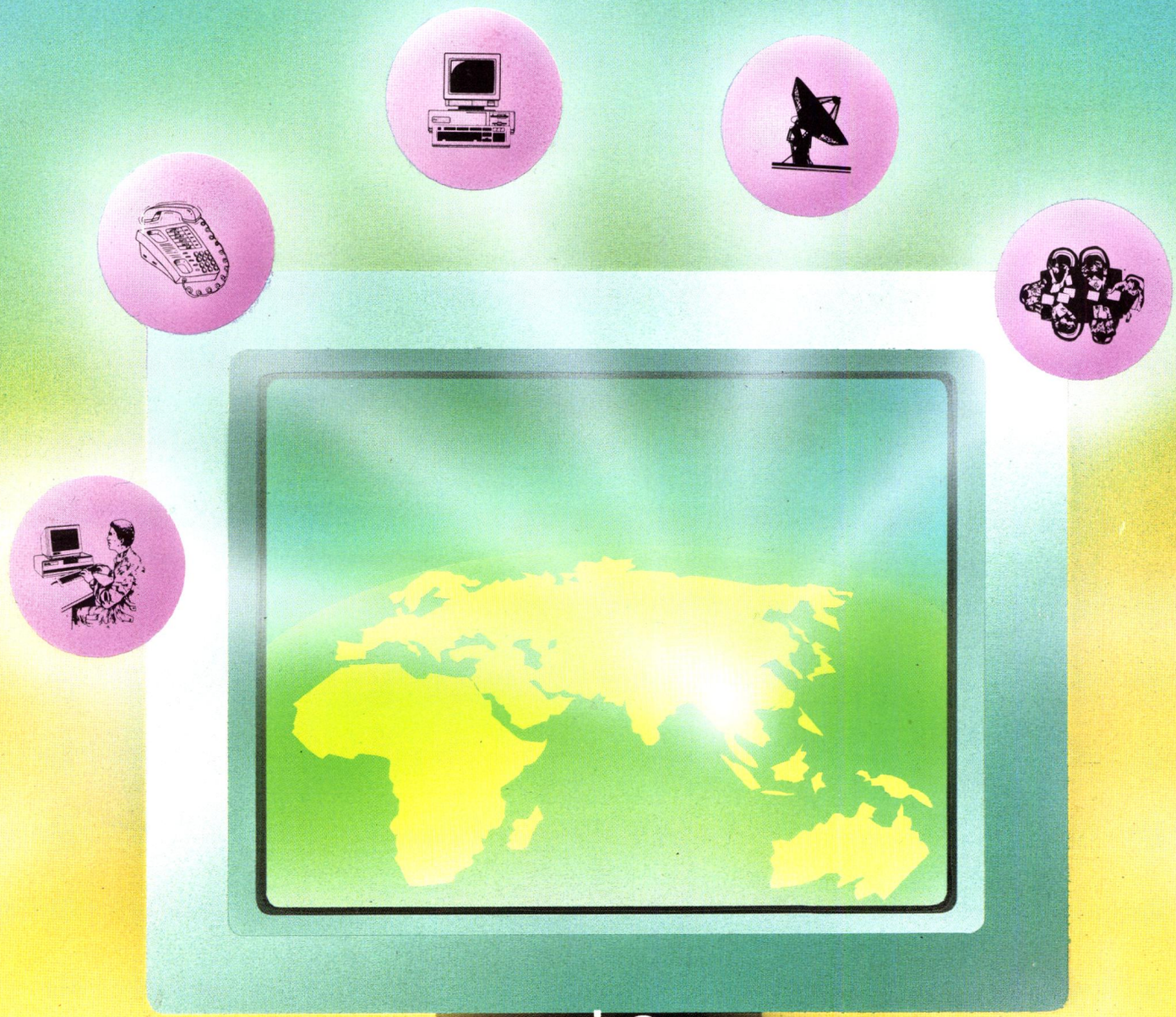
การดำเนินงาน และ การตรวจสอบสถาบันการเงิน ด้านคอมพิวเตอร์

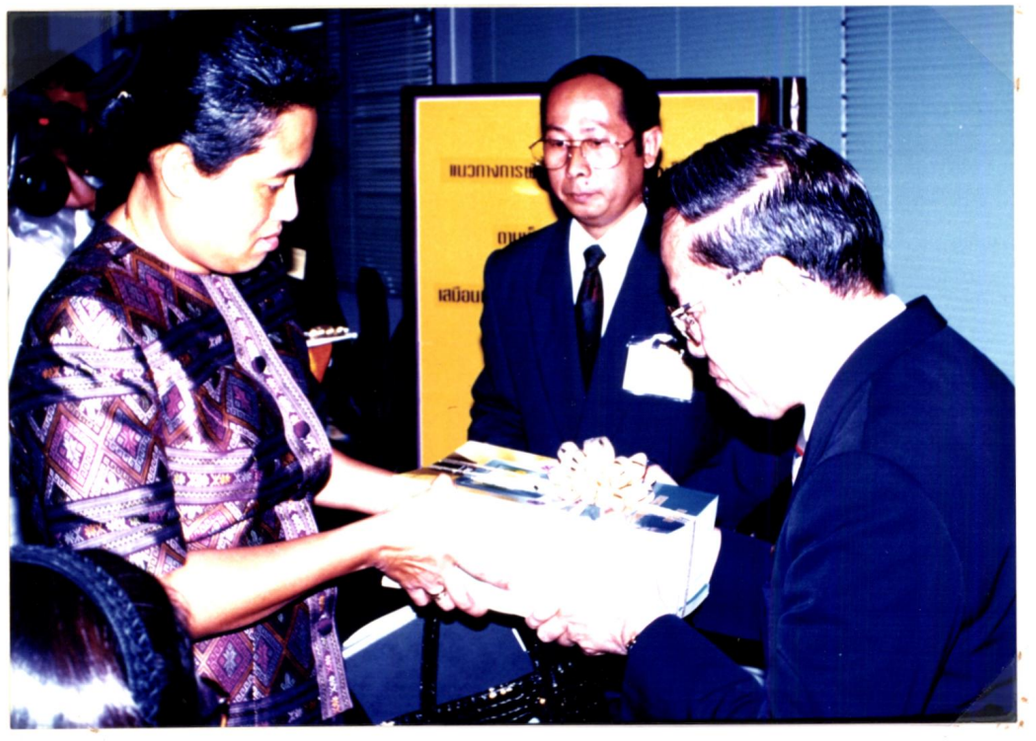


เล่มที่ 2

ภาคการตรวจสอบ

เมธา สุวรรณสาร

การดำเนินงาน
และ
การตรวจสอบสถาบันการเงิน
ด้านคอมพิวเตอร์
เล่ม 2



เมธา สุวรรณสาร

ISBN 974-89878-4-1

คำนำ

1. การจัดทำหนังสือชุดเรื่อง การดำเนินงานและการตรวจสอบสถาบันการเงินด้วยคอมพิวเตอร์ทั้ง 4 เล่ม ครั้งนี้ผมใคร่ขอเรียนวัตถุประสงค์หลักซึ่งเป็นสาระสำคัญของการจัดทำหนังสือชุดนี้คือ

1.1 เพื่อให้การศึกษา ค้นคว้า วิจัย งานด้านคอมพิวเตอร์ โดยไม่มีวัตถุประสงค์ในทางการค้า ทั้งในปัจจุบันและในอนาคตแก่ผู้ตรวจสอบในส่วนกำกับสถาบันการเงิน ที่ทำหน้าที่ตรวจสอบ ดูแล ความมั่นคงของสถาบันการเงินต่างๆ ในภาคตะวันออกเฉียงเหนือ และจะใช้ภายในวงการที่ธนาคารแห่งประเทศไทยมีส่วนเกี่ยวข้องเป็นสำคัญ โดยพิจารณาเป็นส่วนหนึ่งของการให้การศึกษา อบรม ทำความเข้าใจกับหน่วยงานที่ธนาคารแห่งประเทศไทยเป็นผู้กำกับและดูแล

1.2 หนังสือทั้ง 4 เล่มในชุดนี้ เป็นการแนะนำงานที่ได้ศึกษารวบรวมเรียบเรียง รวมทั้งดัดแปลงจากเอกสารต่างประเทศ และเขียนเพิ่มเติมจากประสบการณ์ภาคสนามรวมๆ กันไป จากเอกสารเดิมที่เคยใช้ในการบรรยายให้ความรู้ต่อสถาบันการเงินและมหาวิทยาลัยต่างๆ ที่ผ่านมา ทั้งนี้ได้อ้างถึงที่มาของหนังสือที่ได้ค้นคว้าตามท้ายหนังสือแล้วเพื่อให้ผู้ที่ใช้งานในวงจำกัดเหล่านี้ได้ทราบถึงที่มาในการใช้หนังสือชุดนี้เพื่อการศึกษาโดยมีข้อผิดตกยกเว้น ดังกล่าว

1.3 เพื่อให้การทำงานของส่วนกำกับฯ ได้ผลยิ่งขึ้น จึงได้มีการพูดคุยและให้คำแนะนำการปฏิบัติงาน รวมทั้งการตรวจสอบในที่ประชุมธนาคารพาณิชย์และสถาบันการเงินต่างๆ ในภาคอีสานเช่นเดียวกับที่ผมได้เป็นผู้บรรยายให้แก่สถาบันเหล่านี้ในกรุงเทพฯ และที่อื่นๆ หนังสือชุดดังกล่าว จึงได้ส่งให้สถาบันการเงินที่ธนาคารแห่งประเทศไทย ภาคตะวันออกเฉียงเหนือดูแล โดยมีวัตถุประสงค์เช่นเดียวกันคือให้การศึกษา ค้นคว้า วิจัย โดยถือเสมือนหนึ่งเป็นการป้องกันปัญหา และให้คำชี้นำในการให้การศึกษาเป็นการล่วงหน้าต่อสถาบันการเงินดังกล่าว ตามหน้าที่เพื่อให้เกิดประสิทธิภาพในการปฏิบัติงาน โดยมีเอกสารไว้ใช้ศึกษาดูเมื่อต้องการ ซึ่งจะมีผลต่อความมั่นคงของสถาบันการเงิน ซึ่งเป็นหน้าที่หลักอย่างหนึ่งของธนาคารแแห่งประเทศไทยเป็นสำคัญ

1.4 หนังสือในชุดนี้ทั้งหมด จัดทำขึ้นเพื่อใช้ประโยชน์ในการปฏิบัติงานและการดำเนินการของธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ โดยมิได้เผยแพร่หรือโฆษณาต่อสาธารณชนเป็นการทั่วไป และมิได้มีการจำหน่ายใดๆ ทั้งสิ้น และใคร่ขอย้ำว่าเป็นการจัดทำเพื่อประโยชน์ในการศึกษา งานค้นคว้า การปฏิบัติงานและการตรวจสอบด้านคอมพิวเตอร์ทุกรูปแบบตามภาระและหน้าที่ส่วนหนึ่งในความรับผิดชอบที่ผมปฏิบัติหน้าที่อยู่ทั้งในอดีตและปัจจุบัน

ดังนั้น การนำข้อความหรือบทความในหนังสือชุดนี้ เพื่อจะทำซ้ำหรือดัดแปลงเพื่อประโยชน์ทางการค้า จึงเป็นสิ่งที่ไม่พึงปฏิบัติเพราะผิดวัตถุประสงค์ที่สำคัญของการจัดทำหนังสือชุดนี้เป็นอย่างยิ่ง

1.5 การทำความเข้าใจกับท่านผู้อ่าน และผู้ที่อาจเกี่ยวข้องในหัวข้อนี้ ก็เพื่อสร้างความเข้าใจในการจัดทำหนังสือชุดนี้เป็นสำคัญ ทั้งนี้เป็นการป้องกันปัญหาที่อาจจะเกิดจากความเข้าใจที่ไม่ตรงกันในการปฏิบัติหน้าที่ของแต่ละหน่วยงานได้

2. หนังสือเรื่อง "การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์" เล่ม 2 นี้ เป็นเล่มที่จะเน้นทำความเข้าใจและให้รายละเอียดกับผู้ที่สนใจในการตรวจสอบด้านคอมพิวเตอร์เป็นหลัก ทั้งนี้ มีแนวทางทำความเข้าใจง่าย ๆ โดยเริ่มต้นศึกษาจากวงจรทางเทคโนโลยีกับการควบคุมและตรวจสอบ และการดำเนินงานด้านคอมพิวเตอร์ ซึ่งมีรายละเอียดปรากฏอยู่ในเล่ม 1 และได้สรุปเพิ่มเติมในเล่ม 2 โดยเฉพาะอย่างยิ่งการวางแผนการตรวจสอบ แผนภาพ และข้อควรทราบสำหรับผู้ตรวจสอบโดยทั่วไปก่อนการเข้าตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

3. การตรวจสอบภาคสนาม (field work) สำหรับผู้ตรวจสอบที่ยังไม่เข้าใจระบบงานที่แท้จริงนั้นจะเริ่มจากการศึกษาและทำความเข้าใจระบบงานขององค์กรโดยภาพรวมก่อน นั่นคือการทำความเข้าใจทั้งในระบบงานในส่วนที่ใช้คอมพิวเตอร์และในส่วนที่ไม่ใช้คอมพิวเตอร์ แล้วจึงทำการประเมินระบบการควบคุมภายใน การตรวจสอบระบบการควบคุม การประเมินผลกระทบของข้อบกพร่องในการควบคุม ตลอดจนหาทางใช้ Audit Tools และเทคนิคการตรวจสอบต่าง ๆ

4. ตั้งแต่บทที่ 16 ถึงบทที่ 26 เหมาะสำหรับการตรวจสอบภายใน (Internal Audit) และผู้ตรวจสอบภายนอกที่ไม่ได้เป็น examiner เพราะได้เน้นการตรวจสอบ "งาน" หรือ Application มากกว่า "องค์กร" อย่างไรก็ดีผู้ตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ (EDP examiner) จากธนาคารแห่งประเทศไทยก็สามารถนำไปประยุกต์ใช้ร่วมกับวิธีการและแนวทางการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ได้

5. มีองค์กรที่เกี่ยวข้องกับการตรวจสอบ และมีหนังสือที่เกี่ยวข้องกับการตรวจสอบด้านคอมพิวเตอร์มากมาย ตลอดจนนิตยสารและวารสารการตรวจสอบด้านคอมพิวเตอร์ ที่ออกกันมาเป็นรายเดือนหรือรายไตรมาสติดต่อกันมาเป็นเวลาหลายปีในหลายประเทศทั่วโลก เมื่อกล่าวถึงองค์กรอย่างเช่น Information Systems Audit and Control Association ที่มีสมาชิกมากกว่า 93 ประเทศทั่วโลก ทำหน้าที่ศึกษา ค้นคว้า ให้การอบรม จัดสัมมนา จัดการประชุมงานตรวจสอบด้านคอมพิวเตอร์ (IT หรือ IS Audit) กับสมาชิกและออกวารสาร IS Audit and Control เป็นประจำ มีสำนักงานใหญ่อยู่ที่ประเทศสหรัฐอเมริกา ประเทศไทยเราก็เป็นสมาชิกอยู่ในสมาคมผู้ตรวจสอบงานคอมพิวเตอร์นี้ด้วย นอกจากนั้นก็มีสถาบันต่าง ๆ หลายแห่งที่มีสมาชิกจำนวนมาก ทำหน้าที่คล้าย ๆ กันนี้ แต่เน้นหนักทางด้านการค้นคว้าการตรวจสอบด้านคอมพิวเตอร์และผลิตหนังสือต่าง ๆ ออกมามากมาย

ดังนั้น หากองค์กรของท่านเป็นองค์กรหนึ่งที่มีหน้าที่ในการตรวจสอบ ไม่ว่าจะเป็นการตรวจสอบภายในองค์กรของท่านเอง หรือทำหน้าที่ตรวจสอบองค์กรอื่นที่ใช้คอมพิวเตอร์ในการ Process งานและการบริหารงาน โดยที่ผู้ตรวจสอบที่ท่านดูแลยังมิได้ทำการตรวจสอบในลักษณะ IS Audit หรือ Computer Audit เป็นส่วนหนึ่งของกระบวนการตรวจสอบตามปกติแล้วละก็ ควรจะพิจารณาได้ว่า น่าจะต้องเพิ่มการดำเนินการตรวจสอบในลักษณะ IS Audit ได้แล้ว ทั้งนี้ขอท่านได้โปรดทบทวนและศึกษาจากมาตรฐานการสอบบัญชี ฉบับที่ 28 ฉบับที่ 29 และฉบับที่ 36 ของสมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย เรื่องการสอบบัญชีในกรณีธุรกิจที่ใช้คอมพิวเตอร์ (เล่ม 1) ก็จะเป็นประโยชน์ในการพิจารณาของท่านเป็นอย่างยิ่ง

6. จากข้อ 5 ข้างต้น ผมเองได้ยินเสียงวิจารณ์หรือเสียงบ่นจากการปฏิบัติงานการตรวจสอบของผู้ปฏิบัติงานภาคสนาม หรือผู้ลงมือตรวจสอบในองค์กรที่ใช้คอมพิวเตอร์จริง ๆ จากผู้คุ้นเคยมากรายว่า การตรวจสอบระบบการควบคุมภายในและการบัญชี ตลอดจนการศึกษาทำความเข้าใจระบบงานในองค์กรที่ได้รับการตรวจสอบที่ใช้คอมพิวเตอร์ เพื่อวางแผนและกำหนดเทคนิคหรือวิธีการตรวจสอบ หรือเพื่อหาหลักฐานและความพอเพียงในการตรวจสอบตามเป้าหมายการตรวจสอบ โดยใช้วิธีการตรวจสอบตามปกติหรือ Manual นั้น ได้ถูกจำกัดโดยกระบวนการ process งานด้านคอมพิวเตอร์ เพราะขั้นตอนการควบคุมภายในและการบัญชีส่วนใหญ่ได้ใช้โปรแกรมคอมพิวเตอร์เป็นผู้ควบคุมและดำเนินงานแล้ว ดังนั้นเมื่อไม่มีการตรวจสอบด้านคอมพิวเตอร์หรือ IT Audit เป็นส่วนหนึ่งของ Financial Audit โดยเฉพาะอย่างยิ่งการตรวจสอบการปฏิบัติตามระเบียบกฎเกณฑ์การควบคุมภายในของหน่วยงาน (Compliance Audit) แล้ว ก็จะทำให้การปฏิบัติงานตรวจสอบนั้นต้องข้ามขั้นตอนหรือละเว้นการตรวจสอบที่จำเป็นไปไม่น้อย ทำให้มีปัญหาถึงประสิทธิภาพและประสิทธิผลการปฏิบัติงานการตรวจสอบอันเกิดจากการละเลย ไม่ตรวจสอบงานด้านคอมพิวเตอร์ รวมทั้งไม่ใช้คอมพิวเตอร์เข้าช่วยในการตรวจสอบตามมาตรฐานที่ควรจะเป็นด้วย

ท่านเคยได้ยินคำวิจารณ์หรือเสียงบ่นทำนองนี้บ้างหรือไม่ และท่านควรจะทำการแก้ไขปัญหาหรืออุปสรรคตามที่กล่าวนี้อย่างไร หากท่านไม่ได้ยินเรื่องทำนองข้างต้น ท่านเคยคิดและพิจารณาบ้างหรือไม่ว่าเป็นไปได้หรือที่การตรวจสอบยังคงใช้แนวทางการตรวจสอบเดิมๆ สมัยที่องค์กรยังใช้ระบบ Manual เมื่อองค์กรนั้นนำคอมพิวเตอร์เข้ามาใช้แล้ว

7. ในการตรวจสอบธนาคารพาณิชย์และสถาบันการเงินด้านคอมพิวเตอร์รวมทั้งองค์กรอื่นที่ใช้คอมพิวเตอร์ ผู้ตรวจสอบควรพิจารณาถึงความจำเป็นและความแตกต่างในระบบงานของแต่ละองค์กรเป็นกรณีไป โดยควรเน้นและให้ความสำคัญอย่างยิ่งต่อการควบคุมภายในที่มีประสิทธิภาพ

8. การทำความเข้าใจในเป้าหมาย ขอบเขต กรรมวิธี ในการตรวจสอบงานด้านคอมพิวเตอร์ (IS Audit) และการตรวจสอบทางด้านการเงิน (Financial Audit) และจัดทำรายงานการตรวจสอบตลอดจนความสัมพันธ์ของงานทั้ง 2 ประเภท นับเป็นสิ่งที่มีความสำคัญยิ่งในการปฏิบัติงานการตรวจสอบที่มีประสิทธิภาพสูงสุด เช่น การรู้จักใช้เครื่องมือคอมพิวเตอร์ให้เป็นประโยชน์ในการตรวจสอบ และการทำความเข้าใจในระบบงานด้านคอมพิวเตอร์ เพื่อกำหนดขอบเขตการตรวจสอบให้เหมาะสม เป็นต้น

9. วิธีการตรวจสอบและเทคนิคการตรวจสอบงานด้านคอมพิวเตอร์ จะต้องพัฒนาให้ทันกับ Technology สมัยใหม่ที่ก้าวหน้าอย่างรวดเร็วและไม่หยุดยั้ง ทั้งทางด้าน Hardware และ Software วิธีการตรวจสอบจึงจำเป็นต้องพัฒนาขึ้น เพื่อช่วยให้ผู้ตรวจสอบมีเครื่องมือและรู้จักใช้เครื่องมือปฏิบัติงานอย่างมีประสิทธิภาพ และบรรลุวัตถุประสงค์ในการตรวจสอบ อีกทั้งจะช่วยให้ผู้ตรวจสอบมีความมั่นใจในการเสนอความเห็นในรายงานการตรวจสอบอย่างถูกต้องตามความเป็นจริงและมีเหตุมีผล

10. ผู้ตรวจสอบทางด้านคอมพิวเตอร์ นอกจากจะได้รับมอบหมายให้เป็นผู้ตรวจสอบความถูกต้องและความน่าเชื่อถือได้ของข้อมูลจากงานที่ประมวลผลด้วยคอมพิวเตอร์แล้ว ยังมีหน้าที่ที่สำคัญมากอีกประการหนึ่งก็คือ การร่วมมือและประสานงานตรวจสอบด้านการเงิน (Financial Audit) โดยแนะนำหรือร่วมปฏิบัติงานทางด้านเทคนิคการตรวจสอบในส่วนที่เกี่ยวข้อง เพื่อให้การปฏิบัติงานตรวจสอบทางด้าน Financial มีปัญหาน้อยที่สุด

ดังนั้น การศึกษาเทคนิคใหม่ ๆ ทางด้านคอมพิวเตอร์เพื่อประโยชน์ในการตรวจสอบจึงเป็นสิ่งที่จำเป็นอย่างยิ่ง และจะต้องดำเนินการควบคู่กันไปกับการปฏิบัติงานตรวจสอบด้วยเสมอ ทั้งนี้เพื่อดำรงไว้ซึ่งประสิทธิภาพของการตรวจสอบโดยรวม

11. เมื่อผมได้ไปปฏิบัติหน้าที่ในฐานะ Deputy Principal ของหลักสูตร SEACEN (South East Asian Central Banks) หลักสูตร Inspection and Supervision of Financial Institutions ครั้งที่ 12 ที่กรุงจาการ์ตา ประเทศอินโดนีเซีย เมื่อปี ค.ศ. 1988 ผมได้แนะนำให้เพิ่มวิชาที่มีเนื้อหาในด้านที่เกี่ยวกับคอมพิวเตอร์หลายวิชาในหลักสูตรนี้ ทาง SEACEN ได้เชิญผมไปบรรยายความจำเป็นของวิชาเหล่านี้ให้กับเลขาธิการของ SEACEN ที่ไปดูแลหลักสูตรนี้ที่กรุงจาการ์ตา และผมก็ได้ไปอธิบายเรื่องนี้ ณ ที่ทำการสำนักงานใหญ่ของ SEACEN ที่กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย ในปีเดียวกันนั้น ในเรื่องที่เกี่ยวข้องกับการพัฒนาการกำกับและการตรวจสอบสถาบันการเงินที่ต้องมีวิชานี้เข้าไปเกี่ยวข้องด้วย เพราะเป็นเรื่องที่แยกกันไม่ได้ในวงการกำกับและการตรวจสอบสถาบันการเงินที่ใช้คอมพิวเตอร์และทาง SEACEN ก็ได้บรรจุวิชาต่าง ๆ ที่เกี่ยวกับคอมพิวเตอร์เข้าไปในหลักสูตรนี้นับจากนั้นมาจนกระทั่งปัจจุบัน ซึ่งผมได้มีส่วนช่วยบรรยายหลายวิชาในหลักสูตรนี้ที่จัดขึ้นในประเทศต่าง ๆ ของสมาชิก SEACEN ในเวลาต่อมาด้วย

นั่นคือถึงแม้เป้าหมายของผู้ตรวจสอบจะเป็นการตรวจสอบฐานะความมั่นคงทางการเงินหรือเป็นการตรวจสอบเพื่อรับรองงบการเงิน แต่ข้อมูลและการควบคุมภายในส่วนใหญ่ได้ถูกประมวลโดยระบบคอมพิวเตอร์แล้ว ดังนั้น การวางแผนการตรวจสอบก็จะต้องคำนึงถึงและเข้าใจในระบบงานด้านคอมพิวเตอร์พอสมควรด้วยเสมอ

12. นอกจากที่กล่าวทาง SEACEN ก็ได้จัดหลักสูตรใหม่ขึ้นมาโดยเฉพาะ เรียกว่า Computer Audit (Advanced Level) ขึ้น เป็นหลักสูตรการตรวจสอบคอมพิวเตอร์ และการใช้คอมพิวเตอร์เข้าช่วยในการตรวจสอบในสถาบันการเงินโดยเฉพาะแยกเป็นอีกหลักสูตรหนึ่งโดยอบรมให้แก่ผู้ตรวจสอบจากธนาคารกลางประเทศต่าง ๆ ในเอเชีย

ทาง SEACEN ได้ให้ผมเป็น Course Director สำหรับหลักสูตรนี้อีกครั้ง เพื่อจัดให้มีการอบรมให้กับประเทศต่าง ๆ ที่กรุงเทพฯ เมื่อปลายปี ค.ศ. 1993 ซึ่งช่วงนั้นผมได้บรรยายวิชา EDP Supervision and Financial Institutions ด้วย โดยกล่าวถึง The Thai experienced ในเรื่อง ตามที่สรุปในภาคผนวกเล่มที่ 1 แล้ว แต่วิชาคอมพิวเตอร์อื่น ๆ ในหลักสูตรนี้ที่ผมได้บรรยายให้ SEACEN ในปีก่อนๆ หน้านี้ ผมไม่ได้นำมาให้ผู้อ่านได้อ่านด้วย เพราะมีบางส่วนได้กล่าวเป็นภาษาไทยในหนังสือชุดนี้อยู่แล้ว

13. การตรวจสอบด้านคอมพิวเตอร์ถึงแม้จะมีความจำเป็นเด่นชัด แต่ผู้บริหารในองค์กรต่างๆ ให้ความสำคัญกับการตรวจสอบด้านนี้แตกต่างกัน และมีจำนวนไม่น้อยที่มองข้ามประเด็นที่สำคัญนี้ อย่างไรก็ดี สำหรับธนาคารพาณิชย์ ธนาคารแห่งประเทศไทยได้กำหนดให้มีการตรวจสอบคอมพิวเตอร์เพื่อดูแลเรื่องนี้โดยเฉพาะตั้งแต่ปี 2528 สำหรับสถาบันการเงินอื่นๆ ทางธนาคารแห่งประเทศไทยก็ได้สั่งการให้สถาบันการเงินเหล่านั้นได้จัดให้มีการตรวจสอบงานด้านคอมพิวเตอร์แล้วด้วย

14. งานตรวจสอบด้านคอมพิวเตอร์ (IS Audit หรือ IS Examination) ในด้านของธนาคารแห่งประเทศไทย หรือ FFIEC ของประเทศสหรัฐอเมริกา แล้วมีวัตถุประสงค์อย่างกว้าง ๆ เช่นเดียวกับการตรวจสอบฐานะและความมั่นคงของสถาบันการเงิน นั่นคือ

1) เพื่อประเมินฐานะความมั่นคงของสถาบันการเงิน

2) เพื่อประเมินและวัดคุณภาพการจัดการ และการดำเนินงานของผู้บริหารระดับสูง

3) เพื่อให้คำแนะนำ แก้ไขจุดอ่อนต่าง ๆ ที่อาจก่อให้เกิดปัญหาต่อสถาบันการเงินเป็นการล่วงหน้า เพื่อให้สถาบันการเงินปรับปรุงคุณภาพของการบริหารงาน และการดำเนินงานให้มีความมั่นคง และเป็นไปตามระเบียบ คำสั่ง และกฎหมายที่เกี่ยวข้อง

อย่างไรก็ดี วัตถุประสงค์ของการตรวจสอบด้าน IS Audit ของผู้สอบบัญชีรับอนุญาต และผู้สอบบัญชีภายในจะแตกต่างกันไปตามเป้าหมายหลักของตนเอง

15. การตรวจสอบด้านคอมพิวเตอร์ที่ปัจจุบันมักนิยมเรียกกันว่า IS Audit ในประเทศสหรัฐอเมริกา และ IT Audit ในประเทศอังกฤษและออสเตรเลีย มากกว่าคำที่ใช้เรียกกันเต็ม ๆ ว่า Computer หรือ EDP Audit นั้น มีเรื่องที่ต้องทำความเข้าใจกันมากพอสมควร ยิ่งผู้สนใจท่านใดอ่านหนังสือประเภทนี้จากผู้แต่งหลาย ๆ คน จากประเทศต่าง ๆ แล้ว ก็อาจจะพบกับความสับสนมากขึ้น ทั้งนี้เพราะผู้แต่งแต่ละท่านก็มีความคิด/จุดยืนและทัศนรวมทั้งการผูกเรื่องให้อ่าน หรือทำความเข้าใจแตกต่างกันนั่นเอง

16. จุดยืนและความแตกต่างของตำราที่ผู้เขียนเรื่อง การตรวจสอบด้านคอมพิวเตอร์ ก็ขึ้นกับความถนัดและประสบการณ์ของผู้เขียนแต่ละท่าน เช่น บางท่านถนัดทางด้านการตรวจสอบระบบงานแต่ละอย่าง (Application Audit) เพราะผู้แต่งหรือผู้เขียนทำงานในด้านนี้ บางท่านทำงานในองค์กรเอกชนหรือตามโรงงานอุตสาหกรรมต่างๆ ในขณะที่บางท่านแต่งหรือเขียนหนังสือการตรวจสอบด้านคอมพิวเตอร์ในฐานะที่เป็นผู้กำกับและตรวจสอบสถาบันการเงิน จึงมีหน้าที่และบทบาทต่างกันออกไป เช่น ผู้ตรวจสอบของ FDIC, FRB, OCC ซึ่งเรียกรวม ๆ กันว่า Federal Financial Institution Examination Council (FFIEC) ของประเทศสหรัฐอเมริกาที่เป็นหน่วยงานของรัฐ ซึ่งทำหน้าที่ตรวจสอบทั้งฐานะความมั่นคงและการดำเนินงานโดยทั่วไป ซึ่งเรียกกันว่า Financial Examiner และบางส่วนแบ่งมาทำหน้าที่ตรวจสอบด้านคอมพิวเตอร์ เรียกกันในระยะแรก ๆ ว่า EDP Examiner นั้น ก็มีประสบการณ์การเขียนหนังสือการตรวจสอบด้านคอมพิวเตอร์แตกต่างกันไปตามความรับผิดชอบของตน นั่นคือ FFIEC จะเน้นการตรวจสอบทางด้านศูนย์ประมวลข้อมูลของสถาบันการเงิน (Data Center) ซึ่งจะตรวจงานทางด้านการดำเนินงานและการบริหารงานของศูนย์คอมพิวเตอร์เป็นสำคัญและจะไม่เน้นหรือจะไม่ตรวจสอบทางด้าน Application Audit ซึ่งทาง FFIEC พิจารณาว่าเป็นงานของผู้ตรวจสอบภายนอก (External Auditor) และผู้ตรวจสอบภายในของสถาบันการเงินหรือองค์กรอื่น ๆ ซึ่งผู้ตรวจสอบประเภทหลังนั้นจะตรวจสอบทั้งทางด้าน Data Center หรือตรวจสอบการควบคุมภายในโดยทั่วไป (General Controls) และตรวจสอบการควบคุมภายในเฉพาะระบบงาน หรือ เรียกว่า Application Controls หรือ Application Audit ด้วย

17. เมื่อมาถึงจุด ๆ นี้ ก็มีคำที่ต้องทำความเข้าใจกันต่อก็คือ การตรวจสอบงานด้านคอมพิวเตอร์ที่เรียกและเข้าใจกันง่าย ๆ Computer Audit นั้น มีการตรวจสอบเป็น 2 ลักษณะ

17.1 การตรวจสอบด้านศูนย์ประมวลข้อมูล (Data Center) หรือเรียกกันว่าเป็นการตรวจสอบการควบคุมโดยทั่วไป (General Controls) หรือเป็นการตรวจสอบ "องค์กร" หรือเป็นการตรวจสอบการดำเนินงานและการบริหารงานด้านคอมพิวเตอร์ขององค์กร

17.2 การตรวจสอบงานใดงานหนึ่งเป็นการเฉพาะ เช่น การตรวจสอบงานด้านเงินฝากเงินให้กู้ ฯลฯ ก็เรียกกันว่าเป็นการตรวจสอบด้าน Application หรือเป็นการตรวจสอบการควบคุมภายในเฉพาะงาน (Application Controls) หรือทำให้เข้าใจง่ายยิ่งขึ้นก็เรียกว่าการตรวจสอบ "งาน" ภายในองค์กร

18. การตรวจสอบงานด้านคอมพิวเตอร์ โดยหลักใหญ่ ๆ จึงสรุปได้ว่ามีเพียง 2 ลักษณะ คือ ตรวจสอบ "องค์กร" กับ "งาน" จะเป็นการตรวจสอบด้านใด ก็ขึ้นกับความรับผิดชอบของผู้ตรวจสอบในแต่ละองค์กรว่ายืนอยู่ ณ จุดใด มีความรับผิดชอบด้านใด ท่านต้องการกำหนดขอบเขตการตรวจสอบ (Audit Scope) เพียงใด ดังนั้นผู้อ่านจึงต้องแยกแยะว่าท่านต้องการเรียนรู้งานการตรวจสอบด้านคอมพิวเตอร์ลักษณะใด แล้วจึงค่อย ๆ ทำความเข้าใจกับคำอธิบายเฉพาะส่วนนั้น ๆ และความเกี่ยวพันที่เกี่ยวข้อง เช่น ควรเข้าใจว่าหาก General Controls มีปัญหาก็จะกระทบกับการวางแผนและการตรวจสอบด้าน Application Controls เพียงใด และควรมีวิธีการตรวจสอบอย่างไร เป็นต้น

อนึ่ง ถึงแม้จะมีตำราการตรวจสอบด้านคอมพิวเตอร์บางเล่มได้แยกหัวข้อการตรวจสอบแตกต่างไปจากที่กล่าวข้างต้น เช่น มักจะแยกหัวข้อการตรวจสอบการพัฒนาระบบงานเพิ่มมาอีกก็ตาม ผมก็ยังมีความเห็นว่าน่าจะรวมอยู่ในการตรวจสอบ General Controls จะเหมาะสมกว่า นอกจากนี้แผนภูมิแสดงการตรวจสอบโดยย่อที่มีมากกว่า 1 แห่ง ในหนังสือของผมทั้ง 3 หรือ 4 เล่ม ก็อาจมีความแตกต่างกันในรายละเอียดปลีกย่อย ทั้งนี้ขอให้ผู้อ่านอย่าสับสน เพราะเหตุผลเกิดจากแนวความคิดเบื้องต้นที่อาจแตกต่างกันบ้างของผู้เขียนหนังสือแต่ละคน เช่น บางคนเริ่มจากการวิเคราะห์ความเสี่ยง ซึ่งผมชอบแนวทางนี้ บางคนไม่วิเคราะห์ถึงความเสี่ยงก่อนแต่ให้เริ่มต้นจากการทำความเข้าใจระบบงานก่อนซึ่งในที่สุด ผู้อ่านจะพบว่าไม่ว่าจะเริ่มแบบใด ในที่สุดแล้วก็จะมาสู่จุดเดียวกันจนได้ หากท่านผู้อ่านเข้าใจได้เช่นนี้ก็แสดงว่าท่านเข้าใจแนวทางการตรวจสอบอย่างถ่องแท้แล้ว อย่างไรก็ดีหลักการส่วนใหญ่จะไม่แตกต่างกันมาก แต่จะแตกต่างกันในการบรรยายและการทำความเข้าใจ

19. ผู้อ่านควรทำความเข้าใจในคำต่อไปนี้ คือ EDP examiner, EDP auditor ซึ่งคำ ๆ หลังนี้ยังแยกได้เป็น 2 ส่วน คือ External Auditor และ Internal Auditor สรุปเพียงข้อนี้ก่อนว่าผู้ตรวจสอบด้านคอมพิวเตอร์เองก็มี 3 แบบ มีความรับผิดชอบและหน้าที่แตกต่างกัน และผู้ตรวจสอบต้องเข้าใจลักษณะของหน้าที่และความรับผิดชอบที่แตกต่างกันนั้น ๆ ด้วย เพราะความแตกต่างกันนั้น ยังมีส่วนเหลื่อมที่เป็นความเหมือนหรือความคล้ายกันปะปนกันอยู่ด้วย นั่นคือ การกำหนดขอบเขตและวิธีการตรวจสอบ อาจมีความสัมพันธ์ซึ่งกันและกันตามลักษณะของผู้ตรวจสอบ ทั้ง 3 แบบได้

20. การให้ถ้อยคำเป็นภาษาไทยที่ถอดความจากภาษาอังกฤษ ในศัพท์คอมพิวเตอร์บางครั้งก็มิใช่ของง่ายเพราะถึงแม้จะมีการแปลศัพท์คอมพิวเตอร์เป็นภาษาไทยกันแล้วหลายเล่ม แต่การใช้ภาษาไทยก็ยังมีการใช้แตกต่างกันอยู่ ซึ่งขึ้นกับความถนัดและความเข้าใจของผู้เรียบเรียงหรือผู้เขียนเป็นสำคัญ ดังนั้น การให้ถ้อยคำในภาษาไทยในแต่ละเรื่องถึงแม้มาจากภาษาอังกฤษคำ ๆ เดียวกัน ก็ใช้ถ้อยคำแตกต่างกันที่อาจทำให้ผู้อ่านสับสนได้ อย่างไรก็ดีคำศัพท์ภาษาไทยที่ยังไม่นิยมกัน ผมไม่ได้นำมาใช้ในเอกสารประกอบการบรรยายนี้ และคำศัพท์หลายคำผมได้ให้ความหมายใหม่ตามที่ผมเข้าใจ เช่นคำว่า "default" โดยทั่วไปแปลว่า "โดยปริยาย" แต่ในหลายตอนผมแปลว่า "มาตรฐานของระบบงานที่ได้กำหนดไว้ล่วงหน้า" หรือ "คำสั่งตามเงื่อนไขเบื้องต้นที่กำหนดไว้ในโปรแกรม" นอกจากนี้หากท่านผู้อ่านพบกับคำว่า เกิด default ก็ขอให้เข้าใจว่า "เกิดข้อคลาดเคลื่อน" หรือ "เกิดการปฏิบัติงานที่ผิดไปจากเงื่อนไขหรือคำสั่งงานที่กำหนดไว้" และในบางกรณีก็หมายถึง "เกิดปัญหาการปฏิบัติงานที่เกิดจากมาตรฐานหรือเงื่อนไขเบื้องต้น" ทั้ง ๆ ที่การเกิด default นี้เป็นไปตามคำสั่งหรือมาตรฐานของระบบงานก็ตาม ซึ่งแสดงถึงจุดอ่อนหรือความเสี่ยงที่เกิดจากการทำ default ในโปรแกรมนั่นเอง อย่างไรก็ดีความหมายในภาษาไทยที่ใช้และอาจเกิดความสับสนได้นั้น ผมจะวงเล็บภาษาอังกฤษเพื่อให้เปรียบเทียบประกอบความเข้าใจเป็นส่วนมากไว้ด้วย ดังนั้นหากท่านผู้อ่านจะนำศัพท์ภาษาอังกฤษไปเปรียบเทียบกับ Dictionary ด้านคอมพิวเตอร์ ก็จะพบว่าการให้ความหมายแตกต่างกันไป ซึ่งบางกรณีทำให้เกิดความเข้าใจที่แตกต่างกันด้วย

21. ถ้อยคำในภาษาไทยที่ใช้ในการบรรยายการตรวจสอบด้านคอมพิวเตอร์ในบางครั้งที่พบ เช่น การตรวจสอบระบบคอมพิวเตอร์โดยทั่วไป (ซึ่งหมายถึงการตรวจสอบ Data Center หรือ General Controls) กับคำว่าการตรวจสอบคอมพิวเตอร์เฉพาะงาน หรือบางครั้งก็ใช้คำว่าการตรวจสอบระบบงาน (ซึ่งหมายถึง Application Audit หรือ Application Controls) ถ้าผู้อ่านพยายามนึกถึงภาษาอังกฤษประกอบด้วยแล้ว จะทำให้ความสับสนน้อยลงได้ ทั้งนี้มีข้อแนะนำว่า หากรู้สึกสับสนก็ขอให้ถามตนเองว่าขณะนี้เรากำลังอยู่จุดไหนหรือขั้นตอนใดของงานการตรวจสอบ เรามีเป้าหมายและขอบเขตการตรวจสอบอะไร เพียงใด ก็จะช่วยได้มาก โดยเฉพาะ การให้คำภาษาไทยที่ไม่ได้วงเล็บภาษาอังกฤษไว้ด้วย

การที่ผมย้ำจุดนี้หลายครั้งก็เพราะจากประสบการณ์ที่ผ่านมาในระยะแรก ๆ ทั้งตัวผมเองและผู้ฟังการบรรยายมักจะพบกับปัญหาการทำความเข้าใจจากจุดนี้เป็นสำคัญ

22. ถ้อยคำอื่น ๆ ที่มีปัญหาก็อาจเกิดจากเทคนิคทางด้านคอมพิวเตอร์นอกเหนือจากการใช้ภาษาไทยได้ ตัวอย่างเช่น โปรแกรมระบบงาน (System Program หรือ System Software) และคำว่าโปรแกรมเฉพาะงาน (Application Program หรือ Application Software) โดยมีถ้อยคำภาษาไทยที่คล้ายกันมาก หากไม่วงเล็บภาษาอังกฤษไว้ด้วย จะชวนทำให้สับสนได้ง่ายเช่นกัน หรือการตรวจสอบความถูกต้องของรายการทางการเงิน ก็มีคำภาษาอังกฤษที่ใช้ต่าง ๆ กัน เช่น Validation Procedures หรือ Verification Procedures หรือ Substantive tests เป็นต้น ดังนั้น ผู้ตรวจสอบจึงควรทำความเข้าใจระบบงานของคอมพิวเตอร์ ให้ถ่องแท้ก่อนการวางแผนและดำเนินการตรวจสอบ

23. ถึงข้อนี้ ผมจึงขอกล่าวอีกครั้งว่า การตรวจสอบงานด้านคอมพิวเตอร์ ผู้ตรวจสอบจะต้องทำความเข้าใจกับระบบงานทั้งหมด (Total System Approaches) ในส่วนของงานที่ต้องการตรวจสอบในองค์กร กล่าวคือ ผู้ตรวจสอบต้องทำความเข้าใจทั้งในส่วนที่ใช้คอมพิวเตอร์ และส่วนที่ไม่ใช้คอมพิวเตอร์ และทั้ง 2 อย่างรวมกัน เพื่อแยกแยะให้ได้ว่า จะเริ่มต้นตรวจอะไรที่จุดใด ใช้เทคนิคแบบไหนจะตรวจสอบเมื่อใด และต้องการรูปแบบหลักฐานอย่างไร และควรจะจบลงอย่างไรในการตรวจสอบ ฯลฯ ในงานแต่ละเรื่องตามเป้าหมายที่กำหนดไว้ นอกจากนั้นผู้ตรวจสอบจะต้องเข้าใจความสัมพันธ์ของข้อมูลที่เกี่ยวข้องของ "งาน" (Application) ในแต่ละประเภทภายในองค์กร เพื่อกำหนดจุดตรวจสอบด้วย

24. จากข้อ 23. หากจะกล่าวให้ถูกต้องยิ่งกว่านี้ ก็ควรกล่าวว่าผู้ตรวจสอบทุกประเภทควรเข้าใจระบบงานที่ตรวจสอบทั้งในส่วนที่ใช้คอมพิวเตอร์ และไม่ใช้คอมพิวเตอร์ให้ดี จึงจะสามารถวางแผนและกำหนดขั้นตอนและเทคนิคการตรวจสอบที่เหมาะสม และติดตามการตรวจสอบของผู้ร่วมงานได้อย่างมีประสิทธิภาพ เพราะปัจจุบันทางการของไทยก็ได้ออกมาตรฐานการตรวจสอบบัญชีที่ใช้คอมพิวเตอร์ออกมา 3 ฉบับ ด้วยกัน คือ มาตรฐานการสอบบัญชีฉบับ ที่ 28, 29, 36 ให้ผู้สอบบัญชีโดยทั่วไปถือปฏิบัติอยู่แล้ว และกรมสรรพากรก็ได้ออกกฎเกณฑ์บางประการในการใช้คอมพิวเตอร์มาให้ถือปฏิบัติด้วยเช่นกัน ดังนั้น เมื่อกล่าวถึงการตรวจสอบโดยทั่วไป ผู้ตรวจสอบจึงไม่อาจหลีกเลี่ยงจากการทำความเข้าใจในระบบงานทั้งหมดก่อนการตรวจสอบเริ่มขึ้นได้ ยกเว้นการตรวจสอบที่มีเป้าหมายเฉพาะอย่างบางด้านและผู้ตรวจสอบมีความเข้าใจระบบงานโดยรวมขององค์กรที่จะเข้าตรวจสอบมาก่อนหลังจากองค์กรนำคอมพิวเตอร์มาใช้ในกระบวนการ "process" งานครั้งล่าสุดแล้ว

25. แม้ว่าในการนำคอมพิวเตอร์มาใช้จะไม่เปลี่ยนแปลงวัตถุประสงค์ในการตรวจสอบ แต่ลักษณะการประเมินการควบคุมภายในตลอดจนหลักฐาน และวิธีการตรวจสอบจะเปลี่ยนแปลงไปมาก

ในระบบที่ทำด้วยมือนั้น มักเน้นการทำ substantive test **ซึ่งเป็นการทดสอบรายการทางการเงิน เพราะการใช้คนหรือระบบ** Manual **ในการประมวลผลข้อมูลย่อมมีโอกาสเกิดความผิดพลาดได้ง่าย ซึ่งก่อให้เกิดความเสี่ยงสูง ดังนั้นการใช้** substantive test **จะช่วยลดความเสี่ยงได้มาก**

แต่ในระบบคอมพิวเตอร์ที่มีการพัฒนาก้าวหน้าไปไกลนั้น สภาพแวดล้อมต่าง ๆ ทางธุรกิจได้รับการออกแบบให้ควบคุมด้วยระบบคอมพิวเตอร์เป็นอย่างดี โอกาสที่จะเกิดการผิดพลาดเพราะ Human error อันเกิดจากการประมวลข้อมูลนั้นจะมีน้อยหรือไม่มีโอกาสเกิดขึ้นได้ ถ้าระบบงานและขั้นตอนการควบคุมภายในต่าง ๆ ที่ใช้คอมพิวเตอร์ควบคุมนี้ได้รับการทดสอบเป็นที่แน่ใจแล้วว่ามีประสิทธิภาพยอมรับได้ **ดังนั้นการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์จึงควรเปลี่ยนจากการเน้นตรวจ** substantive test **ไปเป็นการประเมินการควบคุมภายในแทนด้วยเหตุผล 3 ประการ คือ**

25.1 ความสม่ำเสมอของการประมวลผลด้วยคอมพิวเตอร์ช่วยให้มั่นใจได้ว่า การประมวลผลจะมีความสม่ำเสมอด้วย

25.2 การตรวจสอบผลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ในลักษณะของการทำ substantive test นั้น ทำได้ยากขึ้น เพราะหลักฐานการตรวจสอบต่าง ๆ ตลอดจน audit trail ได้เปลี่ยนแปลงไปมากและหลาย ๆ กรณีก็ไม่อาจกระทำการตรวจสอบแบบ manual ได้ด้วยวิธีการปกติ

25.3 ผู้ตรวจสอบถูกกำหนดให้มีความรับผิดชอบมากขึ้นในการตรวจสอบความเพียงพอของการควบคุมภายใน

ดังนั้น จะเห็นว่าผู้ตรวจสอบจำเป็นต้องฝึกฝนทักษะของตนในการประเมินการควบคุมภายในของธุรกิจที่มีการประมวลผลด้วยคอมพิวเตอร์ เหตุผลข้อ 25. นี้ เป็นการย้ำว่าในองค์กรที่ใช้คอมพิวเตอร์การตรวจสอบภายในเป็นเรื่องสำคัญลำดับต้น ๆ และการตรวจสอบด้านคอมพิวเตอร์ (IS Audit) ไม่ว่าจะเป็นการตรวจสอบ "องค์กร" (Data Center) หรือตรวจสอบ "งาน" (Application) ก็เน้นการตรวจสอบการควบคุมภายใน คือ General Controls และ Application Controls ด้านคอมพิวเตอร์นั่นเอง

เมื่อถึงประเด็นตามวรรคข้างต้น ผมคิดว่าเป็นจุดที่น่าสนใจ หากจะกล่าวต่อไปว่าการตรวจสอบเพื่อรับรองงบการเงินขององค์กร ซึ่งปกติเป็นหน้าที่ของผู้สอบบัญชีรับอนุญาต ซึ่งเป็นผู้สอบบัญชีภายนอกประเภทหนึ่งนั้น มีความสัมพันธ์กันอย่างใกล้ชิดกับการตรวจสอบงานด้านคอมพิวเตอร์ในองค์กรที่ใช้คอมพิวเตอร์ เพราะ IS Audit **หรือการตรวจสอบด้านคอมพิวเตอร์ เน้นการตรวจสอบด้านการควบคุมภายในและการดำเนินงานซึ่งเป็นขั้นตอนต้น ๆ ที่จำเป็นของการตรวจสอบฐานะการเงิน ดังนั้นการตรวจสอบด้านคอมพิวเตอร์** (IS **หรือ** IT Audit) **จึงมีความสัมพันธ์อย่างใกล้ชิดกับการตรวจสอบงบการเงินและการดำเนินงาน ซึ่งเรียกว่า** Financial Audit **อย่างสำคัญและไม่อาจหลีกเลี่ยงได้ในปัจจุบัน อย่างไรก็ดีการตรวจสอบฐานะความมั่นคงของสถาบันการเงินในภาพรวม ก็เป็นหน้าที่ของผู้ตรวจสอบจากธนาคารแห่งประเทศไทย ซึ่งเรียกรวม ๆ กันว่า** Financial examiner

จากความสัมพันธ์ดังกล่าว หนังสือเล่มนี้ซึ่งเน้นด้านการตรวจสอบด้านคอมพิวเตอร์ จึงได้กล่าวถึงการตรวจสอบทั้งทางด้าน IS Audit **และ** Manual Audit **ซึ่งเป็นการตรวจสอบแบบเดิมไว้เพื่อการศึกษาเปรียบเทียบและทำความเข้าใจในความแตกต่างของวิธีการตรวจสอบทั้ง 2 แบบ ไว้ด้วย**

26. ก่อนที่จะมีการประเมินประสิทธิภาพการควบคุมภายในไม่ว่าจะเป็น Data Center หรือ Application Audit ผู้ตรวจสอบควรมีการกำหนดเป้าหมายเฉพาะในการตรวจสอบเสียก่อน เพราะจะช่วยให้ทำการตรวจสอบได้โดยมีประสิทธิผลมากขึ้น และสามารถใช้เป็นเกณฑ์ดีในการประเมินผลการตรวจสอบได้อีกด้วย

27. ผู้ตรวจสอบจำเป็นต้องมีทักษะใหม่ ๆ ที่จะช่วยในการตรวจสอบธุรกิจที่มีการนำเอาคอมพิวเตอร์เข้ามาใช้ได้อย่างมีประสิทธิภาพ ทักษะทางด้านคอมพิวเตอร์ของผู้ตรวจสอบแต่ละคนอาจแตกต่างกันออกไป แต่สำหรับทั้งทีมงานแล้วต้องมีทักษะทางคอมพิวเตอร์โดยรวมที่เหมาะสม และเพียงพอแก่การปฏิบัติหน้าที่ตามมาตรฐานการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ของทางการ และของสากล

28. ผู้ที่ควบคุมหรือสอบทานงานตรวจสอบ ต้องมีคุณสมบัติลึกไปทางด้านเทคนิคเพียงพอระดับหนึ่งแก่การสอบทานงานของผู้ตรวจสอบระบบคอมพิวเตอร์ได้ หากการตรวจสอบนั้นเป็นการตรวจสอบด้านคอมพิวเตอร์หรือมีส่วนที่เกี่ยวข้องกับคอมพิวเตอร์

ในที่สุดแล้ว ผู้ตรวจสอบจะไม่สามารถทำงานเหล่านี้ทั้งหมดได้ตามลำพังจากความก้าวหน้าอันรวดเร็วทางเทคโนโลยี จำเป็นต้องให้ผู้บริหารและผู้ใช้ได้รับการฝึกอบรมทางด้านคอมพิวเตอร์ ผู้บริหาร ผู้ใช้ และบุคลากรฝ่ายคอมพิวเตอร์เองก็ควรได้รับการฝึกอบรมเกี่ยวกับมาตรฐานระบบงานและการควบคุมภายในด้วย

29. การทำแผนภูมิหลายแผนในหนังสือเล่มนี้ เป็นการจัดทำขึ้นเพื่อให้ผู้อ่านได้ติดตามและทำความเข้าใจเรื่องราวที่เกี่ยวข้องได้ง่ายและสะดวกขึ้น ทั้งนี้หลาย ๆ กรณีเป็นการประยุกต์มาจากความคิดและความเข้าใจของผมเองเพื่อใช้ในการบรรยายเป็นสำคัญ อย่างไรก็ดีผมใคร่ขอย้ำว่า ท่านผู้อ่านควรตอบตนเองก่อนว่าขณะนี้กำลังทำความเข้าใจเรื่องอะไร ขณะนี้กำลังอยู่ในส่วนใดของกระบวนการตรวจสอบ และกำลังมองมุมผู้ตรวจสอบว่าเป็นประการใดจาก 3 ประเภทดังได้กล่าวข้างต้นแล้ว ทั้งนี้ ต้องมีเป้าหมายและขอบเขตที่แน่นอนของตนเองด้วยว่ากำลังตรวจสอบประเภท และเรื่องอะไรอยู่เป็นต้น

30. เนื่องจากการรวบรวมเอกสารประกอบการบรรยายเรื่อง "การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์" เล่ม 2 นี้ ก็เช่นเดียวกับเล่ม 1 และเล่มที่จะพิมพ์ต่อไป ซึ่งเล่ม 3 จะเน้นเรื่องคอมพิวเตอร์กับการทุจริต และแนวการตรวจสอบการทุจริตที่ใช้คอมพิวเตอร์เป็นเครื่องมือรวมทั้งการจัดทำแผนฉุกเฉิน หนังสือทั้ง 3 หรือ 4 เล่ม เป็นการรวบรวมจากเอกสารประกอบการบรรยายเรื่องดังกล่าว โดยมีชื่อเรียกต่าง ๆ กันไป ในช่วงเวลาตั้งแต่ปี 2524-2536 แก่สถาบันหลายแห่ง และผมมีโอกาสแก้ไขเพิ่มเติมได้ไม่มากนัก เนื่องจากเวลาจำกัดมาก เพราะต้องการพิมพ์ให้เสร็จภายในเดือนกันยายน 2539 ทั้ง 3 เล่ม จึงอาจมีข้อมูลบางส่วนที่อาจไม่ทันสมัยเหมาะกับยุคอยู่บ้าง อย่างไรก็ดี ข้อมูลหรือเนื้อหารวมทั้งแผนภูมิต่าง ๆ มากกว่าร้อยละ 95 ยังคงใช้ได้ดีจนถึงปัจจุบัน เพราะถึงแม้เทคนิคด้านรายละเอียดทางคอมพิวเตอร์จะพัฒนาไปอีกมาก แต่หลักการส่วนใหญ่ของการประมวลงานและการตรวจสอบก็ยังคงใช้หลักการเดิม ทั้งนี้สังเกตได้จากการแต่งหนังสือที่มีการพิมพ์ครั้งหลังๆ ของตำราด้านตรวจสอบคอมพิวเตอร์ก็มีการแก้ไขใหม่ไม่มากนัก

31. สิ่งที่ผมใคร่จะเน้นก็คือการใช้เทคนิคการตรวจสอบว่าสมควรที่ผู้ตรวจสอบใช้เทคนิคใด ซึ่งขึ้นกับความรู้และประสบการณ์ของผู้ตรวจสอบเป็นหลัก และขึ้นกับความจำเป็นตลอดจนสิ่งแวดล้อมและหลักฐานที่ต้องการด้วย เช่น จะใช้การตรวจสอบในแบบ Around the Computer หรือที่นิยมเรียกกันใหม่เพื่อป้องกันความเข้าใจผิดว่า Audit without using the computer เพื่อเน้นว่าไม่ว่าจะเป็นการตรวจสอบแบบใด ผู้ตรวจสอบก็ไม่อาจหลีกเลี่ยงการประเมินประสิทธิภาพการควบคุมภายในได้ หรือใช้วิธีตรวจสอบลึกเข้าไปถึงการทำงานของโปรแกรมคอมพิวเตอร์ (Audit Through The Computer) พอสมควร ส่วนการใช้ Computer เป็นเครื่องมือช่วยในการวางแผนและการตรวจสอบนั้น ปัจจุบันนี้ผู้ตรวจสอบมีโอกาสเลือกน้อยแล้ว กล่าวคือ ผู้ตรวจสอบจำเป็นต้องใช้ Computer ให้มีส่วนช่วยในการตรวจสอบไม่มากก็น้อย ในอดีตผมและคณะผู้ตรวจสอบมักใช้วิธี Test Data ในการทดสอบความน่าเชื่อถือได้ของโปรแกรมซึ่งเป็นการทดสอบในแบบ Through the Computer แบบหนึ่งแต่ผมยังมีประสบการณ์น้อยในการใช้โปรแกรมสำเร็จรูปในการตรวจสอบ หนังสือชุดนี้จึงไม่ได้กล่าวถึงเรื่องนี้มากนัก

32. หนังสือทั้ง 3 เล่มหรืออาจมีถึง 4 เล่ม จากเรื่อง "การดำเนินงานและการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์" เป็นการรวบรวมเอกสารประกอบการบรรยายต่าง ๆ ของผมในช่วงระหว่างปี 2524 ถึง 2536 ดังกล่าวแล้วในคำนำเล่ม 1 โดยได้เขียนคำอธิบายเพิ่มเติมประกอบเรื่อง และแผนภาพในบางเรื่องเพื่อความเข้าใจที่กระจ่างขึ้น การเขียนเรื่องเพิ่มเติมและการตรวจทานความถูกต้องจากการพิมพ์ใช้เวลามากพอสมควร เนื้อหาสาระในหนังสือทุกเล่ม ถึงแม้จะพยายามลำดับเรื่องให้ได้ตามความเหมาะสมแล้วก็ตาม แต่ก็ยังมีเรื่องที่เป็นสิ่งละอันพันละน้อยต่าง ๆ ที่ผมได้สรุปไว้ใช้ในการบรรยายในโอกาสต่าง ๆ กันได้ปรากฏอยู่ในเรื่องหรือหัวข้ออื่นอยู่ด้วย เช่น ข้อสรุปที่ผู้ตรวจสอบและผู้บริหารควรทราบในรูปแบบแผนภูมิบ้าง แผนภาพบ้าง และคำบรรยายสรุปผัง

เป็นต้น สิ่งเหล่านี้จะเป็นประโยชน์และทำความเข้าใจให้กับผู้ฟังและผู้อ่านมากขึ้นถ้าผู้อ่านหรือผู้ใช้หนังสือชุดนี้จะหยิบยกเรื่องที่เกี่ยวข้องมาประกอบในเรื่องที่ศึกษาด้วย โดยเฉพาะอย่างยิ่งการศึกษาเรื่องคอมพิวเตอร์กับการทุจริตและการตรวจสอบ ซึ่งปรากฏในเล่ม 3 โดยสรุปเรื่องตรวจสอบเป็นบทสั้น ๆ เป็นการทบทวนในอีกแนวทางหนึ่งด้วย

33. การพัฒนางานตรวจสอบทั้งด้าน Computer Audit และ Financial Audit โดยจำลองระบบงานที่สำคัญขององค์กรนั้น ๆ เช่น สถาบันการเงิน โดยเน้นด้านการควบคุม และการตรวจสอบที่เป็นจริงให้ผู้ตรวจสอบติดตามได้ในภาคสนาม (Field work) จริง ๆ ที่เรียกกันว่า Simulation Audit นั้น เป็นเรื่องที่น่าสนใจมากเพราะจะทำให้ผู้ตรวจสอบได้ฝึกหัดการตรวจสอบ ณ ที่ทำการได้คล้าย ๆ กับการปฏิบัติงานจริงในภาคสนามเลยทีเดียว

