์จึงมีใช้ทางแก้ไขปัญหาย่าง
แท้จริง แต่เป็นเพียงหนทางหลบเลี่ยงของสถาบันการเงินต่าง ๆ เพื่อเปิดโอกาสมิให้ลูกค้าผู้ใช้บริการยกปัญหาขึ้นมาเรียก
ร้องได้ เช่น การสร้างเงื่อนไขบางประการไว้ในสัญญาการให้บริการ โดยที่ลูกค้าไม่สามารถจะพิสูจน์ได้ว่าตนได้ปฏิบัติตาม
เงื่อนไขดังกล่าวแล้วทุกประการ เป็นต้น ดังนั้น ในบางประเทศจึงพยายามแก้ไขด้วยการจัดร่างเป็นกฎหมายขึ้นเพื่อให้
กฎหมายในธุรกรรมดังกล่าวมีความยุติธรรมยิ่งขึ้น

6. แนวความคิดทางกฎหมายการโอนเงินทางอิเล็กทรอนิกส์ในต่างประเทศ

ในบางประเทศซึ่งใช้วิธีการโอนเงินทางอิเล็กทรอนิกส์อย่างแพร่หลาย ได้เห็นความจำเป็นในการสร้าง
กฎหมายเฉพาะขึ้นมารองรับธุรกรรม ตัวอย่างเช่น ในประเทศสหรัฐอเมริกาได้มีรัฐบัญญัติการโอนเงินทางอิเล็กทรอนิกส์
มาตั้งแต่ปี 2521 และในปัจจุบัน (พ.ศ. 2530) ประเทศอื่น ๆ เช่น อังกฤษ ออสเตรเลีย นิวซีแลนด์ ก็อยู่ในระหว่าง
การผลักดันให้มีกฎหมายในลักษณะดังกล่าวขึ้น

นอกจากนี้ ทางด้านคณะกรรมการการค้าระหว่างประเทศขององค์การสหประชาชาติ (UNCITRAL)
ก็ให้ความสำคัญต่อการจัดให้มีกฎหมายเพื่อการโอนเงินทางอิเล็กทรอนิกส์ด้วย และต้องการให้ประเทศต่าง ๆ มีกฎ-
เกณฑ์ในการโอนเงินทางอิเล็กทรอนิกส์ภายใต้มาตรฐานเดียวกัน (ดังที่ปรากฏอยู่ใน Draft Legal Guide on Electronic
Funds Transfer United Nations Commission on International Trade Law 1984-85)

แนวความคิดทางกฎหมายการโอนเงินทางอิเล็กทรอนิกส์ในต่างประเทศโดยสรุปประกอบด้วย

6.1 สหรัฐอเมริกา

มีกฎหมายเฉพาะสำหรับการโอนเงินทางอิเล็กทรอนิกส์มาตั้งแต่ปี 2521 เรียกว่า Electronic
Funds Transfer Act ซึ่ง Board of Governors of the Federal Reserve System ได้นำมาใช้เป็นกฎข้อบังคับ
ในการให้บริการโอนเงินทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์เพื่อให้ความคุ้มครองแก่ผู้ใช้บริการ โดยเรียกว่า Regulation
E สาระสำคัญของกฎหมายสรุปได้ดังนี้

6.1.1 กำหนดเงื่อนไขในการออกบัตรพลาสติกของธนาคารพาณิชย์ว่า บัตรเดบิต จะมีผลตาม
กฎหมายต่อเมื่อออกตามคำขอของลูกค้า

6.1.2 กรณีที่ลูกค้าทำบัตรเดบิตสูญหายหรือถูกขโมย แล้วพบว่าได้ถูกโอนเงินออกจากบัญชีไปโดยทุจริต ลูกค้าจะรับผิดชอบต่อความเสียหายในบัญชีของตนเพียงไม่เกิน 50 ดอลลาร์ สรอ. ถ้าลูกค้าได้แจ้งให้ธนาคารทราบภายใน 2 วันนับแต่วันที่ทราบว่าบัตรหาย และไม่เกิน 500 ดอลลาร์ สรอ. หากลูกค้าแจ้งให้ธนาคารทราบช้ากว่านั้น แต่ความรับผิดชอบดังกล่าวจะไม่จำกัดจำนวนหากลูกค้าละเลยการแจ้งให้ธนาคารทราบถึงการโอนเงินโดยมิชอบภายใน 60 วันนับแต่วันที่ธนาคารได้ส่งใบยืนยันยอดบัญชีเงินฝากให้แก่ลูกค้า

6.1.3 ธนาคารจะต้องแจ้งให้ลูกค้าทราบถึงเงื่อนไขต่าง ๆ ในการให้บริการโอนเงินทางอิเล็กทรอนิกส์ของธนาคารโดยละเอียด และทุกครั้งที่ธนาคารได้เปลี่ยนแปลงเงื่อนไขก็ต้องแจ้งให้ลูกค้าทราบด้วย

6.1.4 อุปกรณ์ทางอิเล็กทรอนิกส์ซึ่งลูกค้าสามารถใช้บริการด้วยตนเอง จะต้องสามารถออกใบรับเพื่อยืนยันการทำรายการของลูกค้า

6.1.5 ทุกครั้งที่มีการโอนเงินเข้าบัญชีลูกค้าโดยตรง หรือการโอนเงินเข้าบัญชีตามข้อตกลงการโอนล่วงหน้าไม่เป็นไปตามเวลา จะต้องแจ้งให้ลูกค้าทราบกฎเกณฑ์ในการทำงานเดียวกันนี้รวมถึงการโอนเงินออกจากบัญชีด้วย

6.1.6 ในกรณีที่ลูกค้าได้แจ้งถึงรายการโอนเงินผิดพลาดในบัญชีของตนให้ธนาคารทราบภายใน 60 วัน นับแต่วันที่ธนาคารได้จัดส่งใบยืนยันยอดเงินฝากไปให้ลูกค้าแล้ว ธนาคารจะต้องจัดให้มีการสอบสวนและสรุปผลภายในระยะเวลาที่กำหนด

จะเห็นได้ว่า สารสำคัญของ Regulation E นั้น เป็นการให้ความคุ้มครอง เฉพาะธุรกรรมการโอนเงินทางอิเล็กทรอนิกส์ระหว่างธนาคารกับลูกค้า โดยเน้นในเรื่องของสิทธิและหน้าที่ของทั้งลูกค้าผู้ให้บริการ และธนาคารพาณิชย์ผู้ให้บริการ อีกทั้งยังให้ความคุ้มครองความสูญเสียแก่ลูกค้าภายในขอบเขตหนึ่ง หากลูกค้าได้ปฏิบัติตามสิทธิและหน้าที่ซึ่งระบุไว้อย่างสมบูรณ์แล้ว

6.2 อังกฤษ

ประเทศอังกฤษมีกฎหมายซึ่งเกี่ยวข้องกับวิธีการทางอิเล็กทรอนิกส์อยู่บ้าง ได้แก่

6.2.1 Data Protection Act ให้ความคุ้มครองข้อมูลอันเกิดจากการประมวลผลด้วยระบบคอมพิวเตอร์

6.2.2 Bankers Books Evidence Act 1879 แก้ไขเพิ่มเติมในปี 1979 ยินยอมให้การเก็บรักษาข้อมูลของธนาคารพาณิชย์ด้วยวิธีการทางอิเล็กทรอนิกส์เป็นหลักฐานตามกฎหมายได้

6.2.3 Civil Evidence Act 1968 รับรองวิธีการเก็บรักษาข้อมูลด้วยคอมพิวเตอร์ให้เป็นหลักฐานตามกฎหมายได้เฉพาะบางธุรกรรม

6.2.4 Criminal Evidence Act 1965 เคยตัดสินในเรื่องการพิสูจน์หลักฐานโดยยอมให้เอกสาร ซึ่งจัดพิมพ์โดยคอมพิวเตอร์ใช้เป็นหลักฐานอ้างอิงทางศาลได้ในบางกรณี

อย่างไรก็ดี กฎหมายต่าง ๆ ดังที่กล่าวข้างต้น ก็มีใช้มีลักษณะเป็นกฎหมายเฉพาะที่ตรงประเด็นและครอบคลุมธุรกรรมทางการเงินทางอิเล็กทรอนิกส์โดยเฉพาะ โดยเพ่งเล็งถึงธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ในระบบ on-line เช่น การโอนผ่าน CHAPS, ATMs, EFT/POS และธนาคารในบ้านโดยรูปแบบของกฎหมายที่ต้องการมีแนวทางดังนี้

1) ในกรณีการโอนผ่าน CHAPS

- 1.1) จะต้องกำหนดความสมบูรณ์ของธุรกรรม หน้าที่ของฝ่ายต่าง ๆ ที่เกี่ยวข้องกับการโอนเงิน ขอบเขตความรับผิดชอบของแต่ละฝ่าย หากไม่สามารถจะโอนเงินให้สมบูรณ์ได้ตามคำสั่ง
- 1.2) จะต้องกำหนดเงื่อนไขและวิธีการในการแสดงหลักฐานต่อศาล เพื่อพิสูจน์ข้อขัดแย้งต่าง ๆ อันเกิดขึ้นจากธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ เช่น หลักฐานอื่นซึ่งใช้ประกอบเพื่อยืนยันความถูกต้องของเอกสารซึ่งพิมพ์โดยเครื่องคอมพิวเตอร์
- 1.3) จะต้องให้การรับรองสถานะของรหัสต่าง ๆ ที่ใช้ในระบบอิเล็กทรอนิกส์ ซึ่งเปรียบเสมือนการใช้ลายเซ็นในระบบงานเอกสาร

2) ในกรณีการให้บริการทางการเงินทางอิเล็กทรอนิกส์แก่ลูกค้าด้วยเครื่องอัตโนมัติ เช่น ATMs, EFT/POS และ Home banking ซึ่งลูกค้าสามารถใช้เครื่องอัตโนมัติด้วยตนเอง National Consumer Council ของอังกฤษให้ความสำคัญต่อการใช้บัตรเดบิตค่อนข้างมาก เพราะการใช้บัตรเดบิตมีปัญหาสำคัญประกอบด้วย

- (1) บัตรเดบิตซึ่งทำหน้าที่เช่นเดียวกับเช็ค แต่ไม่สามารถนำไปประยุกต์กับ Bill of Exchange Act ได้
- (2) บัตรเดบิตมิใช่คำสั่งให้จ่ายเงินด้วยลายลักษณ์อักษรที่ต้องพิสูจน์คำสั่งด้วยลายเซ็นผู้สั่งจ่าย การชำระเงินด้วยบัตรเดบิตจึงไม่สามารถสั่งระงับได้ และไม่สามารถจะโอนเปลี่ยนมือได้
- (3) มีความขัดแย้งทางกฎหมายเกี่ยวกับการใช้บัตรเดบิต กล่าวคือ เมื่อใช้บัตรเดบิตเบิกเงินเกินบัญชี บัตรเดบิตจะได้รับการคุ้มครองโดย Consumer Credit Act 1974 ซึ่งจำกัดวงเงินรับผิดชอบของเจ้าของบัญชีหากเกิดกรณีทุจริต แต่ถ้าใช้บัตรเดบิตในรูปของการถอนเงินปกติโดยมิได้ใช้วงเงินเบิกเกินบัญชี จะไม่มีกฎหมายใด ๆ คุ้มครองสถานะของบัตรเดบิต
- (4) ทั้ง ๆ ที่บัตรเดบิต บัตรเครดิต และเช็ค ต่างก็เป็นเครื่องมือในการชำระเงินทั้งสิ้น แต่หากเครื่องมือทั้งสามชนิดนี้ถูกขโมยไปใช้ในทางทุจริตแล้ว กลับได้รับความคุ้มครองต่างกัน กล่าวคือ
 - (4.1) การทุจริตโดยเช็คนั้น เจ้าของบัญชีไม่จำเป็นต้องรับความเสียหายเลย เพราะมักจะพิสูจน์การทุจริตได้ด้วยลายเซ็นผู้สั่งจ่ายและตัวเช็ค

- (4.2) การทุจริตจากบัตรเครดิตนั้น เจ้าของบัญชีจะรับผิดชอบในวงเงินไม่เกิน 50 ปอนด์ และหลังจากผู้ถือบัตรได้แจ้งให้ผู้ออกบัตรทราบถึงบัตรหายแล้ว ก็ไม่ต้องรับผิดชอบในความสูญเสียอีกต่อไป
- (4.3) แต่การทุจริตจากบัตรเดบิต ผู้ถือบัตรจะต้องรับผิดชอบกับความเสียหายสูงเท่ากับเงินที่มีอยู่ในบัญชี

* ด้วยสาเหตุดังกล่าว National Consumer Council จึงได้เสนอแนวทางการร่างกฎหมายเพื่อการโอนเงินทางอิเล็กทรอนิกส์ โดยให้ครอบคลุมในเรื่องต่าง ๆ ต่อไปนี้

- 2.1) กำหนดสถานะทางกฎหมายของบัตรเดบิต
- 2.2) กำหนดหลักเกณฑ์ในการออกบัตรเดบิต เช่น จะต้องมีการขอจากเจ้าของบัญชี เป็นต้น
- 2.3) กำหนดประเภทของเอกสารหลักฐานต่าง ๆ ที่ใช้ประกอบหรือเป็นเครื่องยืนยันธุรกรรมการโอนเงินทางอิเล็กทรอนิกส์
- 2.4) กำหนดขอบเขตความรับผิดชอบของฝ่ายต่าง ๆ ที่เกี่ยวข้องเมื่อเกิดความเสียหายในกรณีที่มีการใช้บัตรเดบิตเบิกถอนเงินโดยทุจริต
- 2.5) ในกรณีที่บัตรเดบิตถูกใช้ชำระค่าสินค้าหรือบริการผ่านเครื่องโอนเงินทางอิเล็กทรอนิกส์ ณ จุดขาย โดยร้านค้ายินยอมให้ผู้ถือบัตรใช้เงินเกินกว่าวงเงินที่มีอยู่ ให้กำหนดขอบเขตความรับผิดชอบของแต่ละฝ่ายเอาไว้ เช่นเดียวกับการกำหนดความรับผิดชอบเมื่อมีการใช้บัตรเครดิตตามมาตรา 75 ของ Consumer Credit Act 1974
- 2.6) กำหนดหลักเกณฑ์การปฏิบัติของธนาคารในการรักษาความลับของลูกค้า เมื่อมีการโอนเงินทางอิเล็กทรอนิกส์

6.3 ออสเตรเลียและนิวซีแลนด์

สองประเทศนี้ให้ความสำคัญต่อธุรกรรมการโอนเงินผ่านเครื่องฝากถอนเงินอัตโนมัติมากเป็นพิเศษ

ในประเทศนิวซีแลนด์ บางธนาคารได้กำหนดความรับผิดชอบของเจ้าของบัญชีไว้ในสัญญาการใช้บริการในกรณีที่มีการนำบัตรไปใช้โดยทุจริต ขณะนี้ Ministry of Consumer Affair ก็กำลังผลักดันให้ธนาคารอื่น ๆ ปฏิบัติตาม และหากไม่ได้ผลก็จะประกาศเป็นกฎหมาย (ณ ปี 2537)

ส่วนในประเทศออสเตรเลียอยู่ระหว่างการจัดวางกฎเกณฑ์เพื่อคุ้มครองผลประโยชน์ของผู้บริการด้วยเครื่องฝากถอนเงินอัตโนมัติ ซึ่งมีลักษณะคล้ายคลึงกับของประเทศนิวซีแลนด์

จะเห็นได้ว่า แนวทางด้านกฎหมายที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ในต่างประเทศนั้นให้ความสำคัญในเรื่องการคุ้มครองผลประโยชน์ของผู้ใช้บริการเป็นหลัก ได้มีการพยายามผลักดันให้วิธีการโอนเงินทางอิเล็กทรอนิกส์เป็นที่ยอมรับโดยนัยแห่งกฎหมาย โดยเฉพาะอย่างยิ่งในเรื่องของหลักฐานต่าง ๆ อันเกิดจากการปฏิบัติงานด้วยวิธีการทางอิเล็กทรอนิกส์

6.4 ทางด้าน United Nations Commission on International Trade Law (UNCITRAL) ก็ได้ชี้ให้เห็นประเด็นปัญหาต่าง ๆ ที่เกิดขึ้นจากการเปลี่ยนแปลงวิธีการโอนเงินจากระบบเอกสารมาใช้วิธีการทางอิเล็กทรอนิกส์ และได้ขอความเห็นไปยังประเทศสมาชิกตั้งแต่เมื่อปี 2528 เพื่อวางแนวทางในการจัดร่างกฎหมาย โดยปกติได้ส่งความเห็นไปด้วยดังปรากฏในภาคผนวกเล่มนี้แล้ว UNCITRAL เห็นว่ากฎหมายดังกล่าวควรจะครอบคลุมในเรื่องต่าง ๆ ดังนี้

6.4.1 สิทธิ หน้าที่ ของทุกฝ่ายที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ เช่น สิทธิและหน้าที่ของผู้โอนเงิน ผู้รับโอนเงิน ธนาคารผู้โอน และธนาคารผู้รับโอน

6.4.2 กำหนดเงื่อนไขของการโอน เช่น ความสมบูรณ์ของการโอนเกิดขึ้นเมื่อไร ผลแห่งความสมบูรณ์ในการโอน การยกเลิกหรือล้างรายการโอน เงื่อนไขเวลาของการโอน

6.4.3 รับรองผลทางกฎหมายในวิธีการบันทึก การแสดงหลักฐาน และวิธีการพิสูจน์หลักฐานอันเกิดจากวิธีการปฏิบัติงานด้วยเครื่องอิเล็กทรอนิกส์ เช่น การรับรองสถานะของเอกสารซึ่งแสดงข้อมูลต่าง ๆ ซึ่งบันทึกไว้ด้วยเครื่องคอมพิวเตอร์ การใช้รหัสลับในการส่งโอนเงิน การใช้บัตรเดบิตเป็นเครื่องมือในการชำระเงิน

6.4.4 กำหนดความรับผิดชอบของฝ่ายต่าง ๆ ที่เกี่ยวข้องในการโอนเงินในกรณีที่การโอนเงินล่าช้าหรือมีการทุจริต จนเป็นผลให้ผู้โอนหรือผู้รับโอนได้รับความเสียหาย

6.4.5 ในกรณีบริการโอนเงินระหว่างธนาคารกับลูกค้า จะต้องกำหนดหลักเกณฑ์การทำสัญญาการให้บริการระหว่างธนาคารกับลูกค้า การจัดส่งใบยืนยันยอด และการแจ้งถึงการปฏิบัติตามคำสั่งโอนเงินล่วงหน้า ไม่ว่าจะเป็นการโอนเงินเข้าบัญชีหรือโอนออกจากบัญชี

7. ลักษณะของแนวทางด้านกฎหมายที่จำเป็น

เพื่อให้การโอนเงินทางอิเล็กทรอนิกส์ยืนอยู่บนพื้นฐานแห่งความยุติธรรมตามจารีตประเพณี และมีหลักปฏิบัติในรูปของกฎเกณฑ์ที่แน่นอน กฎหมายเรื่องการโอนเงินทางอิเล็กทรอนิกส์จึงควรมีแนวทางดังนี้

7.1 ให้การรับรองว่าผลแห่งธุรกรรมในการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์เป็นธุรกรรมตามกฎหมาย พร้อมทั้งให้คำจำกัดความในเรื่องความสมบูรณ์ในการโอนเงินทางอิเล็กทรอนิกส์ และเงื่อนไขต่าง ๆ เมื่อจะเพิกถอนหรือยกเลิกการโอนเงิน

7.2 กำหนดเงื่อนไขในการแสดงหลักฐานต่าง ๆ อันเกิดจากการบันทึกและเก็บรักษาข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ พร้อมทั้งให้คำจำกัดความที่ชัดเจนในสถานภาพของบัตรเดบิตและบัตรเครดิต ซึ่งเป็นเครื่องมือทางการเงินตามวิธีการโอนเงินทางอิเล็กทรอนิกส์

7.3 กำหนดสิทธิ หน้าที่ ภาระ และความรับผิดชอบของฝ่ายต่าง ๆ ที่เกี่ยวข้องกันกับธุรกรรมการโอนเงินทางอิเล็กทรอนิกส์

8. ที่มาและข้อมูลที่น่าสนใจบางประการของพระราชบัญญัติการโอนเงินทางอิเล็กทรอนิกส์ (ELECTRONIC FUND TRANSFER ACT)

8.1 คำวินิจฉัยและวัตถุประสงค์

15 USC 1693 (a)

สภาคองเกรสได้เล็งเห็นประโยชน์ของผู้ใช้บริการโอนเงินทางอิเล็กทรอนิกส์ ทั้งนี้เนื่องจากระบบอิเล็กทรอนิกส์มีลักษณะเฉพาะซึ่งกฎหมายที่ใช้อยู่ในปัจจุบันมิได้ระบุการคุ้มครองสิทธิ ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน ดังนั้น จึงควรกำหนดสิทธิความรับผิดชอบของผู้ให้บริการ สถาบันการเงินที่เกี่ยวข้องในการโอนเงินทางอิเล็กทรอนิกส์ไว้อย่างชัดเจน

วัตถุประสงค์ของพระราชบัญญัตินี้เพื่อจัดหากฎเกณฑ์กำหนดสิทธิ ภาระความรับผิดชอบของผู้เกี่ยวข้องในระบบอิเล็กทรอนิกส์ ดังนั้น ในหลักการพื้นฐานจึงต้องระบุสิทธิหน้าที่ของแต่ละบุคคลที่เกี่ยวข้อง

8.2 คำจำกัดความ

(1) คำว่า “บัตรพลาสติกหรือเครื่องมืออื่นใด” หมายถึง บัตร รหัส หรืออุปกรณ์อื่น ๆ สำหรับเข้าถึงบัญชีของลูกค้าเพื่อวัตถุประสงค์ในการโอนเงิน ซึ่งจะทำให้เมื่อบุคคลนั้นได้ยื่นคำขอเป็นผู้ถือบัตร และได้รับบัตรนั้นแล้วหรือได้เซ็นชื่อรับไปแล้วหรือได้เคยใช้ไปแล้วหรือได้ให้บุคคลอื่นใช้บัตรเพื่อใช้ในการโอนเงินระหว่างบัญชีหรือเพื่อให้ได้รับมาซึ่งเงิน ทรัพย์สิน ค่าแรง หรือบริการอื่น ๆ

(2) คำว่า “บัญชีเงินฝาก” หมายถึง บัญชีเงินฝากกระแสรายวัน บัญชีเงินฝากออมทรัพย์ หรือบัญชีเงินฝากอื่น ๆ ซึ่งได้กล่าวไว้ในกฎข้อบังคับของคณะกรรมการ

(3) คำว่า “คณะกรรมการ” หมายถึง คณะกรรมการที่ประกอบด้วย ผู้ว่าการของ Federal Reserve System

(4) คำว่า “วันทำการ” หมายถึง วันใดวันหนึ่งที่สถาบันการเงินเปิดทำการเพื่อทำธุรกิจตามปกติ

(5) คำว่า “ลูกค้า” หมายถึง บุคคลธรรมดาทั่ว ๆ ไป

(6) คำว่า “การโอนเงินทางอิเล็กทรอนิกส์” หมายถึง รายการโอนเงินอื่นใดที่ไม่ได้ใช้เช็ค ดราฟต์ หรือเอกสารหลักฐานอื่น ๆ ที่คล้ายคลึงกัน เป็นการทำการรายการโดยผ่านเครื่องเทอร์มินอล อุปกรณ์สื่อสารหรือคอมพิวเตอร์ หรือเทปแม่เหล็ก เพื่อยืนยันให้สถาบันการเงินทำการโอนเงินเพื่อตัดบัญชี หรือรายการโอนเพื่อเข้าบัญชี คำนี้มีได้จำกัดเพียงการโอนเงิน ณ จุดขาย การโอนเงินโดยเครื่องฝากถอนเงินอัตโนมัติ การฝากเงินโดยตรงหรือการถอนเงินและรายการโอนเงินทางโทรศัพท์ แต่คำนี้ไม่รวมถึงกิจกรรมต่อไปนี้

(A) การรับรองเช็ค หรือการขออนุมัติบริการต่าง ๆ ซึ่งไม่ส่งผลให้มีการตัดบัญชีหรือโอนเข้าบัญชีของลูกค้าโดยตรง

- (B) รายการโอนเงินใด ๆ ของสถาบันการเงินที่นอกเหนือจากการโอนเงินในนามของเจ้าของบัญชี โดยผ่านสำนักหักบัญชี ไม่ว่าจะเป็นการโอนเงินจากบัญชีเงินฝากที่ Federal Reserve หรือสถาบันการเงินอื่นใดก็ตาม และการโอนเงินอื่นใดที่ได้กระทำในนามของเจ้าของบัญชี
- (C) รายการใด ๆ ที่วัตถุประสงค์เบื้องต้นเป็นการซื้อหรือขายหลักทรัพย์หรือสินค้าโภคภัณฑ์ โดยผ่านนายหน้าที่จดทะเบียนและปฏิบัติตามกฎระเบียบข้อบังคับของคณะกรรมการตลาดหลักทรัพย์
- (D) รายการโอนเงินโดยอัตโนมัติจากบัญชีเงินฝากออมทรัพย์ไปยังบัญชีกระแสรายวันตามข้อตกลงระหว่างลูกค้ากับสถาบันการเงิน โดยมีวัตถุประสงค์เพื่อลดยอดวงเงินเบิกเกินบัญชี หรือเพื่อเป็นการดำรงเงินฝากขั้นต่ำในบัญชีกระแสรายวันของลูกค้า หรือ
- (E) รายการโอนเงินใด ๆ ซึ่งเริ่มจากการสนทนาทางโทรศัพท์ระหว่างลูกค้ากับเจ้าหน้าที่ของสถาบันการเงิน ซึ่งไม่ได้มีการตกลงไว้ล่วงหน้าและมีเป็นระยะ ๆ หรือการโอนเงินนั้นมิได้เป็นความมุ่งหมายของข้อกำหนดที่ออกโดยคณะกรรมการ

(7) คำว่า “อิเล็กทรอนิกส์เทอร์มินัล” หมายถึง อุปกรณ์ทางด้านอิเล็กทรอนิกส์นอกเหนือจากโทรศัพท์ที่กระทำโดยลูกค้า ซึ่งคำนี้ไม่ได้จำกัดเฉพาะเครื่องโอนเงิน ณ จุดขาย และเครื่องฝากถอนเงินอัตโนมัติเท่านั้น

(8) คำว่า “สถาบันการเงิน” หมายถึง ธนาคารประเภท State Bank หรือ National Bank หรือ State Saving and Loan Association หรือ Federal Saving and Loan Association, Mutual Savings Bank, State Credit Union หรือ Federal Credit Union หรือบุคคลอื่นใดที่ดูแลบัญชีของลูกค้าไม่ว่าโดยตรงหรือโดยอ้อม

(9) คำว่า “ข้อตกลงล่วงหน้าในการโอนเงินทางอิเล็กทรอนิกส์” หมายถึง การโอนเงินทางอิเล็กทรอนิกส์ที่มีการอนุมัติให้มีการโอนไว้ล่วงหน้า

(10) คำว่า “รัฐ” หมายถึง รัฐใด ๆ หรือสถานที่ใด ๆ ที่เป็นอาณาเขตของประเทศสหรัฐอเมริกา, District of Columbia และเปอร์โตริโก

(11) คำว่า “การโอนเงินทางอิเล็กทรอนิกส์โดยมิชอบด้วยกฎหมาย” หมายถึง การโอนเงินทางอิเล็กทรอนิกส์จากบัญชีลูกค้าโดยบุคคลอื่นที่มีใช้ตัวลูกค้า ซึ่งมีได้มีอำนาจที่แท้จริงและโดยที่ลูกค้ามิได้รับผลประโยชน์แต่มิได้รวมถึงการโอนเงินทางอิเล็กทรอนิกส์ซึ่ง

- (A) เป็นการกระทำโดยบุคคลอื่นที่ลูกค้าได้จัดเตรียมบัตร รหัส และวิธีการเข้าถึงบัญชีลูกค้า เว้นแต่ลูกค้าจะได้แจ้งไปยังสถาบันการเงินว่าไม่ได้อนุมัติให้มีการโอนเงินโดยบุคคลผู้นั้นอีก
- (B) ลูกค้ามีเจตนาที่จะกระทำการทุจริตหรือมีบุคคลอื่นใดที่ทำงานร่วมกันกับลูกค้าหรือ
- (C) จากการที่สถาบันการเงินทำการผิดพลาด

8.3 ระเบียบข้อบังคับ

15 USC 1693 b

(a) คณะกรรมการได้กำหนดระเบียบข้อบังคับเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวโดยคณะกรรมการจะต้องปฏิบัติ ดังนี้

- (1) ปรีกษากับตัวแทนอื่น ๆ ที่อ้างอิงถึงใน 15 USC 1693 d และนำมาพิจารณาเพื่ออนุญาตให้มีการพัฒนาการบริการด้านการธนาคารอิเล็กทรอนิกส์และเทคโนโลยีอื่น ๆ ที่เกี่ยวข้อง
- (2) จัดเตรียมบทวิเคราะห์ผลกระทบทางเศรษฐกิจ ซึ่งพิจารณาถึงค่าใช้จ่ายและผลตอบแทนต่อสถาบันการเงิน ลูกค้า และบุคคลอื่นที่ใช้บริการการโอนเงินทางอิเล็กทรอนิกส์ ทั้งนี้ ต้องครอบคลุมถึงเอกสารต่าง ๆ ที่เพิ่มขึ้น รายงานการบันทึกการและเอกสารอื่นที่ใช้มากขึ้น ผลกระทบของการแข่งขันด้านบริการธนาคารอิเล็กทรอนิกส์ ทั้งในสถาบันการเงินขนาดใหญ่และขนาดเล็ก และความสามารถที่จะให้บริการแก่ลูกค้าทุกระดับ โดยเฉพาะผู้ที่มียาได้ต่ำ
- (3) นอกจากนี้ คณะกรรมการจะต้องแสดงให้เห็นว่า ได้ให้ความสำคัญในการที่จะปกป้องผลประโยชน์ของลูกค้ามากกว่าที่จะพิจารณาทางด้านต้นทุนของสถาบันการเงินและลูกค้า

(b) คณะกรรมการจะต้องให้แนวทางของสำนวนแก่สถาบันการเงินได้ใช้เป็นทางเลือกในการที่จะเผยแพร่ข้อมูลตาม 15 USC 1693 c และเป็นการช่วยให้ลูกค้าเข้าใจถึงสิทธิและความรับผิดชอบร่วมกันของผู้ที่เกี่ยวข้องในการโอนเงินทางอิเล็กทรอนิกส์ โดยใช้ภาษาที่เข้าใจง่ายและตามที่ปรากฏใน section 553 ของ title 5 United States Codes แนวร่างของสำนวนนี้จะมีการปรับปรุงหลังจากลงใน Federal Register และผ่านการเห็นชอบจากสาธารณชน ตามมาตรา 15 USC 1693 c (a) (3) และ (4) คณะกรรมการจะต้องพิจารณาการให้บริการโอนเงินทางอิเล็กทรอนิกส์ และการคิดค่าบริการที่แตกต่างกันด้วย และจะมีการกำหนดแนวทางของสำนวนเพื่อการเปิดเผยเงื่อนไขของบัญชีที่ต่างกัน

(c) จากระเบียบข้อบังคับที่กำหนดไว้นี้ อาจกำหนดประเภทบริการ (classification) คำจำกัดความ การจัดให้มีบทเฉพาะกาล และข้อยกเว้นสำหรับการโอนเงินทางอิเล็กทรอนิกส์แบบใดแบบหนึ่ง เพื่อให้บรรลุวัตถุประสงค์ของเรื่องนี้ คณะกรรมการจะต้องพิจารณาถึงฐานะของสถาบันการเงินขนาดเล็ก โดยอาจจะเปลี่ยนแปลงบทเฉพาะกาลบางบท เพื่อแบ่งเบาภาระของสถาบันการเงินขนาดเล็กและไม่ขัดต่อเป้าหมายของเรื่องนี้

(d) ในกรณีที่การโอนสินทรัพย์นั้นกระทำโดยบุคคลอื่นซึ่งมิใช่สถาบันการเงินที่ลูกค้ามีบัญชีอยู่คณะกรรมการจะต้องมั่นใจว่าหลักการต่าง ๆ เช่น การเปิดเผย การป้องกัน ความรับผิดชอบ และการแก้ไข สามารถที่จะประยุกต์กับบุคคลและบริการเหล่านั้นได้

8.4 ความหมายและเงื่อนไขของการโอน

15 USC 1693 c

(a) ความหมายและเงื่อนไขของการโอนเงินที่เกี่ยวข้องกับบัญชีลูกค้า จะต้องเปิดเผยให้ลูกค้าทราบ ในเวลาที่ลูกค้ามาทำสัญญาการใช้บริการโอนเงินทางอิเล็กทรอนิกส์ เพื่อให้สอดคล้องกับระเบียบข้อบังคับของคณะกรรมการ ซึ่งต้องอยู่ในภาษาที่เข้าใจง่าย และควรจะต้องปรากฏข้อความดังต่อไปนี้

- (1) ในกรณีเจ้าของบัญชีทำบัตรสูญหาย หรือบัตรถูกขโมย อันจะก่อให้เกิดการโอนเงินโดยมิชอบด้วยกฎหมาย หรือมีการใช้บัตร รหัส และวิธีการเข้าถึงระบบโดยปราศจากสิทธิโดยชอบ เจ้าของบัญชีจะต้องแจ้งไปที่สถาบันการเงินผู้ออกบัตรทันที
- (2) หมายเลขโทรศัพท์หรือสถานที่ที่เจ้าของบัญชีสามารถติดต่อและแจ้งความตามข้อ (1)
- (3) ประเภทของการโอนเงิน ซึ่งรวมถึงเงื่อนไขของการโอน เช่นจำนวนครั้งหรือจำนวนเงินสูงสุดในการโอน ยกเว้นรายละเอียดของเงื่อนไขบางประการซึ่งไม่จำเป็นต้องเปิดเผย ถ้าเงื่อนไขเหล่านั้นเป็นความลับที่คณะกรรมการพิจารณาเห็นว่าเป็นสิ่งจำเป็นเพื่อรักษาไว้ซึ่งความปลอดภัยของระบบการโอนเงินทางอิเล็กทรอนิกส์
- (4) การคิดค่าบริการการโอนเงิน และค่าบริการเพื่อสิทธิในการโอน
- (5) สิทธิของลูกค้าในการระงับการจ่าย สำหรับการโอนเงินที่มีข้อตกลงการโอนไว้ล่วงหน้า และระเบียบปฏิบัติในการสั่งระงับการจ่ายเงิน
- (6) สิทธิของลูกค้าในการรับเอกสารที่เกี่ยวข้องกับการโอนเงินตาม 15 USC 1693 d
- (7) สถาบันการเงินจะต้องส่งคำชี้แจงถึงสิทธิของลูกค้าในการสั่งให้ธนาคารแก้ไขข้อผิดพลาด ซึ่งอยู่ในรูปแบบที่กำหนดโดยคณะกรรมการตาม 15 USC 1693 f ให้ลูกค้าอย่างน้อยที่สุดปีละ 1 ครั้ง
- (8) ภาระของสถาบันการเงินต่อลูกค้า ตาม 15 USC 1693 h และ
- (9) รายละเอียดถึงสิทธิของสถาบันการเงินที่จะเปิดเผยข้อมูลซึ่งเกี่ยวข้องกับบัญชีลูกค้าต่อบุคคลที่สามภายใต้สถานการณ์บางประเภท

(b) ในกรณีที่สถาบันการเงินเปลี่ยนแปลงข้อกำหนดและเงื่อนไขในบัญชีของลูกค้า ซึ่งมีผลทำให้ค่าใช้จ่ายและภาระหนี้สินเพิ่มขึ้น หรือลดขั้นตอนการทำรายการของลูกค้า ต้องมีการแจ้งเป็นลายลักษณ์อักษรให้ลูกค้าทราบล่วงหน้า 21 วันก่อนที่จะมีผลบังคับใช้ ซึ่งจะต้องแจ้งให้ลูกค้าทราบตาม subsection (a)

ในกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงอย่างรีบด่วน เพื่อความปลอดภัยในระบบการโอนเงินหรือบัญชีลูกค้า สถาบันการเงินมีสิทธิที่จะดำเนินการได้ก่อนที่จะมีการแจ้งให้ลูกค้าทราบ แต่คณะกรรมการจะต้องแจ้งให้ลูกค้าทราบในภายหลังตาม subsection (a) (3) ถ้าการเปลี่ยนแปลงนั้นเป็นการเปลี่ยนแปลงถาวร

(c) สำหรับบัญชีของลูกค้าที่ใช้บริการการโอนเงินทางอิเล็กทรอนิกส์ก่อนวันที่กฎหมายนี้จะมีผลบังคับใช้ ข้อมูลที่ต้องเปิดเผยให้ลูกค้าทราบตาม subsection (a) จะต้องเปิดเผยไม่ช้ากว่า

- (1) ใบแจ้งยอดเงินฝากฉบับแรกที่สถาบันการเงินส่งให้ลูกค้า ตาม 15 USC 1693 d (c) หลังจากวันที่เรื่องนี้จะมีผลบังคับใช้ หรือ
- (2) 30 วันหลังจากที่เรื่องนี้จะมีผลบังคับใช้

8.5 เอกสารการโอน และใบแจ้งยอดบัญชีเงินฝาก

15 USC 1693 d

(a) สำหรับการโอนเงินที่ลูกค้าทำผ่านเครื่องเทอร์มินอลด้วยตนเอง สถาบันการเงินของลูกค้าจะต้องจัดให้มีเอกสารหลักฐานการโอนเงินทุกครั้งที่มีการโอน โดยหลักฐานดังกล่าวต้องมีรายละเอียด ดังนี้

- (1) วันที่ทำการโอนและจำนวนเงิน
- (2) ประเภทของการโอน
- (3) แสดงรายละเอียดในการโอนเงินเข้าหรือออกจากบัญชีของลูกค้า
- (4) แสดงรายละเอียดในการโอนเงินเข้าหรือออกไปยังบัญชีของบุคคลที่สาม
- (5) สถานที่ตั้งเครื่องเทอร์มินอล

(b) สำหรับบัญชีลูกค้าซึ่งมีการตกลงล่วงหน้าให้มีการโอนเงินเข้าบัญชี อย่างน้อย 1 ครั้ง ภายในระยะเวลา 60 วัน โดยบุคคลคนเดียวกัน สถาบันการเงินจะต้องแจ้งให้ลูกค้าทราบทันทีเมื่อได้มีการโอนเข้าบัญชีตามข้อตกลง หรือแจ้งให้ลูกค้าทราบหากมิได้มีการโอนเข้าบัญชีตามกำหนดอย่างใดอย่างหนึ่งก็ได้ โดยจะต้องบอกให้ทราบล่วงหน้าตาม 15 USC 1693 c เว้นเสียแต่ว่าจะมีข้อตกลงให้ผู้จ่ายเงินเป็นผู้แจ้งให้ลูกค้าทราบเมื่อมีการโอนตามข้อตกลงแล้ว

(c) สถาบันการเงินจะต้องจัดส่งใบแจ้งยอดเงินฝากให้ลูกค้าที่ใช้บริการการโอนเงินทางอิเล็กทรอนิกส์ เว้นแต่ที่กล่าวไว้ในข้อ (d) และ (e) ซึ่งใบแจ้งยอดเงินฝากนี้ ควรส่งให้อย่างน้อยเดือนละครั้งหรือในช่วงระยะเวลาหนึ่งซึ่งมีการใช้บริการโอนเงินนี้ โดยรายละเอียดในใบแจ้งยอดเงินฝากจะต้องครอบคลุมถึงข้อมูลดังต่อไปนี้

- (1) จะต้องมียละเอียดเกี่ยวกับการโอนเงินทุกครั้ง ตามที่ระบุไว้ใน subsection (a)
- (2) ค่าธรรมเนียมหรือค่าบริการที่สถาบันการเงินเรียกเก็บจากลูกค้า
- (3) ยอดเงินคงเหลือในบัญชีลูกค้าที่ปรากฏในใบแจ้งยอดเงินฝาก ทั้งที่เป็นยอดยกมาและยอดยกไป
- (4) ที่อยู่และหมายเลขโทรศัพท์ที่ลูกค้าสามารถติดต่อได้สะดวก หากต้องการขอใบแจ้งยอดเงินฝาก หรือแจ้งข้อผิดพลาดที่พบในใบแจ้งยอดเงินฝาก โดยที่อยู่และหมายเลขโทรศัพท์ควรแสดงให้เห็นเด่นชัด

(d) สำหรับบัญชีเงินฝากประเภทใช้สมุดคู่ฝาก ที่มีได้ใช้บริการโอนเงินทางอิเล็กทรอนิกส์อื่นใดนอกจากการโอนเงินเข้าบัญชีตามข้อตกลงล่วงหน้า สถาบันการเงินจะปรับปรุงรายการในสมุดคู่ฝากให้ลูกค้าให้เป็นปัจจุบัน โดยลงวันที่และจำนวนเงินที่มีการโอนให้ต่อจากการปรับปรุงรายการให้เป็นปัจจุบันในสมุดคู่ฝากครั้งสุดท้าย

(e) สำหรับบัญชีประเภทอื่น ๆ ที่มีได้ใช้สมุดคู่ฝากและมีได้ใช้บริการโอนเงินทางอิเล็กทรอนิกส์ นอกจากการโอนเงินเข้าบัญชีตามข้อตกลงล่วงหน้า สถาบันการเงินจะต้องจัดทำใบแจ้งยอดเงินฝากรายไตรมาสให้ตาม subsection (c)

(f) ไม่ว่ากรณีใด ๆ ก็ตาม ธุรกิจการโอนเงินที่ปรากฏในเอกสารหลักฐานต่าง ๆ ที่ธนาคารได้จัดส่งให้เจ้าของบัญชานั้น จะถือเป็นหลักฐานขั้นต้นตามกฎหมายที่สามารถใช้พิสูจน์ธุรกรรมการโอนเงินได้

การโอนเงินที่มีการตกลงไว้ล่วงหน้า

15 USC 1693 e

(a) การโอนเงินจากบัญชีลูกค้าในกรณีที่มีข้อตกลงการโอนไว้ล่วงหน้า ต้องจัดทำเป็นลายลักษณ์อักษร และสถาบันการเงินจะต้องจัดส่งสำเนาข้อตกลงให้ลูกค้าด้วย หากลูกค้าจะให้สถาบันการเงินระงับการจ่ายเงินตามข้อตกลงล่วงหน้า ก็อาจจะแจ้งต่อสถาบันการเงินนั้นด้วยวาจาหรือเป็นลายลักษณ์อักษรล่วงหน้า 3 วันทำการก่อนที่จะมีการโอนเงิน และถ้าเป็นการแจ้งด้วยวาจา จะต้องทำหนังสือยืนยันส่งไปยังสถาบันการเงินภายใน 14 วัน

(b) ในกรณีการโอนเงินจากบัญชีลูกค้าที่มีการตกลงไว้ล่วงหน้า ไปยังบุคคลคนเดียวกันด้วยจำนวนเงินที่แตกต่างกัน ก่อนที่จะทำการโอนแต่ละครั้ง สถาบันการเงินหรือผู้รับเงินจะต้องมีการแจ้งจำนวนเงินและวันที่ที่จะโอนส่งให้ลูกค้า