34. หนังสือเล่มแรกของชุดนี้ ได้เร่งรีบจัดทำมากเพื่อให้ทันแจกจ่ายในงานวันธนาคารภาคตะวันออกเฉียงเหนือประจำปี 2539 ที่จังหวัดร้อยเอ็ด จึงได้มีการตรวจทานงานพิมพ์เพียงครั้งเดียว ประกอบกับมีความสับสนในการจัด file ที่แก้ไขแล้วและก่อนแก้ไขในการจัดพิมพ์จริง จึงปรากฏข้อผิดพลาดที่ตรวจพบภายหลังการเย็บเล่มแล้วหลายแห่ง จึงขออภัยท่านผู้อ่านมา ณ ที่นี้ด้วย อย่างไรก็ดีผมได้แทรกแก้ไขคำผิดไว้ในหน้าหลังของเล่มแรกแล้ว

35. หนังสือชุดนี้เป็นการให้คำแนะนำล่วงหน้าแก่สถาบันการเงินในด้านการบริหาร การดำเนินงานและการตรวจสอบ รวมทั้งประเด็นปัญหาที่น่าสนใจเพื่อหาทางป้องกันและ/หรือแก้ไขการทุจริต และการจัดทำแผนฉุกเฉินทางด้านคอมพิวเตอร์ ซึ่งจะปรากฏในเล่มต่อไป ทั้งนี้เป็นการดำเนินงานตาม Action plan ของธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ เพื่อให้บรรลุผลตามโครงการนี้ก็น่าจะช่วยลดภาระของธนาคารได้ทั้งในปัจจุบัน และอนาคต

อย่างไรก็ดี การทำความเข้าใจในหนังสือชุดนี้นั้น ผมได้ตั้งแนวทางว่า ท่านผู้อ่านได้ทราบพื้นฐานทางด้านการประมวลงานด้วยคอมพิวเตอร์พอสมควรแล้ว

36. ขอขอบคุณบรรดาเพื่อนร่วมงานในอดีตทุกท่าน โดยเฉพาะรุ่นบุกเบิกการตรวจสอบงานด้านคอมพิวเตอร์ ได้แก่ คุณสุขุม ตันตราจิณ คุณสรสิทธิ์ สุนทรเกศ คุณปรีชา ปรมาพจน์ คุณสมศักดิ์ มหินธิชัยชาญ คุณสุภักดิ์ ภูรยานนทชัย คุณวุฒิพงศ์ สมนึก คุณชาตรี วรวณิชชานันท์ และคุณพงศ์เทพ ชินพัฒน์ และเพื่อนร่วมงานรุ่นใหม่ที่เข้ามาเสริมทีมงานในภายหลังที่ไม่อาจระบุชื่อได้ทั้งหมด ซึ่งมีส่วนสำคัญในการช่วยเรียบเรียงเอกสารประกอบการบรรยายในอดีตหลาย ๆ เรื่อง และทำให้งานตรวจสอบด้านคอมพิวเตอร์แพร่หลายมากขึ้นในปัจจุบัน ขอขอบคุณอีกครั้งสำหรับการมีส่วนร่วมใด ๆ ที่ผ่านมาในกิจกรรมเผยแพร่เอกสารการดำเนินงานการตรวจสอบสถาบันการเงินด้านคอมพิวเตอร์ ขอขอบคุณเพื่อนร่วมงานในส่วนกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ ในปัจจุบันที่ช่วยตรวจทานความถูกต้องในการพิมพ์ครั้งนี้

เมธา สุวรรณสาร
ผู้อำนวยการ
ธนาคารแห่งประเทศไทย สาขาภาคตะวันออกเฉียงเหนือ
7 กันยายน 2539

สารบัญ

หน้า

บทที่ 1. แผนภาพแสดงสาเหตุแห่งความสูญเสียทางด้านคอมพิวเตอร์ที่ส่งผลกระทบต่อความมั่นคงของสถาบันการเงิน(เฉพาะที่มีเหตุมาจากการใช้คอมพิวเตอร์) 1

- ❑ **สาเหตุแห่งความสูญเสียทางด้านคอมพิวเตอร์ที่ส่งผลกระทบต่อความมั่นคงของสถาบันการเงิน(เฉพาะที่มีเหตุมาจากการใช้คอมพิวเตอร์)** 3
- ❑ **ตัวอย่างโครงสร้างของงานคอมพิวเตอร์ที่ผู้ตรวจสอบควรศึกษาและเข้าใจ เพื่อใช้เป็นแนวการตรวจสอบ** 4

บทที่ 2. มาตรฐานขั้นต่ำสำหรับการควบคุมภายในและการรักษาความปลอดภัยเกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของสถาบันการเงินและองค์กรทั่วไป 5

- ❑ **บทนำ** 7
- ❑ **การประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของสถาบันการเงิน** 8
- ❑ **มาตรฐานการควบคุมภายในและการรักษาความปลอดภัยเกี่ยวกับการประมวลผลข้อมูลด้วยคอมพิวเตอร์** 9
  - การควบคุมการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์หลัก 9
    - : การบริหารงานทั่วไป 9
    - : การพัฒนาระบบงานและโปรแกรม 10
    - : เอกสารสนับสนุนการปฏิบัติงานระบบประมวลผลข้อมูล 11
    - : การปฏิบัติการประมวลผล 13
    - : การประมวลผลโดยอาศัยระบบสื่อสาร 14
    - : การควบคุมความถูกต้องและน่าเชื่อถือของข้อมูล 16
    - : การรักษาความปลอดภัย 17
    - : การตรวจสอบงานคอมพิวเตอร์ 19
  - การควบคุมการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์ 20
    - : การรักษาความปลอดภัยเครื่องไมโครคอมพิวเตอร์ 21
    - : การควบคุมความปลอดภัยของแฟ้มข้อมูลและโปรแกรม 21
    - : การตรวจสอบการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์ 21

หน้า

บทที่ 3. เหตุผลการออกมาตรฐานการควบคุมภายในและการรักษาความปลอดภัยระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์ 23

บทที่ 4. แผนภาพแสดงภาพรวมการตรวจสอบสถาบันการเงินที่ใช้คอมพิวเตอร์ 37

บทที่ 5. กระบวนการตรวจสอบด้านคอมพิวเตอร์ 45

บทที่ 6. งานตรวจสอบคอมพิวเตอร์กับผู้บริหาร 53

- ❑ **วัตถุประสงค์ในการตรวจสอบงานด้านคอมพิวเตอร์** 55
- ❑ **ข้อควรทราบสำหรับผู้บริหารในงานตรวจสอบคอมพิวเตอร์** 55

บทที่ 7. การตรวจสอบองค์กรที่ใช้เครื่องคอมพิวเตอร์ 59

บทที่ 8. สรุปหลักการวิเคราะห์ความเสี่ยงเพื่อการตรวจสอบงานด้านคอมพิวเตอร์ 65

- ❑ **บทนำ** 67
- ❑ **หลักการวิเคราะห์ความเสี่ยง** 67
- ❑ **การวิเคราะห์ความเสี่ยงด้านคอมพิวเตอร์** 68
- ❑ **การตรวจสอบระบบงานคอมพิวเตอร์** 68
  - การวิเคราะห์ความเสี่ยง 68
  - การวางแผนการตรวจสอบ 69
  - ขั้นตอนการตรวจสอบ 69
  - การจัดทำรายงานการตรวจสอบ 71
  - การติดตามผลการตรวจสอบ 71
- ❑ **การตรวจสอบทั่วไปด้านคอมพิวเตอร์** 73
  - การวิเคราะห์ความเสี่ยง 73
  - การวางแผนการตรวจสอบ 73
  - ขั้นตอนการตรวจสอบ 74
  - การจัดทำรายงาน 75
  - การติดตามผลการตรวจสอบ 75

หน้า

บทที่ 9. มุมมองของความเสี่ยงด้านคอมพิวเตอร์จากกิจกรรมที่เกิดขึ้นและลักษณะของการควบคุมภายใน 77

- ❑ ความเสี่ยงของการดำเนินงานด้านคอมพิวเตอร์ที่มีผลกระทบต่อการควบคุม (Control risks) 79
- ❑ ตัวอย่างของการวิเคราะห์ความเสี่ยง / ความเสียหายของการประมวลข้อมูลด้วยระบบคอมพิวเตอร์ (จากจุดที่อาจก่อให้เกิดความเสียหาย) 83
- ❑ ระบบงานที่ประมวลข้อมูลด้วยคอมพิวเตอร์ 89
- ❑ ความเสี่ยงของการดำเนินงานด้านคอมพิวเตอร์ที่มีผลกระทบต่อการตรวจสอบ (Audit Risks) 91

บทที่ 10. การวางแผนการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ 101

- ❑ หลักการวางแผนการตรวจสอบ 103
- ❑ การวางแผนสอบบัญชีกับการวิเคราะห์ความเสี่ยง เพื่อให้เข้าถึงจุดควบคุมต่าง ๆ 104
  - ความเสี่ยงกับผู้ตรวจสอบ 105
  - ความเสี่ยงกับผู้บริหารระดับสูง 105
  - ความเสี่ยงกับการวางแผน 106

บทที่ 11. สรุปปัจจัยต่าง ๆ ในการวางแผนการตรวจสอบ 117

บทที่ 12. เปรียบเทียบขอบเขตและความสัมพันธ์ระหว่างการตรวจสอบของผู้สอบบัญชีภายนอกกับผู้สอบบัญชีภายใน 121

บทที่ 13. แผนภาพแสดงขั้นตอนของการประเมินประสิทธิภาพการควบคุมภายใน 127

บทที่ 14. แผนภาพแสดงกระบวนการ 3 ขั้นตอนในการตรวจสอบ 131

บทที่ 15. สรุป : ข้อควรทราบสำหรับผู้ตรวจสอบโดยทั่วไปก่อนการเข้าตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ 135

หน้า

❑ **ผลกระทบของคอมพิวเตอร์ต่อกระบวนการตรวจสอบทั่วไป** 137
❑ **ข้อสังเกตบางประการในการใช้คอมพิวเตอร์ช่วยในการประมวลข้อมูล** 138
❑ **การเข้าใจระบบงานที่ใช้คอมพิวเตอร์ จะช่วยผู้สอบบัญชีได้อย่างไร** 138
❑ **องค์ประกอบในการตรวจสอบในแต่ละเรื่อง** 138
❑ **การพิจารณาผังทางเดินของกิจกรรม และความสัมพันธ์กับข้อผิดพลาดหรือการควบคุมที่เกี่ยวข้อง** 139
❑ **ประเด็นคำถามที่จะช่วยในการตรวจสอบ** 140
❑ **ความรับผิดชอบของผู้สอบบัญชีในด้านการตรวจสอบงานที่ประมวลผลด้วยคอมพิวเตอร์** 141
❑ **ทำอย่างไรจึงจะสามารถทราบได้ว่า ผู้สอบบัญชีมีความเข้าใจในระบบงานที่ตรวจสอบ** 141
❑ **วิธีการตรวจสอบระบบงาน** 141
❑ **แนวการตรวจสอบระบบงานที่ประมวลผลด้วยคอมพิวเตอร์** 148

บทที่ 16. การตรวจสอบระบบข้อมูลที่ใช้คอมพิวเตอร์ 151
❑ **คำนำ** 153
❑ **ลักษณะสำคัญของการตรวจสอบ** 153
- วัตถุประสงค์และขอบเขตการตรวจสอบนั้นแน่นอน 153
- ขั้นตอนการตรวจสอบมีความสัมพันธ์ซึ่งกันและกัน 153
- วิธีการตรวจสอบขึ้นอยู่กับสภาพการณ์ 154
❑ **ขั้นตอนการตรวจสอบ** 154
- การศึกษาและบันทึกระบบงาน 154
  : การตรวจสอบทั่วไป 154
  : การตรวจสอบในระบบคอมพิวเตอร์ 154
- การประเมินระบบการควบคุมภายใน 156
  : การตรวจสอบทั่วไป 156
  : การตรวจสอบในระบบคอมพิวเตอร์ 156
- การตรวจสอบระบบการควบคุม 157
  : การตรวจสอบทั่วไป 157
  : การตรวจสอบในระบบคอมพิวเตอร์ 157

หน้า

- การประเมินผลกระทบของข้อบกพร่องในการควบคุม 158
  : การตรวจสอบทั่วไป 158
  : การตรวจสอบในระบบคอมพิวเตอร์ 158
- การตรวจสอบความถูกต้องของรายการทางการเงิน 158
  : การตรวจสอบทั่วไป 158
  : การตรวจสอบในระบบคอมพิวเตอร์ 159

❑ **สรุป** 159

บทที่ 17 การศึกษาและบันทึกระบบงาน 161

❑ **คำนำ** 163

❑ **การศึกษาระบบคอมพิวเตอร์** 163

- ความรู้ขั้นพื้นฐาน 163
- โครงสร้างและลักษณะของการประมวลผล 163
  : โครงสร้างของการประมวลผล 165
  : ลักษณะของการประมวลผล 166

❑ **การบันทึกระบบงาน** 172

- คุณประโยชน์ของการจัดทำผังงาน 172
- เทคนิคการจัดทำผังงาน 172
- การจัดทำผังงานในระบบคอมพิวเตอร์ 172
  : ผังงานเบื้องต้น 173
  : การจัดทำโปรแกรม 173
  : การแก้ไขข้อมูลถาวร 173
  : วิธีปฏิบัติเมื่อข้อมูลผิดพลาด 173
  : การควบคุมเป็นครั้งคราว 173
  : การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ 174
- เอกสารประกอบ 174
  : เอกสารประกอบระบบงาน 174
  : เอกสารมาตรฐานของระบบงาน 175

❑ **การทบทวนการศึกษาและบันทึกระบบงาน** 175

❑ **สรุป** 176

หน้า

บทที่ 18. การตรวจสอบเพื่อประเมินระบบการควบคุมภายใน 177

❑ **การตรวจสอบทั่วไป** 179

- ขอบเขตของการประเมิน 179
- การควบคุมขั้นพื้นฐานและกฎเกณฑ์การควบคุม 179

❑ **การตรวจสอบในระบบคอมพิวเตอร์** 180

- ลักษณะของการควบคุมในระบบคอมพิวเตอร์ 180
- การควบคุมทางด้านผู้ใช้ 181
- ขั้นตอนการทำงานของโปรแกรม 183
- การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ 184
- กฎเกณฑ์การควบคุม 186
  - : การกำกับ 186
  - : การแบ่งแยกหน้าที่ 186
  - : การพิทักษ์ทรัพย์สิน 186
- การเลือกให้ความเชื่อถือต่อระบบการควบคุม 188
- ช่วงเวลาที่เหมาะสมในการประเมิน 188

❑ **แบบสอบถามการควบคุมภายใน** 188

- ลักษณะของแบบสอบถาม 188
- เป้าหมายของการควบคุม 189
- การใช้แบบสอบถาม 189
  - : จำแนกความสำคัญของเป้าหมายในการควบคุม 189
  - : การตอบแบบสอบถาม 189
  - : การประเมินคำตอบในแบบสอบถาม 189
  - : ขั้นตอนการบันทึกข้อบกพร่องของการควบคุม 190

❑ **สรุป** 190

บทที่ 19. การประเมินผลระบบการควบคุม 191

❑ **แนวความคิดเกี่ยวกับการออกแบบระบบการควบคุม** 193

- โครงสร้างของการควบคุม 193
- มาตรฐานในการกำหนดการควบคุม 193
- ข้อมูลที่ควรจะควบคุม 193

หน้า

❑ **การควบคุมด้านการปฏิบัติงานและด้านโปรแกรม** 194

❑ **ความครบถ้วนของข้อมูลที่จะนำไปใช้ประมวลผล และการบันทึกข้อมูลที่มีการเปลี่ยนแปลง** 194

- การเลือกวิธีการควบคุมหลัก 194
- เทคนิคที่ใช้ในการควบคุม 194
  - : Batch totals 194
  - : การเช็คสอบรายงานจากคอมพิวเตอร์ 196
  - : การเช็คสอบลำดับของหมายเลขข้อมูลนำเข้า 198
  - : Computer matching 200
  - : Updating 201
  - : Rejections 206

❑ **ความถูกต้องของข้อมูลที่จะนำไปใช้ประมวลผล และการบันทึกข้อมูลลงในแฟ้มข้อมูล** 207

- Data Fields ที่ต้องการคุม 208
- เลขที่อ้างอิง (Reference Number) 208
- วันที่ (Date) 208
- สัญลักษณ์ (Indicators) 208
- เทคนิคที่ใช้ในการควบคุม (Control Techniques) 208
- การเลือกวิธีการควบคุมที่ดี 210

❑ **Computer - generated data** 211

❑ **การรับรองความถูกต้องของข้อมูลที่ส่งเข้าไปประมวลผล** 212

- การกำหนดเวลาและการรับรองความถูกต้องของข้อมูล 213
- การเลือกรับรองความถูกต้องข้อมูล 215
- การเช็คสอบความถูกต้องของข้อมูลโดยใช้โปรแกรม 216

❑ **การคำนวณสรุปผล และแยกประเภทข้อมูล** 217

- การคำนวณ 217
- การสรุปผลและแยกประเภทข้อมูล 218

❑ **การตรวจตราความถูกต้องของข้อมูลที่อยู่ในแฟ้มข้อมูล** 220

- การตรวจตราความถูกต้องของ Transaction Data 221
- การตรวจตราความถูกต้องของ Standing Data 221

หน้า

❑ **การสร้างแฟ้มข้อมูล** 222
- การควบคุม Transaction Data 222
- การควบคุม Standing Data 223
  : ระเบียบในการควบคุมการปฏิบัติงาน 223

บทที่ 20. การประเมินการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (1) 225

❑ **คำนำ** 227

❑ **วิธีประเมินผล** 227

❑ **การจัดองค์การในศูนย์คอมพิวเตอร์** 227

❑ **การควบคุมการพัฒนาโปรแกรม** 231
- กรณีระบบงานใหม่ 232
  : การวางระบบงานและการจัดทำโปรแกรม 233
  : การทดสอบโปรแกรมและระบบงาน 234
  : การ Catalog โปรแกรม 235
- การแก้ไขโปรแกรม 235
  : การปฏิบัติตามระเบียบในการแก้ไขโปรแกรม 236
  : ความสมบูรณ์ในการแก้ไขโปรแกรม 238
  : การทดสอบโปรแกรมที่มีการแก้ไข 238
  : การ Catalog โปรแกรมที่มีการแก้ไข 239
  : การแก้ไขโปรแกรมอย่างฉุกเฉิน 242

❑ **การควบคุมและการรักษาความปลอดภัยเกี่ยวกับตัวโปรแกรม** 243
- การควบคุมรักษาความปลอดภัยโปรแกรมที่อยู่ในระหว่างการใช้งาน 243
- การควบคุมและเก็บรักษา Utility Programs 247
- การควบคุมรักษาโปรแกรมที่ไม่ได้ใช้งาน 248

บทที่ 21 การประเมินการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (2) 249

❑ **คำนำ** 251

❑ **การควบคุมการใช้เครื่องคอมพิวเตอร์** 251
- Job Set-up 253
- โปรแกรมควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์และการใช้เครื่องคอมพิวเตอร์ 255
- การใช้แฟ้มข้อมูลให้ถูกต้อง 258
- การแก้ไขความเสียหายที่เกิดขึ้นจากการประมวลผลให้คืนสู่สภาพเดิม 259

หน้า

❑ **การควบคุมและการรักษาความปลอดภัยแฟ้มข้อมูล** 259

- การควบคุมแฟ้มข้อมูลระหว่างการใช้งาน 260
  - : การควบคุมการใช้แฟ้มข้อมูลของ Operator ในระหว่างการประมวลผล 260
  - : การควบคุมการใช้แฟ้มข้อมูลผ่านทางเครื่อง Terminal 261
  - : การใช้รหัสลับควบคุมการใช้แฟ้มข้อมูลผ่านทางเครื่อง Terminal 262
  - : การควบคุมการใช้แฟ้มข้อมูลโดยอาศัยวิธีการรักษาความปลอดภัยทางด้านตัวเครื่อง Terminal 263
  - : การควบคุมโปรแกรมที่ใช้ประมวลผลในการเข้าไปใช้แฟ้มข้อมูล 263
- การควบคุมแฟ้มข้อมูลที่ยังไม่ได้นำมาใช้งาน 264
  - : การรักษาความปลอดภัยสำหรับแฟ้มข้อมูลที่ยังไม่ได้นำมาใช้งาน 264
  - : การบันทึกรายละเอียดในการใช้แฟ้มข้อมูลที่เก็บไว้ใช้งาน 265

❑ **โปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์** 266

- การพัฒนาโปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์ 267
- การรักษาความปลอดภัยโปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์ 267

❑ **การบริหารระบบ Data Base** 268

❑ **สรุป** 268

บทที่ 22 การตรวจสอบระบบการควบคุม 269

❑ **การตรวจสอบทั่วไป** 271

- วัตถุประสงค์และขอบเขตของการตรวจสอบ 271
- การจัดทำเอกสารประกอบการตรวจสอบ 271
- ประเภทการตรวจสอบ 272
  - : การตรวจสอบหลักฐาน 272
  - : การสอบทานการปฏิบัติงาน 273

❑ **การตรวจสอบในระบบคอมพิวเตอร์** 273

- ลักษณะของการตรวจสอบ 273
- เทคนิคการตรวจสอบ 274
  - : การตรวจสอบกฎเกณฑ์การควบคุม 274
  - : การตรวจสอบการควบคุมทางด้านผู้ใช้ 275
  - : การตรวจสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ 275
  - : การตรวจสอบขั้นตอนการทำงานของโปรแกรม 276

หน้า

- ระดับการทดสอบ 286
  - : การตรวจสอบการควบคุมทางด้านผู้ใช้ 286
  - : การตรวจสอบความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ 286
  - : การตรวจสอบขั้นตอนการทำงานของโปรแกรม 287
  - : ข้อควรพิจารณาอื่น 287

❑ **สรุป** 288

บทที่ 23 การประเมินผลกระทบของข้อบกพร่องในระบบการควบคุมภายใน 289

❑ **คำนำ** 291

❑ **การประเมินผลกระทบของข้อบกพร่อง** 291

❑ **หลักเกณฑ์ในการพิจารณาข้อผิดพลาดอันมีนัยสำคัญ** 292

❑ **ผลกระทบต่อวิธีการตรวจสอบ** 293

❑ **การบันทึกข้อบกพร่องในการควบคุม** 294

❑ **ข้อบกพร่องที่พบบ่อยครั้งในระบบคอมพิวเตอร์** 296

❑ **การทุจริตในระบบคอมพิวเตอร์** 297

- การเบียดบังสินทรัพย์ 297
  - : การทุจริตโดยขั้นตอนของโปรแกรม 297
  - : การประมวลผลข้อมูลโดยมิชอบ 298
- การเสนอรายงานเท็จ 298
- ปฏิบัติการด้านกายภาพ 298

❑ **สรุป** 298

บทที่ 24 การตรวจสอบความถูกต้องของรายการทางการเงิน 299

❑ **การตรวจสอบทั่วไป** 301

- วัตถุประสงค์และขอบเขตของการตรวจสอบ 301
- ความสำคัญของการควบคุมภายในต่อการตรวจสอบความถูกต้องของรายการทางการเงิน 301
- ความเชื่อถือต่อการควบคุมภายใน 301
- การขยายขอบเขตการตรวจสอบ 302
- เอกสารประกอบการตรวจสอบความถูกต้องของรายการทางการเงิน 302

หน้า

❑ **การตรวจสอบในระบบคอมพิวเตอร์** 302

❑ **วิธีการตรวจสอบความถูกต้องของรายการทางการเงิน** 302

- ประเภทของการตรวจสอบความถูกต้องของรายการทางการเงิน 302
  - : การทดสอบความถูกต้องของรายการทางการเงิน 303
  - : วิธีการตรวจสอบอื่น ๆ 305
- การนำวิธีการตรวจสอบมาใช้ปฏิบัติงาน 305

❑ **ผลกระทบของคอมพิวเตอร์ต่อวิธีการตรวจสอบความถูกต้องของรายการทางการเงิน** 306

- การใช้โปรแกรมคอมพิวเตอร์ 306
  - : ขอบเขตการใช้โปรแกรมคอมพิวเตอร์ช่วยงานตรวจสอบ 306
  - : วิธีการใช้โปรแกรมคอมพิวเตอร์เข้าช่วยตรวจสอบ 308
  - : การตรวจสอบโดยอาศัยข้อมูลที่ได้จากคอมพิวเตอร์ 308
  - : ตัวอย่างการใช้โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบ 310
- การอาศัยวิธีการควบคุมที่เชื่อถือได้เข้าช่วยงานตรวจสอบ 311
- ประโยชน์ในการปรับปรุงวิธีการวิเคราะห์บัญชี 311
- การตรวจสอบยอดคงเหลือตามงบทดลอง 312
- การตรวจตัดยอด 312
- การกระทบยอด 312
- การสร้างข้อมูลตัวอย่างทดสอบ 312

❑ **เวลาที่ควรลงมือตรวจสอบความถูกต้องของรายการทางการเงิน** 312

❑ **ขอบเขตของการตรวจสอบความถูกต้องของรายการทางการเงิน** 313

- แนวทางทั่วไป 313
  - : ความเชื่อถือต่อการควบคุมภายใน 313
  - : ลักษณะ จำนวน และขนาดของรายการที่ประกอบเป็นยอดคงเหลือตามบัญชี 313
  - : ความสัมพันธ์ของบัญชีที่ตรวจสอบกับบัญชีหรือข้อมูลอื่น 314
  - : รายการที่น่าสังเกต 314
- การขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน 315
  - : วิธีการโดยทั่วไป 315
  - : การขยายขอบเขตการตรวจสอบในระบบคอมพิวเตอร์ 316

❑ **การใช้รหัสและโปรแกรมสำหรับการตรวจสอบ (Resident Code)** 316

- คำจำกัดความและวัตถุประสงค์ของ Resident Code 316

หน้า

- ประโยชน์ของ Resident Code 317
- วิธีการใช้ Resident Code 317

❑ **Snapshot** 317

❑ **การใช้โปรแกรมตรวจสอบโดยวิธีสอบถาม** 319

❑ **สรุป** 319

บทที่ 25 การใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบ 321

❑ **ลักษณะโปรแกรมคอมพิวเตอร์** 323
- โปรแกรมชนิดที่เขียนขึ้นเอง 323
- โปรแกรมตรวจสอบเฉพาะงาน 323
- โปรแกรมเบ็ดเสร็จ 323

❑ **ประเภทของโปรแกรม** 324

❑ **โปรแกรมตรวจสอบประเภท File Interrogation Package** 324
- File Interrogation Package แบบตายตัว 324
- File Interrogation Package แบบยืดหยุ่นได้ 325

❑ **ความสะดวกในการใช้ Computer Audit Package** 328
- องค์ประกอบเกี่ยวกับตัวเครื่องคอมพิวเตอร์ 328
- องค์ประกอบเกี่ยวกับแฟ้มข้อมูล 328
- ลักษณะการทำงานของ Package 328
  : การรวมยอดข้อมูล 328
  : การคัดเลือกตัวอย่าง 330
  : การพิมพ์รายงาน 330

❑ **ขั้นตอนการใช้โปรแกรมคอมพิวเตอร์** 331
- การใช้โปรแกรมในปีแรก 331
  : การเสนอใช้โปรแกรม 331
  : ข้อกำหนดเกี่ยวกับคุณสมบัติของโปรแกรม 331
  : การเตรียมงาน 331
  : การเปลี่ยนแปลงรูปคำสั่งเป็นภาษาเครื่องจักร 331
  : การทดสอบโปรแกรม 331
  : การดำเนินการประมวลผล 332

หน้า

: การควบคุมโปรแกรมที่ใช้ตรวจสอบ 332
: การใช้แฟ้มข้อมูลที่แท้จริงในการตรวจสอบ 332
: แผนการตรวจสอบ 332
: รายงานผลการใช้โปรแกรมตรวจสอบ 333
: การจัดเก็บโปรแกรมและคำสั่งอื่น ๆ ที่ใช้ในการควบคุม 333
: การจัดทำ Work Plan 333
- การใช้โปรแกรมในการตรวจสอบครั้งถัดไป 333
❑ **สรุป** 333

บทที่ 26 การตรวจสอบศูนย์บริการคอมพิวเตอร์ 335
❑ **คำนำ** 337
❑ **ลักษณะทั่วไปของการประมวลผล ณ ศูนย์บริการคอมพิวเตอร์** 337
❑ **ผลกระทบที่มีต่อการตรวจสอบ** 337
- การควบคุมภายใน 337
: ขั้นตอนการทำงานของโปรแกรม 338
: การควบคุมการบำรุงรักษาและแก้ไขเปลี่ยนแปลง 338
: การควบคุมรายงาน 339
- วิธีการตรวจสอบ 339
: การประเมินการควบคุมภายใน 339
: การตรวจสอบระบบการควบคุม 339
: การตรวจสอบความถูกต้องของรายการทางการเงิน 339
❑ **การคัดเลือกศูนย์บริการคอมพิวเตอร์** 340
- มาตรการในการคัดเลือกศูนย์บริการคอมพิวเตอร์ 340
- การประเมินข้อเสนอของศูนย์บริการคอมพิวเตอร์ 341
- การทำสัญญา 341
❑ **การปฏิบัติงานร่วมกับศูนย์บริการคอมพิวเตอร์** 342
- การติดต่อประสานงานระหว่างกัน 342
- การพัฒนาระบบงาน 343
- การปฏิบัติงาน 344
❑ **สรุป** 345

หน้า

บทที่ 27. ตัวอย่างคำถามอีกรูปแบบหนึ่งที่ใช้เป็นเทคนิคในการประเมินการควบคุมภายในสำหรับการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ 347

- **การควบคุมภายในเกี่ยวกับการบริหาร** 350
  - การแบ่งแยกความรับผิดชอบ 350
  - การควบคุมพนักงานผู้ควบคุมการทำงานของเครื่อง 350
  - การควบคุมแฟ้มข้อมูล 351
  - วิธีการในการระบุความแตกต่างของแฟ้มข้อมูล 351
  - วิธีการในการสร้างแฟ้มข้อมูลใหม่ 351
  - มาตรการป้องกันไฟและมาตรการฉุกเฉิน 352
- **การควบคุมการพัฒนาระบบ** 352
- **การควบคุมเฉพาะระบบงาน** 354

บทที่ 28. แนวการตรวจสอบการดำเนินงานและการควบคุมภายในด้านคอมพิวเตอร์ในภาคปฏิบัติ (เป็นการตรวจสอบด้าน General Controls ของคอมพิวเตอร์โดยรวม) 359

- **การตรวจสอบภายในและการตรวจสอบของผู้สอบบัญชี** 361
- **การจัดการ** 370
- **ระบบงานและโปรแกรม** 374
- **ความน่าเชื่อถือของข้อมูล** 381
- **การปฏิบัติงานคอมพิวเตอร์** 385
- **การประมวลผลโดยอาศัยระบบสื่อสาร** 397
- **ระบบเงินโอน** 402
- **การใช้บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน** 412

บทที่ 29. แนวทางการตรวจสอบคอมพิวเตอร์ขนาดเล็ก 415

- **การนำคอมพิวเตอร์มาใช้งาน** 417
- **การเลือก Application Software** 418
- **การสนับสนุนจากผู้ขาย** 418
- **การจัดทำสัญญาซ่อมแซมบำรุงรักษา** 419

หน้า

- ❑ การรักษาความปลอดภัยด้านสถานที่ 419
- ❑ System Software 419
- ❑ การจ้างบุคคลภายนอกเขียนโปรแกรม 420
- ❑ การควบคุมทางด้านเอกสาร 420
- ❑ การแก้ไขโปรแกรมโดยอาศัยระบบสื่อสาร 421
- ❑ การปฏิบัติการทางด้านคอมพิวเตอร์ 421
- ❑ การตรวจสอบ 421
- ❑ การ Backup 422
  - Hardware Backup 422
  - Software Backup 422
  - Data file Backup 422
- ❑ แผนปฏิบัติงานชั่วคราวกรณีเกิดเหตุฉุกเฉิน 422
- ❑ การประกันภัย 423
- ❑ บทสรุป 423

ภาคผนวก ก. การป้องกันระบบงานและการบันทึกรายการเพื่อการตรวจสอบ 427

ภาคผนวก ข. ตัวอย่างเปรียบเทียบการตรวจสอบสินค้าคงคลังในระบบ Manual และ ในระบบ computer 429

ภาคผนวก ค. ผังแสดงขั้นตอนการแปลงโปรแกรมที่เขียนขึ้นด้วยภาษาเขียนให้เป็นโปรแกรมที่พร้อมจะทำงานได้ ขั้นตอนทดสอบการทำงานของโปรแกรม และการ Catalog โปรแกรม 433

ภาคผนวก ง. แนวการตรวจสอบระบบการควบคุม 439

ภาคผนวก จ. การตรวจสอบระบบฐานข้อมูล 455

ภาคผนวก ฉ. การใช้ตัวอย่างข้อมูลทดสอบการประมวลผล 463

ภาคผนวก ช. ตัวอย่างการใช้ตัวอย่างข้อมูลทดสอบการประมวลผล 469

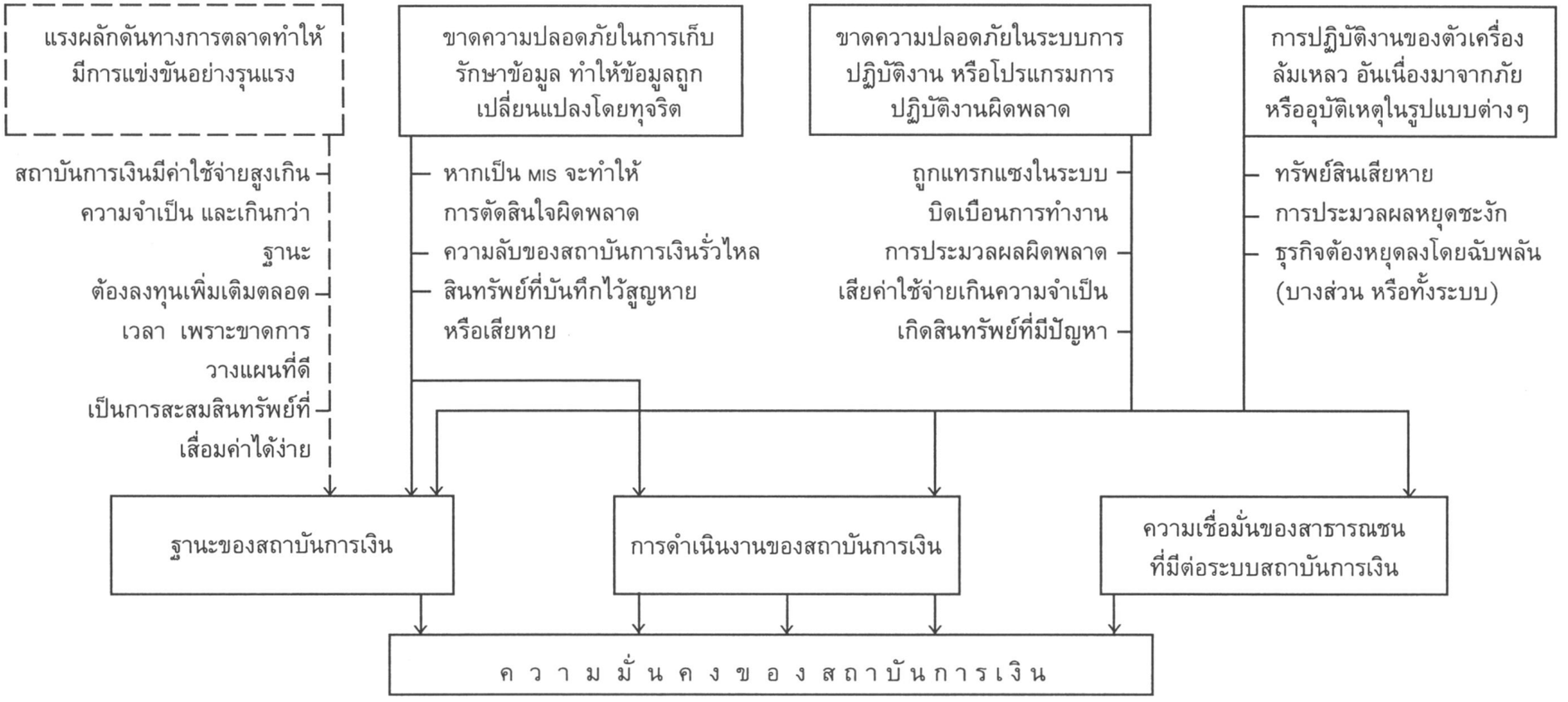
ภาคผนวก ซ. การวิเคราะห์รหัสคำสั่งโปรแกรม 475

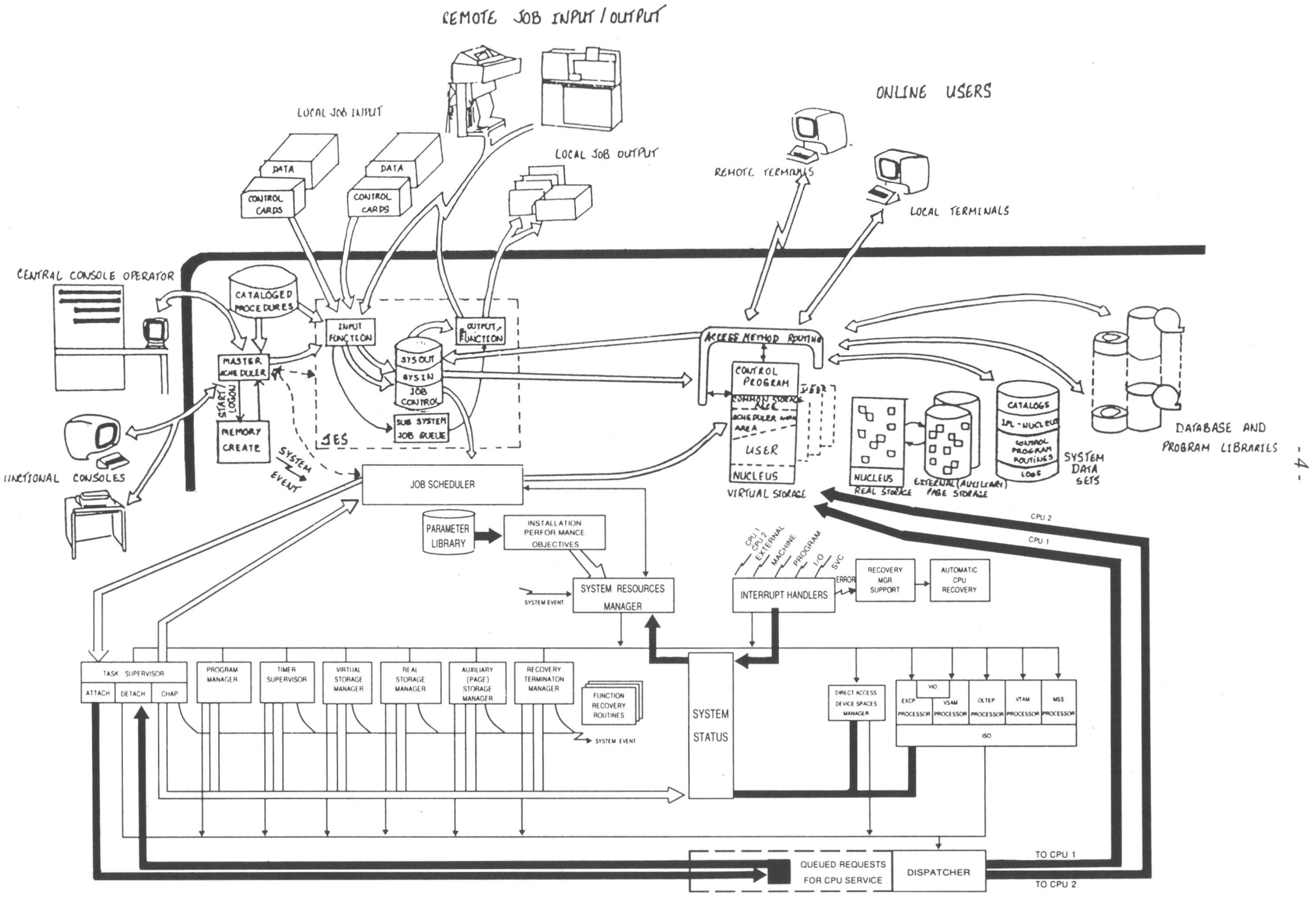
ภาคผนวก ฌ. รายงานหลักที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ 485

1

แผนภาพแสดงสาเหตุแห่งความสูญเสียทางด้านคอมพิวเตอร์ที่ส่งผลกระทบต่อความมั่นคงของสถาบันการเงิน (เฉพาะที่มีเหตุมาจากการใช้คอมพิวเตอร์)

สาเหตุแห่งความสูญเสียทางด้านคอมพิวเตอร์ที่ส่งผลกระทบต่อความมั่นคงของสถาบันการเงิน (เฉพาะที่มีเหตุมาจากการใช้คอมพิวเตอร์)





ตัวอย่างโครงสร้างของงานคอมพิวเตอร์ที่ผู้ตรวจสอบต้องศึกษาและเข้าใจเพื่อใช้เป็นแนวการตรวจสอบ

2

มาตรฐานขั้นต่ำสำหรับการควบคุมภายใน และการรักษาความปลอดภัย เกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ ของสถาบันการเงินและองค์กรทั่วไป

มาตรฐานขั้นต่ำสำหรับการควบคุมภายในและการรักษาความปลอดภัย เกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ ของสถาบันการเงินและองค์กรทั่วไป

1. บทนำ

การนำระบบคอมพิวเตอร์มาใช้ในการประกอบธุรกิจ และการประมวลผลข้อมูลของสถาบันการเงิน รวมทั้งองค์กรอื่น ๆ อาจก่อให้เกิดความเสียหายที่จะกระทบการดำเนินงานและความมั่นคงของสถาบันการเงินและองค์กรในที่สุด อันเนื่องจากสาเหตุที่สำคัญ 4 ประการ คือ

1) ความล้มเหลวในการพัฒนางานคอมพิวเตอร์ หรือใช้งานได้ไม่ตรงตามความต้องการ เป็นเหตุให้เกิดความสูญเสีย (Development risk)

2) ระบบคอมพิวเตอร์เสียหายหรือถูกทำลายโดยอุบัติเหตุหรือเจตนากระทำ เป็นเหตุให้ไม่สามารถประกอบธุรกิจได้ (Business interruption)

3) การทุจริตในระบบคอมพิวเตอร์ (Computer frauds) ซึ่งก่อให้เกิดความเสียหาย อาจเกิดขึ้นได้หลายกรณี ดังนี้

3.1) การลักลอบแก้ไขข้อมูลก่อนนำเข้าคอมพิวเตอร์

3.2) การนำข้อมูลที่ไม่ผ่านการอนุมัติหรือการตรวจสอบเข้าเครื่องคอมพิวเตอร์

3.3) การลักลอบแก้ไขโปรแกรมที่อยู่ระหว่างการพัฒนาหรือการปรับปรุง เพื่อสร้างรายการทุจริตหลีกเลี่ยงการควบคุม ล้างรายการ และเพื่อไม่ให้ปรากฏหลักฐานที่จะใช้ในการตรวจสอบ (Audit trail)

3.4) การลักลอบนำแฟ้มข้อมูลคอมพิวเตอร์ไปใช้ภายนอกเพื่อประโยชน์ส่วนตัว

3.5) การลักลอบเพิ่มเติมและแก้ไขรายการขณะที่อยู่ในระบบสื่อสาร

4) ความผิดพลาดที่เกิดจากการกระทำของพนักงานปฏิบัติงานคอมพิวเตอร์ (Error risks) ซึ่งอาจเกิดขึ้นได้ในหลายกรณี ดังนี้

4.1) ความผิดพลาดที่เกิดจากการป้อนข้อมูล (Data entry error)

4.2) ความผิดพลาดที่เกิดจากการจัดทำหรือแก้ไขโปรแกรมคอมพิวเตอร์ (Programming error)

4.3) ความผิดพลาดที่เกิดจากการออกแบบระบบงาน (Designing error)

4.4) ความผิดพลาดที่เกิดจากการแก้ไขข้อมูลคอมพิวเตอร์ (Correcting error)

ดังนั้น การป้องกันมิให้เกิดความเสียหายดังกล่าว จึงเป็นเรื่องที่มีความสำคัญและจำเป็นอย่างยิ่งสำหรับสถาบันการเงินที่ประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ การจัดให้มีระบบการควบคุมภายใน และการรักษาความปลอดภัยที่เหมาะสม จะสามารถป้องกันหรือจำกัดความเสียหายให้อยู่ในขอบข่ายที่ยอมรับได้

2. การประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของสถาบันการเงิน

การจำแนกประเภทการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของสถาบันการเงิน ไม่ได้ยึดถือตามขนาดของสถาบันการเงินหรือขนาดของเครื่องคอมพิวเตอร์ ทั้งนี้เพราะในปัจจุบันเครื่องคอมพิวเตอร์ขนาดเล็ก (Minicomputer) ได้รับการพัฒนาทางด้านเทคนิค จนกระทั่งมีศักยภาพและประสิทธิภาพทัดเทียมกับเครื่องคอมพิวเตอร์ขนาดใหญ่ ดังนั้น การกำหนดประเภทของระบบการประมวลผลข้อมูลของสถาบันการเงิน จึงถือตามสภาพแวดล้อมและโครงสร้างของการดำเนินงานการประมวลผลข้อมูลของสถาบันการเงินเป็นสำคัญ ซึ่งอาจแบ่งได้เป็น 2 ประเภทใหญ่ ๆ คือ การประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์หลัก (Computer Center) และการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์

2.1 การประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์หลัก หมายถึง ระบบประมวลผลข้อมูลของสถาบันการเงิน ซึ่งมีฝ่ายหรือแผนกคอมพิวเตอร์รับผิดชอบงานประมวลผลข้อมูลให้แก่ฝ่ายงานอื่น ๆ ในบริษัท ระบบประมวลผลข้อมูลหลักยังอาจแบ่งย่อยออกเป็น 3 ขนาด คือ ระบบประมวลผลข้อมูลขนาดเล็ก (Small system) ระบบประมวลผลข้อมูลขนาดกลาง (Medium system) และระบบประมวลผลข้อมูลขนาดใหญ่ (Large system)

1) ระบบประมวลผลข้อมูลขนาดเล็ก ได้แก่ ระบบประมวลผลข้อมูลของสถาบันการเงิน ซึ่งโดยปกติใช้คอมพิวเตอร์ขนาดเล็ก (Minicomputer system) ในการประมวลผล โดยมีบริษัทผู้ผลิตหรือผู้ขายเครื่องคอมพิวเตอร์เป็นผู้พัฒนา หรือจัดหาโปรแกรมระบบงาน (Application programs) ให้ทั้งหมด รวมทั้งการฝึกอบรมพนักงาน หรือที่เรียกว่า ระบบ Turn Key ดังนั้น จึงมักจะไม่พบงานด้านการพัฒนาโปรแกรมระบบงาน (System & Programming function) ในระบบประมวลผลข้อมูลขนาดเล็ก การบริหารงานระบบประมวลผลข้อมูล (EDP Management) จะมุ่งเน้นการควบคุมดูแลการปฏิบัติงานประมวลผลข้อมูลประจำวัน (Daily Operations) อาจไม่มีการกำหนดนโยบาย การจัดทำแผนงาน และระเบียบปฏิบัติงาน เป็นลายลักษณ์อักษร การแบ่งแยกหน้าที่อาจไม่เป็นไปตามหลักการควบคุมภายใน พนักงานคนหนึ่งอาจทำหน้าที่หลายอย่างเพื่อประหยัดรายจ่ายในการดำเนินงาน เช่น คนเดียวกันอาจทำหน้าที่ป้อนข้อมูล ประมวลผลข้อมูล และตรวจสอบความถูกต้องของรายงาน เป็นต้น

2) ระบบประมวลผลข้อมูลขนาดกลาง หมายถึง ระบบประมวลผลข้อมูลของสถาบันการเงิน ซึ่งโดยปกติใช้คอมพิวเตอร์ขนาดเล็กและขนาดกลาง (Minicomputer และ Superminicomputer) ในการประมวลผลข้อมูล แต่ต่างกับระบบประมวลผลขนาดเล็กเนื่องจากมีการพัฒนาโปรแกรมระบบงานด้วยตนเอง ในการบริหารงานระบบประมวลผลข้อมูลจะมีคณะกรรมการคอมพิวเตอร์ (EDP Steering Committee) ทำหน้าที่กำหนดนโยบาย แผนงาน และควบคุมดูแลการดำเนินงานด้านคอมพิวเตอร์ของบริษัท การแบ่งแยกหน้าที่งานประมวลผลข้อมูลมีมากกว่าระบบประมวลผลขนาดเล็ก โดยจะแยกหน้าที่ระหว่างการจัดทำโปรแกรมระบบงาน การใช้เครื่องประมวลผล การป้อนข้อมูล และการควบคุมความถูกต้องของรายงานออกจากกัน

3) ระบบประมวลผลข้อมูลขนาดใหญ่ หมายถึง ระบบประมวลผลข้อมูลของสถาบันการเงิน ซึ่งโดยปกติจะใช้คอมพิวเตอร์ขนาดใหญ่ (Mainframe หรือ Large scale computer) ในการประมวลผลข้อมูลของบริษัท สาขา บริษัทในเครือ และสถาบันภายนอก เนื่องจากเครื่องคอมพิวเตอร์ขนาดใหญ่มีศักยภาพและประสิทธิภาพสูง มีคณะกรรมการคอมพิวเตอร์ทำหน้าที่บริหารงานระบบประมวลผลของบริษัท กำหนดนโยบาย เป้าหมาย แผนงาน และควบคุมดูแลการดำเนินงานด้านคอมพิวเตอร์ของบริษัทให้เป็นไปตามมาตรฐานสากล การแบ่งแยกหน้าที่งานประมวลผลข้อมูลจะละเอียดกว่าระบบประมวลผลขนาดกลาง และจะมีเจ้าหน้าที่ที่มีความรู้ทางเทคนิคและ

ความชำนาญเฉพาะด้านเพิ่มขึ้น เช่น เจ้าหน้าที่ปฏิบัติงานระบบสื่อสารข้อมูล (Data Communication) เจ้าหน้าที่ปฏิบัติงานระบบฐานข้อมูล (Data Base) และเจ้าหน้าที่ปฏิบัติงานโปรแกรมระบบเครื่อง (Technical Support group) เป็นต้น

2.2 การประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์ จัดว่าเป็นระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์ที่มีขนาดเล็กที่สุด สำหรับใช้ประจำส่วนงานและหน่วยงานต่าง ๆ ในบริษัท (End User) ปกติจะใช้กับงานโปรแกรมสำเร็จ เช่น LOTUS 1-2-3, DBASE III PLUS และ WORD PROCESSING เป็นต้น

3. มาตรฐานการควบคุมภายในและการรักษาความปลอดภัยเกี่ยวกับการประมวลผลข้อมูลด้วยคอมพิวเตอร์

เป้าหมายหรือวัตถุประสงค์ในการควบคุมภายในเหมือนกัน ไม่ว่าจะเป็นระบบประมวลผลที่ปฏิบัติโดยบุคคลหรือคอมพิวเตอร์ กล่าวคือ เพื่อให้มีการบันทึกข้อมูลรายการทางการเงินอย่างถูกต้องและครบถ้วน มีการดูแลรักษาทรัพย์สินไม่ให้สูญหายและเสียหาย มีการปฏิบัติงานอย่างมีประสิทธิภาพและเป็นไปตามนโยบาย แผนงาน และระเบียบปฏิบัติตามที่ฝ่ายบริหารกำหนด การกำหนดขอบเขตและลักษณะการควบคุมภายในที่ดีควรคำนึงถึงขนาดธุรกิจ ปริมาณธุรกิจ และลักษณะการนำคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูล

ดังนั้น เพื่อให้สถาบันการเงินที่ใช้ระบบคอมพิวเตอร์ในการให้บริการทางธุรกิจ และการประมวลผลข้อมูลมีแนวทางในการกำหนดการควบคุมภายในที่สามารถป้องกันหรือลดความเสี่ยงต่อความเสียหายที่กล่าวลงได้ ธนาคารแห่งประเทศไทยจึงกำหนดให้สถาบันการเงินที่ใช้ระบบคอมพิวเตอร์ ต้องจัดให้มีการควบคุมภายในและการรักษาความปลอดภัยตามมาตรฐานขั้นต่ำ ดังนี้

3.1 การควบคุมการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์หลัก

3.1.1 การบริหารงานทั่วไป

1) การจัดองค์การ สถาบันการเงินควรจัดให้มีฝ่ายงานที่รับผิดชอบระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์เป็นเอกเทศจากฝ่ายอื่น ๆ และมีการแบ่งแยกหน้าที่รับผิดชอบภายในฝ่ายอย่างชัดเจน โดยเฉพาะอย่างยิ่งการแยกหน้าที่ระหว่างการพัฒนาระบบงาน (System Development & Programming) การปฏิบัติการประมวลผล (Computer Operations) การนำข้อมูลเข้า (Data Entry) และการสอบทานความถูกต้องของข้อมูลผลลัพธ์และรายงาน (Data Output)

2) การวางแผน สถาบันการเงินควรกำหนดนโยบายและจัดทำแผนงานเกี่ยวกับการจัดหาเครื่องคอมพิวเตอร์ โปรแกรมระบบเครื่อง โปรแกรมระบบงาน และบุคลากรที่จะรองรับความต้องการภายในองค์กรและการบริการลูกค้าในระยะสั้นและระยะยาว ในการจัดทำแผนงานสถาบันการเงินอาจมอบหมายให้คณะกรรมการ ซึ่งประกอบด้วยผู้บริหารระดับฝ่ายงานต่าง ๆ ร่วมกันทำหน้าที่วางแผนและควบคุมดูแลให้การปฏิบัติงานเป็นไปตามแผนที่วางไว้

3) ระเบียบปฏิบัติงาน สถาบันการเงินควรกำหนดระเบียบปฏิบัติงานสำหรับหน่วยงานในฝ่ายประมวลผลข้อมูลฯ เพื่อใช้เป็นแนวทางในการปฏิบัติงานให้มีประสิทธิภาพ และใช้ในการฝึกอบรมพนักงานใหม่

4) การรายงานผลการปฏิบัติงาน สถาบันการเงินควรกำหนดให้ฝ่ายประมวลผลข้อมูลฯ จัดทำรายงานผลการปฏิบัติงานเสนอฝ่ายบริหาร ซึ่งอาจแยกเป็น 3 เรื่องใหญ่ ๆ คือ การปฏิบัติงานประมวลผล การพัฒนาระบบงานและการพนักงาน และเรื่องทั่ว ๆ ไป

3.1.2 การพัฒนาระบบงานและโปรแกรม

ในการพัฒนาระบบงาน สถาบันการเงินอาจเลือกกระทำได้ 2 วิธี คือ สถาบันการเงินเป็นผู้กระทำการพัฒนาระบบงานด้วยตนเอง หรือว่าจ้างให้บุคคลภายนอกเป็นผู้พัฒนาหรือจัดหาโปรแกรมระบบงานสำเร็จให้ เนื่องจากยังไม่มีความพร้อมทางด้านนี้ หรือเพื่อประหยัดค่าใช้จ่าย

1) การพัฒนาระบบงานด้วยตนเอง สถาบันการเงินควรกำหนดมาตรฐานและวิธีการปฏิบัติงานเพื่อควบคุมดูแลให้การพัฒนาระบบงานเป็นไปตามแผนงานและบรรลุตรงตามวัตถุประสงค์ที่ต้องการ

มาตรฐานและวิธีการปฏิบัติงานที่ควรกำหนดเกี่ยวกับการพัฒนาระบบงานมีดังนี้

1.1) การศึกษาเบื้องต้นเกี่ยวกับความเป็นไปได้ทางเทคนิคและความคุ้มค่าของระบบงานเพื่อพิจารณาว่าสมควรดำเนินการพัฒนาในขั้นรายละเอียดต่อไปหรือไม่ (Feasibility study)

1.2) การวิเคราะห์และกำหนดลักษณะระบบงานที่ผู้ใช้งานต้องการ เพื่อจัดทำรายละเอียดระบบงาน และโปรแกรมต่อไป (System requirements)

1.3) การกำหนดรายละเอียดของระบบงานเพื่อจัดทำโปรแกรม คำสั่งงาน ทดสอบ และนำระบบงานออกใช้ (System design) รายละเอียดระบบงานที่ควรมี ได้แก่ ขอบเขตและวัตถุประสงค์ของระบบงาน (System objectives) ลักษณะของผลลัพธ์ที่ต้องการ (Output) ลักษณะของข้อมูลนำเข้า (Input) ลักษณะของแฟ้มข้อมูล (File layouts) ขั้นตอนการประมวลผล (System flowchart) คุณสมบัติของโปรแกรม (Program specifications) และลักษณะการควบคุมและความปลอดภัยภายในระบบงาน

1.4) การจัดทำโปรแกรมระบบงาน (Programming) สถาบันการเงินอาจใช้เทคนิคการเขียนโปรแกรมได้หลายแบบ แต่ในโปรแกรมควรมีคำสั่งงานที่เกี่ยวกับการเช็คสอบความครบถ้วนของจำนวนข้อมูล (Control totals techniques) การเช็คสอบความถูกต้องของข้อมูล (Data input editing) และการเช็คสอบความถูกต้องของแฟ้มข้อมูลที่ใช้ในการประมวลผล (File label checking)

1.5) การทดสอบโปรแกรมระบบงาน (System Testing) การทดสอบโปรแกรมเป็นขั้นตอนที่สำคัญในการพัฒนาระบบงาน เพื่อพิสูจน์ว่าการออกแบบและจัดทำโปรแกรมระบบงานถูกต้องตรงความต้องการของผู้ใช้ ก่อนที่จะนำไปติดตั้งใช้งานต่อไป การทดสอบอาจทำได้โดยการใช้ข้อมูลจำลอง (Test data) ทดสอบสถานการณ์ที่อาจนำไปสู่ความผิดพลาดได้ในทุกกรณี และผู้ที่เข้าร่วมการทดสอบควรประกอบด้วยบุคคล 3 ฝ่าย คือ ฝ่ายคอมพิวเตอร์ ฝ่ายผู้ใช้งาน และฝ่ายตรวจสอบภายใน

1.6) การนำระบบออกใช้งาน (System Implementation) การนำระบบงานที่พัฒนาเสร็จเรียบร้อยแล้วออกใช้งาน ควรมีการสอบทานเพื่อให้มั่นใจว่าอยู่ในสภาพที่พร้อมใช้งาน อาทิ เช่น จะต้องผ่านการทดสอบและยอมรับจากส่วนงานที่เกี่ยวข้อง มีเอกสารประกอบระบบงานและโปรแกรม และคู่มือปฏิบัติงานครบถ้วนและมีการจัดทำแผนฝึกอบรมพนักงาน ฝ่ายผู้ใช้งาน และฝ่ายคอมพิวเตอร์ เป็นต้น

1.7) การประเมินผลการปฏิบัติงาน (System evaluation) ภายหลังการปฏิบัติงานไปได้ระยะหนึ่ง ควรมีการประเมินผลการปฏิบัติงานระบบใหม่เกี่ยวกับการใช้งานได้ตามที่ออกแบบไว้ ค่าใช้จ่ายที่เกิดขึ้นจริงกับค่าใช้จ่ายตามประมาณการ และปัญหาในการปฏิบัติงาน

1.8) การปรับปรุงแก้ไขโปรแกรมระบบงาน (System maintenance) การปรับปรุงแก้ไขโปรแกรมระบบงานในช่วงระยะเวลาใดเวลาหนึ่ง อาจเป็นสิ่งที่มีความจำเป็น เนื่องจากปัญหาที่เกิดขึ้นในการปฏิบัติงาน ความต้องการใหม่ๆทางธุรกิจ การเปลี่ยนแปลงระเบียบปฏิบัติงาน กฎหมาย และข้อกำหนดของทางการ ทุกครั้งที่จะปรับปรุงแก้ไขโปรแกรมระบบงานควรกำหนดให้หน่วยงานผู้ใช้โปรแกรมระบบงานจัดทำหลักฐานใบคำขอ ระบุเหตุผลและความต้องการแก้ไข เสนอให้ฝ่ายคอมพิวเตอร์พิจารณาดำเนินการ และควรมีการควบคุมขั้นตอนการปฏิบัติงานอย่างเข้มงวดเช่นเดียวกับการพัฒนาระบบงานใหม่ เพื่อป้องกันความผิดพลาดและการกระทำการทุจริต

2) การว่าจ้างให้บุคคลภายนอกเป็นผู้พัฒนาหรือจัดซื้อโปรแกรมระบบงานสำเร็จ สถาบันการเงิน โดยเฉพาะสถาบันการเงินที่ใช้ระบบประมวลผลข้อมูลขนาดเล็ก ควรกำหนดมาตรฐานในการจัดหาโปรแกรมระบบงาน ดังนี้

2.1) กำหนดคุณสมบัติและลักษณะความต้องการเกี่ยวกับข้อมูลนำเข้า รายงานที่ได้รับ และการควบคุมความถูกต้องและความปลอดภัยของข้อมูล ของโปรแกรมระบบงาน

2.2) วิเคราะห์ผลประโยชน์ตอบแทนกับค่าใช้จ่ายในการว่าจ้าง หรือจัดซื้อโปรแกรมระบบงานภายนอก

2.3) วิเคราะห์ฐานะการเงิน ชื่อเสียง และความพร้อมทางเทคนิคของผู้ผลิตหรือผู้ขายที่จะให้การสนับสนุนในภายหลังหรือเมื่อมีปัญหา