8.6 การแก้ไขข้อผิดพลาด

15 USC 1693 f

(a) ภายใน 60 วันหลังจากที่สถาบันการเงินได้ส่งเอกสารให้ลูกค้าตาม 15 USC 1693 d (a), (c) หรือ (d) หรือการแจ้งตาม 15 USC 1693 d (b) หากสถาบันการเงินได้รับแจ้งจากลูกค้าด้วยวาจาหรือลายลักษณ์อักษร โดยการแจ้งนั้น

- (1) สถาบันการเงินสามารถพิสูจน์ชื่อบัญชีและเลขที่บัญชีของลูกค้าได้
- (2) ลูกค้าชี้แจงว่าเอกสารที่ได้รับจากสถาบันการเงินตาม 15 USC 1693 d (b) มีรายการผิดพลาด และสามารถระบุจำนวนเงินที่ผิดพลาดนั้น
- (3) ลูกค้าได้แสดงหลักฐานที่เชื่อว่ามีข้อผิดพลาดเกิดขึ้น สถาบันการเงินจะต้องทำการตรวจสอบข้อผิดพลาดนั้น แล้วแจ้งให้ลูกค้าทราบภายใน 10 วันทำการ โดยลูกค้าต้องทำหนังสือชี้แจงกลับให้สถาบันการเงินทราบภายใน 10 วันหลังจากที่ได้รับแจ้งจากสถาบันการเงินแล้ว หากสถาบันการเงินไม่ได้รับหนังสือยืนยัน

จากลูกค้าภายใน 10 วัน ก็ไม่จำเป็นต้องนำเงินเข้าบัญชี (recredit) ลูกค้าอีกตาม subsection (c) และไม่ต้องรับผิดชอบตาม subsection (e)

(b) ถ้าสถาบันการเงินพิจารณาเห็นว่ามีข้อผิดพลาดเกิดขึ้น จะทำการแก้ไขทันทีภายใน 1 วันทำการหลังจากที่พบ รวมทั้งคำนวณดอกเบี้ยเข้าบัญชีตาม 15 USC 1693 g

(c) ถ้าสถาบันการเงินรับแจ้งข้อผิดพลาดภายในเวลาที่กำหนดใน subsection (a) คือ ภายใน 10 วันทำการหลังจากที่รับข้อสังเกต สถาบันการเงินจะต้องนำเงินเข้าบัญชี (recredit) ให้ลูกค้าใหม่ตามจำนวนที่ผิดพลาด รวมถึงดอกเบี้ยสำหรับบัญชีที่มีดอกเบี้ยตาม 15 USC 1693 g ที่เกิดขึ้นในระหว่างที่กำลังตรวจสอบรายการผิดพลาดอยู่นั้น ผลการตรวจสอบจะต้องสรุปภายใน 45 วันหลังจากที่ได้รับการแจ้งข้อผิดพลาด และในระหว่างที่คอยผลการตรวจสอบนี้ ลูกค้าจะได้รับประโยชน์ทุกประการจากจำนวนเงินที่โอนเข้าบัญชีให้ใหม่

(d) หลังจากการตรวจสอบตามข้อ (a) หรือ (c) สถาบันการเงินพบว่ามิได้มีข้อผิดพลาดเกิดขึ้น จะต้องส่งคำชี้แจงให้ลูกค้าทราบภายใน 3 วันทำการหลังจากที่มีการสรุปผลการตรวจสอบ พร้อมกับเอกสารต่าง ๆ ที่ใช้ในการอ้างอิง และให้ข้อสังเกต พร้อมคำอธิบายประกอบ

(e) การกระทำใด ๆ ภายใต้ 15 USC 1693 m หากศาลพบว่า

(1) สถาบันการเงินไม่ได้นำเงินเข้าบัญชีลูกค้าภายใน 10 วันตามที่ระบุไว้ใน subsection

(c) และสถาบันการเงิน

(A) ไม่ได้ทำการตรวจสอบเพื่อหาข้อเท็จจริงในข้อผิดพลาดตามที่ได้รับแจ้งหรือ

(B) ไม่มีเหตุผลเพียงพอที่จะเชื่อได้ว่ารายการในบัญชีของลูกค้าไม่มีข้อผิดพลาดแล้ว

(2) สถาบันการเงินได้ทำการสรุปผลว่า ไม่มีรายการผิดพลาดเกิดกับบัญชีลูกค้าโดยการสรุปผลดังกล่าวมิได้ใช้หลักฐานที่มีอยู่ในขณะนั้นอย่างเพียงพอ ดังนั้นถ้าพิจารณาตาม 15 USC 1693 m (a) (i) ลูกค้ามีสิทธิที่จะเรียกร้องค่าเสียหายที่เกิดขึ้นเพิ่มเป็น 3 เท่า

(f) ข้อผิดพลาดตามมาตรานี้ ประกอบด้วย

(1) การถอนเงินทางอิเล็กทรอนิกส์โดยมิชอบด้วยกฎหมาย

(2) การโอนเงินเข้าบัญชีลูกค้าหรือโอนออกจากบัญชีลูกค้าผิดพลาด

(3) การที่สถาบันการเงินไม่ส่งใบยืนยันยอดให้ลูกค้า ในกรณีที่มีการโอนเงินซึ่งเกี่ยวข้องกับบัญชีลูกค้า

(4) การที่สถาบันการเงินคำนวณผิดพลาด

(5) ลูกค้าได้รับหลักฐานการโอนเงินที่ไม่ถูกต้องจากเครื่องเทอร์มินอล

(6) การที่ลูกค้าขอข้อมูลหรือคำชี้แจงเพิ่มเติม ในส่วนที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ หรือเอกสารอื่นตามที่ระบุไว้ในกฎหมายนี้

(7) ข้อผิดพลาดอื่นใดที่กำหนดโดยคณะกรรมการ

8.7 ความรับผิดชอบของลูกค้าในกรณีที่มีการโอนเงินโดยมิชอบด้วยกฎหมาย

15 USC 1693 g

(a) ลูกค้าจะต้องรับผิดชอบต่อการโอนเงินใด ๆ จากบัญชีของลูกค้า ถ้านับหรือสื่อกลางใด ๆ ที่ใช้ในการโอนเงินนั้นถูกใช้ในการโอนเงินโดยสถาบันผู้ออกสื่อกลางเหล่านั้นให้สามารถพิสูจน์ได้ว่าการโอนโดยใช้สื่อเหล่านั้นเป็นไปโดยถูกต้องตามกฎหมาย ไม่ว่าจะเป็นการพิสูจน์โดยใช้ลายเซ็น ภาพถ่าย ลายพิมพ์นิ้วมือ หรือโดยเครื่องมืออิเล็กทรอนิกส์ใด ๆ ก็ตาม ส่วนการโอนเงินโดยมิชอบด้วยกฎหมายนั้น ลูกค้าจะรับผิดชอบในจำนวนเงินดังนี้

- (1) 50 ดอลลาร์ สรอ. หรือ
- (2) จำนวนเงินหรือมูลค่าของทรัพย์สินหรือบริการที่ได้รับจากการโอนเงินทางอิเล็กทรอนิกส์ก่อนที่จะมีการแจ้งไปยังสถาบันการเงินให้ระงับการจ่าย

ทั้งนี้ แล้วแต่จำนวนใดจะน้อยกว่ากัน

สถาบันการเงินไม่ต้องชดเชยให้ลูกค้า หรือรับผิดชอบในกรณีที่เกิดความเสียหายที่สถาบันการเงินได้ระบุไว้ว่าจะเกิดขึ้น แต่เกิดจากการละเลยของลูกค้า กล่าวคือ

- ลูกค้าไม่แจ้งต่อสถาบันการเงินถึงการโอนเงินโดยมิชอบ หรือข้อผิดพลาดทางบัญชีที่ปรากฏในใบยืนยันยอดภายใน 60 วันหลังจากที่ได้รับใบยืนยันยอดที่ลูกค้าได้รับตาม 15 USC 1693 d
- ลูกค้าไม่แจ้งต่อสถาบันการเงินในกรณีบัตรหรือสื่อกลางอื่นใดสูญหายหรือถูกขโมยภายใน 2 วันทำการหลังจากที่ลูกค้าได้รับรู้ถึงการหายหรือการถูกขโมยดังกล่าว แต่ความรับผิดชอบของลูกค้าในกรณีใด ๆ จะต้องไม่เกินกว่า 500 ดอลลาร์ สรอ. หรือตามจำนวนเงินที่โอนโดยมิชอบ ซึ่งเกิดขึ้นใน 2 วันทำการ (หรือนานกว่านั้น) หลังจาก that ลูกค้าได้รู้ถึงการหายหรือการขโมย แต่ก่อนที่จะแจ้งไปยังสถาบันการเงินแล้วแต่จำนวนใดจะน้อยกว่ากัน

(ข้อกำหนดนี้อาจจะอนุโลมให้เวลานานขึ้น ในกรณีที่มีเหตุการณ์หรือสภาพแวดล้อมที่สมเหตุสมผล)

(b) ในการดำเนินงานใด ๆ ที่เกี่ยวข้องกับความรับผิดชอบของลูกค้าต่อการโอนเงินทางอิเล็กทรอนิกส์โดยมิชอบด้วยกฎหมาย สถาบันการเงินมีหน้าที่ในการพิสูจน์เพื่อให้เห็นว่าได้มีการอนุมัติให้มีการโอนเงินดังกล่าว หรือถ้าการโอนเงินนั้นเป็นการโอนโดยมิชอบด้วยกฎหมาย สถาบันการเงินมีหน้าที่ในการพิสูจน์ถึงเงื่อนไขของความรับผิดชอบตาม subsection (a) ถ้าการโอนได้เกิดขึ้นหลังจากวันที่มีผลบังคับใช้ตาม 15 USC 1693 c

(c) ในกรณีที่รายการซึ่งเกี่ยวข้องทั้งการโอนเงินโดยมิชอบด้วยกฎหมาย และการขยายวงเงินที่กำหนดในมาตรา 103 (e) ของพระราชบัญญัตินี้ (15 USC 1602 (e)) ซึ่งเป็นข้อตกลงระหว่างลูกค้าและสถาบันการเงินในการขยายวงเงินให้ลูกค้า ในกรณีที่บัญชีลูกค้ามีการถอนเงินเกินบัญชี ขอบเขตความรับผิดชอบของลูกค้าสำหรับรายการนี้จะต้องแยกประเด็นพิจารณา

(d) ความมาตรานี้ไม่ได้รวมถึงความรับผิดชอบของลูกค้าต่อการโอนเงินโดยมิชอบด้วยกฎหมาย ในส่วนที่เกินกว่าความรับผิดชอบที่กำหนดไว้ในกฎหมายอื่น หรือที่ระบุไว้ตามข้อตกลงกับสถาบันการเงินกับลูกค้า

(e) ลูกค้าไม่ต้องรับผิดชอบต่อการโอนเงินโดยมิชอบด้วยกฎหมายภายใต้สถานการณ์อื่นใดที่ไม่ได้ระบุในมาตรานี้

8.8 ภาระความรับผิดชอบของสถาบันการเงิน

15 USC 1693 h

(a) ตาม subsection (b) และ (c) สถาบันการเงินจะต้องรับภาระความรับผิดชอบต่อลูกค้าสำหรับความเสียหายที่เกิดจาก

(1) การที่สถาบันการเงินไม่สามารถทำการโอนเงินให้ตามข้อกำหนดในเงื่อนไขบัญชีลูกค้าในจำนวนเงินหรือภายในเวลาที่ลูกค้าได้กำหนดไว้ เว้นแต่ว่า

- (A) บัญชีของลูกค้ามีเงินไม่เพียงพอ
- (B) มีข้อจำกัดในการโอนเงินดังกล่าว หรืออยู่ระหว่างดำเนินการทางกฎหมาย
- (C) การโอนเงินดังกล่าวจะเป็นผลให้เงินในบัญชีของลูกค้ามียอดเป็นลูกค้าเกินกว่าวงเงินที่ตกลงไว้กับธนาคาร
- (D) จำนวนเงินในเครื่องเทอร์มินอลมีไม่เพียงพอที่จะทำการโอนให้ลูกค้าได้สมบูรณ์
- (E) ข้อกำหนดอื่น ๆ ที่คณะกรรมการเป็นผู้กำหนด

(2) ในกรณีที่ลูกค้าไม่สามารถทำการโอนเงินได้ เนื่องจากเงินในบัญชีมีไม่เพียงพอ เพราะสถาบันการเงินได้ให้วงเงินเครดิตตามข้อตกลงและเงื่อนไขของบัญชีนั้น ๆ

(3) สถาบันการเงินจะปฏิบัติตามคำสั่งของลูกค้าให้ระงับการโอนเงินออกจากบัญชีลูกค้าตามข้อตกลงการโอนล่วงหน้า

(b) สถาบันการเงินไม่ต้องรับผิดชอบต่อ subsection (a) (1) และ (2) ถ้าสถาบันการเงินสามารถพิสูจน์ให้เห็นว่าการกระทำหรือละเว้นที่จะกระทำนั้นมีสาเหตุมาจาก

- (1) เหตุการณ์ที่อยู่นอกเหนือการควบคุม
- (2) เป็นเหตุขัดข้องทางเทคนิคที่ลูกค้าได้รับรู้ก่อนที่จะใช้บริการการโอนเงินทางอิเล็กทรอนิกส์แล้ว

(c) ในกรณีที่ข้อผิดพลาดที่เกิดขึ้นตาม subsection (a) ซึ่งเป็นข้อผิดพลาดที่เกิดขึ้นโดยไม่ตั้งใจ หรือมิได้เจตนาทุจริตใด ๆ ทั้ง ๆ ที่ได้หาทางป้องกันเพื่อหลีกเลี่ยงข้อผิดพลาดนั้นแล้วก็ตาม สถาบันการเงินจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นตามมูลค่าที่สามารถพิสูจน์ได้อย่างแท้จริง

8.9 การออกบัตรหรือเครื่องมืออื่นใดที่ใช้เพื่อการโอนเงินทางอิเล็กทรอนิกส์

15 USC 1693 i

(a) การออกบัตร รหัส หรือสื่อกลางอื่นใดที่สามารถทำให้ล่วงรู้ถึงบัญชีของลูกค้าเพื่อวัตถุประสงค์ในการโอนเงินทางอิเล็กทรอนิกส์ สถาบันการเงินจะทำได้เมื่อ

- (1) เป็นการออกให้ตามคำขอของลูกค้า
- (2) เป็นการออกให้ใหม่เพื่อทดแทน

(b) ตามข้อกำหนดของ subsection (a) สถาบันการเงินอาจจะจัดทำบัตร รหัส หรือสื่อกลางอื่นที่ใช้รับบริการโอนเงินทางอิเล็กทรอนิกส์ของบัญชีลูกค้าได้ ถ้า

- (1) บัตร รหัส หรือสื่อกลางอื่นใดเหล่านั้นไม่อยู่ในสภาพที่จะใช้งานได้ต่อไป
- (2) ในการจัดส่งสื่อกลางเหล่านั้นให้ลูกค้าจะต้องจัดส่งเอกสารซึ่งแสดงถึงสิทธิและความรับผิดชอบตาม 15 USC 1693 c ซึ่งมีผลบังคับใช้หาก บัตร รหัส หรือสื่อกลางเหล่านั้นอยู่ในสภาพที่ใช้งานได้
- (3) การจัดส่งดังกล่าวควรมีเอกสารประกอบอธิบายไว้ถึงวิธีการที่ลูกค้าควรปฏิบัติในกรณีที่บัตร รหัส หรือสื่อกลางอื่นที่ใช้กับระบบอยู่ในสภาพที่ใช้งานไม่ได้
- (4) บัตร รหัส หรือสื่อกลางอื่นนั้น จะมีผลตามกฎหมายต่อเมื่อเครื่องมือเหล่านั้นถูกจัดทำขึ้นตามคำขอของลูกค้า หลังจาก que สถาบันการเงินได้พิสูจน์คำขอแล้ว

(c) โดยวัตถุประสงค์ของ subsection (b) นั้น บัตร รหัส หรือสื่อกลางอื่นใดจะมีผลตามกฎหมายต่อเมื่อเครื่องมือเหล่านั้นสามารถใช้ในการทำธุรกรรมโอนเงินทางอิเล็กทรอนิกส์ได้สำเร็จ

8.10 การระงับข้อผูกพัน

15 USC 1693 j

ถ้าความล้มเหลวของระบบเป็นผลให้ลูกค้าไม่สามารถโอนเงินไปให้ผู้อื่นได้เสร็จสมบูรณ์ โดยที่บุคคลนั้นยอมรับในวิธีการโอนเงินทางอิเล็กทรอนิกส์นั้นแล้ว ถือว่าผู้นอนปราศจากภาระรับผิดชอบต่อการโอนนั้น จนกว่าระบบจะได้รับการแก้ไขให้สู่สภาพเดิมอันจะช่วยให้การโอนสามารถดำเนินการเสร็จสมบูรณ์ได้ เว้นแต่บุคคลนั้นได้แจ้งเป็นลายลักษณ์อักษรให้โอนเงินโดยวิธีอื่นนอกเหนือจากการโอนเงินทางอิเล็กทรอนิกส์

8.11 ข้อบังคับในการใช้การโอนเงินทางอิเล็กทรอนิกส์

15 USC 1693 k

บุคคลหรือนิติบุคคลใด ๆ ห้ามดำเนินการต่อไปนี้

- (1) กำหนดเงื่อนไขการชำระเงินคืนของลูกค้าจากการใช้วงเงินเครดิต โดยวิธีตกลงการโอนเงินทางอิเล็กทรอนิกส์ไว้ล่วงหน้า

(2) เรียกร้องให้ลูกค้าเปิดบัญชีกับสถาบันการเงินแห่งหนึ่งแห่งใดโดยเฉพาะเจาะจง เพื่อรับการโอนเงินค่าจ้างหรือเงินจากรัฐสวัสดิการ

8.12 การยับยั้งสิทธิ

15 USC 1693 i

ข้อตกลงใด ๆ ระหว่างลูกค้ากับบุคคลอื่น ไม่ว่าจะเป็นลายลักษณ์อักษรหรือไม่ก็ตาม จะไม่มีผลยับยั้งสิทธิต่าง ๆ ของแต่ละฝ่ายที่ระบุไว้ในพระราชบัญญัตินี้ เว้นเสียแต่ว่าข้อตกลงนั้นจะให้สิทธิแก่ลูกค้าเพิ่มขึ้นหรือสามารถปกป้องสิทธิของลูกค้าบางประการที่มีได้กล่าวไว้ในพระราชบัญญัตินี้

8.13 บทลงโทษทางแพ่ง

15 USC 1693 m

(a) นอกจากที่ระบุไว้ตามมาตรานี้ และ 15 USC 1693 h บุคคลใดที่ละเลยที่จะปฏิบัติตามมาตราใด ๆ ที่เกี่ยวพันกับผลประโยชน์ของลูกค้า ยกเว้นการแก้ไขข้อผิดพลาดตาม 15 USC 1693 f จะต้องรับผิดชอบต่อกู้ในจำนวนเงินเท่ากับ

(1) ผลเสียหายที่เกิดขึ้นตามมูลค่าที่แท้จริง เนื่องจากความล้มเหลวดังกล่าว

(2) (A) ในกรณีเป็นการกระทำของบุคคลใดบุคคลหนึ่ง จำนวนเงินจะต้องไม่ต่ำกว่า 100 ดอลลาร์ สรอ. หรือไม่เกินกว่า 1,000 ดอลลาร์ สรอ. หรือ

(B) ในกรณีเป็นการกระทำของกลุ่มบุคคล จำนวนเงินดังกล่าวจะต้องเป็นไปตามที่ศาล

อนุญาต เว้นแต่ว่า

(i) ไม่สามารถกำหนดเงินชดเชยขั้นต่ำสำหรับสมาชิกแต่ละคนในกลุ่มได้

(ii) จำนวนเงินชดเชยทั้งหมด ตามย่อหน้านี้ เกิดจากการกระทำที่ผิดพลาดในลักษณะเดียวกันที่เกิดขึ้นกับบุคคลคนเดียวกัน แต่จำนวนเงินดังกล่าวต้องไม่เกินกว่า 500,000 ดอลลาร์ สรอ. หรือร้อยละ 1 ของมูลค่าสินทรัพย์สุทธิที่ผู้ถูกกล่าวหา มีอยู่

(3) ศาลจะเป็นผู้พิจารณาค่าใช้จ่าย ค่าธรรมเนียมทนายความ ในการบังคับภาระหนี้สินดังกล่าว

(b) การพิจารณามูลค่าความรับผิดชอบจากการกระทำตาม subsection (a) ศาลจะเป็นผู้พิจารณา โดยขึ้นอยู่กับองค์ประกอบอื่น ๆ กล่าวคือ

(1) การกระทำของบุคคลคนเดียวตาม subsection (a) (2) (B) จำนวนครั้ง และระยะเวลาที่ละเลยการปฏิบัติตามข้อกำหนด สาเหตุแห่งการละเลย จำนวนบุคคลที่ได้รับผลเสียหายและการละเลยดังกล่าวเป็นไปโดยเจตนาหรือไม่

(c) บุคคลใด ๆ ที่สามารถพิสูจน์ได้ว่าการปฏิบัติฝ่าฝืนมาตรานี้เป็นการกระทำโดยมิได้เจตนา และความผิดพลาดที่เกิดขึ้นนั้นมิได้มีวัตถุประสงค์อื่นใดแอบแฝง และได้พยายามหลีกเลี่ยงการปฏิบัติผิดพลาดดังกล่าวจนถึงที่สุดแล้ว บุคคลนั้นไม่ถือว่ามีความผิด ยกเว้นเป็นการกระทำความผิดที่ได้กล่าวไว้ใน 15 USC 1693 h

(d) มาตรานี้ หรือ 15 USC 1693 n ไม่มีผลใช้บังคับต่อ

- (1) การกระทำหรือการละเลยการทำตามที่กำหนด หรือตามความหมายของคณะกรรมการ หรือตามความหมายซึ่งกำหนดโดยเจ้าหน้าที่ของธนาคาร Federal Reserve ซึ่งกระทำการตามอำนาจที่ได้รับมอบหมายจากคณะกรรมการ หากเป็นการกระทำโดยสัจยี่ห้อ หรือ
- (2) สถาบันการเงินได้ใช้แนวทางของถ้อยคำที่ออกโดยคณะกรรมการเพื่อเปิดเผยให้ลูกค้าทราบ แต่ก็ละเลยที่จะเปิดเผยต่อลูกค้า ทั้ง ๆ ที่รู้ว่าจะเบี่ยงข้อบังคับ และข้อความที่แสดงเงื่อนไขต่าง ๆ เหล่านั้นได้มีการแก้ไขเปลี่ยนแปลงไป ได้ ถูกยกเลิก หรือได้ผ่านการพิจารณาของศาลให้เป็นโมฆะแล้ว

(e) บุคคลใด ๆ ที่ละเลยปฏิบัติตามมาตรานี้ จะพ้นจากภาระรับผิดชอบดังกล่าว ถ้าบุคคลนั้นได้แจ้งให้ลูกค้าทราบล่วงหน้าในการละเลยการปฏิบัตินั้น และได้ทำการปรับปรุงบัญชีของลูกค้า พร้อมทั้งชดเชยค่าเสียหายที่เกิดขึ้นตามจริง หรือค่าเสียหายที่เกิดขึ้นตาม 15 USC 1693 h

(f) หากศาลพบว่า การฟ้องร้องตามมาตรานี้ไม่สามารถจะเอาผิดแก่จำเลยได้ เนื่องจากเป็นการฟ้องร้องอันมีเจตนาไม่บริสุทธิ์หรือเพื่อทำลายความสงบสุขแล้ว ศาลจะพิจารณากำหนดค่าธรรมเนียมทนายความ และค่าใช้จ่ายอื่น ๆ ให้แก่จำเลย

(g) ไม่ว่าความเสียหายที่เกิดขึ้นมีมูลค่าเท่าไรก็ตาม อายุความที่จะฟ้องร้องตามมาตรานี้ มีกำหนด 1 ปี นับแต่วันที่ได้กระทำความผิด

8.14 บทลงโทษทางอาญา

15 USC 1693 n

(a) ผู้ใดมีเจตนาที่จะ

- (1) ให้ข้อมูลที่เป็นเท็จ หรือละเว้นที่จะให้ข้อเท็จจริงซึ่งบุคคลผู้นั้นมีหน้าที่จะต้องเปิดเผยตามมาตรานี้
- (2) ละเลยที่จะปฏิบัติตามข้อบังคับของมาตรานี้ จะถูกปรับไม่เกิน 5,000 ดอลลาร์ สรอ. หรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ

(b) บุคคลใดที่

- (1) รู้ว่ารายการที่จะเกิดขึ้นนั้นมีผลกระทบต่อการค้าระหว่างรัฐหรือการค้าต่างประเทศ การพยายามหรือร่วมกันคบคิดอุบายที่จะใช้วิธีการปลอมแปลง การเปลี่ยนแปลง การฉ้อฉล ฉ้อโกง หรือวิธีการทุจริตใด ๆ เพื่อที่จะให้ได้มาซึ่งเครื่องมือในการหักบัญชี เพื่อที่จะให้ได้เงิน สินค้าหรือบริการ หรือสิ่งมีค่าอื่นใด ซึ่งภายในระยะเวลา 1 ปีมีมูลค่ารวมกัน 1,000 ดอลลาร์ สรอ. หรือมากกว่า หรือ
 - (2) เจตนาที่จะกระทำทุจริตหรือขัดต่อกฎหมาย การส่งหรือความพยายามหรือการคบคิดอุบายในการส่งระหว่างรัฐ หรือการค้าต่างประเทศ เกี่ยวกับการปลอมแปลง การเปลี่ยนแปลง การฉ้อฉล ขโมย หรือวิธีการทุจริตใด เพื่อที่จะให้ได้มาซึ่งเครื่องมือหักบัญชี
 - (3) เจตนาที่จะกระทำทุจริตหรือละเมิดกฎหมาย โดยการใช้อุปกรณ์ใด ๆ ระหว่างรัฐ หรือการค้าต่างประเทศ ในการขายหรือส่งการปลอมแปลง การเปลี่ยนแปลง การฉ้อฉล ขโมย หรือวิธีการทุจริตใด เพื่อที่จะให้ได้มาซึ่งเครื่องมือในการหักบัญชี
 - (4) รับ ปกปิด ใช้ หรือส่ง เงิน สินค้า บริการ หรือสิ่งที่มีค่าอื่นใด (ยกเว้นตัวที่ใช้ระหว่างรัฐ หรือการขนส่งต่างประเทศ) ซึ่ง
 - (A) ภายในระยะเวลา 1 ปี ซึ่งมีมูลค่ารวมกัน 1,000 ดอลลาร์ สรอ. หรือมากกว่า
 - (B) เข้ามาเป็นส่วนหนึ่ง หรือเป็นส่วนประกอบของการค้าระหว่างรัฐ หรือการค้าต่างประเทศ และ
 - (C) เป็นการปลอมแปลง การเปลี่ยนแปลง การฉ้อฉล ขโมย หรือวิธีการทุจริตอื่นใดเพื่อให้ได้มาซึ่งเครื่องมือในการหักบัญชี
 - (5) รับ ปกปิด ใช้ ขาย หรือการส่ง การค้าระหว่างรัฐ หรือการค้าต่างประเทศ ซึ่งมีตัวที่ใช้ระหว่างรัฐหรือการขนส่งต่างประเทศ ซึ่ง
 - (A) ภายในระยะเวลา 1 ปี มีมูลค่ารวมกัน 500 ดอลลาร์ สรอ. หรือมากกว่า และ
 - (B) ได้ซื้อหรือได้มีการปลอมแปลง การเปลี่ยนแปลง การปลอมลายมือชื่อ ขโมย หรือวิธีการทุจริตใดให้ได้มาซึ่งเครื่องมือการหักบัญชี หรือ
 - (6) รายการที่มีผลต่อการค้าระหว่างรัฐ หรือการค้าต่างประเทศ การจัดเตรียมเงิน ทรัพย์สิน บริการ หรือสิ่งที่มีมูลค่าอื่นใด ซึ่งภายในระยะเวลา 1 ปีมีมูลค่ารวมกัน 1,000 ดอลลาร์ สรอ. หรือมากกว่า จากการใช้การปลอมแปลง การเปลี่ยนแปลง การฉ้อฉล ขโมย หรือวิธีการทุจริตใด เพื่อให้ได้มาซึ่งเครื่องมือในการหักบัญชี จะต้องถูกปรับไม่เกิน 10,000 ดอลลาร์ สรอ. หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ
- (c) คำว่า “เครื่องมือหักบัญชี” ในมาตรานี้ หมายถึง บัตร รหัส หรือเครื่องมืออื่นใดนอกเหนือจากเช็ค ดราฟต์ หรืออุปกรณ์ กระดาษอื่นใดที่ใกล้เคียง โดยวิธีการโอนเงินทางอิเล็กทรอนิกส์

หน่วยงานที่รับผิดชอบให้มีการปฏิบัติตามพระราชบัญญัตินี้

15 USC 1693 c

(a) หน่วยงานที่ต้องคอยควบคุมดูแลให้มีการปฏิบัติตามข้อกำหนดของกฎหมายนี้

(1) ตามมาตรา 8 ของ Federal Deposit Insurance Act ในกรณีของ

(A) National Bank โดย The Comptroller of the Currency

(B) สมาชิกธนาคารของ Federal Reserve System (นอกเหนือจาก National Bank) โดย Board

(C) ธนาคารที่ Federal Deposit Insurance Corp. รับประกัน (นอกเหนือจากสมาชิกของ Federal Reserve System) โดย Board of Director ของ Federal Deposit Insurance Corp.

(2) มาตรา 5 (d) ของ Home Owners' Loan Act ปี 1933

มาตรา 407 ของ National Housing Act และ

มาตรา 6 (i) และ 17 ของ Federal Home Loan Bank Act โดย Federal home Loan Bank Board (ซึ่งเป็นการกระทำโดยตรงกับ Federal Savings and Loan Insurance Corp.)

(3) Federal Credit Union Act โดยผู้บริหารของ National Credit Union Administration ในเรื่องของ Federal Credit Union

(4) Federal Aviation Act ปี 1958 โดย Civil Aeronautics Board ในเรื่องของ air carrier หรือ foreign air carrier ซึ่งเกี่ยวข้องกับพระราชบัญญัตินี้

(5) Securities Exchange Act ปี 1934 โดย Securities and Exchange Commission ในส่วนของ broker หรือ dealer ซึ่งเกี่ยวข้องกับพระราชบัญญัตินี้

(b) เป้าหมายของการปฏิบัติงานของตัวแทนที่กล่าวถึงใน subsection (a) อำนาจหน้าที่ตามพระราชบัญญัตินั้น การกระทำใดที่ขัดต่อหัวข้อนี้เป็นการกระทำที่ขัดต่อพระราชบัญญัติที่กำหนดใน subsection (a) ตัวแทนแต่ละหน่วยงานที่กล่าวถึงใน subsection (a) นั้น อาจมีการปฏิบัติงานโดยมีเป้าหมายเพื่อให้มีการปฏิบัติตามข้อกำหนดที่กล่าวไว้ในหัวข้อนี้ หรืออำนาจหน้าที่ที่อ้างอิงถึงตามกฎหมาย

(c) Federal Trade Commission จะเป็นผู้บังคับให้มีการปฏิบัติตามข้อบังคับที่กำหนดไว้ในหัวข้อนี้ สำหรับเป้าหมายที่ให้ Federal Trade Commission ปฏิบัติตามอำนาจหน้าที่ที่ระบุไว้ใน Federal Trade Commission Act การกระทำใดที่ขัดต่อหัวข้อนี้จะเป็นการขัดต่อพระราชบัญญัตินี้ด้วย

การรายงานต่อสภาองเกรส

15 USC 1693 p

(a) ภายในระยะเวลา 12 เดือน นับแต่ที่หัวข้อนี้มีผลบังคับใช้ และในทุก ๆ ปี The Board and Attorney General จะต้องทำรายงานให้สภา Congress ในส่วนที่เกี่ยวข้องกับการบริหารงานตามหน้าที่ที่ระบุไว้ในหัวข้อเรื่องนี้ รวมถึงข้อเสนอแนะ และรายงานทุกฉบับจะต้องกล่าวถึงการประเมินผลการทำตามบทความนี้ และบทสรุปของการกระทำตามข้อกำหนดที่ระบุไว้ใน 15 USC 1693 P ของหัวข้อนี้ ในรายงานของ Board จะต้องกล่าวถึงผลกระทบในด้านค่าใช้จ่ายและผลตอบแทนที่มีต่อสถาบันการเงินและลูกค้า ในด้านการแข่งขันและการแนะนำเทคโนโลยีใหม่ ๆ มาใช้ การดำเนินงานของสถาบันการเงินและความพอเพียงในการปกป้องคุ้มครองลูกค้า ในรายงานของ Attorney General จะต้องมีการวิเคราะห์สรุปผลกระทบของการดำเนินงาน workload ประสิทธิภาพการทำงานของ Federal Courts

(b) ในการปฏิบัติตามหัวข้อนี้ Board อาจนำความคิดเห็นของ Federal Agency อื่น ๆ มาใช้ในการปฏิบัติตามกฎระเบียบและควบคุมกลุ่มบุคคลดังกล่าว

การประสานกับกฎหมายของแต่ละรัฐ

15 USC 1693 q

กฎหมายนี้มิได้มีผลยกเลิก เปลี่ยนแปลง หรือมีผลกระทบต่อกฎหมายของรัฐใด ๆ ในส่วนที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ ยกเว้นกฎหมายอื่นที่ขัดต่อบทความนี้ กฎหมายของรัฐจะไม่เป็นการขัดกันกับหัวข้อนี้ ถ้ามีการปกป้องคุ้มครองลูกค้ามากกว่าที่กำหนดไว้ในหัวข้อนี้ Board จะจัดส่งระเบียบวิธีปฏิบัติที่ Board กำหนดขึ้น และพิจารณาถึงความต้องการของรัฐที่ขัดกันหรือสามารถให้การปกป้องคุ้มครองที่มากกว่า ซึ่งถ้า Board พิจารณาเห็นว่าข้อกำหนดของรัฐไม่เป็นไปตามที่กำหนดไว้ สถาบันการเงินจะต้องรับภาระหนี้สินตามกฎหมายของรัฐ แม้จะมีการพิจารณาเปลี่ยนแปลง ปรับปรุง หรือยกเลิก ซึ่งมีการพิจารณาในศาล หรืออำนาจอื่นที่เป็นโมฆะ

ข้อยกเว้นของระเบียบข้อบังคับของรัฐ

15 USC 1693 r

Board จะละเว้นการกระทำตามหัวข้อนี้ในการโอนเงินทางอิเล็กทรอนิกส์ภายในรัฐใดก็ได้ ถ้าพิจารณาแล้วเห็นว่า กฎหมายของรัฐนั้น ๆ ที่เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ได้ระบุให้มีการกระทำที่เหมือนกับที่ได้ระบุไว้ในหัวข้อนี้

วันที่มีผลบังคับใช้

15 USC 1693 s

หัวข้อนี้จะมีผลบังคับใช้หลังจากวันที่มีการประกาศใช้พระราชบัญญัติแล้ว 18 เดือน ยกเว้น 15 USC 1693 g และ 1693 i จะมีผลบังคับใช้หลังจากวันที่ประกาศใช้พระราชบัญญัติแล้ว 90 วัน

9 ข้อมูลที่น่าสนใจบางประการ

DATA PROTECTION ACT 1984 สหราชอาณาจักร (เฉพาะส่วนที่สำคัญ)

กฎหมายนี้เป็นกฎหมายที่ใช้บังคับสำหรับการประมวลผลข้อมูลโดยเครื่องอัตโนมัติซึ่งเป็นข้อมูลที่เกี่ยวข้องกับบุคคล และการให้บริการเกี่ยวกับข้อมูลดังกล่าว

ภาคที่ 1 ข้อความเบื้องต้น (Preliminary)

1. คำจำกัดความข้อมูล (Data) และถ้อยคำที่เกี่ยวข้อง

1.1 คำที่บัญญัติไว้ดังต่อไปนี้ให้มีผลใช้บังคับสำหรับการตีความกฎหมายนี้

1.2 ข้อมูล (Data) หมายถึง ข้อมูลที่บันทึกไว้ในรูปแบบซึ่งสามารถจะประมวลผล โดยเครื่องมือที่ทำงานโดยอัตโนมัติตามคำสั่งที่ได้รับเพื่อวัตถุประสงค์ดังกล่าว

1.3 ข้อมูลส่วนบุคคล (Personal data) หมายถึงข้อมูลที่เกี่ยวข้องกับบุคคลซึ่งมีชีวิตอยู่ ซึ่งสามารถระบุได้จากข้อมูลนั้น (หรือจากข้อมูลนั้นและข้อมูลอื่น ๆ ซึ่งอยู่ในความครอบครองของผู้ใช้ข้อมูล) รวมทั้งการแสดงความเห็นใด ๆ เกี่ยวกับบุคคลนั้น แต่ไม่รวมถึงการแสดงใดเกี่ยวกับความสนใจของผู้ใช้ข้อมูล ซึ่งเกี่ยวข้องกับบุคคลนั้น

1.4 เจ้าของข้อมูล (Data subject) หมายถึงบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลนั้น

1.5 ผู้ใช้ข้อมูล (Data user) หมายถึงบุคคลซึ่งครอบครองข้อมูล และบุคคลเป็นผู้ “ครอบครอง” ข้อมูล ถ้า

ก) ข้อมูลนั้นเป็นส่วนหนึ่งของข้อมูลทั้งหมดที่ได้ประมวลผลหรือตั้งใจจะประมวลผล โดยหรือในนามของบุคคลดังกล่าว ตามที่ระบุไว้ในข้อ 1.2 และ

ข) บุคคลนั้น (ไม่ว่าจะโดยลำพังหรือร่วมกับบุคคลอื่น ๆ) ควบคุมสาระและการใช้ข้อมูลที่มีสะสมไว้ และ

ค) ข้อมูลอยู่ในรูปแบบซึ่งได้เคยหรือตั้งใจจะประมวลผลตามที่ระบุในข้อ ก) ข้างต้น หรือ (แม้ว่าในบางขณะจะไม่อยู่ในรูปแบบนั้น) อยู่ในรูปแบบซึ่งได้เปลี่ยนแปลงไปหลังจากได้รับการประมวลผลแล้ว และอาจจะได้รับการประมวลผลต่อไปอีกในโอกาสต่อ ๆ ไป

1.6 บุคคลทำหน้าที่เป็นหน่วยบริการข้อมูลคอมพิวเตอร์ (computer bureau) ถ้าเป็นผู้ที่ให้บริการเกี่ยวกับข้อมูลแก่บุคคลอื่น และบุคคลเป็นผู้ให้บริการดังกล่าว ถ้า

ก) เป็นตัวแทนของบุคคลอื่นในการประมวลผลข้อมูลซึ่งครอบครองโดยบุคคลนั้น ๆ ตามที่ระบุในข้อ 1.2 ข้างต้น หรือ

ข) อนุญาตให้บุคคลอื่นใช้เครื่องมือที่อยู่ในความครอบครองของตน สำหรับการประมวลผลข้อมูลอยู่ในความครอบครองของบุคคลดังกล่าว ตามที่ได้ระบุไว้ในข้อ 1.2

1.7 การประมวลผล (processing) ในส่วนที่เกี่ยวข้องกับข้อมูล หมายถึงการแก้ไข เพิ่มเติม หรือจัดลำดับของข้อมูล หรือย่อความในข้อมูล และในกรณีของข้อมูลส่วนบุคคล หมายถึงการกระทำการใด ๆ ดังกล่าวข้างต้นที่เกี่ยวข้องกับเจ้าของข้อมูล

1.8 ข้อ 1.7 ข้างต้น ไม่หมายความว่ารวมถึงการกระทำใดที่สร้างขึ้นเพียงเพื่อวัตถุประสงค์ในการจัดเตรียมข้อความของเอกสาร (Text of documents)

1.9 การเปิดเผย (Disclosing) ที่เกี่ยวกับข้อมูล รวมถึงการเปิดเผยข้อความที่ดึงออกมาจากข้อมูล และในกรณีที่การระบุตัวบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลนั้นขึ้นอยู่กับข้อความที่อยู่ในข้อมูลนั้นเป็นบางส่วน และบางส่วนขึ้นอยู่กับข้อความอื่นซึ่งอยู่ในความครอบครองของผู้ใช้ข้อมูล จะไม่ถือว่าเป็นการเปิดเผยข้อมูลหรือโอนข้อมูล นอกจากข้อความอื่นนั้นได้รับการเปิดเผยหรือโอนไปด้วย

2. หลักในการป้องกันข้อมูล (The data protection principles)

2.1 ตาม subsection 2.3 ของข้อนี้ การใช้กฎหมายนี้ในหลักการป้องกันข้อมูล หมายถึง หลักการที่กำหนดไว้ใน Part I ของ Schedule 1 ของกฎหมายนี้ และการตีความของหลักการนี้จะต้องเป็นไปตาม Part II ของ Schedule ดังกล่าว

2.2 หลักการ 7 หลักการแรกใช้บังคับสำหรับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของผู้ใช้ข้อมูลและหลักการที่ 8 ใช้บังคับกับทั้งข้อมูลดังกล่าว และข้อมูลส่วนบุคคลที่เป็นการให้บริการของบุคคลที่กระทำการเป็นผู้ให้บริการข้อมูลคอมพิวเตอร์

2.3 The Secretary of State อาจจะมีคำสั่งให้ปรับปรุงหรือเพิ่มเติมหลักการดังกล่าวได้ เพื่อวัตถุประสงค์ในการเพิ่มความปลอดภัยที่เกี่ยวข้องกับข้อมูลส่วนบุคคลซึ่งประกอบด้วยข้อมูลเกี่ยวกับ

- ก) เชื้อชาติของเจ้าของข้อมูล
 - ข) ความคิดเห็นทางการเมืองของบุคคล หรือศาสนา หรือความเชื่ออื่น ๆ
 - ค) สุขภาพทางกาย และสุขภาพทางจิต หรือพฤติกรรมทางเพศ หรือ
 - ง) การต้องโทษทางอาญา
- ฯลฯ

3. นายทะเบียนและการตัดสินปัญหา

3.1 เพื่อปฏิบัติตามวัตถุประสงค์แห่งกฎหมายนี้ จะต้องมี

- ก) เจ้าหน้าที่ซึ่งเรียกว่า Data Protection Registrar (ในกฎหมายนี้จะเรียกย่อ ๆ ว่า นายทะเบียน (The Registrar)) และ
- ข) ผู้ตัดสินปัญหาซึ่งเรียกว่า Data Protection Tribunal (ในกฎหมายนี้ เรียกย่อ ๆ ว่า the Tribunal)

3.2 The Registrar จะได้รับการแต่งตั้งโดยสมเด็จพระราชินีนาถ

3.3 The Tribunal จะประกอบด้วย

- ก) ประธานซึ่งแต่งตั้งโดย the Lord chancellor หลังจากได้ปรึกษากับ the Lord advocate แล้ว

- ข) จำนวนของรองประธานซึ่งจะได้รับการแต่งตั้งโดยวิธีการดังกล่าวข้างต้นขึ้นอยู่กับ การพิจารณาของ the Lord Chancellor และ
- ค) จำนวนของสมาชิกอื่นซึ่งจะได้รับการแต่งตั้งโดย the Secretary of State ขึ้นอยู่กับการพิจารณาของผู้แต่งตั้ง

3.4 สมาชิกของ the Tribunal ซึ่งได้รับการแต่งตั้งตามข้อ 3.3 ก) และ ข) ข้างต้นจะต้องเป็นเนติบัณฑิต ทนายความหรือทนายความชั้น 2 มาเป็นเวลาไม่น้อยกว่า 7 ปี

3.5 สมาชิกของ the Tribunal ซึ่งได้รับการแต่งตั้งตาม 3.3 ค) จะต้องประกอบด้วย

- ก) บุคคลผู้เป็นผู้แทนของผู้ใช้ข้อมูล และ
- ข) บุคคลผู้เป็นผู้แทนของเจ้าของข้อมูล

3.6 Schedule 2 จะกฎหมายนี้จะมีผลต่อ the Registrar และ the Tribunal

ภาคที่ 2 การจดทะเบียนและการควบคุมผู้ใช้ข้อมูลและผู้ให้บริการข้อมูลคอมพิวเตอร์

การจดทะเบียน

4. การจดทะเบียนผู้ใช้ข้อมูลและผู้ให้บริการข้อมูลคอมพิวเตอร์

4.1 The Registrar จะเป็นผู้เก็บรักษาทะเบียนผู้ใช้ข้อมูลและผู้กระทำการให้บริการข้อมูลคอมพิวเตอร์ซึ่งครอบครองหรือให้บริการเกี่ยวกับข้อมูลส่วนบุคคล และจะทำการจดทะเบียนตามคำขอจดทะเบียนซึ่งได้รับตามข้อบัญญัติของภาคที่ 2 ของกฎหมายนี้

4.2 ในการจดทะเบียนจะต้องระบุว่าเป็นการจดทะเบียนในฐานะผู้ใช้ข้อมูลหรือเป็นผู้ให้บริการข้อมูลหรือเป็นผู้ใช้ข้อมูลซึ่งทำหน้าที่ให้บริการข้อมูลด้วย

4.3 ตามบทบัญญัติของ section นี้ การจดทะเบียนผู้ใช้ข้อมูลจะต้องมีรายการดังต่อไปนี้

- ก) ชื่อและที่อยู่ของผู้ใช้ข้อมูล
- ข) ลักษณะของข้อมูลส่วนบุคคลซึ่งจะอยู่ในความครอบครอง และวัตถุประสงค์ในการครอบครอง หรือการใช้ข้อมูลนั้น
- ค) แหล่งข้อมูลซึ่งตนประสงค์หรือต้องการจะได้มาซึ่งข้อมูลหรือข้อความที่ประสงค์จะมีในข้อมูล
- ง) ลักษณะของบุคคลใดซึ่งตนประสงค์หรือต้องการจะเปิดเผยข้อมูล
- จ) ชื่อหรือลักษณะของประเทศใดหรือดินแดนใดนอกราชอาณาจักรซึ่งตนประสงค์หรืออาจต้องการจะส่งข้อมูลไปให้ไม่ว่าโดยตรงหรือโดยอ้อม
- ฉ) ที่อยู่ที่ใช้ในการรับคำสั่งจากเจ้าของข้อมูลเพื่อที่จะเข้าถึงข้อมูล

4.4 ตามข้อบัญญัติของ section นี้ การจดทะเบียนของผู้ทำหน้าที่ให้บริการข้อมูลคอมพิวเตอร์จะต้องประกอบด้วยชื่อและที่อยู่ของบุคคลนั้น

4.5 ตามข้อบัญญัติของ section นี้ การจดทะเบียนของผู้ใช้ข้อมูลทำหน้าที่เป็นผู้ให้บริการข้อมูลคอมพิวเตอร์ด้วย จะต้องประกอบด้วย ชื่อ และที่อยู่ และข้อความตามที่ระบุในข้อ 4.3 ข) ถึง ฉ) ข้างต้น

4.6 ในกรณีที่บริษัทจดทะเบียน ที่อยู่หมายถึงที่อยู่ของสำนักงาน และต้องระบุเลขที่จดทะเบียนเป็นบริษัทด้วย

4.7 ในกรณีบุคคล (นอกจากบริษัทจดทะเบียน) ซึ่งมีสถานประกอบธุรกิจที่อยู่ตามข้อ 4.3 ก), 4.4 และ 4.5 หมายถึงสถานที่ประกอบธุรกิจของตน

4.8 The Secretary of State อาจจะมีคำสั่งเปลี่ยนแปลงรายการในการจดทะเบียนได้

5. ข้อห้ามของการถือครองหรือการดำเนินการอื่นใดเกี่ยวกับข้อมูลส่วนบุคคลโดยไม่ได้จดทะเบียน (Prohibition fo unregistered holding etc. of personal data)

5.1 บุคคลใดจะครอบครองข้อมูลส่วนบุคคลไม่ได้ นอกจากจะได้จดทะเบียนเป็นผู้ใช้ข้อมูล หรือผู้ใช้ข้อมูลที่ทำหน้าที่ให้บริการข้อมูลคอมพิวเตอร์ด้วย

5.2 บุคคลตามที่จดทะเบียนไว้จะต้องไม่

- ก) ครอบครองข้อมูลส่วนบุคคลในลักษณะใดมากไปกว่าที่ระบุไว้ในคำขอจดทะเบียน
- ข) ครอบครองข้อมูลดังกล่าวหรือใช้ข้อมูลดังกล่าวซึ่งตนครอบครองอยู่ เพื่อวัตถุประสงค์อื่นใดนอกเหนือจากวัตถุประสงค์ที่ระบุไว้ในคำขอจดทะเบียน
- ค) ได้ข้อมูลหรือความใดเพื่อรวมไว้ในข้อมูลนั้น เพื่อการครอบครองจากแหล่งข้อมูลอื่นที่มีได้ระบุไว้ในคำขอจดทะเบียน
- ง) เปิดเผยข้อมูลดังกล่าวซึ่งตนครอบครองอยู่ แก่บุคคลใดซึ่งมิได้ระบุไว้ในคำขอจดทะเบียน
- จ) ทำการส่งข้อมูลดังกล่าวซึ่งอยู่ในความครอบครองของตนไปยังประเทศใดหรือเขตแดนใดนอกสหราชอาณาจักร นอกจากประเทศหรือเขตแดนที่ระบุไว้ในการจดทะเบียน ไม่ว่าจะเป็นการส่งโดยตรงหรือโดยอ้อม

5.3 ลูกจ้างหรือตัวแทนของบุคคลซึ่งอยู่ภายใต้ข้อบังคับ 5.2 ข้างต้น จะต้องอยู่ภายใต้ข้อจำกัดดังกล่าวด้วย ในการใช้ การเปิดเผย หรือการส่งข้อมูล เหมือนกับที่บุคคลนั้นต้องอยู่ภายใต้ข้อบังคับข้อ 5.2 ข), ง) และ จ) ในกรณีที่ข้อมูลส่วนบุคคลนั้นอยู่ในครอบครองของบุคคลนั้นและอยู่ภายใต้ข้อบังคับ 5.2 ค) ในกรณีจะหาข้อมูลเพื่อครอบครองของบุคคลนั้น

5.4 บุคคลที่ทำหน้าที่เป็นผู้ให้บริการข้อมูลคอมพิวเตอร์จะต้องไม่ให้บริการเกี่ยวกับข้อมูลส่วนบุคคล นอกจากจะได้ทำการจดทะเบียน และมีชื่ออยู่ในทะเบียนในฐานะผู้ให้บริการข้อมูลคอมพิวเตอร์ หรือผู้ใช้ข้อมูลซึ่งให้บริการข้อมูลคอมพิวเตอร์ด้วย

5.5 บุคคลใดฝ่าฝืนข้อบังคับข้อ 5.1 ข้างต้น หรือฝ่าฝืนโดยเจตนาหรือโดยขาดความระมัดระวังข้อห้ามใด ๆ ในข้อ 5. นี้ จะมีความผิดตามกฎหมาย

6. การขอจดทะเบียนและการขอแก้ไขรายการที่จดทะเบียน

7. การรับและการปฏิบัติตามคำขอจดทะเบียน

7.1 ภายใต้ข้อบังคับข้อนี้ the Registrar จะต้องทำการจดทะเบียนให้โดยเร็วที่สุดเท่าที่จะเป็นไปได้ และในทุกกรณี จะต้องแจ้งเป็นหนังสือให้ผู้ขอจดทะเบียนทราบว่าคำขอจดทะเบียนหรือคำขอเปลี่ยนแปลงรายการจดทะเบียน ได้รับการยอมรับหรือปฏิเสธ ภายในเวลา 6 เดือนหลังจากได้รับคำขอนั้น ๆ และในกรณีที่แจ้งให้ผู้ขอทราบว่าจะได้รับการยอมรับคำขานั้นจะต้องมีข้อความ ดังนี้

- ก) รายการที่ได้รับการจดทะเบียน หรือรายการแก้ไข ซึ่งได้แก้ไขแล้ว ตามคำขอ และ
- ข) วันที่ รายการ หรือการแก้ไข ได้รับการจดทะเบียน

7.2 The Registrar จะต้องไม่ปฏิเสธคำขอซึ่งได้ขอมาตาม section 6 นอกจาก

- ก) พิจารณาเห็นว่า รายการที่ขอจดทะเบียน หรือรายการที่ขอแก้ไข แล้วแต่กรณี ไม่ให้ ข้อมูลอย่างเพียงพอในสิ่งที่เกี่ยวข้อง
- ข) เห็นว่าคำขอนั้นน่าจะเป็นการขัดแย้งกับหลักการในการป้องกันข้อมูล และ
- ค) เห็นว่าข้อมูลที่ได้รับไม่เพียงพอที่จะทำให้เห็นว่าคำขอนั้นจะไม่ขัดต่อหลักการใดดังกล่าวข้างต้น

7.3 subsection 7.2 ก) ข้างต้น มิได้ถือเป็นการห้ามมิให้ the Registrar ยอมรับการจดทะเบียนรายการซึ่งระบุในความหมายกว้าง ๆ ในกรณีที่เห็นว่ามีเหมาะสมและ the Registrar จะต้องยอมรับรายการในทำนองดังกล่าว ในกรณีใดที่เห็นว่ารายการที่ระบุโดยเฉพาะเจาะจงข้อนั้นอาจจะมีผลเสียหายต่อวัตถุประสงค์ในการครอบครองข้อมูลนั้น

7.4 ในกรณีที่ the Registrar ปฏิเสธคำขอตาม section นี้ จะต้องให้เหตุผล และแจ้งให้ผู้ขอทราบถึงสิทธิที่จะอุทธรณ์ตาม section 13 ได้

7.5 ถ้าในกรณีใดที่ the Registrar เห็นว่าคำขอนั้นจะต้องการเวลาในการพิจารณานานกว่าที่กำหนดใน subsection 7.1 ข้างต้น จะต้องมีหนังสือแจ้งให้ผู้ขอทราบโดยเร็วที่สุด และก่อนเวลาที่กำหนดดังกล่าว ในกรณีนี้ไม่ต้องแจ้งการยอมรับหรือปฏิเสธคำขอในเวลาที่กำหนด

7.6 ภายใต้ข้อบังคับของ subsection 7.8 บุคคลซึ่งได้ยื่นคำขอตาม section 6 ข้างต้นจะ

- ก) จนกว่าจะได้รับคำแจ้งตาม subsection 7.1 ข้างต้น หรือขอถอนคำขอ และ
- ข) ถ้าได้รับคำแจ้งตาม subsection 7.1 ปฏิเสธคำขอ จนกระทั่งถึงสิ้นสุดระยะเวลาที่อาจจะยื่นอุทธรณ์แล้วหรือได้ถอนคำอุทธรณ์แล้วถูกถือตามวัตถุประสงค์ของ section 5 ข้างต้น เสมือนว่าคำขอได้รับการยอมรับแล้ว และรายการในคำขอได้รับการจดทะเบียนแล้ว หรือคำขอแก้ไขรายการในคำขอได้รับการแก้ไขแล้ว ในวันที่ได้ยื่นคำขอนั้น

ฯลฯ

8. อายุของทะเบียนและการต่ออายุ

8.1 ผู้ได้รับการจดทะเบียนทุกรายจะถูกลบออกจากทะเบียนหลังจากสิ้นสุดเวลาที่กำหนดในการจดทะเบียน นอกจากนี้จะได้รับการยื่นคำขอต่ออายุต่อ the Registrar ตาม section นี้

8.2 ตาม subsection 8.3 เวลาการคงอยู่ของทะเบียน และเวลาที่ทะเบียนนั้นจะคงอยู่ในระหว่างที่มีการยื่นคำขอต่ออายุ (เวลาต่ออายุ) จะต้องเป็นช่วงเวลา (ไม่น้อยกว่า 3 ปี) ที่ได้รับการระบุไว้ โดยเริ่มจากเวลาที่เริ่มจดทะเบียน หรือเวลาที่ทะเบียนนั้นจะถูกยกเลิกถ้าไม่มีคำขอต่ออายุแล้วแต่กรณี

8.3 บุคคลที่ยื่นคำขอจดทะเบียน หรือคำขอต่ออายุการจดทะเบียน อาจจะระบุอายุของการจดทะเบียน หรืออายุที่ขอต่อออกไป แล้วแต่กรณี เป็นเวลาที่สั้นกว่าที่กำหนดก็ได้โดยจะต้องเป็นเวลาที่เต็มปี

ฯลฯ

9. การตรวจสอบและการดำเนินการประการอื่น ๆ เกี่ยวกับการลงทะเบียนรายการ

9.1 The Registrar จะต้องจัดสิ่งอำนวยความสะดวกสำหรับสาธารณชน ในการที่จะตรวจสอบข้อมูลซึ่งอยู่ในคำขอจดทะเบียน (อยู่ในรูปแบบที่มองเห็นได้และเป็นที่ยอมรับตามกฎหมาย) ในเวลาทำการตามปกติ และโดยไม่คิดค่าใช้จ่ายใด ๆ

9.2 The Registrar ต้องให้สำเนารายการที่ได้จดทะเบียนไว้ และรับรองความถูกต้องแก่สาธารณชน ที่ต้องการจะได้สำเนานั้น โดยคิดค่าธรรมเนียมได้ตามที่กำหนด

การกำกับควบคุม

10. คำเตือนให้ปฏิบัติตาม (Enforcement notices)

10.1 ถ้า the Registrar เห็นว่าบุคคลที่ได้จดทะเบียนไว้ ได้ทำการฝ่าฝืนหรือกำลังฝ่าฝืนหลักการป้องกันข้อมูล ก็อาจจะส่งคำเตือนกำหนดให้ดำเนินการแก้ไขให้เป็นไปตามหลักการนั้น ๆ ภายในระยะเวลาที่กำหนด

10.2 ในการตัดสินใจว่าจะส่งคำเตือนหรือไม่นั้น the Registrar จะต้องพิจารณาว่า การฝ่าฝืนนั้น ทำให้เกิดหรือน่าจะทำให้เกิดความเสียหายหรือความยุ่งยากแก่บุคคลหรือไม่

10.3 คำเตือนที่เกี่ยวกับการฝ่าฝืนหลักการข้อ 5. ในหลักการป้องกันข้อมูล (Schedule 1) อาจ จะกำหนดให้ผู้ให้ข้อมูล

- ก) แก้ไขหรือลบข้อมูลนั้นหรือข้อมูลอื่นใดที่ครอบครองอยู่ และมีการแสดงความเห็น ซึ่ง the Registrar เห็นว่าเกิดขึ้นจากข้อมูลที่ไม่ถูกต้องหรือ
- ข) ในกรณีของข้อมูลตามที่ระบุไว้ใน subsection 22.2 ของ section 22 กำหนดให้กระทำการอย่างเดียวกับข้อ ก) ข้างต้นหรือกระทำการตามที่ระบุมาในคำเตือนเพื่อความปลอดภัยตามข้อกำหนดใน subsection นั้น และถ้า the Registrar เห็นสมควร อาจจะกำหนดให้กระทำการเพื่อเสริมข้อมูลโดยข้อความที่เป็นจริงเกี่ยวกับเรื่องที่เกี่ยวข้องกับข้อมูลตามที่ the Registrar ให้ความเห็นชอบ

10.4 The Registrar จะต้องไม่ออกคำเตือนให้บุคคลปฏิบัติตามข้อ (ก) ของหลักการป้องกันข้อมูลข้อที่ 7 (ใน schedule 1) ที่พาดพิงถึงเจ้าของข้อมูล นอกจากจะเห็นว่าบุคคลนั้นได้ฝ่าฝืน section 21 โดยไม่ให้ข้อมูลซึ่งเจ้าของข้อมูลสมควรได้รับ และได้รับการร้องขอตาม section นี้

10.5 คำเตือนจะต้องมีข้อความดังนี้

- ก) ข้อความของหลักการซึ่ง the Registrar เห็นว่าได้มีการฝ่าฝืนหรือกำลังมีการฝ่าฝืน และเหตุผลที่ทำให้สรุปได้ดังกล่าว
- ข) รายการแห่งสิทธิที่จะอุทธรณ์ซึ่งให้ไว้ใน section 13

ฯลฯ

10.8 คำเตือนนี้อาจถูกยกเลิกได้ โดยทำเป็นหนังสือไปถึงบุคคลที่ได้รับคำเตือนนั้น

10.9 บุคคลใดที่ไม่ปฏิบัติตามคำเตือน จะมีความผิดตามกฎหมาย แต่บุคคลผู้ถูกกล่าวหาว่าไม่มีสิทธิที่จะแก้ข้อกล่าวหาว่ามีความผิดตาม subsection นี้ โดยพิสูจน์ว่าได้กระทำการอย่างแข็งขันตามสมควรแล้วที่จะปฏิบัติตามคำเตือนนั้น

11. คำเตือนว่าจะเพิกถอนการจดทะเบียน (De-registration notices)

11.1 ถ้า the Registrar เห็นว่าบุคคลจดทะเบียนได้ฝ่าฝืนหรือกำลังฝ่าฝืนหลักการการป้องกันข้อมูลหลักการใด อาจจะมีปฏิบัติดังนี้

- ก) ส่งคำเตือนว่าจะเพิกถอนการจดทะเบียน ระบุว่าเพิกถอนการจดทะเบียนทั้งหมดหรือบางส่วนของบุคคลผู้นั้น ภายในเวลาที่กำหนดในคำเตือน
- ข) ภายใต้ข้อบัญญัติใน section นี้ ทำการเพิกถอนรายการจากการจดทะเบียนเมื่อสิ้นสุดระยะเวลาที่กำหนด

11.2 ในการตัดสินใจว่าจะส่งคำเตือนว่าจะเพิกถอนการจดทะเบียนหรือไม่นั้น the Registrar จะต้องพิจารณาว่า การฝ่าฝืนนั้นทำให้เกิดหรือน่าจะทำให้เกิดความเสียหายหรือความยุ่งยากแก่บุคคลใดหรือไม่ และ the Registrar จะต้องไม่ส่งคำเตือนดังกล่าวนอกจากจะเห็นว่าผู้ได้รับคำเตือนให้ปฏิบัติตามหลักการไม่สามารถปฏิบัติตามได้แล้ว

11.3 คำเตือนว่าจะเพิกถอนการจดทะเบียนจะต้องประกอบด้วย

- ก) ข้อความของหลักการที่ the Registrar เห็นว่าได้มีการฝ่าฝืนหรือกำลังมีการฝ่าฝืน และเหตุผลที่ทำให้สรุปได้ดังกล่าว และได้ตัดสินใจว่าคำเตือนให้ปฏิบัติตามไม่ได้ผล
- ข) รายการของสิทธิที่จะอุทธรณ์ที่ให้ไว้ตาม section 13

ฯลฯ

11.6 คำเตือนนี้อาจถูกยกเลิกได้ โดยทำเป็นหนังสือถึงผู้ที่ได้รับคำเตือนนั้น

11.7 คำเตือนที่จะยกเลิกการจดทะเบียนรายการใด ให้รวมกับการยกเลิกบางส่วนของรายการนั้นด้วย

12. คำเตือนห้ามส่งข้อมูล (Transfer prohibition notice)

12.1 ถ้า the Registrar เห็นว่า

- ก) บุคคลซึ่งจดทะเบียนเป็นผู้ใช้ข้อมูล หรือผู้ใช้ข้อมูลซึ่งทำหน้าที่ผู้ให้บริการข้อมูลคอมพิวเตอร์ด้วยหรือ
- ข) บุคคลซึ่งถือเสมือนว่าได้จดทะเบียนแล้วตาม section 7 subsection 7.6 ข้างต้นตั้งใจจะส่งข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองของตนไปยังสถานที่นอกสหราชอาณาจักร the Registrar เห็นว่าเป็นไปตามที่ระบุใน subsection 12.2 หรือ 12.3 ข้างท้ายนี้ ก็อาจจะส่งคำเตือนห้ามส่งข้อมูลโดยเด็ดขาด หรือจนกว่าจะปฏิบัติตามที่ระบุในคำเตือน เพื่อป้องกันผลประโยชน์ของเจ้าของข้อมูลดังกล่าวแล้ว

12.2 หากสถานที่ที่จะส่งข้อมูลไปนั้นมิได้อยู่ในรัฐที่ระบุตาม European Convention แล้ว the Registrar จะต้องเห็นว่าการส่งข้อมูลนั้นน่าจะเป็นการฝ่าฝืนหรือนำไปสู่การฝ่าฝืนหลักการป้องกันข้อมูลในหลักการใดหลักการหนึ่ง

12.3 ในกรณีที่สถานที่ที่จะส่งข้อมูลนั้นไปเป็นรัฐที่ระบุตาม European Convention แล้ว the Registrar จะต้องเห็นว่า

- ก) (i) บุคคลนั้นตั้งใจจะส่งให้ส่งข้อมูลต่อไปยังสถานที่อื่นซึ่งมิได้อยู่ในรัฐนั้น และ
(ii) การส่งต่อดังกล่าวน่าจะเป็นการฝ่าฝืนหรือนำไปสู่การฝ่าฝืนหลักการป้องกันข้อมูลหรือ
- ข) ในกรณีที่ข้อมูลซึ่งต้องปฏิบัติตามคำสั่งที่ออกมาตาม section 2 subsection 2.3 ข้างต้น การโอนนั้นน่าจะเป็นการฝ่าฝืนหรือนำไปสู่การฝ่าฝืนหลักการป้องกันข้อมูลโดยมีผลซึ่งเกี่ยวข้องไปถึงข้อมูลนั้น

12.4 ในการตัดสินใจว่าจะส่งคำเตือนห้ามส่งข้อมูลหรือไม่นั้น the Registrar จะต้องพิจารณาว่าจำเป็นต้องมีคำเตือนนั้นเพื่อป้องกันความเสียหายหรือความยุ่งยากแก่บุคคลใด และต้องพิจารณาระดับความเหมาะสมโดยทั่วไปในการอำนวยความสะดวกในการส่งข้อมูลโดยอิสระระหว่างสหราชอาณาจักรและรัฐและดินแดนอื่นด้วย

12.5 คำเตือนห้ามส่งข้อมูลจะต้องระบุเวลาที่คำเตือนนั้นจะมีผลใช้บังคับด้วยและมีข้อความดังต่อไปนี้

- ก) ข้อความแสดงถึงหลักการซึ่ง The Registrar เห็นว่าน่าจะถูกฝ่าฝืนและเหตุผลที่ทำให้สรุปได้ดังกล่าว และ
- ข) รายการของสิทธิที่จะอุทธรณ์ซึ่งให้ไว้ตาม section 13

ฯลฯ

12.8 the Registrar อาจจะยกเลิกคำเตือนได้ โดยส่งหนังสือแจ้งไปยังบุคคลซึ่งได้รับคำเตือนนั้น

12.9 คำเตือนห้ามส่งข้อมูลดังกล่าวจะต้องไม่ห้ามการโอนข้อมูลใด ซึ่งการโอนนั้นเป็นการโอนข้อมูลซึ่งเป็นที่ต้องการหรือได้อนุญาตโดยหรือตามกฎหมาย หรือเป็นที่ต้องการโดยการประชุมใดหรือโดยเครื่องมือใด ซึ่งเป็นข้อมูลผูกพันระหว่างประเทศซึ่งสหราชอาณาจักรมีอยู่

12.10 บุคคลใดที่ฝ่าฝืนคำเตือนห้ามส่งข้อมูล จะมีความผิดตามกฎหมาย แต่บุคคลนั้นมีสิทธิที่จะป้องกันตนเองตาม subsection นี้ โดยพิสูจน์ว่าได้พยายามสมควรแล้วที่จะหลีกเลี่ยงการฝ่าฝืนคำเตือนดังกล่าว

12.11 เพื่อให้เป็นไปตามวัตถุประสงค์แห่ง section นี้ สถานที่ซึ่งขึ้นอยู่กับรัฐซึ่งถูกระบุไว้ใน European Convention จะถือว่าเป็นรัฐที่ระบุได้ด้วย

การอุทธรณ์ (Appeals)

13. สิทธิที่จะอุทธรณ์ (Right to appeals)

13.1 บุคคลอาจจะอุทธรณ์ต่อผู้ตัดสินปัญหา (The Tribunal) เกี่ยวกับ

- ก) การปฏิเสธโดย the Registrar ที่จะรับจดทะเบียนบุคคลผู้นั้นหรือการปฏิเสธที่จะแก้ไขรายการจดทะเบียน
- ข) คำเตือนให้ปฏิบัติตามคำเตือนที่จะเพิกถอนการจดทะเบียน หรือ คำเตือนห้ามส่งข้อมูลซึ่งบุคคลผู้นั้นได้รับ

ฯลฯ

13.4 Schedule 3 ของกฎหมายนี้จะมีผลเกี่ยวข้องกับการอุทธรณ์ภายใน section นี้ และการดำเนินการของ the Tribunal เกี่ยวกับการอุทธรณ์

14. การพิจารณาคำอุทธรณ์ (Determination of appeals)

14.1 ถ้า the Tribunal เห็นว่าการอุทธรณ์ตาม section 13 subsection 13.1 ข้างต้น

- ก) การปฏิเสธหรือคำเตือนซึ่งได้รับการอุทธรณ์นั้นได้มีขึ้นโดยไม่ตรงตามกฎหมาย หรือ
- ข) การปฏิเสธหรือคำเตือนที่เกี่ยวข้อง ซึ่งเกิดจากดุลพินิจของ the Registrar นั้น ไม่ตรงกับดุลพินิจของ the Tribunal

The Tribunal อาจจะยอมรับคำอุทธรณ์ หรือเปลี่ยนแปลงการตัดสินใจหรือคำเตือนได้ โดยถือเป็นเสมือนการตัดทอนคำเตือนของ the Registrar และ the Tribunal มีสิทธิที่จะยกคำอุทธรณ์ได้

14.2 The Tribunal อาจจะพิจารณาข้อเท็จจริงใด ๆ ซึ่งเป็นเหตุให้มีการปฏิเสธหรือคำเตือนดังกล่าวขึ้น

ฯลฯ

14.5 ผู้ที่อุทธรณ์ต่อ the Tribunal อาจจะอุทธรณ์คำตัดสินของ the Tribunal เกี่ยวกับข้อกฎหมายต่อศาลที่เหมาะสมได้ และศาลจะต้องเป็น

- ก) ศาลสูง (The High court of Justice) ในอังกฤษ ถ้าที่อยู่ของบุคคลซึ่งอุทธรณ์ต่อ the Tribunal นั้นอยู่ในอังกฤษหรือเวลส์
- ข) The court of Session ถ้าที่อยู่นั้นอยู่ในสกอตแลนด์ และ

ค) ศาลสูง (The High court of Justice) ในไอร์แลนด์เหนือ ถ้าที่อยู่นั้นอยู่ในไอร์แลนด์เหนือ

14.6 ใน subsection 14.5 ข้างต้น ที่อยู่ของผู้ทูลขอต่อ the Tribunal จะต้องเป็นที่อยู่ที่รวมหรือเสนอไว้เพื่อรวมอยู่ในการจดทะเบียน

บทเบ็ดเตล็ดและบทเสริม

(Miscellaneous and supplementary)

15. การเปิดเผยข้อมูลโดยมิชอบด้วยกฎหมายของผู้ให้บริการข้อมูลคอมพิวเตอร์ (Unauthorised disclosure by computer bureau)

15.1 ข้อมูลส่วนบุคคลซึ่งอยู่ในการให้บริการของบุคคลซึ่งให้บริการข้อมูลคอมพิวเตอร์ จะต้องไม่ถูกเปิดเผยโดยบุคคลนั้นโดยไม่ได้รับการยินยอมล่วงหน้าจากบุคคลซึ่งตนให้บริการ

15.2 subsection 15.1 ข้างต้น ใช้บังคับกับลูกจ้างหรือตัวแทนของบุคคลผู้ซึ่งทำหน้าที่ให้บริการข้อมูลคอมพิวเตอร์ด้วย

16. อำนาจในการจดทะเบียนและการตรวจสอบ (Powers of Entry and inspection)

Schedule 4 ของกฎหมายนี้จะมีผลต่อการตรวจจับการฝ่าฝืนกฎหมายนี้ และการฝ่าฝืนหลักการป้องกันข้อมูล

17. การเปิดเผยข้อมูล (Disclosure of information)

17.1 กฎหมายหรือข้อบังคับอื่นใดที่ห้ามหรือจำกัดการเปิดเผยข้อมูล มิให้ใช้บังคับสำหรับการให้ข้อมูลที่จำเป็นแก่ the Registrar หรือ the Tribunal ในการปฏิบัติตามหน้าที่ของเจ้าหน้าที่ดังกล่าว ภายใต้กฎหมายนี้

17.2 เพื่อให้เป็นไปตาม section 2 ของ The official Secrets Act 1911 (การสื่อสารข้อมูลโดยผิดกฎหมาย)

ก) The Registrar และเจ้าหน้าที่และลูกจ้าง

ข) สมาชิกของ the Tribunal และ

ค) เจ้าหน้าที่อื่นหรือลูกจ้างของ the Tribunal ซึ่งมีได้เป็นข้าราชการเป็นเจ้าพนักงานตามกฎหมายของพระมหากษัตริย์

17.3 section 2 มิให้นำมาใช้บังคับในการห้ามการเปิดเผยข้อมูลโดยบุคคลใดซึ่งระบุใน subsection 17.2 ก) หรือ ข) ข้างต้น หรือโดยเจ้าพนักงานหรือลูกจ้างของ the Tribunal ซึ่งการเปิดเผยนั้นเป็นไปเพื่อการปฏิบัติหน้าที่ตามกฎหมายนี้ หรือเพื่อการดำเนินการภายใต้หรือเกิดจากกฎหมายนี้ รวมทั้งการดำเนินการในการพิจารณาของ the Tribunal

18. วิธีการส่งคำเตือน (service of notices)

ฯลฯ

19. การดำเนินการตามกฎหมายและบทลงโทษ

19.1 บุคคลที่มีความผิดตามกฎหมายนี้ นอกจากตาม section 6 หรือ paragraph 12 of Schedule 4 จะมีโทษ

ก) ปรับ ตามความผิดตามฟ้อง

ข) ปรับ รวมทั้งสิ้นไม่เกินจำนวนที่กำหนดไว้ตามกฎหมาย (ตามที่กำหนดไว้ใน section 74 ของ criminal Justice Act 1982)

19.2 บุคคลที่มีความผิดตาม section 6 หรือ paragraph 12 ที่กล่าวข้างต้นมีโทษปรับรวมไม่เกิน fifth level ของตารางมาตรฐาน (ตามที่กำหนดไว้ใน section 75 ของ Criminal Justice Act 1982)

19.3 ตาม subsection 19.5 ข้างท้ายนี้ ศาลอาจจะสั่งให้ข้อมูลที่ศาลเห็นว่าเกี่ยวข้องกับการกระทำความผิด ถูกทำให้เสียหาย ถูกทำลาย หรือถูกลบทิ้งเสีย

19.4 ศาลจะไม่สั่งตาม subsection 19.4 เกี่ยวกับวัตถุอื่นใดซึ่งบุคคลใด (นอกจากผู้กระทำความผิด) อ้างว่าเป็นเจ้าของหรือมีผลประโยชน์ในวัตถุนั้น โดยยื่นคำร้องต่อศาลนอกจากจะให้โอกาสแก่บุคคลนั้นในการแสดงเหตุผลว่าเหตุใดจึงไม่ควรออกคำสั่งดังกล่าวแล้ว

20. ภาระของกรรมการฯ (Liability of directors etc.)

20.1 ในกรณีที่การฝ่าฝืนกฎหมายนี้กระทำโดยนิติบุคคล และพิสูจน์ได้ว่าความผิดนั้นได้กระทำขึ้น โดยการรู้เห็นเป็นใจ หรือยินยอม หรือมีส่วนในการละเลย จากกรรมการผู้จัดการ เลขานุการ หรือเจ้าหน้าที่ที่มีตำแหน่งคล้ายคลึงกัน ของนิติบุคคลหรือของบุคคลซึ่งกระทำการในหน้าที่ดังกล่าว บุคคลผู้นั้นจะต้องมีความผิดเช่นเดียวกับนิติบุคคลนั้น และมีภาระที่ต้องถูกดำเนินคดีและลงโทษเช่นเดียวกัน

20.2 ในกรณีที่กิจการของนิติบุคคลได้รับการบริหารโดยสมาชิก subsection 20.1 ข้างต้นก็จะนำมาใช้บังคับสำหรับการกระทำและความผิดของสมาชิก เกี่ยวกับหน้าที่ในการบริหารของตน เสมือนหนึ่งบุคคลนั้นเป็นกรรมการของนิติบุคคลนั้นเช่นกัน

ภาคที่ 3 สิทธิของเจ้าของข้อมูล (Rights of Data Subjects)

21. สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคล

21.1 ตามบทบัญญัติของ section นี้ บุคคลใดมีสิทธิ

- ก) ที่จะได้รับการแจ้งจากผู้ให้ข้อมูลรายใดว่าข้อมูลที่ครอบครองโดยผู้ให้ข้อมูลรายนั้นมีข้อมูลส่วนบุคคล ซึ่งบุคคลนั้นเป็นเจ้าของข้อมูลรวมอยู่ด้วยหรือไม่ และ
- ข) ได้รับสำเนาของข้อมูลซึ่งประกอบขึ้นเป็นข้อมูลส่วนบุคคล ซึ่งผู้ให้ข้อมูลครอบครองอยู่จากผู้ให้ข้อมูลนั้น และในกรณีที่ข้อมูลใดที่กล่าวถึงใน paragraph ข) ข้างต้น อยู่ในรูปที่ไม่สามารถบอกกล่าวได้ โดยไม่มีการอธิบายเพิ่มเติม ข้อมูลจะต้องมีคำอธิบายดังกล่าวประกอบไปด้วย

21.2 ผู้ให้ข้อมูลจะไม่มีข้อผูกพันที่จะให้ข้อมูลใดตาม subsection 21.1 นอกจากเพื่อเป็นไปตามการร้องขอในรูปของหนังสือ และได้ชำระค่าธรรมเนียมตามที่กำหนดแล้วแต่การร้องขอข้อมูลตาม paragraph ทั้ง 2 ของ subsection นั้น จะถือเสมือนเป็นคำร้องขอเดียวกัน คำร้องขอข้อมูลตาม paragraph ก) จะถือว่าเป็นคำร้องขอข้อมูลตาม paragraph ข) ได้ด้วย ถ้าไม่มีสิ่งบ่งชี้เป็นอื่น

21.3 ในกรณีที่ผู้ให้ข้อมูลจดทะเบียนแยกกันเกี่ยวกับข้อมูลซึ่งครอบครองไว้เพื่อวัตถุประสงค์ต่างกัน จะต้องนำคำต้องแยกต่างหากจากกัน และจะต้องจ่ายค่าธรรมเนียมแยกต่างหากจากกันด้วย ในการขอข้อมูลซึ่งแยกจดทะเบียนไว้

21.4 ผู้ให้ข้อมูลจะไม่มีข้อผูกพันที่จะต้องทำตามคำร้องตาม section นี้

- ก) นอกจากจะได้รับข้อมูลตามที่ต้องการเพื่อที่จะสามารถระบุตัวบุคคลผู้ขอได้แน่ชัด และเพื่อจะค้นหาข้อมูลที่ต้องการได้ถูกต้อง และ
- ข) ถ้าไม่สามารถปฏิบัติตามคำขอได้โดยไม่เปิดเผยข้อมูลซึ่งเกี่ยวข้องกับบุคคลอื่นซึ่งสามารถระบุได้จากข้อมูลนั้น นอกจากจะเห็นว่าบุคคลอื่นนั้นได้อนุญาตให้เปิดเผยข้อมูลดังกล่าวแก่บุคคลผู้ขอข้อมูลได้

21.5 ผู้ให้ข้อมูลจะต้องปฏิบัติตามคำขอตาม section นี้ภายใน 40 วัน หลังจากได้รับคำขอหรือหลังจากที่ได้รับข้อมูลตาม paragraph ก) ของ subsection 21.4 แล้ว หรือหลังจากได้รับคำยินยอมตาม paragraph ข) ของ subsection นั้นแล้ว

21.6 ข้อมูล ซึ่งจะต้องให้ตามคำขอตาม section นี้ จะเป็นข้อมูลที่อยู่ ณ เวลา ที่ได้รับคำขอ นอกจากจะมีการแก้ไขหรือลบทิ้งระหว่างเวลานั้น และระหว่างเวลาที่ให้ข้อมูลที่ได้รับการแก้ไขหรือลบทิ้งบางส่วนแล้ว ซึ่งจำเป็นต้องกระทำไม่ว่าจะได้รับการคำขอหรือไม่ก็ตาม

21.7 ถ้าศาลเห็นว่า บุคคลใดซึ่งได้มีคำขอดังกล่าวข้างต้นตาม section นี้ ไม่ได้รับการสนองตอบจากผู้ให้ข้อมูล โดยการฝ่าฝืนข้อบัญญัติดังกล่าว ศาลอาจสั่งให้ปฏิบัติตามคำขอได้ แต่ศาลจะต้องไม่ออกคำสั่งดังกล่าวตาม subsection นี้ ถ้าเห็นว่าไม่มีเหตุผลใด ๆ ที่จะกระทำการดังกล่าว ไม่ว่าจะเนื่องจากความถี่ของคำขอมิมากเกินไปหรือด้วยเหตุอื่นก็ตาม

21.9 The Secretary of State อาจะสั่งให้นำคำขอตาม section นี้ ในนามของบุคคลใดซึ่งเป็นบุคคลที่ไร้ความสามารถที่จะกระทำการใด ๆ ด้วยตนเองได้

22. ค่าชดเชยความเสียหายจากการผิดพลาดของข้อมูล (compensation for inaccuracy)

22.1 บุคคลใดซึ่งเป็นเจ้าของข้อมูลที่อยู่ในความครอบครองของผู้ให้ข้อมูล และได้รับความเสียหายเนื่องจากความผิดพลาดของข้อมูล จะมีสิทธิได้รับค่าชดเชยความเสียหายจากผู้ให้ข้อมูล สำหรับความเสียหายนั้น และสำหรับความยุ่งยากซึ่งบุคคลผู้นั้นได้รับเนื่องจากความผิดพลาดนั้น

22.2 ในกรณีที่ข้อมูลที่ได้บันทึกไว้อย่างถูกต้องตามที่ผู้ให้ข้อมูลได้รับจากเจ้าของข้อมูลหรือจากบุคคลที่สาม subsection 22.1 จะไม่ใช้บังคับถ้าไม่ปฏิบัติตามต่อไปนี้

- ก) ข้อมูลนั้นบ่งว่า ข้อมูลนั้นได้รับหรือได้ตามที่กล่าวข้างต้น หรือไม่มีข้อความใดถูกต้องออกจากข้อมูลนอกจากในรูปซึ่งสามารถระบุถึงผลของการกระทำนั้นได้
- ข) ถ้าเจ้าของข้อมูลได้แจ้งให้ผู้ให้ข้อมูลทราบว่า ข้อมูลนั้นไม่ถูกต้อง หรือก่อให้เกิดความเข้าใจผิด การระบุผลดังกล่าวได้รวมอยู่ในข้อมูลแล้วหรือไม่มีข้อความใดถูกต้องออกจากข้อมูลนอกจากในรูปซึ่งสามารถระบุถึงผลของการกระทำดังกล่าวได้

22.3 ในการดำเนินคดีกับบุคคลใดตาม section นี้ ผู้ถูกกล่าวหาจะต้องเป็นผู้พิสูจน์ว่าได้กระทำการโดยระมัดระวังตามสมควรแล้วในการรักษาความถูกต้องของข้อมูลในเวลาที่เกี่ยวข้อง

22.4 ข้อมูลจะมีความไม่ถูกต้องตามความหมายของ section นี้ ถ้ามีความคลาดเคลื่อนหรือก่อให้เกิดความเข้าใจผิดจากความจริง

23. ค่าชดเชยสำหรับการสูญหายหรือการเปิดเผยโดยมิชอบด้วยกฎหมาย (Compensation for loss or unauthorized disclosure)

23.1 บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของผู้ให้ข้อมูลหรือตามการให้บริการของบุคคลซึ่งทำหน้าที่ให้บริการข้อมูลคอมพิวเตอร์ และได้รับความเสียหายเนื่องจาก

- ก) ข้อมูลนั้นสูญหาย
- ข) ข้อมูลถูกทำลาย โดยที่ผู้ให้ข้อมูลหรือผู้ให้บริการข้อมูลคอมพิวเตอร์ไม่มีสิทธิที่จะกระทำการดังกล่าว แล้วแต่กรณี

- ค) ตาม subsection 23.2 การเปิดเผยข้อมูลหรือการเข้าถึงข้อมูลโดยไม่มีอำนาจหน้าที่ดังกล่าวข้างต้น จะมีสิทธิที่จะได้รับค่าชดเชยจากผู้ให้ข้อมูลหรือผู้ให้บริการข้อมูลคอมพิวเตอร์แล้วแต่กรณี สำหรับความเสียหายหรือความยุ่งยากซึ่งบุคคลผู้นั้นได้รับโดยเหตุผลการสูญหาย ทำลาย หรือการเปิดเผย หรือการเข้าถึงข้อมูล

23.2 ในกรณีที่ผู้ให้ข้อมูลที่จดทะเบียนแล้ว subsection 23.1 ค) ข้างต้นไม่ใช้บังคับสำหรับการเปิดเผยหรือการเข้าถึงข้อมูลโดยบุคคลใดตามที่ระบุไว้ใน section 4 subsection 4.3 ง) ข้างต้น ตามที่ระบุไว้ในการจดทะเบียนของผู้ให้ข้อมูลนั้น

23.3 ในการดำเนินคดีบุคคลใดตาม section นี้ บุคคลนั้นต้องเป็นผู้พิสูจน์ว่าได้กระทำการโดยรอบคอบระมัดระวังตามสมควรแล้วที่จะป้องกันการสูญหาย การทำลาย การเปิดเผย หรือการเข้าถึงข้อมูลนั้น

24. การแก้ไขและลบข้อมูล (Rectification and erasure)