2.4) วิเคราะห์ความเพียงพอและความสมบูรณ์ของเอกสารประกอบการใช้โปรแกรมระบบงาน อาทิ เช่น คำอธิบายลักษณะระบบงาน ลักษณะโปรแกรมระบบงาน ลักษณะแฟ้มข้อมูลและข้อมูล คู่มือสำหรับผู้ปฏิบัติการประมวลผล และคู่มือสำหรับผู้ใช้งาน เป็นต้น

2.5) วิเคราะห์แผนการให้การฝึกอบรมของผู้ผลิตหรือผู้ขาย

3.1.3 เอกสารสนับสนุนการปฏิบัติงานระบบประมวลผลข้อมูล (Documentation)

เอกสารสนับสนุนการปฏิบัติงานด้านคอมพิวเตอร์ เป็นเอกสารที่เกี่ยวกับมาตรฐาน วิธีการปฏิบัติงานในระบบประมวลผลข้อมูล องค์ประกอบของระบบงาน และโปรแกรม ซึ่งหากเอกสารเหล่านี้ได้รับการจัดทำอย่างถูกต้องและสมบูรณ์แล้ว จะเป็นประโยชน์อย่างยิ่งสำหรับผู้ปฏิบัติงาน ผู้ปรับปรุงแก้ไข และผู้มีหน้าที่ตรวจสอบทั้งภายในและภายนอก และนอกจากนั้นยังเป็นประโยชน์ต่อการเปลี่ยนระบบงาน การสับเปลี่ยนพนักงานและหน้าที่ปฏิบัติงาน และช่วยให้การประมวลผลข้อมูลดำเนินการต่อไปได้โดยไม่หยุดชะงัก กรณีที่มีพนักงานที่เป็นบุคคลสำคัญลาออกไป

1) เอกสารสนับสนุนการปฏิบัติงาน

เอกสารสนับสนุนโปรแกรมระบบงาน จัดว่าเป็นเอกสารที่สำคัญและจำเป็นที่สุดในระบบประมวลผลข้อมูล แต่เนื่องจากเป็นเอกสารที่ต้องใช้เวลามากในการจัดทำ และเป็นงานด้านที่ไม่สร้างสรรจึงมักถูกปล่อยปละละเลยอยู่เสมอ ดังนั้น ผู้บริหารสถาบันการเงินจึงควรมีบทบาทสำคัญในการกำหนดมาตรฐาน

เอกสารสนับสนุนการปฏิบัติงานด้านคอมพิวเตอร์ และควบคุมดูแลให้มีการจัดเอกสารตามมาตรฐานที่กำหนด เอกสารที่ควรจัดทำได้แก่

1.1) มาตรฐานและระเบียบปฏิบัติงานประมวลผลข้อมูล เป็นแนวปฏิบัติทั่ว ๆ ไป เกี่ยวกับการออกแบบระบบงาน การจัดทำโปรแกรมระบบงาน การใช้เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ การเตรียมข้อมูลและป้อนข้อมูลเข้าเครื่อง การประมวลผลข้อมูล การรวบรวมและตรวจสอบความถูกต้องของรายงานผลลัพธ์จากการประมวลผล

1.2) เอกสารสนับสนุนระบบงาน

ระบบงานที่ประมวลผลข้อมูลด้วยคอมพิวเตอร์ทุกระบบควรมีคู่มือใช้ประกอบการทำงาน เพื่อให้การประมวลผลข้อมูลเป็นไปด้วยความถูกต้องและลดปัญหาในการปฏิบัติงาน เอกสารที่ควรประกอบอยู่ในคู่มือระบบงาน ได้แก่

ก. รายละเอียดเกี่ยวกับระบบงาน (System Document) ซึ่งประกอบด้วย คำอธิบายลักษณะงาน (System narrative) ผังระบบงาน (System flowchart) ผังข้อมูล (Record layout) ลักษณะของแฟ้มข้อมูล (File description) ลักษณะของรายงาน (Print layout) การควบคุมที่มีอยู่ในระบบ (Control function) รหัสประเภทรายการ บัญชี และอื่น ๆ

ข. รายละเอียดเกี่ยวกับโปรแกรมระบบงาน (Program Documentation) ซึ่งประกอบด้วย คำอธิบายลักษณะของโปรแกรม (Program description) ผังขั้นตอนการทำงานของโปรแกรม (Program flowchart) สำเนาโปรแกรมชุดปัจจุบัน (Program listing) และการควบคุมที่มีอยู่ในโปรแกรม (Programmed controls)

ค. รายละเอียดวิธีการปฏิบัติสำหรับพนักงานเครื่องคอมพิวเตอร์ (Operation documentation) ซึ่งควรอธิบายถึงวัตถุประสงค์ของโปรแกรมระบบงาน แฟ้มข้อมูลที่ใช้ในการประมวลผล รูปแบบของข้อมูลนำเข้าและผลลัพธ์ (Input form & output formats) ชุดคำสั่งงานประมวลผล (Job command language) วิธีปฏิบัติเมื่อโปรแกรมทำงานผิดพลาดและเครื่องหยุดทำงานโดยกระทันหัน (Program error & halts) และวิธีปฏิบัติงานเมื่อเกิดกรณีฉุกเฉิน

ง. รายละเอียดวิธีการปฏิบัติงานสำหรับผู้ใช้ข้อมูล (User documentation) ซึ่งควรอธิบายถึงลักษณะของข้อมูลที่ต้องนำเข้าเครื่อง (Input) ลักษณะและจำนวนรายงานที่ได้จากการประมวลผล (Output) วิธีปฏิบัติในการควบคุมและการตรวจสอบความถูกต้องของข้อมูลนำเข้าและรายงาน และวิธีปฏิบัติเมื่อพบข้อผิดพลาด

2) การควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงาน

เนื่องจากเอกสารที่กล่าวเป็นเอกสารที่สำคัญและจำเป็นอย่างยิ่งต่อการประมวลผลข้อมูลสถาบันการเงิน จึงควรจัดให้มีสถานที่สำหรับเก็บโดยเฉพาะ โดยอาจเก็บรวมไว้ในที่เดียวกับแฟ้มข้อมูลและโปรแกรม และมีเจ้าหน้าที่บรรณารักษ์คอยควบคุมดูแลการเข้าออกสถานที่ การนำออกไปใช้งาน และการปรับปรุงเอกสารให้ถูกต้องและทันสมัยอยู่เสมอ และควรจัดทำสำเนาไว้อย่างน้อย 1 ชุด และเก็บรักษาไว้ในที่ปลอดภัยแยกจากสถานที่ทำการ เพื่อว่าเมื่อเกิดกรณีฉุกเฉินจะสามารถนำมาใช้ในการปฏิบัติงานทดแทนชุดใช้ปฏิบัติงานจริงที่ถูกทำลายเสียหาย

ในกรณีที่สถาบันการเงินมีการจัดหาโปรแกรมระบบงานจากภายนอก หรือระบบประมวลผลข้อมูลขนาดเล็ก ควรกำหนดให้ผู้ผลิตหรือผู้ขายส่งมอบเอกสารประกอบระบบงานให้เป็นไปตามมาตรฐานที่กำหนดด้วยเช่นเดียวกัน

3.1.4 การปฏิบัติการประมวลผล (Computer Operation)

ฝ่ายปฏิบัติการประมวลผลโดยทั่วไป มีหน้าที่ในการประมวลข้อมูลและควบคุมดูแลแฟ้มข้อมูล โปรแกรมและเครื่องคอมพิวเตอร์ ให้อยู่ในสภาพที่ปลอดภัยและพร้อมที่จะใช้งานได้ตลอดเวลา พนักงานปฏิบัติการประมวลผลจึงควรได้รับมอบหมายให้รับผิดชอบเฉพาะงานที่เกี่ยวกับการใช้เครื่องคอมพิวเตอร์เท่านั้น มิควรให้ปฏิบัติหน้าที่อื่น เช่น การเตรียมข้อมูลนำเข้า การจัดทำโปรแกรม และการตรวจสอบข้อมูลที่ได้จากการประมวลผล เป็นต้น

ในการปฏิบัติการประมวลผล คู่มือสนับสนุนการปฏิบัติงานที่สมบูรณ์ และได้รับการปรับปรุงแก้ไขให้ทันเวลาอยู่เสมอ จะช่วยให้เจ้าหน้าที่ปฏิบัติงานได้อย่างมีประสิทธิภาพ และป้องกันความผิดพลาดที่อาจเกิดขึ้น นอกจากนี้สถาบันการเงินควรกำหนดระเบียบปฏิบัติทั่วไปเกี่ยวกับการใช้เครื่อง ดังนี้

1) การรักษาความสะอาดเรียบร้อยภายในสถานที่ทำงาน ซึ่งได้แก่ ห้องเครื่อง หรือบริเวณตั้งเครื่องและพื้นที่ใกล้เคียง เพื่อป้องกันฝุ่นละอองและการเกิดเพลิงไหม้ อันอาจสร้างความเสียหายต่อเครื่องคอมพิวเตอร์

2) การบำรุงรักษาเครื่องคอมพิวเตอร์ ควรกำหนดให้พนักงานทำความสะอาดเครื่องคอมพิวเตอร์ตามกำหนดเวลา และวิธีการที่บริษัทผู้ผลิตคอมพิวเตอร์กำหนด และให้บริษัทผู้ให้เช่าหรือผู้ขายเครื่องคอมพิวเตอร์ตรวจสอบและซ่อมแซมตามระยะเวลาที่ได้ตกลงกัน เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์เสื่อมสภาพเร็วกว่าเวลาอันสมควร

3) การแบ่งแยกและสับเปลี่ยนหน้าที่ เนื่องจากการแบ่งแยกหน้าที่เป็นหลักการที่สำคัญของการควบคุมภายใน สถาบันการเงินจึงควรแบ่งแยกหน้าที่ในการปฏิบัติงานประมวลผลข้อมูล เพื่อมิให้พนักงานผู้หนึ่งผู้ใดปฏิบัติงานหลายอย่าง อาทิเช่น การจัดเตรียมรายการเข้าเครื่อง การป้อนข้อมูลเข้าเครื่อง การใช้งานเครื่องประมวลข้อมูล และการตรวจสอบความถูกต้องของข้อมูล ผลลัพธ์และรายงาน เป็นต้น อันอาจทำให้เกิดการทุจริตและความผิดพลาดได้ง่าย และทั้งยังเป็นการสร้างระบบการสอบยันความถูกต้องในการปฏิบัติงาน ในหน่วยงานประมวลผลข้อมูลขนาดเล็ก ซึ่งมีพนักงานปฏิบัติการประมวลผลจำนวนจำกัด ไม่สามารถแบ่งแยกหน้าที่ได้อย่างสมบูรณ์ และจำเป็นต้องมอบหมายให้พนักงานปฏิบัติมากกว่า 1 อย่าง ควรกำหนดให้มีการหมุนเวียนสับเปลี่ยนหน้าที่ และติดตามดูแลการปฏิบัติงานอย่างใกล้ชิด อย่างไรก็ตามไม่ควรยินยอมให้พนักงานที่นำข้อมูลเข้าเครื่องเป็นผู้ตรวจสอบและกระทบยอดรายงานที่ได้จากการประมวลผลข้อมูลหรือข้อมูลผลลัพธ์

4) การควบคุมการใช้เครื่องคอมพิวเตอร์ประมวลผล ควรกำหนดให้พนักงานถือปฏิบัติในการใช้เครื่องให้เป็นไปตามคู่มือของบริษัทผู้ผลิต คู่มือระบบงาน และตารางปฏิบัติงานโดยเคร่งครัด โดยมีพนักงานปฏิบัติการระดับหัวหน้างานเป็นผู้ควบคุมดูแล และจัดทำรายงานเสนอฝ่ายบริหารเมื่อมีเหตุการณ์ที่ผิดปกติ หรือเมื่อเกิดความเสียหาย ในระบบของเครื่องคอมพิวเตอร์ขนาดใหญ่โดยทั่วไป จะมีเครื่องมือควบคุมการสั่งงานเครื่องคอมพิวเตอร์ เช่น Console printer CPU-clock และ Activity logs เป็นต้น ซึ่งจะบันทึกการสั่งงานเครื่องและเวลาที่ใช้ในการปฏิบัติงาน เพื่อให้ผู้บริหาร ผู้ควบคุมงานและผู้ตรวจสอบ สามารถตรวจสอบความถูกต้องได้ในภายหลัง

5) การจัดทำตารางปฏิบัติงานประมวลผล สถาบันการเงินควรจัดทำตารางกำหนดการใช้เครื่องประมวลผลข้อมูลประจำวัน ประจำสัปดาห์ และประจำเดือน ซึ่งอาจจัดทำด้วยมือหรือใช้เครื่องคอมพิวเตอร์ก็ได้ ตารางปฏิบัติงานเครื่องคอมพิวเตอร์จะช่วยควบคุมให้การใช้เครื่องเป็นไปด้วยความมีประสิทธิภาพและงานเสร็จทันเวลาที่กำหนด

6) การควบคุมการปฏิบัติงานของพนักงานประมวลผลข้อมูล เนื่องจากพนักงานที่มีหน้าที่ประมวลผลสามารถใช้เครื่องคอมพิวเตอร์ในการเรียกใช้โปรแกรม และแฟ้มข้อมูลในการประมวลผลได้อย่างกว้างขวางถ้าสิ่งแวดล้อมเอื้ออำนวย จึงควรกำหนดขอบเขตการปฏิบัติงานของพนักงานประมวลผล มิให้ปฏิบัติงานที่อาจเกิดความเสียหายต่อเครื่องคอมพิวเตอร์ โปรแกรมและข้อมูล เช่น ไม่ควรยินยอมให้เข้าไปยุ่งเกี่ยวกับ Source programs หรือ Program listing และเอกสารอื่นที่ไม่เกี่ยวกับการใช้เครื่อง ไม่ควรยินยอมให้ใช้ Utility programs ที่มีคุณสมบัติในการแก้ไขข้อมูลและโปรแกรมระบบงานได้โดยตรง และไม่ควรยินยอมให้ทำหน้าที่ตรวจสอบความถูกต้องของยอดรวมข้อมูล

7) การควบคุมการใช้แฟ้มข้อมูล โปรแกรม และคู่มือปฏิบัติงาน เพื่อป้องกันการใช้แฟ้มข้อมูลโปรแกรม และคู่มือปฏิบัติงาน โดยไม่ได้รับอนุญาต หรือไม่ให้สูญหายควรมีการควบคุมการจัดเก็บ ดังนี้

7.1) สำหรับแฟ้มข้อมูลและโปรแกรมที่บรรจุอยู่ในม้วนเทปหรือจานแม่เหล็ก และเอกสารคู่มือปฏิบัติงาน ควรแยกเก็บไว้ในสถานที่ซึ่งปลอดภัย และมีการควบคุมการนำออกไปใช้

7.2) สำหรับแฟ้มข้อมูลและโปรแกรมที่เก็บอยู่ในเครื่องคอมพิวเตอร์ควรใช้โปรแกรมพิเศษควบคุมการใช้งาน เช่น RACF, TOP SECRET, LIBRARIAN, SECURE และ PANVALET เป็นต้น หน้าที่หลักของโปรแกรมเหล่านี้ คือ การกำหนดลำดับชั้นการเข้าถึงข้อมูลและโปรแกรมที่อยู่ในเครื่องตามอำนาจหน้าที่ของผู้ปฏิบัติงาน และจัดพิมพ์รายงานการใช้งานเพื่อให้สามารถตรวจสอบความถูกต้องได้

3.1.5 การประมวลผลโดยอาศัยระบบสื่อสาร

ความต้องการทางธุรกิจและความก้าวหน้าทางเทคโนโลยี เป็นเหตุให้มีการนำระบบสื่อสารข้อมูล เช่น การสื่อสารทางสายโทรศัพท์ การสื่อสารไมโครเวฟ และการสื่อสารดาวเทียม เป็นต้น มาใช้ร่วมกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ เพื่อเพิ่มศักยภาพในการใช้งาน ทำให้สามารถสั่งงานเครื่องหรือนำข้อมูลเข้าเครื่องได้จากที่ไกล ๆ รวมทั้งสามารถเชื่อมโยงกับเครื่องคอมพิวเตอร์อื่น เพื่อแลกเปลี่ยนข้อมูลระหว่างกันโดยผ่านระบบสื่อสารที่กล่าว

ลักษณะการประมวลผลที่อาศัยระบบสื่อสารโดยทั่วไป ได้แก่

1) ระบบประมวลผลแบบออนไลน์ (Online System) เป็นระบบการประมวลผลที่ใช้เครื่องเทอร์มินัล (Terminal) เชื่อมต่อกับเครื่องคอมพิวเตอร์หลัก เพื่อทำหน้าที่นำข้อมูลเข้าเครื่อง เรียกข้อมูลจากเครื่องคอมพิวเตอร์ และสั่งงานประมวลผลข้อมูลได้จากที่ไกล ๆ

2) ระบบประมวลผลแบบกระจายศูนย์ (Distributed Processing System) เป็นระบบประมวลผลแบบแยกตามหน่วยงานหรือสาขา แทนที่จะใช้ระบบประมวลผลร่วมกัน (Centralized Processing System) ซึ่งหากระบบประมวลผลกลางขัดข้องหรือเสียหายจนใช้การไม่ได้เป็นเวลานาน ก็จะพลอยทำให้หน่วยงานอื่นหรือสาขาไม่สามารถใช้และสั่งงานประมวลผลข้อมูลของตนเองได้ ระบบประมวลผลแบบกระจายศูนย์ประกอบด้วย

คอมพิวเตอร์หลาย ๆ เครื่อง แต่จะมีเครื่องขนาดใหญ่ทำหน้าที่ประมวลผลข้อมูลกลาง และเครื่องเล็ก ๆ ทำหน้าที่ประมวลผลข้อมูลตามหน่วยงานหรือสาขา แต่ถึงแม้จะประมวลผลข้อมูลโดยอิสระจากกัน เครื่องคอมพิวเตอร์ทุกเครื่องก็ติดต่อกันด้วยระบบสื่อสารเพื่อให้สามารถแลกเปลี่ยนข้อมูลระหว่างกัน และสามารถติดต่อกับคอมพิวเตอร์เครื่องใหญ่ได้เมื่อจำเป็น

การนำระบบสื่อสารมาใช้กับคอมพิวเตอร์ อาจก่อให้เกิดความเสี่ยงเพิ่มขึ้นต่อความถูกต้องและความปลอดภัยของข้อมูล ทั้งที่อยู่ในเครื่องคอมพิวเตอร์ และขณะที่อยู่ระหว่างการสื่อสาร ดังนั้นจึงควรมีการควบคุมเพื่อป้องกันมิให้ข้อมูลผิดพลาด ถูกบิดเบือน หรือนำไปใช้ในทางทุจริต สถาบันการเงินที่มีการนำระบบสื่อสารมาใช้งานประมวลผลข้อมูล ควรจัดให้มีการควบคุม ดังนี้

1) การควบคุมความปลอดภัยเครื่องเทอร์มินัล (Terminal security) เนื่องจากเทอร์มินัลเป็นเครื่องมือสำคัญที่ใช้สื่อสารกับเครื่องคอมพิวเตอร์เพื่อนำข้อมูลเข้าเครื่อง ดึงข้อมูลจากเครื่อง และสั่งให้เครื่องประมวลผลข้อมูล การรักษาความปลอดภัยเครื่องเทอร์มินัลควรทำทั้งที่ตัวเครื่องฯ และการใช้โปรแกรมควบคุมการใช้เครื่อง (Physical restrictions & System controls) เพื่อป้องกันมิให้ผู้ที่ไม่มีสิทธิและบุคคลภายนอกเข้าไปใช้ได้ และจำกัดสิทธิของผู้ใช้เครื่องฯ ให้อยู่ภายในขอบเขตที่ได้รับมอบหมาย

2) การควบคุมการรับส่งข้อมูล (Transmission controls)

จุดอ่อนของการสื่อสารข้อมูลทางโทรศัพท์ ดาวเทียม และไมโครเวฟ อยู่ที่การถูกลักลอบแก้ไขข้อมูลหรือนำข้อมูลไปใช้ประโยชน์ส่วนตัว ซึ่งอาจกระทำได้หลายวิธี เช่น ใช้เครื่องมือดักฟังข้อมูลจากสายสื่อสารระหว่างเทอร์มินัลและคอมพิวเตอร์ หรือใช้เทอร์มินัลส่วนตัวเชื่อมต่อกับสายสื่อสารเพื่อดักข้อมูลที่ส่งมาตามสาย แก้ไขหรือแทนที่ด้วยข้อมูลอื่นแล้วส่งกลับไปยังเครื่องคอมพิวเตอร์ เป็นต้น การป้องกันมิให้ข้อมูลผิดพลาดหรือคลาดเคลื่อนจากสาเหตุที่กล่าวอาจทำได้ ดังนี้

2.1) การควบคุมเอกสารที่เกี่ยวกับระบบสื่อสาร และผังแสดงที่ตั้งเครื่องมือสื่อสารและสายสื่อสาร มิให้ผู้ที่ไม่มีหน้าที่เกี่ยวข้องนำไปใช้งานได้ และไม่ควรให้สายโทรศัพท์ที่ใช้งานระบบออนไลน์ปรากฏแก่สายตาบุคคลทั่วไป หรือมีเครื่องหมายพิเศษ

2.2) ควรแปลงรหัสประจำตัวผู้มีสิทธิเข้าถึงข้อมูล และตัวข้อมูลสำคัญในระบบให้อยู่ในรูปแบบ ซึ่งหากมีการรั่วไหลไปถึงมือบุคคลภายนอกแล้วไม่สามารถนำไปใช้ประโยชน์ได้

2.3) ควรมีการพิสูจน์ความถูกต้องของแหล่งที่มาของข้อมูลนำเข้า เพื่อให้มั่นใจได้ว่าข้อมูลที่ได้รับนั้นถูกต้อง เช่น เติมรหัสต่อท้ายข้อมูล ในทำนองเดียวกับรหัสการโอนเงินทางอิเล็กทรอนิกส์ เป็นต้น

2.4) ควรมีการให้ลำดับเลขหมายกำกับข้อมูล วันที่และเวลาที่ได้รับข้อมูลแต่ละรายการจากเทอร์มินัลแต่ละเครื่อง เพื่อให้สามารถตรวจสอบการสูญหายหรือการซ้ำซ้อนของข้อมูลในระบบสื่อสารได้โดยใช้บุคคลหรือโปรแกรมตรวจสอบ

2.5) ควรกำหนดให้ระบบคอมพิวเตอร์สามารถหยุดการติดต่อกับเทอร์มินัลได้โดยอัตโนมัติ ในกรณีที่เทอร์มินัลเครื่องหนึ่งเครื่องใดขาดการติดต่อกับระบบคอมพิวเตอร์เป็นระยะเวลานาน เพื่อป้องกันมิให้บุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้องสวมรอยเข้าใช้งาน

2.6) ควรมีการควบคุมการใช้เครื่องเทอร์มินัลให้อยู่ภายในกำหนดเวลา หากมีการใช้นอกเหนือเวลาที่กำหนด ต้องได้รับการอนุมัติจากผู้บังคับบัญชา

3) การเตรียมการเมื่อระบบสื่อสารขัดข้อง

ความสำคัญของระบบงานที่ประมวลผลข้อมูลโดยอาศัยระบบสื่อสาร เช่น การซื้อขายหลักทรัพย์ด้วยระบบคอมพิวเตอร์ เป็นต้น เป็นปัจจัยที่กำหนดว่าสถาบันการเงินควรเตรียมการอย่างไร เมื่อระบบการรับส่งข้อมูลทางสายโทรศัพท์ หรือระบบสื่อสารอื่นขัดข้องจนไม่สามารถใช้งานได้เป็นระยะเวลานาน ในกรณีที่ใช้ระบบสื่อสารข้อมูลทางโทรศัพท์ สถาบันการเงินควรพิจารณากำหนดอุปกรณ์สื่อสารและคู่สายโทรศัพท์สำรองไว้ใช้งานในกรณีฉุกเฉิน วิธีปฏิบัติในการใช้ระบบสื่อสารชุดสำรอง และควรมีการทดสอบเป็นครั้งคราว เพื่อให้แน่ใจว่าสามารถปฏิบัติเมื่อเกิดกรณีฉุกเฉิน

ในกรณีของระบบประมวลผลข้อมูลขนาดเล็ก หรือการประมวลผลแบบออนไลน์ภายในสำนักงานหรืออาคารเดียวกัน การควบคุมความปลอดภัยเครื่องเทอร์มินัลเป็นสิ่งที่สำคัญที่สุด เพื่อป้องกันมิให้ผู้ที่ไม่มีสิทธิเข้าไปถึงโปรแกรมงานและแฟ้มข้อมูลภายในเครื่องคอมพิวเตอร์ได้ และจำกัดสิทธิของผู้ใช้เครื่องให้อยู่ภายในขอบเขตที่ได้รับมอบหมาย โปรแกรมระบบเครื่อง (Operating System) โดยทั่วไปมีคุณสมบัติที่สถาบันการเงินสามารถใช้ในการควบคุมดังกล่าวได้ และมีหลายระบบที่สามารถบันทึกผลการใช้งานเครื่องเทอร์มินัลแต่ละเครื่อง (Activity log) เพื่อให้ผู้บริหารและผู้ควบคุมงานตรวจสอบรายการที่ผิดปกติได้เช่นกัน

3.1.6 การควบคุมความถูกต้องและน่าเชื่อถือของข้อมูล (Data integrity)

ความถูกต้องและความน่าเชื่อถือของข้อมูลในระบบที่ประมวลผลด้วยเครื่องคอมพิวเตอร์ ขึ้นอยู่กับกระบวนการควบคุมที่เหมาะสม เริ่มตั้งแต่จุดที่ข้อมูลเกิดขึ้น การเตรียมข้อมูลให้อยู่ในสภาพที่เครื่องอ่านได้ การนำข้อมูลเข้าเครื่อง การประมวลผลข้อมูล และการออกผลลัพธ์หรือรายงาน ซึ่งอาจจะเป็นการควบคุมที่ปฏิบัติโดยบุคคล โดยโปรแกรมระบบงาน หรือทั้งสองอย่างรวมกัน สถาบันการเงินจึงควรจัดให้มีการควบคุมเพื่อให้ข้อมูลถูกต้องและน่าเชื่อถือได้ ดังนี้

1) การควบคุมการนำข้อมูลเข้าเครื่อง (Data entry controls)

ปัจจุบันการนำข้อมูลเข้าเครื่องคอมพิวเตอร์ส่วนใหญ่กระทำโดยใช้เครื่องเทอร์มินัล(On-line entry) สถาบันการเงินจึงควรมีการควบคุมเพื่อให้แน่ใจได้ว่าข้อมูลรายวันที่เกิดขึ้นทั้งหมดเข้าไปในเครื่องคอมพิวเตอร์จนครบถ้วนและถูกต้องทุกรายการ การควบคุมความครบถ้วนและถูกต้องของข้อมูลอาจทำได้ ดังนี้

1.1) ควรมีการสะสมยอดรวมจำนวนข้อมูลทั้งหมดก่อนหน้าและหลังจากการป้อนรายการเข้าเครื่องเทอร์มินัล และเมื่อข้อมูลเข้าไปในคอมพิวเตอร์แล้ว (batch total) เพื่อใช้ในการสอบทานความครบถ้วนของข้อมูล

1.2) ควรมีการตรวจเช็คความถูกต้องของข้อมูลแต่ละรายการในขณะที่ทำการป้อนข้อมูล (Data entry validation) ก่อนหน้าที่ข้อมูลจะเข้าไปในคอมพิวเตอร์ เช่น การตรวจเช็ครหัสรายการ การตรวจเช็คลำดับของรายการ การตรวจเช็คจำนวนเงินที่มากเกินกำหนด และการตรวจเช็คเลขที่บัญชีเจ้าของรายการ เป็นต้น เพื่อป้องกันมิให้ข้อมูลที่ผิดพลาดหรือแปลกปลอมเข้าไปในคอมพิวเตอร์ ซึ่งหากปล่อยให้เข้าไปแล้วอาจทำให้ยากต่อการค้นหาและแก้ไขในภายหลัง

1.3) ควรมีรายงานคอมพิวเตอร์แสดงรายละเอียดข้อมูลทุกรายการที่เข้าไปในเครื่องคอมพิวเตอร์ เพื่อใช้ในการเช็คสอบความถูกต้องกับเอกสารหลักฐานเบื้องต้นที่ใช้ในการบันทึกรายการ เช่นเดียวกับการบันทึกรายการในสมุดรายวันทั่วไป (Transaction journals)

2) การควบคุมการออกข้อมูลผลลัพธ์และรายงาน (Output Controls)

2.1) ควรมีการสอบทานความเรียบร้อยและความถูกต้องของข้อมูล ผลลัพธ์ และรายงาน (Review and reconcilement of output) โดยการตรวจสอบและกระทบยอดรวมกับยอดรวมของข้อมูลที่นำเข้าเครื่องเทอร์มินัล ยอดรวมข้อมูลที่นำเข้าคอมพิวเตอร์ ยอดรวมในบัญชีแยกประเภททั่วไป และยอดคงเหลือในงบทดลอง เพื่อพิสูจน์ความถูกต้องของข้อมูล ผลลัพธ์ และรายงาน

2.2) ควรมีการควบคุมการจัดส่งข้อมูลผลลัพธ์ และรายงาน (Distribution Control) ให้ถึงมือผู้ใช้อย่างถูกต้องและครบถ้วน โดยจัดทำทะเบียนบันทึกรายงานที่ได้รับจากการประมวลผลรายวัน รายสัปดาห์ และรายเดือน ผู้รับหรือผู้ใช้รายงาน ลายมือชื่อ และวันที่ที่รับรายงาน เพื่อป้องกันมิให้เกิดการสูญหายหรือถูกนำไปใช้ในทางทุจริต

3) การควบคุมอุปกรณ์ที่ใช้บันทึกข้อมูล (Data file media controls)

อุปกรณ์ที่บันทึกข้อมูลคอมพิวเตอร์ ซึ่งได้แก่ จานแม่เหล็กและแถบแม่เหล็ก (Disk และ Tape) อาจเสียหายหรือถูกทำลายได้ง่ายกว่าข้อมูลที่อยู่บนแผ่นกระดาษ จึงต้องมีการควบคุมดูแลอุปกรณ์ที่กล่าวในขณะที่ยังไม่ได้นำไปใช้งานประมวลผลอย่างรัดกุม เพื่อป้องกันมิให้เกิดความเสียหาย ดังนี้

3.1) ควรเก็บรักษาอุปกรณ์บันทึกข้อมูลขณะที่ไม่ได้นำไปใช้งานประมวลผลไว้ในสถานที่ปลอดภัย มีการควบคุมอุณหภูมิ ความชื้น ฝุ่นละออง การป้องกันเพลิงไหม้ อุปกรณ์ดับเพลิง และจัดให้มีเจ้าหน้าที่เฉพาะควบคุมดูแลการนำออกไปใช้งาน และมีการตรวจนับจำนวนคงเหลือเป็นครั้งคราว

3.2) ควรจัดทำป้ายชื่อติดกำกับภายนอกอุปกรณ์บันทึกข้อมูล ภายในบริเวณหัวและท้ายแฟ้มข้อมูลควรบันทึกข้อมูลเกี่ยวกับชื่อแฟ้มข้อมูลวันที่และจำนวนรายการข้อมูลทั้งหมดที่บรรจุอยู่ในแฟ้มข้อมูลนั้น

3.3) ควรมีอุปกรณ์บันทึกข้อมูลชุดสำเนา (Back-up file) แยกเก็บไว้ในที่ที่ปลอดภัยห่างจากอาคารที่ทำการประมวลผลข้อมูล

3.1.7 การรักษาความปลอดภัย (Physical Security)

สถาบันการเงินควรมีมาตรการรักษาความปลอดภัย เพื่อคุ้มครองป้องกันความเสียหายที่จะเกิดกับเครื่องคอมพิวเตอร์ โปรแกรม และข้อมูล จากเหตุการณ์ที่เกิดขึ้นโดยไม่คาดฝัน หรือโดยการกระทำอย่างจงใจของบุคคลภายในและภายนอกบริษัท ทั้งนี้เพื่อมิให้การประมวลผลข้อมูลหยุดชะงัก ดังนี้

1) แผนรักษาความปลอดภัย แผนรักษาความปลอดภัยโดยทั่วไปควรประกอบด้วย การป้องกันความเสียหายที่จะมีต่อเครื่องคอมพิวเตอร์ โปรแกรม ข้อมูล และพนักงานปฏิบัติการคอมพิวเตอร์ แต่ถึงจะมีการป้องกันอย่างดีก็อาจเกิดเหตุการณ์ที่ไม่คาดคิดขึ้นได้ ในแผนฯ จึงควรกำหนดการปฏิบัติงานขณะที่ความเสียหายเกิดขึ้น และการปฏิบัติการเพื่อย้ายการประมวลผลข้อมูลไป ณ ที่แห่งใหม่ที่ได้จัดเตรียมไว้

2) การป้องกันความเสียหายจากภัยพิบัติและสาเหตุอื่นๆ

ภัยที่จะก่อให้เกิดความเสียหายต่อการประมวลผลข้อมูลด้วยคอมพิวเตอร์โดยทั่วไป ได้แก่ อุทกภัย อัคคีภัย การก่อวินาศกรรม กระแสไฟฟ้าดับหรือแรงดันตก การโจรกรรม และเครื่องคอมพิวเตอร์ขัดข้องใช้การไม่ได้เป็นเวลานาน สถาบันการเงินจึงควรกำหนดมาตรการป้องกันความเสียหายจากสาเหตุที่กล่าว ดังนี้

2.1) การเลือกสถานที่ตั้งเครื่องคอมพิวเตอร์ควรพิจารณาถึงสภาพแวดล้อมที่ปลอดภัย เช่น ไม่ควรอยู่ในบริเวณที่อาจเกิดเพลิงไหม้ได้ง่าย น้ำท่วมถึง บริเวณที่มีคนพลุกพล่าน และบริเวณที่อาจถูกคลื่นแม่เหล็กรบกวน เป็นต้น ภายในอาคารที่ตั้งฯควรจัดให้มียามรักษาการทางเข้า และติดตั้งเครื่องมือป้องกันการโจรกรรมและการบุกรุกในยามวิกาล ประตูทางเข้าและหน้าต่างควรปิดสนิทตลอดเวลา

2.2) ภายในห้องหรือบริเวณที่ตั้งเครื่องคอมพิวเตอร์ควรมีอุปกรณ์ดับเพลิงอยู่ในที่ที่เห็นได้ชัดเจน มีอุปกรณ์ตรวจวัดความร้อนและควันไฟเพื่อเตือนก่อนเกิดเพลิงไหม้ มีอุปกรณ์ควบคุมอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมตามที่บริษัทผู้ผลิตเครื่องคอมพิวเตอร์กำหนด ซึ่งระบบคอมพิวเตอร์ขนาดเล็กอาจไม่มีความจำเป็นในเรื่องนี้ มีเครื่องวัดและปรับแรงดันกระแสไฟฟ้าให้คงที่ และมีเครื่องกำเนิดไฟฟ้าสำรองไว้ใช้งานเมื่อไฟฟ้าของทางราชการดับกระทันหัน เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์ โปรแกรม และข้อมูลที่อยู่ในเครื่องเสียหายหรือทำงานผิดปกติ

2.3) ไม่ควรแสดงสถานที่ตั้งเครื่องคอมพิวเตอร์ให้ปรากฏแก่บุคคลทั่วไป เช่น ป้ายชื่อหรือสัญญลักษณ์ที่ระบุว่าเป็นศูนย์ ฝ่าย หรือส่วนงานปฏิบัติการประมวลผล เป็นต้น

2.4) ไม่ควรให้บุคคลอื่น เว้นแต่พนักงานปฏิบัติการประมวลผลอยู่ในห้องหรือบริเวณที่ตั้งเครื่องคอมพิวเตอร์ กรณีมีผู้มาเยี่ยมเยียนหรือดูงานเป็นครั้งคราว ควรจัดทำทะเบียนบันทึกการเข้า-ออกไว้เป็นหลักฐานในการตรวจสอบ

2.5) ตู้นิรภัยและห้องมั่นคงที่ใช้ในการเก็บรักษาแฟ้มข้อมูล และโปรแกรมที่บรรจุอยู่ในม้วนเทปหรือจานแม่เหล็ก และเอกสารคู่มือปฏิบัติงาน ควรเป็นชนิดที่สามารถป้องกันไฟและการโจรกรรมได้

3) การจัดเตรียมระบบประมวลผลสำรอง

ถึงแม้จะมีการรักษาความปลอดภัยที่เข้มงวดเพียงใดก็ตาม บางครั้งอาจเกิดเหตุการณ์ที่ไม่คาดคิด และส่งผลเสียหายต่อระบบคอมพิวเตอร์จนไม่สามารถประมวลผลข้อมูลต่อไปได้ ดังนั้นสถาบันการเงินจึงควรจัดเตรียมระบบประมวลผลสำรองไว้ปฏิบัติในยามฉุกเฉิน ระบบประมวลผลสำรองของสถาบันการเงินที่ประมวลผลข้อมูลด้วยคอมพิวเตอร์ขนาดเล็ก อาจจะเป็นระบบที่ปฏิบัติงานโดยบุคคล (Manual system) หรือระบบคอมพิวเตอร์ (Computer system) ก็ได้ ขึ้นอยู่กับความจำเป็นทางธุรกิจ และความสามารถของสถาบันการเงินแต่ละราย กรณีเลือกระบบประมวลผลสำรองซึ่งปฏิบัติโดยบุคคล สถาบันการเงินควรฝึกฝนพนักงานให้สามารถปฏิบัติงานตามแบบเดิมได้ และควรมีการทดสอบการปฏิบัติงานอย่างสม่ำเสมอ

3.1) ระบบประมวลผลด้วยคอมพิวเตอร์สำรอง ควรประกอบด้วยเครื่องคอมพิวเตอร์ โปรแกรม และแฟ้มข้อมูลที่เตรียมไว้อีกอย่างน้อย 1 ชุด สำหรับปฏิบัติในกรณีฉุกเฉิน ในการจัดหาเครื่องคอมพิวเตอร์สำรอง สถาบันการเงินอาจทำข้อตกลงกับสถาบันการเงินอื่นที่มีเครื่องคอมพิวเตอร์ที่สามารถใช้ร่วมกันได้ หรือกับบริษัทผู้ผลิตหรือผู้ขาย เพื่อขอใช้เครื่องในกรณีฉุกเฉิน และควรมีการทดสอบการปฏิบัติงานระบบประมวลผลสำรองเป็นครั้งคราว เพื่อให้มั่นใจว่าไม่มีเหตุขัดข้องเมื่อปฏิบัติงานจริง

3.2) โปรแกรมและเอกสารสนับสนุนการปฏิบัติงานประมวลผลควรมีชุดสำเนาเก็บไว้อย่างปลอดภัยนอกสถานที่ทำการ เพื่อป้องกันมิให้เสียหายไปพร้อมกับชุดที่ใช้งานประจำ

3.3) แฟ้มข้อมูลชุดสำรอง ควรมีให้เพียงพอสำหรับการสร้างข้อมูลให้เป็นปัจจุบัน กรณีแฟ้มข้อมูลปัจจุบัน (current master file) ที่อยู่ในเครื่องเสียหายหรือถูกทำลายจนใช้การไม่ได้ และควรเก็บรักษาไว้นอกสถานที่ทำการเช่นเดียวกับโปรแกรมและเอกสารสนับสนุนการปฏิบัติงาน

4) การประกันภัย

การรักษาความปลอดภัยแต่ประการเดียว อาจไม่สามารถป้องกันความเสียหายได้ทั้งหมด สถาบันการเงินจึงควรจัดให้มีการประกันภัยเพื่อคุ้มครองความเสียหายที่อาจเกิดขึ้น โดยเฉพาะความเสียหายที่มีมูลค่าจำนวนเงินสูง อาทิ เช่น เครื่องคอมพิวเตอร์และอุปกรณ์ที่จำเป็นในการประมวลผลข้อมูล และค่าใช้จ่ายพิเศษที่เกิดจากการประมวลผลข้อมูลด้วยคอมพิวเตอร์สำรอง เป็นต้น

3.1.8 การตรวจสอบงานคอมพิวเตอร์

เพื่อให้การบริหารและควบคุมการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ที่กล่าว บรรลุตามวัตถุประสงค์ที่กำหนด สถาบันการเงินควรจัดให้มีการตรวจสอบการปฏิบัติงานด้านคอมพิวเตอร์ของบริษัท เพื่อให้มั่นใจว่าการปฏิบัติงานประมวลผลข้อมูลเป็นไปตามนโยบายมาตรฐานและระเบียบปฏิบัติงานที่บริษัทกำหนด เครื่องคอมพิวเตอร์ โปรแกรม และแฟ้มข้อมูลได้รับการปฏิบัติอย่างถูกต้องและปลอดภัย ข้อมูลผลลัพธ์และรายงานที่ได้จากการประมวลผลมีความถูกต้อง เชื่อถือได้

1) ควรมอบหมายให้ผู้ตรวจสอบภายใน หรือว่าจ้างให้ผู้สอบบัญชีภายนอก หรือร่วมกันตรวจสอบการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของบริษัท และให้รายงานผลการตรวจสอบโดยตรงต่อคณะกรรมการบริษัท เพื่อให้มีความเป็นอิสระในการปฏิบัติงาน

2) ควรกำหนดบทบาท มาตรฐาน และวิธีการปฏิบัติงานตรวจสอบด้านคอมพิวเตอร์โดยละเอียดไว้ในคู่มือการตรวจสอบ เพื่อให้ผู้ตรวจสอบภายในถือปฏิบัติ และเพื่อใช้ประโยชน์ในการฝึกอบรมพนักงานใหม่

3) การตรวจสอบด้านคอมพิวเตอร์ ควรมีขอบเขตการตรวจสอบที่ครอบคลุมถึงการพัฒนาระบบงานและโปรแกรม (System development & programming) การปฏิบัติงานประมวลผลข้อมูล (Computer operations) การรักษาความปลอดภัย การนำข้อมูลเข้า (Data entry) และการสอบทานความถูกต้องของข้อมูลผลลัพธ์ และรายงานที่ได้จากการประมวลผล (Data output & report)

4) การปฏิบัติงานตรวจสอบในแต่ละเรื่อง ควรมีขั้นตอนการตรวจสอบอย่างน้อย 3 ขั้นตอน คือ

4.1) การสอบทานและวิเคราะห์ความเพียงพอเบื้องต้นของการควบคุมภายใน

4.2) การทดสอบการปฏิบัติงานเพื่อประเมินประสิทธิภาพของการควบคุม

4.3) การทดสอบความถูกต้องของข้อมูล ในกรณีที่เห็นว่าการควบคุมภายในที่ถือปฏิบัติไม่เพียงพอ หรือไม่มีประสิทธิภาพ

ในการทดสอบการควบคุมและทดสอบความถูกต้องของข้อมูล ผู้ตรวจสอบอาจใช้คอมพิวเตอร์ช่วยในการตรวจสอบก็ได้ ซึ่งจะทำให้สามารถขยายขอบเขตการทดสอบ และสามารถตรวจสอบการทำงานของโปรแกรมระบบงาน และข้อมูลในเครื่องได้โดยตรง แทนที่จะถูกจำกัดให้ตรวจสอบได้เพียงข้อมูลนำเข้าและข้อมูลผลลัพธ์

5) การจัดทำรายงานผลการตรวจสอบ รายงานสรุปผลการตรวจสอบ ควรประกอบด้วยหัวข้อดังนี้

5.1) เรื่องที่ตรวจสอบ
5.2) วันที่เริ่มตรวจสอบ และวันที่ตรวจสอบเสร็จ
5.3) รายชื่อผู้ตรวจสอบ
5.4) ขอบเขตและวัตถุประสงค์ในการตรวจสอบ
5.5) ข้อสังเกตและข้อเสนอแนะ
5.6) รายละเอียดเอกสารประกอบผลการตรวจสอบ

6) การจัดทำกระดาษทำการ เนื่องจากกระดาษทำการเป็นหลักฐานสำคัญที่แสดงถึงขอบ-เขต วิธีการปฏิบัติงานของผู้ตรวจสอบ และข้อสรุปของผู้ตรวจสอบ ดังนั้นสถาบันการเงินจึงควรกำหนดมาตรฐานของการจัดทำกระดาษทำการ กระดาษทำการตรวจสอบด้านคอมพิวเตอร์ควรประกอบด้วย

6.1) แผนการตรวจสอบ
6.2) ขอบเขตและวัตถุประสงค์ของการตรวจสอบ
6.3) การบรรยายสรุปวิธีการปฏิบัติงานและการควบคุมภายใน
6.4) แบบสอบถาม และวิธีการอื่น ๆ ที่ใช้ในการตรวจสอบ
6.5) บันทึกสรุปข้อสังเกตและปัญหาที่พบระหว่างการตรวจสอบ
6.6) หัวข้อการประชุมหรือการหารือร่วมกับส่วนงานที่ถูกตรวจสอบ

7) การติดตามผลการตรวจสอบ ควรกำหนดให้ส่วนงานที่ถูกตรวจสอบจัดทำหนังสือตอบชี้แจงการปรับปรุงแก้ไขตามข้อแนะนำของผู้ตรวจสอบ เสนอต่อฝ่ายบริหารระดับสูงภายในระยะเวลาอันควร และให้ฝ่ายตรวจสอบติดตามผลการดำเนินการแก้ไขดังกล่าวเสนอคณะกรรมการบริษัทต่อไป

3.2 การควบคุมการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์

ไมโครคอมพิวเตอร์เป็นเครื่องประมวลผลข้อมูลที่มีขนาดเล็กที่สุด ซึ่งถูกนำมาใช้งานในหลายลักษณะ คือ แบบอิสระในตัวเอง (Stand alone) หรือเป็นเทอร์มินัลของเครื่องคอมพิวเตอร์ใหญ่ (Computer Terminal) หรือเป็นเครือข่ายภายในสำนักงาน (Local area network) การใช้งานไมโครคอมพิวเตอร์เป็นไปด้วยความสะดวก ผู้ที่ไม่มีความรู้ทางคอมพิวเตอร์เทคนิคก็สามารถเรียนรู้และใช้งานไมโครคอมพิวเตอร์ได้ไม่ยาก เป็นระบบประมวลผลข้อมูลแบบเบ็ดเสร็จด้วยบุคคลเพียงคนเดียว ไม่มีการแบ่งแยกหน้าที่ปฏิบัติงาน ซึ่งแตกต่างไปจากระบบการประมวลผลด้วยเครื่องคอมพิวเตอร์ขนาดใหญ่ ดังนั้นหากไม่มีการควบคุมที่เหมาะสมก็อาจก่อให้เกิดความเสียหายได้ง่ายต่อเครื่องไมโครคอมพิวเตอร์ แฟ้มข้อมูล และโปรแกรม สถาบันการเงินที่มี เครื่องไมโคร-คอมพิวเตอร์ไว้ใช้งาน จึงควรกำหนดให้มีการควบคุมการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์ ดังนี้

3.2.1 การรักษาความปลอดภัยเครื่องไมโครคอมพิวเตอร์

เนื่องจากไมโครคอมพิวเตอร์มีขนาดเล็ก สะดวกในการใช้งานและการเคลื่อนย้าย จึงควรติดตั้งไว้ในสถานที่ที่สามารถควบคุมการเข้าออก เพื่อป้องกันการขโมยตัวเครื่อง และมิให้บุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปใช้เครื่องและมอบหมายให้หน่วยงานเจ้าของเครื่องเป็นผู้รับผิดชอบการใช้งานและดูแลรักษาเครื่อง

3.2.2 การควบคุมความปลอดภัยของแฟ้มข้อมูลและโปรแกรม

ข้อมูลและโปรแกรมที่มีความสำคัญต่อการดำเนินงานประจำวัน การตัดสินใจของฝ่ายบริหาร และที่เป็นความลับของลูกค้า สถาบันการเงินควรมีการควบคุมเพื่อป้องกันมิให้เกิดความเสียหาย เนื่องจากการสูญหาย ถูกทำลาย ถูกแก้ไข หรือถูกถ่ายสำเนา โดยไม่ได้รับอนุญาต

1) แฟ้มข้อมูลและโปรแกรมที่บรรจุอยู่ในจานแม่เหล็ก (Floppy diskette) ขณะที่ยังไม่ได้ใช้งานควรเก็บไว้ในสถานที่ที่ปลอดภัย สามารถควบคุมและป้องกันมิให้ผู้ที่ไม่มีสิทธินำออกไปใช้งานได้ และปิดสลากภายนอกแฟ้มข้อมูลและโปรแกรมทุกแผ่น เพื่อป้องกันการนำไปใช้ผิดพลาด

2) แฟ้มข้อมูลและโปรแกรมที่อยู่ในเครื่อง (Hard disks) ขณะที่ยังไม่ได้ใช้งานควรปิดเครื่องและล็อคกุญแจประจำเครื่อง เพื่อป้องกันมิให้ผู้ไม่มีสิทธิไปใช้เครื่องและข้อมูลในเครื่อง กรณีเป็นไมโครคอมพิวเตอร์ที่ใช้ร่วมกันหลายงานและหลายคน ควรกำหนดรหัสประจำตัวผู้มีสิทธิเข้าถึงแฟ้มข้อมูลและโปรแกรม (Identification code) และรหัสการใช้งาน (password) ซึ่งระบุขอบเขตของการใช้งานแฟ้มข้อมูลและโปรแกรมดังกล่าว

3) ควรจัดทำสำเนาแฟ้มข้อมูลและโปรแกรมที่สำคัญ ๆ ไว้ใช้ทดแทนในกรณีที่แฟ้มข้อมูลและโปรแกรมที่ใช้อยู่ปัจจุบันสูญหาย หรือเสียหายจนใช้การไม่ได้ เพื่อป้องกันมิให้การประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์หยุดชะงัก

4) ควรมีเอกสารประกอบระบบงานที่ใช้ไมโครคอมพิวเตอร์ อาทิ เช่น ลักษณะของงาน ลักษณะของแฟ้มข้อมูล ขั้นตอนการเตรียมข้อมูลนำเข้า การประมวลผลข้อมูล ลักษณะของผลลัพธ์หรือรายงานที่ได้ และการตรวจสอบความถูกต้องของข้อมูลและรายงาน เป็นต้น เพื่อให้แน่ใจว่าการปฏิบัติงานเป็นไปตามที่กำหนด และสามารถดำเนินต่อไปได้อย่างราบรื่นกรณีพนักงานประจำเครื่องไมโครคอมพิวเตอร์ลาออกไป

3.2.3 การตรวจสอบการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์

ควรมอบหมายให้ผู้ตรวจสอบภายในหรือหน่วยงานที่ไม่เกี่ยวข้องกับการประมวลผลข้อมูลตรวจสอบการรักษาความปลอดภัยไมโครคอมพิวเตอร์ แฟ้มข้อมูล และโปรแกรม การจัดทำสำเนาแฟ้มข้อมูลและโปรแกรม และตรวจสอบความถูกต้องของข้อมูลและรายงานที่ได้จากการประมวลผล

3

เหตุผลการออกมาตรฐาน การควบคุมภายในและการรักษาความปลอดภัย ระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์

เหตุผลการออกมาตรฐาน
การควบคุมภายในและการรักษาความปลอดภัยระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์

รายละเอียด	เหตุผล
1. การประมวลผลข้อมูลด้วยคอมพิวเตอร์หลัก 1.1 การบริหารงานทั่วไป 1.1.1 ควรจัดให้มีฝ่ายงานรับผิดชอบการประมวลผลข้อมูลด้วยคอมพิวเตอร์เป็นเอกเทศจากฝ่ายงานอื่น และมีการแบ่งแยกหน้าที่ระหว่างการพัฒนาระบบงาน การปฏิบัติงานประมวลผล การนำข้อมูลเข้า และการสอบทานความถูกต้องของข้อมูล ผลลัพธ์และรายงาน	1.1.1 เพื่อให้ทราบหน้าที่ความรับผิดชอบและสายการบังคับบัญชาที่ชัดเจน เพื่อประโยชน์ในการควบคุมและติดตามผลการปฏิบัติงาน
1.1.2 ควรกำหนดนโยบายและแผนการดำเนินงานเกี่ยวกับการจัดหาเครื่อง โปรแกรม และบุคลากร ที่จะรองรับความต้องการของบริษัทในระยะสั้นและระยะยาว	1.1.2 เพื่อให้การดำเนินงานเป็นไปตามทิศทางที่ต้องการ และใช้เป็นเครื่องมือในการวัดผลการดำเนินงานด้านคอมพิวเตอร์ของบริษัท
1.1.3 ควรกำหนดมาตรฐานและระเบียบปฏิบัติงานสำหรับฝ่ายประมวลผลฯ	1.1.3 เพื่อใช้เป็นแนวทางในการปฏิบัติงานให้มีประสิทธิภาพ การติดตามผลการปฏิบัติงานของพนักงาน และเป็นแนวทางในการประเมินผลเบื้องต้นเกี่ยวกับการควบคุมภายในของบริษัทด้วย
1.1.4 ควรกำหนดให้ฝ่ายประมวลผลฯ จัดทำรายงานผลการปฏิบัติงานเสนอฝ่ายบริหาร ซึ่งอาจแยกได้เป็น 3 เรื่องใหญ่ ๆ คือ การปฏิบัติงานประมวลผล การพัฒนาระบบงาน และการพนักงาน	1.1.4 เพื่อให้ฝ่ายบริหารมีข้อมูลประกอบการตัดสินใจ การวางแผน การติดตามและแก้ไขปัญหาโดยใกล้ชิด
1.2 การพัฒนาระบบงานและโปรแกรม 1.2.1 การพัฒนาระบบงานด้วยตนเอง 1) ควรมีการศึกษาเบื้องต้นเกี่ยวกับความเป็นไปได้ทางเทคนิค และความคุ้มค่าของระบบงาน	1) เพื่อให้ฝ่ายบริหารมีข้อมูลในการตัดสินใจว่าสมควรดำเนินการพัฒนา เป็นระบบงานต่อไปหรือไม่
2) ควรมีการวิเคราะห์และกำหนดลักษณะของระบบงานที่ผู้ใช้งานต้องการ	2) เพื่อให้แน่ใจว่าการออกแบบรายละเอียดของระบบงานตรงตามความต้องการใช้งานของบริษัทอย่างแท้จริง

รายละเอียด	เหตุผล
3) ควรมีการกำหนดรายละเอียดของระบบงานเกี่ยวกับขอบเขตและวัตถุประสงค์ของระบบงาน ลักษณะของผลลัพธ์ที่ต้องการ ลักษณะข้อมูลนำเข้า ลักษณะของแฟ้มข้อมูล ขั้นตอนการประมวลผล คุณสมบัติของโปรแกรม และการควบคุมภายในระบบงาน	3) เพื่อให้การจัดทำโปรแกรม เป็นไปตามวัตถุประสงค์ของระบบงาน
4) ในการจัดทำโปรแกรมระบบงาน ควรมีคำสั่งงานที่เกี่ยวกับการเช็คสอบความครบถ้วนของข้อมูล ความถูกต้องของข้อมูล และความถูกต้องของแฟ้มข้อมูลที่ใช้ในการประมวลผล	4) เพื่อให้แน่ใจว่าในโปรแกรมระบบงานมีการควบคุมที่เพียงพอ เพื่อป้องกันความผิดพลาดและการทุจริต
5) ควรมีการทดสอบโปรแกรมระบบงานก่อนนำออกใช้งาน โดยอาจใช้ข้อมูลจำลองทดสอบสถานการณ์ที่อาจนำไปสู่ความผิดพลาด และผู้ที่เข้าร่วมการทดสอบควรประกอบด้วยบุคคล 3 ฝ่าย คือ ฝ่ายคอมพิวเตอร์ ฝ่ายผู้ใช้งาน และฝ่ายตรวจสอบภายใน	5) เพื่อให้แน่ใจว่าการประมวลผลข้อมูลและรายงานข้อมูลผลลัพธ์ถูกต้องตรงความต้องการ มีการป้องกันความผิดพลาดในการปฏิบัติงานและการทุจริต และยังใช้เป็นแนวทางในการประเมินผลเบื้องต้น และทดแทนการทดสอบการควบคุมภายในของบริษัท
6) ในการนำโปรแกรมระบบงานออกใช้งาน ควรมีการสอบทานเกี่ยวกับการทดสอบและยอมรับจากส่วนงานที่เกี่ยวข้อง เอกสารประกอบระบบงานและโปรแกรมคู่มือปฏิบัติงานและแผนการจัดฝึกอบรมพนักงานฝ่ายผู้ใช้งานและฝ่ายคอมพิวเตอร์	6) เพื่อให้แน่ใจว่าโปรแกรมระบบงานที่พัฒนาเสร็จแล้วอยู่ในสภาพพร้อมที่จะใช้งานและเป็นที่ยอมรับของส่วนงานที่เกี่ยวข้อง
7) ควรมีการประเมินผลการปฏิบัติงานภายหลังที่ปฏิบัติไปได้ระยะหนึ่งเกี่ยวกับการใช้งานได้ตามที่ออกแบบไว้ ค่าใช้จ่ายที่เกิดขึ้นกับค่าใช้จ่ายตามประมาณการ และปัญหาในการปฏิบัติงาน	7) เพื่อพิสูจน์ความคุ้มค่า ความมีประสิทธิภาพของการปฏิบัติงานในระบบงานใหม่ และสิ่งที่ควรได้รับการแก้ไข
8) ในการปรับปรุงแก้ไขโปรแกรมระบบงาน ควรให้ฝ่ายผู้ใช้งานจัดทำหลักฐานใบคำขอระบุเหตุผลและความต้องการแก้ไข และให้ฝ่ายคอมพิวเตอร์ดำเนินการปรับปรุงแก้ไขตามมาตรฐานเช่นเดียวกับการพัฒนาระบบงานใหม่	8) เพื่อป้องกันมิให้เกิดการผิดพลาด และการกระทำการทุจริต

รายละเอียด	เหตุผล
1.2.2 การว่าจ้างให้บุคคลภายนอกเป็นผู้พัฒนาหรือจัดซื้อโปรแกรมระบบงาน โดยเฉพาะสถาบันการเงินที่ใช้ระบบประมวลผลข้อมูลขนาดเล็กควรมีมาตรฐานในการจัดหาโปรแกรมระบบงาน ดังนี้	
1) กำหนดคุณสมบัติและรายละเอียดเกี่ยวกับลักษณะของข้อมูลนำเข้าข้อมูลผลลัพธ์และรายงานการควบคุมความถูกต้องและความปลอดภัยของข้อมูลในโปรแกรมระบบงานที่ต้องการ	1) เพื่อให้แน่ใจว่าการประมวลผลข้อมูลและรายงานที่ได้รับถูกต้องตรงความต้องการ มีการป้องกันความผิดพลาดในการปฏิบัติงานและการทุจริต
2) วิเคราะห์ผลประโยชน์ตอบแทนกับค่าใช้จ่ายในการว่าจ้างหรือจัดซื้อโปรแกรมระบบงานภายนอก	2) เพื่อให้ฝ่ายบริหารมีข้อมูลสำหรับการตัดสินใจเช่นเดียวกับการพัฒนาระบบงานด้วยตนเอง
3) วิเคราะห์ฐานะการเงิน ชื่อเสียงและความพร้อมทางเทคนิคของบริษัทผู้ผลิตหรือผู้ขายโปรแกรมระบบงาน ที่จะให้การช่วยเหลือเมื่อมีปัญหา	3) เพื่อให้แน่ใจว่าผู้ผลิตหรือผู้ขายสามารถให้การสนับสนุนได้ตลอดไป เมื่อมีปัญหาหรือต้องการปรับปรุงระบบงาน
4) วิเคราะห์ความเพียงพอและความสมบูรณ์ของเอกสารประกอบการใช้โปรแกรมระบบงาน ได้แก่ คำอธิบายลักษณะของระบบงาน ลักษณะของโปรแกรมและคำสั่งงาน ลักษณะข้อมูลนำเข้าและแฟ้มบันทึกข้อมูล คู่มือสำหรับผู้ใช้เครื่อง และคู่มือสำหรับผู้ใช้ระบบงาน	4) เพื่อประโยชน์ในการปฏิบัติงานของพนักงาน การแก้ไขและปรับปรุงงาน และยังเป็นแนวทางสำหรับการประเมินผลเบื้องต้นเกี่ยวกับการควบคุมภายในของบริษัทอีกด้วย
5) วิเคราะห์ความเพียงพอของแผนการให้การฝึกอบรมของผู้ผลิตหรือผู้ขาย	5) เพื่อให้แน่ใจว่าพนักงานมีความรู้ความเข้าใจ และการฝึกฝนเพียงพอสำหรับการปฏิบัติงาน
1.3 เอกสารสนับสนุนการปฏิบัติงาน	
1.3.1 ควรจัดให้มีเอกสารสนับสนุนการปฏิบัติงานประมวลผลข้อมูลอย่างครบถ้วน และให้เป็นปัจจุบันอยู่เสมอ ได้แก่	1.3.1 เพื่อใช้เป็นแนวทางในการปฏิบัติงาน การปรับปรุงแก้ไขระบบงานการสับเปลี่ยนหมุนเวียนหน้าที่งาน และยังช่วยให้การประมวลผลข้อมูลดำเนินต่อไปได้ กรณีที่มีพนักงานตำแหน่งสำคัญลาออกไป นอกจากนั้นยังใช้เป็นแนวทางในการประเมินผลเบื้องต้นเกี่ยวกับการควบคุมภายในของบริษัทด้วย