24.1 ถ้าศาลเห็นว่า ผู้ร้องซึ่งเป็นเจ้าของข้อมูลว่า ข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองของผู้ใช้ข้อมูล ซึ่งผู้ร้องเป็นเจ้าของข้อมูลอยู่นั้น มีความผิดพลาดตามความหมายของ section 22 ข้างต้น ศาลอาจจะสั่งให้แก้ไขหรือลบข้อมูลนั้น หรือข้อมูลอื่นใดซึ่งอยู่ในความครอบครองของผู้ใช้ข้อมูล ซึ่งแสดงความคิดเห็นซึ่งปรากฏต่อศาลว่าขึ้นอยู่กับข้อมูลที่ผิดพลาดนั้น

24.2 ถ้าศาลเห็นด้วยตามคำร้องของเจ้าของข้อมูลว่า

- ก) บุคคลผู้นั้นได้รับความเสียหายจากการเปิดเผยข้อมูลส่วนบุคคล หรือการเข้าถึงและได้มาซึ่งข้อมูลส่วนบุคคล ทำให้บุคคลนั้นมีสิทธิได้รับค่าชดเชยตาม section 23 ข้างต้น และ
- ข) เห็นว่ามีความเสี่ยงพอสมควรที่จะมีการเปิดเผยข้อมูลหรือเข้าถึงข้อมูลนั้นต่อไปอีกโดยปราศจากอำนาจหน้าที่ตามที่ระบุไว้ใน section 23 ศาลอาจจะสั่งให้ลบข้อมูลนั้นทิ้ง แต่ในกรณีที่ข้อมูลนั้นเป็นข้อมูลที่อยู่ในการบริการของบุคคลผู้ทำหน้าที่ให้บริการข้อมูล ศาลจะยังไม่สั่งการดังกล่าว นอกจากจะได้แจ้งให้ผู้ให้บริการได้รับทราบตามระยะเวลาอันสมควรแล้ว

25. การตัดสินและกระบวนการ (Jurisdiction and procedure)

25.1 การตัดสินตาม section 21 และ 24 ข้างต้น เป็นอำนาจ High court หรือ Country court หรือในกรณีของสกอตแลนด์ เป็นอำนาจของ The court of Session หรือนายอำเภอ

ภาคผนวก ง

การศึกษาการหักกลบลบหนี้ระหว่างประเทศ

การหักกลบลบหนี้ที่ประเทศกลุ่ม G-10 ได้ศึกษาไว้ในปี 2532 มีรายละเอียดจากเอกสารเรื่องร่าง รายงานโครงการหักกลบลบหนี้ (ระหว่างประเทศ) ซึ่งเป็นเอกสารที่ผมได้มาจากการได้ไปเป็น Thailand representation ว่าด้วยเรื่อง Electronic funds transfer ซึ่งต่อมาทาง UNCITRAL (The United Nations Commission on International Trade Law) ได้เปลี่ยนชื่อเป็น Draft Model Law on International Credit Transfers เพื่อให้ครอบคลุมการโอนเครดิตทุกประเภทที่ดำเนินการในแบบ Electronics และในแบบตราสารปกติ ทั้งนี้มีเรื่องน่าสนใจโดยสรุปดังนี้

1. คณะทำงานที่เชี่ยวชาญระบบการชำระเงินจากธนาคารกลางของประเทศกลุ่ม G-10 ได้ศึกษาเกี่ยวกับ ข้อตกลงในการหักกลบลบหนี้ที่เกี่ยวข้องกับการเงินระหว่างประเทศ และได้สรุปผลการศึกษาออกมาเป็นรายงานโครงการ เรื่อง การหักกลบลบหนี้
2. ธนาคารกลาง ผู้ควบคุมดูแลธนาคารพาณิชย์ และสถาบันอื่นที่มีส่วนเกี่ยวข้องกับข้อตกลงในการหักกลบลบหนี้ ควรเข้าใจถึงความเสี่ยงต่าง ๆ ที่เกิดขึ้น เช่น ความเสี่ยงเกี่ยวกับฐานะ (Credit risk) ความเสี่ยงเกี่ยวกับสภาพคล่อง (Liquidity risk) และความเสี่ยงเกี่ยวกับระบบ (Systemic risk) การเข้าใจถึงความเสี่ยงจะช่วยให้ผู้มีส่วนเกี่ยวข้องหามาตรการต่าง ๆ เพื่อควบคุมหรือลดความเสี่ยงเหล่านี้ให้เกิดขึ้นน้อยที่สุด
3. ข้อตกลงในการหักกลบลบหนี้ ตามสัญญาแลกเปลี่ยนเงินตราต่างประเทศ และคำสั่งให้ชำระเงิน เป็น ส่วนหนึ่งของระบบหักบัญชีระหว่างธนาคารและชำระบัญชีกัน ซึ่งถือว่าเป็นส่วนหนึ่งของระบบการชำระเงินที่น่าสนใจของประเทศต่าง ๆ

รายงานโครงการเรื่องการหักกลบลบหนี้ (Report on Netting Schemes)

คำนำ

ในช่วงกลางปี พ.ศ. 2531 คณะทำงานที่เชี่ยวชาญระบบชำระเงินจากธนาคารกลางของประเทศกลุ่ม G-10 ได้จัดประชุมที่ Basle เพื่อเริ่มต้นศึกษาเกี่ยวกับข้อตกลงในการหักกลบลบหนี้การที่เกี่ยวข้องกับการเงินระหว่างประเทศ ซึ่งมีอยู่หลายประเภทอย่างละเอียด ในปัจจุบันข้อตกลงดังกล่าวมีหลาย ๆ ประเทศได้นำไปปฏิบัติเพื่อจัดการเกี่ยวกับ เรื่องของข้อตกลงและการชำระเงินที่เกิดขึ้นจากสัญญาแลกเปลี่ยนเงินตราต่างประเทศและสัญญาอื่น ๆ นอกจากนี้ ยัง มีการเสนอหรือพัฒนาระบบการหักกลบ (netting arrangements) ที่มีอยู่และที่เกิดขึ้นในอนาคตว่า อาจจะมีส่วน ช่วยสนับสนุนตลาดการเงินระหว่างประเทศ และระบบการชำระเงินระหว่างประเทศได้อย่างไร และจะมีผลกระทบต่อ ความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องของคู่สัญญาอย่างไร

รายงานฉบับนี้แสดงให้เห็นถึงผลลัพธ์จากการศึกษาดังกล่าว ซึ่งชี้ให้เห็นถึงประเด็นต่าง ๆ อย่างกว้าง ๆ ที่อาจจะเกิดขึ้น รูปแบบและโครงสร้างของข้อตกลงในการหักกลบที่แตกต่างกัน ดังนั้น ธนาคารกลางผู้กำกับดูแล ธนาคาร และแม้แต่ธนาคารและสถาบันอื่น ๆ ที่มีส่วนเกี่ยวข้องกับข้อตกลงเหล่านั้นจำเป็นต้องพิจารณากันอย่างละเอียดรอบคอบ ในส่วนของธนาคารกลางก็มีการสอบทานประเด็นที่มีความสลับซับซ้อนและยุ่งยากอย่างต่อเนื่อง ธนาคารต่าง ๆ จะมีรายงานฉบับนี้อยู่ เพราะมีความหวังว่าธนาคารจะใช้เพื่อประเมินการปฏิบัติงานของตน ในปัจจุบันและความเสี่ยงที่เกี่ยวข้อง และผู้ที่มีจุดมุ่งหมายจะมีส่วนร่วมในข้อตกลงต่าง ๆ ในอนาคต นอกจากนี้ รายงานดังกล่าวยังอาจจะเป็นประโยชน์ต่อผู้จัดหาเครือข่ายในการติดต่อสื่อสารและผู้ค้าขายอื่น ๆ ที่เกี่ยวข้องกับระบบในการหักกลบ

รายงานฉบับนี้เป็นความเห็นซึ่งมีผลมาจากการศึกษาของคณะทำงาน และไม่จำเป็นต้องเป็นความเห็นของธนาคารกลางของประเทศกลุ่ม G-10 หรือ BIS สมาชิกของคณะทำงานที่รับผิดชอบเบื้องต้นในการร่างรายงานประกอบด้วย

1. ความนำ (Introduction)

1.1 ในเดือนมิถุนายน พ.ศ. 2531 คณะทำงานที่เชี่ยวชาญระบบการชำระเงินของธนาคารกลางของประเทศกลุ่ม G-10 หรือที่เรียกสั้น ๆ ว่า “Payments Group” ได้จัดเตรียมรายงานเกี่ยวกับโครงการข้อตกลงในการหักกลบรายการที่เกี่ยวข้องกับการเงินระหว่างประเทศซึ่งมีอยู่หลายประเภทโดยเริ่มนำไปปฏิบัติหรือมีการนำเสนออย่างจริงจัง เป้าหมายก็เพื่อประเมินข้อตกลงที่อาจจะใช้ในการหักกลบจำนวนเงินที่ครบกำหนดแล้วระหว่างธนาคารซึ่งเกิดจากสัญญาแลกเปลี่ยนเงินตราต่างประเทศ (foreign exchange contracts) ไม่ว่าจะเป็นกรณีที่มีคู่สัญญาสองฝ่ายหรือหลาย ๆ ฝ่ายก็ตาม ข้อตกลงต่าง ๆ เหล่านี้ควรจะมีการวิเคราะห์โดยไม่มองแต่เพียงว่ามีส่วนช่วยสนับสนุนตลาดการเงินระหว่างประเทศและระบบการชำระเงินระหว่างประเทศเท่านั้น แต่还必须พิจารณาถึงผลกระทบของความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องของคู่สัญญาอีกด้วย นอกจากนี้ ยังมีความเสี่ยงเกี่ยวกับระบบ (systemic risk) เข้ามาเกี่ยวข้อง ในระหว่างหกเดือนหลังของปี พ.ศ. 2531 นั้น คณะทำงานได้ปรึกษาหารือกันถึงประเด็นทางด้านเทคนิค กฎหมาย และการเงิน โดยมีผู้ปฏิบัติงานและผู้สนับสนุนในเรื่องข้อตกลงในการหักกลบระหว่างธนาคารร่วมกันให้ข้อมูลข่าวสารในรายงานฉบับนี้ รายงานฉบับนี้ได้ร่างขึ้นจากประเด็นต่าง ๆ ที่ปรึกษาหารือกัน แต่ไม่ได้มาจากข้อตกลงใด ๆ ที่มีอยู่หรือที่มีการเสนอมาเป็นพิเศษ

1.2 รายงานฉบับนี้ได้วิเคราะห์ถึงข้อตกลงในการหักกลบ โดยพิจารณาจากความได้เปรียบที่เห็นได้อย่างชัดเจน 2 จุด คือ

- (1) วิเคราะห์ในฐานะที่เป็นรูปแบบ (models) ที่จะแบ่งความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องได้อย่างไรในกรณีที่มีโครงสร้างในการหักกลบและชำระบัญชีแตกต่างกัน
- (2) วิเคราะห์ในฐานะที่เป็นตัวอย่าง (examples) ของประเด็นเกี่ยวกับนโยบายทางการเงินระหว่างประเทศที่มีปัญหายุ่งยากซึ่งเกิดขึ้นโดยการพัฒนาและผลของระบบการชำระเงินต่างประเทศ (cross-border of offshore payment system) และข้อตกลงในการหักกลบตามสัญญา ในตัวรายงานที่วิเคราะห์จะเน้นประเด็นความเสี่ยงเกี่ยวกับฐานะ

และสภาพคล่อง อย่างไรก็ตาม ในส่วนของการสรุปและข้อสังเกตได้กล่าวไว้ว่า การปฏิบัติตามข้อตกลงเหล่านี้ในเรื่องของ cross-border จะแย้งกับข้อสมมุติฐานของการปฏิบัติงานและการกำกับดูแลของตลาดการธนาคารระหว่างประเทศที่เข้าใจกันอยู่ในปัจจุบัน

1.3 โดยปกติแล้วข้อแตกต่างระหว่างข้อตกลงในการหักกลบเกี่ยวกับสัญญาแลกเปลี่ยนเงินตราต่างประเทศทันที อาจจะมีวันครบกำหนด 1 หรือ 2 วัน ในขณะที่คำสั่งให้ชำระเงินอาจจะเป็นวันเดียวกันกับวันที่มีคำสั่งเกิดขึ้น แต่กระนั้นก็ตามจุดมุ่งหมายของรายงานฉบับนี้นั้นก็คือ สัญญาแลกเปลี่ยนเงินตราต่างประเทศ และคำสั่งให้ชำระเงินมีลักษณะพิเศษที่เหมือนกันคือ มีเทคนิคในการหักกลบประเภทเดียวกัน รายงานฉบับนี้ขึ้นอยู่กับข้อเท็จจริงในการวิเคราะห์ความเสี่ยงของการหักกลบในรูปแบบต่าง ๆ ที่จัดให้มีขึ้น

1.4 ข้อตกลงในการหักกลบสัญญาแลกเปลี่ยนเงินตราต่างประเทศที่มีคู่สัญญาหลายฝ่าย ประกอบด้วยผู้มีส่วนเกี่ยวข้องจากประเทศต่าง ๆ จำนวนหนึ่งสามารถใช้ระบบการชำระเงินได้ ดังนั้น เรื่องที่เกี่ยวข้องกับระบบการชำระเงินอาจจะขยายรวมไปถึงข้อตกลงในการหักกลบสัญญาแลกเปลี่ยนเงินตราต่างประเทศ

1.5 รายงานฉบับนี้แบ่งออกเป็น 7 ส่วน เรื่องที่ต่อส่วนแรกที่เป็นความนำก็เป็นส่วนที่ 2 ซึ่งคณะทำงานได้ให้ข้อสังเกตสำคัญ ๆ บางเรื่อง และบางเรื่องก็ชี้ให้เห็นถึงประเด็นต่าง ๆ เกี่ยวกับขอบเขตของรายงาน ส่วนที่ 3 วิเคราะห์ถึงประเภทต่าง ๆ ของความเสี่ยงทางการเงินซึ่งผู้มีส่วนเกี่ยวข้องในระบบการหักบัญชี (clearing systems) จะต้องเสี่ยง ส่วนที่ 4 จะบรรยายถึงเหตุผลว่าทำไมธนาคารเข้ามาทำข้อตกลงในการหักกลบและทำไม suppliers อาจจะต้องเสนอขายอุปกรณ์อำนวยความสะดวกต่าง ๆ ส่วนที่ 5 เป็นการวิเคราะห์อย่างย่อ ๆ ถึงหลักการทางกฎหมายในการหักกลบ ส่วนที่ 6 กล่าวถึงข้อตกลงใน 4 ประเภท และวิเคราะห์ถึงลักษณะของความเสี่ยงที่แตกต่างกัน ในส่วนสุดท้ายคือส่วนที่ 7 จะแสดงให้เห็นถึงภาพทั้งหมดของลักษณะของความเสี่ยงเกี่ยวกับสภาพคล่องที่ผู้มีส่วนเกี่ยวข้องจะต้องประสบในการหักกลบ นอกจากนี้ ในตอนท้ายยังได้แนบอธิบายศัพท์ต่าง ๆ ที่ใช้ในรายงานฉบับนี้ เพื่อให้เข้าใจในความหมายเดียวกันและป้องกันความสับสน

2. บทสรุปและข้อสังเกตต่าง ๆ (Summary and Observations)

วิวัฒนาการต่าง ๆ ที่สร้างขึ้นมาเพื่อใช้ในการหักบัญชีระหว่างธนาคารและชำระบัญชีกันก่อให้เกิดการเปลี่ยนแปลงในเรื่องความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องที่เกิดจากการหักกลบรายการระหว่างธนาคาร (netting of interbank transactions) ข้อตกลงต่าง ๆ ในการหักกลบ (netting arrangements) อาจจะก่อให้เกิดการเปลี่ยนแปลงทางการเงินที่สำคัญ ๆ ซึ่งมีผลต่อตลาดระหว่างธนาคาร และยังเปลี่ยนแปลงความสัมพันธ์ระหว่างระบบต่าง ๆ และเกี่ยวกับการกำกับดูแลระบบการชำระเงินนอกประเทศ (offshore payment systems) ที่ค่อย ๆ วัฒนาการขึ้น

2.1 ประสิทธิภาพและความเสี่ยงของการหักกลบ (Efficiency and risks of netting) ปัจจัยต่าง ๆ ที่ช่วยกระตุ้นให้มีการลดความเสี่ยงเกี่ยวกับฐานะและการชำระเงินมีหลายประการคือ

- (1) ต้นทุนของรายการต่าง ๆ รวมทั้งค่าธรรมเนียมและค่าใช้จ่ายในการติดต่อสื่อสารในการชำระบัญชีรายการเกี่ยวกับเงินตราต่างประเทศ
- (2) เกิดจากนายธนาคารต่าง ๆ ตระหนักถึงการลดความเสี่ยงจากคู่สัญญามากขึ้น
- (3) เพื่อตอบสนองต่อเครื่องมือของ Basle Capital Agreement ที่กำลังจะนำมาใช้เพื่อลดภาระเกี่ยวกับเงินทุนซึ่งเกี่ยวข้องกับ credit exposures

กลไกต่าง ๆ สำหรับการหักกลบตามสัญญาและการชำระเงินระหว่างธนาคารสามารถก่อให้เกิดประสิทธิภาพในตลาดระหว่างธนาคารและกระบวนการชำระเงิน ประสิทธิภาพของข้อตกลงในการหักกลบ (netting arrangements) ไม่ได้ตัดสินจากการลดลงของค่าใช้จ่ายในการติดต่อสื่อสารเท่านั้น ยังต้องพิจารณาถึงความเสี่ยงของผู้ที่มีส่วนเกี่ยวข้องและความเสี่ยงเกี่ยวกับการเงินของระบบการธนาคารโดยรวมด้วย นอกจากนี้ การเปลี่ยนแปลงความเสี่ยงระหว่างคู่สัญญาและ cross borders ถ้าไม่มีการกำหนดไว้และทำความเข้าใจให้ชัดเจนแจ่มแจ้งแล้ว ข้อตกลงในการหักกลบระหว่างธนาคาร (interbank netting arrangements) อาจจะก่อให้เกิดความไม่แน่นอนโดยปิดบังข้อเท็จจริงเกี่ยวกับความเสี่ยง

ข้อตกลงในการหักกลบเป็นสาเหตุทำให้มีการเปลี่ยนแปลงความเสี่ยงซึ่งทำให้เกิดความยุ่งยากขึ้น ธนาคารในประเทศหนึ่งอาจจะพอใจกับประสิทธิภาพของต้นทุนเกี่ยวกับรายการต่าง ๆ ของตนที่ประหยัดได้ในขณะที่ระบบธนาคารของประเทศหนึ่งจะประสบกับความเสี่ยงเกี่ยวกับฐานะและสภาพคล่อง

ความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องเกิดขึ้นได้จากรูปแบบของการหักกลบที่แตกต่างกัน ซึ่งจะได้กล่าวถึงดังต่อไปนี้

1) **bilateral position netting** ลดความเสี่ยงเกี่ยวกับสภาพคล่องให้กับคู่สัญญา และบางทีก็ลดความเสี่ยงให้กับธนาคารตัวแทน (correspondent banks) เมื่อเทียบกับกรณีที่ไม่มีการหักกลบ (no netting) แต่คู่สัญญายังมีความเสี่ยงเกี่ยวกับฐานะไม่เปลี่ยนแปลงหรืออาจจะมีความเสี่ยงเพิ่มขึ้น ถ้าถือปฏิบัติต่อ net exposures ราวกับว่าเป็น true exposure

2) **bilateral netting by novation** ลดทั้งความเสี่ยงเกี่ยวกับสภาพคล่องและความเสี่ยงเกี่ยวกับฐานะให้กับคู่สัญญา และอาจเป็นไปได้ว่าในระบบการเงินด้วย (หรือสิ่งอื่น ๆ ที่เท่ากัน) เมื่อเทียบกับกรณี no netting และ bilateral position netting

3) **multilateral position netting** อาจลดความเสี่ยงเกี่ยวกับสภาพคล่องเมื่อเทียบกับกรณี no netting และ bilateral netting ถ้ามีการผิดสัญญาซึ่งมีนัยสำคัญเกิดขึ้น ความเสี่ยงเกี่ยวกับสภาพคล่องอาจจะสูงขึ้น ส่วนความเสี่ยงเกี่ยวกับฐานะจะเหมือนเดิมหรืออาจจะมากกว่าก็ได้กล่าวคือ ในกรณีของ no netting ความเสี่ยงเกี่ยวกับฐานะจะมากกว่าในกรณีของ bilateral netting by novation

4) **multilateral netting by novation and substitution** มีแนวโน้มว่าจะลดความเสี่ยงเกี่ยวกับสภาพคล่องมากกว่ารูปแบบอื่น ๆ แต่ขึ้นอยู่กับภาวะการเงินของคู่สัญญาที่เป็นศูนย์กลาง (central

counterparty) ในการหักกลบ ถ้า central counterparty มีสภาพคล่องอ่อนแล้ว ความเสี่ยงเกี่ยวกับสภาพคล่องก็อาจจะมากกว่าในกรณีของ bilateral netting by novation ส่วนความเสี่ยงเกี่ยวกับฐานะโดยทั่ว ๆ ไปจะน้อยกว่ารูปแบบอื่น ๆ ทั้งนี้ ขึ้นอยู่กับชื่อเสียงและฐานะของ central counterparty

ข้อสมมติฐานที่สำคัญ (Key assumption) ของข้อตกลงในการหักกลบจะต้องถูกต้องและใช้บังคับได้ตามกฎหมาย มิเช่นนั้นแล้วความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องจะมากกว่าปกติ ธนาคารกลางและผู้กำกับดูแลธนาคารจะต้องตรวจสอบการปฏิบัติงาน การเงิน กฎหมายและรายละเอียดอื่น ๆ ที่สร้างขึ้นมาในระบบ ทั้งนี้ เพื่อประเมินความเสี่ยงของระบบการหักกลบ

2.2 ประเด็นเกี่ยวกับนโยบายที่ขยายออกไป (Broader policy issues) ปัญหาด้านนโยบายเพิ่มเติมจะเกิดขึ้นโดยการพัฒนาและการปฏิบัติงานของระบบเหล่านี้

2.2.1 ในส่วนที่เกี่ยวข้องกับตัวเงิน (monetary implications)

ตามที่สัญญาการเงินจะมีการชำระกันด้วยตัวเงิน แต่ระบบการหักกลบจะใช้วิธีการชดเชยสัญญาหนึ่งกับอีกสัญญาหนึ่งแทน และมีการชำระเงินเฉพาะส่วนแตกต่างสุทธิเท่านั้น ระบบดังกล่าวเป็นการให้บริการประเภทหนึ่งเสมือนสื่อกลางในการเปลี่ยนแทนการชำระด้วยตัวเงิน การพัฒนาของข้อตกลงในการหักกลบ (netting arrangements) ก่อให้เกิดการเปลี่ยนแปลงทั้งเชิงปริมาณและคุณภาพในกระบวนการชำระเงินระหว่างธนาคาร การแพร่กระจายของข้อตกลงในการหักกลบอาจจะมีผลต่อการพัฒนาตลาดสินเชื่อระหว่างธนาคารรายวัน (intra-day interbank credit market) ยิ่งกว่านั้น ธนาคารกลางต้องมองถึงระบบการชำระเงินเพื่อที่จะประเมินปัญหาความมั่นคงและประสิทธิภาพของข้อตกลงเหล่านั้น

2.2.2 ในส่วนที่เกี่ยวข้องกับการเงิน (financial implications)

การพัฒนาอย่างกว้างขวางของสำนักหักบัญชีหรือข้อตกลงต่าง ๆ ของคู่สัญญาที่มีหลายฝ่ายที่คล้ายคลึงกันจะมีแนวโน้มที่จะเปลี่ยนแปลงโครงสร้างความสัมพันธ์ทางเครดิตระหว่างธนาคารที่สำคัญ ๆ ธนาคารจะทำการซื้อขายในตลาดล่วงหน้า เช่น ตลาดยูโรดอลลาร์ล่วงหน้า (Euro - dollar futures markets) แทนเรื่องอัตราดอกเบี้ยและอัตราแลกเปลี่ยนในเงินสดและเงินฝากธนาคาร โดยเป็นสิทธิเรียกร้องสุทธิต่อสำนักหักบัญชี

การพัฒนาของสำนักหักบัญชีของคู่สัญญาหลายฝ่าย (multilateral clearing house) สำหรับตลาดการแลกเปลี่ยนเงินตราต่างประเทศระหว่างธนาคารซึ่งเป็นตลาดที่มีลักษณะไม่เป็นทางการ (over-the-counter markets) จะมีผลต่อ credit exposures ในลักษณะเดียวกับการซื้อขายแลกเปลี่ยนอย่างเป็นทางการ (organised exchange trading) คู่สัญญารายสุดท้าย (ultimate counterparty) จะกลายเป็นสำนักหักบัญชี ซึ่งมี credit exposure และความเสี่ยงเกิดขึ้น

2.2.3 ในส่วนที่เกี่ยวข้องกับการกำกับดูแลและการตรวจตราของธนาคารกลาง (implications for supervision and central bank oversight)

ธนาคารกลางต้องแน่ใจว่าองค์กรธนาคารระหว่างประเทศมีการกำกับดูแลอย่างเพียงพอ โดย Basle Concordat กำหนดให้อยู่ในความรับผิดชอบของ home-country และ host country อย่างไรก็ตาม ยังมีข้อตกลงในการหักกลบระหว่างประเทศที่มีความยุ่งยากในการที่จะกำหนดว่าอยู่ในความรับผิดชอบของใคร ซึ่งบางครั้งอาจจะหลุดรอดจากการกำกับดูแลหรือตรวจตราโดยพนักงานเจ้าหน้าที่ได้ ปัญหามิดังนี้คือ

(1) ข้อตกลงในการหักกลบอย่างเป็นทางการและระบบการชำระเงินระหว่างประเทศจะแตกต่างจากองค์กรธนาคาร กล่าวคือ เป็นกลุ่มของธนาคารซึ่งมีความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องที่สัมพันธ์กันมีกฎเกณฑ์และวิธีปฏิบัติงานโดยทั่ว ๆ ไปสัมพันธ์กับระบบที่มีคู่สัญญาหลายฝ่ายจะก่อให้เกิดความเสี่ยงเกี่ยวกับระบบ (systemic risks) โดยมีการเปลี่ยนแปลงความเสี่ยงระหว่าง participants, providers และ settlement agent ซึ่งจำเป็นต้องพิจารณาว่าผู้กำกับดูแลควรจะตรวจสอบความเสี่ยงเกี่ยวกับฐานะ สภาพคล่องและการปฏิบัติงานของแต่ละระบบหรือไม่

(2) อาจจะมีปัญหาในการแบ่งความรับผิดชอบของผู้กำกับดูแลระหว่างประเทศ ประเทศต่าง ๆ ต่างก็มีส่วนได้ส่วนเสียในการดูแลตรวจตราความเสี่ยงประเภทต่าง ๆ ในเขตอำนาจของตน ธนาคารกลางของประเทศที่กำหนดให้หักบัญชีด้วยสกุลเงินของประเทศนั้น ต้องมีประสิทธิภาพและมั่นคง ข้อตกลงในการหักบัญชีที่มีเงินตราหลายสกุลจะมีประเทศที่เกี่ยวข้องหลายประเทศ หน้าที่ในการหักกลบตามข้อตกลงที่มีหลายฝ่ายนั้น อาจจะเป็นประเทศใด ๆ ก็ได้ และผู้มีส่วนเกี่ยวข้อง (participants) อาจเป็นธนาคาร สถาบันการเงินหรือบริษัทที่ไม่ได้ทำธุรกิจการเงิน ดังนั้น ส่วนงานและการแบ่งความรับผิดชอบของกรณีดังกล่าวจะมีปัญหาได้

(3) ปัญหาต่อไปก็คือ clearing house มีลักษณะคล้ายกับ clearing corporations ของตลาดหลักทรัพย์และตลาดแลกเปลี่ยนล่วงหน้า (organised securities และ futures exchanges) ดังนั้น บางประเทศอาจจะมีปัญหาในการกำกับดูแลคาบเกี่ยวกัน นอกจากนี้ ถ้ามาตรฐานและวิธีในการกำกับดูแลแตกต่างกันแล้ว จะส่งผลในการตรวจตราดูแลและเรื่องความเสี่ยงแตกต่างกันไปด้วย

2.2.4 บริการของธนาคารกลาง (Central Bank Services)

มีการเสนอให้ธนาคารกลางเป็นผู้ให้บริการในการชำระบัญชีตามข้อตกลงต่าง ๆ ซึ่งก่อให้เกิดประเด็นต่าง ๆ เช่น สิทธิตามกฎหมายของสำนักหักบัญชีที่จะได้รับบริการ การชำระบัญชีและการโอนบัญชีช่วงกลางคืน ฐานะของธนาคารกลางและการใช้หลักประกัน

3. ประเภทของความเสี่ยงทางการเงิน (Types of Financial Risk)

ผู้ที่มีส่วนเกี่ยวข้องทั้งระบบการหักบัญชี (clearing systems) และตลาดการเงิน (financial markets) จะมีความเสี่ยงทางการเงินอยู่ 3 ประเภท คือ

(1) **ความเสี่ยงเกี่ยวกับฐานะ (credit risk)*** เป็นความเสี่ยงที่คู่สัญญาไม่สามารถปฏิบัติตามสัญญาเมื่อครบกำหนด และไม่สามารถชำระได้ครบทั้งจำนวน เช่น กรณีคู่สัญญาฝ่ายใดฝ่ายหนึ่งล้มละลาย

(2) **ความเสี่ยงเกี่ยวกับสภาพคล่อง (liquidity risk)*** เป็นความเสี่ยงที่คู่สัญญารายหนึ่งหรือมากกว่านั้นไม่สามารถหักบัญชีหรือชำระบัญชี หรือชำระเงินเมื่อสัญญาครบกำหนดแล้ว ถึงแม้ว่าคู่สัญญาดังกล่าวจะมีสินทรัพย์หรือสินทรัพย์สุทธิเพียงพอ ตัวอย่างเช่น กรณีที่ไม่สามารถแปลงสภาพสินทรัพย์ให้เป็นเงินสดได้ซึ่งจะเกิดขึ้นเป็นกรณีชั่วคราว หรือมีความยุ่งยากในการปฏิบัติงานต่าง ๆ

ความเสี่ยงที่ไม่อาจหักบัญชีตามสัญญาของคู่สัญญาบางครั้งจะเรียกว่าความเสี่ยงในการชำระบัญชี (settlement risk) ความเสี่ยงดังกล่าวอาจเป็นความเสี่ยงเกี่ยวกับฐานะหรือความเสี่ยงเกี่ยวกับสภาพคล่องหรือทั้งสองอย่าง

(3) **ความเสี่ยงเกี่ยวกับระบบ (system or systemic risk)*** เป็นความเสี่ยงที่ผู้มีส่วนเกี่ยวข้องรายหนึ่งในระบบการจ่ายเงิน (payment system) หรือตลาดการเงิน (financial markets) ไม่สามารถปฏิบัติตามสัญญาเมื่อครบกำหนดและเป็นสาเหตุให้ผู้มีส่วนเกี่ยวข้องรายอื่น ๆ ไม่อาจปฏิบัติตามสัญญาเมื่อครบกำหนด

4. ตลาดสำหรับข้อตกลงในการหักกลบลบหนี้ (The Market for Netting Arrangements)

ธนาคารและกิจการต่าง ๆ ที่เข้ามาทำข้อตกลงในการหักกลบลบหนี้ในเรื่องของสัญญาที่เกี่ยวข้องกับการจ่ายหรือรับเงินตราต่างประเทศ มีจุดมุ่งหมายแตกต่างกัน 4 ประการคือ

(1) ลดจำนวนข่าวสารในการชำระเงิน (payment messages) ที่จะต้องแลกเปลี่ยนกันระหว่างคู่สัญญากับธนาคารตัวแทนในประเทศที่เกี่ยวข้องกับเงินตราสกุลนั้น ๆ จุดมุ่งหมายประการนี้ก็เพื่อต้องการลดต้นทุนในการส่งข่าวสาร ต้นทุนการปฏิบัติงาน และโอกาสที่จะเกิดข้อผิดพลาดโดยธนาคารตัวแทน ทั้งยังก่อให้เกิดการตรวจสอบและมีการกระทบบยอดกันอย่างคร่าว ๆ ด้วย

(2) ลดความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องของคู่สัญญา

(3) ลดความต้องการที่จะต้องดำรงสภาพคล่องระหว่างวันหรือสินเชื่อที่จะใช้ในการประสานช่องว่างของเวลา (timing gaps) ระหว่างยอดเงินที่จะต้องจ่ายและยอดเงินที่จะต้องรับเบื้องต้น

(4) เป็นเครื่องมือของ Basle Capital Agreement

ความต้องการให้มีการหักกลบลบหนี้ดังกล่าว ทำให้ต้องนำเอาเทคโนโลยีในการให้ข้อมูลข่าวสารมาใช้ไม่ว่าจะเป็นเครือข่ายระหว่างธนาคาร เครื่องคอมพิวเตอร์ การติดต่อสื่อสาร การส่งข้อมูล การชำระเงิน ต้องมีระบบอัตโนมัติ ระบบการประมวลผลน่าเชื่อถือได้ และส่งข้อมูลได้ทันเวลา

5. รูปแบบตามกฎหมายของการหักกลบลบหนี้ (Legal Forms of Netting)

การหักกลบลบหนี้ที่มีรูปแบบต่าง ๆ ตามกฎหมายสามารถนำไปประยุกต์ใช้กับรายการเกี่ยวกับการเปลี่ยนเงินตราต่างประเทศ ไม่ว่าจะเป็น spot หรือ forward และสัญญาทางการเงินและการชำระเงินในรูปแบบต่าง ๆ

5.1 position netting* เป็นรูปแบบการหักกลบลบหนี้เงินตราแต่ละสกุลและจำนวนเงินที่ครบกำหนดโดยธนาคารสองแห่งทำข้อตกลงกันอย่างไม่เป็นทางการในอันที่จะชำระกันด้วยยอดสุทธิเพียงยอดเดียวอาจจะเรียกว่า payments netting หรือ bulking of payments ความเสี่ยงเกี่ยวกับฐานะระหว่างคู่สัญญายังคงไม่เปลี่ยนแปลงเพราะไม่มีการเปลี่ยนแปลงในตัวสัญญา คู่สัญญายังคงต้องผูกพันกันตามกฎหมายตามยอดเงินจำนวนเดิม แต่จะลดจำนวนข้อมูลข่าวสารในการชำระบัญชี และจำนวนเงินที่จะต้องชำระบัญชีในแต่ละรายการ

5.2 netting by novation* ลดความเสี่ยงเกี่ยวกับฐานะของคู่สัญญาโดยผลจากการปฏิบัติตามสัญญาแลกเปลี่ยนเงินตราต่างประเทศแต่ละสัญญาหรือสัญญาอื่น ๆ ที่มีการหักกลบลบหนี้อาจเรียกว่า obligation netting/netting by novation มีจุดประสงค์ที่จะให้มีการปฏิบัติตามจุดมุ่งหมายตามที่กล่าวไว้ในข้อ 4 โดยเฉพาะอย่างยิ่งต้องการลดความเสี่ยงเกี่ยวกับสภาพคล่องทั้งของคู่สัญญาและธนาคารตัวแทน พร้อมทั้งลดความเสี่ยงเกี่ยวกับฐานะของคู่สัญญา ทั้งนี้ ต้องขึ้นอยู่กับความสามารถบังคับได้ตามกฎหมายของ novated net contract ที่เข้ามาแทนที่สัญญาเดิม

โดยเนื้อแท้แล้ว netting by novation เป็นกลไกที่ใช้กับคู่สัญญาสองฝ่ายแต่ก็สามารถดำเนินการโดยมีหลาย ๆ ฝ่ายได้ภายในกลุ่มธนาคารขนาดใหญ่ ในกรณีต้องใช้บริการจากฝ่ายที่สามในรูปของสำนักบัญชี โดยดำเนินการตามสัญญาในฐานะเหมือนกับคู่สัญญาของธนาคารที่เกี่ยวข้องแต่ละธนาคาร กระบวนการนี้อาจเรียกได้ว่าเป็น novation and substitution*

5.3 netting by close-out* เป็นวิธีการปฏิบัติเกี่ยวกับสัญญาในอนาคต (future obligations) ระหว่างธนาคารสองแห่งเมื่อมีเหตุการณ์ใดที่กำหนดไว้เกิดขึ้น เช่น มีการแต่งตั้งผู้พิทักษ์ทรัพย์หรือผู้ชำระบัญชีเกิดขึ้น เมื่อมีการปิดกิจการ สิ่งที่จะต้องทำคือคำนวณค่าปัจจุบันของจำนวนเงินที่จะครบกำหนดในอนาคตระหว่างคู่สัญญาในวันนั้นแล้วคำนวณให้อยู่ในรูปของเงินตราสกุลหลักเพื่อที่จะให้มียอดเงินเพียงยอดเดียวที่จะต้องจ่ายหรือได้รับจากธนาคารที่ปิดกิจการไปแล้ว ซึ่งผู้พิทักษ์ทรัพย์และผู้ชำระบัญชีผูกพันตนที่จะจ่ายเพื่อให้มีการปฏิบัติตามสัญญาที่ค้างชำระระหว่างธนาคารทั้งสองแห่ง บทบัญญัติในเรื่อง close-out ใช้ได้ทั้งในกรณีที่มีคู่สัญญาสองฝ่ายหรือหลาย ๆ ฝ่ายได้

จะมีการปฏิบัติโดยวิธี netting by close-out ต่อเมื่อมีเหตุการณ์ใดเหตุการณ์หนึ่งเกิดขึ้น ดังนั้น จึงไม่มีผลกระทบต่อจำนวนข่าวสารในการชำระเงิน ความเสี่ยงเกี่ยวกับสภาพคล่องหรือความเสี่ยงเกี่ยวกับฐานะของธนาคารตัวแทนของคู่สัญญา

6. รูปแบบต่าง ๆ ที่จัดสร้างขึ้นจากการศึกษาเรื่องการหักกลบและความเสี่ยง (The Institutional forms of Netting Studies and Their Risks)

คณะทำงานได้ศึกษาข้อตกลงในการหักกลบระหว่างธนาคาร (interbank netting arrangements) ที่มีอยู่และที่เสนอไว้สำหรับใช้ในสัญญาแลกเปลี่ยนเงินตราและการชำระเงินตราต่างประเทศ ลักษณะความเสี่ยงของข้อตกลงต่าง ๆ ที่ทำการศึกษาสามารถแบ่งออกได้เป็น 4 ประเภท ซึ่งจะแตกต่างกันไป ขึ้นอยู่กับว่าเป็นลักษณะของคู่สัญญาสองฝ่ายหรือหลายฝ่าย ลักษณะทางกฎหมายของจำนวนเงินสุทธิที่ครบกำหนดแล้ว และคู่สัญญาที่เป็นศูนย์กลาง (central counterparty) ที่มีอยู่ รูปแบบต่าง ๆ ทั้ง 4 ประเภท คือ

- bilateral position netting
- bilateral netting by novation
- multilateral position netting
- multilateral netting by novation and substitution

นอกจากนี้ ยังมีข้อตกลงที่เรียกว่า no netting ซึ่งใช้เป็นมาตรฐานเปรียบเทียบกับความเสี่ยงเกี่ยวกับฐานะและสภาพคล่องของระบบการหักกลบที่แตกต่างกัน ในกรณีของ no netting จะมีข้อสมมติฐานว่าสัญญาเดิมจะยังคงค้างอยู่จนกว่าจะครบกำหนดและมีการปฏิบัติตามสัญญาให้ลุล่วงไปโดยการชำระบัญชี

6.1 bilateral position netting

ด้วยความพยายามที่จะลดจำนวนรายการในการชำระระหว่างคู่สัญญา จึงมีข้อตกลงในการหักกลบเกี่ยวกับการแลกเปลี่ยนเงินตราต่างประเทศอย่างไม่เป็นทางการในรูปแบบต่าง ๆ ในศูนย์กลางทางการเงิน ซึ่งวิธี bilateral position netting ก็เป็นวิธีหนึ่ง โดยธนาคารคู่สัญญาสองฝ่ายคำนวณจำนวนเงินสุทธิที่ครบกำหนดจากสัญญาแลกเปลี่ยนเงินตราต่างประเทศและชำระกันด้วยยอดสุทธิ ในกรณีที่คู่สัญญาฝ่ายใดฝ่ายหนึ่งประสบปัญหาทางการเงินแล้ว กฎหมายและชำระกันด้วยยอดสุทธิ ในกรณีที่คู่สัญญาฝ่ายใดฝ่ายหนึ่งประสบปัญหาทางการเงินแล้ว กฎหมายก็ไม่ได้ระบุไว้ชัดเจนว่าจะต้องชำระหนี้สินกันด้วยจำนวนเดิมหรือจำนวนสุทธิ แต่ข้อสมมติฐานที่ใช้กันอย่างกว้างขวางนั้น คู่สัญญาต้องรับผิดชอบต่อจำนวนเดิมถ้ามีปัญหาดังกล่าวเกิดขึ้น

6.2 bilateral netting by novation

การหักกลบตามวิธีนี้จะมีประสิทธิภาพคล้ายคลึงกับ bilateral position netting แม้ว่าต้นทุนในการพัฒนาและการเจรจาต่อรองในการทำข้อตกลงจะสูงก็ตาม แต่จะลดความเสี่ยงเกี่ยวกับฐานะเมื่อเทียบกับ position netting หรือ no netting

6.3 multilateral position netting

การหักกลบดังกล่าวจะพบในระบบคู่สัญญาที่มีหลายฝ่าย โดยมีการติดต่อสื่อสารและข้อตกลงต่าง ๆ ทางบัญชีเป็นพิเศษ ตัวแทนในการหักบัญชีหรือชำระบัญชี (clearing or settlement agent) อาจจะเป็นบัญชี “clearing accounts” ให้กับผู้ที่มีส่วนเกี่ยวข้องเพื่อให้มียอดเงินในบัญชีหรือจัดหาสินเชื่อให้กับผู้มีส่วนเกี่ยวข้องเพื่อที่จะเกิดความสะดวกในการชำระบัญชี สำคัญสำคัญของ multilateral netting ก็คือ คำนวณจำนวนเงินสุทธิของแต่ละคน

จะต้องชำระหรือได้รับเมื่อเปรียบเทียบกับทั้งกลุ่ม แล้วโอนจากฝ่ายที่เป็นลูกหนี้สุทธิ (net debtors) ไปให้กับเจ้าหนี้สุทธิ (net creditors)