รายละเอียด	เหตุผล
1) มาตรฐานและระเบียบปฏิบัติงานทั่วไปเกี่ยวกับการพัฒนาระบบงานและโปรแกรม การใช้คอมพิวเตอร์ประมวลผลข้อมูล การเตรียมข้อมูลและป้อนข้อมูลด้วยเครื่องเทอร์มินัล และการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์และรายงาน 2) เอกสารประกอบระบบงาน ประกอบด้วยรายละเอียดเกี่ยวกับระบบงาน รายละเอียดเกี่ยวกับโปรแกรม และคู่มือสำหรับผู้ปฏิบัติงาน	
1.3.2 ควรจัดเก็บเอกสารสนับสนุนการปฏิบัติงานไว้ในสถานที่ที่ปลอดภัย และควบคุมดูแลการนำออกไปใช้งาน และควรจัดทำสำเนาไว้อย่างน้อย 1 ชุด เก็บไว้ในที่ที่ปลอดภัย แยกจากชุดที่ใช้งาน	1.3.2 เพื่อป้องกันมิให้เอกสารคู่มือปฏิบัติงานที่จำเป็นต่อการประมวลผลข้อมูลสูญหายหรือถูกทำลาย อันเป็นเหตุให้การปฏิบัติงานผิดพลาด หรือเกิดการทุจริต
1.4 การปฏิบัติการประมวลผล	
1.4.1 การรักษาความสะอาดเรียบร้อยภายในห้องเครื่องคอมพิวเตอร์หรือบริเวณที่ติดตั้งเครื่อง	1.4.1 เพื่อป้องกันฝุ่นละอองและการเกิดเพลิงไหม้ อันอาจสร้างความเสียหายต่อเครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบเครื่อง
1.4.2 การบำรุงรักษาเครื่องคอมพิวเตอร์ให้อยู่ในสภาพที่พร้อมใช้งาน	1.4.2 เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์เสื่อมสภาพเร็วกว่าเวลาอันสมควร อันอาจทำให้การประมวลผลผิดพลาด
1.4.3 การแบ่งแยกและสับเปลี่ยนหน้าที่ของผู้ปฏิบัติงานประมวลผลข้อมูล อาทิเช่น การป้อนข้อมูลเข้าเครื่อง การใช้งานเครื่องประมวลผลข้อมูล และการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์และรายงาน	1.4.3 เพื่อมิให้บุคคลใดบุคคลหนึ่งทำงานโดยลำพังตั้งแต่ต้นจนจบ อันเป็นหลักในการป้องกันการทุจริต
1.4.4 การกำหนดตารางปฏิบัติงานประมวลผลข้อมูลประจำวัน ประจำสัปดาห์ และประจำเดือน	1.4.4 เพื่อให้การใช้เครื่องเป็นไปด้วยความมีประสิทธิภาพ และงานเสร็จทันเวลาที่กำหนด นอกจากนี้ยังใช้เป็นเครื่องมือในการป้องกัน และตรวจสอบการใช้เครื่องโดยมิได้รับอนุญาต หรือปฏิบัติงานนอกเหนือจากที่ได้รับมอบหมาย
1.4.5 การควบคุมการใช้เครื่องคอมพิวเตอร์ควรมอบหมายให้พนักงานปฏิบัติการระดับหัวหน้า	1.4.5 เพื่อให้ฝ่ายบริหารมีข้อมูลประกอบการตัดสินใจ การติดตามและแก้ไขปัญหาในการ

รายละเอียด	เหตุผล
งานเป็นผู้ควบคุมดูแลการใช้เครื่องให้เป็นไปตามตารางปฏิบัติงาน และจัดทำรายงานเมื่อมีเหตุการณ์ผิดปกติ หรือเมื่อเกิดความเสียหาย รวมทั้งควรมีเครื่องมือสำหรับบันทึกการสั่งงานเครื่องคอมพิวเตอร์และเวลาที่ใช้ในการปฏิบัติงานโดยอัตโนมัติ เช่น Console printer และ Activity logs เป็นต้น	ปฏิบัติงานโดยใกล้ชิด นอกจากนี้ยังใช้เป็นเครื่องมือในการป้องกันและตรวจสอบการใช้เครื่องโดยไม่ได้รับอนุญาต
1.4.6 การควบคุมการใช้แฟ้มข้อมูลโปรแกรม และคู่มือปฏิบัติงาน 1) สำหรับแฟ้มข้อมูลและโปรแกรมที่บรรจุอยู่ในเทปหรือจานแม่เหล็ก และเอกสารคู่มือปฏิบัติงาน ควรเก็บไว้ในที่ปลอดภัย และมีเจ้าหน้าที่เฉพาะควบคุมการนำออกไปใช้งาน 2) สำหรับแฟ้มข้อมูลและโปรแกรมระบบงานที่อยู่ในเครื่องคอมพิวเตอร์ ควรมีการควบคุมการใช้งานด้วยโปรแกรมพิเศษ เช่น RACF, TOP SECRET, LIBRARIAN, SECURE และ PANVALET เป็นต้น	1.4.6 เพื่อควบคุมดูแลและรักษาข้อมูล โปรแกรม และเอกสารคู่มือปฏิบัติงานที่สำคัญให้ปลอดภัย ป้องกันการสูญหาย และการนำไปใช้โดยมิได้รับอนุญาต
1.4.7 การกำหนดขอบเขตการปฏิบัติงาน พนักงานที่ทำหน้าที่ประมวลผลข้อมูล มิให้ปฏิบัติงานที่อาจก่อให้เกิดความเสียหายแก่เครื่องคอมพิวเตอร์ โปรแกรม และข้อมูล เช่น ไม่ควรยินยอมให้เข้าไปยุ่งเกี่ยวกับ Source program, Program listing และเอกสาร อื่นที่ไม่เกี่ยวกับการใช้เครื่อง Utility program ที่มีคุณสมบัติในการแก้ไขข้อมูลและโปรแกรมระบบงาน และไม่ควรให้ทำหน้าที่ตรวจสอบความถูกต้องของข้อมูลผลลัพธ์และรายงาน	1.4.7 เนื่องจากพนักงานที่ทำหน้าที่ประมวลผลสามารถใช้เครื่องคอมพิวเตอร์ในการเรียกใช้โปรแกรมและข้อมูลในการประมวลผลได้อย่างกว้างขวาง หากไม่มีการควบคุมการปฏิบัติ อาจก่อให้เกิดความเสียหายและการทุจริตได้
1.5 การประมวลผลในระบบสื่อสาร	
1.5.1 การรักษาความปลอดภัยเครื่องเทอร์มินัล ควรทำทั้งที่ตัวเครื่องฯ และการใช้โปรแกรมควบคุมการใช้เครื่อง	1.5.1 เพื่อป้องกันมิให้ผู้ที่ไม่มีสิทธิ และบุคคลภายนอกเข้าไปใช้เครื่องฯ และจำกัดสิทธิของผู้ใช้เครื่องฯ ให้อยู่ภายในขอบเขตที่ได้รับมอบหมาย

รายละเอียด	เหตุผล
1.5.2 การรักษาความปลอดภัยในการรับส่งข้อมูลระหว่างเทอร์มินัลและคอมพิวเตอร์ 1) เก็บรักษาเอกสารที่เกี่ยวกับระบบสื่อสารและผังแสดงที่ตั้งอุปกรณ์สื่อสารไว้ในที่ปลอดภัย 2) แปลงรหัสประจำตัวผู้มีสิทธิเข้าถึงข้อมูล และข้อมูลที่มีความสำคัญให้อยู่ในรูปแบบซึ่งเมื่อรั่วไหลไปถึงมือบุคคลภายนอกแล้วไม่สามารถนำไปใช้ประโยชน์ได้ 3) กำหนดรหัสแสดงแหล่งที่มาของข้อมูลนำเข้า เพื่อใช้ในการพิสูจน์ความถูกต้องของผู้ส่ง 4) ให้ลำดับเลขหมายกำกับข้อมูล วันที่และเวลาที่ส่งข้อมูลแต่ละรายการจากเครื่องเทอร์-มินัล 5) กำหนดเวลาให้คอมพิวเตอร์หยุดติดต่อกับเทอร์มินัลโดยอัตโนมัติ เมื่อมีเทอร์มินัลเครื่องใดเครื่องหนึ่งเปิดทิ้งไว้ไม่ได้ใช้งานเป็นระยะเวลานาน 6) กำหนดเวลาเปิดปิดการรับส่งข้อมูลระหว่างคอมพิวเตอร์และเทอร์มินัลประจำวัน	1.5.2 เพื่อป้องกันมิให้ข้อมูลสูญหายหรือถูกลักลอบเพิ่มเติม เปลี่ยนแปลงแก้ไข ระหว่างการสื่อสารจากเครื่องเทอร์มินัลไปยังคอมพิวเตอร์
1.5.3 การจัดเตรียมอุปกรณ์สื่อสารชุดสำ-รองไว้ใช้ในกรณีฉุกเฉิน สำหรับระบบงานที่มีความสำคัญ และควรมีการทดสอบใช้งานเป็นครั้งคราว	1.5.3 เพื่อป้องกันมิให้การปฏิบัติงานของบริษัทหยุดชะงักและเกิดความเสียหายในทางธุรกิจ เช่น การซื้อขายหลักทรัพย์ด้วยคอมพิวเตอร์ เป็นต้น
1.6 การควบคุมความถูกต้องและความน่าเชื่อถือของข้อมูล 1.6.1 การควบคุมการนำข้อมูลเข้าเครื่อง 1) ควรมีการสะสมยอดรวมจำนวนข้อมูลทั้งหมดก่อนหน้าและหลังจากการป้อนรายการเข้าเครื่องเทอร์มินัล และเมื่อข้อมูลเข้าไปในคอมพิวเตอร์แล้ว เพื่อใช้ในการสอบทานความครบถ้วนของข้อมูล 2) ควรมีการตรวจเช็คความถูกต้องของข้อมูลแต่ละรายการ ในขณะที่ทำการป้อนข้อมูล	1.6.1 เป็นมาตรการควบคุมทางบัญชี เพื่อพิสูจน์ความครบถ้วนและความถูกต้องเบื้องต้นของข้อมูล หากมีความแตกต่างจะได้ค้นหาสาเหตุต่อไป เป็นการป้องกันความผิดพลาดและการทุจริตในการนำข้อมูลเข้าคอมพิวเตอร์

รายละเอียด	เหตุผล
ก่อนหน้าที่ข้อมูลจะเข้าไปในคอมพิวเตอร์ เช่น การตรวจเช็ครหัสรายการ การตรวจเช็คลำดับของรายการ การตรวจเช็คจำนวนเงิน และการตรวจเช็คเลขที่บัญชีเจ้าของรายการ เป็นต้น เพื่อป้องกันข้อมูลที่ผิดพลาดหรือแปลกปลอมเข้าไปในเครื่อง 3) ควรจัดทำรายงานคอมพิวเตอร์แสดงรายละเอียดข้อมูลทุกรายการที่เข้าไปในคอมพิวเตอร์ เพื่อใช้ในการเช็คสอบความถูกต้องกับเอกสารหลักฐานเบื้องต้นที่ใช้ในการบันทึกรายการ เช่นเดียวกับการบันทึกรายการในสมุดรายวันทั่วไป	
1.6.2 การควบคุมการออกข้อมูลผลลัพธ์และรายงาน	
1) ควรมีการสอบทานความเรียบร้อย และความถูกต้องของข้อมูลผลลัพธ์และรายงาน โดยการตรวจสอบและกระทบยอดรวมข้อมูลที่นำเข้าเครื่องเทอร์มินัล ยอดรวมข้อมูลที่เข้าคอมพิวเตอร์ ยอดรวมในบัญชีแยกประเภททั่วไปและยอดคงเหลือในงบทดลอง เพื่อพิสูจน์ความถูกต้องของข้อมูลผลลัพธ์และรายงาน	1) เป็นมาตรการควบคุมทางบัญชีเพื่อพิสูจน์ความถูกต้องเบื้องต้นของรายงานข้อมูลผลลัพธ์ หากมีข้อมูลสูญหายหรือไม่สามารถบันทึกบัญชีได้ จะได้ค้นหาสาเหตุ และปรับปรุงแก้ไขให้ถูกต้อง เป็นการป้องกันความผิดพลาดและการทุจริต
2) ควรมีการควบคุมการจัดส่งข้อมูลผลลัพธ์และรายงานให้ถึงมือผู้รับอย่างถูกต้องและครบถ้วน โดยจัดทำทะเบียนบันทึกรายงานที่ได้จากการประมวลผลรายวัน รายสัปดาห์ และรายเดือน ผู้รับหรือผู้ใช้รายงาน ลายมือชื่อ และวันที่ที่รับรายงาน	2) เพื่อป้องกันมิให้รายงานสูญหายหรือถูกนำไปใช้ในการทุจริต
1.6.3 การควบคุมอุปกรณ์บันทึกข้อมูล (Data file media controls)	
1) ควรเก็บรักษาอุปกรณ์บันทึกข้อมูลขณะที่ยังไม่ได้นำไปใช้งานประมวลผลไว้ในสถานที่ปลอดภัย มีการควบคุมอุณหภูมิ ความชื้น ฝุ่นละออง และอุปกรณ์ดับเพลิง และจัดให้เจ้าหน้าที่เฉพาะควบคุมดูแลการนำออกไปใช้งาน และมีการตรวจนับ	1) เพื่อป้องกันมิให้ข้อมูลสูญหายหรือถูกทำลาย เนื่องจากข้อมูลที่บรรจุอยู่ในเทปหรือจานแม่เหล็กเสียหายหรือถูกทำลายได้ง่ายกว่าข้อมูลบนแผ่นกระดาษ

รายละเอียด	เหตุผล
จำนวนคงเหลือเป็นครั้งคราว 2) ควรจัดทำป้ายชื่อติดกำกับภายนอกอุปกรณ์บันทึกข้อมูล ส่วนภายในบริเวณหัวและท้ายแฟ้มข้อมูลควรบันทึกข้อมูลเกี่ยวกับ ชื่อแฟ้มข้อมูล วันที่ และจำนวนรายข้อมูลทั้งหมดที่บรรจุอยู่ในแฟ้มข้อมูลนั้น	2) เพื่อป้องกันการนำไปใช้งานประมวลผลผิดพลาด
3) ควรมีอุปกรณ์บันทึกข้อมูลชุดสำเนา (Back-up file) แยกเก็บไว้ในที่ปลอดภัยห่างจากอาคารสถานที่ประมวลผลข้อมูล	3) เพื่อป้องกันมิให้ข้อมูลของบริษัทถูกทำลายไปโดยสิ้นเชิงและสามารถนำมาใช้ประมวลผลได้ในกรณีฉุกเฉิน
1.7 การรักษาความปลอดภัย 1.7.1 ควรกำหนดแผนการรักษาความปลอดภัย โดยมีรายละเอียดเกี่ยวกับการป้องกันความเสียหายที่จะมีต่อเครื่องคอมพิวเตอร์ โปรแกรม และข้อมูล การปฏิบัติงานขณะที่เกิดความเสียหายจากเหตุการณ์ที่ไม่คาดคิด และการปฏิบัติงานประมวลผล ณ สถานที่แห่งใหม่ที่ได้จัดเตรียมไว้	1.7.1 เพื่อให้มีระบบการประมวลผลข้อมูลที่มั่นคงและปลอดภัย ไม่ทำให้การประกอบธุรกิจของบริษัทหยุดชะงัก เนื่องจากขาดข้อมูลและรายงานที่ใช้ในการตัดสินใจและการปฏิบัติงาน
1.7.2 การป้องกันภัยพิบัติและความเสียหายจากสาเหตุอื่น 1) สถานที่ตั้งหน่วยงานประมวลผลข้อมูล ไม่ควรเป็นบริเวณที่มีคนพลุกพล่าน น้ำท่วมถึงและคลื่นแม่เหล็กรบกวนภายในอาคารที่ตั้ง มียามรักษาการทางเข้า และติดตั้งเครื่องมือป้องกันการโจรกรรมและการบุกรุกในยามวิกาล ประตูทางเข้าและหน้าต่างปิดสนิทตลอดเวลา	1) เพื่อป้องกันการเกิดภัยพิบัติการโจรกรรมและการบุกรุกทำลาย ซึ่งก่อให้เกิดความเสียหายต่อเครื่องคอมพิวเตอร์ โปรแกรม และข้อมูลจนไม่สามารถประมวลผลต่อไปได้
2) ภายในห้องหรือบริเวณติดตั้งเครื่องคอมพิวเตอร์ควรมีอุปกรณ์ดับเพลิง อุปกรณ์ตรวจวัดความร้อนและควันไฟอุปกรณ์ควบคุมอุณหภูมิและความชื้นตามที่บริษัทผู้ผลิตเครื่องกำหนด มีเครื่องวัดและปรับแรงดันกระแสไฟฟ้าให้คงที่ และเครื่องกำเนิดไฟฟ้าสำรองไว้ใช้กรณีไฟฟ้าดับกระทันหัน	2) เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์ โปรแกรม และข้อมูล ที่อยู่ในเครื่องเสียหายหรือทำงานผิดปกติ

รายละเอียด	เหตุผล
3) ไม่ควรแสดงสถานที่ตั้งเครื่องคอมพิวเตอร์ให้ปรากฏแก่บุคคลทั่วไป เช่น ป้ายชื่อหรือสัญลักษณ์ที่ระบุว่าเป็นศูนย์ ฝ่ายหรือส่วนงานประมวลผลข้อมูล เป็นต้น	3) เพื่อป้องกันการบุกรุกทำลายเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบโปรแกรมและข้อมูล
4) ไม่ควรให้บุคคลอื่นเว้นแต่พนักงานปฏิบัติการประมวลผลอยู่ในห้องหรือบริเวณที่ตั้งเครื่อง	4) เพื่อป้องกันมิให้เกิดความเสียหายต่อเครื่องคอมพิวเตอร์ โปรแกรมและข้อมูล โดยการกระทำที่รู้เท่าไม่ถึงการณ์ หรือเจตนากระทำการทุจริต
5) ตู้นิรภัยและห้องมั่นคงที่ใช้เก็บรักษาข้อมูลและโปรแกรมที่บรรจุในเทปหรือจานแม่เหล็ก และเอกสารคู่มือปฏิบัติงานควรเป็นชนิดที่สามารถป้องกันไฟและการโจรกรรมได้	5) เพื่อป้องกันความเสียหายที่จะเกิดกับอุปกรณ์และเอกสารสำคัญสำหรับการประมวลผล อันจะทำให้การประมวลผลหยุดชะงัก
1.7.3 การจัดเตรียมระบบประมวลผลสำรอง	1.7.3 ระบบประมวลผลด้วยคอมพิวเตอร์สำรองประกอบด้วย เครื่องคอมพิวเตอร์ โปรแกรม แฟ้มข้อมูล และเอกสารคู่มือปฏิบัติงานที่เตรียมกรณีที่เกิดเหตุการณ์ที่ไม่คาดคิด และสร้างความเสียหายต่อคอมพิวเตอร์จนไม่สามารถประมวลผลข้อมูลต่อไปได้ เช่น เพลิงไหม้ น้ำท่วม หรือกระแสไฟฟ้าดับเป็นเวลานาน เป็นต้น ทั้งนี้เพื่อป้องกันมิให้การประมวลผลข้อมูลหยุดชะงัก จนเป็นผลเสียหายต่อการประกอบธุรกิจ
1) ควรจัดหาเครื่องคอมพิวเตอร์สำรองไว้ใช้ในกรณีฉุกเฉิน หรือจัดทำข้อตกลงกับสถาบันการเงินอื่นที่มีเครื่องคอมพิวเตอร์ที่ใช้ร่วมกันได้ หรือกับบริษัทผู้ผลิตหรือผู้ขายเพื่อขอใช้เครื่องประมวลผลในกรณีฉุกเฉิน และควรมีการทดสอบการประมวลผลด้วยระบบสำรองเป็นครั้งคราว	
2) ควรจัดทำโปรแกรมและเอกสารคู่มือปฏิบัติงานชุดสำเนา เก็บไว้ในสถานที่ปลอดภัยนอกที่ทำการ	
3) ควรจัดทำแฟ้มข้อมูลชุดสำรองไว้ให้เพียงพอสำหรับการสร้างแฟ้มข้อมูลใหม่ให้เป็นปัจจุบัน และเก็บรักษาไว้ในสถานที่ปลอดภัยนอกที่ทำการ	
4) กรณีเลือกระบบประมวลผลสำรอง ซึ่งปฏิบัติโดยบุคคล ควรฝึกฝนพนักงานให้สามารถปฏิบัติงานตามแบบเดิมได้ และทดสอบการปฏิบัติงานอย่างสม่ำเสมอ	

รายละเอียด	เหตุผล
1.7.4 ควรมีการประกันภัยเพื่อคุ้มครองความเสียหายที่อาจเกิดขึ้นกับการประมวลผลข้อมูลด้วยคอมพิวเตอร์ โดยเฉพาะความเสียหายที่มูลค่าจำนวนเงินสูง เช่น เครื่องคอมพิวเตอร์และอุปกรณ์ที่จำเป็นในการประมวลผลข้อมูล และค่าใช้จ่ายพิเศษที่เกิดจากการประมวลผลข้อมูลด้วยคอมพิวเตอร์สำรอง เป็นต้น	.1.7.4 การรักษาความปลอดภัยแต่ประการเดียว อาจไม่สามารถป้องกันความเสียหายได้ทั้งหมด การประกันภัยจะช่วยคุ้มครองความเสียหายที่อาจเกิดขึ้นได้
1.8 การตรวจสอบงานคอมพิวเตอร์ (Computer Audit)	
1.8.1 ควรกำหนดให้มีการตรวจสอบด้านคอมพิวเตอร์ภายในบริษัท โดยมอบหมายให้ผู้ตรวจสอบภายใน หรือผู้สอบบัญชีภายนอกหรือร่วมกันตรวจสอบ และให้รายงานผลการตรวจสอบโดยตรงต่อคณะกรรมการบริษัท	1.8.1 ฝ่ายบริหารมีหน้าที่ต้องจัดให้มีการตรวจสอบภายในด้านคอมพิวเตอร์ เพื่อติดตามดูแลว่าการปฏิบัติงานเป็นไปตามระบบการควบคุมภายในที่บริษัทกำหนด และให้รายงานผลการตรวจสอบโดยตรงต่อคณะกรรมการบริษัท เพื่อให้เกิดความเป็นอิสระในการปฏิบัติงานตรวจสอบ
1.8.2 ควรจัดทำคู่มือการตรวจสอบด้านคอมพิวเตอร์ โดยมีรายละเอียดเกี่ยวกับการจัดทำแผนการตรวจสอบวัตถุประสงค์และขอบเขตการตรวจสอบ วิธีการตรวจสอบ การจัดทำรายงานผลการตรวจสอบ กระดาษทำการตรวจสอบ และการติดตามผลการตรวจสอบ 1.8.3 ขอบเขตการตรวจสอบด้านคอมพิวเตอร์ของบริษัท ควรมีรายละเอียดครอบคลุมถึงการพัฒนาระบบงานและโปรแกรม และการปฏิบัติงานประมวลผลข้อมูล การรักษาความปลอดภัย การนำข้อมูลเข้า และการสอบทานความถูกต้องข้อมูลผลลัพธ์และรายงานที่ได้จากการประมวลผล 1.8.4 การปฏิบัติงานตรวจสอบด้านคอมพิวเตอร์ ควรมีขั้นตอนเกี่ยวกับการสอบทาน การควบคุมภายในการทดสอบ การปฏิบัติงาน และการทดสอบความถูกต้องของข้อมูล	1.8.2-1.8.7 เพื่อให้การตรวจสอบมีประสิทธิภาพและบรรลุวัตถุประสงค์ตามที่ต้องการ ฝ่ายบริหารควรพิจารณากำหนดมาตรฐานและวิธีการตรวจสอบด้านคอมพิวเตอร์ให้ครอบคลุมงานทุกด้าน นอกจากนี้คู่มือการตรวจสอบยังใช้ประโยชน์ในการฝึกอบรมผู้ตรวจสอบ และเป็นแนวทางสำหรับการประเมินผลเบื้องต้นเกี่ยวกับการควบคุมภายในของบริษัท และอาจใช้เป็นหลักฐานทดแทนการทดสอบประสิทธิภาพการควบคุมและความถูกต้องของข้อมูลอีกด้วย

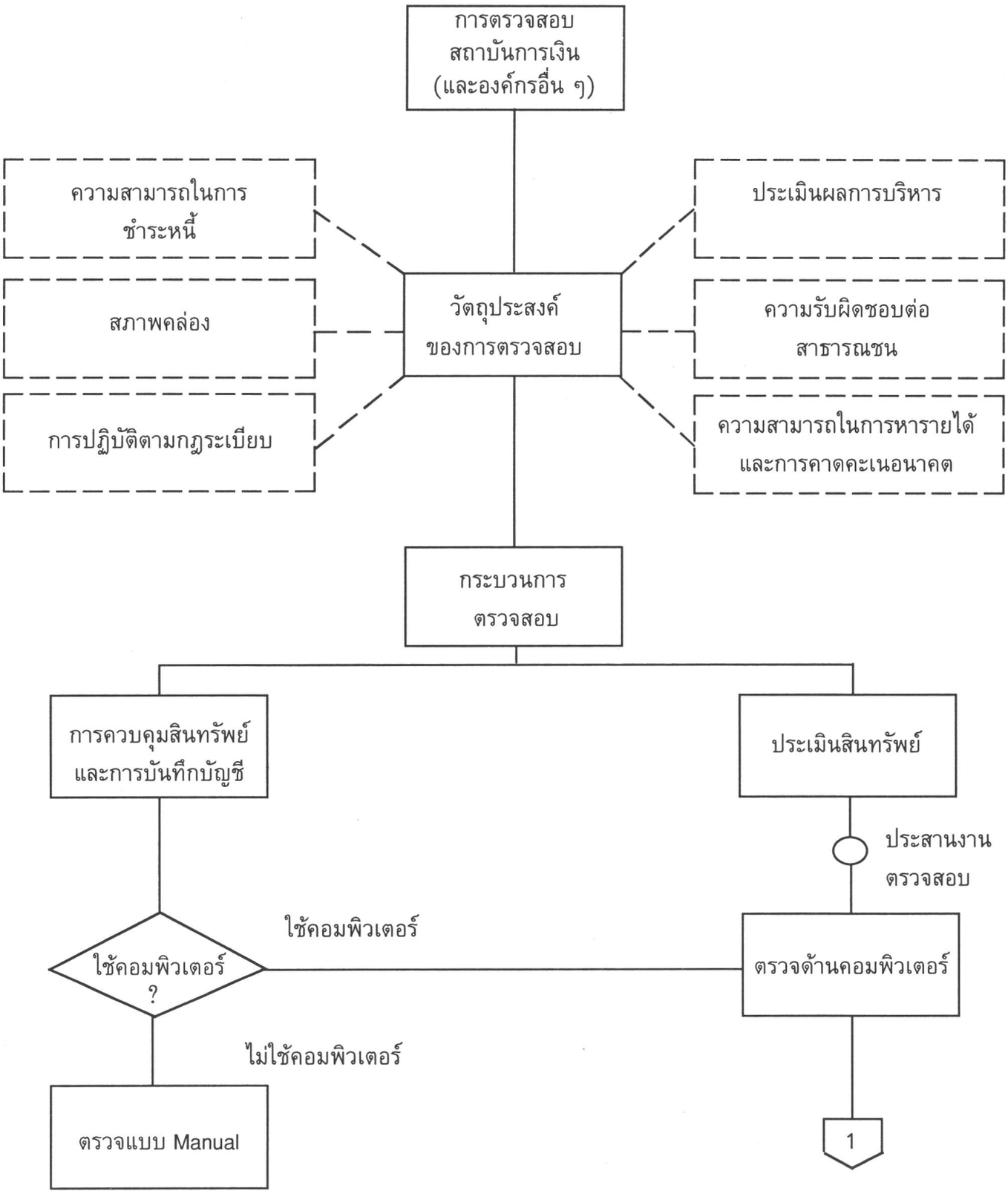
รายละเอียด	เหตุผล
1.8.5 รายงานผลการตรวจสอบควรประกอบด้วยหัวข้อเกี่ยวกับเรื่องที่ตรวจสอบ ขอบเขต และวัตถุประสงค์ในการตรวจสอบข้อสังเกตและข้อเสนอแนะ และรายละเอียดเอกสารประกอบผลการตรวจสอบ 1.8.6 กระดาษทำการตรวจสอบควรประกอบด้วย แผนการตรวจสอบ ขอบเขต และวัตถุประสงค์ของการตรวจสอบ การบรรยายสรุปวิธีการปฏิบัติงาน และการควบคุมภายในแบบสอบถามและเทคนิคอื่น ๆ ที่ใช้ในการตรวจสอบ บันทึกสรุปข้อสังเกตและปัญหาที่พบระหว่างการตรวจสอบ และหัวข้อการประชุมหรือการหารือกับส่วนงานที่ถูกตรวจสอบ 1.8.7 ควรกำหนดให้ส่วนงานที่ถูกตรวจสอบจัดทำหนังสือตอบชี้แจงการปรับปรุงแก้ไข เสนอฝ่ายบริหารระดับสูงภายในเวลาอันควร และให้ฝ่ายตรวจสอบติดตามผลการดำเนินการแก้ไขดังกล่าวเสนอคณะกรรมการบริษัทต่อไป 2. การประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์ 2.1 การรักษาความปลอดภัย 2.1.1 เครื่องไมโครคอมพิวเตอร์ควรติดตั้งไว้ในที่ปลอดภัย มีการป้องกันการขโมยตัวเครื่องและการเข้าไปใช้เครื่องโดยผู้ที่ไม่มีส่วนเกี่ยวข้อง และให้หน่วยงานเจ้าของเครื่องเป็นผู้รับผิดชอบการใช้งาน และการดูแลรักษาเครื่อง 2.1.2 ข้อมูลและโปรแกรมที่มีความสำคัญต่อการดำเนินงานของบริษัท และที่เป็นความลับของลูกค้า ควรดำเนินการดังนี้ 1) แฟ้มข้อมูลและโปรแกรมที่บรรจุอยู่ในจานแม่เหล็ก ขณะที่ยังไม่ได้ใช้งานควรเก็บไว้ในสถานที่ปลอดภัย และปิดฉลากภายนอกทุกแผ่น เพื่อป้องกันการนำไปใช้ผิดพลาด	2.1.1 เนื่องจากไมโครคอมพิวเตอร์เป็นเครื่องคอมพิวเตอร์ขนาดเล็ก สะดวกต่อการใช้งานและการเคลื่อนย้าย จึงควรมีการป้องกันมิให้เกิดการสูญหาย หรือใช้งานโดยมิได้รับอนุญาต 2.1.2 เพื่อป้องกันมิให้เกิดความเสียหายเนื่องจากการสูญหาย ถูกทำลาย ถูกแก้ไข หรือถูกถ่ายสำเนา โดยไม่ได้รับอนุญาต และมีเอกสารคู่มือปฏิบัติงาน โปรแกรม และข้อมูลเพียงพอต่อการปฏิบัติงานในกรณีฉุกเฉิน

รายละเอียด	เหตุผล
2) แฟ้มข้อมูลและโปรแกรมที่อยู่ในเครื่อง เมื่อเลิกใช้งานควรปิดเครื่องและล็อคกุญแจประจำเครื่อง กรณีเป็นเครื่องไมโครคอมพิวเตอร์ที่ใช้ร่วมกันหลายงานและหลายคนควรกำหนดรหัสประจำตัวผู้มีสิทธิเข้าถึงแฟ้มข้อมูลและโปรแกรม และรหัสการใช้งาน 3) ควรจัดทำสำเนาแฟ้มข้อมูลและโปรแกรมที่สำคัญ ๆ ไว้ อย่างน้อย 1 ชุด 4) ควรมีเอกสารประกอบงานที่ใช้ไมโครคอมพิวเตอร์ประมวลผล โดยมีรายละเอียดเกี่ยวกับลักษณะงาน ลักษณะของแฟ้มข้อมูล ขั้นตอนการเตรียมข้อมูลนำเข้า การประมวลผลลักษณะของข้อมูลผลลัพธ์และรายงาน และการตรวจสอบความถูกต้อง 2.2 การตรวจสอบการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์ ควรมอบหมายให้ผู้ตรวจสอบภายในหรือหน่วยงานที่ไม่เกี่ยวข้องกับการประมวลผลทำหน้าที่ตรวจสอบ การรักษาความปลอดภัยไมโครคอมพิวเตอร์ แฟ้มข้อมูล และโปรแกรม การจัดทำสำเนาแฟ้มข้อมูลและโปรแกรม และความถูกต้องของข้อมูลและรายงานที่ได้จากการประมวลผล	2.2 เพื่อให้ฝ่ายบริหารมีความมั่นใจว่าบริษัทมีการรักษาความปลอดภัยระบบการประมวลผลด้วยไมโครคอมพิวเตอร์ การนำเข้าข้อมูล และรายงานที่ได้จากการประมวลผลมีความถูกต้องเชื่อถือได้ไม่ก่อให้เกิดความเสียหายหรือการทุจริต

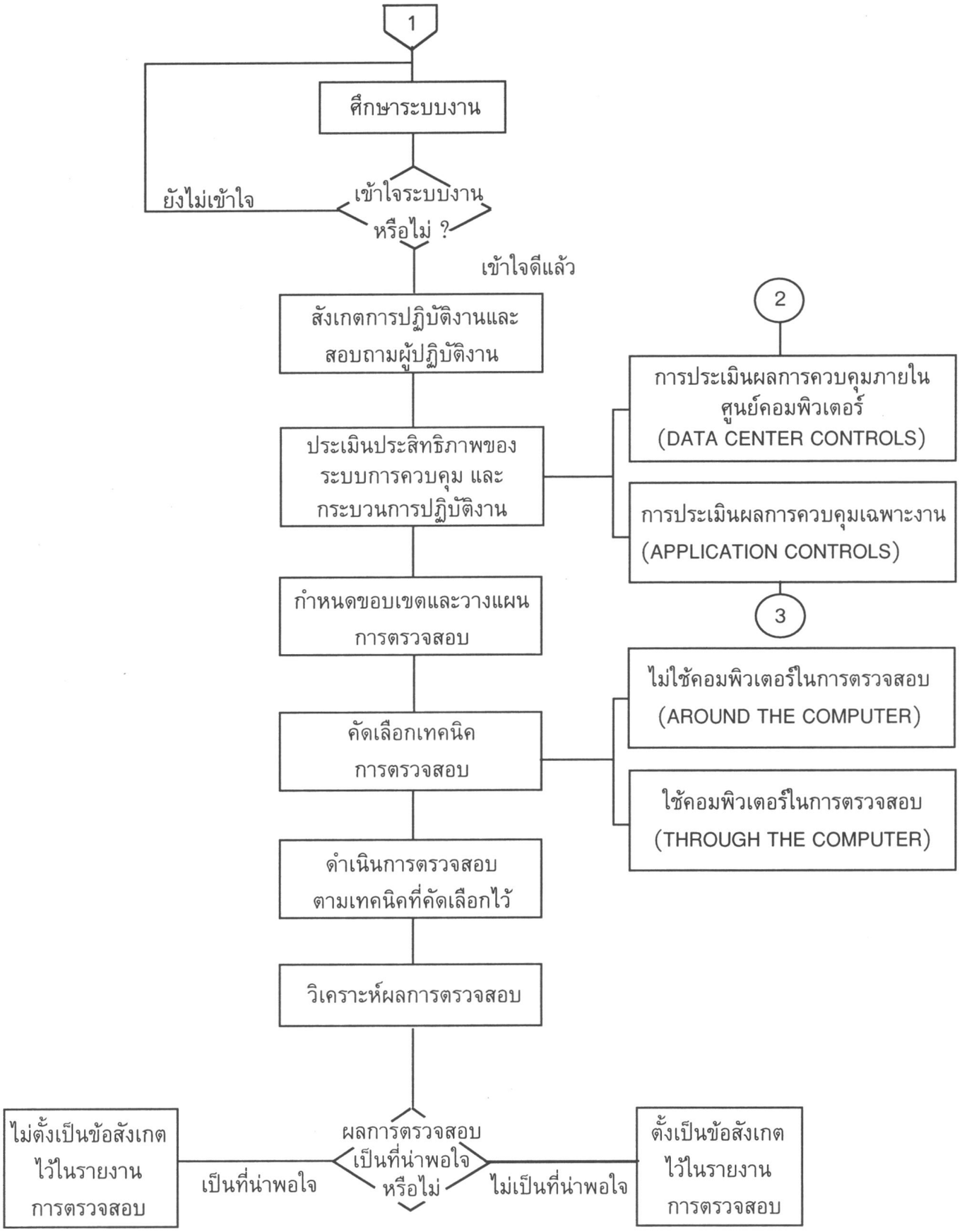
4

แผนภาพแสดงภาพรวม
การตรวจสอบสถาบันการเงินที่ใช้คอมพิวเตอร์

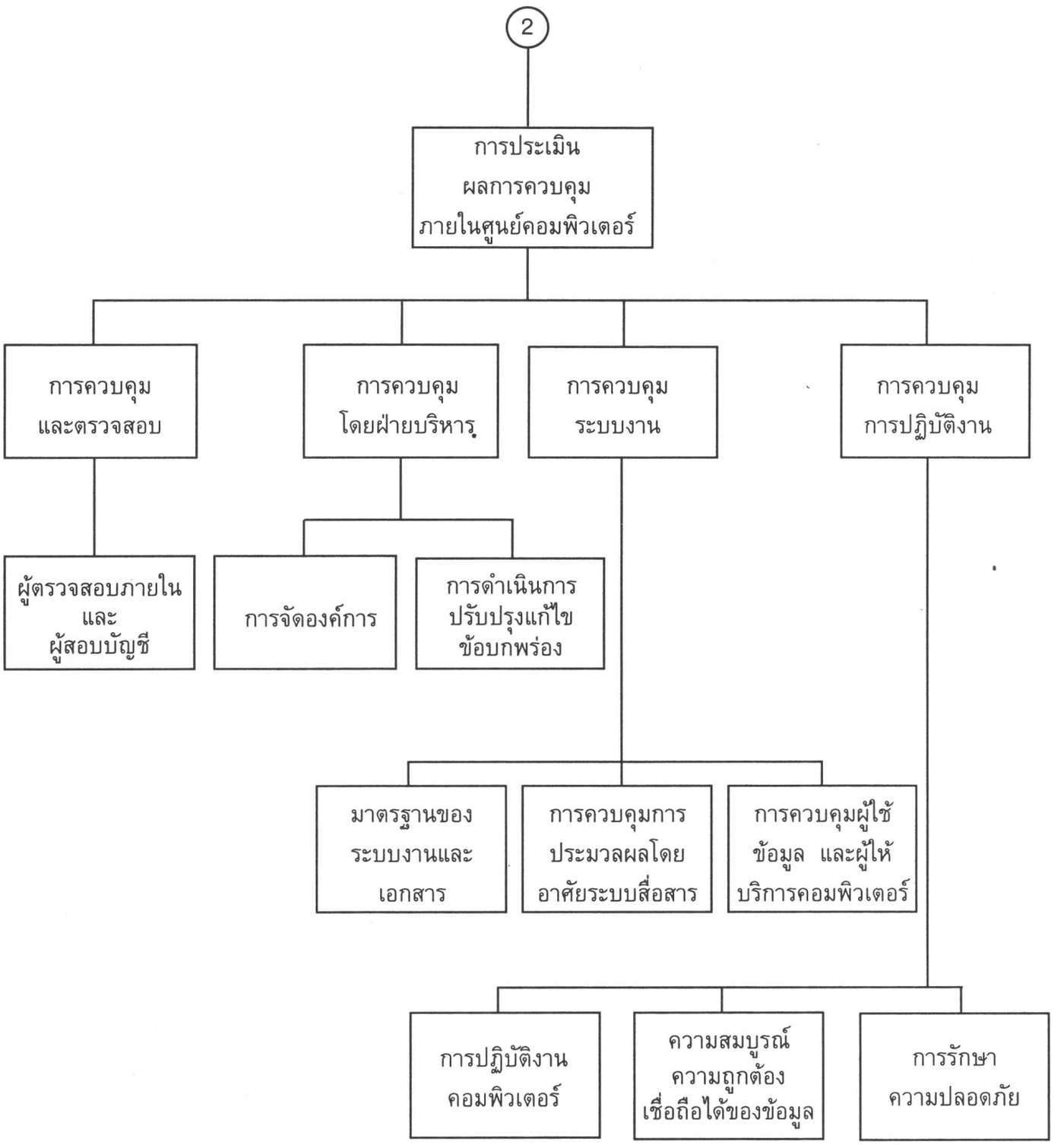
แผนภาพแสดงภาพรวมการตรวจสอบสถาบันการเงินที่ใช้คอมพิวเตอร์



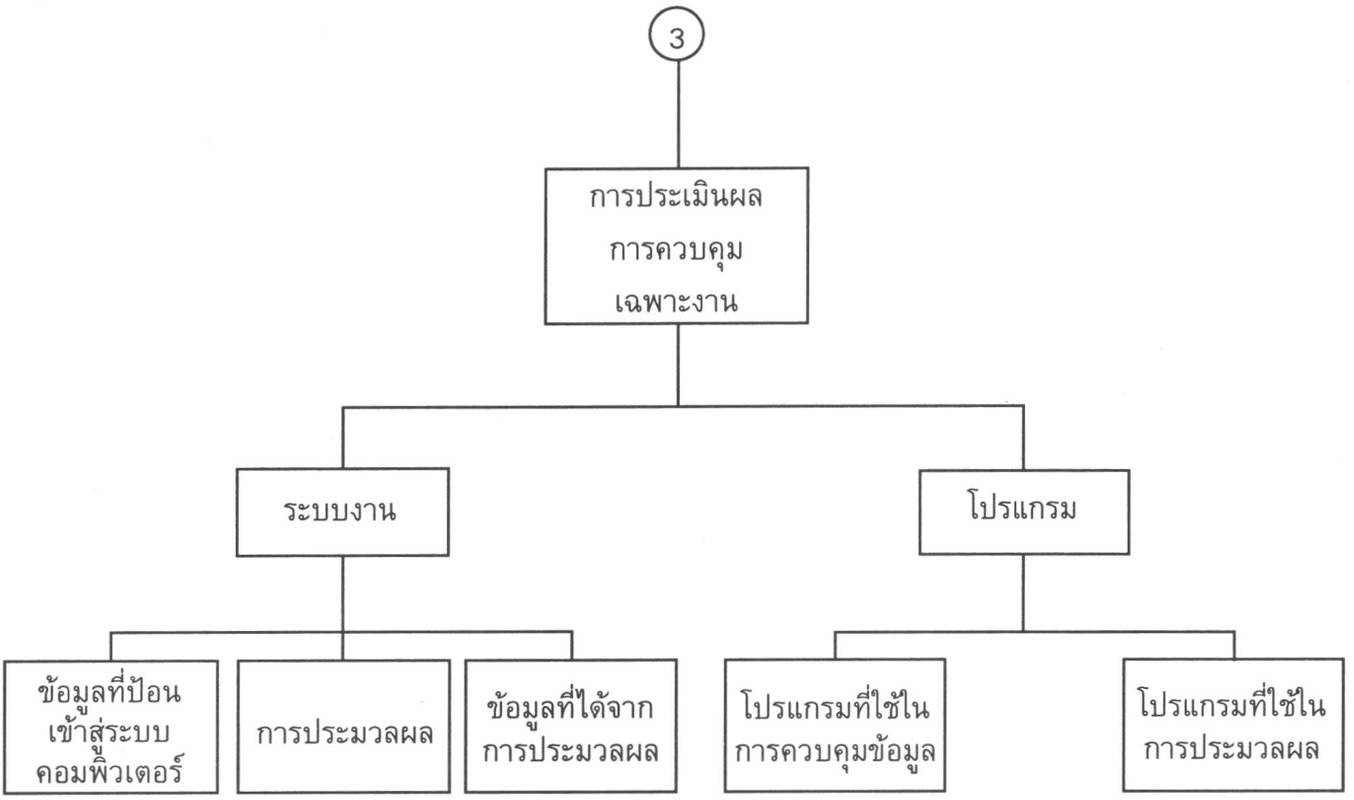
หมายเหตุ : เพื่อให้ผู้บริหารและผู้ตรวจสอบได้เห็นภาพกว้าง ๆ อย่างสังเขป ก่อนพิจารณาเรื่องอื่น ๆ ที่เกี่ยวข้องต่อไป



หมายเหตุ : โปรดดูรายละเอียด แนวการตรวจสอบเรื่องการประเมินผลการควบคุมภายในศูนย์คอมพิวเตอร์ และการควบคุมภายในเฉพาะงานจากแนวคำถามในเรื่องที่เกี่ยวข้องด้วย

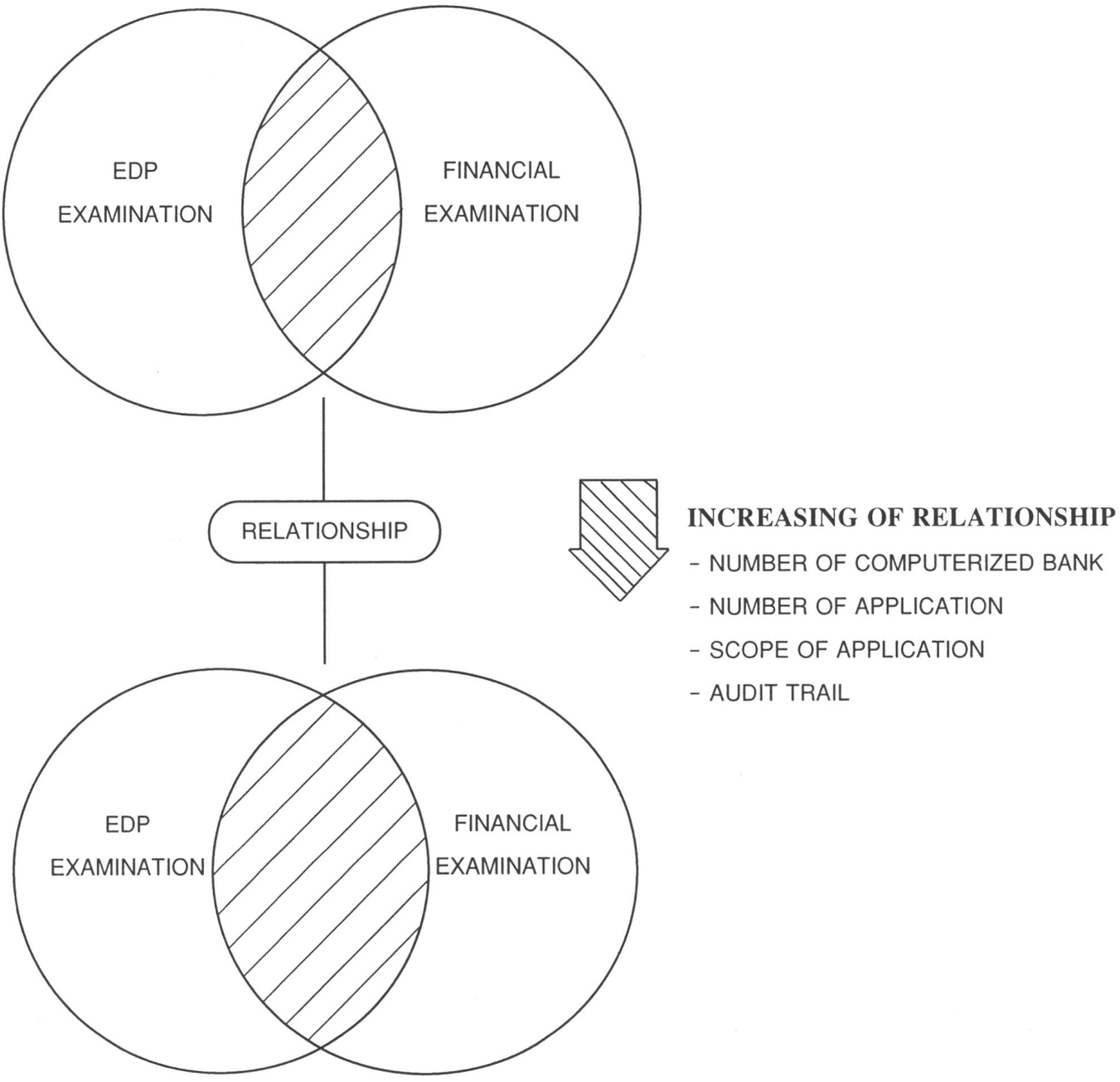


หมายเหตุ : แผนภาพดังกล่าว เป็นการตรวจสอบ Data Center หรือ General Controls ด้านคอมพิวเตอร์ขององค์กรและสถาบันการเงิน ซึ่งส่วนใหญ่จะเป็นหน้าที่ของ Financial Institution's examiner หรือผู้ตรวจการสถาบันการเงินจากทางการและเกี่ยวข้องกับทั้ง External Auditor และ Internal Auditor ซึ่งขึ้นกับเป้าหมายการตรวจสอบของผู้ที่เกี่ยวข้องด้วย



หมายเหตุ : เป็นการตรวจสอบด้าน Applications หรือการควบคุมเฉพาะระบบงานที่ตรวจสอบในแต่ละระบบ ซึ่งส่วนใหญ่จะเป็นหน้าที่ของ Internal Auditor และ External Auditor แต่จะเกี่ยวข้องกับผู้ตรวจการจากทางการ เช่น ผู้ตรวจการจากธนาคารแห่งประเทศไทย (examiner) ด้วย โดยเฉพาะอย่างยิ่งหากเป้าหมายการตรวจสอบอยู่ที่การตรวจสอบฐานะและความมั่นคงของสถาบันการเงิน ดังนั้น ความสัมพันธ์ระหว่าง Internal Auditor, External auditor และ Financial examiner จึงขึ้นอยู่กับเป้าหมาย และวัตถุประสงค์ของการตรวจสอบเป็นสำคัญ ดังนั้น ผู้อ่านขอได้โปรดสังเกตถ้อยคำที่ใช้เพื่อทำความเข้าใจในเรื่องที่เกี่ยวข้องด้วย ทางการต้องการให้งานตรวจสอบด้านนี้ (Application Audit) ดูแลกันเองภายในองค์กร เพราะเป็นเรื่องรายละเอียดต่าง ๆ ที่องค์กรควรควบคุมได้อยู่แล้ว แต่งานขั้นตอนนี้จะถูกประเมินประสิทธิภาพโดยทางการ เพื่อกำหนดขอบเขตของการตรวจสอบให้เหมาะสมตามสภาพการณ์ อย่างไรก็ดีการทำความเข้าใจในการตรวจสอบ "งาน" หรือ Application สามารถติดตามได้จากเรื่องที่เกี่ยวข้อง

ความสัมพันธ์ระหว่าง EDP EXAMINATION และ FINANCIAL EXAMINATION

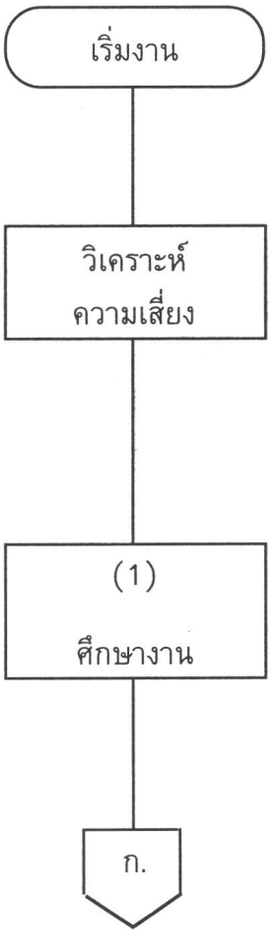


หมายเหตุ : ภาพนี้แสดงความสัมพันธ์ระหว่าง EDP auditor หรือ EDP Examiner ที่เพิ่มขึ้น เมื่อจำนวนองค์กร ระบบงานที่ใช้คอมพิวเตอร์มีมากขึ้น สำหรับเหตุผลอื่นได้กล่าวไว้ในบทต่าง ๆ แล้ว

5

กระบวนการตรวจสอบด้านคอมพิวเตอร์

กระบวนการตรวจสอบ



(1) ศึกษางานก่อนตรวจสอบ

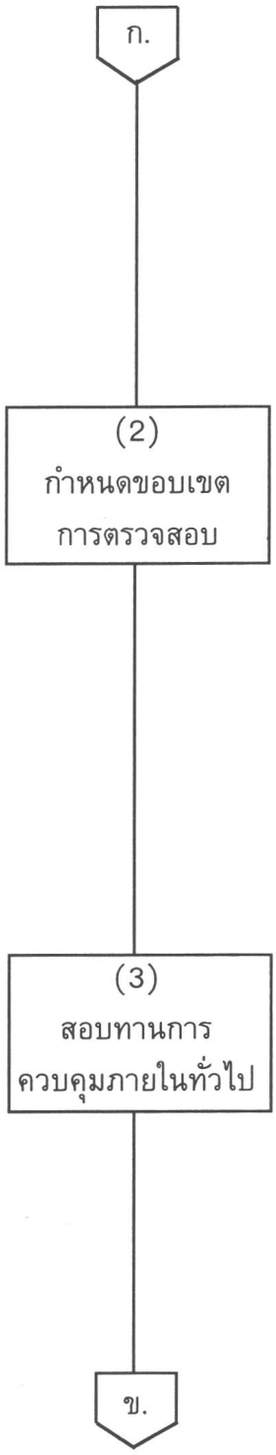
(Preliminary phase of review)

วัตถุประสงค์

เพื่อทำความเข้าใจระบบบัญชีที่ใช้คอมพิวเตอร์ และส่วนที่ไม่ได้ใช้คอมพิวเตอร์ โดยศึกษา

- ทางเดินของรายการและรายงานที่มีความสำคัญ
- ขอบเขตการใช้คอมพิวเตอร์ของฝ่ายบริหาร และงานบัญชีที่มีความสำคัญ





- โครงสร้างพื้นฐานของการควบคุมทางการบัญชี การควบคุมภายในด้านคอมพิวเตอร์ และการควบคุมผู้ใช้ข้อมูล

วิธีการ

โดยการสอบถาม สังเกตการณ์ ศึกษาจากเอกสารที่พอจะหาได้ ติดตามความเคลื่อนไหวของรายการใช้แบบสอบถาม การควบคุมภายใน และ Check list

(2) กำหนดขอบเขตการตรวจสอบ
(Determine scope of audit)

วัตถุประสงค์

- เพื่อประเมินขอบเขตการควบคุมภายในด้านคอมพิวเตอร์ และด้านอื่นๆ
- เพื่อกำหนดขอบเขตการตรวจสอบ

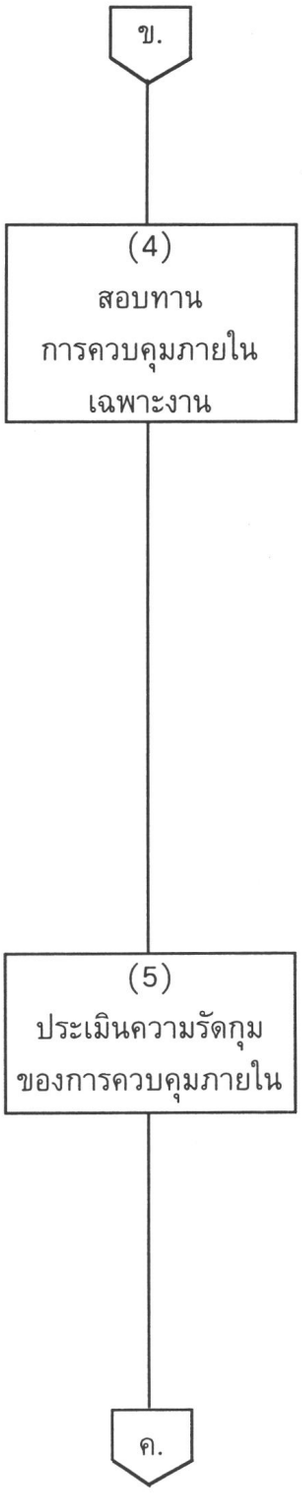
วิธีการ

ขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบ

(3) สอบทานการควบคุมภายในทั่วไป
(Review of general controls)

วัตถุประสงค์

- เพื่อศึกษาการควบคุมภายในทั่วไป และลักษณะการทำงานของการควบคุมภายในทั่วไป
- เพื่อศึกษาความรัดกุมและจุดอ่อนของการควบคุมภายในทั่วไป และผลกระทบที่มีต่อการควบคุมเฉพาะงาน
- พิจารณาถึงความจำเป็นในการทดสอบการควบคุมภายในทั่วไปบางประเภท



วิธีการ

ศึกษาระเบียบข้อบังคับและมาตรฐานการปฏิบัติงานของหน่วยงานคอมพิวเตอร์ สอบถาม และสังเกตการณ์

(4) สอบทานการควบคุมภายในเฉพาะงาน
(Review of application controls)

วัตถุประสงค์

- เพื่อศึกษาการควบคุมภายในเฉพาะงาน และลักษณะการทำงานของการควบคุมภายในเฉพาะงาน
- พิจารณาถึงความจำเป็นในการทดสอบการควบคุมภายในเฉพาะงานบางประเภท

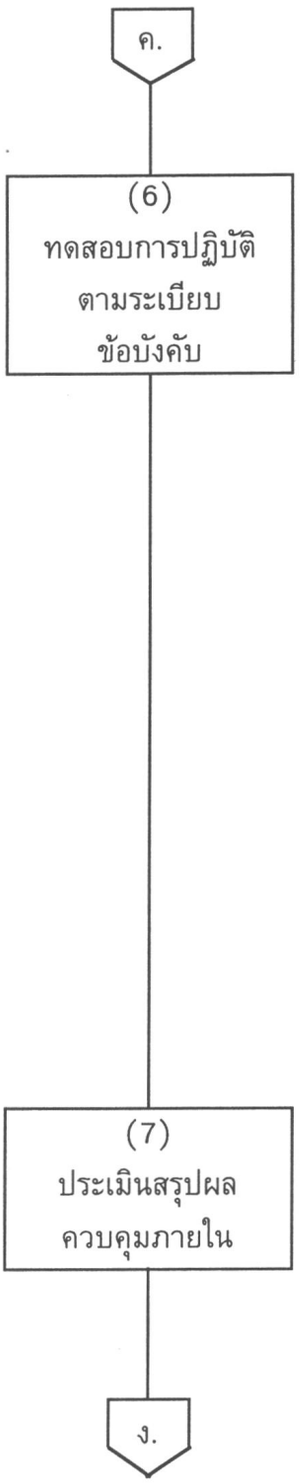
วิธีการ

ศึกษาเอกสารระบบงานและโปรแกรมและระเบียบข้อบังคับ หรือคู่มือปฏิบัติงานของหน่วยงานผู้ใช้ข้อมูล สอบถาม และสังเกตการณ์

(5) ประเมินความรัดกุมของการควบคุมภายในที่สอบทานแล้ว
(Assessment of Controls)

วัตถุประสงค์

- เพื่อพิจารณาว่าข้อผิดพลาดหรือสิ่งผิดปกติที่จะเกิดขึ้นในแต่ละระบบงานเป็นข้อผิดพลาดชนิดใด
- วิธีการควบคุมที่ใช้สามารถป้องกันและค้นหาข้อผิดพลาดได้เพียงใด
- เพื่อประเมินประสิทธิภาพการควบคุมภายในด้านคอมพิวเตอร์ และด้านอื่น ๆ ที่เกี่ยวข้อง



วิธีการ

ขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบ

(6) ทดสอบการปฏิบัติตามระเบียบข้อบังคับหรือข้อกำหนดในการประมวลผลข้อมูล (Test of Compliance)

วัตถุประสงค์

- เพื่อพิจารณาว่ามีการปฏิบัติตามระเบียบข้อบังคับหรือข้อกำหนดในการประมวลผลข้อมูลเพียงใด
- เพื่อหาเหตุผลสนับสนุนก่อนที่จะแน่ใจว่า การควบคุมภายในที่ต้องการทดสอบทำหน้าที่ได้อย่างเหมาะสม
- เพื่อพิจารณาความเหมาะสมของขอบเขตการควบคุมภายในเอกสารหลักฐาน ผู้รับผิดชอบ กำหนดเวลา และวิธีการที่ใช้เพื่อประโยชน์ในการควบคุมภายใน

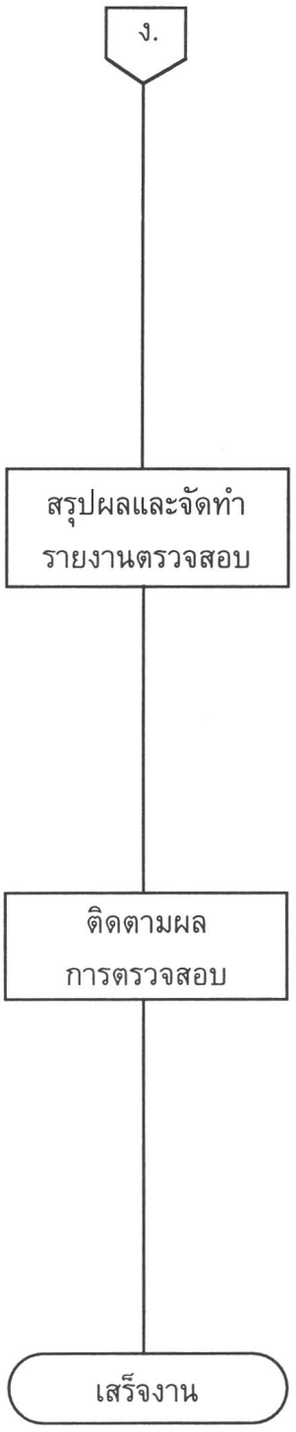
วิธีการ

ตรวจสอบบันทึกการปฏิบัติงาน ทดสอบวิธีการควบคุม สอบถามและสังเกตการณ์

(7) ประเมินสรุปผลการควบคุมภายใน (Evaluation of Controls)

วัตถุประสงค์

- เพื่อพิจารณาว่าข้อผิดพลาดหรือสิ่งผิดปกติที่อาจเกิดขึ้นในแต่ละระบบงานเป็นข้อผิดพลาดชนิดใด
- วิธีการควบคุมที่ใช้สามารถป้องกันและค้นหาข้อผิดพลาดได้เพียงใด



- พิจารณาว่าได้จัดให้มีการควบคุมภายในที่สำคัญไว้หรือไม่ และมีการปฏิบัติตามระเบียบการควบคุมภายในดังกล่าวเป็นที่น่าพอใจเพียงใด
- ประเมินจุดอ่อนและผลกระทบที่มีต่อลักษณะ เวลา และขอบเขตการตรวจสอบ

วิธีการ

ขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบ



6

งานตรวจสอบคอมพิวเตอร์กับผู้บริหาร

งานตรวจสอบคอมพิวเตอร์กับผู้บริหาร

1. วัตถุประสงค์ในการตรวจสอบงานด้านคอมพิวเตอร์

เพื่อประเมินและตรวจสอบการควบคุม "ความเสี่ยง" จากการดำเนินงานด้วยระบบคอมพิวเตอร์ และการรักษาความปลอดภัยต่าง ๆ ที่จะมีผลกระทบต่อประสิทธิภาพการดำเนินงาน ความมั่นคง ความเชื่อถือได้ของการควบคุมภายใน ซึ่งมีผลต่อความถูกต้องของข้อมูลทางการเงินและระบบงานโดยทั่วไปขององค์กรที่ใช้คอมพิวเตอร์

2. ข้อควรทราบสำหรับผู้บริหารในงานตรวจสอบคอมพิวเตอร์

(1.) ผู้บริหารควรกำหนดหน้าที่และความรับผิดชอบของหน่วยงานตรวจสอบคอมพิวเตอร์ รวมทั้งผู้ตรวจสอบภายในแต่ละตำแหน่ง เป็นลายลักษณ์อักษรให้ชัดเจน

(2.) เนื่องจากผู้ตรวจสอบด้านคอมพิวเตอร์จะต้องมีความรู้ความสามารถเกี่ยวกับบัญชี การประมวลผลข้อมูล และเทคนิคการตรวจสอบ จึงควรมีแผนฝึกอบรมผู้ตรวจสอบอย่างต่อเนื่อง

(3.) ควรรายงานผลการตรวจสอบให้แก่คณะกรรมการบริหารหรือกรรมการผู้จัดการโดยตรง เพื่อความเป็นอิสระของผู้ตรวจสอบ

(4.) คณะกรรมการบริหารควรพิจารณาให้ความเห็นชอบเกี่ยวกับมาตรฐาน และวิธีการตรวจสอบที่ระบุไว้ในคู่มือการตรวจสอบเพื่อให้ครอบคลุมงานทุกด้าน นอกจากนี้จะได้มีหลักเกณฑ์ในการประเมินผลการตรวจสอบ

(5.) ผู้บริหารอยากทราบว่าผู้ปฏิบัติงานทั้งในศูนย์คอมพิวเตอร์ และหน่วยงานผู้ใช้ (User) ได้ปฏิบัติตามมาตรฐานหรือระเบียบปฏิบัติที่กำหนดไว้หรือไม่ และหากเรื่องใดยังไม่มีมาตรฐานหรือระเบียบปฏิบัติกำหนดไว้ก็จะได้พิจารณากำหนดเป็นมาตรฐานหรือระเบียบปฏิบัติต่อไป

(6.) ผู้บริหารอยากทราบว่าหน่วยงานตรวจสอบคอมพิวเตอร์ได้ปฏิบัติงานบรรลุเป้าหมายที่กำหนดไว้ในแต่ละปีหรือไม่ ถ้าไม่บรรลุ เพราะสาเหตุใด และในปีต่อไปจะมีแผนงานตรวจสอบอะไรบ้าง

(7.) ผู้ตรวจสอบคอมพิวเตอร์กับผู้ตรวจสอบด้าน Financial มีการแบ่งหน้าที่และขอบเขตการตรวจสอบกันอย่างไร ตลอดจนการประสานงานการตรวจสอบของผู้ตรวจสอบทั้งสอง

(8.) ควรทราบวัตถุประสงค์ในการตรวจสอบของผู้ตรวจสอบภายใน คือ

- เพื่อให้แน่ใจว่า ในองค์การนั้นมีและใช้ระบบการควบคุมที่เหมาะสม
- การใช้ทรัพย์สินมีประสิทธิภาพหรือไม่
- มีการป้องกันรักษาทรัพย์สินขององค์การอย่างเหมาะสมหรือไม่
- ระบบการบันทึกข้อมูลและการจัดทำงบการเงินถูกต้องและเชื่อถือได้

โดยเน้นว่าวิธีและเทคนิคที่ใช้ในการตรวจสอบคอมพิวเตอร์ต้องเปลี่ยนแปลงไปจากระบบเดิม (Manual System) อันเนื่องจากระบบการบันทึกบัญชีและการควบคุมได้เปลี่ยนแปลงไปโดยสิ้นเชิง

(9.) ควรมีรายงานสำหรับพนักงานชั้นบริหารที่ใช้ในการควบคุม และตรวจสอบการปฏิบัติงานประจำวัน เช่น Console log, Exception Report (เช่น การแก้ไขอัตราดอกเบี้ย การเพิ่มวงเงินกู้ยืม การแก้ไขข้อผิดพลาดต่าง ๆ ฯลฯ) เป็นต้น นอกจากนี้ควรมีรายงานผลการปฏิบัติงานของหน่วยงานตรวจสอบภายในประจำเดือนเสนอผู้บริหารทราบด้วย

(10.) ความถูกต้องของข้อมูลหรือผลลัพธ์ จะมีผลกระทบต่อการตัดสินใจของผู้บริหารอย่างมาก ดังนั้นงานตรวจสอบคอมพิวเตอร์จะช่วยทำให้ผู้บริหารแน่ใจว่าข้อมูลหรือผลลัพธ์เหล่านั้นถูกต้องเชื่อถือได้

(11.) ก่อนที่จะนำคอมพิวเตอร์มาใช้งาน จำเป็นต้องศึกษาความเหมาะสมหรือความเป็นไปได้ (Feasibility Study) ซึ่งหากผู้พิจารณามีความต้องการจะใช้คอมพิวเตอร์อยู่แล้ว ก็อาจทำให้การพิจารณาไม่รอบคอบเท่าที่ควร ดังนั้น ถ้าหากมีผู้ตรวจสอบมาช่วยพิจารณากลั่นกรองอีกครั้งหนึ่ง ก็จะทำให้การพิจารณาตัดสินใจใช้คอมพิวเตอร์มีความรอบคอบรัดกุมยิ่งขึ้น

(12.) ผู้ตรวจสอบคอมพิวเตอร์จะตรวจสอบกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลนับตั้งแต่การออกแบบระบบงาน การจัดทำโปรแกรม การทดสอบโปรแกรม การเตรียมข้อมูล การประมวลผลข้อมูล ตลอดจนการจัดส่งรายงานให้หน่วยงานผู้ใช้ เพื่อให้ทุกขั้นตอนของแต่ละกิจกรรมมีการควบคุมภายในที่ดี

(13.) ผู้ตรวจสอบจะต้องให้ความสำคัญกับเรื่องเอกสารประกอบระบบงานและโปรแกรม รวมทั้งคู่มือสำหรับผู้ใช้งาน (User Manual) เพื่อให้ผู้ปฏิบัติงานมีแนวทางหรือมาตรฐานในการปฏิบัติงาน และใช้เป็นเอกสารสำหรับการอบรมพนักงานด้วย นอกจากนี้ ยังเป็นประโยชน์ในการบำรุงรักษาระบบงานและโปรแกรมในอนาคต

(14.) การรักษาความปลอดภัยของศูนย์คอมพิวเตอร์ ซึ่งครอบคลุมเรื่องสถานที่ตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ แฟ้มข้อมูล โปรแกรม และเอกสารต่างๆ เป็นอีกเรื่องหนึ่งที่มีความสำคัญอย่างยิ่ง ผู้ตรวจสอบจะต้องวิเคราะห์ความเป็นไปได้หรือโอกาสของภัยต่าง ๆ ทั้งที่เกิดขึ้นจากธรรมชาติและการกระทำของมนุษย์ และประเมินความเสียหายที่จะได้รับหากเกิดภัยเหล่านั้น พร้อมทั้งหาวิธีการหรือมาตรการป้องกันและแก้ไข เพื่อมิให้เกิดภัยเหล่านั้นขึ้นได้ หรือหากเกิดขึ้นก็จะได้รับผลเสียหายหรือกระทบกระเทือนน้อยที่สุด

(15.) นอกจากผู้บริหารจะให้ความสนใจงานตรวจสอบคอมพิวเตอร์ของผู้ตรวจสอบภายในแล้ว ควรให้ความสนใจงานตรวจสอบคอมพิวเตอร์ของผู้สอบบัญชีและผู้ตรวจการธนาคารพาณิชย์อีกด้วย เพราะอาจมีบางเรื่องหรือบางประเด็นที่ผู้ตรวจสอบภายในไม่ได้ตรวจสอบ แต่ผู้สอบบัญชีและผู้ตรวจการธนาคารพาณิชย์ได้ตรวจสอบทำให้ผู้บริหารได้ทราบเรื่องต่าง ๆ ที่น่าสนใจ ซึ่งยังไม่เคยทราบเพิ่มขึ้น และหากเรื่องใดมีผลเสียหายก็จะได้รีบหาทางปรับปรุงแก้ไขโดยเร็ว

(16.) ปัจจุบันเป็นยุค Electronic Banking คือ ธนาคารพาณิชย์ส่วนใหญ่ได้แข่งขันกันบริการลูกค้าด้วยอุปกรณ์อิเล็กทรอนิกส์ทันสมัย โดยมีเครื่องคอมพิวเตอร์ที่สำนักงานใหญ่เป็นตัวหลัก แม้ว่าบางครั้งจะรวมตัวกันเป็นกลุ่ม (Pool) เพื่อให้บริการลูกค้าก็ตาม เช่น ATM, POS เป็นต้น ดังนั้น ในเรื่องความสะดวก รวดเร็ว ปลอดภัย และถูกต้อง จึงเป็นปัจจัยสำคัญที่จะทำให้ลูกค้าพึงพอใจต่อการบริการดังกล่าว ผู้ตรวจสอบภายในจะเข้ามาตรวจสอบในเรื่องเหล่านี้ และรายงานให้ผู้บริหารทราบ

(17.) อาชญากรรมทางคอมพิวเตอร์ซึ่งเคยเกิดขึ้นในต่างประเทศหลายครั้งหลายหนและแต่ละครั้งเป็นจำนวนเงินมหาศาล เป็นตัวอย่างอันดีที่ผู้บริหารธนาคารพาณิชย์ในประเทศไทยควรสังวรณ์ไว้ เพราะอาชญากรไม่ว่าจะเป็นพนักงานของธนาคารหรือบุคคลภายนอกก็ตาม ที่มีความรู้เกี่ยวกับระบบคอมพิวเตอร์ และรู้จุดอ่อนในระบบงานเป็นอย่างดี และหากการควบคุมภายในไม่เพียงพอแล้ว บุคคลเหล่านั้นก็จะใช้ประโยชน์จากจุดอ่อนนั้นประกอบอาชญากรรมทางคอมพิวเตอร์ได้ ซึ่งจะทำให้ธนาคารและหรือลูกค้าได้รับความเสียหาย ดังนั้น หากมีการตรวจสอบงานคอมพิวเตอร์ย่อมจะพบจุดอ่อนในระบบงานได้ และหาทางป้องกันมิให้เกิดอาชญากรรมดังกล่าว

(18.) การที่ธนาคารมีศูนย์คอมพิวเตอร์เพื่อพัฒนาระบบงานและประมวลผลงาน และมีหน่วยงานตรวจสอบคอมพิวเตอร์เพื่อตรวจสอบระบบงานคอมพิวเตอร์ว่า มีความถูกต้องน่าเชื่อถือเพียงใด และตรวจสอบการดำเนินงานด้านคอมพิวเตอร์ของศูนย์คอมพิวเตอร์ว่ามีการควบคุมเพียงพอหรือไม่ ผู้บริหารระดับสูงไม่ควรปล่อยให้หน่วยงานทั้งสองทำงานไปโดยลำพัง แต่ควรที่จะเข้ามามีบทบาทมากยิ่งขึ้น เพื่อช่วยกำหนดแนวทางหรือชี้นำต่อไป อย่างไรก็ดีการที่ผู้บริหารจะมีบทบาทตามที่กล่าวได้ ผู้บริหารจะต้องมีความรู้ความเข้าใจเกี่ยวกับระบบคอมพิวเตอร์และงานตรวจสอบคอมพิวเตอร์พอสมควร กล่าวคือ จะต้องมีการอบรมพนักงานบริหารระดับสูงเช่นเดียวกับที่มีการให้การอบรมแก่พนักงานของศูนย์คอมพิวเตอร์ และหน่วยงานตรวจสอบภายใน แต่เนื้อหาสาระของวิชาที่อบรมอาจจะแตกต่างกันบ้างตามความเหมาะสม

(19.) เนื่องจากปัจจุบันบุคลากรด้านคอมพิวเตอร์รวมทั้งผู้ตรวจสอบภายในด้วย ยังมีจำนวนจำกัดโดยเฉพาะอย่างยิ่งการพัฒนาตัวผู้ตรวจสอบต้องใช้เวลาอย่างน้อย 2 ปีจึงจะสามารถทำงานได้ ซึ่งธนาคารต้องใช้เงินลงทุนจำนวนมาก ดังนั้นหากมีการลาออกของพนักงานดังกล่าวเป็นจำนวนมาก จะทำให้ธนาคารสูญเปล่าในการลงทุนพัฒนาทรัพยากรบุคคล ฉะนั้น เพื่อป้องกันมิให้ทรัพยากรบุคคลไหลออกไปสู่ภายนอก ธนาคารควรพิจารณาให้ผลตอบแทนการทำงานแก่พนักงานทางด้านคอมพิวเตอร์ในลักษณะที่ก่อให้เกิดแรงจูงใจต่าง ๆ

(20.) โดยที่หน่วยงานตรวจสอบภายในเปรียบเสมือนแขนขาของผู้บริหาร ในการสอดส่องดูแลการปฏิบัติงานของพนักงาน แล้วรายงานข้อบกพร่องหรือข้อสังเกต พร้อมทั้งข้อแนะนำให้ผู้บริหารระดับสูงทราบ จึงเป็นประโยชน์อย่างยิ่งสำหรับผู้บริหาร ผู้บริหารระดับสูงจึงควรสนับสนุนหน่วยงานที่กล่าวทุกวิถีทางที่จะทำได้ ทั้งด้านงบประมาณ กำลังคน เครื่องมืออุปกรณ์ต่าง ๆ ที่จำเป็นต้องใช้ ตลอดจนช่วยแก้ไขปัญหาอุปสรรคต่าง ๆ ที่อาจจะเกิดขึ้นกับหน่วยงานตรวจสอบภายใน เพื่อให้งานตรวจสอบดำเนินไปอย่างราบรื่นและมีประสิทธิภาพ



7

การตรวจสอบองค์กรที่ใช้เครื่องคอมพิวเตอร์

การตรวจสอบองค์กรที่ใช้เครื่องคอมพิวเตอร์

เนื่องจากขอบเขตการปฏิบัติงานของธุรกิจต่าง ๆ ในปัจจุบัน ได้ขยายออกไปอย่างกว้างขวาง ทั้งปริมาณงานและเทคนิคการดำเนินงาน ผู้บริหารจึงจำเป็นต้องวางวิธีการควบคุมอย่างใดอย่างหนึ่ง เพื่อป้องกันมิให้เกิดมีการเสียหายแก่สินทรัพย์ขององค์กร และในขณะเดียวกันก็ให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ การควบคุมดังกล่าวเรียกกันว่า การควบคุมภายใน

การควบคุมภายใน หมายถึง วิธีการต่าง ๆ ที่กำหนดไว้ในพิธีการปฏิบัติงานของแต่ละหน่วยงาน รวมทั้งวิธีการอื่น ๆ ที่องค์กรจัดให้มีขึ้น โดยมีวัตถุประสงค์เพื่อ

1. ป้องกัน ควบคุม และเก็บรักษาสินทรัพย์
2. ทำให้มั่นใจในความถูกต้อง เชื่อถือได้ของข้อมูล
3. ส่งเสริมให้การใช้ทรัพยากรขององค์กรเป็นไปอย่างมีประสิทธิภาพ และมีประสิทธิผล
4. สนับสนุนให้การดำเนินงานเป็นไปตามนโยบายที่กำหนดไว้
5. ลดการทำงานผิดพลาดที่เกิดจากความตั้งใจและไม่ตั้งใจ

ในปัจจุบันองค์กรต่าง ๆ ได้นำอุปกรณ์คอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลกันอย่างแพร่หลาย ถึงแม้วัตถุประสงค์ในการควบคุมภายในจะไม่เปลี่ยนแปลง แต่วิธีการควบคุมภายในบางด้านอาจจะแตกต่างจากเดิมไปบ้าง เราอาจแบ่งการควบคุมภายในด้านคอมพิวเตอร์ได้ดังนี้ คือ

1) ด้านการจัดองค์กรของศูนย์คอมพิวเตอร์

ศูนย์คอมพิวเตอร์ควรเป็นส่วนงานอิสระขึ้นตรงต่อผู้บริหารระดับสูง และมีการแบ่งแยกงานและหน้าที่ของแต่ละหน่วยงานภายในศูนย์ และมีรายงานผลการปฏิบัติงานทุกระยะต่อผู้บริหาร

2) ด้านการรักษาความปลอดภัยอุปกรณ์ในระบบคอมพิวเตอร์

การเลือกที่ตั้งของศูนย์คอมพิวเตอร์ ควรหลีกเลี่ยงสถานที่มีน้ำท่วมขังและมีการก่อสร้าง เพื่อป้องกันความผิดพลาดที่อาจเกิดขึ้นจากแรงสั่นสะเทือน และมีการควบคุมทางกายภาพ ติดตั้งอุปกรณ์ดับเพลิง สัญญาณเตือนภัย ระบบการจ่ายกระแสไฟฟ้าสำรอง ตลอดจนควบคุมอุณหภูมิ ความชื้น

3) ด้านการรักษาความปลอดภัยของการใช้วัสดุและข้อมูล

เพื่อให้สามารถรักษาความลับของข้อมูล ต้องป้องกันการเข้าถึงวัสดุอุปกรณ์และแฟ้มข้อมูล โปรแกรม ทั้งชุดที่ใช้ปฏิบัติงานจริงและชุดสำรองจากบุคคลผู้ไม่มีอำนาจ โดยกำหนดระเบียบปฏิบัติให้มีการควบคุมทางกายภาพรหัส password และตรวจสอบรายงาน log ต่าง ๆ นอกจากนี้ต้องมีระบบการ Back up ข้อมูลสำรองไว้ใช้ในกรณีข้อมูลเสียหายด้วย

4) ด้านพนักงาน

ควรจัดให้มีนโยบายด้านบุคคลในเรื่องการคัดเลือกพนักงาน การฝึกอบรม การลาพักผ่อน การหมุนเวียนสับเปลี่ยนงาน การแบ่งแยกหน้าที่ความรับผิดชอบ การเลื่อนตำแหน่ง ตลอดจนการลาออก/เลิกจ้าง

5) ด้านการพัฒนาระบบงาน

เพื่อให้การบริหารโครงการพัฒนาระบบงานบรรลุเป้าหมาย มีการควบคุมภายในเฉพาะงานนั้นเหมาะสม และสามารถควบคุมค่าใช้จ่ายและเวลาที่ใช้ในการพัฒนาได้ ควรมีการควบคุมวงจรการพัฒนาระบบงาน มาตรฐานการพัฒนาระบบงาน การวัดความก้าวหน้าของโครงการในแต่ละขั้นตอน วิธีการควบคุมและตรวจเช็คการตรวจรับระบบงานโดยผู้ใช้ข้อมูลและฝ่ายตรวจสอบ การทำ Parallel Run การแก้ไขโปรแกรม ตลอดจนการจัดทำเอกสารสนับสนุนการปฏิบัติงานให้สมบูรณ์และทันเวลาอยู่เสมอ

6) ด้านการประมวลผลข้อมูล

เพื่อให้มั่นใจว่ามีการควบคุมอย่างเพียงพอในการกำหนดขั้นตอนการปฏิบัติงาน การนำข้อมูลเข้าเพื่อประมวลผล และการใช้งานอุปกรณ์/เครื่องคอมพิวเตอร์ ต้องมีการจัดทำตารางการปฏิบัติงาน การควบคุมข้อมูลนำเข้า เอกสารข้อมูลเบื้องต้น การสื่อสารข้อมูล การกระทบยอดข้อมูล และการแก้ไขข้อมูลแต่ละประเภทตลอดจนการจัดส่งรายงานข้อมูลผลลัพธ์ที่ได้

7) ด้านการป้องกันการหยุดชะงักในการดำเนินงาน

ในกรณีเกิดเหตุฉุกเฉิน เพื่อความปลอดภัยของพนักงานและสินทรัพย์ และมิให้งานหยุดชะงัก องค์กรจะต้องเตรียมแผนฉุกเฉินและแผนการกู้ระบบไว้ล่วงหน้า โดยจัดเตรียมวัสดุอุปกรณ์ทั้ง Hardware Software แฟ้มข้อมูล และเอกสารสนับสนุนการปฏิบัติงานชุดสำรอง พร้อมทั้งวิธีการปฏิบัติงานด้วย โดยต้องมีการฝึกอบรมและทดสอบระบบงานชุดสำรองบ้างเป็นครั้งคราว

การจัดวางระบบการควบคุมภายในเป็นหน้าที่ของผู้บริหารขององค์กร ที่จะต้องดูแลและปรับปรุงแก้ไขให้เหมาะสมอยู่เสมอ เพราะไม่มีระบบการควบคุมภายในใดที่ดีได้ตลอดกาล ดังนั้นจึงจำเป็นอย่างยิ่งที่ผู้บริหารจะต้อง

1. กำหนดนโยบายที่แน่นอนและปฏิบัติตามโดยเคร่งครัด
2. ปรับปรุงภาวะการทำงานให้พ้นจากความยุ่งยาก ล้าสมัย หรือไร้เหตุผล
3. สั่งการแก้ไขทันทีในกรณีที่ปรากฏว่ามีข้อบกพร่องเกิดขึ้น

การตรวจสอบภายใน

ระบบการควบคุมภายในขององค์กรจะดีหรือไม่ ขึ้นอยู่กับการให้ความร่วมมือและรับฟังข้อคิดเห็นเสนอแนะของผู้ตรวจสอบภายใน เพราะผู้ตรวจสอบภายในเป็นบุคคลสำคัญของระบบการควบคุมภายใน ในฐานะเป็นผู้ประเมินผลการปฏิบัติงาน โดยมีหน้าที่

- ดูแลการดำเนินงานให้เป็นไปตามระเบียบข้อบังคับที่ได้กำหนดไว้
- ตรวจสอบความถูกต้องเชื่อถือได้ของระบบการบันทึกข้อมูลและรายงานทางการเงิน
- สอบหาข้อเท็จจริงเมื่อมีการปฏิบัติงานบกพร่องหรือเกิดการทุจริต
- ทบทวนและให้ข้อเสนอแนะปรับปรุงวิธีการปฏิบัติงาน หรือระเบียบคำสั่งที่เห็นว่าไม่รัดกุมและเหมาะสมกับการดำเนินงานในปัจจุบัน เพื่อให้การปฏิบัติงานรัดกุม และเป็นไปอย่างมีประสิทธิภาพ

จะเห็นได้ว่าผู้ตรวจสอบภายในก็มีหน้าที่ที่สำคัญในการดำเนินงานขององค์กร ดังนั้นผู้บริหารควรให้ความสำคัญกับงานตรวจสอบภายใน โดยการ

- จัดโครงสร้างงานตรวจสอบภายในให้มีความเป็นอิสระ ขึ้นตรงต่อผู้บริหารระดับสูง
- คัดเลือกผู้ตรวจสอบภายในที่มีคุณสมบัติเหมาะสม ได้แก่ มีความรู้และประสบการณ์ในด้านคอมพิวเตอร์ การตรวจสอบ การบัญชี และมีสัญชาติญาณในการตรวจสอบ
- จัดให้มีการฝึกอบรมผู้ตรวจสอบให้มีความรู้เกี่ยวกับ Technology ที่ก้าวหน้าอย่างรวดเร็ว
- จัดให้มีคู่มือการตรวจสอบ โดยระบุถึงนโยบาย มาตรฐาน และวิธีการตรวจสอบ และให้ผู้รับผิดชอบขององค์กรเป็นผู้พิจารณาก่อนนำใช้งาน
- ติดตามผลการแก้ไขตามข้อแนะนำของผู้ตรวจสอบภายใน



8

สรุปหลักการวิเคราะห์ความเสี่ยง เพื่อการตรวจสอบงานด้านคอมพิวเตอร์

สรุปหลักการวิเคราะห์ความเสี่ยง เพื่อการตรวจสอบงานด้านคอมพิวเตอร์

1. บทนำ

การตรวจสอบโดยไม่มีการวางแผนและกำหนดวิธีการตรวจสอบ (Planning and Programming) ไว้ล่วงหน้าเป็นสิ่งที่อันตรายอย่างยิ่ง ผลเสียที่เห็นได้ชัดเจนมี 2 ประการ คือ

(1) ไม่สามารถตรวจพบข้อผิดพลาดและผลกระทบต่อระบบงานและฐานะทางการเงินในปัจจุบันและในอนาคตได้ หรือที่ร้ายแรงกว่าก็คือ การทุจริต

(2) ใช้เวลาและแรงงานในการตรวจสอบค่อนข้างมาก ซึ่งจะส่งผลต่อการรายงานการตรวจสอบและความถี่ในการตรวจสอบ

การวางแผนการตรวจสอบแม้จะเป็นสิ่งที่มีประโยชน์ แต่ก็ไม่ใช่จะทำได้อย่างง่าย ๆ ปัญหาที่สำคัญก็คือทำอย่างไรจึงจะสามารถกำหนดจุดหรือเรื่องที่ควรตรวจสอบได้อย่างเหมาะสมและมีประสิทธิภาพ เนื่องจากธุรกิจบางองค์กรประกอบด้วยกิจกรรมมากมาย และมีความสำคัญไม่เท่าเทียมกัน การตรวจสอบให้ได้ทุกเรื่องจึงอาจกล่าวได้ว่าเป็นเหตุสุดวิสัย และหากดึงดันที่จะทำให้ได้ก็จะมีผลต่อคุณภาพของการตรวจสอบ ซึ่งถือว่าเป็นสิ่งสำคัญยิ่งกว่าปริมาณการตรวจสอบ ดังนั้น จึงกล่าวได้ว่าในการวางแผนการตรวจสอบ ควรมีเฉพาะเรื่องที่สำคัญมากเท่านั้น

2. หลักการวิเคราะห์ความเสี่ยง

การวัดความสำคัญของกิจกรรมหรือเรื่องที่ควรตรวจสอบประการหนึ่งก็คือ การพิจารณาผลกระทบต่อฐานะการเงินและการดำเนินงานขององค์กรนั้น ๆ ผลกระทบที่ว่านี้ถ้าจะกำหนดให้แคบลงไปอีกก็คือ เหตุการณ์ที่ไม่พึงปรารถนา และความเสียหายที่จะติดตามมากับเหตุการณ์นั้น

ดังนั้น จึงอาจสรุปได้ว่า ถ้าเราสามารถทราบหรือวิเคราะห์ให้ได้มาซึ่งเหตุและผลเสียหาย หรือที่เรียกว่าการวิเคราะห์ความเสี่ยง (Risk Analysis) ของธุรกิจหรือการประกอบการใดแล้ว เราก็จะสามารถวางแผนและกำหนดวิธีการตรวจสอบได้อย่างเหมาะสมและมีประสิทธิภาพ ในวงการตรวจสอบที่เป็นระบบในปัจจุบันการวิเคราะห์ความเสี่ยงได้เข้ามามีบทบาทอย่างจริงจังในการวางแผนและกำหนดวิธีการตรวจสอบ





3. การวิเคราะห์ความเสี่ยงด้านคอมพิวเตอร์

ในการตรวจสอบองค์กรด้านคอมพิวเตอร์ก็เช่นเดียวกัน หากผู้ตรวจสอบสามารถศึกษาและวิเคราะห์จนทราบว่าอะไรคือสาเหตุ และความเสียหายที่อาจเกิดกับระบบคอมพิวเตอร์และระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ขององค์กร โดยทั่วไป ผู้ตรวจสอบก็จะสามารถวางแผนและกำหนดวิธีการตรวจสอบได้อย่างเหมาะสมและมีประสิทธิภาพ โดยแยกการตรวจสอบเป็น 2 ด้าน คือ การตรวจสอบระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ (Computer Application System) กับการตรวจสอบระบบคอมพิวเตอร์หรือการตรวจสอบทั่วไป (General Controls)

4. การตรวจสอบระบบงานคอมพิวเตอร์

4.1 การวิเคราะห์ความเสี่ยง

วัตถุประสงค์

ก. เพื่อให้ทราบระบบงานที่มีความเสี่ยงต่อความเสียหาย เช่น

1) มีข้อบังคับของทางราชการ
2) มีผลกระทบต่อฐานะการเงิน
3) มีปริมาณงานมาก ซึ่งอาจก่อให้เกิดข้อผิดพลาดได้มาก

ข. เพื่อให้ทราบขั้นตอนภายในระบบงานที่เสี่ยงต่อความเสียหาย หากมีการควบคุมไม่เพียงพอ

ค. เพื่อเป็นแนวทางในการกำหนดขอบเขตและลำดับความสำคัญในการตรวจสอบ

ง. เพื่อให้ทราบถึงความเสียหายอันอาจเกิดจากระบบงานคอมพิวเตอร์

วิธีการ

ก. ศึกษาเพื่อให้ทราบข้อกำหนดและข้อห้าม ในการประกอบการในองค์กรที่ทำการตรวจสอบ

ข. ศึกษาและวิเคราะห์งบการเงินขององค์กรที่จะเข้าทำการตรวจสอบ เพื่อให้ทราบสัดส่วนของสินทรัพย์และหนี้สินที่สำคัญ ๆ ขององค์กร

ค. คัดเลือกระบบงานที่มีความเสี่ยง โดยพิจารณาจากข้อมูลที่ได้จากการศึกษาในข้อ ก. และ ข.

ง. ศึกษาแฟ้มถาวรและกระดาษทำการของการตรวจสอบครั้งก่อน เพื่อให้ทราบ Background ของระบบงาน โดยเฉพาะขอบเขต Function และการควบคุม

1) ความเสียหายที่อาจเกิดขึ้นได้ทั้งหมด

2) มูลเหตุหรือการปฏิบัติที่นำไปสู่ความเสียหาย

จ. จัดทำตารางความเสี่ยงเพื่อสรุปความสัมพันธ์ระหว่าง (1) และ (2) (ตามตัวอย่างแนบ)

4.2 การวางแผนการตรวจสอบ

จากการวิเคราะห์ความเสี่ยง ทำให้ผู้ตรวจสอบสามารถกำหนดขอบเขตและเป้าหมายในการตรวจสอบเบื้องต้นได้อย่างชัดเจน แต่อาจมีการเปลี่ยนแปลงได้หลังจากที่เข้าไปทำการตรวจสอบระยะหนึ่ง ทั้งนี้เพื่อให้สอดคล้องกับสภาพที่แท้จริงขององค์กร

(1) ขอบเขตการตรวจสอบ

ก. ระบบงานที่ตรวจสอบ โดยพิจารณาจากขนาดของความเสี่ยง

ข. เป้าหมายในการตรวจสอบระบบงาน โดยพิจารณาจากลักษณะของความเสี่ยงภายในระบบงาน เช่น การปฏิบัติฝ่าฝืนกฎหมาย การทุจริต เป็นต้น

(2) จำนวนผู้ตรวจสอบและระยะเวลาที่จะใช้ในการตรวจสอบและจัดทำรายงาน

โดยพิจารณาจากจำนวนคนและเวลาทั้งสิ้นที่ใช้ในการตรวจสอบครั้งก่อน กับปริมาณงานที่คาดว่าจะเพิ่มขึ้นในการตรวจสอบครั้งนี้

4.3 ขั้นตอนการตรวจสอบ

(1) ศึกษาและสำรวจระบบงาน

วัตถุประสงค์

ก. เพื่อให้ทราบขอบเขต ขั้นตอนการปฏิบัติงานและการควบคุม

ข. เพื่อรวบรวมข้อมูลสำหรับการทำการทดสอบ

วิธีการ

ก. ศึกษาเอกสารประกอบระบบงานโดยละเอียด

1) System Description
2) System Flow
3) Functional Flow
4) Program Flow
5) Input Spec.
6) File Spec.
7) Output Spec.
8) User Manuals

ฯลฯ

ข. สอบถามเจ้าหน้าที่ผู้รับผิดชอบขององค์กร และสังเกตการปฏิบัติงาน โดยเฉพาะในกรณีที่เอกสารประกอบระบบงานมีไม่เพียงพอ หรือยากต่อการทำความเข้าใจ

(2) สอบทานการควบคุมภายใน

วัตถุประสงค์

ก. เพื่อศึกษาลักษณะและการทำงานของระบบการควบคุม

ข. เพื่อจัดลำดับความสำคัญของการควบคุม ซึ่งจะทำให้ทราบถึงการควบคุมซึ่งเป็นหลักของระบบงาน

วิธีการ ใช้แบบสอบถามเกี่ยวกับการควบคุมภายใน (ICQ) เป็น Guide ในการศึกษาเอกสารระบบงานและในการสอบถามเจ้าหน้าที่ผู้รับผิดชอบ

(3) ประเมินผลการควบคุมขั้นต้น

วัตถุประสงค์

ก. เพื่อพิจารณาประสิทธิภาพของการควบคุม
ข. เพื่อพิจารณาความเพียงพอ
ค. เพื่อพิจารณาข้อผิดพลาดที่อาจเกิดขึ้น
ง. เพื่อพิจารณาหาวิธีการป้องกันหรือค้นหาข้อผิดพลาด

วิธีการ อยู่ในดุลยพินิจของผู้ตรวจสอบ

(4) ทดสอบการควบคุมหลักตามข้อ (2)

วัตถุประสงค์ เพื่อให้ได้หลักฐานซึ่งแสดงถึงประสิทธิภาพแท้จริงของการควบคุมที่มีอยู่ภายในระบบงาน

วิธีการ

ก. ทดสอบ Manual Controls โดยการติดตามและตรวจสอบเอกสารหลักฐานซึ่งแสดงถึงการควบคุม

ข. ทดสอบ Program Controls โดยการทำ Test data และตรวจสอบความถูกต้องของผลลัพธ์

(5) ประเมินผลขั้นสุดท้าย

วัตถุประสงค์ เพื่อจัดทำรายงานข้อสังเกตและข้อแนะนำที่จะยกขึ้นสรุปผลกับองค์กร

วิธีการ อยู่ในดุลยพินิจของผู้ตรวจสอบ

4.4 การจัดทำรายงานการตรวจสอบ

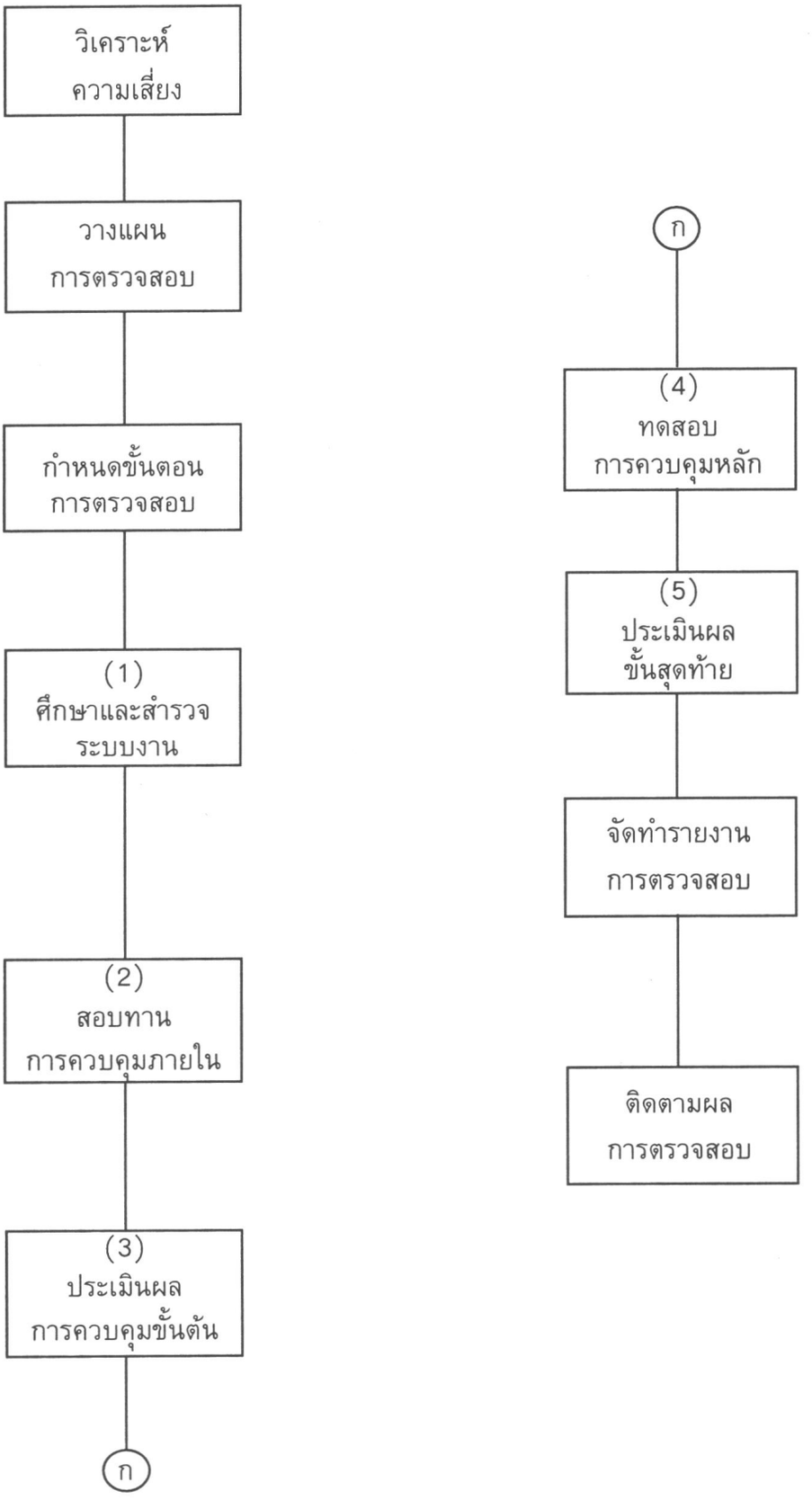
(1) บันทึกสรุปการสนทนา
(2) รายงานการตรวจด้านคอมพิวเตอร์

4.5 การติดตามผลการตรวจสอบ

(1) หนังสือตอบขององค์กร
(2) การตรวจสอบครั้งต่อไป



ผังการตรวจสอบระบบงาน



5. การตรวจสอบทั่วไปด้านคอมพิวเตอร์

5.1 การวิเคราะห์ความเสี่ยง

วัตถุประสงค์

ก. เพื่อให้ทราบถึงความเสียหายทั่วไป อันอาจเกิดจากการใช้ระบบการประมวลผลด้วยคอมพิวเตอร์ ซึ่งไม่เจาะจงว่าจะเกิดกับระบบงานใดระบบงานหนึ่ง

ข. เพื่อเป็นแนวทางในการกำหนดขอบเขตและลำดับความสำคัญในการตรวจสอบ

ค. เพื่อให้ทราบถึงขั้นตอนการปฏิบัติงานที่อาจนำมาซึ่งความเสียหาย

วิธีการ

ก. ศึกษาการดำเนินงานการประมวลผลข้อมูลด้วยคอมพิวเตอร์ในองค์กรและทั่วไป

(1) สำรวจความเสียหายที่อาจเกิดขึ้นได้ทั้งหมด

(2) มูลเหตุหรือการปฏิบัติงานที่นำไปสู่ความเสียหาย

ข. จัดทำตารางความเสี่ยงเพื่อสรุปความสัมพันธ์ระหว่าง (1) และ (2)

5.2 การวางแผนการตรวจสอบ

จากการวิเคราะห์ความเสี่ยง ทำให้ผู้ตรวจสอบสามารถกำหนดขอบเขตและเป้าหมายในการตรวจสอบเบื้องต้นได้อย่างชัดเจน แต่อาจมีการเปลี่ยนแปลงได้หลังจากที่เข้าไปทำการตรวจสอบระยะหนึ่ง ทั้งนี้เพื่อให้สอดคล้องกับสภาพที่แท้จริงขององค์กร

(1) ขอบเขตการตรวจสอบ

ก. การบริหารงาน

ข. การปฏิบัติการศูนย์คอมพิวเตอร์

ค. การพัฒนาระบบงาน

(2) เป้าหมายของการตรวจสอบ เพื่อค้นหาจุดอ่อนและประเมินความเสียหายที่อาจเกิดขึ้น อาทิเช่น การหยุดชะงักของการประกอบการ การทุจริต และการประมวลผลผิดพลาด เป็นต้น

(3) จำนวนผู้ตรวจสอบและเวลาที่จะใช้ในการตรวจสอบและจัดทำรายงาน โดยพิจารณาจากจำนวนคนและเวลาทั้งสิ้นที่ใช้ในการตรวจสอบครั้งก่อน กับปริมาณงานที่คาดว่าจะเพิ่มขึ้นหรือลดลงในการตรวจสอบครั้งนี้



5.3 ขั้นตอนการตรวจสอบ

(1) ศึกษาและสำรวจการดำเนินงานการประมวลผลด้วยคอมพิวเตอร์ขององค์กรที่เข้าทำการตรวจสอบ

วัตถุประสงค์

ก. เพื่อให้ทราบหลักการบริหารงานคอมพิวเตอร์ขององค์กร การปฏิบัติงานและการควบคุมทั่วไปในศูนย์คอมพิวเตอร์ และการพัฒนาระบบงาน

ข. เพื่อรวบรวมข้อมูลสำหรับการทดลอง

วิธีการ

ก. ศึกษาเอกสารขององค์กรโดยละเอียด

1) การจัดการ
   - เป้าหมายและแผนงาน
   - การจัดองค์การและพนักงาน
   - มาตรฐานในการปฏิบัติงานและระบบงาน
   - การตรวจสอบ
2) การปฏิบัติงานคอมพิวเตอร์
3) การพัฒนาระบบงาน
4) การจัดทำข้อมูลที่น่าเชื่อถือได้
5) การรักษาความปลอดภัยของระบบคอมพิวเตอร์

ฯลฯ

ข. สอบถามเจ้าหน้าที่ผู้รับผิดชอบขององค์กร และสังเกตการปฏิบัติงาน โดยเฉพาะในกรณีที่เอกสารขององค์กรมีไม่เพียงพอ หรือยากต่อการทำความเข้าใจ

(2) การสอบทานการควบคุมภายใน

วัตถุประสงค์

ก. เพื่อศึกษาลักษณะและการทำงานของระบบการควบคุม

ข. เพื่อจัดลำดับความสำคัญของการควบคุม ซึ่งจะทำให้ทราบถึงการควบคุมที่เป็นหลักของการดำเนินงานการประมวลผลด้วยคอมพิวเตอร์

วิธีการ ใช้แบบสอบถามเกี่ยวกับการควบคุมภายใน (ICQ) เป็น Guide ในการศึกษาและในการสอบถามเจ้าหน้าที่ผู้รับผิดชอบ

(3) ประเมินผลการควบคุมขั้นต้น

วัตถุประสงค์

ก. เพื่อพิจารณาประสิทธิภาพของการควบคุม
ข. เพื่อพิจารณาความเพียงพอ
ค. เพื่อพิจารณาข้อผิดพลาดที่อาจเกิดขึ้น
ง. เพื่อพิจารณาวิธีการป้องกันหรือค้นหาข้อผิดพลาด

วิธีการ อยู่ในดุลยพินิจของผู้ตรวจสอบ

(4) ทดสอบการควบคุมหลักตามข้อ (2)

วัตถุประสงค์ เพื่อให้ได้หลักฐานซึ่งแสดงถึงประสิทธิภาพที่เป็นจริงของการควบคุม

วิธีการ ทดสอบโดยการติดตามและตรวจสอบเอกสารหลักฐานซึ่งแสดงถึงการควบคุม

(5) ประเมินผลขั้นสุดท้าย

วัตถุประสงค์ เพื่อจัดทำรายงานข้อสังเกตและข้อแนะนำที่จะยกขึ้นสรุปผลกับองค์กร

วิธีการ อยู่ในดุลยพินิจของผู้ตรวจสอบ

5.4 การจัดทำรายงาน

(1) บันทึกการสรุปสนทนา
(2) รายงานการตรวจสอบด้านคอมพิวเตอร์

5.5 การติดตามผลการตรวจสอบ

(1) หนังสือตอบขององค์กร
(2) การตรวจสอบครั้งต่อไป

9

มุมมองของความเสี่ยงด้านคอมพิวเตอร์ จากกิจกรรมที่เกิดขึ้น และลักษณะของการควบคุมภายใน

ความเสี่ยงของการดำเนินงานด้านคอมพิวเตอร์ ที่มีผลกระทบต่อการควบคุม (Control risks)

ความเสี่ยง คือ เหตุการณ์ที่อาจเกิดขึ้นได้ภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลเสียหายหรือสร้างความล้มเหลวให้แก่ส่วนรวมหรือส่วนบุคคล ความเสี่ยงหรือมูลเหตุที่สร้างความเสียหายให้แก่ EDP หมายถึง เหตุการณ์ อุบัติเหตุ หรือการกระทำที่มีผลกระทบในทางที่เสียหายต่อ Computer system และ Data ซึ่งสามารถแบ่งออกเป็นประเภทใหญ่ได้ 6 ประเภท คือ

แนวความคิดในการศึกษาเรื่อง "ความเสี่ยง" ต่าง ๆ จะทำให้มีการวิเคราะห์ผลกระทบจากความเสี่ยงและความเสียหายต่าง ๆ ซึ่งจะทำให้ฝ่ายบริหารสามารถพิจารณาจุด "ควบคุม" และกำหนดระเบียบและกฎเกณฑ์ต่าง ๆ ขององค์กรได้อย่างเหมาะสม ดังนี้

1. ภัยธรรมชาติ เป็นเหตุการณ์ที่ไม่สามารถหลีกเลี่ยงได้ เช่น แผ่นดินไหว พายุ น้ำท่วม เป็นต้น การป้องกันความเสี่ยงประเภทนี้ได้แก่ พยายามหลีกเลี่ยงพื้นที่ที่คาดว่าจะเกิดเหตุที่กล่าว ข้อมูลทางสถิติเกี่ยวกับภัยพิบัติในพื้นที่ตั้ง Computer จึงมีประโยชน์อย่างมากต่อการประเมินเหตุการณ์ หรือกำหนด Emergency & Recovery plans ไว้ล่วงหน้า เพื่อบรรเทาความเสียหาย และกลับคืนสภาพปกติได้รวดเร็ว

2. มนุษย์ เป็นเหตุการณ์ที่เกิดจากการกระทำโดยตั้งใจและไม่ได้ตั้งใจ เช่น เจตนาทำลาย Computer, data, files หรือ programs ให้เสียหายจนใช้งานไม่ได้ หรือการปฏิบัติงานที่ไม่ถูกต้อง ไม่เหมาะสม ก็อาจนำไปสู่ความเสียหายได้เช่นกัน การป้องกันสามารถกระทำได้โดยการสร้างระบบการควบคุมและระเบียบการปฏิบัติงานที่รัดกุม

3. เทคโนโลยี เทคโนโลยีใหม่ ๆ มีส่วนทำให้การปฏิบัติมีประสิทธิภาพและอำนวยความสะดวกรวดเร็วให้แก่ผู้ใช้ แต่ในขณะเดียวกันก็เพิ่มความเสี่ยงใหม่ ๆ ขึ้น เช่น ข้อมูลอาจถูกทำลายหรือเปลี่ยนแปลงโดยสาเหตุจากความวิปริตของ Hardware จนเป็นเหตุให้แผ่น Disk เสียหาย เทคโนโลยีก่อให้เกิดความเสี่ยงทั้งทางด้าน Hardware และ Software ซึ่งอาจจะเนื่องมาจากตัวของมันเอง หรือจากผู้ใช้ที่ไม่มีความสามารถ การป้องกันสามารถทำได้โดยการเข้มงวดการเลือกระบบคอมพิวเตอร์ หรือจัดให้มี Maintenance program เป็นต้น

4. ระเบียบปฏิบัติงาน การปฏิบัติงานที่ไม่เป็นไปตามระเบียบและพิธีการที่กำหนด หรือการกำหนดระเบียบปฏิบัติงานที่ไม่เหมาะสม เป็นเหตุให้เกิดความผิดพลาดในการปฏิบัติงานได้ ซึ่งอาจมีผลกระทบต่อการบริหารและการดำเนินงาน ตลอดจนฐานะและความมั่นคงขององค์กรได้

5. การจัดองค์งาน เกิดจากการมอบหมายอำนาจหน้าที่ ความรับผิดชอบ และการติดต่อประสานงานที่ไม่เหมาะสม เช่น 2 หน่วยงานมีหน้าที่และความรับผิดชอบเหมือนกัน ผลก็คือจะไม่มีหน่วยงานใดปฏิบัติหน้าที่ได้อย่างสมบูรณ์ และก่อให้เกิดการผิดพลาด การป้องกันสามารถทำได้โดยการให้มีข้อบัญญัติเกี่ยวกับอำนาจ หน้าที่ ความรับผิดชอบ และการประสานงานที่ดี จะช่วยลดข้อผิดพลาดลงได้

6. ระบบงาน ความเสี่ยงที่เกิดจากระบบงานมักจะเกี่ยวข้องกับ Functions หรือ Transactions และ Data ของระบบงานนั้น เช่น บันทึกรายการไม่ถูกต้อง เป็นต้น ดังนั้นการป้องกันและการควบคุมในระบบงานนั้น ปกติมักจะรวมอยู่เป็นส่วนหนึ่งของระบบงาน (Computerized Application) อยู่แล้ว เพื่อให้สามารถป้องกันเหตุร้ายหรือค้นพบได้ในทันที โดยเฉพาะระบบงานที่เป็นลักษณะ Online

เมื่อกล่าวถึงระบบงานเราควรจะเข้าใจตรงกันว่า งานที่เริ่มตั้งแต่การพัฒนาระบบงานไปจนถึงขั้นการบำรุงรักษาและแก้ไขระบบงานเพื่อจัดงานนั้นออกใช้งานแล้ว

เมื่อทราบมูลเหตุความเสี่ยงแล้ว จะต้องพิจารณาว่าจะจัดการกับความเสี่ยงได้อย่างไร การจัดการกับความเสี่ยงมี 2 แบบ คือ

1. Risk Financing คือ การโอนความเสี่ยงไปให้บุคคลอื่น เช่น การประกันภัย เป็นต้น ปกติการประกันภัยมักจะถูกใช้ควบคู่ไปกับการควบคุมความเสี่ยงเสมอ ทั้งนี้เพราะการควบคุมแต่เพียงอย่างเดียวไม่อาจป้องกันหรือบรรเทาความเสียหายได้ร้อยเปอร์เซ็นต์ หรือได้ทุกกรณี เราไม่อาจเสี่ยงต่อความเสียหายได้แม้จะมีโอกาสเกิดน้อยก็ตาม เนื่องจากความเสียหายบางอย่างมีมูลค่าสูงเกินกว่าที่จะยอมรับได้ เช่น เครื่องคอมพิวเตอร์ถูกทำลายเสียหายจนใช้การไม่ได้ เป็นต้น

2. Risk control คือ การใช้มาตรการทางด้านการควบคุมเพื่อกำจัดหรือลดความเสี่ยงและความเสียหาย

การควบคุมมีความมุ่งหมายเพื่อขจัดหรือลดความเสี่ยงและความเสียหายที่อาจเกิดกับองค์กร อย่างน้อยที่สุดหากมีภัยและความเสียหายเกิดขึ้น ก็อยู่ในวิสัยที่จะรับได้ หรือทำให้กลับคืนสู่สภาวะปกติได้ สิ่งที่ควรพิจารณาเกี่ยวกับการควบคุมมีดังนี้

1. จุดที่ควบคุม เราไม่สามารถควบคุมตัวความเสี่ยงได้โดยตรง แต่ควบคุมจุดที่เกิดเหตุและความเสียหายได้ เพราะฉะนั้นจุดที่เกิดความเสี่ยงและจุดที่มีการควบคุม จึงเป็นจุดเดียวกัน การเลือกจุดที่ควรควบคุมมีอยู่ 2 แนวทาง ขึ้นอยู่กับความเสี่ยงว่าเป็นความเสี่ยงของระบบคอมพิวเตอร์ (EDP resource) หรือระบบงานคอมพิวเตอร์ (EDP applications)

ก. ความเสี่ยงของระบบคอมพิวเตอร์ ส่วนใหญ่จะเกิดกับ Hardware, Software, Data Files และ Operation เป็นต้น

ข. ความเสี่ยงของระบบงานคอมพิวเตอร์ ส่วนใหญ่จะเกิดกับ Transactions หรือ Functions ของระบบงาน อันเนื่องมาจากข้อมูลถูกเปลี่ยนแปลงแก้ไข รายการถูกดึงออกไปจากระบบงาน ข้อมูลบางส่วนหายไป เป็นต้น จุดที่ควรควบคุมก็คือจุดที่อาจทำให้ Transactions มีการเปลี่ยนแปลง

2. ลักษณะของการควบคุม การควบคุมโดยทั่วไปอาจแบ่งออกได้เป็น 2 ประเภท คือ การควบคุมทางด้านการเงิน (Financial controls) และการควบคุมการปฏิบัติงาน (Operation controls)

การควบคุมทางด้านการเงิน (Financial controls) หมายถึง การควบคุมเพื่อให้รายการทางการเงินถูกต้องสมบูรณ์ และเป็นไปตามหลักการบัญชีที่ยอมรับกันโดยทั่วไป

การควบคุมการปฏิบัติงาน (Operation controls) หมายถึง การควบคุมให้มีการปฏิบัติงานเป็นไปอย่างมีประสิทธิผลและประสิทธิภาพ

นอกจากนั้นการควบคุมอาจแบ่งออกได้เป็น 3 วิธี คือ

ก. การป้องกันหรือหลีกเลี่ยงมูลเหตุที่นำไปสู่ความเสียหาย (Prevention controls) ควรใช้กับความเสี่ยงที่ก่อให้เกิดความเสียหายและยากต่อการแก้ไข หรือเสียค่าใช้จ่ายมาก เช่น การป้องกันมิให้เข้าไปในห้องคอมพิวเตอร์และใช้เครื่องโดยไม่ได้รับอนุญาต เป็นต้น การป้องกันอาจทำได้โดยให้มียามรักษาการณ์และออกPassword ให้แก่ผู้มีสิทธิใช้เครื่อง เป็นต้น

ข. การตรวจให้พบปัญหาที่อาจนำไปสู่ความเสียหาย (Detective controls) ควรใช้กับความเสี่ยงที่ยังไม่ได้เกิดความเสียหาย โดยทันที หรืออาจไม่เกิดความเสียหายร้ายแรง หรือถ้าจะคิดป้องกันก็คงทำได้ยากและเสียค่าใช้จ่ายมาก เช่น การป้อนข้อมูล การป้องกันมิให้มีการป้อนข้อมูลผิดพลาด ย่อมทำได้ยากกว่าตรวจสอบว่ามีข้อมูลผิดพลาดหรือไม่ เป็นต้น การควบคุมในลักษณะนี้มักใช้เพื่อเสริมให้การควบคุมในแบบแรกมีประสิทธิภาพมากยิ่งขึ้น ข้อที่ควรระวังก็คือ การควบคุมนี้เป็นเพียงเครื่องมือค้นพบปัญหา แต่หากปัญหานั้นไม่ได้รับการแก้ไขหรือแก้ไขไม่ถูกต้อง ความเสียหายก็ยังเกิดขึ้นได้อีก โดยเฉพาะกรณีที่มีเจตนาละเมิดหรือ Override การควบคุมนั้น

ค. การตรวจให้พบมูลเหตุหรือปัญหาที่นำไปสู่ความเสียหาย และพร้อมกับกำหนดวิธีการแก้ไขล่วงหน้า (Detective and corrective controls) การควบคุมวิธีนี้ดีกว่าวิธีที่สอง เพราะว่าปัญหาที่ตรวจพบจะได้รับการแก้ไขอย่างเหมาะสมและรวดเร็ว เช่น การควบคุมความเสี่ยงอันเกิดจากไฟไหม้ โดยการติดตั้งเครื่อง Fire alarm แต่เพียงอย่างเดียวยังไม่เพียงพอ ควรจัดติดตั้งเครื่องดับไฟอัตโนมัติควบคู่กันไปด้วย ซึ่งจะทำให้สามารถควบคุมความเสียหายได้ดีขึ้น

3. วิธีปฏิบัติในการควบคุม แบ่งออกได้เป็น 7 วิธี คือ

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

ข. Verify หมายถึง การตรวจสอบกับหลักฐานที่เชื่อถือได้ เช่น ตรวจสอบเลขที่บัญชีกับ Data base เป็นต้น

ค. Confirmation หมายถึง การให้ยืนยันความถูกต้อง เช่น กำหนดให้ผู้ป้อนรายการข้อมูลในระบบ Online ยืนยันความถูกต้องของข้อมูลที่ปรากฏอยู่บนจอ Terminal ก่อนที่ข้อมูลจะเข้าสู่ระบบ

ง. Recalculation หมายถึง การคำนวณซ้ำในจุดที่มีการคำนวณ ปกติจะใช้คำนวณด้วยมือ (Manual) แล้วเทียบกับการคำนวณด้วยคอมพิวเตอร์ หรือสลับกันโดยสูตรในการคำนวณเหมือนกัน

จ. Limit หมายถึง การกำหนดขอบเขตของหน้าที่ การกระทำหรือรายการไว้แน่นอน ซึ่งสามารถทำได้ทั้งปริมาณและจำนวนเงิน เวลาและความถี่ เช่น การยินยอมให้ป้อนรหัสประจำตัว (Password) ผิดพลาดได้ไม่เกิน 3 ครั้ง ครั้งที่ 4 เครื่องจะยึดบัตร เป็นต้น

ฉ. Containment หมายถึง การสกัดกั้นมิให้ความเสียหายระบาดหรือลุกลามไปยังที่อื่น เช่น การมีเครื่องคอมพิวเตอร์ตั้งอยู่ใกล้กัน 2 เครื่อง ควรกั้นผนังทนไฟระหว่างเครื่องคอมพิว-เตอร์ เพื่อป้องกันมิให้ไฟลุกลามจากเครื่องหนึ่งไปอีกเครื่องหนึ่ง เป็นต้น

ช. Fallback หมายถึง การกำหนดวิธีปฏิบัติหรือระบบสำรอง ในกรณีที่เกิดความเสียหายบางส่วนหรือทั้งหมด เพื่อให้สามารถดำเนินงานต่อไปได้ เช่น กรณี Data base ถูกทำลายหรือเสียหาย ให้ทำระบบสำรอง (Backup) มาทำการ Copy เพื่อจะได้ดำเนินงานต่อไป เป็นต้น

4. การควบคุมที่ดีควรมีหลักฐานที่แสดงให้เห็นว่าได้ควบคุมจริง และเป็นไปตามแผนงานที่วางไว้ตัวอย่างบางประการที่เกิดจากความเสี่ยงของการดำเนินงานด้านคอมพิวเตอร์ที่มีผลกระทบต่อการควบคุม (Control risk)



ตัวอย่างของการวิเคราะห์ความเสี่ยง/ความเสียหาย ของการประมวลข้อมูลด้วยระบบคอมพิวเตอร์ (จากจุดที่อาจก่อให้เกิดความเสียหาย)

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
	การจัดองค์การ	
1	Structure	- ไม่มีการมอบหมายอำนาจหน้าที่และความรับผิดชอบ - ไม่ได้มอบหมายอำนาจหน้าที่และความรับผิดชอบเป็นลายลักษณ์อักษร - ไม่ได้จัดทำ Job description และ Organization charts
2	Policies & Procedures	- ไม่มีแผนงานประจำปี หรือไม่ปฏิบัติตามแผนงาน - ไม่มีการจัดทำงบประมาณประจำปี หรือไม่ปฏิบัติตามงบประมาณ - ไม่มีนโยบายและระเบียบปฏิบัติงานประมวลข้อมูลด้วยคอมพิวเตอร์ - ไม่มีระเบียบปฏิบัติในการจ้างงานและระบบเงินเดือน - ไม่มีการวิเคราะห์ความเสี่ยงและการควบคุมทรัพย์สินแต่ละประเภท
	การพัฒนาระบบงาน	
3	System specification	- Syst. designer ไม่เข้าใจความต้องการของ User หรือเข้าใจคลาดเคลื่อน - Syst. designer ไม่ได้ใช้เครื่องฯ และคน ให้เป็นประโยชน์มากที่สุด
4	Programming	- Programmer เข้าใจคำขอแก้ไขโปรแกรมผิดพลาด - Programmer ทำการแก้ไข Object program โดยตรง - มีการแอบแก้ไขเพิ่มเติมโปรแกรม เป็นเหตุให้โปรแกรมขาด คุณสมบัติทางด้านการป้องกันความ