ถ้าธนาคารที่มียอดเป็นลูกหนี้สุทธิไม่สามารถชำระบัญชีได้ กฎเกณฑ์ระบบอนุญาตให้มีการผ่อนคลาย (unwinding) การชำระเงินให้กับหรือได้รับจากผู้มีส่วนเกี่ยวข้องที่มีปัญหาเพื่อให้มีการปฏิบัติตามสัญญา และสามารถชำระบัญชีกันในวันอื่นนับจากวันที่ครบกำหนดเดิม

multilateral position netting มีความเสี่ยงเกี่ยวกับฐานะเช่นเดียวกับกรณีของ no netting เนื่องจากสัญญาเดิมยังคงมีผลอยู่ สำหรับความเสี่ยงเกี่ยวกับสภาพคล่องเป็นปัญหาที่ยุ้งยากมากต้องมีการคำนวณจำนวนเงินสุทธิที่จะต้องชำระแก่กันของคู่สัญญาสองฝ่ายเมื่อได้ฐานะของคู่สัญญาทั้งสองฝ่าย (bilateral position) แล้ว ซึ่งไม่ว่าจะเป็นบวกหรือเป็นลบก็ตาม จะต้องนำไปคำนวณหาจำนวนเงินสุทธิจากคู่สัญญาขึ้นมาให้เหลือเพียงยอดเดียว (multilateral net amount) ซึ่งต้องชำระหรือได้รับจากกลุ่ม ถ้าผู้มีส่วนเกี่ยวข้องคนใดคนหนึ่ง ไม่สามารถชำระบัญชีตามฐานะที่ตนเองมีอยู่ได้ ก็ต้องมีการคำนวณ multilateral position กันใหม่ เพราะผู้มีส่วนเกี่ยวข้องรายที่ผิดสัญญา มียอดเจ้าหนี้สุทธิก็ไม่มีเงินที่จะมาชำระให้กับรายอื่น ๆ ตาม multilateral net settlement obligation ทำให้เกิดปัญหาด้านสภาพคล่องเพิ่มขึ้น ซึ่งจะมีผลต่อฐานะทางการเงินของผู้มีส่วนเกี่ยวข้องเหล่านี้

ปัญหาด้านสภาพคล่องอาจจะเกิดขึ้นได้อีกทางหนึ่งจากผลของความยุ่งยากในการปฏิบัติงาน เช่น ตัวแทนในการชำระบัญชี (settlement agent) ของ multilateral position netting system อาจจะไม่เต็มใจหรือไม่สามารถชำระบัญชีให้กับเจ้าหนี้สุทธิได้จนกว่าจะได้รับชำระจากลูกหนี้สุทธิ ความล่าช้าที่เกิดจากกรณีลูกหนี้สุทธิดังกล่าวเพียงรายเดียวก่อให้เกิดปัญหากับเจ้าหนี้สุทธิทุก ๆ ราย และอาจจะมีผลกระทบต่อการชำระบัญชีที่ครบกำหนดแล้วในตลาดอื่น ๆ หรือต่อทั้งระบบได้

6.4 multilateral netting by novation and substitution

อาจจะต้องมีการจัดตั้งสำนักหักบัญชีแห่งชาติ (national clearing houses) ขึ้น เพื่ออนุญาตให้ผู้ที่มีส่วนเกี่ยวข้องดำเนินการหักกลบสัญญาเกี่ยวกับการแลกเปลี่ยนเงินตราต่างประเทศกับรายอื่น ๆ โดยให้มีผลบังคับใช้ตามกฎหมายได้ เมื่อมีการส่งมอบสัญญาของคู่สัญญาสองฝ่าย สำนักหักบัญชีจะดำเนินการแทนเสมือนเป็นคู่สัญญาของแต่ละฝ่าย และถือว่าสัญญาเดิมระหว่างสองฝ่ายมีการปฏิบัติตามแล้ว สำนักหักบัญชียังทำการคำนวณ net position ในรูปของสกุลเงินที่เกี่ยวข้อง และวันครบกำหนดของผู้มีส่วนเกี่ยวข้องแต่ละรายอีกด้วย กระบวนการดังกล่าวนี้เป็นผลให้มีการหักกลบสัญญาต่าง ๆ ให้เหลือเพียงจำนวนเงินสุทธิที่จะต้องชำระให้กับสำนักหักบัญชีหรือได้รับจากสำนักหักบัญชี ซึ่งเป็น multilateral net position ของผู้มีส่วนเกี่ยวข้องแต่ละรายเมื่อเปรียบเทียบกับทั้งกลุ่ม

สำนักหักบัญชีซึ่งอยู่ในฐานะคู่สัญญาที่เป็นศูนย์กลาง (central counterparty) จึงมีความเสี่ยงเกี่ยวกับฐานะและสภาพคล่อง จึงต้องมีการบริหารความเสี่ยงโดยเรียกหลักประกันจากผู้มีส่วนเกี่ยวข้องทุกรายและปฏิเสธสัญญาที่มีหลักประกันไม่เพียงพอได้ ในการลดความเสี่ยงเกี่ยวกับฐานะจะต้องมีการทำข้อตกลงไว้ให้ครอบคลุม multilateral netting by novation and substitution เพราะถ้าข้อตกลงเหล่านี้ไม่ถูกต้องแล้ว ความเสี่ยงเกี่ยวกับฐานะก็จะสูงกว่ากรณีของ no netting

ผลของ multilateral netting by novation and substitution ต่อความเสี่ยงเกี่ยวกับสภาพคล่องยังไม่ชัดเจนเมื่อเทียบกับกรณี bilateral netting by novation จำนวนเงินสุทธิที่ครบกำหนดแล้วจะลดลงหรือไม่เปลี่ยนแปลงสำหรับผู้มีส่วนเกี่ยวข้องบางรายเมื่อเทียบกับกรณี bilateral netting วิธีนี้จะลดความเสี่ยงเกี่ยวกับสภาพคล่องให้กับผู้มีส่วนเกี่ยวข้องเป็นราย ๆ ไป เมื่อมีการหักกลบกับกลุ่มทั้งหมด และอาจจะลดให้กับตลาดการเงินโดยทั่ว ๆ ไป หรือกล่าวอีกนัยหนึ่งคือข้อตกลงของสำนักหักบัญชีจะต้องเป็นศูนย์กลางในการชำระบัญชีทุกรายการ ในกรณีที่ผู้มีส่วนเกี่ยวข้องรายใดรายหนึ่งไม่สามารถชำระบัญชีได้ก็จะก่อให้เกิดความขาดแคลนเงินสดในเงินสกุลใดสกุลหนึ่งหลาย ๆ สกุลเงินจำเป็นต้องทำการชำระบัญชีความเสี่ยงเกี่ยวกับสภาพคล่องของผู้มีส่วนเกี่ยวข้องรายอื่น ๆ ขึ้นอยู่กับความสามารถของสำนักหักบัญชีว่าหาเงินมาชำระบัญชีได้อย่างไร ดังนั้น การที่มีคู่สัญญาหลายฝ่ายก็ไม่ก่อให้เกิดความมั่นใจได้ว่าจะมีความเสี่ยงเกี่ยวกับสภาพคล่องน้อยกว่ากรณี bilateral netting by novation โดยข้อเท็จจริงแล้วอาจจะสูงกว่า และในกรณีความเสี่ยงเกี่ยวกับสภาพคล่องของทั้งระบบ (systemic liquidity risk) ก็สามารถสรุปได้ในลักษณะคล้าย ๆ กัน

สมาชิกและโครงสร้างเงินทุนของสำนักหักบัญชีจะก่อให้เกิดความเสี่ยงที่สำคัญได้ เมื่อก่อตั้งขึ้นมาแล้วจะต้องขยายจำนวนสมาชิกให้มีจำนวนมากเพื่อให้เกิดความประหยัดและลดต้นทุนเฉลี่ยต่อหน่วยของการลง อย่างไรก็ตาม การเพิ่มจำนวนของสมาชิกให้มากขึ้น อาจจะได้สมาชิกที่มีฐานะไม่ดี ซึ่งจะมีผลต่อฐานะและสภาพคล่องของสำนักหักบัญชี รวมทั้งคุณภาพของข้อตกลงเกี่ยวกับการแบ่งความเสียหายในระหว่างคู่สัญญา

7. ภาพทั้งหมดของความเสี่ยงเกี่ยวกับสภาพคล่อง

(A Global Perspective on Liquidity Risk)

การเกิดขึ้นของ foreign exchange and other clearing house arrangements จะขยายขอบเขตการใช้ netting facilities ที่มีอยู่ และมีศูนย์กลางที่ใดที่หนึ่งไปยังตลาดระหว่างประเทศที่สำคัญ ๆ ดังนั้น จึงจำเป็นต้องสอบทานโครงสร้างทั้งหมดของการชำระบัญชีสำหรับระบบการชำระเงินนอกประเทศ (offshore payment systems) และข้อตกลงในการหักกลบต่าง ๆ ที่อาจจะเกิดขึ้นในภายหน้า พร้อมทั้งต้องเน้นในเรื่องปัญหาทั้งหมดของความเสี่ยงเกี่ยวกับสภาพคล่อง คณะทำงานได้ชี้ให้เห็นถึงประเด็นที่ควรพิจารณา 4 ประเด็น ดังนี้

- (1) ผลกระทบของการหักกลบ ในเรื่องความเสี่ยงเกี่ยวกับสภาพคล่องของข้อตกลงทั้งที่มีคู่สัญญาสองฝ่ายและคู่สัญญาหลายฝ่าย พร้อมทั้งธนาคารตัวแทน
- (2) บทบาทของ settlement agent ใน multilateral systems และการแบ่งความเสี่ยงเกี่ยวกับสภาพคล่องระหว่าง settlement agent และ participants
- (3) การปรับใช้ระหว่างประเทศของความเสี่ยงเกี่ยวกับสภาพคล่องในข้อตกลงในการหักบัญชีระหว่างประเทศ โดยเฉพาะอย่างยิ่งในเรื่องของการกำหนดความเสี่ยงระหว่างประเทศระหว่าง settlement agent และ participants
- (4) ผลกระทบของ centralised multi-currency clearing house arrangements ต่อความเสี่ยงเกี่ยวกับสภาพคล่องทั่วไปของตลาด

7.1 impact of netting arrangements

โดยทั่ว ๆ ไปแล้วจะลดความเสี่ยงเกี่ยวกับสภาพคล่องสำหรับธนาคารตัวแทนและอื่น ๆ ที่เกี่ยวข้องกับกระบวนการชำระหนี้ เพราะลดจำนวนเงินที่ครบกำหนดจะต้องมีการชำระบัญชีกันโดยใช้ยอดสุทธิหลังจากหักกลบ ถ้าไม่มีการหักกลบแล้ว กรณีจะเป็นดังนี้คือ ธนาคารตัวแทนแห่งหนึ่งอาจจะได้รับคำสั่งให้ชำระหนี้จากธนาคารของลูกค้าในระหว่างวันให้มีการส่งมอบเงินเข้าบัญชีของธนาคารตัวแทนแห่งที่สอง ในกรณีเช่นเดียวกันธนาคารตัวแทนแห่งที่สองอาจจะได้รับคำสั่งให้ส่งมอบเงินเข้าบัญชีในธนาคารตัวแทนแห่งแรก ซึ่งในการปฏิบัติแล้วธนาคารตัวแทนทั้งสองแห่งมีความไม่แน่นอนเกี่ยวกับเวลาและจำนวนเงินที่ต้องมาชดเชยกัน ซึ่งมีความเสี่ยงเกี่ยวกับฐานะเงินสดหรือฐานะสภาพคล่องในแต่ละวัน แต่ในกรณีของ bilateral netting และ multilateral netting ก่อให้เกิดความมั่นใจว่าการชำระหนี้เพื่อชดเชยกันจะกระทำพร้อม ๆ กัน ซึ่งจะกำจัดความเสี่ยงเกี่ยวกับสภาพคล่องให้กับธนาคารตัวแทน

7.2 rule of settlement agent and allocation of liquidity risk

บทบาทของ settlement agent ก็คือ รับจากลูกหนี้สุทธิในการหักกลบและจ่ายให้กับเจ้าหนี้สุทธิ นอกจากนี้ยังมีหน้าที่อื่น เช่น ให้สินเชื่อเพื่อสนับสนุนทางการเงินในการชำระบัญชี และเก็บรักษาหลักประกัน ติดตามรายการที่มีปัญหาในการปฏิบัติงานและทางการเงินในบางเรื่อง settlement agent อาจจะกลายมาเป็นผู้วางกฎระเบียบ (regulator) ของ multilateral netting arrangement โดยเฉพาะอย่างยิ่งถ้ารับผิดชอบ ในการกำหนดเงื่อนไขต่าง ๆ ตามข้อตกลงและยอมรับสัญญาที่จะมาทำการหักกลบ

การแบ่งความเสี่ยงเกี่ยวกับสภาพคล่องระหว่าง settlement agent และ participants ขึ้นอยู่กับหน้าที่ต่าง ๆ ของธุรกิจการธนาคาร (banking functions) ที่มอบหมายให้กับ settlement agent ในแง่หนึ่ง settlement agent อาจจะไม่ต้องรับความเสี่ยงเกี่ยวกับสภาพคล่องเลย โดยแบ่งความเสี่ยงให้กับ participants ในระบบ ในอีกแง่หนึ่ง settlement agent ต้องรับภาระความเสี่ยงเกี่ยวกับสภาพคล่องในการชำระบัญชีทั้งหมด เช่น กรณีที่มีการชำระบัญชีให้กับเจ้าหนี้สุทธีก่อนที่จะได้รับจากลูกหนี้สุทธิในการหักบัญชีซึ่งเป็นลักษณะชั่วคราว กรณีนี้ต้องรับความเสี่ยงเกี่ยวกับสภาพคล่องทั้งหมด

ระบบที่เกี่ยวข้องกับต่างประเทศ (offshore systems) จะมีปัญหาในการบริหารสภาพคล่อง อันเนื่องมาจากเวลาที่แตกต่างกัน เวลาในการชำระบัญชีอาจจะเป็นตอนกลางคืนหรือตอนรุ่งเช้าของประเทศอื่น ผู้บริหารที่เกี่ยวข้องก็ไม่อาจให้คำปรึกษาหรือตัดสินใจในการแก้ไขปัญหาด้านสภาพคล่อง ซึ่งอาจทำให้การชำระบัญชีไม่ทันเวลา บุคลากรของธนาคารกลางในบางประเทศก็อาจจะมีไม่พร้อม

7.3 cross-border implications of liquidity risk in offshore clearing arrangements

อาจจะต้องมีการนำความเสี่ยงเกี่ยวกับสภาพคล่องในข้อตกลงระหว่างประเทศมาปรับใช้ ปัญหาต่าง ๆ ขึ้นอยู่กับการชำระบัญชี ถ้าการชำระบัญชีสำหรับ offshore system ใช้ยอดสุทธิจากการหักกลบในประเทศที่ใช้สกุลเงินตราประเทศนั้นชำระบัญชี (country that issues the settlement currency) หรือเรียกว่า country of issue ถ้ามีปัญหาด้านสภาพคล่องที่ทำให้การชำระบัญชีล่าช้าใน country of issue ก็จะทำให้การชำระบัญชีใน offshore system พลอยล่าช้าไปด้วย

ถ้าการชำระบัญชีใน offshore system กระทำผ่านธนาคารตัวแทนหรือระบบการชำระเงินที่ดำเนินการโดยเอกชนใน country of issue แล้ว ความเสี่ยงเกี่ยวกับสภาพคล่อง อาจจะตกอยู่กับระบบการธนาคารของเอกชนในประเทศนั้น แต่ถ้าธนาคารกลางเป็นผู้ให้บริการชำระบัญชี cross-border ใน offshore systems แล้ว ความเสี่ยงเกี่ยวกับสภาพคล่องจะย้ายไปอยู่ที่ธนาคารกลางอย่างไรก็ตาม ถ้าธนาคารกลางหรือธนาคารตัวแทนในประเทศที่มีการชำระบัญชีใน offshore system ความเสี่ยงเกี่ยวกับสภาพคล่องก็จะอยู่ในประเทศนั้น

7.4 centralised multi-currency clearing houses

ระบบดังกล่าวพัฒนามาจากตลาดการแลกเปลี่ยนเงินตราต่างประเทศแบบดั้งเดิม โดยมีปัญหาเกี่ยวกับโครงสร้างการชำระบัญชีระหว่างประเทศ และความเสี่ยงเกี่ยวกับสภาพคล่องเพิ่มเข้ามา ซึ่งจะเกิดขึ้นมาจากระบบการหักบัญชีของ currency futures และ currency options

สำนักหักบัญชีจะเปรียบเสมือนกับเป็น settlement agent สำหรับข้อตกลงในการหักบัญชี ถ้าทำหน้าที่ทั้งรับและจ่ายในการชำระบัญชี ยิ่งกว่านั้นสำนักหักบัญชียังเป็นผู้กลางของสัญญาแลกเปลี่ยนเงินตราต่างประเทศ ต้องรับภาระความเสี่ยงเกี่ยวกับสภาพคล่องเป็นรายแรก

ข้อเสนอให้มีการชำระบัญชีสัญญาแลกเปลี่ยนเงินตราต่างประเทศโดยกระทำผ่านสำนักหักบัญชีนั้นเกิดขึ้นจากประเด็นเกี่ยวกับสภาพคล่องที่สำคัญ ๆ อย่างน้อย 3 ประเด็นด้วยกันคือ

(1) การพัฒนาของสถาบันการเงินที่เป็นศูนย์กลางขนาดใหญ่ที่เกิดขึ้นมาใหม่ ๆ (new largescale central financial institutions) ก่อให้เกิดปัญหาเกี่ยวกับเรื่อง ความสัมพันธ์ทางการเงินระหว่างธนาคารและสถาบันการเงินดังกล่าว เดิมทีนั้นความเสี่ยงเกี่ยวกับสภาพคล่องเกิดขึ้นจากธนาคารตัวแทนกลุ่มใหญ่ ๆ กลุ่มหนึ่งในสถาบันการเงินซึ่งธนาคารและตลาดระหว่างประเทศเข้ามาเกี่ยวข้อง จะทำให้สำนักหักบัญชีมีความสำคัญมากขึ้นไปในการทำหน้าที่เป็นตลาดการเงินซึ่งย่อมมีความล้มเหลวเกิดขึ้น

(2) สำนักหักบัญชีจะเผชิญกับความเสี่ยงเกี่ยวกับสภาพคล่องที่เป็น cross-currency แม้ว่ายอดที่ต้องชำระให้กับเจ้าหนี้ด้วยเงินตราสกุลหนึ่งสามารถชดเชยกับยอดที่จะได้รับจากลูกหนี้ด้วยเงินตราอีกสกุลหนึ่งได้ครบถ้วนทั้งจำนวน ถ้าฝ่ายใดฝ่ายหนึ่งผิดสัญญาสำนักหักบัญชีที่มีส่วนเกินหรือหลักประกันอาจจะป้องกันความเสี่ยงเกี่ยวกับฐานะได้ อย่างไรก็ตาม สำนักหักบัญชีจะประสบปัญหาสภาพคล่องชั่วคราวถ้าเงินตราสกุลที่จะต้องจ่ายนั้นไม่มีสภาพคล่องพอที่จะชำระบัญชีตามสัญญากับเงินตราสกุลอื่น ๆ ได้ทันเวลา

(3) เป็นปัญหาจากกรณีของธนาคาร Herstatt เช่น สำนักหักบัญชีอาจจะเลือกที่จะชำระบัญชีเงินตราแต่ละสกุลในวันที่ครบกำหนดเร็วที่สุดเท่าที่จะทำได้ ซึ่งจะทำให้ลำดับการชำระบัญชีย้ายจากเวลาหนึ่งไปยังอีกเวลาหนึ่ง สำนักหักบัญชีไม่จำเป็นต้องตัดผลที่มีต่อสภาพคล่องของธนาคารที่ปิด ในขณะที่อีกฝ่ายหนึ่งยังไม่มีภาระชำระบัญชีตามสัญญาแลกเปลี่ยนเงินตราต่างประเทศ การวิเคราะห์เช่นนี้ชี้ให้เห็นว่าทั้งสำนักหักบัญชีและ participants ต่าง ๆ ต้องบริหารสภาพคล่องของเงินตราหลาย ๆ สกุลเงินและหลักประกันอย่างระมัดระวัง

ถ้าสำนักหักบัญชีต้องทำการชำระบัญชีผ่านสถาบันการเงินใดแล้ว ก็จะมีเรื่อง settlement agent เข้ามาเกี่ยวข้อง โดยมีธนาคารตัวแทนหนึ่งธนาคารหรือมากกว่านั้นกระทำการเป็น settlement agent ของเงินตราแต่ละสกุล ถ้าธนาคารเหล่านี้ผิดสัญญาแล้วจะทำให้สำนักหักบัญชีมีปัญหาสภาพคล่องและความเสี่ยงอื่น ๆ และกับ participants ทุกรายด้วย

มีบางท่านเสนอว่าให้ธนาคารกลางกระทำการเป็น settlement agent ให้กับสำนักหักบัญชีโดยเฉพาะที่เป็นธนาคารพาณิชย์ ซึ่งก่อให้เกิดปัญหาต่าง ๆ ขึ้น เช่น

- ธนาคารต้องเปิดบัญชีให้กับสำนักหักบัญชีหรือ participant ซึ่งไม่มีตัวตนอยู่ในประเทศของธนาคารกลางนั้นหรือไม่?
- ธนาคารกลางต้องขยายเวลาในการปฏิบัติงานเพื่ออำนวยความสะดวกให้กับสำนักหักบัญชีในการชำระบัญชีหรือไม่?
- จะมีผลอะไรต่อตลาดทุนในประเทศในกรณีที่มีการขยายระยะเวลาในการปฏิบัติงาน?
- จะต้องมียุทธศาสตร์ผูกพันเพื่อให้การสนับสนุนทางการเงินสำนักหักบัญชีหรือไม่?
- ธนาคารกลางจะต้องเป็นผู้รักษาลูกประกันที่ participants จำนองไว้กับธนาคารหรือไม่?
- ลูกประกันดังกล่าวสามารถนำไปแปรสภาพให้เป็นสภาพคล่อง แล้วนำไปใช้ในการชำระบัญชีเงินตราสกุลอื่นซึ่งเกี่ยวข้องกับธนาคารกลางอื่น ๆ ได้หรือไม่?

ทางเลือกอีกทางหนึ่งคือ ธนาคารพาณิชย์เป็น settlement agents ให้กับสำนักหักบัญชี ซึ่งก่อให้เกิดประเด็นต่าง ๆ ให้กับผู้กำกับดูแลและธนาคารกลางของธนาคารต่าง ๆ และเงินตราสกุลต่าง ๆ ที่เกี่ยวข้อง ธนาคารเหล่านั้นจะมีความเสี่ยงเกี่ยวกับสภาพคล่อง ซึ่งเกี่ยวพันกับการชำระเงินของธนาคารผ่านระบบการชำระเงินภายในประเทศ โดยเฉพาะอย่างยิ่งถ้าข้อตกลงของสำนักหักบัญชีมีแนวโน้มที่จะผ่อนคลาย (unwind) ฐานะสุทธิประจำวันของ participants

ในที่สุดจะต้องพิจารณาถึงความเกี่ยวพันของสำนักหักบัญชีเกี่ยวกับการแลกเปลี่ยนเงินตราต่างประเทศในประเทศต่าง ๆ โดยปกติแล้วจะต้องเชื่อมโยงสำนักหักบัญชีเข้าด้วยกัน เพื่อบริการรายการ cross-border foreign exchange transactions และเพื่อให้ได้ประโยชน์จากการหักกลบ อย่างไรก็ตาม ความเสี่ยงเกี่ยวกับสภาพคล่องของระบบที่เกิดจากการเชื่อมโยงนี้จะต้องมีการประเมินอย่างระมัดระวัง ถ้าสำนักหักบัญชีแห่งใดแห่งหนึ่งในระบบที่เชื่อมโยงกันประสบปัญหาเกี่ยวกับสภาพคล่องแล้ว ก็มีทางเป็นไปได้ว่าระบบที่เชื่อมโยงกันทั้งหมดประสบปัญหาเช่นกัน

โดยสรุปแล้ว ถ้ามีการจัดตั้ง centralised clearing houses แล้ว จะสามารถหลีกเลี่ยงความเสี่ยงเกี่ยวกับสภาพคล่องได้โดยนัยหนึ่งสัญญาในการหักกลบจะลดความเสี่ยงเกี่ยวกับสภาพคล่องสำหรับ participants ในสำนักหักบัญชีและตลาดการเงินโดยทั่ว ๆ ไป ส่วนอีกนัยหนึ่งการชำระบัญชีที่ศูนย์กลางก่อให้เกิดปัญหาด้านสภาพคล่องอย่างมาก ในการประเมินความเสี่ยงเกี่ยวกับสภาพคล่องของข้อเสนอเกี่ยวกับสำนักหักบัญชีต้องคำนึงถึงปัจจัยดังกล่าวด้วย

คำอธิบายศัพท์

Clearing system

เป็นกลไกในการคำนวณฐานะที่มีต่อกัน (mutual position) ภายในกลุ่มของผู้ที่มีส่วนเกี่ยวข้องเพื่อก่อให้เกิดความสะดวกในการชำระบัญชีตามสัญญาโดยใช้หลักการหักยอดสุทธิจากการหักกลับ (net basis)

Confirmation matching

เป็นกระบวนการเพื่อให้แน่ใจว่าเงื่อนไขต่าง ๆ ที่เจรจาต่อรองกันในสัญญาที่คู่สัญญาได้รายงานไว้นั้นเหมือนกัน

Credit risk

ความเสี่ยงที่เกิดขึ้นจากคู่สัญญาฝ่ายใดฝ่ายหนึ่งไม่สามารถชำระบัญชีตามสัญญาได้ครบถ้วน ไม่ว่าสัญญานั้นจะครบกำหนดแล้ว หรือในเวลาใด ๆ ภายหลังจากวันครบกำหนดตามสัญญา

Final settlement

การชำระบัญชีตามสัญญาระหว่างคู่สัญญาสองฝ่าย โดยการโอนที่ยกเลิกไม่ได้เข้าบัญชีของคู่สัญญาที่สถาบันชำระบัญชีแห่งใดแห่งหนึ่งตามที่กำหนดไว้ (ข้อสังเกต : ในกรณีที่มีการโอนโดยยกเลิกไม่ได้เข้าบัญชีของธนาคารกลางแล้ว การโอนดังกล่าวสามารถอธิบายได้ 2 ความหมายความหมายแรกเรียกว่า “final settlement” เป็นความหมายในแง่ของกฎหมายซึ่งมีผลว่ามีการปฏิบัติตามสัญญา และอีกความหมายหนึ่งคือ “ultimate settlement” ซึ่งเป็นความหมายในเชิงเศรษฐศาสตร์มีผลต่อหนี้สินของธนาคารกลาง)

Liquidity risk

ความเสี่ยงที่เกิดขึ้นจากการชำระบัญชีตามสัญญาที่ไม่ได้กระทำในวันครบกำหนดหรือวันใดวันหนึ่งภายหลังจากนั้น

Netting by close-out

ข้อตกลงในการชำระบัญชีตามสัญญาทุก ๆ สัญญาที่ยังไม่ครบกำหนดไม่ว่าจะเป็นภาระหนี้สินและสิทธิเรียกร้องต่อธนาคาร โดยการชำระเพียงครั้งเดียวในทันทีทันทีที่เหตุการณ์ใดเหตุการณ์หนึ่งตามที่ระบุไว้เกิดขึ้น (เช่น มีการแต่งตั้งผู้ชำระบัญชีธนาคารนั้น)

Netting by novation

การทดแทนสัญญา 2 ฉบับระหว่างคู่สัญญา 2 ฝ่ายที่ตกลงส่งมอบเงินตราตามที่ระบุไว้ในวันเดียวกัน โดยทำเป็นสัญญาเดียวโดยมีวันครบกำหนดตามเดิมโดยถือว่าสัญญาเดิมทั้งสองสัญญามีการปฏิบัติตามข้อตกลงในสัญญาให้ลุล่วง (หรืออาจเรียก obligation netting)

Netting provider

สถาบันที่ตั้งขึ้นเพื่อคำนวณฐานะสุทธิของสมาชิกของระบบหักหารบัญชี

Novation

การปฏิบัติตามข้อตกลงในสัญญา และการปฏิบัติหน้าที่ตามสัญญาให้ลุล่วงไปโดยการปรับปรุงหรือเปลี่ยนแปลงแก้ไขสัญญาเดิมของทั้ง 2 ฝ่าย

Novation and substitution

กระบวนการในการเพิ่มเติมสัญญาระหว่างคู่สัญญา 2 ฝ่าย จนกระทั่งบุคคลที่สามเข้ามาแทรกแซงในฐานะเป็นเจ้าหนี้ระหว่างคู่สัญญาทั้ง 2 ฝ่าย สัญญาที่เพิ่มเติมจะมีการเปลี่ยนใหม่ ดังนั้น ถือว่าสัญญาเดิมระหว่างคู่สัญญา 2 ฝ่ายมีการปฏิบัติตามข้อสัญญาให้ลุล่วงไป

Obligation

หน้าที่ตามสัญญาที่จะต้องส่งมอบหรือได้รับสินทรัพย์ (เงินตราต่างประเทศ หรือ หลักทรัพย์ เป็นต้น) ตามที่ระบุ ณ วันใดวันหนึ่งที่ตกลงกันได้

Payment

การปฏิบัติตามข้อตกลงในสัญญา และการปฏิบัติหน้าที่ตามสัญญาให้ลุล่วงไปโดยข้อกำหนดของลูกหนี้ ซึ่งยกเลิกไม่ได้ ซึ่งเป็นสิทธิเรียกร้องอันปราศจากเงื่อนไขต่อบุคคลที่สามซึ่งเจ้าหนี้อยอมรับ

Payment instruction

คำสั่งหรือข่าวสารให้มีการโอนเพื่อเครดิตบัญชี (สิทธิเรียกร้องต่อบุคคลที่สามตามคำสั่งของเจ้าหนี้)

Position netting

การหักกลบคำสั่งให้ชำระเงินของสัญญาระหว่างคู่สัญญาตั้งแต่ 2 ฝ่ายขึ้นไป แต่ไม่ใช่เป็นการปฏิบัติตามข้อตกลงในสัญญาให้ลุล่วงไป (อาจเรียกว่า payment netting)

Settlement

การชำระให้เสร็จสมบูรณ์ (หรือการปฏิบัติตามสัญญาให้ลุล่วงไป) ระหว่างคู่สัญญา 2 ฝ่าย (ที่ใช้กันบ่อย ๆ หมายถึงการชำระหรือการปฏิบัติตามสัญญาของรายการที่เป็นรายการใหญ่ ๆ หรือกลุ่มของรายการที่เกิดขึ้นมาก่อน - ดู Final settlement)

Settlement agent

สถาบันที่จัดตั้งขึ้นเพื่อทำการชำระบัญชีครั้งสุดท้ายของการหักบัญชีในนามของผู้ที่มีส่วนเกี่ยวข้องทุกคน (บางทีก็มีการปฏิบัติหน้าที่อื่น ๆ อีกด้วย)

Settlement risk

ความเสี่ยงที่เกิดขึ้นจากคู่สัญญาฝ่ายใดฝ่ายหนึ่งผิดสัญญาตั้งแต่ 1 สัญญาขึ้นไป ต่อกคู่สัญญาอื่น ๆ หรือ Settlement agent

Systemic risk

ความเสี่ยงที่สถาบันใดสถาบันหนึ่งไม่อาจชำระได้ภายในระบบการโอน ซึ่งโดยทั่วไปในตลาดการเงินนั้น การปฏิบัติตามสัญญาเมื่อครบกำหนดจะเป็นสาเหตุให้คู่สัญญาฝ่ายอื่น หรือ กิจกรรมที่เกี่ยวกับการเงินไม่สามารถปฏิบัติตามสัญญาเมื่อครบกำหนด

ภาคผนวก จ

การตรวจสอบคอมพิวเตอร์ของหน่วยงานของรัฐในประเทศสหรัฐอเมริกา

1. การตรวจสอบคอมพิวเตอร์ของ FDIC

EDP examiner จะตรวจสอบเฉพาะงานด้านคอมพิวเตอร์เท่านั้น งานด้านอื่นโดยปกติจะไม่ตรวจสอบ อย่างไรก็ตาม ในปัจจุบันมี examiner ที่ปฏิบัติหน้าที่ทั้ง EDP examiner และ Financial examiner ผสมกันไปด้วย งานด้านการตรวจสอบคอมพิวเตอร์สรุปได้ดังนี้

FDIC แบ่งงานตรวจสอบคอมพิวเตอร์เป็น 2 ประเภท คือ

- Evaluation
- Examination

1.1) Evaluation ได้แก่การประเมินผลด้าน Data Center ซึ่งกล่าวได้ว่าเป็นงานหลัก ซึ่งปกติ FDIC จะมีจดหมายพร้อมกับรายการที่ต้องการทราบไปยังธนาคารที่จะตรวจสอบเป็นการล่วงหน้า เพื่อให้เตรียมข้อมูลบางประเภทไว้ให้ EDP examiner ซึ่งโดยปกติจะแบ่งการประเมินผลด้าน Data Center เป็นดังนี้

- Internal and External Audit Coverage
- Organization
- System and Programming
- Computer Operation
- Service Centers
- Computer Services
- Others

อย่างไรก็ดี ตั้งแต่เดือนมีนาคม 2521 เป็นต้นไป FDIC ได้เปลี่ยนแนวการประเมินด้าน Data Center ใหม่หลังจากที่ได้มีการประชุมหารือกับ Comptroller of the Currency และ FRB โดย FDIC และ FRB ได้ใช้แนวการประเมินผลด้าน Data Center ของ Comptroller of the Currency เป็นหลัก

1.2) ขั้นตอนในการ Evaluation และการออกรายงานการตรวจสอบคอมพิวเตอร์

การ Evaluation มีขั้นตอนในการดำเนินการและการปฏิบัติที่สังเกตได้ดังนี้

- ก. ขอบพบกับผู้จัดการธนาคารที่จะตรวจสอบ
- ข. ขอบพบกับผู้จัดการแผนก ฝ่ายคอมพิวเตอร์ และขอดูรายงานผู้สอบบัญชีภายนอก และรายงานผู้สอบบัญชีภายในของธนาคารในด้านที่เกี่ยวกับคอมพิวเตอร์ เพื่อนำมาประเมินงานและขอบเขตการตรวจสอบ
- ค. พบกับหัวหน้าผู้ควบคุมงานด้าน Data Center เพื่อซักถามงานทั่ว ๆ ไป พร้อมกับขอดูรายการที่ได้ขอให้ธนาคารจัดทำว่าสมบูรณ์เพียงใด มีปัญหาอะไร และงานใดที่สัมพันธ์เกี่ยวเนื่องกันบ้าง

- ง. ดู Work program เกี่ยวกับการ Evaluation แล้วกรอรายการตาม Questionnaire ในแต่ละ section ซึ่ง EDP examiner จะต้องพิจารณา มีอยู่ 4 section คือ
- ง.1) ประเมินการตรวจสอบของผู้สอบบัญชีภายในและผู้สอบบัญชีภายนอก
 - ง.2) ประเมินการจัดการของฝ่ายบริหาร
 - ง.3) ประเมินระบบงานและคำสั่งงาน
 - ง.4) ประเมินผลด้านการปฏิบัติการ

เป้าหมายในการประเมินงานแต่ละเรื่องมีเช่นเดียวกับแนวของ OCC ทุกประการ ทั้งนี้เพราะในปัจจุบันทั้ง FDIC และ FRB ก็ใช้แนวการประเมินของ OCC เป็นหลัก (โปรดดูเป้าหมายในการประเมินงานแต่ละเรื่องในหัวข้อ 5.4)

EDP examiner จะติดตาม Questionnaire ในแต่ละ section ดังกล่าว ซึ่งใช้เป็นแนวทางการตรวจสอบคอมพิวเตอร์ในขั้นปฏิบัติงาน

- จ. โดยปกติผู้ตรวจจะไม่อ่าน Questionnaire เพื่อสอบถามพนักงานธนาคารโดยตรง แต่จะถามเพื่อเอาข้อมูลมาตอบใน Questionnaire ของตน
- ฉ. การ evaluation นอกจากจะได้จากการสอบถามจากผู้รับผิดชอบในแต่ละหน่วยงานแล้ว ผู้ตรวจยังจะต้อง
- ฉ.1) สังเกตการปฏิบัติของพนักงานว่าเป็นไปตามที่ได้รับชี้แจงหรือไม่ด้วย
 - ฉ.2) อ่านเอกสารต่าง ๆ ซึ่งเป็น Documentation ของธนาคารในแต่ละหน่วยงานว่ามีพร้อมและ Up-date หรือไม่ และสมบูรณ์พอที่จะช่วยแก้ปัญหาต่าง ๆ ของธนาคารหรือไม่ งานขั้นตอนนี้นับว่ามีความสำคัญและรอบคอบ กล่าวคือ ผู้ตรวจจะต้องมีความรู้ในงานคอมพิวเตอร์ด้านต่าง ๆ ของธนาคารนั้น และตัดสินใจจาก Documentation ที่มีเป็นจำนวนมากภายในแต่ละหน่วยงาน เช่น ธนาคารขนาดกลางอาจมี Documentation ตั้งแต่หลายร้อยเล่ม จนถึงหลายพันเล่มก็ได้ ดังนั้นถึงแม้ว่าผู้ตรวจจะเลือก Sampling ในการตรวจสอบเป็นปกติก็ตาม ผู้ตรวจคอมพิวเตอร์จะต้องวินิจฉัยว่าควรจะดูเอกสารอะไรบ้าง ประเภทใดและควรจะดูเท่าใดถึงพอเพียงรวมทั้งจะต้องแน่ใจว่า มีการปฏิบัติตาม Documentation นั้นจริงหรือไม่ด้วย ระบบงานที่แตกต่างกัน การใช้เครื่องคอมพิวเตอร์ที่ต่างชนิดกันของธนาคารพาณิชย์ต่าง ๆ ทำให้มีความจำเป็นอย่างยิ่งที่ผู้ตรวจสอบจะต้องศึกษาและติดตามความก้าวหน้าด้านเทคนิคและความรู้ด้านใหม่ ๆ เกี่ยวกับคอมพิวเตอร์ของแต่ละบริษัทอยู่เสมอ
- ช. การ Evaluation ผู้ตรวจจะพบว่า Technical Term และระบบงานใหม่ ๆ อยู่เสมอ ซึ่งผู้ตรวจสอบจะรู้และถ้าจำเป็นต้องสอบถามถึงความหมายและที่มาของคำนั้น ๆ ว่าเกี่ยวข้องกับงานอะไรบ้าง และถ้าเกี่ยวกับระบบงาน จะต้องทราบว่าระบบงานนั้น ๆ ทำงานอย่างไร และจะมีผลเกี่ยวกับการตรวจสอบและการปฏิบัติงานของธนาคารโดยทั่วไปอย่างไร เป็นต้น

- ข. จาก Work program ที่ได้ข้อมูลจาก Questionnaire ใน section ต่าง ๆ ผู้ตรวจสอบจะรวบรวมรายการที่จะ Comments ไว้ใน Work sheet ต่างหากเพื่อนำไปหาหรือ EDP examiner ที่อาวุโสกว่า (ถ้าจำเป็น) ทั้งนี้ใช้โทรศัพท์เป็นหลักในการติดต่อ
- ฅ. ข้อ Comments ต่าง ๆ พร้อมกับความเห็นของผู้ตรวจสอบจะนำไปหาหรือกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เพื่อรับฟังความเห็นและรวบรวมคำชี้แจงทั้งนี้เพื่อป้องกันปัญหาการโต้แย้งในภายหลังเมื่อกระทำเป็นรูปรายงานและคำแนะนำเป็นทางการแล้ว (เพราะจากประสบการณ์ที่ผ่านมาทั้ง FDIC และ OCC มักจะพบกับปัญหาเช่นนี้เสมอ ๆ)
- ญ. ผลของการตรวจสอบด้านคอมพิวเตอร์และคำแนะนำของผู้ตรวจการจะนำไปสรุปสนทนากับผู้จัดการแผนก ฝ่ายคอมพิวเตอร์ หรือผู้จัดการใหญ่หรือคณะกรรมการธนาคาร ทั้งนี้ขึ้นกับการตัดสินใจของผู้อำนวยการฝ่ายตรวจสอบด้านคอมพิวเตอร์ของแต่ละเขต อนึ่ง การ Comments ปกติต้องกล่าวถึงคำชี้แจงของผู้ที่เกี่ยวข้องพร้อมคำแนะนำของผู้ตรวจสอบด้วย
- ฎ. สรุปสนทนาผลการตรวจสอบไม่มีเป็นลายลักษณ์อักษร
- ฏ. รายงานซึ่งเรียกว่า “Electronic Data Processing Control Evaluation จะทบทวนโดย Review examiner (EDP) ซึ่งทำหน้าที่ทบทวนความถูกต้องโดยการเช็คสอบความเหมาะสมของรายงานทั้งฉบับ
- ฐ. รายงานที่ผ่านการทบทวนจะผ่านความเห็นชอบจาก Director และเมื่อพิมพ์เสร็จแล้วจะถูกจัดส่งดังนี้
- ส่งไป FDIC, Washington D.C.
 - ส่งไปยังธนาคารพาณิชย์ที่เกี่ยวข้อง
 - ส่งไปยัง OCC และ FRB ตามโครงการร่วมมือกันของสถาบันทั้ง 3 แห่ง ซึ่งเริ่มเดือนมิถุนายน 2521
 - ส่งไปยัง Services ในกรณีที่ธนาคารใช้บริการคอมพิวเตอร์จากที่อื่น
 - เก็บไว้ที่สำนักงานของแต่ละเขต
- ท. การจัดทำรายงานจะจัดทำที่สำนักงานธนาคารพาณิชย์นั้น ๆ เอง โดยปกติสำหรับธนาคารพาณิชย์ขนาดกลาง การตรวจสอบและการทำรายงานการตรวจสอบคอมพิวเตอร์นี้ใช้เวลาประมาณ 3-12 สัปดาห์ ทั้งนี้ ขึ้นกับปริมาณงานและระบบงานของธนาคาร ตลอดจนขอบเขตของการตรวจสอบและปัญหาในการตรวจสอบครั้งก่อนกับการตรวจสอบครั้งใหม่

สำหรับการจัดส่งรายงานที่ได้ผ่านการทบทวนโดย Review examiner (EDP) และโดยความเห็นชอบของ Director ที่ประจำแต่ละสำนักงานทั้ง 14 แห่งแล้วจะจัดพิมพ์และส่งให้สถาบันที่เกี่ยวข้อง รวมทั้ง FDIC Washington D.C. ด้วย ทั้งนี้ใช้เวลานับตั้งแต่การตรวจสอบประมาณ 5 สัปดาห์ ถึง 16 สัปดาห์

1.3) Examination

เป็นงานลำดับรองลงมาเมื่อเทียบกับงาน Evaluation ด้าน Data Center งานด้านนี้เป็นเพียงสนับสนุนและช่วยเหลือ Financial Examiner ในการตรวจสอบงานด้านอื่น ๆ งานของ EDP examiner ในส่วนนี้มีดังนี้

1.3.1) ขอ Report ต่าง ๆ ที่จำเป็นในการทำ Evaluation ซึ่งเป็นงานที่เกี่ยวข้องตามข้อ 4.1