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
		ปลอดภัย เช่น แฟ้ม ข้อมูลที่สำคัญถูกลบล้างออกไปหมดทันทีที่มีการ Run งาน - Programmer มิได้จัดทำเอกสารประกอบโปรแกรม หรือการแก้ไขโปรแกรม หรือทำอย่างไม่เป็นทางการ
5	Testing	- ไม่ได้ทดสอบโปรแกรมอย่างเพียงพอก่อนนำออกใช้งาน - การแก้ไขโปรแกรมอาจก่อให้เกิดความผิดพลาดที่คาดไม่ถึง - ไม่ได้รวบรวมข้อมูลที่ใช้ในการทดสอบ ผลการทดสอบ และ เอกสารรับรองความถูกต้องของโปรแกรมไว้เป็นหลักฐาน
6	Documentation	- เอกสารสนับสนุนระบบงานไม่เพียงพอ เป็นเหตุให้การแก้ไขโปรแกรมไม่ถูกต้อง หรือไม่สามารถกระทำได้ - เอกสาร ฯ ไม่ชัดเจน
7	Conversion	- ไม่สามารถนำโปรแกรม/ระบบงานออกใช้ได้ทันความต้องการ - เกิดข้อมูลผิดพลาดระหว่างทำการ Conversion - สูญเสีย File integrity
	การปฏิบัติการคอมพิวเตอร์	
8	Hardware	- ทำการ Maintenance ในขณะที่ยัง Run งาน Online ตามปกติ และไม่ได้แยก Hardware ส่วนนั้นออกจากระบบ - ในขั้นตอนการทำงาน Tape ไม่ได้มีการบันทึกสถานะของ Tape ไว้ทั้งหมด - ตั้งใจหรือประมาท ให้ชื่อ Media ไม่ถูกต้อง เป็นเหตุให้ข้อมูลใน Media ถูกล้างออกไปหมด - ไม่มีการตรวจสอบความถูกต้องของ Internal label

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
		- Expiry date ใน File ไม่ถูกต้อง เป็นเหตุให้ข้อมูลถูกล้างออกไปหมด - มี Write rings ค้างอยู่ในม้วน Tape หรือ Mount เทปผิดพลาด เป็นเหตุให้การประมวลข้อมูลหรือ Update ข้อมูลผิดพลาด
9	Software (O/S)	- มีการใช้ File เดียวกันพร้อมกัน 2 งาน ทำให้ข้อมูลอาจสะดุด - ไม่ได้ใช้ Controls ที่มีอยู่ใน O/S ให้เป็นประโยชน์ - ไม่สามารถปรับปรุง O/S ให้เป็นไปตามที่ต้องการได้
10	Operations	- Restart ไม่ถูกต้องหรือโดยประมาท เป็นเหตุให้ไม่ทราบสถานะของการทำรายการที่ค้างอยู่ - Operator ป้อนข้อมูลผิดพลาดเข้าไปใน Console เช่น ยกเลิกงานผิด - ใช้โปรแกรมที่ไม่ใช่ชุดปัจจุบัน Run งาน - ใช้ข้อมูลไม่ถูกต้องกับโปรแกรม - Operator ข้ามหรือละเลยการควบคุมความปลอดภัย เช่น ไม่ยอมให้ Write rings บน Tape - Operator เรียนรู้งานอย่างไม่ถูกต้อง ทำให้ข้อมูลใน Master file คลาดเคลื่อน หรือถูกลบทิ้งไป - Mount เทปโดยไม่มี Write ring protection
11	Backup recovery	- O/S อาจเสียหายหรือผิดปกติจนไม่สามารถรักษา Audit trail ไว้ได้ครบถ้วน เช่น ไม่ได้บันทึกการออก Output จาก Spooled storage devices - เมื่อทำ Restart หลังจากระบบล้มเหลวแล้ว O/S ไม่ได้ตรวจสอบสภาพของ Terminal location - File อาจถูก Read หรือ Write โดยที่ไม่ได้ Open - File อาจถูกทำลายระหว่างทำ Reorganize หรือ

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
12	การรักษาความปลอดภัย	Release ข้อมูล - Record อาจถูกดึงหายไปจาก File ที่สำคัญโดยไม่มีหลักประกันว่าจะสามารถสร้างขึ้นได้ใหม่ - Temporary file ที่เกิดระหว่างประมวลผล อาจถูกลบล้างหรือแก้ไข เนื่องจากขาดการควบคุม หรือระบบคอมพิวเตอร์หยุดอย่างผิดปกติ - Data หรือโปรแกรมถูกขโมยจากห้องคอมพิวเตอร์หรือที่เก็บอื่น - เครื่องฯ ถูกทำลายเสียหายโดยผู้บุกรุกจากภายนอกหรือพนักงานลูกจ้าง - ไม่มีการตรวจสอบผู้ที่จะเข้าไปใน EDP area - ไม่มีการป้องกันการใช้ Remote terminal - ผู้ไม่ได้รับอนุญาตอาจเข้าถึงระบบคอมพิวเตอร์โดยทางสายโทรศัพท์และ Password ของพนักงาน - User อาจเปิดเผย Password ของตัวเองโดยไม่รู้ตัว เช่น จดทิ้งไว้ในสถานที่เห็นได้ง่าย ปรากฏอยู่บน Print out หรือถูกสังเกตขณะที่ใช้งาน - User เปิด Terminal ทิ้งคาไว้ เปิดโอกาสให้ผู้ที่ไม่ได้รับอนุญาตเข้าไปใช้งานได้ทันที - พนักงานที่ถูกพักงานหรือออกจากงานแล้วยังสามารถเข้าถึงระบบได้อยู่ เนื่องจากชื่อและ Password ยังไม่ได้ถูกลบล้างออกไปจาก Tables หรือ Control lists - ไม่มีการติดตามหรือตรวจสอบความพยายามที่จะเข้าถึงระบบหรือ File โดยไม่ได้รับอนุญาต - Console operator อาจละเลย Label check แต่ไม่ปรากฏหลักฐานใน Security log - ไม่ได้กำหนดขอบเขต User ในการเข้าถึงระบบงาน (โปรแกรมและ Data) - ไม่มีการทบทวนความถูกต้องของรายการที่เป็นจำนวน

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
		เงินมาก ๆ หรือที่ผิดปกติ - ไม่มีการทบทวนรายงานวิเคราะห์การปฏิบัติงาน เพื่อดูว่า มีการละเมิดความปลอดภัยหรือไม่ - เจ้าพนักงานควบคุมความปลอดภัย เมื่อได้รับรายงานการละเมิดระบบการรักษาความปลอดภัย อาจสั่งการที่ไม่เหมาะสม เพราะไม่มีระเบียบปฏิบัติที่เป็นแบบแผนกำหนดไว้ - Operator ประทุษร้ายต่อเครื่องฯ - พนักงานอาจขโมยโปรแกรมไปใช้ประโยชน์ส่วนตัว เช่น นำออกไปขายให้บุคคลภายนอก - เจ้าหน้าที่บริหารศูนย์ฯ ใช้อุบายหรืออำนาจ ทำให้การควบคุมการปฏิบัติงานไม่มีผล เพื่อแก้ไขหรือนำข้อมูลออกมาใช้ - ไม่ได้เก็บเอกสารประกอบโปรแกรมที่สำคัญไว้ในที่ปลอดภัย - Programmers เพิ่มเติมข้อความพิเศษเข้าไปใน Programe เพื่อเปลี่ยนแปลงข้อมูลที่เกี่ยวกับตนเอง เช่น บัญชีเงินเดือน - Encryption key อาจถูกขโมย - ข้อความแปลกปลอมอาจถูกส่งเข้ามาในระบบ - O/S อาจถูกแก้ไขโดยไม่ได้รับอนุญาต ให้เสมียนป้อนรายการสามารถป้อนโปรแกรมเข้าไปทำลายหรือล้มล้างระบบ - Line อาจถูกตรวจสอบหรือติดตามความเคลื่อนไหวจากบุคคลที่ไม่ได้รับอนุญาต - ข้อมูลหรือโปรแกรมอาจถูกขโมยทางสายโทรศัพท์ - ข้อมูลอาจถูกเปลี่ยนแปลงแก้ไขจากการ Tapping โดยไม่ได้รับอนุญาต - Media ประเภทสารแม่เหล็ก อาจถูกทำลายสภาพหรือสถานะของแม่เหล็ก

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
13	Communications	- User ที่สามารถเข้าถึงข้อมูลรายตัวใน File อาจ List ข้อมูลทั้งหมดโดยไม่ได้รับอนุญาต เพื่อประโยชน์ส่วนตัว เช่น เพื่อขายรายชื่อและที่อยู่พนักงานให้บุคคลภายนอก - ข้อมูลอาจถูกส่งไปผิด Terminal โดยไม่ได้ตั้งใจ - Protocal ล้มเหลวจนไม่สามารถตรวจสอบความถูกต้องของ Transmitter หรือ Receiver ได้ - ในระหว่างที่การประมวลผลหยุดชะงักงันโดยไม่คาดคิด Network-controller อาจทิ้งข้อมูลบางส่วนค้างไว้ใน Memory โดยไม่มีการป้องกันใด ๆ



ระบบงานที่ประมวลข้อมูลด้วยคอมพิวเตอร์

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
1	Origination	- ไม่มีการนับจำนวนเอกสารหรือวิธีการควบคุม Source data อื่น - Data หรือ Transaction สูญหายหรือเพิ่มเติมขึ้นมาโดยไม่สามารถตรวจสอบได้ - ไม่ได้ตรวจสอบรายการที่มีจำนวนเงินผิดปกติ
2	Authorization	- ไม่มีหรือไม่ได้ปฏิบัติตามระเบียบคำสั่งในการมอบหมายอำนาจหน้าที่ - ไม่ได้ลงลายมือชื่อรับรองของผู้รับมอบอำนาจ - ไม่ควบคุมหรือจำกัดขอบเขตการเข้าถึงระบบงาน - ไม่มีระเบียบคำสั่งเกี่ยวกับการ Authorize - ไม่ได้ใช้เอกสารที่มีหมายเลขกำกับ หรือแบบฟอร์มเฉพาะ - ไม่มีการแบ่งแยกหน้าที่เพื่อป้องกันมิให้บุคคลใดบุคคลหนึ่ง สามารถควบคุมความถูกต้องของรายการได้แต่เพียงผู้เดียว - ไม่มีการทบทวนความถูกต้องของรายการ (Transactions) ก่อนนำไปประมวลผล - Password ของเจ้าหน้าที่บริหาร ปรากฏบนจอภาพของ Operator
3	Data Entry	- ผ่านรายการสำคัญโดยไม่ต้องขออนุมัติหรือควบคุมจากพนักงานขั้นบริหาร - ตรวจไม่พบข้อผิดพลาดในขณะที่ทำการป้อนรายการ - ข้อมูลที่ไม่ครบถ้วนหรือไม่ตรงตาม Format ยังสามารถผ่านเข้าไปได้เสมือนหนึ่งถูกต้อง - Record ที่พบข้อผิดพลาด เมื่อได้รับการแก้ไขแล้วอาจไม่ผ่านการตรวจสอบทั้ง Record อีกครั้ง

ลำดับ	จุดที่อาจก่อให้เกิดความเสียหาย	มูลเหตุของความเสียหาย
4	Processing	- ความผิดพลาดของโปรแกรมเป็นเหตุให้การประมวลข้อมูลผิดพลาด - ตรวจไม่พบข้อผิดพลาดที่น่าจะพบ - ข้อมูลบางอย่างที่อยู่นอกเหนือการกำหนดไว้ เช่น Code อาจถูกประมวลผลในลักษณะที่คาดไม่ถึง
5	File storage	- ไม่ได้ให้ชื่อกำกับไว้ ในที่สุดสูญหาย - จำนวน Records ไม่ตรงกับ Control totals - เป็น File ที่ผิด Version
6	Output	- ส่งรายงานให้ผิดคนหรือผิด Terminal - รายงานสูญหาย - วัสดุเหลือใช้ เช่น รายงานชุดสำเนาที่ไม่ได้ใช้ประโยชน์กระดาษคาร์บอนที่ใช้แล้ว ฯลฯ อาจได้รับการทำลายหรือ จำหน่ายออกไปไม่เหมาะสม

ความเสี่ยงของการดำเนินงาน
ด้านคอมพิวเตอร์ที่มีผลกระทบต่อการตรวจสอบ (Audit Risks)

ความเสี่ยงในแง่ของการตรวจสอบ (Audit risks) มีอยู่ 2 ประเภทใหญ่ ๆ คือ

1. เหตุการณ์ต่าง ๆ ที่ไม่น่าพอใจหรือไม่อาจยอมรับได้ เกิดขึ้นอยู่ในระบบงาน ซึ่งวิธีการตรวจสอบ (Audit Procedure) ไม่อาจตรวจพบได้

2. เหตุการณ์ที่ไม่น่าพอใจหรือไม่อาจยอมรับได้ ที่อาจตรวจพบได้โดยวิธีการตรวจสอบ แต่ผู้ตรวจสอบอาจเข้าใจเหตุการณ์หรือเงื่อนไข (Condition) ผิดพลาดหรือไม่ถูกต้องอย่างแท้จริง

ความเสี่ยงของการตรวจสอบคอมพิวเตอร์ (Risk in auditing EDP) จุดประสงค์ของการควบคุมต่าง ๆ ที่ใช้กับระบบงานคอมพิวเตอร์ยังคงเหมือนกับจุดประสงค์ในการควบคุมที่ใช้ในระบบงานทั่วไป สิ่งที่เปลี่ยนแปลงไปก็คือ วิธีการควบคุม (Methods of Control) เพื่อให้เหมาะสมกับลักษณะการทำงานด้วยเครื่องคอมพิวเตอร์ ซึ่งประกอบด้วยเรื่องต่าง ๆ ดังนี้

1. หลักฐานมีรูปแบบและลักษณะแตกต่างจากระบบงานที่ปฏิบัติด้วยมือ (Manual) มาก
2. มีเอกสาร (Hard copy) น้อยลง
3. เปลี่ยนแปลงการมอบหมายหน้าที่ความรับผิดชอบมากขึ้น
4. มีการควบคุมโดยเครื่องคอมพิวเตอร์ (Automated control)
5. มีลักษณะการทำงานแบบสม่ำเสมอ (ไม่ว่าจะถูกหรือไม่ถูก)

ความเสี่ยงของการตรวจสอบคอมพิวเตอร์มีประเภทต่าง ๆ ดังนี้

1. ความเสี่ยงอันเนื่องจากการแปลงข้อมูล (Data conversion risk) หมายถึงว่า การแปลงข้อมูลจากข้อมูลในเอกสารต่าง ๆ เป็นข้อมูลที่เครื่องคอมพิวเตอร์สามารถอ่านได้ อาจมีการแปลงข้อมูลผิด

2. ความเสี่ยงอันเนื่องจากการผิดพลาดซ้ำ (Repetition of Errors Risk) ความผิดพลาดอันเกิดขึ้นซ้ำ ๆ กันได้ เนื่องจากระบบงานคอมพิวเตอร์จะทำงานเป็นรูปแบบสม่ำเสมอ

3. ความเสี่ยงอันเนื่องจากการผิดพลาดเป็นทอด ๆ (Cascading of Error risk) ความผิดพลาดที่เกิดขึ้นในระบบงาน อาจมีผลกระทบกระเทือนข้อมูลอื่นในระบบงานนั้นให้เกิดความผิดพลาดด้วย

4. ความเสี่ยงอันเกิดจากการประมวลผลขาดตอน (Discontinuity of Processing risk) ความเพียงพอของการจัดทำ Backup และ Documentation ของระบบงาน ย่อมมีผลอย่างยิ่งต่อการประมวลผล ถ้า Documentation และการ Backup ไม่เพียงพอ อาจทำให้การประมวลผลขาดตอนได้

5. ความเสี่ยงอันเกิดจากผลทางเทคโนโลยี (Technological Risk) อาจมีการใช้เทคโนโลยีแบบผิด ๆ ซึ่งจะทำให้ผลการปฏิบัติงานผิดพลาดหรือขาดประสิทธิภาพ

6. ความเสี่ยงอันเกิดจากประพฤติไม่ชอบโดยอาศัยคอมพิวเตอร์ (Computer Abuse risk) อาจมีผู้ใช้คอมพิวเตอร์ไปในทางที่ไม่ชอบ เพื่อหาประโยชน์ให้แก่ตนเอง หรือก่อการทุจริตด้วยคอมพิวเตอร์

ตารางวิเคราะห์ความเสี่ยงและการควบคุมระบบงานที่ประมวลผลด้วยคอมพิวเตอร์

ความเสี่ยง (Risks) / กิจกรรม (resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	เอกสารปลอมหรือไม่ผ่านการอนุมัติ	เอกสารไม่ครบถ้วนและสมบูรณ์	เอกสารผิดพลาด				ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
Source Documents	X	X	X	X	X				การบันทึกบัญชีและยอดคงเหลือตามบัญชี ไม่ถูกต้องและหรือการทุจริต	**AUTHORIZATION** - มีแบบฟอร์มเอกสารเฉพาะ หรือแบบฟอร์มมาตรฐานที่มีหมายเลขกำกับ - มีการควบคุมการเข้าถึงแบบฟอร์มเปล่า โดยเฉพาะตราสารการเงิน เช่น สมุดเช็ค ดราฟท์ และตั๋วแลกเงิน เป็นต้น - มีการอนุมัติด้วยลายมือชื่อในเอกสารสนับสนุนรายการทุกประเภท - ไม่ควรให้เจ้าหน้าที่คนหนึ่งสามารถอนุมัติรายการได้หลายประเภท เช่น การเปิดบัญชี การปิดบัญชี หรือการแก้ไขรายการ เป็นต้น - แยกหน้าที่จัดทำเอกสารสนับสนุนรายการออกจากหน้าที่อื่น หรือไม่ให้ทำหน้าที่อย่างอื่น เช่น การป้อนรายการ หรือตรวจสอบรายงาน เป็นต้น **COMPLETE & ACCURACY** - มีการตรวจสอบข้อมูลในเอกสารสนับสนุนรายการโดยบุคคล - มีการควบคุมความครบถ้วนแบบ Batch Controls ได้แก่ - Source Document Counts - Record Counts - Total Values หรือ Control Totals - มีทะเบียนบันทึกรายละเอียดของ Batches - มีการตรวจสอบความถูกต้องของ Batch Totals โดยเปรียบเทียบ Manual กับ Computer Totals - มีการเก็บรวบรวมเอกสารสนับสนุนรายการ หรือตัวสำเนาเอกสารไว้ให้ครบถ้วนและเป็นระเบียบ เพื่อไว้ใช้ในการตรวจสอบภายหลัง หรือสร้างข้อมูลขึ้นใหม่

ความเสี่ยง (Risks) / กิจกรรม (Resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	เอกสารปลอมหรือไม่ผ่านการอนุมัติ	เอกสารไม่ครบถ้วนและสมบูรณ์	เอกสารผิดพลาด				ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
				X	X					**ERROR CORRECTION** - มีรายงานข้อมูลที่ผิดพลาด ผิดปกติ และข้อมูลที่ถูก reject ให้ user ตรวจสอบหาสาเหตุและทำการแก้ไขต่อไป - มีทะเบียนบันทึกรายการผิดพลาด - มีบัญชีพัก (Suspense A/C) สำหรับบันทึกรายการที่ผิดพลาดและถูก reject สิ้นวัน สำหรับติดตามและควบคุมการแก้ไขในวันถัดไป (Manual หรือ Computer) - มีการควบคุมและตรวจสอบความถูกต้องเช่นเดียวกับรายการปกติประจำวัน

ความเสี่ยง (Risks) / กิจกรรม (resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	รายการไม่ครบถ้วนและสมบูรณ์	รายการลอย หรือไม่มีเอกสารสนับสนุน	รายการเกิดขึ้นเองจากโปรแกรมในเครื่อง	รายการผิดพลาด			ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
Data Entry				X					การบันทึกบัญชีและยอดคงเหลือตามบัญชีไม่ถูกต้อง และหรือ การทุจริต	**AUTHORIZATION** - มีการแยกหน้าที่ระหว่างการจัดทำเอกสารสนับสนุนรายการ การอนุมัติรายการ และการป้อนข้อมูล - Terminal อยู่ในที่ปลอดภัย และมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต - ใส่กุญแจเครื่อง Terminal หลังเสร็จงานแล้ว - มีการ Sign-on หรือ initiate เครื่อง Terminal โดยเจ้าหน้าที่ระดับหัวหน้าปฏิบัติการ ก่อนที่ Operator จะสามารถใช้เครื่องได้ - มีการใช้ Password ควบคุมและป้องกันการใช้เครื่อง Terminal โดยไม่ได้รับอนุญาต หรือเกินกว่าขอบเขตที่กำหนด - มีรายงานให้ติดตามและตรวจสอบการพยายามใช้ Terminal โดยไม่ได้รับอนุญาต หรือเกินกว่าขอบเขตที่กำหนด
	X	X	X		X	X			การบันทึกบัญชีและยอดคงเหลือตามบัญชีไม่ถูกต้องและหรือ การทุจริต	**COMPLETE & ACCURACY** - มี Screen Format สำหรับใช้ในการป้อนรายการ เพื่อให้ Operator สามารถป้อนรายการได้สะดวกและตรวจสอบความถูกต้องได้ด้วยสายตา - มีการตรวจสอบข้อมูลทุก Field โดยโปรแกรมคอมพิวเตอร์ Field ที่ควรทำการตรวจสอบ ได้แก่ - Transaction ID (Check digit) - Transaction Code - Transaction Date

ความเสี่ยง (Risks) / กิจกรรม (Resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	เอกสารปลอมหรือไม่ผ่านการอนุมัติ	เอกสารไม่ครบถ้วนและสมบูรณ์	เอกสารผิดพลาด	รายการผิดพลาด			ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
										- Amounts - Limit - Range - Signs - Balance - มีการตรวจสอบความครบถ้วนของรายการโดยวิธี Sequence Check (Manual หรือ Computer) - มีการตรวจสอบความครบถ้วนของรายการ โดยการตรวจสอบ Batch Total และ Terminal log. - Record counts - Total Value หรือ Control totals - มีข้อห้ามในการ Override รายการที่ไม่ถูกต้อง หรือให้อยู่ในอำนาจของเจ้าหน้าที่ระดับบริหาร และมี Automatic log สำหรับบันทึกรายการที่ถูก Override เพื่อให้สามารถทบทวนความเหมาะสมได้ในภายหลัง
						X			การบันทึกบัญชีและยอดคงเหลือตามบัญชีไม่ถูกต้อง	**ERROR COLLECTION** - มีคำอธิบายข้อผิดพลาดในการป้อนข้อมูลและการแก้ไข - แสดงข้อผิดพลาด (Error Messages) บนจอ Terminal หรือมีรายงานทันทีเพื่อให้ Operator ทำการแก้ไขได้อย่างรวดเร็ว - มี Suspense File สำหรับบันทึกรายการที่ถูก reject ทั้งหมด (Manual หรือ computer) และออกรายงานให้ user เป็นผู้ทำการแก้ไขต่อไป

ความเสี่ยง (Risks) / กิจกรรม (resources)	เอกสารสูญหาย	เอกสารซ้ำซ้อน	รายการไม่ครบถ้วนและสมบูรณ์	รายการลอย หรือไม่มีเอกสารสนับสนุน	รายการเกิดขึ้นเองจากโปรแกรมในเครื่อง	รายการผิดพลาด			ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
										- มีเจ้าหน้าที่ระดับบริหารเป็นผู้ทำการตรวจสอบความถูกต้องของรายแก้ไขเช่นเดียวกับรายการปกติ - การแก้ไขรายการที่ค้างใน Suspense File ไม่ควรใช้วิธีล้างหรือลบรายการออกจาก File แต่ควรใช้เป็นรายการเดบิทหรือเครดิต เพื่อให้สามารถติดตามและตรวจสอบการแก้ไขได้ - มีรายงานรายการที่ค้างนานใน Suspense File

ความเสี่ยง (Risks) / กิจกรรม (Resources)	ประมวลผลโดยใช้ข้อมูลผิดพลาด	ประมวลผลโดยใช้โปรแกรมผิดพลาด	ประมวลผลไม่ครบถ้วน	ประมวลผลไม่ถูกต้อง	รายการเกิดขึ้นเองโดยไม่มีเงื่อนไข				ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
Data Processing	X	X	X	X	X				การบันทึกบัญชีและยอดคงเหลือทางบัญชีไม่ถูกต้องการประกอบธุรกิจหยุดชะงักสูญเสียรายได้ภาพพจน์เสียหายและอาจเกิดการทุจริต	**COMPLETENESS & ACCURACY** - มีการตรวจสอบความถูกต้องของ Transaction แต่ละรายการก่อนนำไปประมวลผลกับ Master File - Matching - Limit - Reasonableness - มีการตรวจสอบความถูกต้องของ File ก่อนประมวลผล (Header Label Check) - มีการตรวจสอบความถูกต้องของ File หลังประมวลผล (Trailer Label Check - Control record) - มี Run-to-Run control สำหรับงานที่มี intermediate run ก่อนถึงการประมวลผลขั้นสุดท้าย - มีการตรวจสอบความถูกต้องของผลลัพท์กับข้อมูล input โดยบุคคล - ตรวจสอบ Output control total กับ Input control total - ตรวจสอบรายงาน Update, Change, Add และ Delete - มีการทดสอบการคำนวณโดยบุคคล - เลือกทดสอบบางรายการ - ทดสอบผลรวม - มีการตรวจสอบ Master File เป็นครั้งคราว โดยการตรวจสอบกับเอกสารสนับสนุนรายการที่เกี่ยวข้อง

ความเสี่ยง (Risks) / กิจกรรม (resources)	รายงานผิดพลาด	รายงานล่าช้า	รายงานสูญหาย	รายงานไม่เหมาะสม					ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
DATA OUTPUT	X	X	X	X					การประกอบธุรกิจชะงักเกิดความเสียหายทางการเงิน อันเนื่องจากการตัดสินใจและการปฏิบัติงานผิดพลาด และอาจเกิดการทุจริต	**COMPLETE & ACCURACY** - มีการตรวจสอบ Output โดยบุคคลของศูนย์ฯ และ Users **การตรวจสอบของศูนย์ฯ** - ตรวจสอบ Output Batch totals กับ Input Batch totals - ตรวจสอบ Output record counts กับ Input record counts - ตรวจสอบจำนวนฉบับรายงานเทียบกับโปรแกรมสั่งงาน - ตรวจสอบลำดับหน้าของรายงาน - ตรวจสอบหัวและท้ายของรายงาน - ชื่อรายงาน - โปรแกรมที่ใช้ในการประมวลผล - วันและเวลาที่ออกรายงาน - ระยะเวลาที่ออกรายงาน - หน่วยงานผู้ใช้ - Record counts - Control totals **การตรวจสอบของ Users** - ตรวจสอบรูปแบบของรายงาน - ตรวจสอบ Computer control total กับ Manual control total

ความเสี่ยง (Risks) / กิจกรรม (Resources)	รายงานผิดพลาด	รายงานล่าช้า	รายงานสูญหาย	รายงานไม่ครบถ้วน					ความเสียหายที่อาจเกิดขึ้น (Losses)	การควบคุม (Controls)
										- ตรวจสอบ Output record counts กับ Input record counts - ตรวจสอบรายการเปลี่ยนแปลงข้อมูลใน Master File (List of changes) - ตรวจสอบรายการที่เกิดจากเงื่อนไขในโปรแกรม (List of Computer generated Transactions) - ตรวจสอบรายการที่ป้อนเข้าระบบงานทั้งสิ้น (Transaction List) - มี Distribution List สำหรับควบคุมการจัดส่งรายงานให้ Users

10

การวางแผนการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

หลักการวางแผนการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

การนำคอมพิวเตอร์เข้ามาใช้อย่างแพร่หลายในองค์กรต่าง ๆ ในปัจจุบัน ได้ก่อให้เกิดผลกระทบในด้านต่าง ๆ ซึ่งรวมทั้งงานตรวจสอบองค์กรที่นำคอมพิวเตอร์เข้ามาใช้ในการประมวลงานต่าง ๆ ด้วย ผู้สอบบัญชีหรือผู้ตรวจสอบควรได้ทราบถึงสภาพการเปลี่ยนแปลงถึงแนวทางหรือวิธีการตรวจสอบ โดยเฉพาะอย่างยิ่งผู้ที่ทำหน้าที่ในการควบคุมและดูแลงานตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ ทั้งนี้เพราะเทคโนโลยีด้านคอมพิวเตอร์ได้มีผลอย่างสำคัญต่อรูปแบบทางหลักฐาน วิธีการเก็บข้อมูล รวมทั้ง Audit trail ซึ่งจะมีผลต่อเทคนิคและวิธีการตรวจสอบในสภาพแวดล้อมใหม่อย่างสำคัญด้วย

การควบคุมการตรวจสอบที่ดีที่ใช้คอมพิวเตอร์อย่างมีประสิทธิภาพ จะดำเนินการอย่างได้ผลพอสมควรหากจะได้ทราบถึงขั้นตอนการวางแผนการตรวจสอบ

1. หลักการวางแผนการตรวจสอบ

ขั้นตอนที่สำคัญที่สุดของการตรวจสอบส่วนใหญ่คือ การวางแผน ถ้าได้มีการทำการวางแผนล่วงหน้าก่อนที่งานการตรวจสอบอย่างละเอียดจะเริ่มขึ้นแล้ว จะมีความเป็นไปได้สูงที่งานการตรวจสอบนั้นจะประสบความสำเร็จอย่างมีประสิทธิภาพ

1.1 มาตรฐานการสอบบัญชีตามประกาศ ก.บช. ฉบับที่ 19 (พ.ศ.2518) ข้อ 4 ได้กำหนดไว้ว่า "ผู้สอบบัญชีต้องวางแผนการตรวจสอบและควบคุมผู้ช่วย (ถ้ามี) ให้ปฏิบัติงานโดยถูกต้อง" ดังนั้น คณะอนุกรรมการมาตรฐานการสอบบัญชี สมาคมนักบัญชีรับอนุญาตแห่งประเทศไทย จึงเห็นสมควรกำหนดแนวทางและวิธีการในการวางแผนและควบคุมงานสอบบัญชีให้เป็นไปตามมาตรฐานการสอบบัญชีที่รับรองทั่วไป เพื่อให้ผู้สอบบัญชีได้ใช้ปฏิบัติเป็นแนวเดียวกัน

1.2 ผู้สอบบัญชีต้องวางแผนก่อนการตรวจสอบ การวางแผน หมายถึง การกำหนดขอบเขตเทคนิคและวิธีการที่ใช้ในการสอบบัญชี ความรู้และประสบการณ์ของผู้สอบบัญชีเกี่ยวกับกิจการที่ตรวจสอบ เป็นปัจจัยสำคัญที่ช่วยในการวางแผน การวางแผนขึ้นอยู่กับขนาดของกิจการและความซับซ้อนของธุรกิจที่กิจการนั้นประกอบการอยู่ ดังนั้นเพื่อให้การวางแผนมีประสิทธิภาพและได้ผล ผู้สอบบัญชีควรมีความรู้ในเรื่องต่าง ๆ เกี่ยวกับกิจการดังนี้

1) เรื่องต่าง ๆ เกี่ยวกับธุรกิจที่กิจการนั้นประกอบการอยู่
2) ระบบและวิธีการบัญชี ทั้งทางด้าน Manual และ Computer
3) ระบบการควบคุมภายใน ทั้งทางด้าน Manual และ Computer
4) ขนาดและประเภทของรายการที่ถือว่าเป็นสาระสำคัญ
5) รายการปรับปรุงงบการเงินที่คาดว่าจะมี
6) สภาวะที่อาจก่อให้เกิดการเปลี่ยนแปลงในปริมาณหรือวิธีการทดสอบ
7) ลักษณะของรายงานการสอบบัญชีที่คาดว่าจะเสนอ

1.3 ในการวางแผนงานสอบบัญชี ผู้สอบบัญชีจะต้องรวบรวมข้อมูลเกี่ยวกับระบบคอมพิวเตอร์ อาทิเช่น

1) การจัดองค์การและการแบ่งงานในหน้าที่ที่เกี่ยวข้องกับระบบการประมวลผลข้อมูล
2) ขอบเขตของการใช้งานของคอมพิวเตอร์ในธุรกิจ
3) ลักษณะของคอมพิวเตอร์และอุปกรณ์ พร้อมทั้งโปรแกรม
4) วิธีการประมวลผลข้อมูลของระบบงานที่มีสาระสำคัญต่องานการเงิน รวมทั้งวิธีการจัดเก็บข้อมูลและนโยบายการรักษาข้อมูล
5) โครงการปัจจุบันของธุรกิจเกี่ยวกับการจัดทำระบบใหม่ หรือการแก้ไขเปลี่ยนแปลงระบบที่ใช้อยู่ในปัจจุบัน

1.4 ผู้สอบบัญชีจะต้องมีความรู้เกี่ยวกับการควบคุมภายในของระบบการประมวลผลข้อมูลโดยคอมพิวเตอร์ การควบคุมภายในของธุรกิจที่ใช้คอมพิวเตอร์แบ่งได้เป็น 2 ลักษณะ ดังนี้

1) การควบคุมภายในทั่วไป ได้แก่ การควบคุมที่เกี่ยวกับกิจการของหน่วยงานคอมพิวเตอร์
2) การควบคุมภายในเฉพาะระบบงาน ได้แก่ การควบคุมภายในซึ่งเกี่ยวกับความสมบูรณ์และถูกต้องของข้อมูลในแต่ละระบบงาน

1.5 ผู้สอบบัญชีจะต้องพิจารณาเรื่องต่าง ๆ ในข้อ 1 และข้อ 2 เพื่อใช้ในการวางแผนบัญชี เช่น

1) การวางแผนเพื่อสอบทานการปฏิบัติงานของระบบคอมพิวเตอร์ว่าควรจะใช้วิธีการและเทคนิคการตรวจสอบได้เมื่อไร และในส่วนไหนของระบบ
2) การค้นหาจุดอ่อนของระบบการประมวลผลข้อมูล ซึ่งอาจมีข้อผิดพลาดหรือเปิดโอกาสมีการทุจริตได้
3) การพิจารณาระดับความเชื่อถือเกี่ยวกับการควบคุมต่าง ๆ ในการประเมินประสิทธิภาพการควบคุมภายในทั้งหมดของธุรกิจ
4) การวางแผนการใช้คอมพิวเตอร์มาช่วยในการปฏิบัติงานสอบบัญชี
5) การวางแผนการใช้บุคลากรที่มีความสามารถเฉพาะทางคอมพิวเตอร์ในกรณีที่จำเป็น

2. การวางแผนสอบบัญชีกับการวิเคราะห์ความเสี่ยง เพื่อให้เข้าถึงจุดควบคุมต่าง ๆ

ผลกระทบ TECHNOLOGY ทำให้ขั้นตอนและวิธีการปฏิบัติงานเปลี่ยนแปลงไปมาก การเปลี่ยนแปลงบางลักษณะได้ก่อให้เกิดความเสี่ยง (RISK) ที่ติดตามมาในรูปแบบต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อองค์การได้ เช่น

ความเสี่ยงทางด้านการบริหารงานและการดำเนินงานในกรณีที่ระบบการควบคุมและรักษาความปลอดภัยไม่เพียงพอ เช่น การสูญหายของข้อมูลทางการเงินในระบบคอมพิวเตอร์ ความเสี่ยงจากระบบงานขัดข้องหรือเสียหาย ซึ่งอาจมีผลกระทบต่อชื่อเสียงหรือฐานะของกิจการอย่างร้ายแรงได้ หากองค์การนั้นเป็นองค์การที่เกี่ยวข้องกับการเงินที่ต้องติดต่อกับประชาชนจำนวนมาก ๆ

ผู้ตรวจสอบควรพยายามมองให้เห็นภาพพจน์ของกิจกรรม ขบวนการขั้นตอนต่าง ๆ ในระบบ ในขณะที่จะเริ่มขบวนการรวบรวมเอกสารข้อมูล และอาจใช้เทคนิคการตั้งคำถามเพื่อหาจุดที่สามารถก่อให้เกิดข้อผิดพลาดขึ้นได้ในแต่ละขบวนการและในแต่ละขั้นตอน คำตอบที่ได้จะชี้ถึงลักษณะของสาเหตุและความเฉพาะของความผิดพลาดที่เกิดขึ้น เช่น สาเหตุหนึ่งที่อาจทำให้เกิดจุดอ่อน คือ การบันทึกบัญชีผิดพลาด ซึ่งเป็นความผิดพลาดจากการทำด้วยมือ ลักษณะของความผิดพลาดก็อาจมีผลมาจากความผิดพลาดของพนักงาน เช่น ไม่บันทึกรายการให้ครบถ้วน หรือบันทึกรายการผิดพลาด หรือจำแนกประเภทรายการผิด เป็นต้น

คำถามที่ผู้ตรวจสอบควรถามต่อไป คือ ความผิดพลาดที่เกิดขึ้นนั้นมีสาระสำคัญหรือไม่ มีการควบคุมอะไรบ้าง ณ จุดนั้น ถ้าจะป้องกันมิให้เกิดจุดอ่อนขึ้นจะต้องมีการควบคุมอย่างไร

ผู้ตรวจสอบควรพัฒนาแผนแสดงถึงกิจกรรมที่มีการปฏิบัติต่อรายการต่าง ๆ (TRANSACTION ACTIVITY FLOWCHARTS) ก่อนที่จะมุ่งรวบรวมข้อมูลในรายละเอียดและทำความเข้าใจให้ถ่องแท้ ซึ่งจะช่วยให้ผู้ตรวจสอบสามารถเข้าใจจุดที่ตรวจสอบและลักษณะของข้อมูลที่ต้องการได้

ข้อมูลต่าง ๆ ที่รวบรวมได้ โดยเฉพาะกิจกรรมที่มีความสัมพันธ์กับข้อผิดพลาดหรือการควบคุม จะทำให้ผู้ตรวจสอบวางแผนการตรวจสอบได้อย่างมีประสิทธิภาพได้มากกว่าการใช้คำถามทั่วไป

2.1 ความเสี่ยงกับผู้ตรวจสอบ

การวิเคราะห์ความเสี่ยงโดยผู้ตรวจสอบ เป็นแนวคิดใหม่ที่สำคัญยิ่งในการตรวจสอบองค์การที่ใช้คอมพิวเตอร์ และการใช้เทคนิคการวิเคราะห์ความเสี่ยงที่มีประสิทธิภาพ จะช่วยให้ผู้ควบคุมงานและผู้บริหารมีความมั่นใจในประสิทธิภาพของการตรวจสอบได้อย่างเต็มที่ ไม่ว่าการตรวจสอบนั้นจะเป็นการตรวจสอบฐานะและการดำเนินงานตามปกติ (FINANCIAL OR REGULAR AUDIT) ขององค์การ หรือเป็นการตรวจสอบทางด้านคอมพิวเตอร์โดยเฉพาะ (EDP AUDIT) และโดยเฉพาะอย่างยิ่งการตรวจสอบการทุจริตการใช้เทคนิคการวิเคราะห์ความเสี่ยง จะช่วยกำหนดขอบเขต กำหนดขั้นตอน และใช้เครื่องมือการตรวจสอบได้อย่างมีประสิทธิภาพเพิ่มขึ้น

การวิเคราะห์ความเสี่ยง จะมีบทบาทที่สำคัญยิ่งในการวางแผนการตรวจสอบ โดยเฉพาะในเรื่องที่เกี่ยวกับการพิจารณาจุดอ่อนที่อาจมีได้ในองค์การ ตั้งแต่ระดับสูงสุดถึงระดับต่ำสุด การวิเคราะห์ความเสี่ยงจึงควรทำในลักษณะ TOP-DOWN เสมอ เพื่อที่ผู้ตรวจสอบจะได้เห็นภาพความเสี่ยงที่มีผลกระทบและเกี่ยวเนื่องซึ่งกันและกัน เพราะโดยทั่วไปหากมีจุดอ่อนในการบริหารงานระดับนโยบาย ซึ่งเป็นระดับ TOP แล้ว จุดอ่อนที่มีความเสี่ยงก็จะมีผลกระทบต่อระดับล่างอย่างหลีกเลี่ยงไม่ได้

2.2 ความเสี่ยงกับผู้บริหารระดับสูง

ในการประเมินความเสี่ยงภัยและการวิเคราะห์หาจุดสำคัญ ๆ ในแต่ละระดับของการควบคุมทั่วไปในระดับของผู้บริหารระดับสูงนั้นมีขั้นตอนโดยสรุปดังนี้

ขั้นที่ 1 พิจารณาว่าความรับผิดชอบของผู้บริหารระดับสูงเพียงพอกับความเสี่ยงภัยในแต่ละเรื่องหรือไม่

ขั้นที่ 2 เรื่องใดที่ไม่พอเพียงก็ให้ทบทวนขั้นตอนการปฏิบัติที่ใช้อยู่ในเรื่องความรับผิดชอบของผู้บริหาร ซึ่งเป็นเรื่องการจัดองค์การ การวางแผน การสั่งการ การควบคุม รวมทั้งขั้นตอนการควบคุม (CONTROL FUNCTIONS) ของฝ่ายบริหารในด้านการอนุมัติรายการ การแบ่งแยกหน้าที่ การรับทราบผลการปฏิบัติงาน และการติดตามให้ปฏิบัติตามระเบียบขององค์การ

ขั้นที่ 3 ความเสี่ยงในเรื่องใดที่สรุปว่ามีการควบคุมไม่เพียงพอ ก็ให้ประเมินค่าความเสียหายที่อาจเกิดขึ้นออกมา และต้องตรวจสอบการควบคุมต่าง ๆ ภายในระบบงาน (APPLICATION CONTROLS) ด้วยว่าจะสามารถชดเชยการควบคุมทั่วไป (ENVIRONMENTAL CONTROLS) ที่ขาดหายไป ในระดับบริหารในเรื่องที่เกี่ยวข้องได้หรือไม่ แต่อย่างไรก็ดีมักจะเป็นเรื่องผิดปกติที่การควบคุมภายในระบบงานจะใช้ได้ผลถ้าการควบคุมทั่วไปบกพร่อง

ผู้สอบบัญชีจำเป็นต้องพิจารณาถึงวัตถุประสงค์ของการควบคุมทั่วไปกับความเสี่ยง (EXPOSURES) ที่อาจเกิดขึ้นง่ายๆ โดยนึกถึงวัตถุประสงค์ในการควบคุมว่า "ความถูกต้องในการปฏิบัติงานควรเป็นอย่างไร" แล้วพิจารณาถึงความเสี่ยงภัยที่อาจเกิดขึ้นได้ประกอบกันไปว่า "มีอะไรบ้างที่เป็นปัจจัยที่ทำให้เกิดข้อมูลที่ผิดพลาดได้" การพิจารณาในลักษณะนี้มักจะทำให้พบวัตถุประสงค์ของการควบคุมทั่วไปไว้ตั้งแต่ต้น

ความเสี่ยงภัยกับผู้บริหาร โดยแท้จริงแล้วก็คือ การสะท้อนให้เห็นถึงวัตถุประสงค์ของการควบคุมทั่วไปอย่างมีหลักเกณฑ์ในด้านที่เกี่ยวข้อง

2.3 ความเสี่ยงกับการวางแผน

การประเมินควบคุมภายใน เป็นขั้นตอนหนึ่งของการวางแผนงานสอบบัญชี ความเสี่ยงเป็นนามธรรมที่ไม่อาจตรวจสอบได้ แต่การวิเคราะห์ความเสี่ยงเป็นหลักสำคัญที่จะทำให้ผู้ตรวจสอบทราบถึงกิจกรรมที่อาจมีจุดอ่อนที่มีผลกระทบอย่างสำคัญต่อองค์การ เพื่อค้นหาจุดควบคุมหลักและจุดควบคุมรองต่าง ๆ ที่มีอยู่ในองค์การได้อย่างเหมาะสม ซึ่งจะช่วยให้การวางแผนการตรวจสอบมีหลักเกณฑ์ และช่วยให้ผู้บริหารมั่นใจประสิทธิภาพผลการตรวจสอบมากขึ้น

การวิเคราะห์และประเมินระบบการควบคุมภายในของระบบงาน จะรวมทั้งส่วนที่เป็น PHYSICAL และ LOGICAL เพื่อให้การตรวจสอบมีประสิทธิผลและประสิทธิภาพเต็มที่นั้น ผู้ตรวจสอบต้องสามารถกำหนดขอบเขตของระบบงานที่ประมวลด้วยคอมพิวเตอร์ และด้วย MANUAL ให้ได้เสียก่อน แล้วจึงค่อยๆแยกแยะไปในส่วนย่อย ๆ แตกแขนงกันออกไปในลักษณะของ TOP-DOWN BASIS เช่น ระบบเงินฝาก ก็จะต้องมีระบบการคำนวณดอกเบี้ยด้วย เป็นต้น กระบวนการวิเคราะห์แยกแยะในลักษณะของระบบงานนี้ ผู้ตรวจสอบจะต้องเข้าใจความหมายของคำว่า "มาตรฐานระบบงาน" ว่ามีขอบเขตเพียงใดก่อนด้วย

การประเมินจุดที่ควรมีการควบคุมนั้น ผู้ตรวจสอบไม่อาจกำหนดหรือคาดคะเนได้ล่วงหน้าเลย ถ้าไม่มีหลักการในการกำหนดจุดอ่อนที่ว่านั้น แนวความคิดในที่นี้ก็คือ การตั้งคำถามที่มีแบบแผนในแต่ละส่วนและในแต่ละหน้าที่ของงานที่ตรวจสอบนั้น ๆ เพื่อที่จะกำหนดได้ว่า ควรมีจุดควบคุมอะไรบ้าง ในขั้นตอนใด และในเวลาไหนของส่วนงานนั้น ๆ เช่น การตั้งคำถามดังนี้

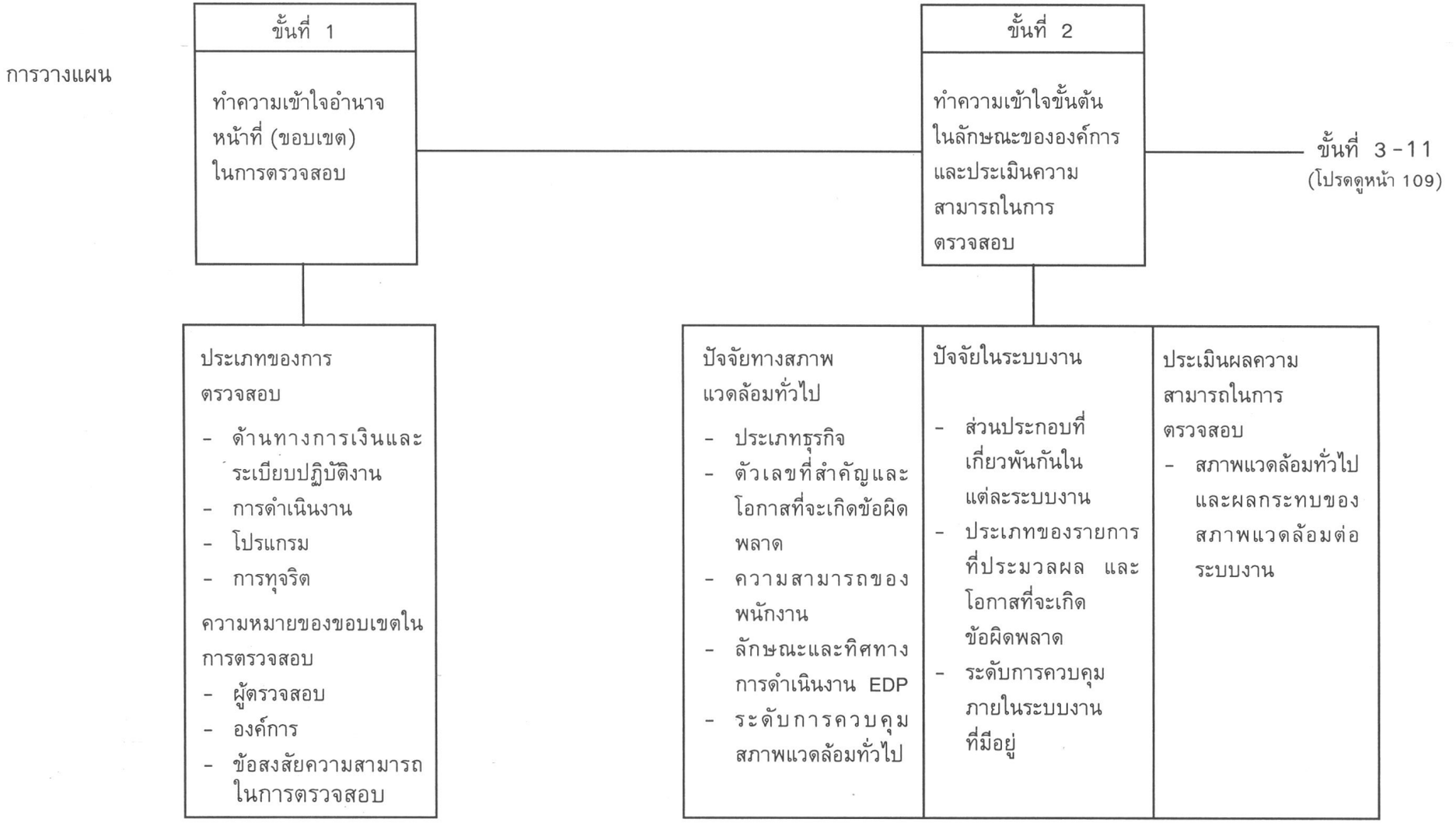
- ขั้นตอนนั้นเกี่ยวข้องกับหลักการบัญชีที่เป็นที่ยอมรับกันหรือไม่
- ขั้นตอนนั้นเกี่ยวข้องกับสินทรัพย์ในปัจจุบันหรือในภายหน้าหรือไม่
- ขั้นตอนนั้นเป็นขั้นตอนรับเงินหรือจ่ายเงิน
- ระบบงานนั้นๆจะมีผลกระทบต่อการบันทึกความถูกต้องของข้อมูลหรือไม่
- มีนโยบายหรือมีข้อผูกพันทางกฎหมาย และระเบียบข้อบังคับใด ๆ เกี่ยวข้องและต้องพิจารณาหรือไม่
- มีความเสี่ยงในขั้นตอนใด เมื่อพิจารณาในลักษณะ TOP-DOWN ของส่วนงานนั้น ๆ

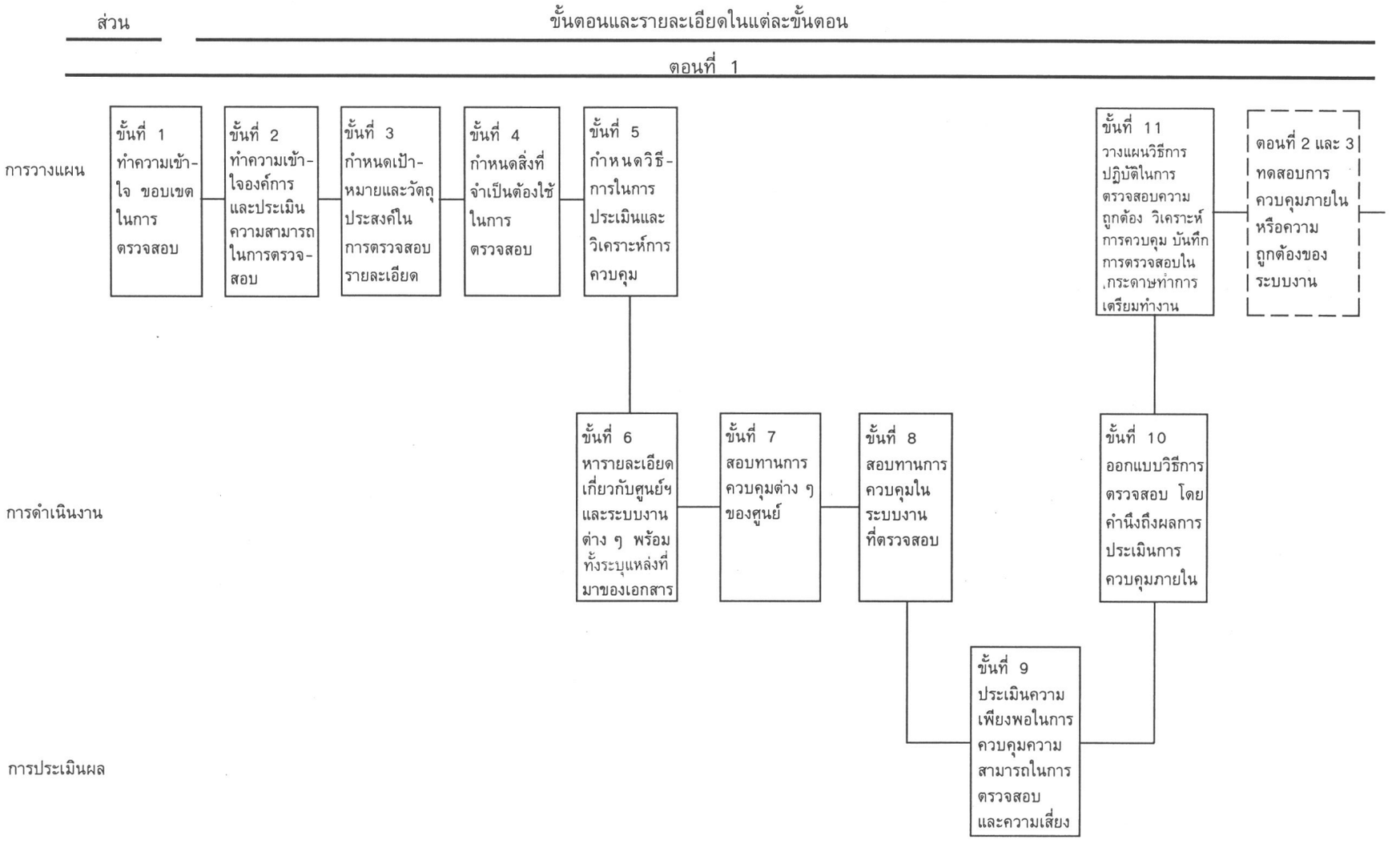
จากคำถามข้างต้นจะทำให้ผู้ตรวจสอบสามารถบ่งชี้ถึงจุดควบคุมภายในที่ควรจะมีได้ ทั้งในแบบ AUTOMATED และในระบบ MANUAL และสามารถกำหนดจุดควบคุมหลักและจุดควบคุมรอง เพื่อการวางแผนและการทดสอบต่อไปได้

ต่อไปนี้จะแสดงขั้นตอนของการวางแผนและการปฏิบัติงานตรวจสอบเป็นแผนภูมิอย่างละเอียด



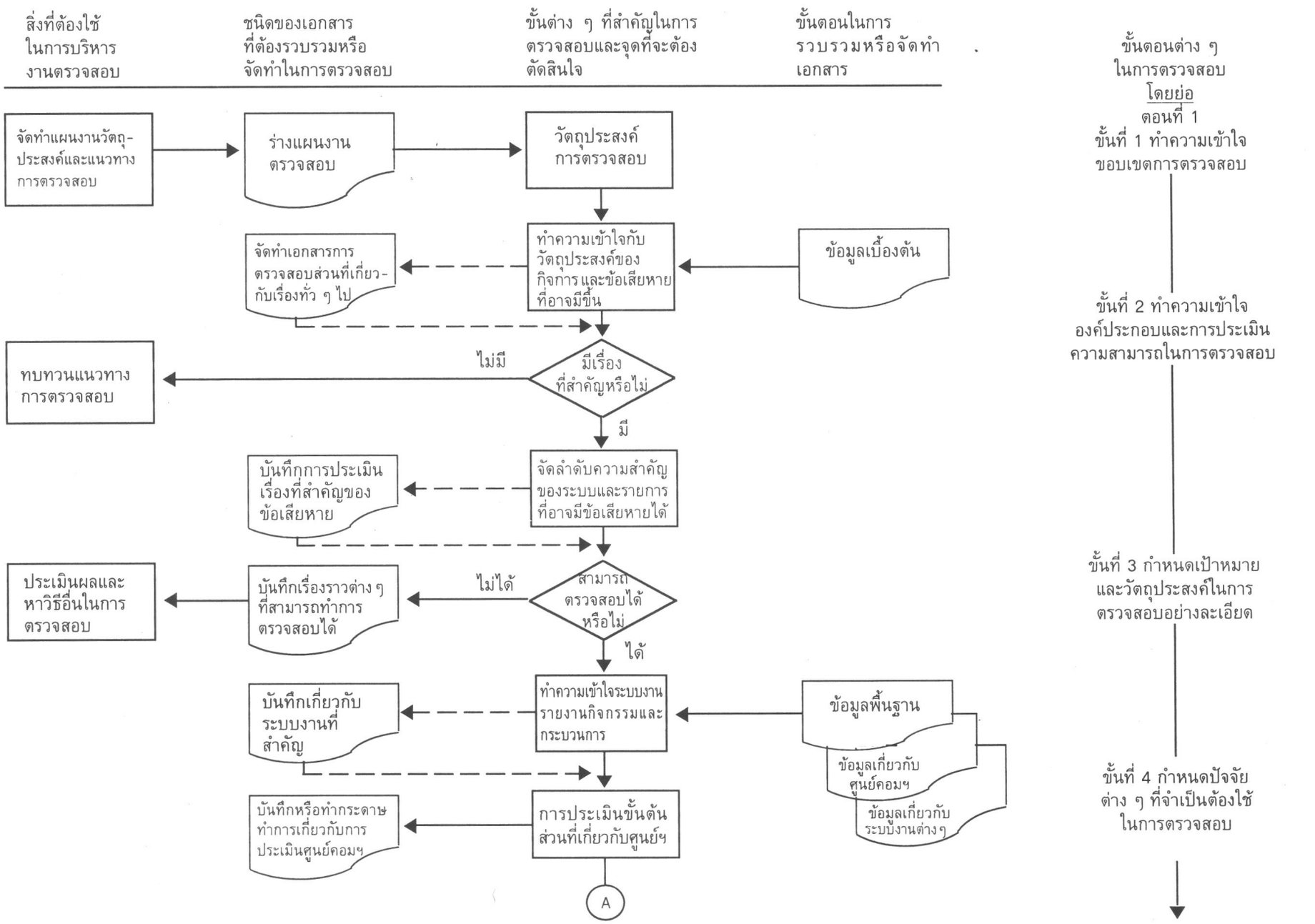
สรุป ขั้นตอนที่ 1 และ 2 ของการวางแผนงานตรวจสอบ



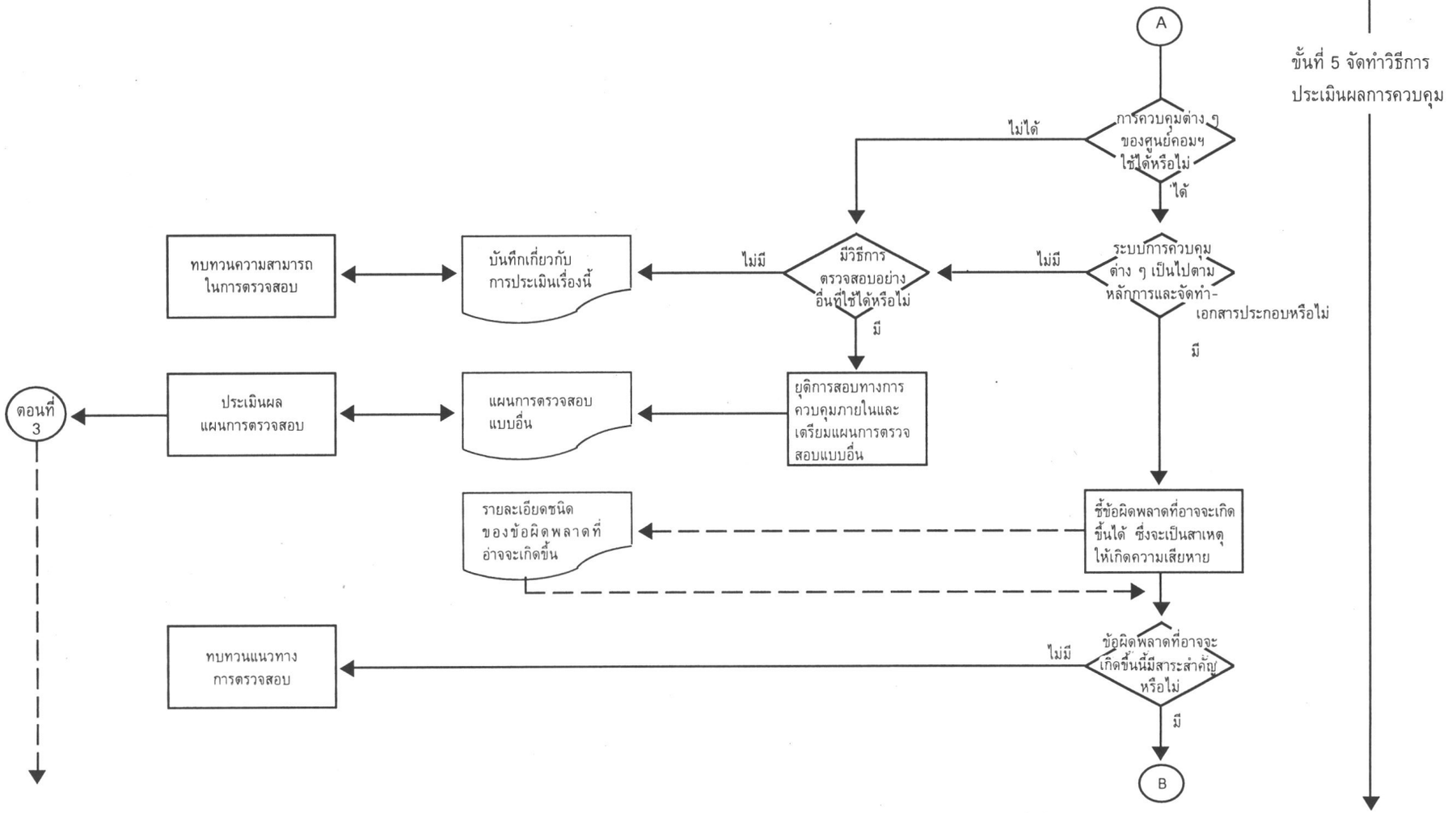


ตอนที่ 1 ขั้นตอนการสอบทาน ประเมินผลการควบคุมภายใน เพื่อใช้พิจารณากำหนดวิธีการตรวจสอบความถูกต้องของระบบงาน