1.3.2) ขอ Report ที่จำเป็นเพื่อการปฏิบัติงานของ Financial (Regular) examiner

1.3.3) ใช้ program หรือคำสั่งงานของ FDIC เอง เพื่อดึงข้อมูลที่ต้องการตรวจสอบซึ่งบันทึกอยู่ในม้วน Tape หรือ Disk ของธนาคาร ทั้งนี้ อาจกระทำเพื่อให้ได้ข้อมูลตามที่ Financial examiner ต้องการ หรือเพื่อการทดสอบงานของ EDP examiner เองบางส่วนก็ได้ งานชิ้นนี้นับว่ามีความสำคัญไม่น้อยเพราะเป็นวิธีการตรวจสอบที่เรียกว่า “Through the Computer” กล่าวคือ มีการใช้ program ของผู้ตรวจสอบเอง ในการทดสอบข้อมูลของธนาคาร ไม่ว่าจะเป็นการดึงข้อมูลจาก File (Tape หรือ Disk) ของธนาคารในรูปแบบเดิมหรือเปลี่ยนแปลงข้อมูลให้ปรากฏในรูปแบบที่ผู้ตรวจสอบต้องการ รวมทั้งการทำข้อมูลใหม่โดยอาศัยข้อมูลเดิมของธนาคารด้วยก็ได้

การปฏิบัติงานการตรวจสอบที่เรียกว่า “Through the Computer” ของ FDIC นี้ เป็นการใช้เทคนิคการตรวจสอบมาก ผู้ตรวจสอบจะต้องเข้าใจในระบบงานอย่างแท้จริง และลึกซึ้งถึงจะปฏิบัติงานขั้นนี้ได้ และในทางปฏิบัติผู้ตรวจสอบก็พบกับปัญหาอยู่ไม่น้อย ซึ่งจะต้องทำการแก้ไขโปรแกรมในการตรวจสอบเสมอ ดังนั้นทาง Comptroller of the Currency จึงไม่ใช่วิธีการตรวจสอบชนิดนี้ทั้ง ๆ ที่ทาง FDIC เสนอให้ยืม program ในการตรวจสอบไปใช้ก็ตาม

1.4) เหตุผลที่ FDIC ใช้แนวการตรวจสอบแบบ Through the Computer

1.4.1) ไม่ต้องอาศัยข้อมูลของธนาคารแต่อย่างใด เพราะ FDIC สามารถสร้างข้อมูลใหม่หรือเปลี่ยนรูปแบบของข้อมูลเดิมโดยอาศัย program ปฏิบัติการในด้านนี้ ทำให้เป็นอิสระที่จะใช้ข้อมูลเท่าที่จำเป็นในการตรวจสอบ

1.4.2) ช่วยประหยัดเวลาในการปฏิบัติงานของ Financial examiner ลงได้มาก และทำให้การตรวจสอบมีประสิทธิภาพมากขึ้น

1.4.3) เป็นการยกระดับผู้ตรวจสอบด้านคอมพิวเตอร์ และทำให้ผู้ตรวจสอบแน่ใจความรู้นี้ของตนมากยิ่งขึ้น

อย่างไรก็ดีข้อมูลที่ได้จากการใช้ Through the Computer ในการตรวจสอบก็เพื่อใช้งานในด้าน Financial examiner เป็นหลัก

1.5) งานที่ตรวจสอบแบบ Through the Computer ของ FDIC

- Installment loans
- Demand deposits

- Savings deposits
- Certificates of deposits

งานที่ตรวจสอบในแบบ Through the Computer เริ่มในปี 1975 จากงาน Installment loans เป็นอันดับแรก ปัจจุบัน FDIC กำลังพัฒนา program ที่จะตรวจสอบงานประเภทอื่น ๆ ให้มากขึ้น

1.6) ข้อสังเกตเกี่ยวกับการใช้ Software package ในการตรวจสอบของ FDIC และผู้สอบบัญชี

1.6.1) FDIC ได้พัฒนา Software package ของตนเองเพื่อการตรวจสอบในลักษณะ Through the Computer โดยเฉพาะทั้งนี้โดยมี Division of Management System and Financial Statistics ประจำ FDIC, Washington D.C. เป็นผู้ทำหน้าที่พัฒนาเรื่องนี้โดยตรง และจะนำ Software package ที่พัฒนาแล้วให้ผู้ตรวจสอบทดลองใช้งาน และแก้ไขไปจนกว่าจะนำไปใช้ปฏิบัติงานได้จริง

1.6.2) EDP examiner เป็นผู้ใช้ Software package แต่ไม่ได้เป็นผู้เขียน program เอง EDP examiner ที่ช่วย Financial examiner โดยการใช้ Software package ดึงข้อมูลจาก tape หรือ disk เพื่อการตรวจสอบงานของ Financial examiner และของ examiner เองนี้ จะต้องมีความรู้ด้านการเขียน program ดีพอ เพราะในทางปฏิบัติการใช้ Software package ในการตรวจสอบมักมีปัญหาอยู่เสมอที่ EDP examiner จะต้องแก้ไข program ด้วยตนเอง และถ้าไม่อาจแก้ไขได้ก็ต้องโทรศัพท์หาหรือโดยตรงไปยัง FDIC, Washington D.C. และบางกรณีผู้เชี่ยวชาญจาก Washington D.C. จำเป็นต้องเดินทางไปแก้ไขปัญหาด้วย

1.6.3) ผู้ตรวจสอบบัญชีภายนอกและผู้ตรวจสอบบัญชีภายในของธนาคารพาณิชย์ที่ใช้ Software package ในการตรวจสอบโดยปกติจะไม่พัฒนาหรือเขียน program ในการตรวจสอบข้อมูลโดยตรง แต่จะใช้ Software package จากบริษัทผู้ผลิตหรือบริการด้าน Software โดยเฉพาะ เช่น Cullinane Corporation ซึ่งบริษัทประเภทนี้จะมีความเชี่ยวชาญโดยเฉพาะเกี่ยวกับการเขียน program ในการตรวจสอบงานการผลิตข้อมูลที่ดำเนินการโดยเครื่องคอมพิวเตอร์ของ IBM ซึ่งไม่เหมาะสม และอาจใช้งานไม่ได้ผลสำหรับคอมพิวเตอร์ชนิดอื่น ๆ

อย่างไรก็ดี งานตรวจสอบบางประเภทผู้สอบบัญชีอาจเขียน program เพื่อการตรวจสอบเองทั้งหมดก็ได้

1.6.4) ในการใช้ Audit software package เพื่อปฏิบัติงานผู้ตรวจสอบจะต้องเขียน parameter คือเขียนคำสั่งงานในแบบฟอร์มซึ่งจะนำไปเจาะรูในบัตรเจาะรู (Punch card) ขนาดมาตรฐาน บัตรเจาะรูดังกล่าวเป็นเสมือนหนึ่งเป็นบัตรนำในการสั่งงานให้เครื่อง Compile program กล่าวคือ ให้เครื่องแปลภาษาคอมพิวเตอร์ที่ programmer เขียนขึ้นให้เป็นภาษาของเครื่องจักร (Machine readable form) ซึ่งในที่สุดแล้วคำสั่งงานการตรวจสอบในเรื่องที่เกี่ยวข้องจะถูกบันทึกลงในส่วนที่เป็นสมอง หรือ memory ของเครื่องคอมพิวเตอร์ เพื่อการปฏิบัติงานในขั้นต่อไปได้

1.6.5) เมื่อเครื่องคอมพิวเตอร์ Compile program ของงานที่จะตรวจสอบแล้ว จะมีการทดสอบ program ที่พร้อมจะปฏิบัติงานได้นั้นกับ Program file ของผู้ตรวจสอบซึ่งส่วนมากมีลักษณะเป็น tape ของ

application ที่ตรวจสอบ เช่น Installment loans ซึ่งผู้ตรวจสอบต้องการจะได้ข้อมูลในรูปแบบของผู้ตรวจสอบเองว่า “เป็นไปได้” หรือ “ปฏิบัติได้” หรือ “agree” งานขั้นนี้ปกติจะต้องให้พนักงานของธนาคารปฏิบัติให้โดยผู้ตรวจสอบจะมอบ tape ของผู้ตรวจซึ่งเตรียมมาแล้ว ถ้าคำสั่งงาน (program) ขัดแย้งกับรูปแบบของงานที่ผู้ตรวจต้องการ เครื่องคอมพิวเตอร์จะพิมพ์ listing program ที่จะต้องแก้ไขพร้อมกับข้อความโดยย่อแต่ละขั้นให้ทราบ ซึ่งผู้ตรวจสอบต้องแก้ไขให้ถูกต้องก่อนการ “run” งานจริง ๆ กับข้อมูลของธนาคารซึ่งอยู่ใน tape ต่อไป

1.6.6) การแก้ไข Program ที่ผิดพลาด จะต้องเจาะบัตรเจาะรูใหม่และ Compile program ใหม่ทั้งหมด แต่สำหรับเครื่องคอมพิวเตอร์บางชนิดเช่นเครื่อง Burrough B 3700 นี้เพียงแค่ Compile บัตรเจาะรูที่แก้ไขใหม่เข้าไปแทนบัตรเจาะรูเดิมก็ใช้ได้ ทำให้ประหยัดเวลาและสะดวกในการปฏิบัติงานมากขึ้น

1.6.7) ผู้ตรวจสอบจะบอกหัวหน้า Operator ของ Data Center เกี่ยวกับงานที่จะต้องตรวจสอบดังนี้

- ชื่อของงานที่จะตรวจสอบ เช่น Installment loans
- วันที่ใน file หรือ Master file ที่จะใช้ในการตรวจสอบ

1.6.8) เมื่อ EDP examiner ได้ข้อมูลในการตรวจสอบซึ่งปกติจะพิมพ์มาจาก printer ก็จะนำมาดู Total balance เป็นหลัก และตรวจสอบเปรียบเทียบกับยอดรวมของ Master file อื่น ๆ ที่เกี่ยวข้อง ส่วนรายละเอียดในการตรวจสอบกับเอกสารของธนาคารและการดูข้อมูลอื่น ๆ เป็นหน้าที่ของ Regular examiner หรือ Financial examiner จะดำเนินการต่อไป

1.6.9) Audit software package จากบริษัทผู้ผลิตคอมพิวเตอร์ หรือ จากบริษัทผู้ดำเนินการบริการเขียน Audit software package โดยเฉพาะนี้ มีราคาแตกต่างกันขึ้นอยู่กับปัจจัยต่อไปนี้

- ขอบเขตการใช้งาน
- ลักษณะงานที่ใช้
- ระบบงานของเครื่องคอมพิวเตอร์ซึ่งแตกต่างกันในแต่ละผลิตภัณฑ์
- ต้นทุนหรือการตั้งราคาจำหน่ายแต่ละบริษัท
- เงื่อนไขการให้บริการ

โดยทั่วไป Audit software package ที่มีขนาดและขอบเขตการใช้งานขนาดกลางมีราคา ระหว่าง US\$ 20,000 ถึง US\$ 50,000 ทั้งนี้ขึ้นกับปัจจัยดังกล่าวข้างต้น บางบริษัทนอกจากขาย software package แล้ว ยังคิดค่าบริการในลักษณะ Annual fee อีกต่างหากด้วย

2. การตรวจสอบคอมพิวเตอร์ของ OCC (Office of the Comptroller of the Currency)

2.1 ผู้ตรวจสอบคอมพิวเตอร์ (EDP Examiners)

The Comptroller ได้แต่งตั้งผู้ตรวจสอบที่มีประสบการณ์ในการตรวจสอบให้ปฏิบัติงานเป็นผู้ตรวจสอบด้านคอมพิวเตอร์ (EDP Examiners) และได้จัดให้บุคคลเหล่านี้เข้ารับการฝึกอบรมเป็นพิเศษ เพื่อให้เป็นผู้ที่มีความสามารถในการที่จะตรวจสอบระบบการผลิตข้อมูลด้วยคอมพิวเตอร์ของธนาคารและของศูนย์บริการด้านคอมพิวเตอร์ (Service Center) ต่าง ๆ ที่ธนาคารให้บริการอยู่

ผู้ตรวจการด้านคอมพิวเตอร์จะรายงานต่อ Regional Administrator ซึ่งตนสังกัดอยู่ แต่อย่างไรก็ตาม งานทางด้านเทคนิคต่าง ๆ ของการตรวจสอบด้าน EDP ยังคงอยู่ในความรับผิดชอบของฝ่ายกิจการธนาคาร (The Banking Operation Department) ในวอชิงตัน จำนวนผู้ตรวจการ สถานที่ทำงาน และตารางเวลาการปฏิบัติงานของผู้ตรวจการดังกล่าวยังคงขึ้นอยู่กับ regional administrator ซึ่งผู้บริหารงานของแต่ละ office การคัดเลือกผู้ตรวจการและการจัดให้เข้ารับการอบรมต้องประสานงานและได้รับอนุมัติจากสำนักงานตรวจสอบคอมพิวเตอร์ (EDP Examination Division) ในวอชิงตัน มาตรฐานและการดำเนินการฝึกอบรมให้ถือเป็นความรับผิดชอบของ Washington office

ผู้ตรวจการด้าน EDP มีหน้าที่ในการตรวจสอบการผลิตข้อมูลด้วยคอมพิวเตอร์ในแต่ละธนาคารและในศูนย์บริการซึ่งผลิตข้อมูลให้แก่ธนาคาร

แผนการปฏิบัติงาน (work programs) และรายงานการตรวจสอบและจัดทำขึ้นโดยเฉพาะสำหรับแต่ละกิจการที่ตรวจสอบ วัตถุประสงค์ของการตรวจสอบก็เพื่อที่จะวัดผลการควบคุมภายในของระบบการผลิตข้อมูลด้วยคอมพิวเตอร์

ความจำเป็นของแต่ละท้องถิ่น ความสนใจและความชำนาญงานของผู้ตรวจการแต่ละคนจะเป็นปัจจัยที่กำหนดระยะเวลาที่จะใช้ในการตรวจสอบของผู้ตรวจการด้าน EDP ผู้ตรวจการด้าน EDP จะต้องเป็นผู้ที่มีความสนใจในงานด้านการผลิตข้อมูลด้วยเครื่องจักรนี้เป็นอย่างมากเพื่อที่จะให้เป็นผู้ตรวจการที่มีประสิทธิภาพอยู่เสมอ

ผู้ตรวจการด้าน EDP ของ The Comptroller จะต้องเป็นผู้ที่คุ้นเคยกับงานด้านการตรวจสอบกิจการค้า กิจการทรัสต์ และกิจการธนาคารระหว่างประเทศ (international bank) หรือเคยผ่านงานดังกล่าวมาบ้างอย่างน้อยที่สุดต้องเป็นผู้ที่สามารถเข้าใจถึงกิจการดังกล่าวโดยตลอด

ดังนั้น จึงอาจกล่าวได้ว่า ผู้ตรวจสอบคอมพิวเตอร์ (EDP examiner) จะต้องรู้ถึงแนวการตรวจสอบงานในแบบธรรมดาแล้วเป็นอย่างดี และโดยปกติ EDP examiner มักจะได้รับการคัดเลือกหรือมาจากความสมัครใจของผู้ตรวจสอบธรรมดา (Financial examiner) ที่มีประสบการณ์การตรวจกิจการของธนาคารโดยทั่วไปมาแล้ว

2.2 การตรวจสอบคอมพิวเตอร์ (EDP examination)

การตรวจสอบด้าน EDP ประกอบด้วยหลักการที่จะประเมินผลการควบคุมภายในที่มีศูนย์ประมวลผลแต่ละแห่ง ศูนย์ประมวลผลที่ดำเนินการประมวลผลข้อมูลและเก็บรักษาคัดลอกข้อมูล (master file records) ของธนาคารทุกศูนย์ที่จะต้องได้รับการตรวจสอบ รายละเอียดข้างล่างนี้แสดงถึงลักษณะของศูนย์ประมวลผลที่จะต้องได้รับการตรวจสอบจากสำนักงานของ Comptroller:-

- * ศูนย์ประมวลผลข้อมูลของธนาคารที่ตั้งอยู่ในที่ทำการ (in-house data processing center)
- * สาขาย่อยของศูนย์ประมวลผลของธนาคาร
- * กิจการในเครือของธนาคาร (affiliates of national bank) หรือ สาขาของธนาคาร (subsidiaries of bank holding companies) ซึ่งให้บริการผลิตข้อมูลแก่ธนาคาร
- * สถาบันการเงินที่มีใช้ธนาคาร (nonbanking companies) ซึ่งให้บริการด้านการประมวลผลข้อมูลแก่ธนาคาร (national bank)
- * ระบบคอมพิวเตอร์ขนาดเล็ก (minicomputer systems) ของธนาคารที่ธนาคารใช้บันทึกข้อมูลเข้า master files ของระบบ computer

ศูนย์ประมวลผลต่อไปนี้ไม่ต้องได้รับการตรวจสอบโดยสำนักงานของ comptroller คือ

- * State banks หรือสาขาของ State banks ซึ่งให้บริการประมวลผลข้อมูลแก่ National Bank
- * ศูนย์ประมวลผลซึ่งมิใช่ของธนาคาร National Bank หรือสาขาของ national bank และมีได้ให้บริการดังกล่าวแก่ national bank

ส่วนเครื่องคอมพิวเตอร์ขนาดเล็กซึ่งใช้ประโยชน์เฉพาะเพื่อการถ่ายทอดข้อมูลจากเอกสารต้นฉบับและส่งผ่าน (transmitting) ไปยังศูนย์ประมวลผลเพื่อผ่านบัญชี (posted), ประมวลผล (processed) และบันทึกข้อมูลและใช้เพื่อรับผล (output) จากศูนย์และส่งกลับเพื่อแสดงผล ณ จุดต่าง ๆ ตามที่ต้องการ

การตรวจสอบระบบดังกล่าวซึ่งมักเรียกว่า “front-end devices” มีข้อแนะนำดังต่อไปนี้

เมื่อใดก็ตามที่ธนาคารที่ตรวจสอบมีระบบ front-end system เชื่อมโยงกับศูนย์คอมพิวเตอร์มากกว่า 1 แห่ง ผู้ตรวจการจะต้องเลือกไปตรวจสอบและดูความเหมาะสม 1 แห่งและในการตรวจสอบครั้งต่อไปจะต้องเลือกแห่งใหม่ที่ไม่ซ้ำกับที่เดิม แต่เนื่องจากการที่สถานที่ตั้งของ front-end system อยู่คนละแห่งกันกับศูนย์ข้อมูลที่เข้าตรวจสอบตามกำหนดการ ดังนั้น การตรวจสอบ front-end device ซึ่งอยู่คนละสถานที่กันอาจทำให้ขณะที่เข้าตรวจสอบศูนย์ข้อมูลอื่นซึ่งตั้งอยู่ในท้องถิ่นดังกล่าวได้ในภายหลัง และในกรณีนี้จะต้องมีรายละเอียดระบุไว้ด้วยว่าได้ตรวจสอบครั้งก่อนเมื่อใด ใครเป็นผู้ตรวจสอบ front-end system ดังกล่าวอาจรวมเข้ากับรายงานการตรวจสอบศูนย์ข้อมูลที่ได้ตรวจสอบเมื่อก่อนหน้านี้ก็ได้

2.2.1 การตรวจสอบประสานกัน (Concurrent Examination)

การตรวจสอบกิจการของธนาคารและศูนย์ข้อมูลของธนาคารอาจจะกระทำพร้อมกันไปได้ เพื่อให้มีการประสานงานระหว่างผู้ตรวจสอบด้าน EDP และผู้ตรวจสอบด้านเงินให้กู้ยืมและให้เครดิต และด้านกิจการทรัสต์ ในกรณีที่มีปัญหาหรือพบข้อแตกต่างในระหว่างการตรวจสอบร่วมกันนี้ ผู้ตรวจการด้าน EDP จะเป็นผู้รับผิดชอบในการชี้แจงแก่ผู้บริหารระดับสูง (Senior Management) และแนะนำแก่ผู้ตรวจสอบเงินให้กู้ยืมและให้เครดิต (examiner in charge of the commercial examination) ถึงข้อแตกต่างที่ตรวจพบ

2.2.2 การตรวจสอบร่วมกัน (Joint Examination)

ในบางกรณี EDP examiner ของ Comptroller อาจตรวจสอบร่วมกับ EDP examiner ของสถาบันอื่นที่มีหน้าที่ควบคุมธนาคาร (other regulatory authorities) ก็ได้ เช่น ผู้ตรวจสอบของ FDIC และ/หรือ FRB

ผู้ตรวจการควรพยายามประสานงานเพื่อตรวจสอบกิจการต่อไปนี้

- * กิจการในเครือ (affiliate) ของ National Bank หรือสาขา (subsidiary) ของ holding company ของธนาคารซึ่งเป็นผู้ให้บริการผลิตข้อมูลแก่ national และ state banks
- * สถาบันการเงินที่ไม่ใช่ธนาคาร (nonbanking companies) ซึ่งให้บริการแก่ national และ state banks
- * องค์การที่ตั้งขึ้นเพื่อให้บริการแก่ธนาคาร (bank services corporations) ทั้งในรูปของการลงทุนร่วมกันหรือสหกรณ์ (joint ventures or corporations) ซึ่งให้บริการดังกล่าวแก่ national และ state banks

5.2.3 การตรวจสอบในแบบ Evaluation หรือ Around the Computer

การ Evaluation ของ OCC ก็คือ การตรวจสอบด้านคอมพิวเตอร์ของ EDP examiner นั้นเอง ทั้งนี้เพราะ OCC. พิจารณาว่า การ Evaluation แต่เพียงอย่างเดียวก็บรรลุวัตถุประสงค์ของ EDP examination ทุกประการ

ดังนั้น OCC จึงค้นคว้าวิธีการตรวจสอบคอมพิวเตอร์ด้วยวิธีการ “ประเมิน” งานด้านที่เกี่ยวข้องจนกระทั่งเป็นที่ยอมรับกันอย่างกว้างขวาง ซึ่งต่อมาทั้ง FDIC และ FRS ก็ได้นำวิธีการ Evaluation ทุกขั้นตอนของ OCC ไปใช้ในทางปฏิบัติจนกระทั่งปัจจุบันนี้ แต่ FDIC มีวิธีการเพิ่มเติมเป็นพิเศษของตนเองตามลำพัง คือ การตรวจในแบบ through the computer โดยใช้ software package ช่วยในการตรวจสอบด้าน financial examination ด้วย

การประเมินผลอาจกระทำที่ธนาคารพาณิชย์และ/หรือ ณ ศูนย์ปฏิบัติการคือ Data Center ซึ่งดำเนินการโดยธนาคารพาณิชย์นั้น ๆ เอง หรือประเมินผลที่บริษัทผู้รับประมวลข้อมูลให้ธนาคาร

การประเมินผลจะใช้เวลาระหว่าง 2 สัปดาห์ ถึง 12 สัปดาห์ ทั้งนี้ขึ้นกับ

- จำนวน Data Center ซึ่งอาจมีหลายแห่ง
- ขนาดของ Data Center
- ระบบงาน
- ปริมาณงานและชนิดของงาน
- ผลการตรวจสอบครั้งก่อน

การ Evaluation จนกระทั่งถึงการออกรายงานการตรวจสอบคอมพิวเตอร์ของ OCC มีขั้นตอนในการดำเนินงานเช่นเดียวกับที่กล่าวไว้ในหัวข้อ 5.2 ทุกประการ

การ Evaluation ของ EDP examiner มี work program ในการปฏิบัติงานอย่างละเอียดในแต่ละส่วนงานที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งมีหัวข้อและเป้าหมายกว้าง ๆ ในการตรวจสอบดังนี้

- การประเมินการตรวจสอบของผู้สอบบัญชีของธนาคาร เพื่อ.-
- ก) เพื่อกำหนดขอบเขตการปฏิบัติงานของผู้ตรวจสอบ ทั้งนี้เพราะผู้ตรวจสอบจะทราบสิ่งต่อไปนี
 - ปัญหาและข้อบกพร่องที่ตรวจพบโดยผู้สอบบัญชีของธนาคาร
 - การตรวจสอบของผู้สอบบัญชีธนาคารว่าปฏิบัติงานตรวจสอบในสิ่งที่ควรจะได้ตรวจหรือไม่ เพราะผู้ตรวจสอบของ OCC จะขอดู work sheets ของผู้สอบบัญชีภายในของธนาคารด้วย
- ข) ติดตามการแก้ไขข้อบกพร่องตามที่ปรากฏในรายงาน
- ค) สามารถทราบความสนใจของฝ่ายบริหารว่าสนใจเรื่องราวที่เกี่ยวกับคอมพิวเตอร์หรือไม่ ทั้งนี้โดยดูจากรายงานการประชุมที่มีการพิจารณาและสั่งการประการใดบ้างในส่วนที่เกี่ยวข้องกับข้อ comment และข้อเสนอแนะในรายงานตรวจสอบ
- การประเมินการจัดการของฝ่ายบริหาร ก็เพื่อ
- ก) พิจารณาการจัดองค์กร โดยเฉพาะในส่วนที่เกี่ยวข้องกับคอมพิวเตอร์ว่ามีหน่วยงานที่พอเพียงหรือไม่
- ข) พิจารณาถึงการมอบหมายหน้าที่การงานและขอบเขตการรับผิดชอบให้กับแต่ละบุคคลซึ่งมีส่วนรับผิดชอบในการบริหารงานเหมาะสมหรือไม่
- ค) พิจารณาถึงนโยบายและการแก้ไขปัญหาของฝ่ายบริหาร

- การประเมินรายงานและคำสั่งงาน (systems and programming) เพื่อ
- ก) พิจารณาว่า ธนาคารสามารถดำเนินการได้ตามปกติหรือไม่ ถ้าเกิดกรณีต่อไปนี้
 - ไฟไหม้
 - น้ำท่วม
 - แผ่นดินไหว
 - ไฟฟ้าดับ
 - โทรศัพท์ขัดข้อง
 - อุปกรณ์คอมพิวเตอร์เสียหายหรือขัดข้อง

ทั้งนี้ เพราะปัญหาที่เกิดขึ้นกับธนาคารจะมีผลกระทบกระเทือนถึงประชาชนโดยตรง

ข) พิจารณาว่ามีการปฏิบัติตามคู่มือการปฏิบัติงานที่ได้วางไว้เป็นบรรทัดฐานหรือไม่ และคู่มือดังกล่าวยังมีผลในทางปฏิบัติเพียงใด

- การประเมินผลด้านการปฏิบัติงาน (computer operation) เพื่อ
- ก) พิจารณาถึงความพอเพียงของกระบวนการปฏิบัติงานในแต่ละขั้นตอนของการประมวลข้อมูลว่ามีความน่าเชื่อถือได้เพียงใดเมื่อได้ปฏิบัติตามระบบงานที่ได้เขียนเป็นลายลักษณ์อักษรไว้แล้ว
- ข) พิจารณาถึงการควบคุมการประมวลข้อมูลทุกขั้นตอนว่ากระทำการอย่างมีประสิทธิภาพเพียงใด อาจมีจุดอ่อนที่ใดได้บ้าง และมีการป้องกันอย่างไร และจะตรวจพบได้เพียงใด

2.2.4 สรุปงานของ EDP examiner ขณะปฏิบัติงานด้านตรวจสอบประกอบด้วย :-

- * ปฏิบัติงานด้าน Review System ปัจจุบันธนาคารที่กำลังใช้งานประมาณร้อยละ 40
- * ปฏิบัติงานด้าน Review System ใหม่ที่ธนาคารจะนำมาใช้ในอนาคตประมาณร้อยละ 30
- * ปฏิบัติงานด้านเทคนิคให้กับ Regular examiner หรือ Financial examiner ประมาณร้อยละ 20
- * ปฏิบัติงาน Review ด้าน Data Center ประมาณร้อยละ 10

2.2.5 เหตุผลที่ OCC ไม่ใช้วิธีการตรวจสอบในแบบ Through the Computer

เป็นที่น่าสังเกตว่า Comptroller of the Currency ใช้วิธีการ Evaluation ซึ่งพิจารณาได้ว่าเป็นแนวการตรวจสอบในแบบ “Around the Computer” แต่เพียงอย่างเดียว โดยไม่มีวิธีการตรวจสอบในแบบ “Through the Computer” ซึ่ง FDIC ใช้ในการปฏิบัติควบคู่กับวิธีการ “Around the Computer” ด้วย

เหตุผลที่ Comptroller of the Currency ไม่ใช้ software package หรือวิธีการ “Through the Computer” ในการตรวจสอบคอมพิวเตอร์อาจสรุปได้ดังนี้

- * มีปัญหามากในการใช้ปฏิบัติงาน พิจารณาว่าไม่คุ้มกัน เช่น ธนาคารเปลี่ยนแปลงฟอร์มหรือเทคนิคใหม่ ๆ ผู้ตรวจก็ต้องแก้ไข software package และต้องศึกษาเทคนิคนั้น ๆ ให้รู้ซึ่งด้วย ส่วนมากใช้เวลา และในหลาย ๆ กรณีที่ต้องแก้ไข software package เนื่องจากธนาคารเปลี่ยน operating system อาจใช้เวลานานกว่าที่ประมาณไว้มาก และการตรวจโดยใช้ software package มักพบกับปัญหาเช่นนี้เสมอ ๆ
- * ต้องใช้ความชำนาญของผู้ตรวจสอบมาก สลับเปลี่ยนมาก และก็ไม่ได้เป็นที่แน่ใจว่าผู้ตรวจสอบประเภทนี้สามารถแก้ไขปัญหได้ทุกเรื่อง เนื่องจากเวลาส่วนใหญ่หรือแทบทั้งหมดใช้ไปในงานตรวจสอบ จนกระทั่งไม่มีเวลาศึกษาเทคนิคใหม่ ๆ
- * การตรวจสอบโดยใช้ software package เพียงแต่ทำให้รู้สึกว่าเป็นการตรวจสอบอิสระที่ไม่จำเป็นต้องใช้ข้อมูลของธนาคาร แต่ในทางปฏิบัติต้องอาศัยพนักงานและความร่วมมือจากธนาคารพาณิชย์ที่ถูกตรวจสอบอยู่มาก เช่น
 - การให้เวลาปฏิบัติการ
 - การเลือก file ในการ generate ข้อมูล
 - การชี้แนะเทคนิคต่าง ๆ ที่เกี่ยวข้องในการ process ข้อมูล เป็นต้น
 - ผู้ตรวจสอบไม่อาจควบคุมการ process งานทุกขั้นตอนได้
- * ผู้ตรวจสอบภายในของธนาคารส่วนใหญ่ก็ใช้ software package ในการตรวจสอบ ดังนั้นการประเมินการตรวจสอบภายในก็อาจจะพอเพียง ทั้งนี้เมื่อพิจารณาว่ารายละเอียดต่าง ๆ ควรเป็นหน้าที่ของผู้ตรวจสอบภายในของธนาคารเอง เพราะมีหน้าที่โดยตรงอยู่แล้ว
- * การใช้ software package ในการตรวจสอบแบบ Through the Computer นั้น แต่ละ package ไม่อาจใช้กับงานที่จะตรวจทุกชนิดได้ (ยกเว้น package ง่าย ๆ ที่ไม่มีประโยชน์ในการใช้งานในภาคปฏิบัติมากนัก) ดังนั้น แต่ละงานจะต้องใช้ แต่ละ package ที่เกี่ยวข้อง นอกจากนี้ ถ้าเป็นคอมพิวเตอร์ต่างชนิด ต่างระบบ ก็ไม่อาจใช้ software package อันเดียวกันได้ถึงแม้จะเป็นงานชนิดเดียวกันก็ตาม ดังนั้น จึงนับว่าสิ้นเปลืองมาก
- * การกำหนดข้อมูลขั้นต่ำที่จำเป็นต้องใช้ในการตรวจสอบให้ธนาคารพาณิชย์ที่ใช้คอมพิวเตอร์จัดทำในรูป Report ได้เช่นเดียวกับข้อมูลที่จะได้จากการตรวจสอบด้วยวิธีธรรมดาหรือในแบบ Around the Computer ดังนั้น การตรวจสอบคอมพิวเตอร์โดยใช้วิธีการประเมินตามขั้นตอนที่ปฏิบัติอยู่ก็ได้ผลเช่นกัน
- * การใช้ software package ของ FDIC เป็นเพียงเครื่องมือที่ช่วยในการตรวจสอบด้าน financial ซึ่งช่วยงานตรวจสอบของ financial examiner เท่านั้นไม่มีผลในการตรวจสอบเกี่ยวกับคอมพิวเตอร์โดยตรง เช่น 120 package (Installment Loan Package) ที่ใช้ในการตรวจสอบ Installment loans พัฒนาขึ้นเพื่อให้ผู้ตรวจ Installment loans ซึ่งเป็นงานของ financial examiner ได้ตรวจสอบและรวดเร็วโดยได้ข้อมูลที่ต้องการเท่านั้น

2.3 ขอบเขตของการตรวจสอบ (Scope of Examination)

ผู้ตรวจสอบควรมีการศึกษาข้อมูลขั้นต้น (Preliminary Review) ถึงหน้าที่ต่าง ๆ ของงานด้าน EDP ทั้งหมดก่อน แล้วจึงใช้วิธีตรวจสอบโดยละเอียด (examine in depth) ถึงงานแต่ละด้านเพื่อดูถึงขอบกพร่องของการควบคุมภายใน ถ้าปรากฏว่ามีขอบกพร่องที่เป็นสิ่งสำคัญก็จำเป็นต้องพิจารณาขยายขอบเขตของการตรวจสอบด้านการให้กู้ยืมและให้เครดิตให้มากยิ่งขึ้น (concurrent commercial examination) เนื่องจากว่ามีความสัมพันธ์โดยตรงกับระบบงานที่ใช้อยู่ (automated applications) ถ้าวิธีการควบคุมภายในของงาน EDP ช่วงดังกล่าวบกพร่องก็ไม่สามารถใช้ข้อมูลที่ได้จากระบบนั้นเพื่อการตรวจสอบงานด้านเกี่ยวกับธุรกิจ (commercial) ของธนาคารนั้นได้

2.4 ความถี่ของการตรวจสอบ (Frequency of Examination)

การตรวจสอบศูนย์ข้อมูลต่าง ๆ นั้นคือเกณฑ์ปีละครั้ง (annual basis) และอย่างช้าที่สุดต้องไม่เกินกว่า 18 เดือนต่อครั้ง ในกรณีที่พบว่าการควบคุมภายในบกพร่องมากก็จำเป็นต้องมีการตรวจสอบให้บ่อยครั้งยิ่งขึ้น บางครั้งก็จะต้องมีการไปตรวจสอบเพื่อติดตามความก้าวหน้าในการแก้ไขข้อผิดพลาดของธนาคารตามที่ระบุไว้ในรายงานการตรวจสอบ

2.5 แผนการตรวจสอบ (Work Program)

ทุกครั้งที่ตรวจสอบจะต้องมีการจัดทำแผนการตรวจสอบสำคัญศูนย์ข้อมูลแต่ละแห่งเรียงลำดับขั้นตอนให้เรียบร้อยแล้วส่งให้ Regional EDP Associate เพื่อพิจารณา หลังจากนั้น Regional Office จะเป็นผู้เก็บรักษาและแจกจ่ายรายงานนั้นตามควรแก่กรณี และต้องจัดให้มีวิธีป้องกันรักษา work program ดังกล่าวอย่างรัดกุมทุกขั้นตอน

2.6 รายงานตรวจสอบ (Report of Examination)

รายงานการตรวจสอบด้าน EDP จะต้องทำให้เสร็จโดยสมบูรณ์ในระหว่างการตรวจสอบขั้นตอนของงานใดที่มีอาจตรวจสอบได้ (nonapplicable sections) จะต้องเปิดเผยไว้ให้ชัดเจนในรายงาน ขอบกพร่องต่าง ๆ ที่รายงานไว้จะต้องปรึกษากับเจ้าหน้าที่ผู้รับผิดชอบและผู้บริหารของศูนย์ข้อมูลนั้น การสรุปสนทนาครั้งสุดท้าย (A final discussion) จะต้องกระทำกับผู้บริหารชั้นสูงสุดของธนาคารและของแผนก EDP แม้จะไม่มีขอบกพร่องที่จะยกขึ้นเป็นข้อสังเกตหรือคำวิจารณ์ (adverse criticism) ก็ตาม

ความรับผิดชอบในการควบคุมดูแลรายงานการตรวจสอบทั้งหมดเป็นหน้าที่ของ Regional Office ต้องรายงาน และเอกสารประกอบทั้งหมดจะต้องไม่อยู่ในความครอบครองของเจ้าหน้าที่ที่ตรวจนานเกินกว่าระยะเวลาอันสมควรหลังจากที่ได้มีการสรุปผลการตรวจสอบเสร็จสิ้นเรียบร้อยแล้ว

หลังจากเสร็จสิ้นการตรวจสอบแล้วจะต้องจัดการกับรายงานการตรวจสอบดังนี้

- * รายงานการตรวจสอบฉบับร่าง (Examiner's pencil copy) จะต้องส่งไปยัง regional office เพื่อตรวจงาน (review) จัดพิมพ์ (processed) และจัดส่ง (distribution) ต่อไป
- * จะจัดส่งรายงานให้แก่ Washington Office, ศูนย์ข้อมูลที่ได้รับการตรวจสอบ (the data center examined) และสาขา (subregional office) ของธนาคารนี้จะต้องเก็บไว้รวมกับกระดาษทำงานจากการตรวจสอบด้านอื่น ๆ (Commercial examination work papers) เพื่อใช้อ่านเป็นการเตรียมการตรวจสอบครั้งต่อไป รายงานอีกฉบับหนึ่งจะต้องส่งให้กับ subregional office ของผู้ตรวจการ EDP ที่มีหน้าที่พิจารณาติดตามและแนะนำในการตรวจสอบครั้งต่อไป
- * ภายใต้ดุลยพินิจของ Regional Administrator, อาจมีการส่งสำเนารายงานการตรวจสอบให้แก่ National Bank ทุกธนาคารที่ใช้บริการของศูนย์คอมพิวเตอร์ที่ตรวจสอบก็ได้ หรือ Regional Administrator อาจใช้วิธีแจ้งไปยังธนาคารสมาชิกที่ใช้บริการของศูนย์คอมพิวเตอร์ที่ได้รับการตรวจสอบดังกล่าวว่าได้ตรวจสอบศูนย์คอมพิวเตอร์นั้นเสร็จสิ้นแล้ว หากธนาคารใดประสงค์จะได้รายงานการตรวจสอบดังกล่าวเพื่อไปศึกษารายละเอียดก็ให้เขียนจดหมายไปขอได้จาก Regional Office
- * สำเนารายงานการตรวจสอบบางฉบับอาจจะจัดส่งให้สถาบันอื่นที่มีหน้าที่ควบคุมธนาคารพาณิชย์ (Other Regulatory Agencies) รวมทั้ง State examining authorities ด้วยตามที่ขอมาโดยถือเป็นการแลกเปลี่ยนซึ่งกันและกัน (on a reciprocal basis)
- * ถ้าปรากฏว่าศูนย์ข้อมูลใดให้บริการแก่ธนาคารหลายแห่งที่ตั้งอยู่ต่างท้องถิ่น (National Bank Region) ก็จำเป็นต้องส่งรายงานการตรวจสอบให้กับที่เห็นว่าเหมาะสม

2.7 วิธีตรวจทานรายงานและการติดตามผล

เมื่อทำรายงานการตรวจสอบเสร็จแล้ว ก่อนที่จะจัดส่งรายงานฉบับสุดท้าย (final report) ไปควรจะได้มีการตรวจสอบความถูกต้องเกี่ยวกับตัวเลข, สภาพการทำงานของศูนย์ข้อมูล เนื้อหาของรายงาน การตรวจสอบตลอดจนวิธีปฏิบัติในการติดตามผล การตรวจทานรายงานนี้จะต้องกระทำโดย National EDP associate ส่วน Washington Office จะเป็นผู้ตรวจทานเกี่ยวกับความต่อเนื่องของการตรวจสอบ (continuity) เนื้อหาและความเพียงพอของการติดตามผล

รายงานหน้าการวิเคราะห์จะทำโดยผู้ตรวจสอบด้าน EDP และส่งให้แก่ Regional Office พร้อมกับร่างรายงานการตรวจสอบ ซึ่ง Regional Office จะเป็นผู้ตรวจทานรายงานการตรวจสอบดังกล่าว พร้อมทั้งให้คะแนนเพื่อจัดอันดับศูนย์ข้อมูลดังกล่าว นั้น โดยมีสำเนาการให้คะแนนไว้ติดตามเปรียบเทียบกับ การตรวจสอบครั้งต่อไป

และจัดอันดับจัดส่งไปพร้อมกับรายงานการตรวจสอบให้แก่ Washington Office และผู้ตรวจการด้วย

การเขียนคำวิจารณ์รายงานการตรวจสอบจะเป็นหน้าที่ของ EDP associate และมีสำเนาถึง Washington Office

คณะกรรมการสนับสนุนด้าน EDP ของสำนักงานวอชิงตัน จะเป็นผู้กำหนดมาตรฐานและนโยบายในการตรวจสอบ นอกจากนี้ คณะกรรมการดังกล่าวยังพร้อมที่จะให้คำปรึกษาทั้งทางเทคนิคและวิธีการในกรณีที่มีปัญหายุ่งยากหรือมีเหตุการณ์ผิดปกติ

3. การพัฒนาการตรวจสอบคอมพิวเตอร์ของ FDIC (Washington D.C.)