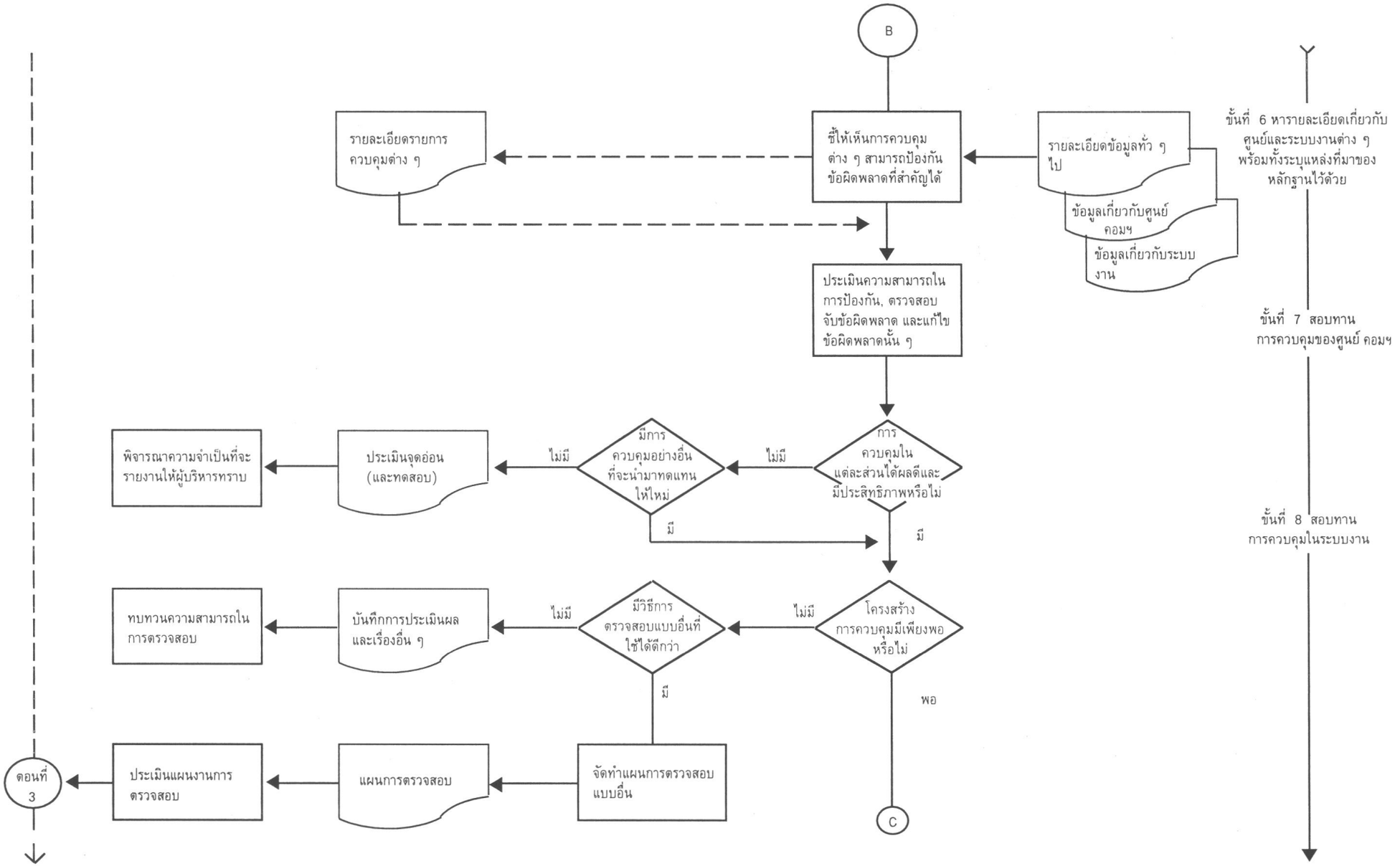
แผนภาพที่ 10.1 แสดงขั้นตอนความเกี่ยวพันในการวางแผนและการปฏิบัติงานตรวจสอบ



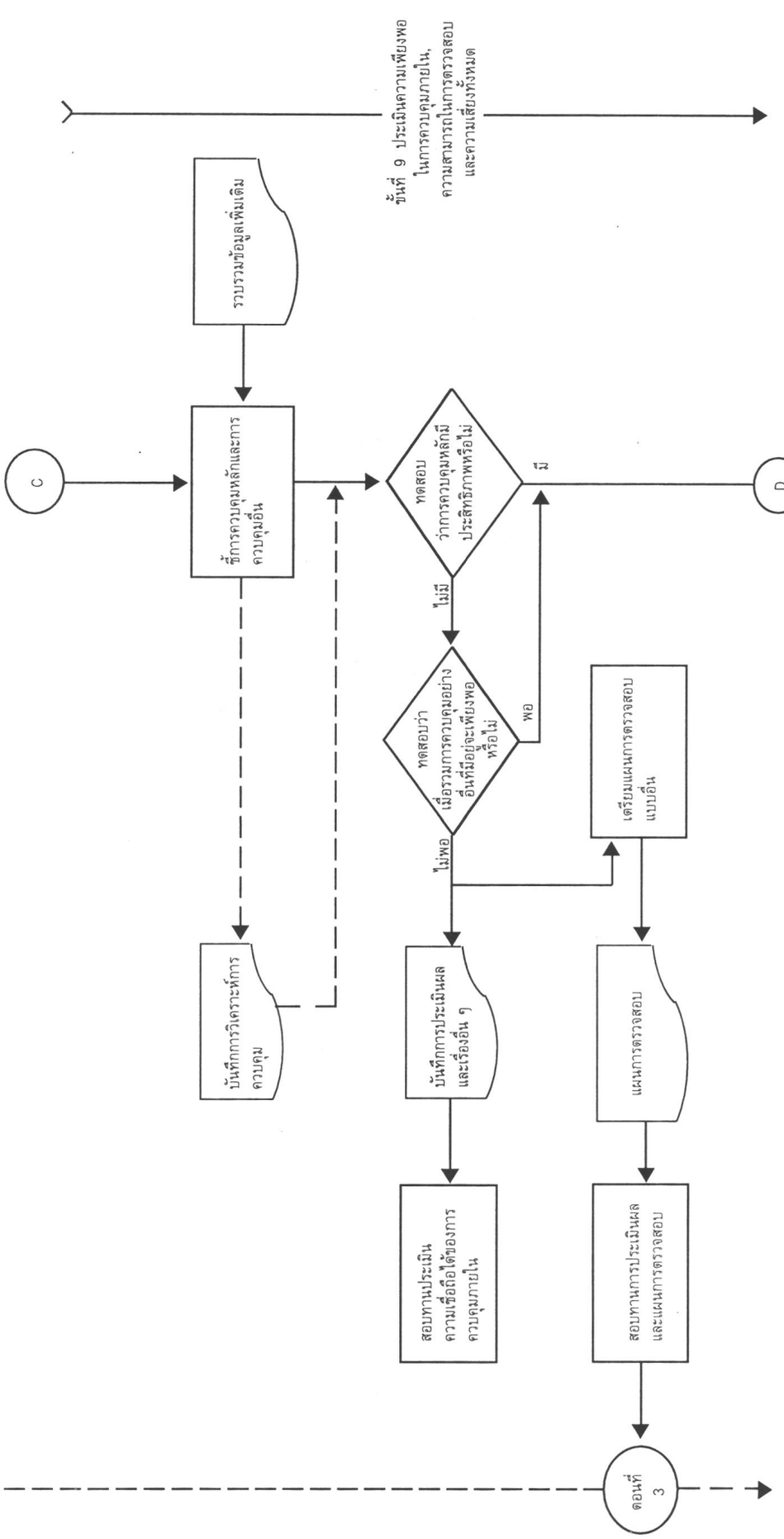
แผนภาพที่ 10.2 แสดงขั้นตอนความเกี่ยวพันในการวางแผนงานและการปฏิบัติงานตรวจสอบ (ต่อ)



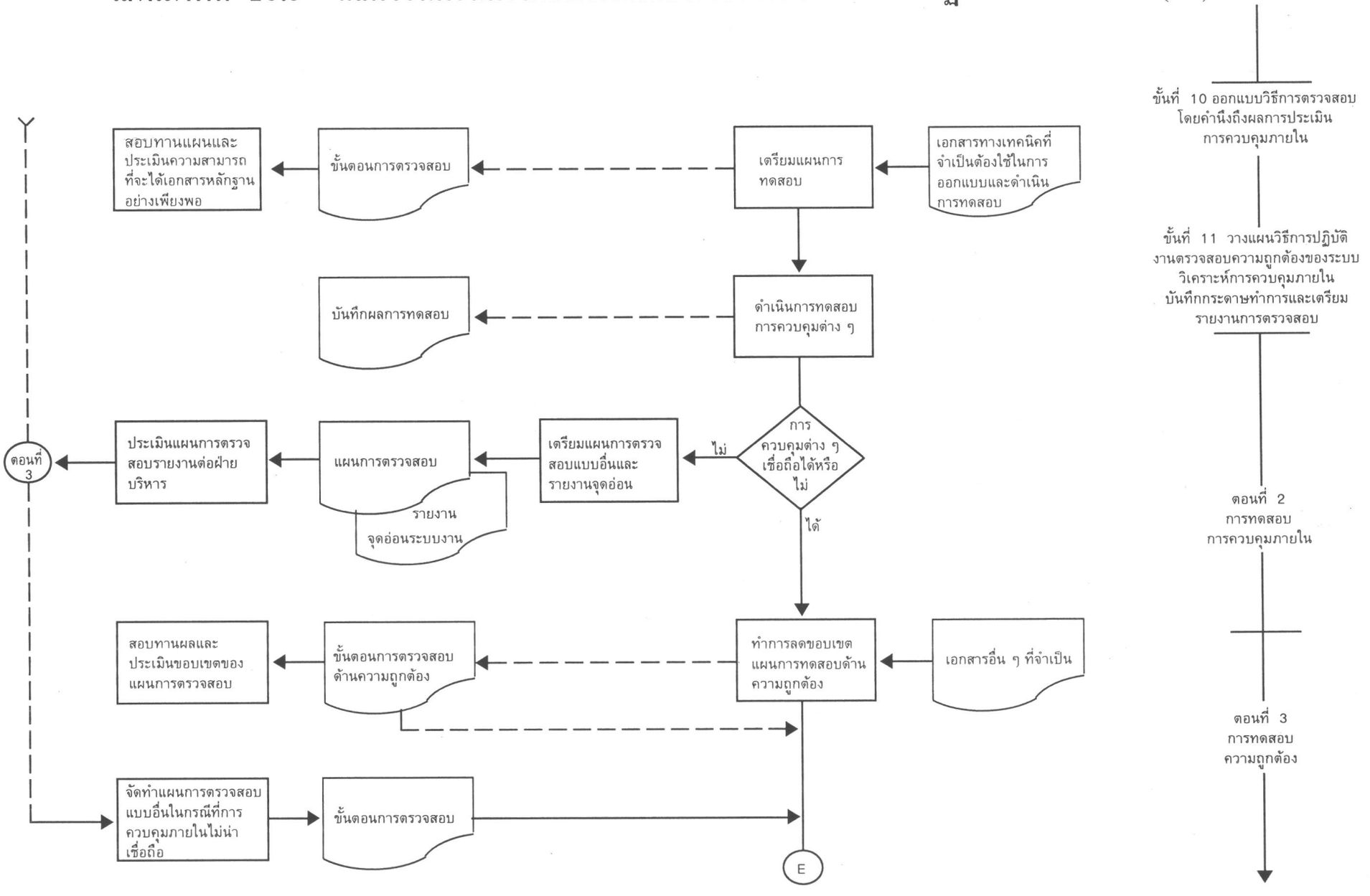
แผนภาพที่ 10.3 แสดงขั้นตอนความเกี่ยวพันในการวางแผนงานและการปฏิบัติงานตรวจสอบ (ต่อ)



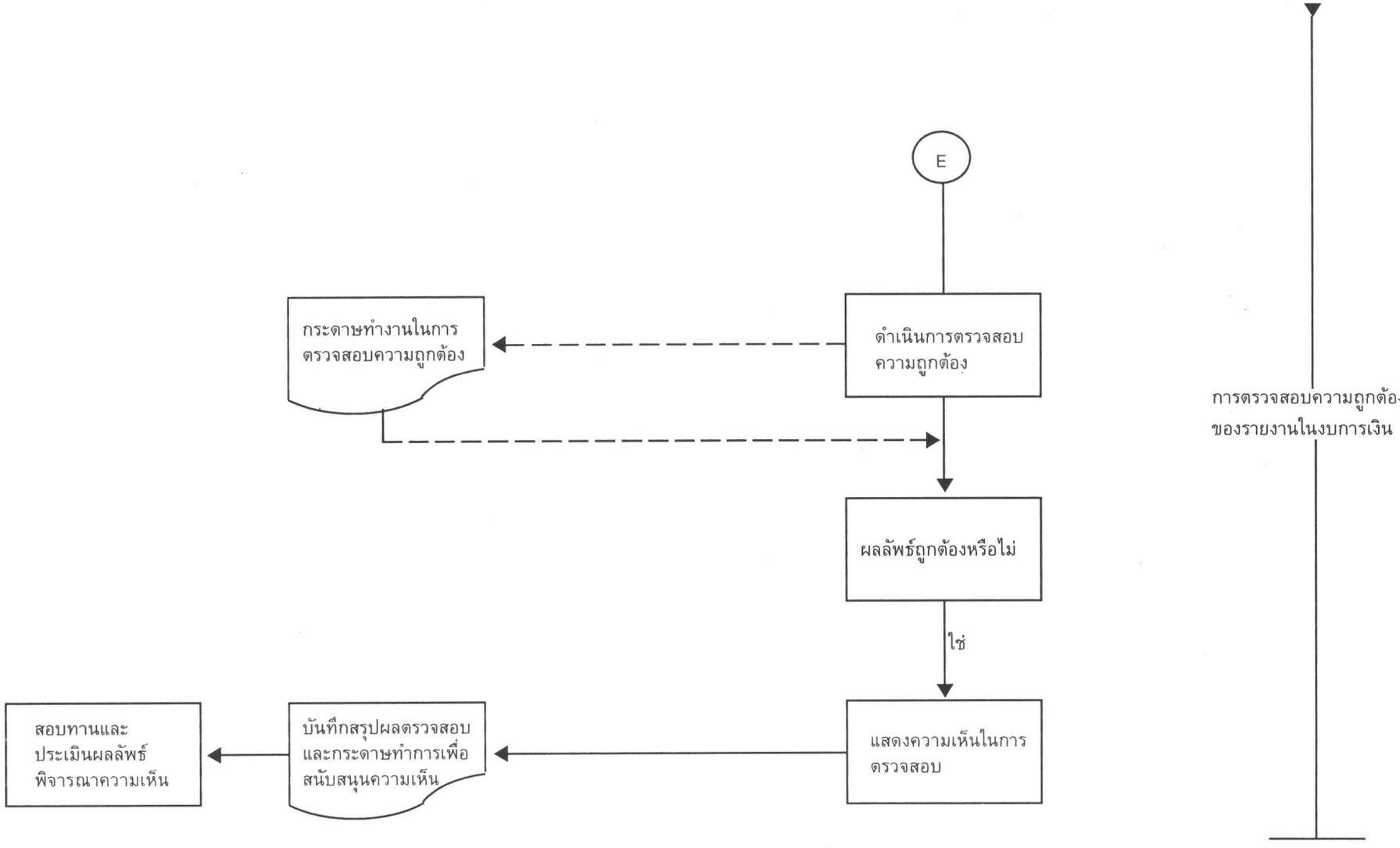
แผนภาพที่ 10.4 แสดงขั้นตอนความสัมพันธ์ในการวางแผนงานและการปฏิบัติงานตรวจสอบ (ต่อ)



แผนภาพที่ 10.5 แสดงขั้นตอนความเกี่ยวพันในการวางแผนงานและการปฏิบัติงานตรวจสอบ (ต่อ)



แผนภาพที่ 10.6 แสดงขั้นตอนความเกี่ยวพันในการวางแผนงานและการปฏิบัติงานตรวจสอบ (ต่อ)



11

สรุปปัจจัยต่าง ๆ ในการวางแผนการตรวจสอบ

สรุปปัจจัยต่าง ๆ ในการวางแผนการตรวจสอบ

ส่วนประกอบ	ประเภท	วัตถุประสงค์
<u>สภาพแวดล้อมทั่วไป</u>		
อำนาจหน้าที่ (ขอบเขต) ในการตรวจสอบ	ทางด้านการเงิน, ทางด้านปฏิบัติการ, ทางด้านคอมพิวเตอร์, การทุจริต	กำหนดประเภทการตรวจสอบ
ประเภทธุรกิจ	ประเภทสินทรัพย์และหนี้สินขนาดของการใช้คอมพิวเตอร์ ในการดำเนินงาน ชนิดของระเบียบกฎหมายต่าง ๆ	กำหนดขนาดการปฏิบัติงานตรวจสอบ
ตัวเลขที่สำคัญ, ลักษณะการดำเนินงาน	อัตราส่วนต่อยอดคงเหลือทั้งหมด ระดับความสำคัญ โอกาสที่จะเกิดความเสียหาย	กำหนดขนาดและแนวทางการปฏิบัติงานตรวจสอบ
ความสามารถของพนักงาน	สูง, ปานกลาง, ต่ำ	กำหนดขนาดการปฏิบัติงานตรวจสอบ
ขนาดและทิศทางในการดำเนินงาน EDP	ขนาด - เล็ก, กลาง, ใหญ่ ทิศทาง - คงที่ - ความเปลี่ยนแปลงอย่างรวดเร็ว - การเข้าร่วมตัดสินใจของฝ่ายบริหาร	กำหนดความรู้ความชำนาญของผู้ตรวจสอบและแนวทางการตรวจสอบในปัจจุบันและอนาคต
ส่วนประกอบของโปรแกรมระบบงาน		กำหนดความรู้ความชำนาญของผู้ตรวจสอบ และแนวทางกิจกรรมการตรวจสอบ

ส่วนประกอบ	ประเภท	วัตถุประสงค์
ระดับการควบคุมสภาพแวดล้อม	แข็ง, ปานกลาง, อ่อน	กำหนดว่าจุดที่จะตรวจสอบและ จุดใดที่น่าเชื่อถือได้
<u>ระบบงาน</u>		
ส่วนประกอบที่เกี่ยวพันในระบบงาน	ง่าย, ธรรมดา, ซับซ้อน	กำหนดความรู้ความชำนาญของผู้ตรวจสอบ
ประเภทรายการที่ประมวลผลและข้อผิดพลาดที่อาจจะเกิดขึ้น	รายการ ระบบงานย่อย ระบบงานที่สำคัญ ข้อผิดพลาดที่อาจเกิดขึ้น ผลกระทบของข้อผิดพลาดต่อบัญชี แข็ง, ปานกลาง, อ่อน	กำหนดรายการที่จะต้องตรวจสอบ และประเมินโอกาสที่จะเกิดข้อผิดพลาด
ระดับการควบคุมระบบงาน	สูง, ปานกลาง, ต่ำ	กำหนดว่าการควบคุมในจุดใดน่าเชื่อถือได้ และควรตรวจสอบอย่างไร
ความน่าเชื่อถือของระบบงาน	แข็ง, ปานกลาง, อ่อน	กำหนดขนาดและประเภทการตรวจสอบ
<u>การประเมินผล</u>		
สภาพแวดล้อมทั้งหมดและผลกระทบของสภาพแวดล้อมต่อระบบงาน และความน่าเชื่อถือในการควบคุมภายใน		กำหนดความสามารถที่จะตรวจสอบแนวทางการตรวจสอบและปัจจัยต่าง ๆ ที่จำเป็น



12

เปรียบเทียบขอบเขตและความสัมพันธ์ระหว่างการตรวจสอบของผู้สอบบัญชีภายนอกกับผู้สอบบัญชีภายใน

เปรียบเทียบขอบเขตความรับผิดชอบและความสัมพันธ์ของผู้สอบบัญชีภายนอกและผู้สอบบัญชีภายใน ทั้งองค์กรที่ใช้คอมพิวเตอร์และไม่ใช้คอมพิวเตอร์

ผู้สอบบัญชีรับอนุญาต (CPA)	ผู้สอบบัญชีภายใน (Internal Auditor)
เน้นด้านความน่าเชื่อถือ และความเสียหายที่อาจเกิดขึ้นได้ทางด้านการเงิน (Financial exposures) รับผิดชอบและเสนอความเห็นต่องบการเงินขององค์กร โดยตรวจสอบความน่าเชื่อถือได้ของงบการเงิน และผลกระทบที่อาจก่อให้เกิดความเสียหายต่อองค์กรและรายงานผลต่อผู้ถือหุ้นและองค์กรที่เกี่ยวข้อง	เน้นด้านการปฏิบัติงานและความเสียหายที่อาจจะเกิดขึ้นจากการไม่ปฏิบัติตามระเบียบกฎเกณฑ์ที่กำหนดขึ้นโดยองค์กร (Operational exposures) รับผิดชอบและตรวจสอบทางด้านการปฏิบัติตามนโยบาย กฎเกณฑ์ คำสั่ง ระเบียบต่าง ๆ และความเสียหายที่อาจจะเกิดขึ้นภายในขององค์กรเป็นหลัก โดยทั่วไปจะรายงานต่อคณะกรรมการหรือผู้บริหารระดับสูงสุดขององค์กร

ความสัมพันธ์และข้อแตกต่างของผู้สอบบัญชีรับอนุญาตกับผู้สอบบัญชีภายใน		
เน้นตรวจสอบความถูกต้องและความเสียหายที่อาจจะเกิดจากรายการทางการเงินในงบการเงินขององค์กร (Substantive Audit) มากกว่าการทำ Compliance audit	ตรวจสอบและประเมินการปฏิบัติตามนโยบาย ระเบียบและคำสั่งต่างๆ(Compliance Audit)ขององค์กรในขอบเขตที่จำกัดเพื่อกำหนดขอบเขตการตรวจสอบทางการเงินที่เหมาะสม	ตรวจสอบการปฏิบัติตามระเบียบ กฎเกณฑ์ และคำสั่งต่าง ๆ ขององค์กรเป็นหลัก (Compliance Audit) และจะปฏิบัติการตรวจสอบทางด้านการเงินแต่เพียงเล็กน้อย เพียงเพื่อยืนยันการทำ Compliance audit

ผู้สอบบัญชีภายนอก (External Auditor)	ผู้สอบบัญชีภายใน (Internal Auditor)
ผู้สอบบัญชีภายนอก (External Auditor) หรือผู้สอบบัญชีรับอนุญาต (Certified Public Accountant - CPA) จะทำการประเมินระบบการควบคุมภายใน ซึ่งเป็นการตรวจสอบด้าน Compliance Audit ส่วนหนึ่ง เพื่อกำหนดขอบเขตการตรวจสอบงบการเงินตามมาตรการตรวจสอบ ทั้งนี้ ผู้สอบบัญชีภายนอกจะทำหน้าที่ส่วนหนึ่งคล้ายกับผู้ตรวจสอบภายในด้วย นั่นคือ การตรวจสอบการปฏิบัติงานและการปฏิบัติตามระเบียบคำสั่งขององค์กรในด้านต่าง ๆ เพียงเท่าที่จำเป็นตามมาตรฐาน แต่ไม่ใช่เป็นงานหลักของ External Auditor หรือ CPA (Certified Public Accountant - CPA) นอกจากนี้ผู้สอบบัญชีภายนอกจะต้องทำการทดสอบรายการคงเหลือต่าง ๆ ในงบการเงิน เพื่อรับรองและแสดงความเห็นต่องบการเงิน ซึ่งเป็นหน้าที่หลัก	ผู้สอบบัญชีภายใน (Internal auditor) มีหน้าที่หลักที่สำคัญ คือ การตรวจสอบนโยบายการควบคุมภายใน รวมทั้งการปฏิบัติตามระเบียบคำสั่งต่าง ๆ ทั้งด้านการปฏิบัติงานและการบัญชีขององค์กร แล้วรายงาน ตลอดจนให้คำแนะนำแก่ผู้บังคับบัญชาในด้านที่เกี่ยวข้องกับงานที่กล่าวข้างต้น ที่จะปรับปรุงงานให้มีประสิทธิภาพยิ่งขึ้น แต่ไม่มีหน้าที่ในการออกความเห็นต่องบการเงินโดยตรง แต่อาจตรวจสอบรายการทางการเงินหรือยอดคงเหลือทางการเงินต่าง ๆ (Substantive test) ซึ่งเป็นหน้าที่หลักของผู้สอบบัญชีภายนอกเพียงส่วนน้อย เพื่อยืนยันผลการปฏิบัติงานทาง Compliance Audit ดังนั้น ส่วนหนึ่งที่สัมพันธ์กันคือ ทั้งผู้สอบบัญชีภายในและผู้สอบบัญชีภายนอกต้องตรวจสอบ Compliance Audit และ substantive Audit โดยมีขอบเขตและความรับผิดชอบแตกต่างกันไปตามเป้าหมายและหน้าที่การตรวจสอบของตน

หากมีผู้สนใจใคร่จะทราบว่า ผู้สอบบัญชีภายนอก (External auditor) หรือผู้สอบบัญชีรับอนุญาต (CPA) กับผู้ตรวจการธนาคารพาณิชย์ ผู้ตรวจสอบสถาบันการเงินของทางการ (Financial Examiner) หรือเรียกรวมๆ ว่า examiner ซึ่งพิจารณาว่าเป็นผู้สอบบัญชีภายนอกประเภทหนึ่งด้วยนั้น มีความสัมพันธ์และแตกต่างกันอย่างไร ในประเด็นนี้ ใคร่ขอสรุปข้อแตกต่างที่สำคัญย่อ ๆ ระหว่างผู้สอบบัญชีทั้งสองประเภท ดังนี้

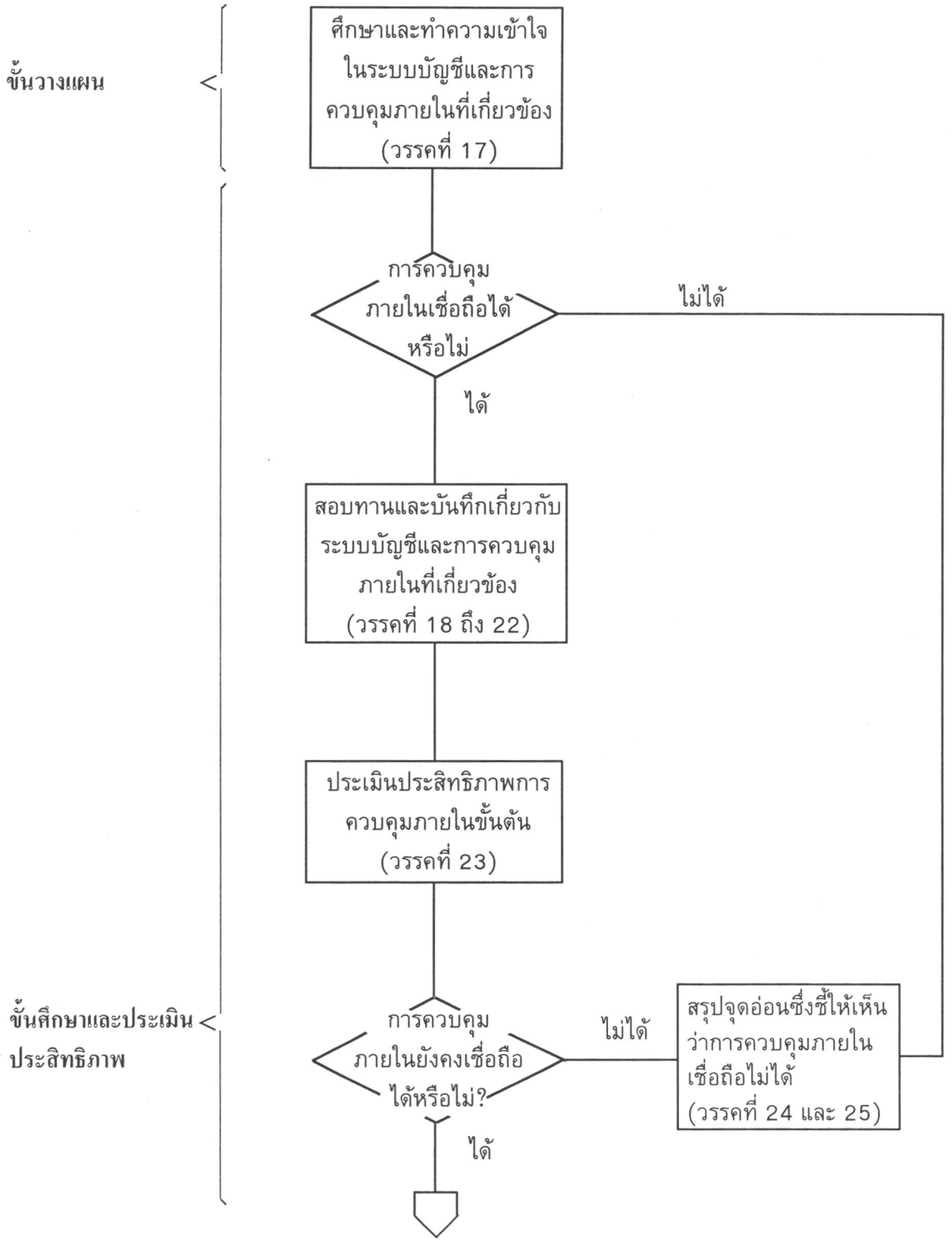


Examiner	External Auditor หรือผู้สอบบัญชีรับอนุญาต (CPA)
1. เป็นผู้ตรวจสอบจากทางการ เช่น ธนาคารแห่งประเทศไทย หรือ OCC, FRB, FDIC ของสหรัฐอเมริกา เป็นต้น	1. เป็นผู้สอบบัญชีรับอนุญาตทั่วไปและประกอบอาชีพเป็นอิสระในกรอบที่กำหนดของทางการ โดยมีมาตรฐานและต้องมีใบอนุญาตให้เป็นผู้สอบบัญชีของกระทรวงพาณิชย์
2. ปฏิบัติงานภายใต้กฎหมายเฉพาะกิจที่เกี่ยวข้องเช่น พรบ.การธนาคารพาณิชย์ พรบ. การประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์ และธุรกิจเครดิตฟองซิเอร์ไม่ตรวจสอบองค์กรอื่น ๆ ที่ไม่เกี่ยวข้องกับพรบ.ดังกล่าว	2. ปฏิบัติงานตามที่กำหนดโดยกระทรวงพาณิชย์ (ก.บช.)ต่อองค์กรทั่ว ๆ ไป รวมทั้งธนาคารพาณิชย์ สถาบันการเงินต่าง ๆ ด้วย
3. หน้าที่หลักคือ การตรวจสอบและดูแลให้คำแนะนำเกี่ยวกับฐานะและความมั่นคงของสถาบันการเงิน เพื่อประโยชน์แก่ระบบการเงินของประเทศโดยรวม และเพื่อประชาชนและบุคคลที่เกี่ยวข้อง	3. หน้าที่หลักคือ การตรวจสอบหรือรับรองงบการเงิน และให้ความเห็นต่องบการเงินนั้น ในฐานะผู้สอบบัญชีอิสระ เพื่อผลประโยชน์ของผู้ถือหุ้น และประชาชนผู้ที่เกี่ยวข้อง
4. เป้าหมายการตรวจสอบต่างกับผู้สอบบัญชีรับอนุญาต (CPA) หรือผู้สอบบัญชีภายนอก และก็ต่างกับผู้สอบบัญชีภายในด้วย แต่การวางขอบเขตการตรวจสอบก็อาศัยความน่าเชื่อถือ หรือประสิทธิภาพของการตรวจสอบทั้งของ Internal Auditor และ External Auditor มาช่วยด้วย	4. ขอบเขตการตรวจสอบแตกต่างกันไป ตามเป้าหมายและหน้าที่หลัก ๆ ตามที่กล่าวข้างต้น
5. ความถี่ในการตรวจสอบขึ้นอยู่กับความจำเป็นของฐานะและความมั่นคงของสถาบันการเงินแต่ละแห่ง เช่น อาจตรวจสอบปีละ 2 ครั้ง หรือ 2-3 ปีต่อครั้งก็ได้ตามความจำเป็น	5. ปกติตรวจสอบปีละครั้ง แต่อาจมีการทำ Internal Audit ระหว่างปี
6. เป็นองค์กรอิสระ และผู้ตรวจสอบไม่จำเป็นต้องเป็นผู้สอบบัญชีรับอนุญาต (CPA)	6. ผู้ตรวจสอบอยู่ภายใต้การดูแลและกำกับของทางการ ทั้งกระทรวงพาณิชย์และธนาคารแห่งประเทศไทย
7. รายงานต่อกระทรวงการคลัง และประธานกรรมการของสถาบันการเงินที่เกี่ยวข้อง	7. รายงานต่อผู้ถือหุ้นหรือผู้เป็นหุ้นส่วน และส่งให้กระทรวงพาณิชย์

13

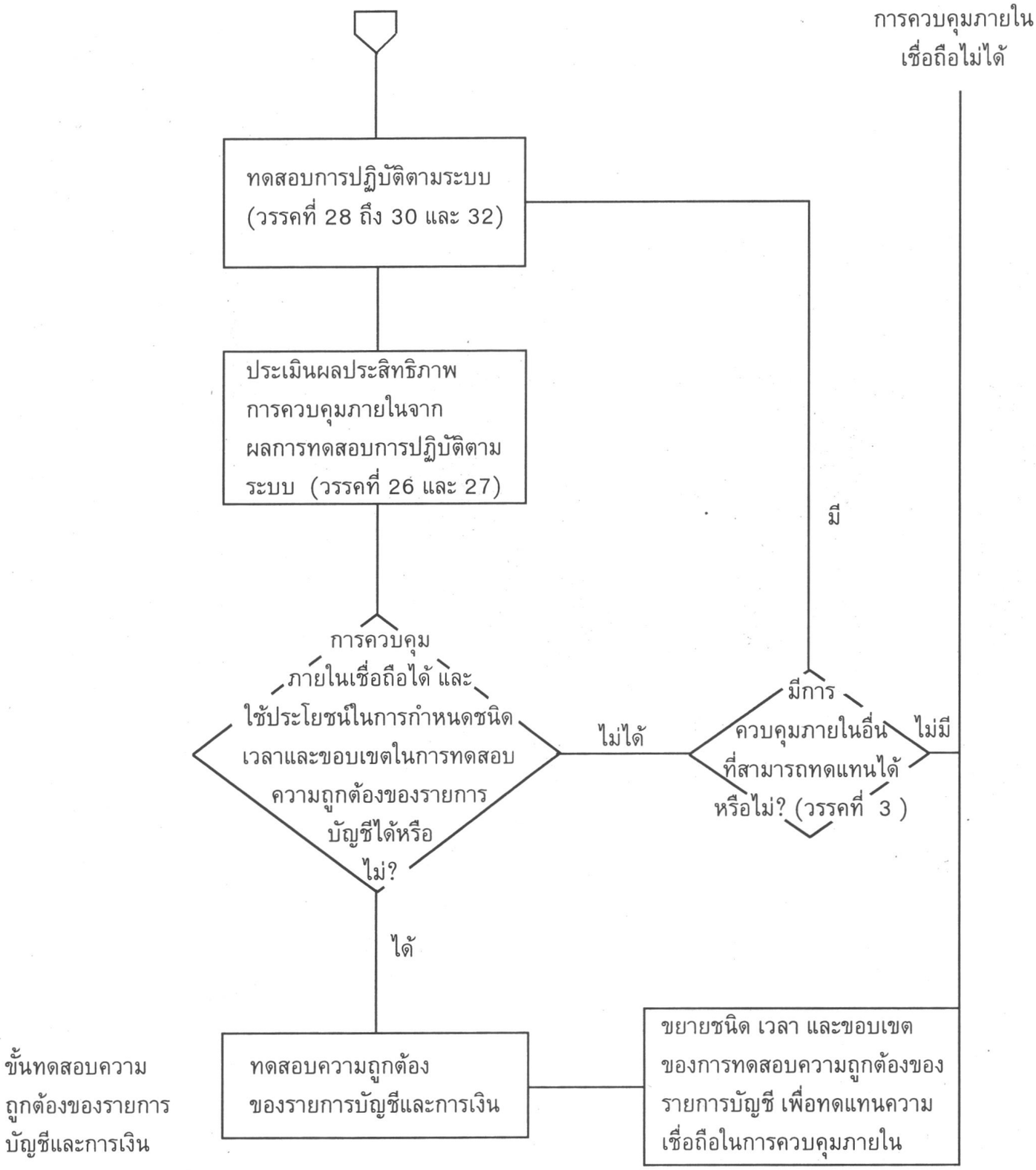
แผนภาพแสดงขั้นตอนของการประเมินประสิทธิภาพการควบคุมภายใน

แผนภาพการแสดงขั้นตอนของการประเมินประสิทธิภาพการควบคุมภายใน



หมายเหตุ : เป็นการย้ำให้ผู้ตรวจสอบและผู้บริหารเข้าใจถึงมาตรฐานการตรวจสอบแบบหนึ่ง ซึ่งใช้ได้ทั่ว ๆ ไปในองค์กรที่ไม่ใช้คอมพิวเตอร์และใช้คอมพิวเตอร์

แผนภาพแสดงขั้นตอนของการประเมินประสิทธิภาพการควบคุมภายใน (แผ่น 2)



14

แผนภาพแสดงกระบวนการ 3 ขั้นตอนในการตรวจสอบ

แผนภาพแสดงกระบวนการ 3 ขั้นตอนในการตรวจสอบ





15

สรุป : ข้อควรทราบสำหรับผู้ตรวจสอบโดยทั่วไป ก่อนการเข้าตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

ผลกระทบของคอมพิวเตอร์ต่อกระบวนการตรวจสอบทั่วไป

สรุปเป็นข้อ ๆ เพื่อความเข้าใจง่าย ๆ ได้ดังนี้

1. วัตถุประสงค์เป้าหมายหลัก ๆ ของการตรวจสอบไม่เปลี่ยนแปลงไปจากระบบ Manual
2. สิ่งที่เปลี่ยนแปลงไปก็คือ เทคนิคและวิธีการตรวจสอบ ตลอดจนขอบเขตการตรวจสอบเปลี่ยนแปลงไป
3. หลักฐานการตรวจสอบเปลี่ยนแปลงไปอย่างมากมาย ทั้งในรูปแบบที่ไม่สามารถมองเห็นได้ด้วยตา และรูปแบบที่มองเห็นได้ด้วยตา นี่คือสิ่งสำคัญและท้าทายอย่างยิ่งต่อการตรวจสอบ
4. ระบบงานและการควบคุมภายใน มีทั้งระบบ Manual เดิมมีทั้งระบบที่ประมวลข้อมูลด้วยคอมพิวเตอร์ล้วน ๆ มีทั้งแบบผสมระหว่าง Manual กับคอมพิวเตอร์ ผู้ตรวจสอบโดยทั่วไปจึงควรทำความเข้าใจกับระบบงานทั้ง 3 ส่วน ตามมาตรฐานการตรวจสอบด้วย
5. คอมพิวเตอร์สร้างข้อมูลใหม่ได้ ลบหรือล้าง หรือซ่อนเร้นข้อมูลที่ไม่ต้องการให้เปิดเผยได้ ทั้งในแบบถาวรหรือชั่วคราว ทั้งนี้เป็นไปตามโปรแกรมระบบงานที่จัดทำไว้ ผู้ตรวจสอบจึงต้องเข้าใจ logic หรือต้องเข้าใจหลักการทำงานของระบบคอมพิวเตอร์ให้ถ่องแท้ เพื่อให้การทำความเข้าใจต่อระบบงาน การวางแผนการตรวจสอบ การกำหนดขอบเขตการตรวจสอบ เป็นไปได้อย่างมั่นใจ เพราะตัวเลขหรือข้อมูลใน Hard copy นั้น มักใช้เป็นแนวทางหลักในการตรวจสอบงบการเงิน หรือบริหารการเงินค่อนข้างมาก และข้อมูลจาก Hard copy นี้ได้ทำให้ผู้บริหารตัดสินใจผิด ๆ และถูกหลอกจากการทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือมาไม่น้อยเลย
6. คอมพิวเตอร์สามารถสร้างข้อมูลในระบบรายงาน ตลอดจนการเข้าถึงข้อมูลได้หลายลักษณะตามความ ต้องการของผู้บริหารและ/หรือผู้ใช้ ดังนั้น ผู้ตรวจสอบควรได้ทราบถึงรายงานแบบต่าง ๆ ที่อาจมีประโยชน์ที่ใช้ในการตรวจสอบได้
7. แนวการตรวจสอบ รวมทั้งร่องรอยการตรวจสอบเปลี่ยนแปลงไป
8. รูปแบบและวิธีการประเมินการควบคุมภายในเปลี่ยนแปลงไป
9. รูปแบบของการจัดเก็บข้อมูล ฐานข้อมูลเปลี่ยนแปลงไป
10. มีการใช้ผู้เชี่ยวชาญเฉพาะด้านที่เกี่ยวกับคอมพิวเตอร์ช่วยงานตรวจสอบมากขึ้น
11. มีการใช้คอมพิวเตอร์เข้าช่วยในการตรวจสอบ
12. ต้องเปลี่ยนรูปแบบในการวางแผนการตรวจสอบค่อนข้างมาก เพราะการตรวจสอบในลักษณะ Substantive test หลายลักษณะ มีปัญหาค่อนข้างมาก และบางกรณีก็ไม่อาจทำได้ด้วยวิธีปกติ
13. หากผู้ตรวจสอบเชื่อถือในระบบการควบคุมภายในและระบบงานขององค์กรที่ใช้คอมพิวเตอร์หรือตั้งข้อสมมุติฐานว่าการประมวลงานโดยระบบคอมพิวเตอร์ขององค์การนั้นเชื่อถือได้ โดยข้ามขั้นตอนหลัก ๆ ของการศึกษาระบบงานและการควบคุมภายในเบื้องต้นแล้ว การตรวจสอบในลักษณะ Manual เดิมโดยอาศัย Report หรือ Hard copy ขององค์นั้น ๆ โดยมีเป้าหมายเฉพาะอย่างก็อาจดำเนินการไปโดยใช้เทคนิคดั้งเดิมแบบ Manual ได้ระดับหนึ่ง แต่ทั้งนี้ผู้ตรวจสอบควรหมายเหตุให้ผู้อ่านงบการเงินได้ทราบถึงขอบเขตหรือข้อจำกัดนั้นให้ผู้ใช้ข้อมูลได้ทราบด้วย

หมายเหตุ

โปรดสังเกตทำความเข้าใจกับข้อสังเกตบางประการในการใช้คอมพิวเตอร์ช่วยในการประมวลข้อมูลในหน้าถัดไปด้วย

โปรดอ่านมาตรฐานการสอบบัญชีของ ก.บช. และสมาคมฯ ฉบับที่ 28,29 และฉบับที่ 36 ซึ่งอยู่ในเล่ม 1 แล้ว

ข้อสังเกตบางประการในการใช้คอมพิวเตอร์ช่วยในการประมวลข้อมูล

1. ไม่ทำให้เป้าหมายของการควบคุมภายในและหลักพื้นฐานเกี่ยวกับการควบคุมแตกต่างออกไป
2. แต่จำเป็นต้องมีวิธีการควบคุมใหม่ที่เหมาะสมเพิ่มขึ้น ในขณะที่วิธีการควบคุมแบบเดิมบางชนิดอาจใช้ไม่ได้ต่อไป
3. เอกสารแสดงให้เห็นถึงการปฏิบัติหน้าที่ในการควบคุมทางการบัญชีมีน้อยลง
4. ข้อมูลที่เก็บไว้ในระบบคอมพิวเตอร์มองไม่เห็นด้วยตาเปล่า ต้องอาศัยคอมพิวเตอร์เข้าช่วยจึงสามารถทราบได้ว่ามีข้อมูลอะไรอยู่บ้าง
5. ระบบข้อมูลที่ใช้คอมพิวเตอร์มีความเสี่ยงภัยต่อการเสียหายสูงกว่าระบบข้อมูลที่ไม่ใช้คอมพิวเตอร์
6. ต้องอาศัยการวางแผนและการคาดคะเนปัญหาและเหตุการณ์ในอนาคตอย่างรอบคอบ
7. งานที่ปฏิบัติโดยบุคคลหลาย ๆ ฝ่ายอาจมารวมอยู่ด้วยกัน และปฏิบัติโดยคอมพิวเตอร์
8. สามารถใช้คอมพิวเตอร์ช่วยในการควบคุมได้ และในขณะเดียวกันก็สามารถใช้คอมพิวเตอร์ช่วยในการทำทุจริตได้ด้วยเช่นกัน

การเข้าใจระบบงานที่ใช้คอมพิวเตอร์ จะช่วยผู้สอบบัญชีได้อย่างไร

การศึกษาถึงขั้นตอนการตรวจสอบระบบในส่วนรวม (Total System Approaches) จะช่วยงานตรวจสอบของผู้สอบบัญชีได้ดังนี้ คือ

1. รู้ว่ามีงานอะไรบ้างที่สมควรจะต้องเข้าไปตรวจสอบ และควรจะเริ่มงานอย่างไร
2. รู้ว่ามีเอกสารเกี่ยวกับอะไรบ้างที่ควรได้รับการตรวจสอบ
3. รู้ขั้นตอนการปฏิบัติงาน และรู้ว่าควรจะทำเมื่อใด
4. รู้ว่าเมื่อใดที่ฝ่ายบริหารควรจะเข้ามามีส่วนในการตัดสินใจก่อนที่จะเริ่มงานตรวจสอบต่อไป

องค์ประกอบในการตรวจสอบในแต่ละเรื่อง

ในการตรวจสอบในเรื่องใด ๆ ก็ตาม ควรมีองค์ประกอบในการตรวจสอบดังต่อไปนี้

- วัตถุประสงค์ที่ต้องการบรรลุ
- กิจกรรมที่มีอยู่ในแต่ละเรื่อง หรือในแต่ละขั้นตอนที่จะตรวจสอบหรือเกิดขึ้นในการประมวลผลรายการ
- ข้อผิดพลาดที่อาจเกิดขึ้นได้ในแต่ละขั้นตอนการประมวลผล สาเหตุของข้อผิดพลาด ความบ่อย และขนาดของข้อผิดพลาดที่อาจจะเกิดขึ้น
- การควบคุมที่สามารถกำหนดเพื่อป้องกันสาเหตุของข้อผิดพลาด หรือติดตามและแก้ไขข้อผิดพลาดและประสิทธิผลของการควบคุมเหล่านั้น
- จุดอ่อนที่สามารถเกิดขึ้นได้ถ้าการควบคุมสาเหตุของข้อผิดพลาดและจุดอ่อนนั้น ๆ ขาดประสิทธิผล
- การทดสอบเพื่อตรวจสอบการควบคุมจุดอ่อนอย่างเหมาะสม

แนวคำถามที่จะแสดงต่อไปเป็นคำถามที่ผู้ตรวจสอบต้องตอบ ซึ่งแม้ผู้ตรวจสอบจะคุ้นเคยดี แต่ก็มีประเด็นที่ต้องพิจารณาในการเริ่มการตรวจสอบ ซึ่งมี 4 อย่าง คือ

1. การมองผังทางเดินของกิจกรรมและความสัมพันธ์กับข้อผิดพลาดหรือการควบคุมที่เกี่ยวข้องให้ออก
2. การพิจารณาตัดสินใจเลือกเอกสารที่จำเป็นในการทำความเข้าใจกิจกรรมต่าง ๆ และการหาจุดที่อาจเกิดข้อผิดพลาด ระดับและความบ่อยของข้อผิดพลาดที่อาจเกิดขึ้น จุดที่ควรมีการควบคุม และจะประสานทั้งสองสิ่งอย่างไรในลักษณะที่เหมาะสม และเป็นเหตุเป็นผลต่อกัน
3. เพื่อเข้าใจว่าการควบคุมบางอันมีประสิทธิภาพและประสิทธิผลเหนือการควบคุมอื่น และในบรรดาการควบคุมอื่น ๆ นั้นอาจมีประสิทธิผลและประสิทธิภาพพอ ๆ กัน
4. เพื่อเข้าใจว่าจุดอ่อนบางอันอาจไม่มีความสำคัญต่อวัตถุประสงค์ในการตรวจสอบเลย ในขณะที่จุดอ่อนบางอันกลับมีความสำคัญอย่างยิ่งยวด

การพิจารณาผังทางเดินของกิจกรรมและความสัมพันธ์กับข้อผิดพลาดหรือการควบคุมที่เกี่ยวข้อง

ผู้ตรวจสอบควรพยายามมองให้เห็นภาพพจน์ของกิจกรรม ขบวนการ ขั้นตอนต่าง ๆ ในระบบ ในขณะที่จะเริ่มขบวนการรวบรวมเอกสารข้อมูล และอาจใช้เทคนิคการตั้งคำถามเพื่อหาจุดที่สามารถก่อให้เกิดข้อผิดพลาดขึ้นได้ในแต่ละขบวนการและในแต่ละขั้นตอน คำตอบที่ได้จะชี้ถึงลักษณะของสาเหตุและความเฉพาะของความผิดพลาดที่เกิดขึ้น เช่น สาเหตุหนึ่งที่อาจทำให้เกิดจุดอ่อน คือ การบันทึกบัญชีผิดพลาด ซึ่งเป็นความผิดพลาดจากการทำด้วยมือ ลักษณะของความผิดพลาดก็อาจมีผลมาจากความผิดพลาดของพนักงาน เช่น ไม่บันทึกรายการให้ครบถ้วน หรือบันทึกรายการผิดพลาด หรือจำแนกประเภทรายการผิด เป็นต้น

คำถามที่ผู้ตรวจสอบควรถามต่อไปคือ ความผิดพลาดที่เกิดขึ้นนั้นมีสาระสำคัญหรือไม่ มีการควบคุมอะไรบ้าง ณ จุดนั้น ถ้าจะป้องกันมิให้เกิดจุดอ่อนขึ้นจะต้องมีการควบคุมอย่างไร



ประเด็นคำถามที่จะช่วยในการตรวจสอบ

องค์ประกอบในการตรวจสอบ	คำถามโดยทั่วไปของผู้ตรวจสอบ
จุดที่ตรวจสอบ	มีนัยสำคัญต่อการตรวจสอบหรือไม่
↓	
วัตถุประสงค์ในการควบคุมจุดนั้นหรือขบวนการนั้น	ทำไมจุดดังกล่าวจึงมีความสำคัญต่อการตรวจสอบ
↓	
กิจกรรมและการควบคุมต่าง ๆ ที่มี ณ จุดนั้น	กิจกรรมเหล่านั้นมีความสัมพันธ์กันอย่างไร
↓	
ลักษณะข้อผิดพลาดที่อาจเกิดขึ้นได้	ข้อผิดพลาดใดที่อาจเกิดขึ้นและมีนัยสำคัญ และโอกาสที่จะเกิดบ่อยเพียงไร
↓	
สาเหตุของข้อผิดพลาด	ทำไมจึงเกิดข้อผิดพลาด (ตั้งใจหรือไม่ได้ตั้งใจ)
↓	
สามารถควบคุมข้อผิดพลาดดังกล่าวได้อย่างไร	มีการควบคุมในจุดที่เป็นสาเหตุของข้อผิดพลาดที่ปรากฏหรือไม่ ถ้ามีการควบคุมดังกล่าวได้รับการออกแบบอย่างมีประสิทธิภาพและประสิทธิผลหรือไม่
↓	
ผลที่ตามมาถ้าไม่ได้มีการควบคุมข้อผิดพลาดดังกล่าว	ถ้าไม่ได้มีการควบคุมข้อผิดพลาด จุดอ่อนดังกล่าวจะมีผลเช่นไร
↓	
การกำหนดจุดควบคุมลงไป	มีวิธีทดสอบอย่างไรเพื่อตรวจสอบว่าการควบคุมสาเหตุข้อผิดพลาด และจุดอ่อนดังกล่าว ทำงานได้อย่างเหมาะสม

ความรับผิดชอบของผู้สอบบัญชีในด้านการตรวจสอบงานที่ประมวลผลด้วยคอมพิวเตอร์

1. ต้องเข้าใจขั้นตอนการทำรายการ (Flow of Transaction) เบื้องต้นที่ทำผ่านระบบงาน (Application) ที่มีนัยสำคัญต่อการประมวลผลและความถูกต้องของรายงานทางการเงิน
2. ต้องเข้าใจโครงสร้างของการควบคุมขั้นต้น (ทั้งในระบบ Manual และ Computerized)
3. ต้องเข้าใจรายละเอียดของข้อมูลที่บันทึกไว้ในแฟ้มข้อมูล (Content of EDP Files) และความเกี่ยวข้องของข้อมูลนั้น ๆ ที่มีต่อรายละเอียดในงบการเงิน
4. ถ้าหากองค์การผู้รับตรวจใช้เทคนิคการตรวจสอบโดยใช้โปรแกรมการตรวจสอบ จะต้องมีการทบทวน และทดสอบก่อนที่จะให้ความเชื่อถือ
5. การทบทวนระบบการควบคุมภายในของงานที่ประมวลผลด้วยคอมพิวเตอร์ และการใช้เทคนิคทางด้านการตรวจสอบโดยใช้คอมพิวเตอร์ จะต้องปฏิบัติงานโดยผู้สอบบัญชีที่มีความรู้ทางด้านเทคนิคอย่างเพียงพอ

ทำอย่างไรจึงจะสามารถทราบได้ว่า ผู้สอบบัญชีมีความเข้าใจในระบบงานที่ตรวจสอบ

1. ผู้สอบบัญชีสามารถที่จะกำหนดจุดที่จะทำการตรวจสอบในระดับต่าง ๆ ในองค์การนั้นได้อย่างเหมาะสมหรือไม่
2. ผู้สอบบัญชีได้บรรลุวัตถุประสงค์ในการรวบรวมหลักฐาน (Audit Evidence) ได้เพียงพอหรือไม่
3. ผู้สอบบัญชีสามารถที่จะบอกรูปแบบของการควบคุมที่สำคัญในระบบคอมพิวเตอร์ได้ครบถ้วนเพียงพอหรือไม่ และ
4. ผู้สอบบัญชีใช้เกณฑ์อะไรในการตัดสินใจในความเพียงพอของเขา

วิธีการตรวจสอบระบบงาน (Application Audit)

การตรวจสอบระบบงานที่ประมวลผลด้วยคอมพิวเตอร์ ควรจะทำในลักษณะ TOP DOWN ซึ่งจะประกอบด้วยขั้นตอนใหญ่ ๆ 3 ขั้นตอน คือ

ขั้นตอนที่ 1 สอบทานระบบการควบคุมภายใน
ขั้นตอนที่ 2 ทดสอบการควบคุมภายในด้านที่สำคัญ
ขั้นตอนที่ 3 ตรวจสอบความถูกต้องของรายงานทางการเงิน

ขั้นตอนที่ 1 สอบทานระบบการควบคุมภายใน

วัตถุประสงค์ : เพื่อประเมินความเพียงพอของการควบคุมภายใน ทั้งโดยคนและโดยคอมพิวเตอร์

วิธีการที่ใช้ในการวิเคราะห์และประเมินผล

- กำหนดขอบเขตระบบงาน
- พิจารณาว่าอะไรบ้างที่สามารถเกิดข้อผิดพลาดได้
- ชี้จุดที่ต้องการควบคุม

ขั้นตอนที่ 2 ทดสอบการควบคุมภายในที่สำคัญ

ผู้ตรวจสอบต้องแน่ใจว่า องค์การมีการดำเนินการควบคุมในจุดที่สำคัญ โดย

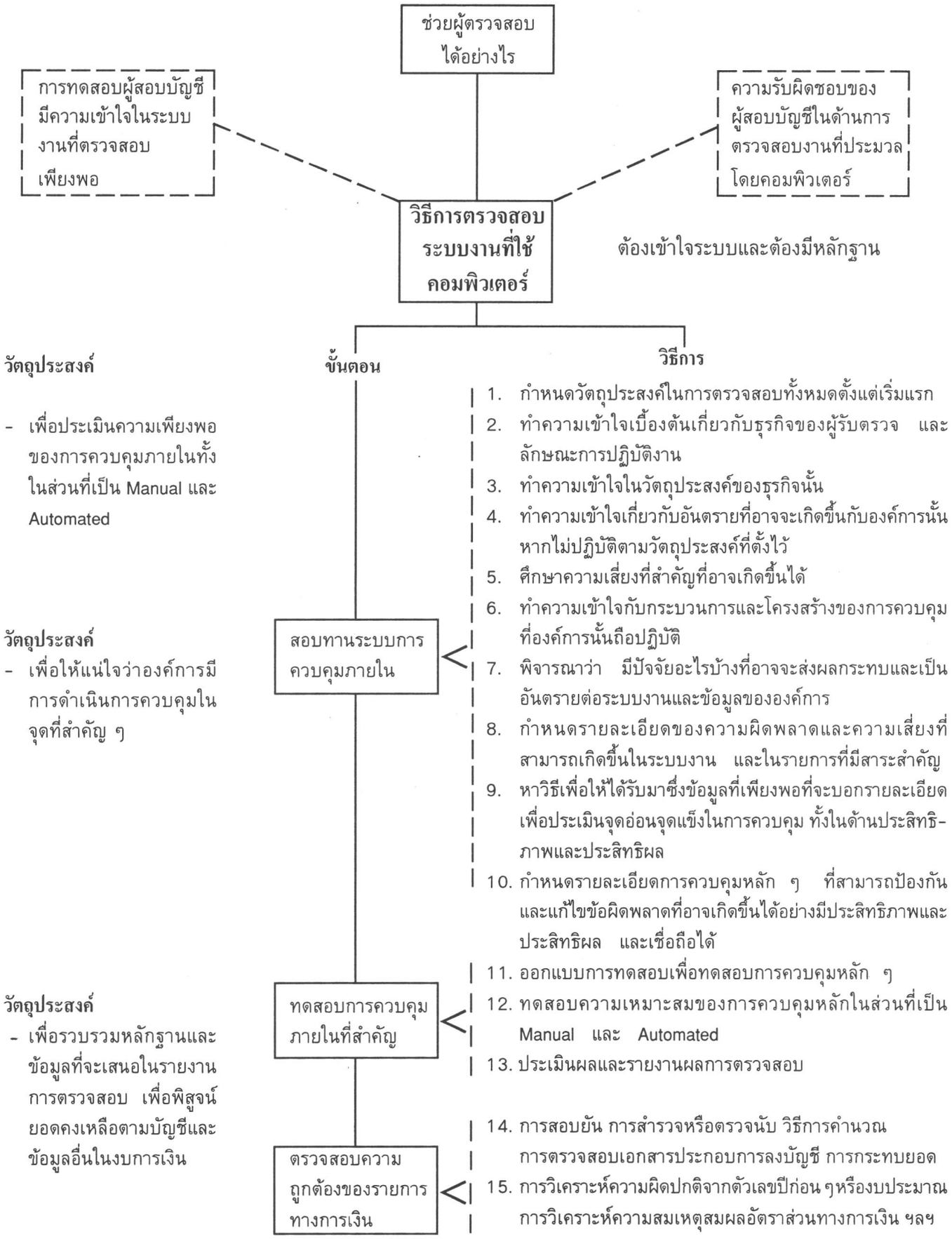
- ทำการทดสอบความเหมาะสมของการควบคุมด้วยเครื่องคอมพิวเตอร์
- ทำการทดสอบ การควบคุมในส่วนที่ทำด้วยคน