ระบบคอมพิวเตอร์ได้เข้ามามีบทบาทในวงการธนาคารพาณิชย์ในประเทศสหรัฐอเมริกาแล้ว FDIC ซึ่งเป็นหน่วยงานหนึ่งที่ควบคุมธนาคารพาณิชย์ในประเทศสหรัฐอเมริกาจึงได้จัดตั้งหน่วยงานตรวจสอบคอมพิวเตอร์ขึ้นมาโดยเฉพาะในปี 1960 และได้ขยายหน่วยงานนี้และหน่วยงานที่เกี่ยวข้องตลอดมา และได้ขยายหน่วยงานนี้และได้ยกฐานะเป็นสำนักงานให้มีทุกสำนักงานซึ่งประจำอยู่ตามรัฐต่าง ๆ รวม 14 แห่ง ด้วยกัน แต่สำหรับ OCC ได้ยกฐานะเป็นฝ่ายโดยให้ Regional Office ทั้ง 14 แห่งมี EDP Director ประจำทุกแห่ง

เดิมทีเดียวหน่วยงานคอมพิวเตอร์นี้ทำหน้าที่ประมวลผลและให้การอบรมความรู้ในการเขียนโปรแกรมให้แก่ผู้ตรวจสอบด้วย จากการอบรมดังกล่าวก่อให้เกิดคณะกรรมการดำเนินงานเกี่ยวกับคอมพิวเตอร์ ประกอบด้วยตัวแทนของ FDIC, FRB และ OCC ในเดือนมกราคม 1962 ได้จัดให้มีการอบรมผู้ตรวจสอบของสถาบันทั้งสามขึ้น ในปีต่อ ๆ มา FDIC และ FRB ได้ร่วมกันปรับปรุงแก้ไขหลักสูตรการอบรมให้ดีขึ้น สำหรับ OCC นั้น มิได้เข้าร่วมอีกเลยหลักจากการอบรมในครั้งแรก ทั้งนี้อาจจะเพราะ OCC มีนโยบายในการตรวจสอบด้านคอมพิวเตอร์แตกต่างจาก FDIC ก็ได้

ประโยชน์ที่ได้รับจากการอบรมประการหนึ่งก็คือ มีแบบสอบถาม (questionnaire) สำหรับใช้ในการตรวจสอบด้านคอมพิวเตอร์ออกมาใช้เมื่อวันที่ 15 ตุลาคม 1962 ซึ่งได้รับการปรับปรุงแก้ไขให้ดีขึ้นเพื่อให้เหมาะสมกับระบบประมวลผลของธนาคารที่ใช้คอมพิวเตอร์เรื่อยมา แต่ยังไม่ทันสมัยนัก (เมื่อเทียบกับมาตรฐานที่วางไว้ในปัจจุบัน)

หน่วยงานนี้ได้ร่วมมือกับฝ่ายวิจัยใช้คอมพิวเตอร์ทำแนวโน้มเงินฝาก (deposit trend) พอถึงปี 1967 จึงใช้คอมพิวเตอร์ประมวลผลและจัดทำรายงานต่าง ๆ ตามต้องการ เพื่อศึกษารู้นและแนวโน้มของธนาคารแต่ละแห่ง

ในปี 1967 โครงการฝึกอบรมคอมพิวเตอร์ได้ทำสัญญาจ้าง Peat, Marwick, Mitchell and Company (PMM) ซึ่งเป็นบริษัทผู้สอบบัญชี (CPA) และที่ปรึกษา มาให้การอบรมผู้ตรวจสอบเกี่ยวกับคอมพิวเตอร์เป็นระยะเวลา 1 สัปดาห์ (ใช้ชื่อหลักสูตรว่า CECB-I) เพื่อปูพื้นฐานเบื้องต้นเกี่ยวกับคอมพิวเตอร์และการควบคุม ต่อมาในปี 1970 ได้จัดให้มีการอบรมขึ้นอีกเป็นระยะเวลา 2 สัปดาห์ (ชื่อหลักสูตร CECB-II) ตามสัญญาจ้าง PMM เช่นเดียวกัน โดยมีสำนักงานทางวอชิงตันเป็นผู้สนับสนุนโครงการ ประกอบกับผู้ตรวจสอบมีความต้องการที่จะรักษาประสิทธิภาพให้ทันกับภาวะการที่เปลี่ยนแปลงไปอย่างรวดเร็วและเพิ่มความรู้ในระดับกลางให้กว้างขวางยิ่งขึ้นด้วย จนถึงปี 1972 จึงได้เลิกสัญญากับ PMM และเปลี่ยนไปทำสัญญาจ้าง Information Services Branch (ISB) ซึ่งมีผู้ตรวจสอบและ

ช่างเทคนิคเป็นผู้บรรยาย ทำหน้าที่ให้การอบรมต่อไป นอกจากนี้ในปี 1972 ได้จัดให้มีการอบรมเพื่อหวังผลการปฏิบัติงานโดยเฉพาะทบทวนเป็นครั้งที่สองให้แก่ผู้ตรวจสอบอีกด้วย เนื่องจากบริษัทที่ให้การฝึกอบรมคอมพิวเตอร์แก่ผู้ตรวจสอบต้องทำหน้าที่จัดหลักสูตรอบรมตามโครงการนี้ด้วย และเพื่อให้หลักสูตรการอบรมมีเนื้อหาสาระพอสมควร จึงได้ขยายระยะเวลาฝึกอบรมออกไปนับแต่ปี 1973

สำหรับหลักสูตรที่ใช้ระยะเวลาการอบรม 2 สัปดาห์ (CECB-II) ที่มีมาตั้งแต่ปี 1962 ยังคงจัดให้มีเรื่อยมาจนถึงปัจจุบัน โดยมีการเปลี่ยนแปลงเนื้อหาบ้างเพื่อให้มีความสมบูรณ์ส่วนการอบรมที่ใช้ระยะเวลา 1 สัปดาห์ (CECB-I) ได้ถูกบรรจุไว้ในหลักสูตรการฝึกอบรมผู้ช่วยผู้ตรวจสอบอาวุโส (School for Senior Assistant Examiners) นับแต่ปี 1971 เป็นต้นมาผู้ตรวจสอบที่ผ่านการอบรมจะได้ความรู้ในการควบคุมและเทคนิคต่าง ๆ ซึ่งมีผู้ผ่านการอบรมในระดับ CECB-I และระดับ CECB-II มากกว่า 1,400 คน และ 600 คน ตามลำดับ เพื่อให้เนื้อหาและผู้บรรยายในหลักสูตรต่าง ๆ มีคุณภาพ จึงจำเป็นต้องจัดให้มีผู้ตรวจสอบเป็น “ผู้จัดหลักสูตร” ทำงานประจำเต็มเวลา 1 คน ปัจจุบันคณะกรรมการบริหารซึ่งเป็นผู้ควบคุมการตรวจสอบถูกกำหนดให้ทำงานประจำเต็มเวลาทันทีที่ได้มอบหมายงานที่ตนรับผิดชอบให้ผู้อื่นที่มารับมอบงานแล้ว ปัจจุบันผู้ตรวจสอบคอมพิวเตอร์อาวุโสได้รับการมอบหมายให้เป็นผู้ให้การอบรมแก่ผู้ตรวจสอบหลักสูตร CECB-I และ CECB-II มากขึ้น

ในปี 1971 ได้เพิ่มตำแหน่งช่างเทคนิคเพื่อทำหน้าที่ประมวลผลตามแบบฟอร์มที่ต้องการ และ DBS (Division of Bank Supervision) ได้เริ่มใช้เครื่องรับและส่งข้อมูล (เครื่อง Terminal) ติดต่อกับศูนย์คอมพิวเตอร์เป็นครั้งแรกด้วย นอกจากนี้ยังได้พัฒนาระบบการวิเคราะห์ประจำสัปดาห์ (Weekly Analysis System) โดยป้อนข้อมูลที่ได้รับจากการตรวจสอบเข้าคอมพิวเตอร์เพื่อทราบฐานะของธนาคารต่าง ๆ ซึ่งได้เริ่มใช้มาตั้งแต่ต้นปี 1972

ในปี 1973 มีปัญหาในการขยายตัวของ EFTS (Electronic Fund Transfers System) และขีดความสามารถในการควบคุมบางประการ เนื่องจากธนาคารเริ่มใช้คอมพิวเตอร์ขนาดเล็ก (mini computer) จำเป็นต้องคอยติดตามความเคลื่อนไหวที่ก้าวไปข้างหน้าอย่างไม่หยุดยั้ง ทั้งคอมพิวเตอร์ขนาดใหญ่และขนาดเล็ก ซึ่งทีมฝึกอบรมได้จัดให้มีหลักสูตรการใช้คอมพิวเตอร์ขนาดเล็ก (Small Computer Training Course) การฝึกอบรมได้เริ่มเป็นครั้งแรกเมื่อเดือนเมษายน 1978 และใช้คอมพิวเตอร์ของบริษัท IBM รุ่น System 3 ในการสอนที่ FDIC Training Center มาถึงปัจจุบัน (1978) โดยมีวัตถุประสงค์ที่จะให้ผู้ตรวจสอบสามารถใช้โปรแกรมสำเร็จรูปที่บริษัทผู้ผลิตคอมพิวเตอร์สร้างไว้สำหรับผู้ตรวจสอบใช้ในการตรวจสอบ (Examiner Support Program-ESP) สำหรับคอมพิวเตอร์ขนาดเล็กได้ และเพื่อให้ผู้ตรวจสอบทราบแนวทางการตรวจสอบในระบบนี้ด้วย นอกจากนี้ยังหวังที่จะเสนอแนะแนวทางการใช้คอมพิวเตอร์ขนาดเล็กที่ถูกต้องให้แก่ธนาคารต่าง ๆ อีกด้วย

ในปี 1973 FDIC ได้ใช้เวลากว่า 90 วันทำการทดลองเพื่อฝึกอบรมผู้ตรวจสอบและสำเร็จเป็นรูปร่างขึ้นมาได้ในปี 1974 โดยมีผู้ตรวจสอบที่ได้รับการอบรมระดับสูง 2 คน เป็น FEAAT (Field Examiner Advanced Automation Training) FDIC ได้ใช้โปรแกรมสำเร็จรูปจากบริษัทผู้ผลิตคอมพิวเตอร์สำหรับผู้ตรวจสอบใช้ในการตรวจสอบ (Examiner Support Program - ESP) ในปี 1974 ตามคำแนะนำของบริษัทที่ปรึกษา โดยใช้กับการเงินให้กับยืมชนิดผ่อนชำระซึ่งเคยทดสอบในชั้นเรียนของผู้ตรวจสอบชั้นสูงรุ่นบุกเบิก (FEAAT) มาแล้ว

FEAAT ได้เริ่มใช้ ESP เพื่อช่วยในการตรวจสอบธนาคารทางด้านเงินให้กู้ยืมทั้งชนิดธรรมดาและชนิดผ่อนชำระ เงินฝากทั้ง 3 ประเภท และงานอื่น ๆ (เช่น เงินให้กู้ยืมแก่ธุรกิจและทรัสต์) สุดแต่ความต้องการ ผู้ตรวจสอบคอมพิวเตอร์ได้พิสูจน์ให้เห็นแล้วว่า ESP มีประโยชน์ต่อการตรวจสอบมาก (ในทัศนะของ FDIC) เช่น ช่วยลดงานเกี่ยวกับการลอกกรายงานของผู้ตรวจสอบให้น้อยลง ได้รับข้อมูลครบถ้วนตามความต้องการ และช่วยตรวจสอบการบันทึกบัญชีของธนาคารโดยอิสระ นอกจากนี้ผู้ตรวจสอบยังแสดงให้เห็นว่าเป็นผู้ที่มีความรู้ในการตรวจสอบคอมพิวเตอร์อย่างลึกซึ้งอีกด้วย (ด้วยความรู้ลึกซึ้งที่ว่าข้อมูลในการตรวจสอบของ Financial examiner ได้มาจากการเตรียมงานของ EDP examiner ของ FDIC เอง มิได้ใช้ข้อมูลของธนาคาร ซึ่งเรื่องนี้ผมมีความเห็นว่า FDIC ทำข้อมูลบางประเภทได้โดยอาศัยข้อมูลจาก file ของธนาคารนั่นเอง เพียงแต่นำมาดัดแปลงเป็นอีกรูปแบบหนึ่งตามที่ต้องการ) อย่างไรก็ดี เทคนิคการใช้ ESP ในการตรวจสอบส่วนใหญ่เป็นการอำนวยความสะดวกต่อการตรวจสอบด้านธรรมดา (Financial Examination)

เนื่องจากความรับผิดชอบและธนาคารใช้คอมพิวเตอร์ประมวลผลมากขึ้นจึงจำเป็นต้องมีการปรับปรุงแก้ไขแนวทางตรวจสอบและแบบฟอร์มที่ใช้ในการตรวจสอบใหม่เสมอ ดังที่ได้กล่าวไว้แต่แรกแล้วว่า แบบสอบถามที่ใช้ในการตรวจสอบ EDP ที่นำออกมาใช้ใน 1962 นั้น ไม่ค่อยสมบูรณ์นัก และถูกปรับปรุงแก้ไขทุกปีจนถึงปี 1970 จึงนับว่ามีเนื้อหาพอสมควร ได้ถูกปรับปรุงใหญ่อีกในปี 1974 เพื่อเปลี่ยนแปลงวิธีการตรวจสอบโดยไม่ใช้โปรแกรมช่วยในการตรวจสอบให้เหมาะสมด้วยซึ่งเป็นเวลาเดียวกับการปรับปรุงแก้ไขโปรแกรมที่ใช้ในการตรวจสอบเป็นครั้งที่สี่ เพื่อให้มีเนื้อหาสาระและมีคุณภาพดีขึ้น นอกจากนี้ยังต้องการผู้ตรวจสอบคอมพิวเตอร์ที่มีประสบการณ์ที่สูงกว่านี้ซึ่งต้องใช้เวลาที่ยาวกว่า

อย่างไรก็ดี เมื่อต้นปี 1978 ทาง FDIC, FRB และ OCC ได้ร่วมประชุมหารือเพื่อพิจารณากำหนดแนวทางการตรวจสอบและประสานงานการตรวจสอบด้วยกัน ผลการประชุมสรุปได้ดังนี้

- 1) ทั้ง 3 สถาบัน ตกลงใช้แบบ Questionnaire ของ OCC เป็นหลักในการตรวจสอบด้านคอมพิวเตอร์ โดย FDIC และ FRB จะเริ่มใช้ตั้งแต่ปลายปี 1978 หรือต้นปี 1979 เป็นต้นไป
- 2) จัดให้มีการแลกเปลี่ยนรายงานผลการตรวจสอบระหว่างกัน กล่าวคือ ถ้าตรวจสอบธนาคารในความรับผิดชอบของตนก็จะส่งรายงานผลการตรวจสอบที่ได้จัดพิมพ์เรียบร้อยแล้วไปให้ FDIC และ FRB หรือกลับกัน เป็นต้น ทั้งนี้ จะเป็นประโยชน์อย่างยิ่งในกรณีที่ธนาคารใช้บริการจากบุคคลภายนอกร่วมกัน (ธนาคารไม่มีเครื่องคอมพิวเตอร์เป็นของตนเอง แต่นำข้อมูลไปจ้างบริษัทภายนอกที่ใช้คอมพิวเตอร์ process ข้อมูลให้ เพราะ EDP examiner ของสถาบันเหล่านี้จะได้ไม่ต้องส่งผู้ตรวจสอบของตนออกไปตรวจซ้ำอีก)

ความต้องการที่จะยกระดับการตรวจสอบคอมพิวเตอร์ให้ดีขึ้นทำให้เกิดความจำเป็นที่จะต้องมีการปรับปรุงแก้ไขวิธีการให้ดีขึ้น และมีการติดตามผลอยู่ตลอดเวลา ได้มีการตรวจสอบและทบทวนแก้ไขบทบัญญัติที่เกี่ยวข้องติดต่อประสานงานกับผู้ควบคุมการตรวจทุกเขต (ทั้ง 14 เขต) ปรับปรุงแก้ไขคู่มือปฏิบัติงานและแบบฟอร์ม ทำงานตามที่ได้รับมอบหมาย ดำเนินการและวางนโยบายการตรวจสอบคอมพิวเตอร์

ฝ่ายอำนวยการได้กำหนดให้มีการพัฒนาเพื่อใช้คอมพิวเตอร์ให้เป็นประโยชน์ต่อไปในการบริหารและควบคุมดูแล โดยใช้ DMSFS (Division of Management System and Financial Statistics) ช่วยดำเนินการ

เครื่องรับส่งข้อมูลตามสายโทรศัพท์ (on-line terminal) เครื่องแรกของฝ่ายได้ติดตั้งเมื่อปี 1970 ปัจจุบันติดตั้งไว้ที่สำนักงานวอชิงตัน 6 เครื่อง โดยใช้ติดต่อรับส่งข้อมูลกับสำนักงานเขตต่าง ๆ 3 เครื่อง ใช้สำหรับศูนย์ฝึกอบรม 2 เครื่อง ที่เหลืออีก 1 เครื่อง ใช้สำหรับวางแผนและส่งโครงการให้สำนักงานต่าง ๆ ปัจจุบันจะมีการทดสอบการรายการที่เกิดขึ้นในระบบ on-line และทำการแก้ไขตามแบบฟอร์ม แต่ระบบนี้ยังไม่ประสบผลเท่าที่ควร ทั้งที่ได้ตั้งใจนำมาใช้ตั้งแต่ปี 1973 จวบจนถึงปัจจุบันมีงานใหม่ ๆ หลายอย่างที่สามารถจะเพิ่มเติมเข้าไปช่วยให้ประสิทธิภาพในการบริหารดีขึ้น

นอกจากนี้ สำนักเขตทุกแห่งจะมีเครื่อง on-line terminal ติดตั้งไว้ ดังนั้นส่วนตรวจสอบคอมพิวเตอร์จึงมีหน้าที่รับผิดชอบฝึกอบรมผู้ใช้เครื่อง DBS ทุกคนด้วย เช่นเดียวกับการชี้แนวทางการใช้ระบบ on-line ในการควบคุมดูแล

Integrated Monitoring System ที่จะนำมาใช้ในปลายปี 1977 อยู่ในระหว่างการพัฒนามาตั้งแต่กลางปี 1974 ส่วนตรวจสอบคอมพิวเตอร์ได้ประเมินสถานการณ์ไว้แล้วตั้งแต่ปี 1974 ถึงปี 1976 ซึ่งในปัจจุบันรับผิดชอบด้านข้อมูลที่ป้อนเข้าคอมพิวเตอร์สำหรับใช้ในระบบบัญชี เพื่อให้เขตต่าง ๆ จัดทำ Action Report และให้ความช่วยเหลือทางด้านเทคนิคแก่สำนักงานต่าง ๆ นอกจากนี้ยังต้องรับผิดชอบในการให้ความช่วยเหลือทางด้านเทคนิคแก่ส่วนวิเคราะห์ (Analysis Section) และจะต้องติดตามดูแลการปฏิบัติงานของตัวแทนที่ใช้เครื่องฟางอื่น ๆ ด้วย

ในแต่ละปี ส่วนงานนี้จะจัดให้มีการประชุมผู้ตรวจสอบคอมพิวเตอร์ 1 ครั้ง และมีการสัมมนาในระดับ FEAAT ปีละ 2 ครั้ง ถึง 4 ครั้ง ในปี 1978 ได้จัดหลักสูตรอบรมคอมพิวเตอร์ขึ้นมาใหม่สองหลักสูตร หลักสูตรแรกเป็นสูตรสำหรับผู้ที่เคยผ่านการอบรมในระดับ FEAAT มาแล้ว เพื่อฝึกใช้โปรแกรมสำหรับตรวจสอบคอมพิวเตอร์แบบใหม่ที่ยังมิได้นำออกมาใช้ ส่วนอีกหลักสูตรหนึ่งเป็นการสัมมนาของผู้ที่เคยอบรมหลักสูตร CECB-II มาแล้ว ซึ่งเป็นเรื่องเกี่ยวกับบทบาทของคอมพิวเตอร์และ DFTS

อย่างไรก็ดี หน่วยงานตรวจสอบด้านคอมพิวเตอร์ถึงแม้จะมี Washington D.C. เป็น Administrator Office ก็ตาม รายละเอียดในการตรวจสอบและการตัดสินใจข้อปลีกย่อยย่อมขึ้นต่อหัวหน้าหน่วยงานด้านคอมพิวเตอร์ที่ประจำในแต่ละ Regional office ด้วยเช่น การใช้ package ในการตรวจสอบ ซึ่ง FDIC ที่ Washington D.C. ต้องการให้แต่ละ Regional Office ใช้ แต่ในทางปฏิบัติ Regional Office บางแห่งยังไม่พร้อมจะใช้ ทั้งนี้เพราะมีปัญหาด้านพนักงานที่จะใช้ เป็นต้น

เมื่อทาง FDIC ที่ Washington D.C. รับรายงานมา งานที่เกี่ยวข้องกับการตรวจสอบด้านคอมพิวเตอร์จะถูกส่งมาทาง Automation Section ซึ่งจะทำให้การทบทวนมาตรฐานการปฏิบัติงาน ทำประวัติและบันทึกผลการตรวจสอบ ตลอดจนข้อมูลที่สำคัญ ๆ ลงในเครื่องคอมพิวเตอร์ในระบบ on-line เมื่อต้องการจะติดตาม พนักงานหรือผู้ที่เกี่ยวข้องก็สามารถกดปุ่มสอบถามเครื่อง Terminal เพื่อดูข้อมูลทางจอรับภาพได้ทันที และถ้าต้องการเป็น

paper ก็กดปุ่มให้ printer พิมพ์มาให้ก็ชุดในทันทีก็ได้ การบันทึกสถิติและข้อมูลที่สำคัญ ๆ ที่ได้จากการตรวจสอบ หรือจากรายงานที่ธนาคารพาณิชย์ต่าง ๆ ที่ประกันเงินฝากไว้กับ FDIC ส่งมาให้นี้ ทาง Regional Office ทั้ง 14 แห่ง สามารถติดต่อหรือ key ถามข้อมูลที่ต้องการดูแลธนาคาร แต่ละเรื่องได้ทั่วประเทศสหรัฐอเมริกาในทันทีเช่นเดียวกับที่ Washington D.C.

ในกรณีที่ FDIC ณ Washington D.C. ไม่เห็นด้วยกับรายงานการตรวจสอบในบางเรื่อง (ซึ่งทาง Regional Office ได้ส่งให้ธนาคารที่เกี่ยวข้องแล้ว ทาง Review examiner-EDP ที่ประจำอยู่ ณ Washington D.C. จะ comment เพิ่มเติมลงไปใน Summary of data processing evaluations ฟอรัม และเก็บเข้าแฟ้มไว้โดยไม่ต้องรายงานต่อให้ใครอีก ในทางปฏิบัติ review examiner-EDP จะโทรศัพท์ไปหารือกับ review examiner ของ Regional office ที่เกี่ยวข้องก่อน

ข้อ Comment เพิ่มเติมที่ทาง Review examiner-EDP ประจำ Washington D.C. จะถูกรวบรวมไว้เพื่อเป็นหัวข้อที่ใช้ในการสัมมนาประจำปีต่อไป



ภาคผนวก ฉ

Role of The Bank of Thailand in Banking Computerization

by

Mr. Metha Suvanasarn

Director

Bank of Thailand, Northeastern Region Branch

**Keynote Address to the 12 th Annual Asia Pacific Computer Audit, Control and Security (CACS) Conference,
23 September 1996, at the Imperial Queen's Park Hotel, Bangkok.**

Role of the Bank of Thailand in Banking Computerization

Mr. Akha Matsuo, International President

Distinguished delegates and participants,

Ladies and Gentlemen,

Good morning, I would like to welcome those of you from abroad and in Thailand, to participate in this conference. Hopefully you have a pleasant stay in Bangkok.

1. Introduction

This keynote session emphasises the importance of information quality with a view to the 21st century. I am honored, therefore, to have the opportunity to address the "Role of the Bank of Thailand in Banking Computerization" in this respect, to this, the 12 th Annual Asia Pacific CACS Conference, sponsored by the Information Systems Audit and Control Association.

As a brief background: Computerization of banking business was introduced to Thai Commercial banks in 1970. In 1982, or 12 years after the Bangkok Bank's first on-line computerized system was established, EDP Auditing was introduced to follow up this new technology in Thailand. The organization playing the role central to the success of the introduction of these systems is the Bank of Thailand. In this perspective, it is therefore appropriate that the topic of the "Role of the Bank of Thailand in banking computerization", is presented today.

The body of information technology professionals, that is, the IT audit and control specialists, are very crucial not only for IT auditing or IT system development but also the management of all commercial institutions.

The Information Systems Audit and Control Association (ISACA) represents an extremely critical linkage between these people and the organizations concerned. Without this link we cannot function, or would function with very much greater difficulty. This is due in large to the important responsibilities of the Bank of Thailand in supervising financial institutions to ensure that they are secure and are supportive of economic development and also to develop and supervise the financial system.

The major section of the Bank undertaking these responsibilities is the Financial Supervision and Examination Dept. Its main functions are to analyze and examine the operations of the financial Institutions and to develop efficient procedures for examining and analyzing financial statements. We have to thank the ISACA for its overall support which is also shown through its sponsorship of this 12 th annual Asia Computer Audit, Control and Security Conference, on this occasion, and of course, for the year to come.

The wide use of computers in banking and financial activities has contributed to remarkable changes in all financial institutions' operations, internal control, audit and management systems. New techniques and procedures for banking practice have been developed and implemented into Thai commercial banks and other organizations. In addition, a remarkable expansion of banking services has occurred through the on-line network between commercial bank Head Offices and their branches facilitating their customers requirements and recording and exchanging accounting information. This is especially so for depository and funds transfer transactions of inter-branch customers..

Even though computerization in banking can provide high efficiency with low cost to customers and banks, the complexity of computerized banking, at the same time, has brought new risks into the banking system. In this regard, the Bank of Thailand, as the supervisory agency, needs to closely control and supervise computerized banking and other financial organizations in order to reduce these risks and safeguard the banking system and its customers.

The relationship among internal auditors, CPAs and examiners

First of all I would like to explain and differentiate the words "Examiner", "External auditor", "CPA" or chartered accountant, and "Internal auditor". The examiner is a type of an external auditor but functions under the Central Banking Act and performs duties under the Commercial Banking Act and Financial Institution Act. The examiner works under regulatory agencies like FRB, FDIC or OCC in the USA or at the Bank of England. Prudential controls, safety and soundness of commercial banks and financial institution systems are the main function of the examiner. We may describe the main difference among them as follows:

The Examiners

The major function of the Examiner is on the safety and soundness of financial institutions under special Acts such as the Commercial Banking Act and Financial Institution Act. The Examiner is responsible for examination and supervision of the stability of the financial institutions that operate under these special Acts and they report to the Ministry of Finance and the Chairman of the financial institutions.

The CPAs

The major function of the CPAs is on the reliability of financial statements and financial exposures that may occur within the organization. The major responsibility is to perform substantive audits, verify and certify financial statements and audit the reliability and fairness of financial records including information that may cause exposures to the organization in reports to the shareholders and relevant persons of the organization.

The Internal Auditor

The major function of the Internal Auditor is concerned with the operational exposures that may arise from the disorder, the disregard or the violation of the organization's rules and regulations. The Internal Auditor is responsible for compliance auditing including internal exposures that may occur within the organization and report to the Board of Directors or the top management of the organization.

The Examiner, CPAs and Internal Auditor may be subdivided into two types: 1) the Financial Auditor and 2) the EDP or IS Auditor. The difference between the Financial Auditor and the EDP or IS Auditor is that the Financial Auditor focuses on the manual operation audit while the EDP or IS Auditor focuses on the computerized operation audit.

The major functions of the Examiner, CPAs and the Internal Auditor may differ as mentioned, however, in practice there are some functions that overlap among them. In general, the scope of the work of the Examiner is broader than that of the CPAs and Internal Auditors, while, in turn, the scope of the work of CPAs is also broader than the Internal Auditors.

In practice, even though the Internal Auditors concentrate on compliance auditing they also put emphasis on substantive procedures which is the major function of the CPAs. This is due to the fact that the results of substantive tests are seldom employed as part of a compliance audit. At the same time, the CPAs have to verify the results of a compliance audit, which is the major function of Internal Auditing, in order to support the reliability of their substantive test. Similarly, the Examiner, who performs much broader functions, needs to evaluate the results of a compliance audit and substantive audit which are the major functions of the Internal Auditor and CPAs. This is a minor part of their work in order to employ these results as supportive information for the assessment of safety and soundness of financial institutions.

2. Development of Computerized Banking in Thailand

2.1 Electronic Banking

As new service competition, ATMs were introduced in January 1983. In December 1984, the Bank of Thailand issued a major guideline on electronic banking development, by requiring banks to offer shared ATM services or a "pool" that must be comprised of at least 3 member banks. New products that were 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 a Commercial Bank known as "The Computer Branch" services. This provided self-service facilities at the branch lobby including Personal Banking, Current Account Statement Inquiry, ATM, Tele-banking, Info Banking, Graphic Banking, and Videotext Banking.

2.2 Other services

New concepts for computerized services are 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 to provide a database for all necessary financial and business information. This proposed computerized trade data center was first discussed in 1991. They also hope to collect business and financial data from overseas sources in the future.

2.3 Electronic payment system

The rapid growth of financial activities, the trend of increasing volumes of transactions in terms of paper notes, large-value fund transfers, retail fund transfers, and the global trend towards computerized payment systems is contributing to the development of a new Thai Payment System.

A Payment System Development Plan has been developed under the Bank of Thailand's financial reform scheme for the regional financial center in 1995. The plan has three major goals:

- 1) to improve the country's financial infrastructure
- 2) to reduce risk in the payment system, and
- 3) to increase the efficiency of fund transfers.

The plan outlines three phases. In phase I, the main tasks are to construct an interbank electronic funds transfer network in the Bangkok Metropolitan area to increase the efficiency of large-value fund transfers, cheque clearing, and off-line retail fund transfers. On-line retail fund transfers will be improved by the Thai Bankers Association meanwhile.

The Bank of Thailand has established two major electronic payment networks to support the phase I operation: 1) BAHTNET and 2) THAICLEAR. BAHTNET is an electronic funds transfer network between the Bank of Thailand and the member banks to service the large-value funds transfer transactions. THAICLEAR, meanwhile, is designed as an electronic cheque clearing system (ECS) and media clearing.

The second phase focuses on extending the service area, providing more services, and increasing the functions of the system. As a result, large-value fund transfers will be available in areas outside Bangkok and the clearing and settlement of both government and Bank of Thailand bonds will be in service. Eventually, the use of on-line file transfers for large volumes of low-value transactions will also be included in the system.

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

3. Major risks in computerized banking

3.1 Risk of system failure

When commercial banks apply electronic banking into their business, they immediately bear the risk of computer system failure. This is the risk that the system can not continuously process and operations are paused. In this instance commercial banks can not operate and provide services to their customers. The failure of computerized systems is the most significant risk of electronic banking, however, banks can reduce this risk by preparing supportive or emergency plans for such situations before significant damages will affect the bank's operations.

3.2 Risk of the loss of information

This is the risk that information in the system is damaged, lost or destroyed due to an absence of internal control and back up systems. Thus, when errors appear in the system when banks have no recovery system or audit trail system to retrieve the lost information, it will have severe implications for the banks. For advanced and complex technology systems, it is necessary to design these more carefully.

3.3 Risk of imperfect planning

The rushed development of computerized banking without an adequate study of both short term and long term impacts will create many problems in organizations. Such problems may include defective software or incompatible software which cannot be applied with older systems, lack of computer personnel, and inefficient organizational and personnel management including that of the internal control system.

3.4 Risk of inadequate internal control.

This is the risk that computerized systems accidentally or purposely accessed due to inadequate internal controls. This may lead to information files and system programs being destroyed, stolen, spied upon, changed, added or erased by an attempt to distort information. This lessens the reliability of financial statements which in turn requires the Bank of Thailand and IS auditors to examine these more carefully.

4. The impact of Electronic Banking on Commercial Bank examination and supervision.

In general, there are two major control methods for commercial bank supervision:

1. Supervision by regulations

The first control of supervision is through guidance by rule, regulations and provisions to commercial banks in the forms of Acts, notifications, circulars, and through licensing in accordance with authorities given by the Banking Act. These are in order to encourage sound banking practices and to standardize banking business corresponding to government policy and also to give the banks a strong position with high public confidence.

2. Supervision by bank operation following-ups

The second control method is to assess each commercial bank's status and follow-up the banks' operations to ensure that commercial banks activities are carried out in accordance with law and regulations and in an appropriate manner. This kind of work can be analyzed from the commercial bank's reports and on site audits at the banks and financial institutions.

The principles adhered to for commercial bank assessments and examinations are known as the CAMEL principles. These comprise of 1) Capital adequacy 2) Assets quality 3) Management 4) Earnings ability and 5) Liquidity position. Examiners will assess the bank's status from their financial statements such as their balance sheet and income statements including other items relating to such statements.

Banking business has developed and changed markedly in their operations and services compared with the past. New Banking technology and transactions have been introduced which have introduced various types of risks and difficulties required to be measured or evaluated. It is particularly important therefore to be aware of off-balance sheet business such as syndicate loans, letters of credit, foreign Exchange, wired transfers, Electronic Data Processing (EDP) or electronic banking etc. In this regard, the authorized examiners and supervisors of commercial banks have to study and understand the risk which may affect an assessment of the banks' status.

5. Electronic Banking Examination

The rationale and the necessity to have an electronic banking examination is due to the change of banking technology which, in turn, contributes to the change of banking practice and operations and leads to the various forms of risk that have already been mentioned. Subsequently, to protect possible financial disaster that may arise, the conventional "CAMEL" principles for banking examination may not be sufficient to evaluate the commercial banks status for the following reasons:

1. Conventional supervision and examination which evaluates the manual practice is mainly an evaluation of past evidence or after-the-fact. This is in instances such as balance sheet examinations, quality of lending, ability of asset and debt repayment, earnings ability, and the past performance of the banks.

2. Conventional supervision and examination is not concerned about the risk of loss as a result of inadequate security in computerized banking controls. Such losses may include financial data in the computer system, fraudulence through telecommunication systems, and risk of system failure which has a great effects on the commercial bank's operations.

3. The present examination does not, but should, emphasize evaluation of new management systems for electronic banking, and point out possible future problems before it points to us. This is due to the necessity of development under the rapid changes of technology. Strategic planning for technology and electronic banking should be implemented to ensure that the bank's executives are able to know the real position of the bank. In addition, this evaluation will help reduce the risk which may arise in the future which, as well, will be useful for determining the bank's direction now and in the future.

In order to have an efficient examination, one must be able to evaluate and analyze the bank's status correctly, appropriately, and be up-to-date. Electronic banking examination, therefore, needs additional examination measures besides those ordinarily employed corresponding to the rapid changes of Banking technology. In some developing countries, the central banks never consider these problems.

5.1 Audit and Control summary in a computerized business environment

Computer Technology creates new and increased risk which requires New Methods of Audit and Control and needs Auditors with new skills to review Computer Technology and associated technology and systems.

5.2 Electronic Data Processing (EDP) Examination

During 1970-1981, commercial bank examination always concentrated on financial examination by way of evaluating documents, reports and financial statements that were produced by the computer. With these banks, the provision of information, verification of data accuracy and reliability, had been limited. There had over this time been a gradual increase in the examiner's concern as to how to maintain their role and capability for conducting effective and appropriate banking examinations. In 1972, the Bank of Thailand set up a working group of the EDP examiners to study the feasibility and guidelines on the electronic data processing examination. In 1981, the Commercial Bank's Computer Examination Section was established to perform EDP or IS audit. At that time, there were no EDP or IS auditors in Thailand.

Sequences of EDP examination development:

1. The manual or guidelines on how to use commercial bank computerized reports was developed in order to support the financial examination that included:

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

- 1.2 Reports and Transaction Code definitions.

- 1.3 Reporting frequency such as daily, weekly, monthly, or semi-annually including the reports and file retention periods.

- 1.4 Reconciliation of report total and control accounts.

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 banks with guidelines on the EDP operation and the EDP examination scope.

4. The commercial bank EDP examination was first conducted in 1983.

5.3 Security Requirements for Commercial Banks setting up and Operating Electronic Machine Services

The minimum standard requirements on security procedures:

1. Segregation of duties and responsibilities under 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 equipment currently in use and backup equipment
 - Data management and backup data files.
 - Interrelationship of all application system and control functions.
 - Output report description of all applications.
 - 2.2 Program Description Manual
 - Detailed description of the individual program including objectives, function processing instructions and the interrelationships to the other programs.
 - Program listing
 - Editing and control procedures
 - Record of all program changes and system modifications
 - 2.3 User Manuals
 - Description of their functions and responsibilities.
 - User operation instructions
 - Error and problem resolution procedures

2.4 Electronic funds transfer system documentation.

- Equipment description
- Customer card
- Customer personal identification number
- Program messages
- ATM Cash Handling
- Data Communication commands and messages
- Receipt of Funds Transfer Transactions
- 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 Logging all transactions to include:

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

4. Customer Security

- Must have written notices to educate the customers on usage and safeguarding of the ATM card and PIN including warnings and precautionary measures upon 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 messages or protective devices to prevent the customers' failure to retain their card and receipt of transaction after the completion of the transaction.

5. Site Location Security

- The terminal devices must be situated publicly in an open area with sufficient lighting for illumination.
- The terminals must have an installed 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 defines methods and procedures for system recovery.

7.3 Backup Plan that provides minimum requirements as follows:

- Must provide a back up capability for data facility
- Backup procedures and operational instructions including the use of alarm or security devices 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 critical functions in order to define backup processing requirement.

5.4 EDP Audit Requirements

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 organizations or Service Bureaus

1.2 Computer Application

- Documentation
- System Tests
- Application and Program Maintenance
- Data Access Control
- Data Files and Program Controls
- Backup System

1.3 Financial loss caused by computer operation or computer internal control weakness by the following causes.

- Failure or destruction of the computer system, equipment, peripheral, Application Systems, and Data Communication System.
- Fraud, theft or any loss which is caused by a 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 measures implemented

2.7 Application System Audit Documentation.

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

6. Bank of Thailand's measures and policies regarding computerized banking.

6.1 The main objective of The Bank of Thailand

The main objective of the Bank of Thailand is to maintain both internal and external financial stabilization, enhance sound financial institutions and encourage economic growth at the appropriate level.

The progress of telecommunication technology has caused the world's financial businesses to have close relations, in both domestic networks and internationalized networks. Financial institutions, the international money market and the capital market are globalized. Financial systems for both commercial banks and other financial institutions have to concentrate on improving their efficiency and at the same time, the Bank of Thailand has to keep this under surveillance to ensure that these improvements are not frustrated or result in decreased stability of the banking system.

The electronic banking examination is not committed only to the computerized systems and its operations but also extends to analyze and evaluate the risks of banking technology and electronic banking. This additional analysis is aimed at controlling and discriminating all risks associated with commercial bank stability as a whole and especially for protection before damages occur.

The Bank of Thailand has paid attention to electronic banking services and followed-up on the commercial banks' progress. Since 1981 the Bank of Thailand has established the Special Assignment Division to examine electronic banking and to take part in the process of setting up regulations and conditions for the opening of commercial banks' ATM services. These regulations set minimum security requirements in order to strengthen security and to safeguard the bank's customer. In addition, the BOT also continues its study on new technology that commercial banks have implemented in their banking services.

6.2 Revision of the Banking Act and Other Regulations

6.2.1 Banking Act

In May 1985, the Bank of Thailand formalized the enforcement policy amending the Banking Act. For the electronic banking examination practice, a revision had been made on section 35, to empower the examiner to examine banks' electronic data processing systems and/or their EDP services.

6.2.2 Contingency Plan

On December 24, 1987 the Bank of Thailand invited commercial banks to attend a meeting on the subject of the development of an Emergency Plan and a computer backup system. The meeting was held on January 14, 1988. The Bank of Thailand 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 Contingency Plans should include effective provisions for off-site backup of critical data files, software, hardware, documentation, forms, and supplies as well as an alternate means of processing transactions electronically or manually. Bank management should review and employ the most appropriate method for its organization.

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

1. Commercial banks must develop a contingency plan that provides an alternative backup system off-premises and shall be completed by 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 by Bank of Thailand.

3. To minimize cost and fully utilize resources, commercial banks are advised 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 computer facilities.

6.2.3 External Auditor

According to the Auditing standard no. 28 and 29 issued by the Institute of Certified Accountants and Auditors of Thailand in March 1990, chartered accountants in Thailand are required to evaluate internal controls in the EDP environment system and it is insisted that they use computers as audit tools. Prior to their appointments, commercial bank & financial institution auditors have to submit EDP audit programs to the Bank of Thailand for approval.

6.2.4 Minimum Standard of Information

In April 1991, minimum standards of information were set as a guide for designing and keeping data processing records required to expedite supervisory examinations.

6.2.5 Data Processing by a Third Party

Commercial banks and/or financial institutions may have their data processed by external data processing services, 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 permission from the Bank of Thailand to establish the conditions that have to be made in the agreement with the servicers or third parties. This may allow the Bank of Thailand's examiners to perform EDP examinations at the data center of the servicers or third parties.

6.2.6 Summary of measures relating to control of commercial banks

Measures, regulations and conditions which have been determined in order to increase efficiency, accuracy and reliability of commercial banks' accounting and financial systems can be summarized as follows:

Year	Sequence	Subject	Rationale
1981	1	Establish Commercial Banks' Computer Examination Section.	To study and develop the supervision and examination of computer tasks and to conduct instructions of appropriate computer operations in order to reduce computer failure risks to commercial banks.

Year	Sequence	Subject	Rationale
1982	2	Send inspectors to inform commercial bank executives of forth-coming computer examinations. Distribute "The Computer Operation and Data Processing of Commercial Banks" which outlines guide-lines for these examinations.	To ensure commercial bank executives realize and accept administration and systems of standard computer use and efficiency and to generally accompany this by advanced instruction on the necessities of controlling computer operation.
1985	3	The commercial banks have to set up a computer security system to meet minimum standard requirements.	To reduce risk that may affect security and continuity of operation of commercial banks.
1985	4	Once in every 12 month period, commercial banks must perform computer auditing that involves adequate examination as the BOT assigns, and submit a report on this to the BOT.	To enhance commercial banks' provision of internal EDP auditing, especially for developing the examination system. This system must be compatible with other developments, such as SDLC, and other systems for catching up to commercial bank computer technology which is getting more sophisticated.

Year	Sequence	Subject	Rationale
1988	5	The commercial banks must install emergency and recovery plans outside their host computer building and these must be ready to utilize before 1989.	To protect the commercial banks services from sudden shut-down, whether caused by hardware, software, or people ware, no later than 1988. The temporary cessation of services caused by computer or any technical problems must not extend beyond one day.
1988	6	The commercial banks' external auditors must submit both financial and computer auditing programs to BOT in order to get consideration and approval from BOT to be the banks auditors.	To evaluate auditor efficiency and reliability financially as appropriate to their business and data processing requirements from the year 1988.
1988	7	Set up conditions far data processing outside the country and evaluate the procession of the data center of the third party both in domestic and in foreign countries.	To maintain the standard of financial examinations from third parties and the EDP examinations. This is also to serve the country's objective of being the monetary center of its region.

Year	Sequence	Subject	Rationale
1990	8	Study new types of risks from computer technology in today's banking and financial institutions.	To protect and reduce risks which may occur from computer technology and their applications that commercial banks and other financial institutions now utilize. This is especially so for electronic fund transfers and netting schemes both at the domestic and international levels. Such risks include systemic risk, settlement risk, receiver risk, sender risk, and liquidity risk.
1990	9	Study minimum standards of information (MSI) that is necessary for financial examinations.	To protect the financial examination from the problems of technology and the paperless system. Some types of hard copies are now limited by the current system.

Year	Sequence	Subject	Rationale
1993- 1996	10	Reform the Clearing and Settlement Systems. This is known as payment system development, a part of BOT's financial sector reform. These consist of: - BAHTNET - Electronic Cheque Clearing System (ECS) - Media Clearing	To reduce the costs of note printings, storage and consignment. To increase the efficiency and integrity of the payment system.

In addition to these measures there has been cooperation between the financial examiners, EDP examiners and analysts to develop the examination of commercial bank supervision and examination.

As a result of these obligations it is necessary to have an instrument to oversee the electronic banking activities in accordance with banking law and regulations. The examination may be conducted by on site examination or by analyzing and evaluating the bank's reports.

Similarly, examination of electronic banking and electronic services needs instruments and supportive factors to help the examination process. This is in order to determine the appropriate direction which should be most useful for the banking system. The techniques used however require continual updates as the commercial bank's business and technology grows and advances. Using old techniques to oversee and examine these banks may be out-of-date thereby not revealing the real situation. The Bank of Thailand therefore must pay more attention to computer and electronic banking examination and supervision.

The proper methodology of the audit therefore assists the auditor in determining:

- : what should be done
- : what documentation should be examined or obtained.
- : when it should be done
- : what can go wrong, what should be right, and to know what needs to be controlled and audited.

The IT auditor must understand:

- The basic flow of transactions through each significant EDP application.
- The basic control structure
- The content of EDP files and the relevance of the data to financial statements, and of course IT auditor must understand

- Where computer assisted audit technology is employed
- EDP or IT control review and the application of computer-assisted auditing technologies must be performed by persons with technical proficiency appropriate to the complexity of the system under review.

It is generally true that the more competent and control conscious the strategy is from the risk environment of the IT, and the better the understanding of the application relation complexities of the audit personnel, the less difficult will be the auditing. Don't forget that, people are not the system of internal control but people make the system of internal control function. A poor system of internal control monitored by highly competent people frequently works much better than an excellent system of internal control staffed with incompetent people. Competence is the ability to perform the assigned tasks and at the same time show the initiative and alertness to anticipate and correct problems before they become serious.

All of what I mentioned earlier are the main goals and are included in the role of the Bank of Thailand.

6.2.7 Other related issues

Study and develop relevant activities which have an effect on commercial bank's supervision and examination under the following scope:

- The development of commercial technology, hardware and software of computer.
- The innovation of technology affecting the commercial bank's planning and control.
- Risk arising from electronic banking, both wholesale and retail services including those associated with major services which commercial banks offer at present.

- The determination of emergency plans protects against damages from the use of electronic systems, both internally and externally in banking business
- The additional alternatives of commercial bank's supervision which may be suitable and could be taken as part in the standardization of the bank's system.
- The amendment of laws and regulations relating to banking technology.
- The impact of technological evolution to commercial bank examination and supervision policy.
- The Bank of Thailand which is responsible for the stability of the financial system, is required to take all these factors into consideration and needs to balance the following activities:
 1. The encouragement of banking system stability and safe and sound banking practice following the set regulations.
 2. The encouragement of banking business towards high efficiency high reliability and high stability.

7. Conclusion

The changing methods of information technology and processing requires all levels of management and auditors to evaluate their responsibilities for establishing and maintaining a proper structure of control throughout the organization.

Auditing in a computerized business environment requires approaches and skills different from those required for audits of entirely manual systems. Experience has shown that because of the misunderstanding between users and managers on one side, and the IT or EDP personnel on the other, most control problems can be associated with the point at which the clerical and automated systems meet.

IT is playing a more important role in Thailand. The understanding among the users, IT managers and IT auditors is very important for the success of their operation, audit and control in a computerized business environment.

The next step of the IT auditor and managers of all organizations should be to prepare themselves for further study of IT technology to cope with IT management and auditing in the dynamic world of technology and new products of the banking and financial business.

The 12 th Annual Asia Pacific CACS Conference sponsored by ISACA gives one of the best opportunities for learning, practising and gaining the new IT experience through its sessions covering many interesting IT topics. These relate to exploring current technology and its impact on auditing, control and security which are also included in the conferences workshops. These will enlighten its participants to follow the right path.

Hopefully, all the delegates and participants will find the information gained in the following days most fruitful to the improvement of your career paths.

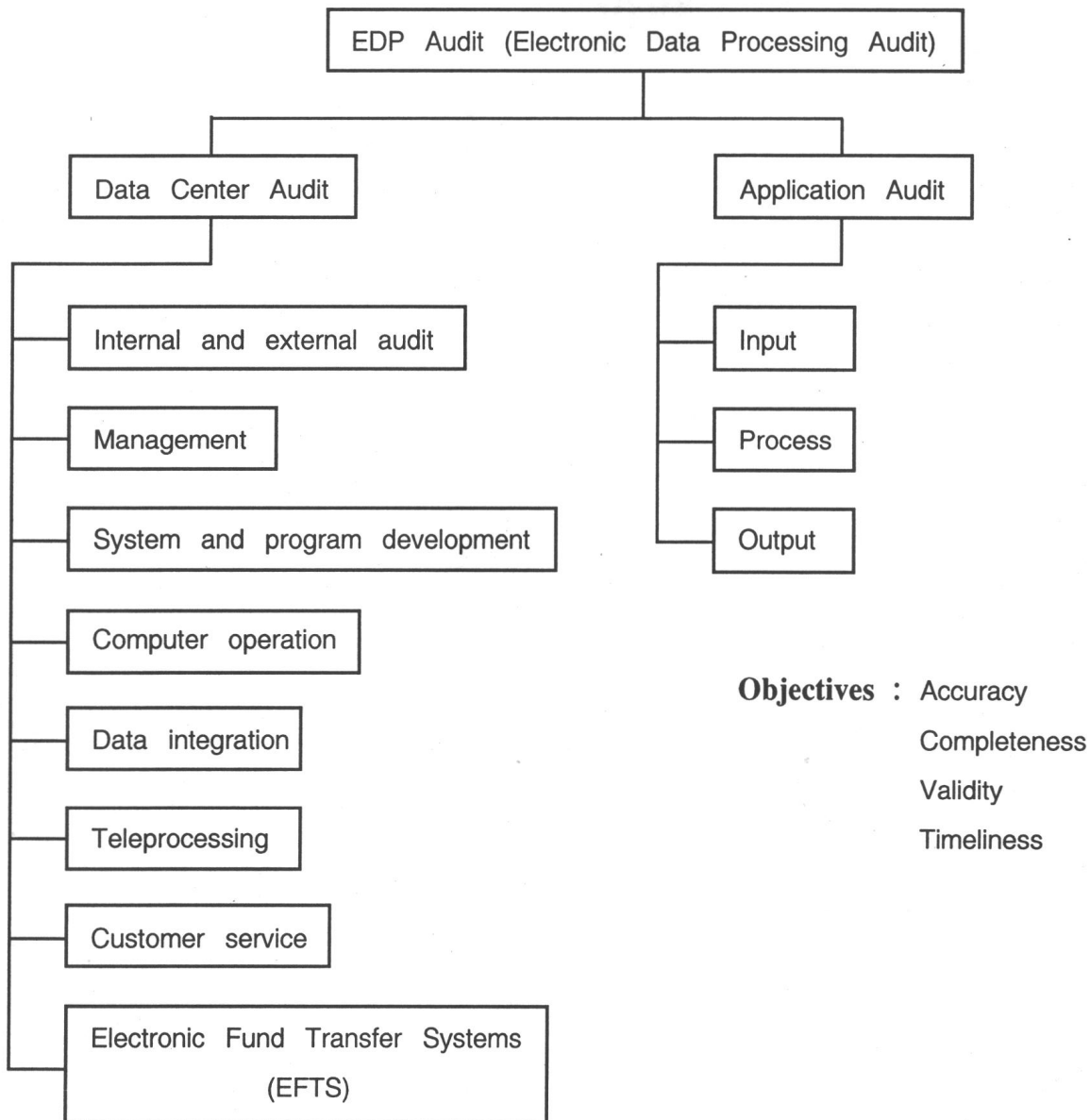
Thank you.

Appendix *
Electronic banking and its impact on CAMEL

objectives Areas	Adequacy	Accuracy	Quality	Integrity	Stability	Security
Capital	C ₁ C ₂ C ₈ C ₉ C ₁₀					
Assets			A ₁ A ₂ A ₃ A ₄ A ₅ A ₆ A ₇ A ₈ A ₉ A ₁₀			
Management				M ₁ M ₂ M ₃ M ₄ M ₅ M ₆ M ₇ M ₈ M ₉ M ₁₀		
Earnings					E ₁ E ₂ E ₃ E ₄ E ₅ E ₆ E ₇ E ₈ E ₉ E ₁₀	
Liquidity	L ₄ L ₅ L ₆ L ₇ L ₉					

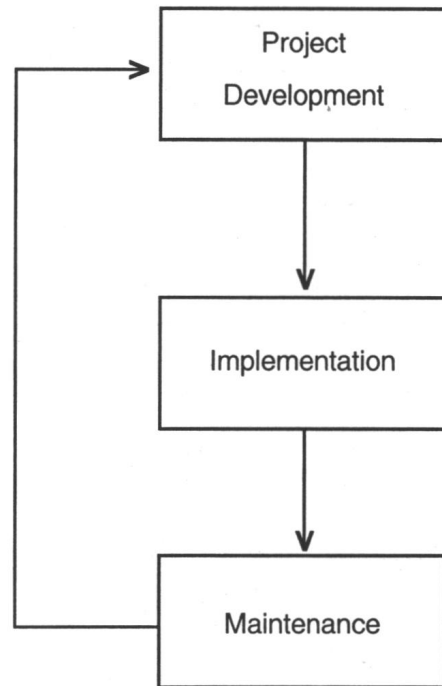
* ส่วนที่เป็น Appendix นี้ ไม่ได้นำเสนอรายละเอียดใน Keynote Address เมื่อวันที่ 23 กันยายน 2539 เพราะมีเวลาจำกัด ส่วนนี้เคยใช้บรรยายในหลักสูตร Inspection and Supervision of Financial Institution ของ South East Asia Central Banks (SEACEN) หลายครั้ง

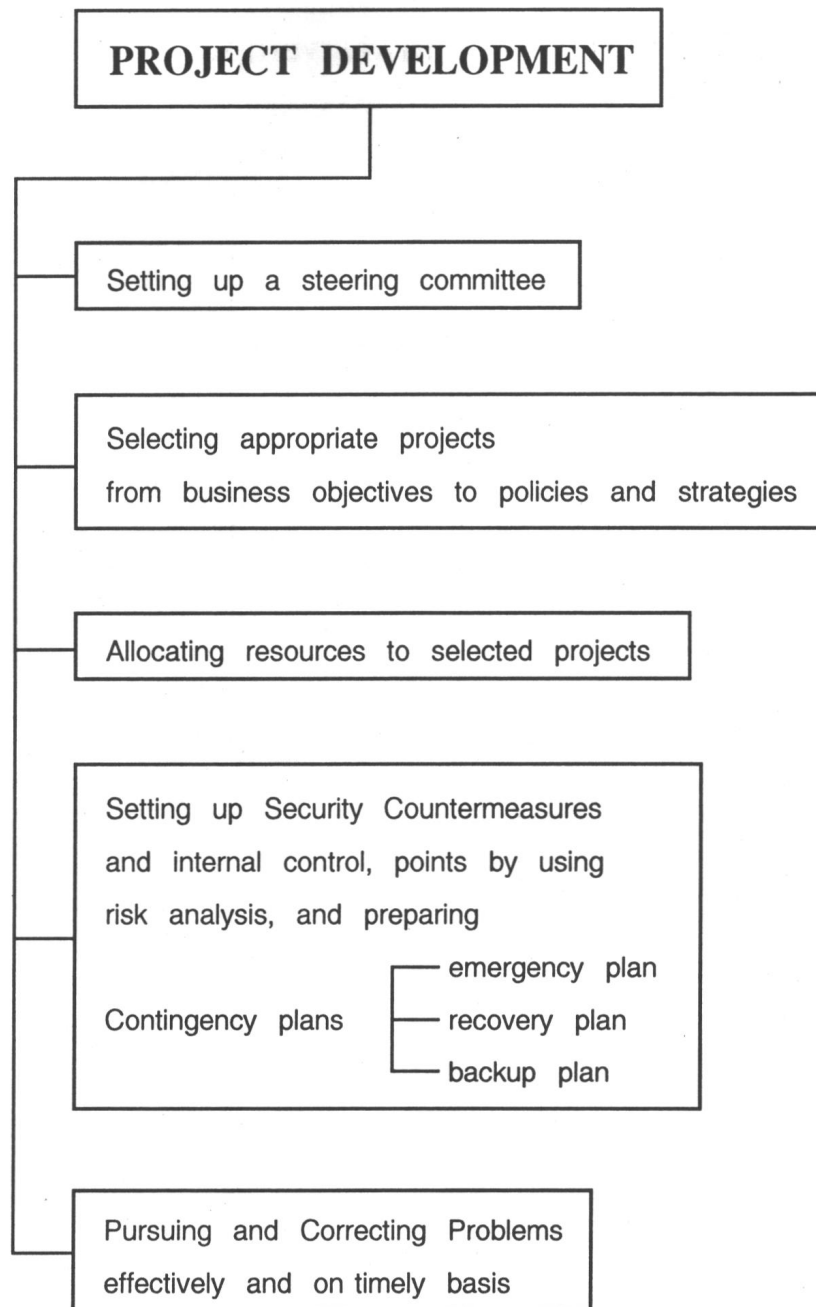
How to Examine Computerized Commercial Banks

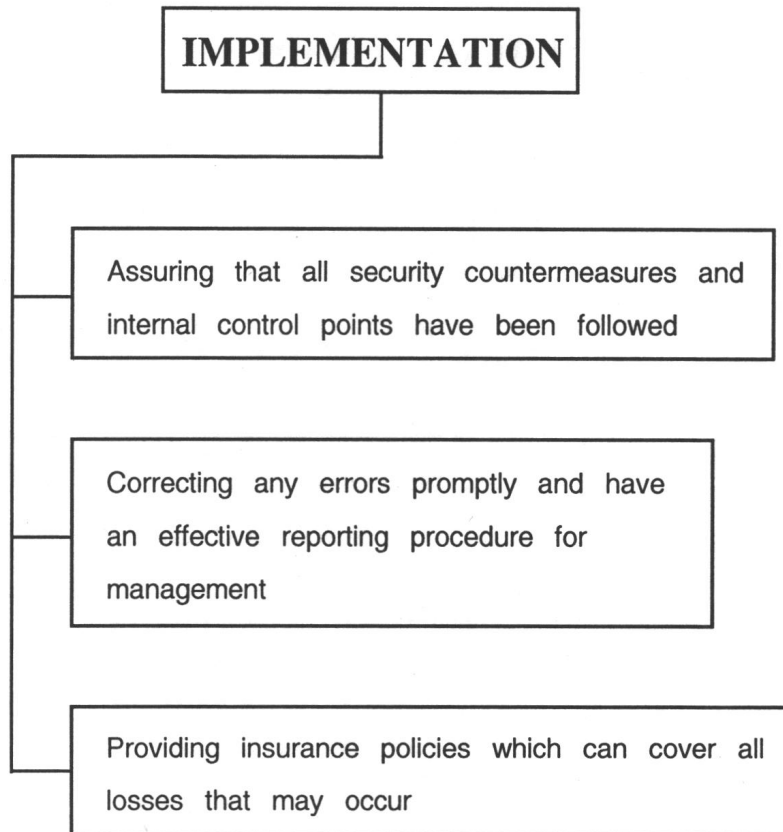


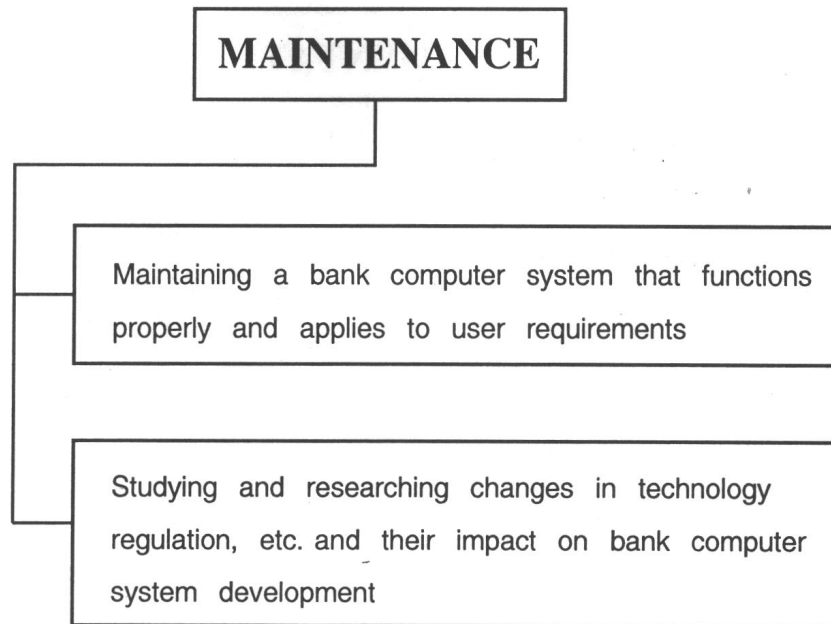
Objectives : Integrity of management,
System development,
System operation, and
System maintenance

Computer System Development Cycle









PROJECT DEVELOPMENT

1. Setting up the steering Committee

Impacted
Areas

- : lack of steering Committee
↓
- : some departments may not participate
↓
- : developed system may not serve every department well,
therefore, wastes of capital (in extreme case where we had to
spend a lot of money to develop the system)
↓
- : if the computer system is unable to serve the purposes well,
it means failure and a waste of computer assets and
human resources
↓
- : also, we have to realize losses of operating expenses
which decrease net profit

M₁

A₁

E₁

2. Selecting projects that are compatible with business objectives, policies and strategies

- : lack of consideration of business objectives, policies
and strategies means sloppy management
↓
- : cannot gain a marketing advantage, cost-
effectiveness or follow with in the overall
strategies
↓
- : project failure
↓
- C A E
(as in the 1st item)

M₂

C₂ A₂ E₂

3. Allocating resources to selected projects

Impacted

Areas

: without sufficient allocated resources (manpower, time, capital), the project may not be developed as targeted

M_3



: less qualified hardware or program errors because of insufficient funds and time



: the system may not serve the users well or can not be implemented or may have to be changed in a short period of time



C A E

$C_3 A_3 E_3$

4. Setting security countermeasures and internal control points after performing risk analysis and the preparation of contingency plans

: not performing things that are mentioned above, can cause error, fraud and disaster

M_4



: use may have to cut some losses and write off certain damaged assets

$E_4 A_4$



: loss of bank image which has mostly serious negative effect

$E_4 A_4 L$



: in the case of unable to continue business or service any transaction to customers such as money withdrawal, so it appear to be a lack of liquidity

L_4



: for wholesale banking, the interbank settlement transactions have a very high volume as if the computer system fails and can not process these transactions, this will cause additional damage

C_4

5. Following and Correcting problems effectively and on timely basis

Impacted Areas

: without an effective control system, the project may
be delayed and have an effect on the marketing plan,
that will increase expenditures



: more expenditures mean less net income



: the developed project may not be good enough
and some significant errors will cause additional effects
on C A L as in the 1st item

M₅

E₅

C₅ A₅ L₅

IMPLEMENTATION

6. Assuring that all security countermeasures and internal control points have been followed Impacted Areas

(Having the same impact on CAMEL as in the 4th item.

The difference is, in the 4th item, you don't even have it yet but in this item, you have it but do not perform it)

$M_6 E_6 A_6 L_6 C_6$

7. Correcting any errors promptly and having an effective reporting procedures to management

: without prompt error-correction and reports to management, can cause extended damages or losses

M_7



: E A

$E_7 A_7$



: In the extreme case, if the computer system fail and cannot provide any services, it looks like the commercial banks lost their liquidity

L_7

8. Providing insurance policies which can cover all losses that, can possibly occur

: without blanket-bond insurance policy
(insurance policy that covers all losses)

M_8



: which is the last step of risk management, banks may lose assets and increase expenditures which can cause serious effects on E A C

$E_8 A_8 C_8$

MAINTENANCE

9. Maintaining a bank computer system that functions properly and applies to user requirements

Impacted Areas

: without regular preventive maintenance, the computer system may be devalued in a short time or and suddenly bail without the user realizing it.

M_9

A_9



: The replacement cost may be higher than the maintenance cost

E_9



: it is sometimes needed to change all of the system costs a lot of money

C_9



: during a system failure, the business may come to a stand still which will have an effect on the lack of liquidity

L_9

10. Studying and researching changes in technologies, regulations, etc and their impact on bank computer system development

: without such studies and research, it can cause mismanagement and mislead strategic planning

M_{10}



: failure to gain the marketing advantage or cost effectiveness

E_{10}



: have to change hardware, software or the network to be compatible with other pool banks or because of obsolescence

$A_{10} C_{10}$

ภาคผนวก ข

การพิสูจน์โปรแกรมระบบงานที่สถาบันการเงินให้ใช้ทดสอบ เป็นโปรแกรมระบบงานชุดเดียวกับที่ใช้ปฏิบัติงานจริง

1. ควบคุมการ Copy โปรแกรมระบบงานและแฟ้มข้อมูลหลัก (Master File) ที่จะใช้ในการทดสอบ
2. รวบรวมและตรวจสอบรายงานการใช้เครื่องคอมพิวเตอร์ (Computer Log)
3. ผู้ตรวจสอบลงนามและปิดผนึกบนภาชนะที่ใส่ Media ที่เก็บโปรแกรมและข้อมูล เพื่อให้ธนาคารพาณิชย์เก็บรักษาไว้และนำมาให้ผู้ตรวจสอบทดสอบในภายหลัง
4. รวบรวมคำสั่ง JCL ที่ใช้ภายในศูนย์คอมพิวเตอร์ที่ตรวจสอบทั้งหมด
5. รวบรวมคู่มือการปฏิบัติงานของผู้ใช้ระบบงานศูนย์คอมพิวเตอร์ในกรณีที่ไม่สามารถทำการทดสอบที่ศูนย์คอมพิวเตอร์นั้นได้
6. ขอรายงาน Daily Transaction ของวันทำการถัดจากวันที่ของข้อมูลใน Master File ที่ให้ธนาคารพาณิชย์ Copy ไว้ เพื่อคัดเลือกรายการที่ต้องการนำไปรวมกับรายการทดสอบที่สร้างขึ้น
7. ให้ผู้ตรวจสอบเปิดผนึกภาชนะบรรจุ Media ที่เก็บโปรแกรมและข้อมูลที่จะใช้ในการทดสอบและควบคุมการ Load โปรแกรมและข้อมูลที่กล่าวเข้าระบบคอมพิวเตอร์เพื่อทดสอบต่อไป
8. ตรวจสอบการ Load* โปรแกรมที่จะทดสอบจากรายงานการใช้เครื่องคอมพิวเตอร์ในการประมวลผล
9. ตรวจสอบ Log ต่าง ๆ ที่เกิดขึ้นในช่วงการทดสอบและเปรียบเทียบกับ Log ที่เกิดจากการปฏิบัติงานจริง
10. เปรียบเทียบผลลัพธ์ในรายงานที่ได้จากการประมวลผลข้อมูลจริงที่เลือกมาทดสอบกับข้อมูลในรายงานที่ได้จากการปฏิบัติงานจริง

จากขั้นตอนการปฏิบัติงานที่กล่าวข้างต้น ผู้ตรวจสอบอาจมีปัญหาในการเรียกใช้และทำความเข้าใจข้อมูลใน Log ต่างๆ รวมทั้งขั้นตอนการควบคุมการปฏิบัติงานของพนักงาน Operator ในศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ด้วย ดังนั้น เพื่อให้ปัญหาดังกล่าวหมดไปควรจัดให้มีการอบรมผู้ตรวจสอบทั้งหมดให้เข้าใจในเรื่องดังกล่าว ซึ่งนอกจากจะช่วยให้ผู้ตรวจสอบสามารถพิสูจน์โปรแกรมระบบงานได้แล้ว ยังเป็นการพัฒนาผู้ตรวจสอบให้มีประสบการณ์ในด้านการปฏิบัติงานภายในศูนย์คอมพิวเตอร์และอาจใช้ประโยชน์ในการปฏิบัติงานกรณีธนาคารพาณิชย์มีปัญหาด้านการดำเนินงานด้วย

ทั้งนี้ โปรดดูปัญหาของแนวทางพิสูจน์โปรแกรมฯ ในหน้าถัดไป

แนวทางการพิสูจน์โปรแกรมระบบงานที่ใช้ทดสอบเป็นโปรแกรมระบบงานจริง

วิธีที่ 1

ใช้ข้อมูลจริงมาทดสอบโปรแกรมระบบงานและตรวจสอบผลการทำงานของโปรแกรกดังกล่าวกับผลที่ได้รับจากการใช้ปฏิบัติงานจริง โดยมีวิธีการดังนี้

1. ใช้ข้อมูลจริงของธนาคารพาณิชย์ในการทดสอบโปรแกรมระบบงาน
2. ให้ข้อมูลทดสอบ 5-10 Cycle

ปัญหาในการใช้วิธีที่ 1 มีดังนี้

- 1) ใช้เวลาและข้อมูลในการทดสอบมาก
- 2) ข้อมูลจริงที่ใช้ทดสอบและผลที่ได้รับจากการทดสอบไม่ตรงกับผลที่ได้รับจากการปฏิบัติงานจริง เนื่องจากมีการแก้ไขโปรแกรมระบบงาน
- 3) อาจมีการแก้ไขโปรแกรมในจุดอื่น ซึ่งยังมีผลให้ข้อมูลที่ได้จากการทดสอบตรงกับข้อมูลการปฏิบัติงานจริง

วิธีที่ 2

ตรวจสอบรายละเอียดจาก Log ต่างๆ เพื่อดูว่าโปรแกรมระบบงานที่ใช้ในการทดสอบ ใช้หน่วยความจำภายในเครื่องคอมพิวเตอร์ (Memory) เท่ากันหรือไม่ วันที่ Compile โปรแกรมเป็นวันเดียวกัน และเป็นโปรแกรม Version เดียวกันด้วย

ปัญหาในการใช้วิธีที่ 2 มีดังนี้

วิธีนี้เป็นการตรวจสอบข้อมูลที่เกี่ยวข้องกับโปรแกรมระบบงาน ซึ่งผู้ตรวจสอบอาจมีปัญหาในด้านการอ่าน Computer Log ของระบบคอมพิวเตอร์ที่เกี่ยวข้อง

วิธีที่ 3

ตรวจสอบโปรแกรมระบบงานที่ใช้ทดสอบกับโปรแกรมระบบงานจริง โดยใช้โปรแกรมตรวจสอบเพื่อเปรียบเทียบคำสั่งของโปรแกรมทั้งสองชุด คำสั่งต่อคำสั่ง ถ้าหากไม่ตรงกันก็จะให้เครื่องคอมพิวเตอร์พิมพ์คำสั่งที่ไม่ตรงกันออกมาตรวจสอบได้

ปัญหาในการใช้วิธีที่ 3 มีดังนี้

วิธีนี้เป็นเทคนิคการตรวจสอบโปรแกรมระบบงานเพื่อพิสูจน์ว่าได้มีการแก้ไขโปรแกรมระบบงานโดยไม่ได้รับอนุญาตหรือไม่ ซึ่งสามารถนำมาใช้พิสูจน์โปรแกรมทดสอบได้ แต่วิธีนี้ผู้ตรวจสอบจะต้องทราบวิธีการใช้โปรแกรมตรวจสอบที่กล่าว และจะต้องควบคุมการนำโปรแกรมระบบงานจริงมาให้ตรวจสอบด้วย

การพิสูจน์โปรแกรมระบบงานที่ธนาคารพาณิชย์ให้ใช้ทดสอบเป็นโปรแกรมระบบงานชุดเดียวกับที่ใช้ปฏิบัติงานจริง

ขั้นตอนการปฏิบัติงานของผู้ตรวจสอบ	กรณีทดสอบโปรแกรมในศูนย์ฯ ที่ตรวจสอบ	กรณีไปทดสอบโปรแกรมที่ศูนย์ฯ อื่นๆ	วัตถุประสงค์ในการกำหนดวิธีปฏิบัติงาน	ปัญหาที่ต้องพิจารณา
1. ควบคุมการ Copy โปรแกรมระบบงานและเพิ่มข้อมูล โดย 1.1 Copy โปรแกรม Online เก็บไว้ใน Media หลังการปิดระบบ Online และก่อนการ Load โปรแกรม Batch 1.2 Copy โปรแกรม Batch เก็บไว้ใน Media ก่อนการประมวลผลงาน Batch 1.3 Copy แฟ้มข้อมูล (Master File) ของวันทำการที่อยู่ในระหว่างการตรวจสอบในวันหนึ่ง	/ หรือใช้โปรแกรมชุดสำรอง	/	1. เพื่อให้แน่ใจว่าการ Copy โปรแกรมที่ใช้ในการปฏิบัติงานจริง	1. เนื่องจากผู้ตรวจสอบส่วนใหญ่ไม่ทราบขั้นตอนการ Copy โปรแกรมและแฟ้มข้อมูล
2. รวบรวมและตรวจสอบรายงานการใช้เครื่องคอมพิวเตอร์ (Log)	/	/	2. เพื่อเพิ่มความมั่นใจว่าการ Copy เป็นไปอย่างถูกต้อง และการทำงานด้านอื่น ๆ ด้วย	2. อาจมีปัญหาในการอ่านและเลือกใช้ Log ซึ่งมีหลายรูปแบบ และบางธนาคารไม่พิมพ์ออกมา
3. ผู้ตรวจสอบลงนามและปิดนียบนภาษาชนะที่ใส่ Media ที่เก็บโปรแกรมและข้อมูล เพื่อให้ธนาคารพาณิชย์เก็บรักษาไว้และนำมาให้ผู้ตรวจสอบทดสอบในภายหลัง	/	/	3. เพื่อป้องกันการเปลี่ยนแปลงโปรแกรมใน Media	3. อาจมีการเปลี่ยน Media ที่เก็บโปรแกรมโดยเจ้าหน้าที่ธนาคารพาณิชย์ได้
4. รวบรวมคำสั่ง JCL ที่ใช้ภายในศูนย์คอมพิวเตอร์ ที่ตรวจสอบทั้งหมด	/	/	4. เพื่อนำไปใช้งานและพิสูจน์การทำงานของโปรแกรมต่างๆ ที่ใช้ทดสอบเป็นชุดเดียวกับที่ใช้ปฏิบัติงานจริง	4. อาจมีปัญหาในการทำความเข้าใจ JCL และรวบรวมได้ไม่ครบถ้วน

ขั้นตอนการปฏิบัติงานของผู้ตรวจสอบ	กรณีทดสอบโปรแกรมในศูนย์ฯ ที่ตรวจสอบ	กรณีที่ไม่ทดสอบโปรแกรมที่ศูนย์ฯ อื่นๆ	วัตถุประสงค์ในการกำหนดวิธีปฏิบัติงาน	ปัญหาที่ต้องพิจารณา
5. รวบรวมคู่มือการปฏิบัติงานของผู้ใช้ระบบงานของศูนย์คอมพิวเตอร์ในกรณีที่ไม่สามารถทำการทดสอบที่ศูนย์คอมพิวเตอร์นั้นได้	/	/	5. เพื่อให้การป้อนข้อมูลเข้าระบบคอมพิวเตอร์ในการทดสอบได้ถูกต้องเช่นเดียวกับการปฏิบัติงานจริง	5. การรวบรวมคู่มือปฏิบัติงานของธนาคารพาณิชย์ได้ไม่ครบถ้วน
6. ขอรายงาน Daily Transaction ของวันทำการถัดจากวันที่ของข้อมูลใน Master File ที่ให้ธนาคารพาณิชย์ Copy ไว้ เพื่อคัดเลือกรายการที่ต้องการนำไปรวมกับรายการทดสอบที่สร้างขึ้น	/	/	6. เพื่อนำไปคัดเลือกข้อมูลไว้ทดสอบและตรวจสอบผลการทดสอบข้อมูลเปรียบเทียบกับรายการในรายงานจริง	6. -
7. ให้ผู้ตรวจสอบเปิดเป็นภิกษาบรรจุ Media ที่เก็บโปรแกรมและข้อมูลที่จะใช้ในการทดสอบและควบคุมการ Load โปรแกรมและข้อมูลเข้าระบบคอมพิวเตอร์เพื่อทดสอบต่อไป	/	/	7. เพื่อป้องกันการเปลี่ยน Media เก็บโปรแกรมระบบงาน	7. การควบคุมการปฏิบัติงานของพนักงานธนาคารพาณิชย์ไม่สามารถควบคุมได้ตลอดเวลา
8. ตรวจสอบการ Load โปรแกรมที่จะทดสอบจากรายงานการใช้เครื่องคอมพิวเตอร์ในการประมวลผล	/	/	8. เพื่อให้แน่ใจว่าได้มีการ Load โปรแกรมได้ถูกต้องครบถ้วน	8. อาจมีปัญหาในการดูรายงาน
9. ตรวจสอบ Log ต่าง ๆ ที่เกิดขึ้นในช่วงการทดสอบและเปรียบเทียบกับ Log ที่เกิดจากการปฏิบัติงานจริง	/	/	9. เพื่อตรวจสอบการใช้โปรแกรมและเพิ่มข้อมูลต่างๆ เหมือนกับที่ใช้ปฏิบัติงานจริง	9. อาจมีปัญหาที่ธนาคารพาณิชย์จะไม่พิมพ์ Log ออกมาให้ทั้งหมด
10. เปรียบเทียบผลลัพธ์ในรายงานที่ได้จากการประมวลผลข้อมูลจริงที่เลือกมาทดสอบกับข้อมูลในรายงานที่ได้จากการปฏิบัติงานจริง	/	/	10. เป็นการพิสูจน์ได้ว่าโปรแกรมจริงได้ส่วนหนึ่ง	10. -

ภาคผนวก ข

วัตถุประสงค์ในการขอ Source Program Listing

1. วัตถุประสงค์หลัก

- เพื่อให้แน่ใจว่า ธนาคารพาณิชย์มี Source Program Listing อยู่จริง เพราะหากไม่มี Source Program Listing ถ้าระบบงานเกิดการเสียหาย ธนาคารพาณิชย์จะไม่สามารถทำงานต่อไปได้
- เพื่อให้แน่ใจว่า source program Listing ที่ธนาคารมีอยู่นั้นเป็นชุดสุดท้ายที่ได้ทำการแก้ไขและได้ใช้ในการปฏิบัติงานในปัจจุบันจริง

2. เหตุผลในด้าน logic และความสมเหตุสมผลในขั้นตอนการประมวลผล

- เพื่อพิจารณาในโปรแกรมที่ธนาคารใช้ประมวลผลในปัจจุบันนั้น มีส่วนใดส่วนหนึ่งของโปรแกรม (หรือ sub-routine) ซึ่งไม่เกี่ยวข้องกับ application นั้นแอบแฝงอยู่หรือไม่
- เพื่อแยกโปรแกรมที่ใช้งานจริงออกจากโปรแกรมที่ไม่ได้ใช้งาน
- เป็นการสอบถาม logic และขั้นตอนการทำงานใน Source Program Listing ว่าสอดคล้องกับรายละเอียดใน documentation หรือไม่
- เพื่อให้แน่ใจว่า field ที่สำคัญ ๆ ได้ถูกนำมาประมวลผลตามประเภทและลักษณะของงานอย่างถูกต้องและครบถ้วน
- เพื่อเป็นการยืนยันว่า รายการ error ที่ปรากฏในรายงานต่าง ๆ นั้นเป็นผลมาจากโปรแกรมได้ทดสอบและ edit ข้อมูลนั้นจริง

3. การขาด documentation

- การขาด documentation ทำให้มีความจำเป็นอย่างยิ่งในการตรวจสอบ Source Program Listing เพราะหากธนาคารมี documentation ที่สมบูรณ์ การขอ Source Program Listing จะทำเมื่อจำเป็นเท่านั้น

4. อื่น ๆ

- การที่ระบุการขอ Source Program Listing ในรายการขอนั้น ผู้ตรวจสอบควรขอเมื่อมีความจำเป็นจริง ๆ เท่านั้น และมีรายละเอียดมากมายในการทำความเข้าใจ

บรรณานุกรม*

1. Contingency Planning Guidelines for Financial Institutions
2. Applied Security Management โดย Clay E. Higgins
3. Computer Fraud J Security Bulletin Vol.6 No 10/1984
4. Report on Netting Schemes-BIS 1989
5. รายงานการฝึกอบรมและดูงานเกี่ยวกับการตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์
ของเมธา สุวรรณสาร

* ผิด ตก ยกเว้น

ประวัติโดยย่อ

นายเมธา สุวรรณสาร

1. ประวัติการศึกษา

- 1.1 ปริญญาตรี พานิชศาสตร์บัณฑิต จากมหาวิทยาลัยธรรมศาสตร์
บัญชีบัณฑิต จากมหาวิทยาลัยธรรมศาสตร์

2. การอบรมและงานที่สำคัญ

- 2.1 ประกาศนียบัตรด้าน Management จาก University of California at Berkeley ประเทศสหรัฐอเมริกา
2.2 ประกาศนียบัตร การตรวจสอบคอมพิวเตอร์ จาก Federal Deposit Insurance Corporation (FDIC) ประเทศสหรัฐอเมริกา
2.3 ฐานการตรวจสอบด้านคอมพิวเตอร์ และด้าน Electronic Banking หลายธนาคารที่ประเทศสหรัฐอเมริกา อังกฤษ และประเทศญี่ปุ่น
2.4 อบรมหลักสูตร UNIX and Internet for Executive จากมหาวิทยาลัยเทคโนโลยีสุรนารี

3. การเป็นกรรมการและกิจการต่าง ๆ

- อดีต

- 3.1 เป็นหัวหน้าคณะผู้แทนของไทย (Thailand Representative) ในการประชุมที่สำนักงานใหญ่องค์การสหประชาชาติ (UN) ที่ New York ประเทศสหรัฐอเมริกา ในปี 2532 เรื่อง Draft Model Rules on Electronic Funds Transfer
3.2 ประธานกรรมการบริษัทเครดิตฟองซิเอร์สาขาสยาม
3.3 ประธานคณะกรรมการพิจารณากำหนดรายการและความหมายของรายการในงบดุล และบัญชีกำไรขาดทุนของบริษัทมหาชนที่ประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์ ธุรกิจเงินทุนหลักทรัพย์ และธุรกิจเครดิตฟองซิเอร์
3.4 ประธานคณะกรรมการด้านเศรษฐกิจและการเงินจังหวัดขอนแก่นในการเชื่อมความสัมพันธ์กับเมืองหนานหนิง ปี 2537
3.5 หัวหน้าคณะทำงานศึกษาปัญหาการค้าชายแดนไทย-ลาว ปี 2537
3.6 รองประธานคณะกรรมการพิจารณาผลตอบแทนและความเสี่ยงของบริษัทเงินทุนและสถาบันการเงิน

หมายเหตุ : จัดทำขึ้นตามคำแนะนำของท่านผู้อ่านบางท่านที่ได้แนะนำมา เพื่อจะได้แลกเปลี่ยนข้อสังเกตและข้อเสนอแนะระหว่างผู้อ่านหนังสือเล่มนี้กับผู้จัดทำ

- 3.7 ผู้ร่วมก่อตั้ง สมาคมผู้ตรวจสอบงานคอมพิวเตอร์ ภาคพื้นกรุงเทพฯ The EDP Auditors Association (EDPAA) Bangkok Chapter ซึ่งปัจจุบันได้เปลี่ยนชื่อเป็น Information Systems Audit and Control Association, (ISACA), Bangkok Chapter
- 3.8 รองประธานสหกรณ์ออมทรัพย์พนักงานธนาคารแห่งประเทศไทย
- 3.9 ที่ปรึกษาด้านการเงินและการบัญชีสหกรณ์ออมทรัพย์พนักงานธนาคารแห่งประเทศไทย
- 3.10 ที่ปรึกษากิตติมศักดิ์โครงการศึกษาและจัดทำแผนลงทุนจังหวัดขอนแก่น กาฬสินธุ์ มหาสารคาม และหนองบัวลำภู

- ปัจจุบัน

- 3.11 อนุกรรมการสอบบัญชีกิจการที่ใช้คอมพิวเตอร์
- 3.12 ที่ปรึกษาของสมาคมผู้ตรวจสอบงานคอมพิวเตอร์ภาคพื้นกรุงเทพฯ (ISACA), Bangkok Chapter
- 3.13 กรรมการพัฒนาจังหวัดขอนแก่น (กพจ.)
- 3.14 กรรมการพัฒนาเทศบาลนครขอนแก่น
- 3.15 ที่ปรึกษาคณะกรรมการศึกษารูปแบบการบริการวิชาการของมหาวิทยาลัยขอนแก่น
- 3.16 คณะทำงานศึกษาศักยภาพและแนวทางการพัฒนาเพื่อกระจายความเจริญสู่ภูมิภาคจังหวัดขอนแก่น
- 3.17 กรรมการผู้ทรงคุณวุฒิประจำศูนย์บริการวิชาการ มหาวิทยาลัยขอนแก่น
- 3.18 ที่ปรึกษาโครงการพัฒนาเศรษฐกิจประเทศลุ่มแม่น้ำโขง
- 3.19 สมาชิกโปโลคลับ กรุงเทพฯ
- 3.20 ผู้สอบบัญชีรับอนุญาต

4. การเข้ามีส่วนร่วมในกิจกรรมของมหาวิทยาลัย กิจกรรมอุดมศึกษา และการบรรยายที่สำคัญ

- 4.1 เป็นผู้บรรยายให้กับนักศึกษาระดับปริญญาโทในมหาวิทยาลัยธรรมศาสตร์ ด้านการตรวจสอบคอมพิวเตอร์และปริญญาตรีในมหาวิทยาลัยหลายแห่ง
- 4.2 เป็นผู้บรรยายการตรวจสอบสถาบันการเงินที่ใช้คอมพิวเตอร์ของ SEACEN (กลุ่มธนาคารกลางต่าง ๆ ในประเทศแถบเอเชีย รวมเกาหลีใต้ และไต้หวัน)
- 4.3 เป็นผู้บรรยายให้กับองค์กรต่าง ๆ รวมทั้งสถาบันเทคโนโลยีแห่งเอเชีย (Asian Institute of Technology – AIT) ส่วนใหญ่เน้นหนักไปในเรื่อง Computer Audit
- 4.4 เป็นวิทยากรบรรยายหลักสูตรปริญญาโทให้คณะวิทยาการจัดการและหลักสูตรอื่น ๆ แก่มหาวิทยาลัยขอนแก่น
- 4.5 เป็น Course Director หลักสูตร Computer Audit (Advanced Level) ของ SEACEN ที่กรุงเทพฯ
- 4.6 เป็น Deputy Principal หลักสูตร Inspection and Supervision of Financial Institution ของ SEACEN ที่ประเทศ Indonesia
- 4.7 อาจารย์ที่ปรึกษาวิทยานิพนธ์ทางด้านคอมพิวเตอร์
- 4.8 เป็นผู้บรรยายด้านเศรษฐกิจ การเงิน การธนาคาร การตรวจสอบสถาบันการเงินให้กับส่วนงานต่าง ๆ
- 4.9 เป็นวิทยากรบรรยาย เรื่องเศรษฐกิจการเงินของภาคตะวันออกเฉียงเหนือแก่นักศึกษา วปอ. ปรอ. และคณะอื่น ๆ

5. งานอื่น ๆ

- 5.1 จัดทำและเรียบเรียงหนังสือ “การจัดระบบควบคุมภายในของสถาบันการเงิน”
- 5.2 จัดทำและเรียบเรียงหนังสือ “การดำเนินงาน และการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์
- 5.3 เป็นผู้ริเริ่มโครงการตรวจสอบด้านคอมพิวเตอร์ (Computer Audit หรือ IS Audit) ให้กับธนาคารพาณิชย์และสถาบันการเงินต่าง ๆ และการจัดให้มี Second Site Back Up ของธนาคารพาณิชย์

6. ประวัติการทำงานที่ธนาคารแห่งประเทศไทย

- อดีต

- 6.1 หัวหน้าผู้ตรวจสอบ ฝ่ายกำกับสถาบันการเงิน
- 6.2 หัวหน้าส่วนตรวจสอบธนาคารพาณิชย์ด้านคอมพิวเตอร์
- 6.3 รองผู้อำนวยการฝ่ายกำกับและตรวจสอบธนาคารพาณิชย์
- 6.4 รองผู้อำนวยการฝ่ายกำกับและตรวจสอบสถาบันการเงิน

- ปัจจุบัน

- 6.5 ผู้อำนวยการแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ

บันทึก

บันทึก

บันทึก

พิมพ์ที่

หอจก. โรงพิมพ์คดล้งนนวนวทยา

33/17-18 ถนนหน้าเมือง ค.โนมเมือง อ.เมือง จ.ขอนแก่น 40000 โทร. (043) 236344, 332152-3 Fax. 333785