ขั้นตอนที่ 3 ตรวจสอบความถูกต้องของรายงานทางการเงิน

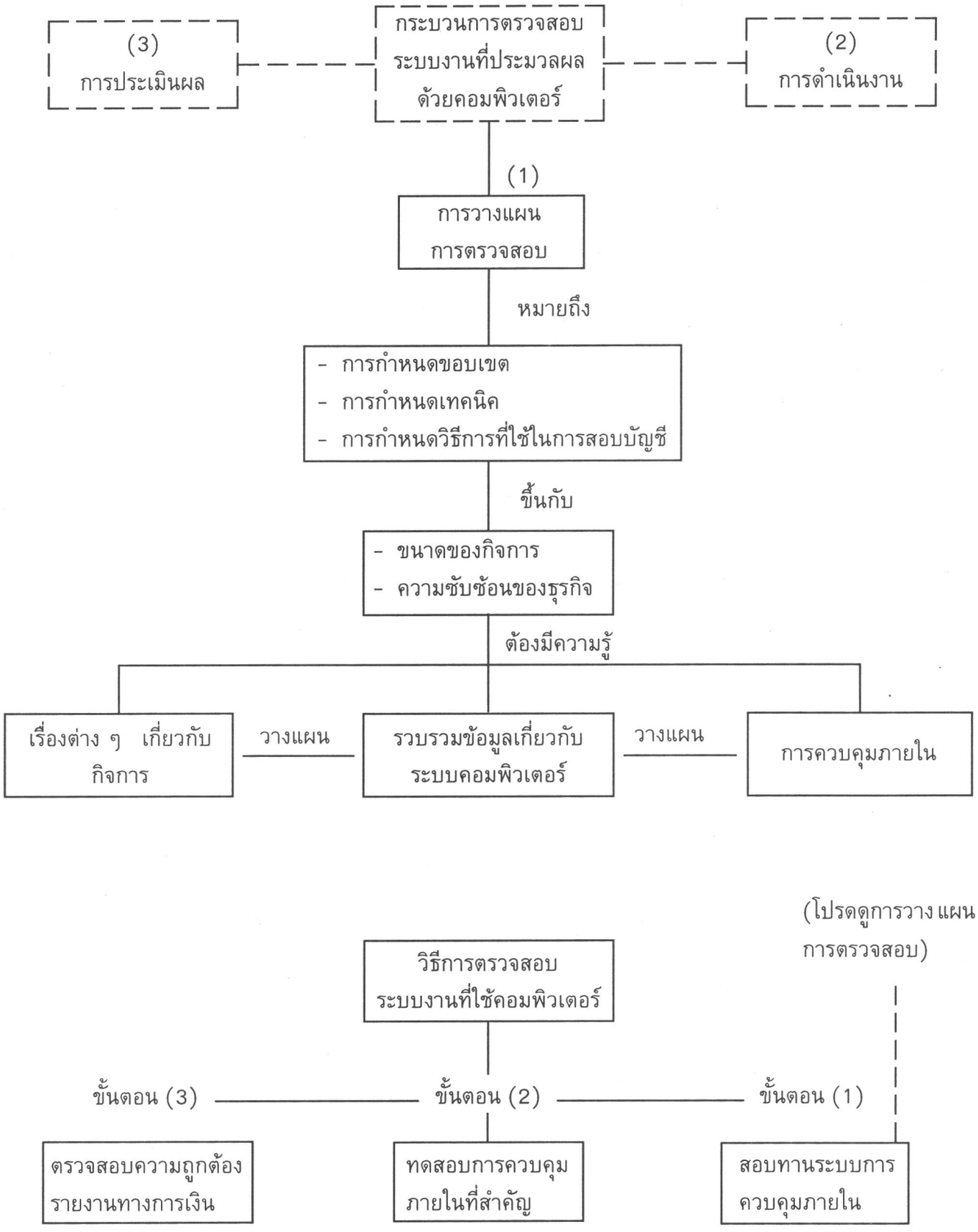
ผู้ตรวจสอบต้องนำผลการทดสอบการควบคุมภายในมาใช้ในการกำหนดขอบเขตและวิธีการปฏิบัติในการตรวจสอบความถูกต้องของรายงานทางการเงินให้เหมาะสม ถ้าหากว่าองค์การมีการควบคุมภายในอย่างเพียงพอและสามารถใช้ได้ผลแล้ว ขอบเขตในการตรวจสอบในขั้นตอนที่ 3 ก็จะน้อยลงในสัดส่วนเดียวกัน

ในการตรวจสอบระบบงานใด ๆ ผู้ตรวจสอบต้องตรวจสอบทั้งในส่วนที่ประมวลผลด้วยคนและด้วยเครื่องคอมพิวเตอร์ ตลอดจนระบบงานอื่น ๆ ที่เกี่ยวข้อง เช่น การตรวจสอบบัญชีเงินฝากกระแสรายวัน ผู้ตรวจสอบต้องพิจารณาทั้งในส่วนคนและเครื่องคอมพิวเตอร์ และระบบการบัญชี การเรียกเก็บเงินตามเช็ค และเงินฝากประเภทอื่นที่เกี่ยวข้องกัน



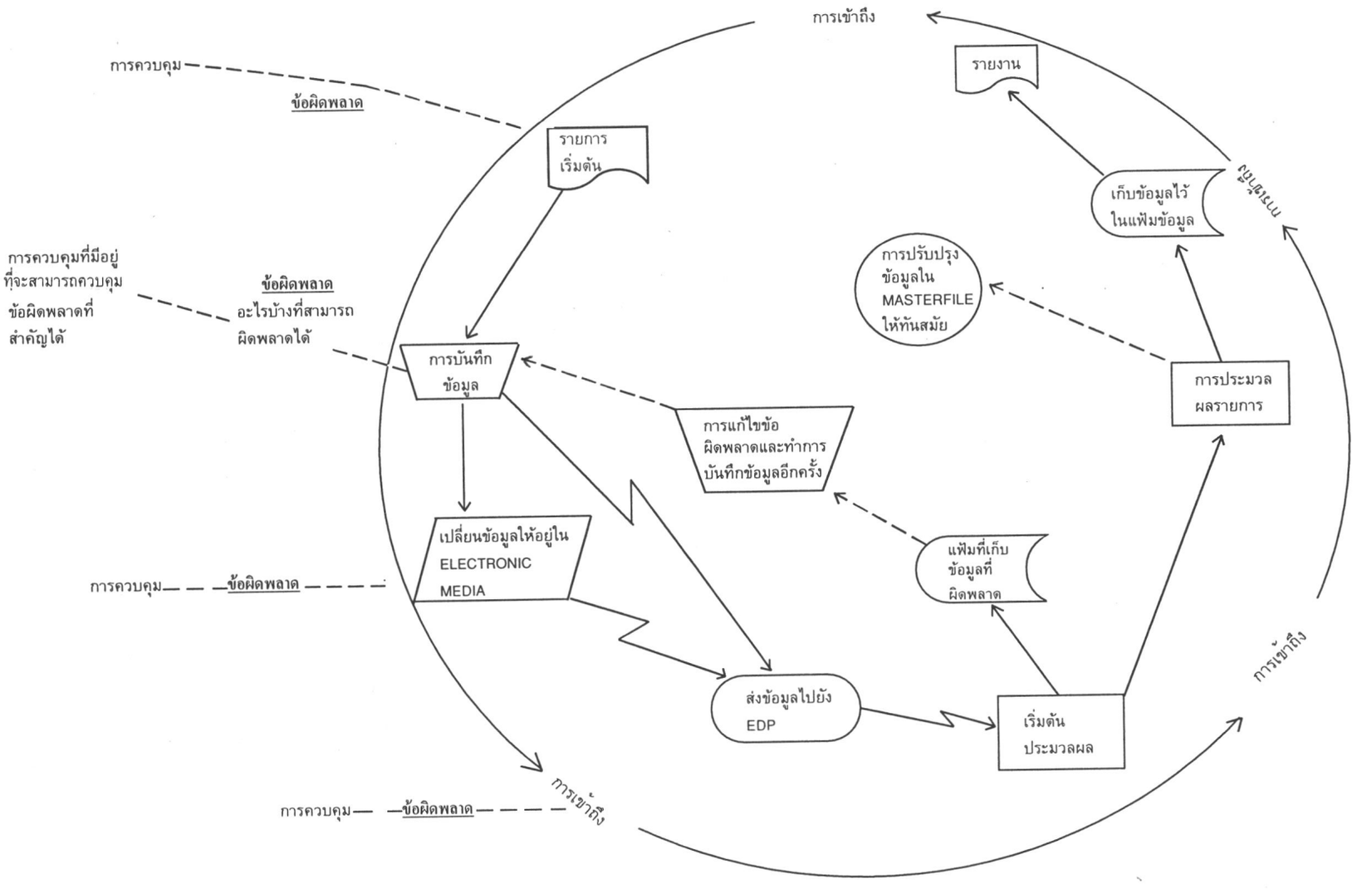


สรุป - วิธีการตรวจสอบระบบงาน (Application Audit) ที่ใช้คอมพิวเตอร์ในรูปแบบที่เข้าใจได้ง่าย ๆ

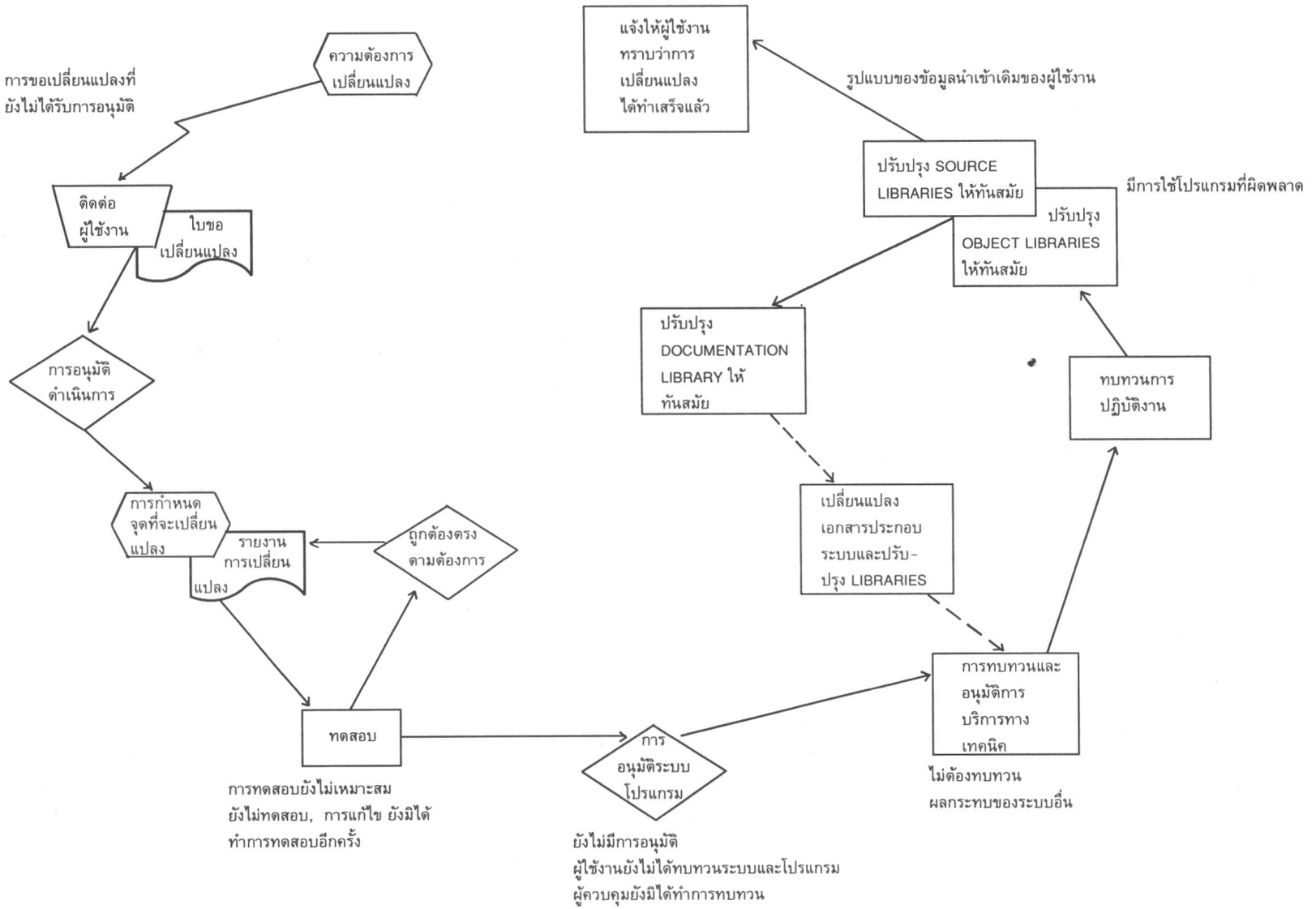


สรุป : อีกรูปแบบหนึ่งของการทำความเข้าใจการตรวจสอบระบบงานที่ใช้คอมพิวเตอร์ (Applications audit)

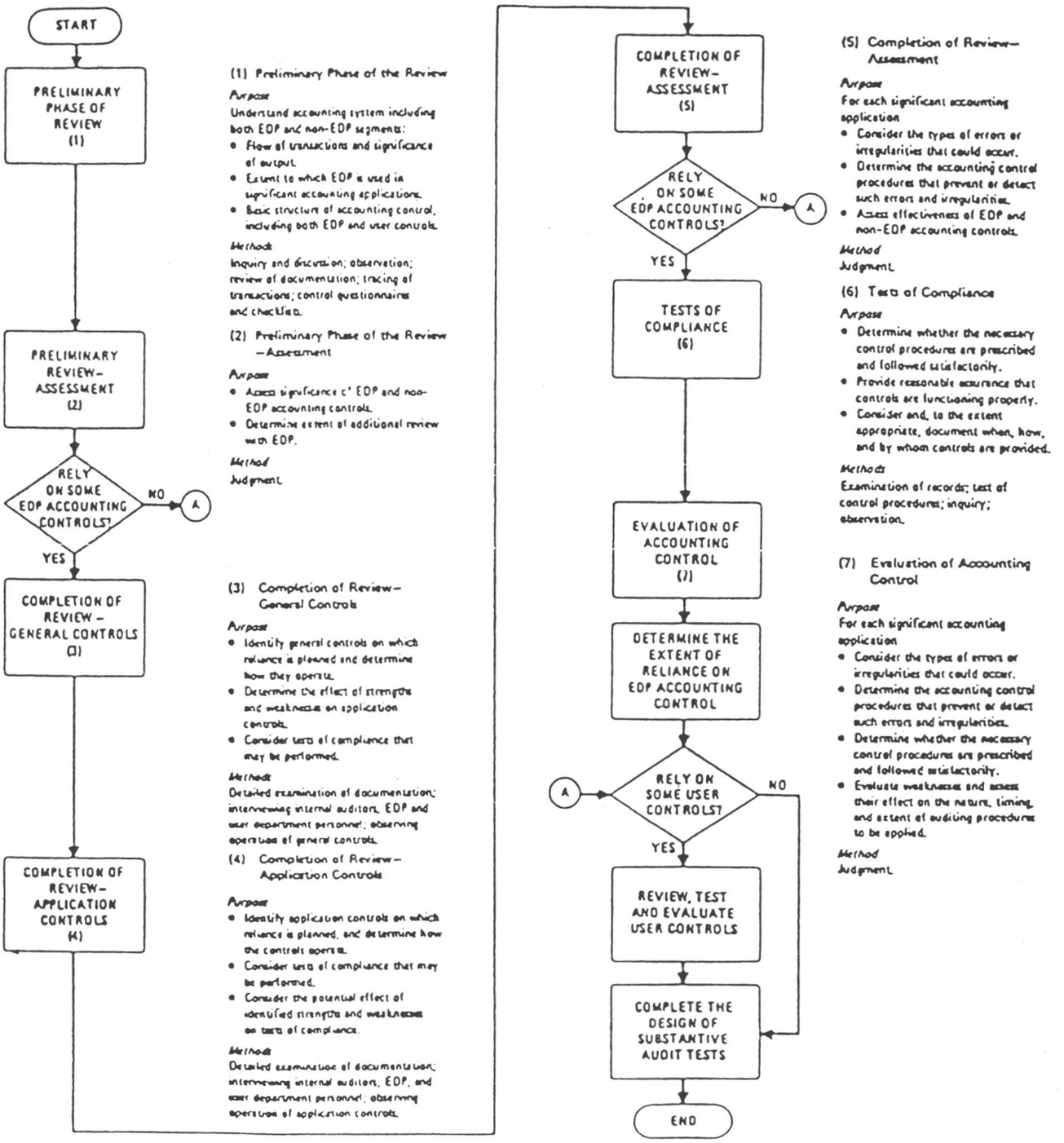
แผนภาพที่ 15.1 แสดงกิจกรรมการประมวลผลรายการแสดงจุดที่จะเกิดข้อผิดพลาดและการควบคุม



แผนภาพที่ 15.2 แสดงกิจกรรมในการปรับปรุงโปรแกรม การควบคุมและตัวอย่างข้อผิดพลาดที่อาจเกิดขึ้น



แผนภาพที่ 15.3 : คัดย่อแสดงแนวการศึกษาและขั้นตอนการตรวจสอบงานที่ใช้คอมพิวเตอร์อีกรูปแบบหนึ่ง ซึ่งเป็นแผนภาพที่สมบูรณ์ แสดงการตรวจสอบในภาพรวมทั้งหมด ขอบเขตการตรวจสอบจึงขึ้นกับเป้าหมายเป็นสำคัญ อย่างไรก็ดีขอให้ท่านผู้อ่านโปรดใช้ความสังเกตแผนภาพนี้ ก็จะพบว่าเป็นการตรวจสอบทั่วไปในองค์กรที่ใช้คอมพิวเตอร์นั่นเอง



NOTE: At any point after the preliminary phase of the review, the auditor may decide not to rely on EDP accounting controls for all or some applications (see *SAS No. 3*, par. 26). The auditor would then complete the design of the substantive audit tests. According to *SAS No. 1*, Section 320.70, substantive tests consist of the following classes of audit procedures: (1) tests of details of transactions and balances and (2) analytical review of significant ratios and trends and resulting investigation of unusual fluctuations and questionable items.

แนวการตรวจสอบระบบงานที่ประมวลผลด้วยคอมพิวเตอร์

1. แนวการตรวจสอบการควบคุมข้อมูลนำเข้า (Input controls)

1.1 ประเมินผลความเพียงพอของการควบคุมข้อมูลนำเข้า

การควบคุมข้อมูลนำเข้าควรมีดังนี้ คือ

ก. ขั้นตอนหรือวิธีการที่ทำให้รู้ได้ทันทีว่าข้อมูลที่นำเข้าคอมพิวเตอร์ มีข้อบกพร่องหรือผิดพลาด และสามารถแก้ไขได้ทันที

ข. การออกยอดรวมหรือวิธีการอย่างอื่นที่ทำให้รู้ว่า ข้อมูลนำเข้าถูกนำไป ประมวลผลเพียงครั้งเดียว

1.2 ดู Data Fields ที่สำคัญๆ และโปรแกรมที่ใช้ทดสอบ Data Fields ต่าง ๆ เหล่านั้น เพื่อทำให้รู้ได้ว่าข้อมูลนั้นสมบูรณ์และถูกต้อง

1.3 สรุปรายละเอียดรหัสหรือขั้นตอนพิเศษต่าง ๆ ที่จะทำให้ข้อมูลที่นำเข้าคอมพิวเตอร์ไม่ต้องผ่านการตรวจทานความถูกต้องของโปรแกรม (Editing) หรือไปแก้ไขให้ข้อมูลผิดพลาดได้

1.4 อธิบายวิธีดำเนินการกับข้อมูลนำเข้าที่ตรวจพบข้อผิดพลาด และถ้าข้อมูลนั้นยังผ่านเข้าไปประมวลผล ก็ให้อธิบายวิธีการค้นหาข้อมูลที่ผิดพลาดนั้นให้ตรงกับรายการแรกเริ่ม

1.5 อธิบายขั้นตอนหรือรายงานของฝ่ายผู้ใช้ที่ใช้ในการตรวจทานข้อผิดพลาดที่พบทั้งหมด

1.6 ให้ข้อสังเกตเกี่ยวกับปริมาณและชนิดของข้อผิดพลาด และอัตราการเปลี่ยนแปลงที่ผิดปกติของความผิดพลาดที่เกิดขึ้น

1.7 อธิบายวิธีการควบคุมรายงาน รายการที่ถูกบันทึก และขั้นตอนการทำงานต่าง ๆ ของผู้ใช้ข้อมูลที่ทำให้รายการต่าง ๆ ที่เกิดขึ้นได้รับการประมวลผลครบถ้วนและไม่ตกหล่น

1.8 อธิบายโปรแกรมควบคุมรายการที่ประมวลผลให้รายการต่าง ๆ ได้รับการประมวลผลครบถ้วนและไม่ตกหล่น

1.9 อธิบายวิธีการควบคุมการจัดทำข้อมูลนำเข้าที่ถูกต้อง แล้วจึงเข้าประมวลผล

1.10 ใช้เทคนิคการตรวจสอบ เช่น

ก. ใช้ข้อมูลทดสอบ (Test Data)

ข. การตรวจสอบโปรแกรมงาน

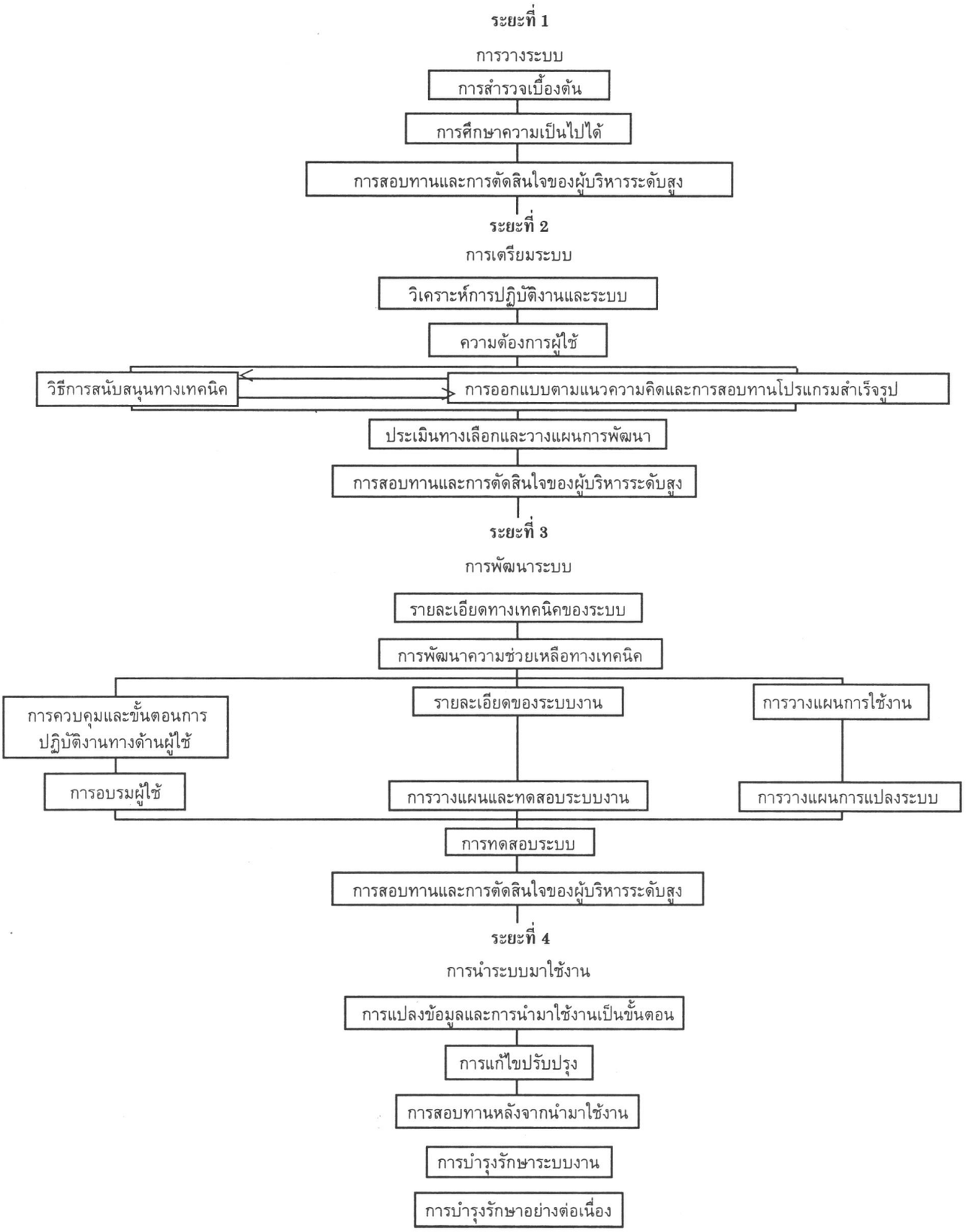
ค. ทบทวน Program Listing สอบทานการควบคุมที่กล่าวในขั้นต้นว่ามีความเพียงพอและได้รับการปฏิบัติจริง

1.11 ทบทวนระบบการควบคุมภายในโดยใช้ Internal control questionnaire (ICQ)

หมายเหตุ : แนวการตรวจสอบการควบคุมข้อมูลนำเข้า (Input Controls) นี้สามารถประยุกต์ใช้กับการตรวจสอบ Processing และ Output Controls ได้ด้วย

แผนภาพที่ 15.4 แสดงการพัฒนาระบบงาน

แผนผังข้างล่างนี้เป็นตัวอย่างของการพัฒนาระบบงาน ซึ่งแบ่งออกได้เป็น 4 ระยะ คือ



หมายเหตุ : เป็นการทำความเข้าใจในการพัฒนาระบบงานที่ใช้คอมพิวเตอร์เพื่อการตรวจสอบ

16

การตรวจสอบระบบข้อมูลที่ใช้คอมพิวเตอร์

การตรวจสอบระบบข้อมูลที่ใช้คอมพิวเตอร์ *

1. คำนำ

คำแนะนำต่อไปนี้ (ตั้งแต่บทที่ 16 ถึงบทที่ 26) เป็นการแนะนำสำหรับการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์ ซึ่งจะกล่าวรวมกันไปถึงการตรวจสอบทั้งทางด้านการเงิน (Financial Audit) และการตรวจสอบด้านคอมพิวเตอร์ (Computer Audit) ดังนั้นขอได้โปรดแยกแยะว่าท่านกำลังปฏิบัติงานตรวจสอบด้านใดเป็นสำคัญ สำหรับผู้ตรวจสอบบัญชีภายนอก (External Auditor) และผู้ตรวจสอบบัญชีภายใน (Internal Auditor) สามารถใช้แนวทางในการตรวจสอบได้ดี สำหรับ EDP examiner จากหน่วยงานของรัฐ เช่น ธนาคารแห่งประเทศไทย ผู้ตรวจสอบต้องดูขอบเขตการตรวจสอบตนเองเป็นสำคัญ

แนวการตรวจสอบนี้เป็นการเสนอหลักการและวิธีปฏิบัติทั่วไป ซึ่งอาจถือเป็นมาตรฐานการปฏิบัติงานตรวจสอบระบบข้อมูลทางการบัญชีที่ใช้คอมพิวเตอร์ในการประมวลผล วิธีการตรวจสอบได้พัฒนาขึ้นเพื่อช่วยให้ผู้ตรวจสอบมีเครื่องมือปฏิบัติงานอย่างมีประสิทธิภาพ และบรรลุวัตถุประสงค์ในการตรวจสอบ ทั้งยังช่วยให้ผู้ตรวจสอบมีความมั่นใจในการเสนอความเห็นในรายงานการตรวจสอบอย่างถูกต้องตามความเป็นจริง และมีเหตุมีผลมากที่สุด ณ วันที่ตรวจสอบ และสำหรับรอบระยะเวลาบัญชีที่ตรวจสอบ

2. ลักษณะสำคัญของการตรวจสอบ

ก่อนที่จะกำหนดโครงสร้างของลำดับขั้นการตรวจสอบ ควรจะทำความเข้าใจกับลักษณะสำคัญของการตรวจสอบ 3 ประการ คือ

2.1 วัตถุประสงค์และขอบเขตการตรวจสอบนั้นแน่นอน

การปฏิบัติงานใดๆของผู้ตรวจสอบ ย่อมกระทำขึ้นด้วยความจำเป็นและมีความสำคัญต่อการรายงานฐานะและผลการดำเนินงานของกิจการ ดังนั้น วิธีการปฏิบัติงานและการค้นหาเอกสารหลักฐานของผู้ตรวจสอบ จึงกำหนดขึ้นเพื่อให้ผู้ตรวจสอบทุ่มเทความพยายามในการปฏิบัติงานลงไปเฉพาะรายการ หรือการดำเนินงานใด ๆ ที่มีผลกระทบต่อข้อเท็จจริงและความสมเหตุสมผลของรายงานแสดงฐานะการเงินและผลการดำเนินงานนั้น ผู้ตรวจสอบจะให้ความสนใจเพียงเล็กน้อยต่อรายการอื่น ๆ ซึ่งไม่เกี่ยวข้องกับวัตถุประสงค์ดังกล่าว หรือรายการที่มีการประมวลผลอย่างมีประสิทธิภาพและรัดกุมเพียงพอแล้ว และรายการที่ไม่มีนัยสำคัญ (immaterial) อันได้แก่ ขนาดของความผิดพลาดที่เกิดขึ้นพอจะยอมรับได้ และไม่มีผลกระทบต่อข้อเท็จจริงและความสมเหตุสมผลของรายงานแสดงฐานะการเงินและผลการดำเนินงาน

2.2 ขั้นตอนการตรวจสอบมีความสัมพันธ์ซึ่งกันและกัน

ขั้นตอนการตรวจสอบแต่ละขั้นตอนจะมีความสัมพันธ์ซึ่งกันและกัน ผลของการปฏิบัติงานในขั้นตอนหนึ่งอาจสำเร็จโดยสมบูรณ์ในการปฏิบัติงานอีกขั้นตอนหนึ่ง หรือการปฏิบัติงานในขั้นตอนหนึ่งจะแสดงให้เห็นสิ่งผิดปกติและข้อบกพร่องหรือจุดอ่อนอย่างสำคัญ ซึ่งกระทบกระเทือนต่อการปฏิบัติงานในขั้นตอนต่อไป

---

*หมายเหตุ : จากหนังสือ An Audit Approach to computer โดย Brian Jenkins & Anthony Pinkney

2.3 วิธีการตรวจสอบขึ้นอยู่กับสภาพการณ์

ผู้ตรวจสอบอาจเลือกที่จะผสมผสานวิธีการตรวจสอบหลายวิธีเข้าด้วยกัน หรือเลือกที่จะใช้วิธีการตรวจสอบอย่างใดอย่างหนึ่งเมื่อผู้ตรวจสอบพิจารณาเห็นว่าจะเกิดประสิทธิภาพมากที่สุดภายใต้สภาพการณ์ที่เกิดขึ้น

3. ขั้นตอนการตรวจสอบ

ขั้นตอนการปฏิบัติงานตรวจสอบที่สำคัญแบ่งออกเป็น 5 ขั้นตอนตามลำดับ ดังนี้

3.1 การศึกษาและบันทึกระบบงาน (Understanding and Recording the System) ขั้นตอนนี้รวมถึงการตรวจสอบขั้นต้น (Preliminary Phase of Review) และการทดสอบการควบคุมทั่วไป (Review of General Controls)

3.2 การประเมินระบบการควบคุมภายใน (Evaluation of Internal Control)

3.3 การตรวจสอบระบบการควบคุม (Functional Tests)

3.4 การประเมินผลกระทบของข้อบกพร่องในการควบคุม (The Examination Response to Control Weaknesses)

3.5 การตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures)

ผลจากการปฏิบัติงานทั้ง 5 ขั้นตอนที่กล่าวข้างต้น จะนำไปสู่การจัดรายงานการตรวจสอบ ซึ่งเป็นการสรุปผลและให้ความเห็นจากการตรวจสอบ (Examination opinion) ต่อไป

ขั้นตอนการปฏิบัติงานโดยลำดับแสดงได้ตามแผนภาพที่ 16.1

3.1 การศึกษาและบันทึกระบบงาน (Understanding and Recording the System)

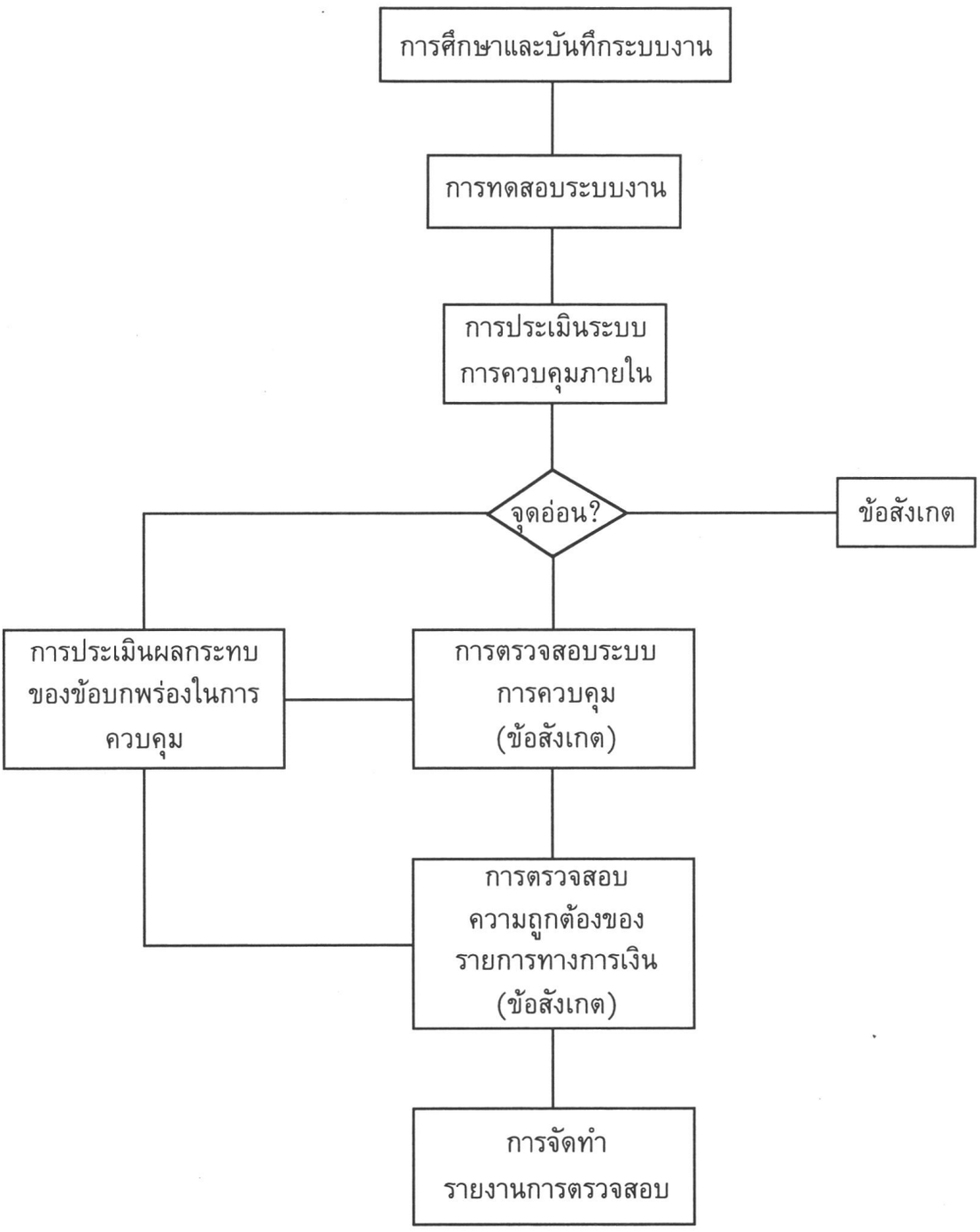
การตรวจสอบทั่วไป

ก่อนตัดสินใจใช้วิธีการตรวจสอบใด ๆ ผู้ตรวจสอบจำเป็นต้องทำการศึกษาและจดบันทึกวิธีการและการควบคุมเกี่ยวกับระบบบัญชีและการดำเนินงาน โดยศึกษาจากคู่มือการปฏิบัติงาน หรือสนทนากับพนักงานชั้นบริหารหรือผู้ปฏิบัติงาน แล้วจดบันทึกในรูปของแผนผัง (Flow-charts) หรือจัดทำคำอธิบายแสดงวิธีการปฏิบัติงานโดยย่อ (Narrative notes)

หลังจากที่ได้จัดทำ (หรือปรับปรุง-ถ้าเป็นการตรวจสอบครั้งต่อไป) แผนผังการปฏิบัติงานหรือคำอธิบายแสดงวิธีการปฏิบัติงานของระบบบัญชี หรือการดำเนินงานนั้น ๆ แล้ว ก่อนที่จะลงมือตรวจสอบผู้ตรวจสอบจะต้องทดลองติดตามรายการ (Trace Transaction) อย่างน้อยหนึ่งรายการที่ผ่านเข้ามาในแต่ละส่วนของระบบบัญชีหรือการดำเนินงานนั้นๆเพื่อความมั่นใจว่าการศึกษาและบันทึกระบบงานของผู้ตรวจสอบมีความถูกต้องแล้ว การปฏิบัติดังกล่าวเรียกว่าการทดสอบระบบงาน (Transaction Review)

การตรวจสอบในระบบคอมพิวเตอร์

การศึกษาและบันทึกระบบงานที่ใช้คอมพิวเตอร์ในการประมวลผล มีลักษณะเฉพาะที่แตกต่างไปจากการตรวจสอบทั่วไป ทั้งนี้เนื่องมาจากผลกระทบของระบบคอมพิวเตอร์ จะได้กล่าวโดยละเอียดในเรื่อง "การศึกษาและบันทึกระบบงาน" ต่อไป



แผนภาพที่ 16.1 ขั้นตอนการปฏิบัติงานตรวจสอบโดยทั่วไป

หมายเหตุ : จากแผนภาพนี้ จะได้อธิบายรายละเอียดในแต่ละขั้นตอน ซึ่งได้แบ่งแยกเป็นบท ๆ ที่เกี่ยวข้อง

3.2 การประเมินระบบการควบคุมภายใน (Evaluation of Internal Control)

การตรวจสอบทั่วไป

ผู้ตรวจสอบจำเป็นอย่างยิ่งที่จะต้องเข้าไปเกี่ยวข้อง และให้ความสำคัญแก่ระบบการควบคุมภายใน เพราะผู้ตรวจสอบจะต้องตัดสินใจด้วยว่าสมควรที่จะให้ความเชื่อถือแก่ระบบการควบคุมภายในนั้นมากน้อยเพียงใด เพื่อประโยชน์ในการกำหนดขอบเขตการตรวจสอบ และช่วงเวลาของข้อมูลหรือรายการที่จะตรวจสอบ นอกจากนั้นผู้ตรวจสอบจะต้องให้ความเห็นและข้อเสนอแนะเพื่อปรับปรุงแก้ไขระบบการควบคุมภายในที่ปรากฏข้อบกพร่อง เพื่อประโยชน์ในการให้ความคุ้มครองการบันทึกบัญชีและการพิทักษ์ทรัพย์สิน

ในการให้ความเชื่อถือต่อระบบการควบคุมภายในก่อนอื่นผู้ตรวจสอบจะต้องทำความเข้าใจกับปัจจัย 2 ประการ ในที่นี้ได้แก่ การควบคุมขั้นพื้นฐาน (Basic Controls) และกฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐาน (Disciplines over Basic Controls) การควบคุมขั้นพื้นฐาน หมายถึง การควบคุมเพื่อความมั่นใจว่าเฉพาะรายการที่ได้รับอนุมัติ (Valid transactions) เท่านั้นที่ได้รับการประมวลผลและจดบันทึกอย่างสมบูรณ์และถูกต้อง ส่วนกฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐาน หมายถึง กฎเกณฑ์หรือระบบการควบคุมเพื่อความมั่นใจว่า การควบคุมขั้นพื้นฐานได้มีการปฏิบัติอย่างต่อเนื่องและเหมาะสม ตลอดจนให้ความคุ้มครองทรัพย์สินที่มีอยู่โดยครบถ้วน กฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐาน ได้แก่ การแบ่งแยกหน้าที่ การตรวจสอบยันผลการปฏิบัติงานระหว่างบุคคล ตลอดจนการควบคุมทางกายภาพ เพื่อป้องกันการเข้าถึงและจัดการเปลี่ยนแปลงทรัพย์สินหรือรายการทางบัญชี โดยมิได้รับอนุญาต

การทำความเข้าใจกับปัจจัยทั้ง 2 ประการที่กล่าวข้างต้น มีความสำคัญสำหรับผู้ตรวจสอบ คือ โดยปกติในการตรวจสอบผู้ตรวจสอบจะต้องมั่นใจว่าได้มีการปฏิบัติตามการควบคุมขั้นพื้นฐานอย่างต่อเนื่องและเหมาะสม นั่นคือ จะต้องมีกฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐานอยู่อย่างแน่นอน ผู้ตรวจสอบจึงจะสามารถให้ความเชื่อถือต่อระบบการควบคุมภายใน แล้วปฏิบัติงานตรวจสอบได้ด้วยความเชื่อถือนั้นได้ แต่ถ้าหากพบว่าไม่มีกฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐานบังคับใช้อยู่ในระบบงานใด ผู้ตรวจสอบอาจจำเป็นต้องขยายขอบเขตและช่วงเวลาที่ตรวจสอบออกไปจากการตรวจสอบปกติ เพื่อให้ได้รับความพอใจในการตรวจสอบมากที่สุด

การตรวจสอบในระบบคอมพิวเตอร์

ลักษณะของการควบคุมขั้นพื้นฐานและกฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐาน วิธีการประเมินระบบการควบคุมภายใน ตลอดจนแบบสอบถามที่ใช้ในการประเมินระบบการควบคุมภายใน สำหรับระบบการประมวลผลด้วยคอมพิวเตอร์จะได้กล่าวโดยละเอียดในเรื่อง “การประเมินระบบการควบคุมภายใน” ต่อไป

กล่าวโดยทั่วไป นอกจากผู้ตรวจสอบจะต้องให้ความสนใจการควบคุมด้วยบุคคล (Manual Controls) หรือในที่นี้หมายถึง การควบคุมทางด้านผู้ใช้ (User Controls) แล้ว ผู้ตรวจสอบจะต้องให้ความสนใจหรือเข้าไปเกี่ยวข้องกับพิธีปฏิบัติและการควบคุมในรูปแบบอื่นๆ ซึ่งเป็นลักษณะเฉพาะของระบบคอมพิวเตอร์ ได้แก่ ขั้นตอนการทำงานของโปรแกรม (Program Procedures) และการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Controls) ขั้นตอนการทำงานของโปรแกรม หมายถึง ลำดับขั้นการทำงานของโปรแกรมคอมพิวเตอร์ ซึ่งจะช่วยควบคุมข้อมูลต่าง ๆ ที่อยู่ระหว่างการประมวลผลไปด้วย ส่วนการควบคุมความ

สมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ หมายถึง การควบคุมพิธีปฏิบัติงานทั้งหมดในศูนย์คอมพิวเตอร์ ได้แก่ การควบคุมอุปกรณ์และเครื่องมือเครื่องใช้ การรักษาความปลอดภัย และการควบคุมการใช้โปรแกรมและแฟ้มข้อมูล

3.3 การตรวจสอบระบบการควบคุม (Functional Tests)

การตรวจสอบทั่วไป

การตรวจสอบระบบการควบคุม หมายถึง การตรวจสอบเพื่อให้ได้หลักฐานว่า ระบบการควบคุมได้มีการปฏิบัติตามอย่างต่อเนื่องและเหมาะสมสำหรับรอบระยะเวลาบัญชีที่ตรวจสอบ Functional Tests มีความหมายเช่นเดียวกับ Compliance Tests และ Procedural Tests

โดยทั่วไปผู้ตรวจสอบจะดำเนินการตรวจสอบระบบการควบคุมในทุกขอบเขตของการควบคุม อย่างไรก็ตามในบางกรณีผู้ตรวจสอบอาจใช้วิธีการขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Tests) แทนที่จะตรวจสอบระบบการควบคุมในบางขอบเขต เมื่อพิจารณาเห็นว่าการปฏิบัติเช่นนั้นจะมีประสิทธิภาพมากกว่า

การตรวจสอบระบบการควบคุมนั้น ควรจะได้ดำเนินการทั้งในส่วนของการควบคุมขั้นพื้นฐาน (Basic Controls) และส่วนของกฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐาน (Disciplines over Basic Controls) แต่โดยปกติผู้ตรวจสอบจะเพ่งเล็งไปที่กฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐาน และถ้าได้ตรวจสอบการปฏิบัติตามกฎเกณฑ์สำหรับการควบคุมขั้นพื้นฐานจนเป็นที่พอใจแล้ว การตรวจสอบการควบคุมขั้นพื้นฐานก็อาจลดปริมาณลงได้

วิธีการตรวจสอบระบบการควบคุมที่สำคัญ ได้แก่ การตรวจสอบหลักฐาน (Examination of Evidence) และการปฏิบัติงานซ้ำรอย (Reperformance) แต่ในกรณีที่ไม่อาจใช้วิธีการทั้งสองแบบได้ ผู้ตรวจ-สอบก็อาจใช้วิธีสังเกตการณ์ (Observation) หรือขอคำยืนยันการปฏิบัติงาน (Inquiry) ก็ได้

การตรวจสอบในระบบคอมพิวเตอร์

การตรวจสอบระบบการควบคุมในระบบคอมพิวเตอร์ มีความยุ่งยากและซับซ้อนมากกว่าการตรวจสอบทั่วไป เพราะบ่อยครั้งที่ไม่ปรากฏร่องรอยหรือหลักฐานให้ตรวจสอบได้ วิธีการตรวจสอบที่ใช้ ได้แก่ การสร้างข้อมูลตัวอย่างทดสอบ (Test Data) การวิเคราะห์คำสั่งงาน (Program Code Analysis) และการใช้โปรแกรม (Software) ตรวจสอบ เป็นต้น

ในบางกรณีผู้ตรวจสอบอาจใช้วิธีการอื่นที่จะให้ประสิทธิภาพมากกว่า แทนการตรวจสอบระบบการควบคุมเสียทั้งหมด แต่ทั้งนี้ขึ้นอยู่กับเทคนิคของคอมพิวเตอร์ด้วย วิธีการแรกได้แก่ การใช้โปรแกรมคอมพิวเตอร์ตรวจสอบความถูกต้องของรายการทางการเงิน (Validation procedures)

3.4 การประเมินผลกระทบของข้อบกพร่องในการควบคุม (The Examination Response to Control Weakness)

การตรวจสอบทั่วไป

ในการที่ผู้ตรวจสอบจะตัดสินใจให้ความเชื่อถือต่อระบบการควบคุมภายในได้หรือไม่ ผู้ตรวจสอบจะต้องจำแนกจุดอ่อนหรือข้อบกพร่องของระบบการควบคุมภายในนั้นแล้วประเมินผลกระทบอันอาจเกิดขึ้นและส่งผลต่อวิธีการตรวจสอบในลำดับต่อไป จุดอ่อนหรือข้อบกพร่องอาจมีสาเหตุมาจากขาดวิธีการควบคุมที่จำเป็นหรือมิได้ปฏิบัติตามระบบการควบคุมที่ดีที่ได้กำหนดไว้

ในการตัดสินใจ ผู้ตรวจสอบจะต้องพิจารณาปัจจัยทุกปัจจัยที่เกี่ยวข้อง โดยประเมินว่าข้อบกพร่องของระบบการควบคุมภายในนั้น จะก่อให้เกิดข้อผิดพลาดอันมีนัยสำคัญ หรือความผิดปกติอย่างยิ่งต่อรายงานแสดงฐานะการเงินหรือไม่ หากพิจารณาเห็นว่าจะไม่เกิดข้อผิดพลาดอันมีนัยสำคัญ ผู้ตรวจสอบก็ไม่จำเป็นต้องเปลี่ยนแปลงวิธีการตรวจสอบ คือ ไม่จำเป็นต้องให้ความสนใจต่อข้อบกพร่องที่เกิดขึ้นนั้น แต่หากพิจารณาเห็นว่าข้อผิดพลาดอันมีนัยสำคัญอาจเกิดขึ้นได้เนื่องจากข้อบกพร่องของระบบการควบคุมภายในนั้น ผู้ตรวจสอบจะต้องใช้วิธีการตรวจสอบที่จำเป็นและสมควร เพื่อให้ทราบผลเป็นที่พอใจว่าข้อผิดพลาดอันมีนัยสำคัญจะเกิดขึ้นหรือไม่ และหากเกิดขึ้นผู้ตรวจสอบจะต้องทราบขอบเขตที่แน่นอนของข้อผิดพลาดต่าง ๆ ที่ตามมา

การตรวจสอบในระบบคอมพิวเตอร์

องค์ประกอบและวิธีการที่จะช่วยให้ผู้ตรวจสอบพิจารณาได้ว่า ข้อผิดพลาดที่มีนัยสำคัญจะเกิดขึ้นหรือไม่ และถ้าหากเกิดขึ้นจะมีผลกระทบต่อวิธีการตรวจสอบอย่างไร จะได้กล่าวต่อไปในเรื่อง “การประเมินผลกระทบของข้อบกพร่องในการควบคุม”

3.5 การตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures)

การตรวจสอบทั่วไป

การตรวจสอบความถูกต้องของรายการทางการเงิน เป็นการปฏิบัติงานขั้นสุดท้ายของผู้ตรวจสอบ เพื่อรวบรวมหลักฐานและข้อมูลที่จะเสนอในรายงานการตรวจสอบต่อไป วัตถุประสงค์ที่สำคัญคือ เพื่อพิสูจน์ความถูกต้องของยอดคงเหลือตามบัญชีและข้อมูลอื่นที่ปรากฏในรายงานแสดงฐานะการเงิน การตรวจสอบความถูกต้องของรายงานทางการเงินยังช่วยให้ขั้นตอนการตรวจสอบระบบการควบคุมสมบูรณ์ขึ้น เพราะเป็นการให้หลักฐานเพิ่มเติมที่แสดงว่าได้มีการปฏิบัติตามระบบการควบคุมภายในอย่างต่อเนื่องและเพียงพอหรือไม่ Validation Procedures มีความหมายเช่นเดียวกับ Verification Procedures และ Substantive Tests

โดยปกติเงื่อนไขที่มีความสำคัญต่อลักษณะ ช่วงเวลา และขอบเขตของการตรวจสอบความถูกต้องของรายการทางการเงิน ได้แก่ ความมากน้อยของรายการ และระดับความเชื่อถือซึ่งผู้ตรวจสอบมีต่อการควบคุมภายใน โดยเฉพาะอย่างยิ่งสำหรับความเชื่อถือต่อการควบคุมภายในนั้น ถ้าหากสามารถให้ความไว้วางใจได้มาก ผู้ตรวจสอบก็อาจลดทอนขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินลงได้บางส่วน แต่ถ้า

ไม่อาจให้ความไว้วางใจได้ ผู้ตรวจสอบก็จำเป็นต้องขยายขอบเขตการตรวจสอบให้เพิ่มมากขึ้น การขยายขอบเขตการตรวจสอบ ได้แก่ การเพิ่มจำนวนรายการข้อมูลที่ตรวจสอบ หรือขยายช่วงเวลาของข้อมูลที่ตรวจสอบ และการขอคำยืนยันยอด เป็นต้น

การตรวจสอบในระบบคอมพิวเตอร์

วัตถุประสงค์ของการตรวจสอบความถูกต้องของรายการทางการเงินในระบบคอมพิวเตอร์ รวมทั้งความสัมพันธ์ระหว่างการตรวจสอบกับระบบการควบคุมภายใน มิได้เปลี่ยนแปลงไปจากการตรวจสอบทั่วไป แต่ด้วยเหตุที่ในบางครั้งการตรวจสอบจำเป็นต้องใช้โปรแกรมคอมพิวเตอร์เพื่อตรวจสอบข้อมูลในแฟ้มข้อมูล และด้วยลักษณะเฉพาะของการควบคุมในระบบคอมพิวเตอร์ วิธีการตรวจสอบความถูกต้องของรายการทางการเงินในระบบคอมพิวเตอร์จึงจำต้องเปลี่ยนแปลงไป

การใช้โปรแกรมคอมพิวเตอร์ช่วยในการตรวจสอบ เป็นการพัฒนาหลักการตรวจสอบขั้นพื้นฐาน และแสดงความก้าวหน้าของเทคนิคการตรวจสอบในระบบคอมพิวเตอร์ คุณลักษณะที่เป็นประโยชน์ 2 ประการของการตรวจสอบโดยใช้โปรแกรมคอมพิวเตอร์ มีดังนี้

1) เป็นการตรวจสอบข้อมูลหรือรายการที่เกี่ยวข้องทั้งหมด ซึ่งหากเป็นการตรวจสอบแบบปกติ (Manual Tests) แล้วจะกระทำได้เพียงสุ่มตัวอย่างข้อมูลมาตรวจสอบเท่านั้น

2) ช่วยให้ได้ข้อมูลและหลักฐานเพิ่มขึ้น อันจะเป็นประโยชน์และช่วยเหลือการตรวจสอบด้านอื่น ๆ ด้วย

คุณลักษณะที่เป็นประโยชน์ทั้ง 2 ประการนี้ ทำให้ประสิทธิภาพของการตรวจสอบความถูกต้องของรายการทางการเงินในระบบคอมพิวเตอร์สูงกว่าการตรวจสอบในระบบปกติ อย่างไรก็ตามการตัดสินใจใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบหรือไม่นั้น จำเป็นต้องคำนึงถึงต้นทุนของการตรวจสอบด้วย

4. สรุป

กล่าวโดยทั่วไป การตรวจสอบในระบบคอมพิวเตอร์มีลำดับขั้นตอนการตรวจสอบเช่นเดียวกับการตรวจสอบในระบบปกติที่มิได้ใช้คอมพิวเตอร์ กล่าวคือ ผู้ตรวจสอบจะต้องทำความเข้าใจและจดบันทึกระบบบัญชีหรือระบบการปฏิบัติงาน ประเมินผลการควบคุมภายในและตรวจสอบระบบการควบคุม (Functional Tests) เพื่อความพอใจว่าได้มีการปฏิบัติตามระบบการควบคุมที่กำหนดไว้ ในการปฏิบัติตามที่กล่าวมาข้างต้น ผู้ตรวจสอบจะต้องเข้าไปเกี่ยวข้อง ทดสอบ และประเมินการควบคุมในรูปแบบใหม่ที่ผิดไปจากความคุ้นเคย ซึ่งผู้ตรวจสอบจำเป็นต้องนำเทคนิคใหม่ ๆ เข้ามาใช้ด้วย

ความเชื่อถือที่ผู้ตรวจสอบมีต่อระบบการควบคุมภายในในระบบคอมพิวเตอร์นั้น มีขอบเขตจำกัดกว่าการตรวจสอบระบบปกติ จึงมีผลกระทบต่อขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) ซึ่งจำเป็นต้องขยายออกไป การใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบความถูกต้องของรายการทางการเงิน เป็นความก้าวหน้าของเทคนิคการตรวจสอบ และช่วยให้มีประสิทธิภาพในการตรวจสอบสูงกว่าการตัดสินใจให้ความเชื่อถือต่อระบบการควบคุมภายใน

17

การศึกษาและบันทึกระบบงาน

การศึกษาและบันทึกระบบงาน

1. คำนำ

ก่อนที่จะทำการตรวจสอบ ผู้ตรวจสอบจำเป็นที่จะต้องทำความเข้าใจวิธีการปฏิบัติงานและการควบคุมในระบบงานที่จะตรวจสอบ โดยปกติผู้ตรวจสอบจะทำความเข้าใจในเรื่องดังกล่าวได้ โดยศึกษาจากรายละเอียดประกอบระบบงาน (System Descriptions) ซึ่งธนาคารพาณิชย์จัดทำไว้ ประกอบกับการสนทนา ซักถามผู้บริหารและผู้ปฏิบัติงานของธนาคารพาณิชย์ แล้วสรุปความเข้าใจโดยจดบันทึกในรูปของแผนผังระบบงาน (Flowcharts) และจัดทำคำอธิบายประกอบ (Narrative Notes) ในกรณีที่จำเป็นและเหมาะสม

2. การศึกษาระบบคอมพิวเตอร์ (Understanding Computer System)

2.1 ความรู้ขั้นพื้นฐาน

ผู้ตรวจสอบจำเป็นต้องมีความรู้ขั้นพื้นฐานเกี่ยวกับคอมพิวเตอร์ ได้แก่ หลักการของคอมพิวเตอร์ (Principles of Computer) และการประมวลผลด้วยคอมพิวเตอร์ (Computer Processing) ความรู้ขั้นพื้นฐานที่กล่าวนี้ประกอบด้วยความรู้เกี่ยวกับองค์ประกอบเบื้องต้นของคอมพิวเตอร์ หรือที่เรียกว่า Computer Configuration ความสัมพันธ์ระหว่างองค์ประกอบต่าง ๆ ของอุปกรณ์คอมพิวเตอร์ ความเข้าใจเกี่ยวกับหลักการจัดทำคำสั่งงานหรือโปรแกรม และความรู้เกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์ (Operating System)

นอกเหนือจากความรู้ขั้นพื้นฐาน ผู้ตรวจสอบจำเป็นต้องมีความรู้ที่ลึกซึ้งมากไปกว่านี้ ขึ้นอยู่กับความซับซ้อนและลักษณะเฉพาะของระบบการประมวลผลด้วยคอมพิวเตอร์แต่ละระบบ ซึ่งจะมีความแตกต่างกันไป รวมทั้งความแตกต่างอันเนื่องมาจากวิธีการควบคุมที่ใช้

2.2 โครงสร้างและลักษณะของการประมวลผล

ในการศึกษาระบบคอมพิวเตอร์ ผู้ตรวจสอบจะต้องทำความเข้าใจเกี่ยวกับโครงสร้างและลักษณะของการประมวลผลเสียก่อนเป็นเบื้องแรก

โครงสร้างของการประมวลผลโดยทั่วไป แบ่งออกได้ดังนี้

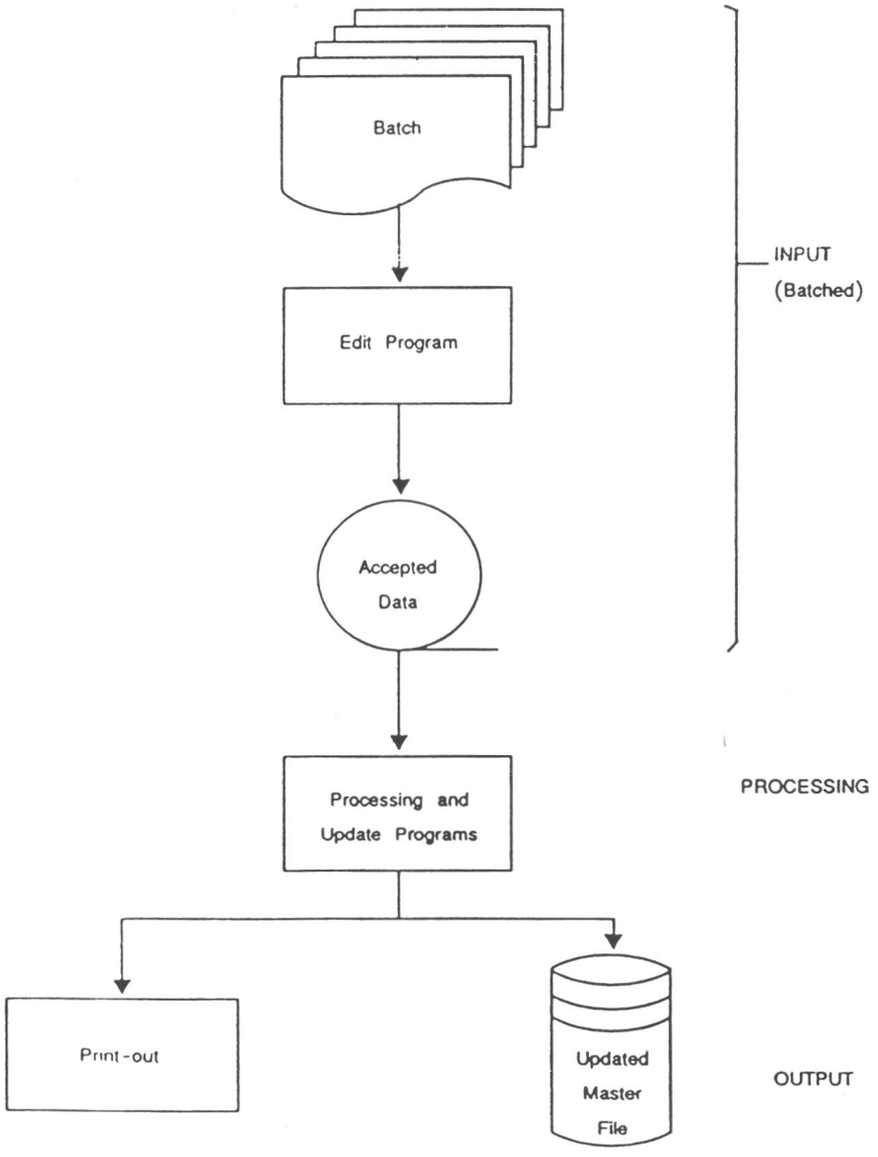
- การนำข้อมูลเข้า (Input) หมายถึง กระบวนการตั้งแต่การเกิดขึ้นของข้อมูล กิจกรรมที่ต่อเนื่องถัดมาจนกระทั่งข้อมูลได้รับการบันทึกไว้ในแฟ้มแม่เหล็ก (Magnetic File) ของคอมพิวเตอร์
- การประมวลผล (Processing) หมายถึง กระบวนการทำงานภายในเครื่องคอมพิวเตอร์
- การแสดงผลลัพธ์ (Output) หมายถึง กระบวนการแสดงผลของข้อมูลที่ประมวลผลเรียบร้อยแล้ว ปกติจะแสดงผลลัพธ์ในรูปของแฟ้มข้อมูล (File) หรือเอกสารตัวพิมพ์ (Print-out) สำหรับลักษณะของการประมวลผลที่สำคัญ ได้แก่ การประมวลผลในลักษณะของ Batch

System (ระบบ Batch System จะใช้ในการอธิบายโครงสร้างของการประมวลผลในลำดับต่อไป)

นอกจากนั้นแล้วลักษณะของการประมวลผลที่ควรกล่าวถึงมีดังนี้

- การนำข้อมูลเข้าและการแสดงผลลัพธ์ระบบ On-line
- การประมวลผลระบบ Real-time
- ระบบฐานข้อมูล (Database)
- ระบบการประมวลผลแบบกระจาย (Distributed Processing)

แผนผังของ Batch System แสดงได้ตามแผนภาพที่ 17.1



แผนภาพที่ 17.1 Batch System

2.2.1 โครงสร้างของการประมวลผล

1) การนำข้อมูลเข้า (Input)

กระบวนการเกี่ยวกับการนำข้อมูลเข้า แบ่งออกเป็น 3 ขั้นตอน ได้แก่ การจดบันทึกข้อมูล (Recording) การแปลงข้อมูล (Converting) ไปสู่ input media และการบันทึกข้อมูล (Writting) ลงบนแฟ้มแม่เหล็ก (Magnetic File) ส่วนมากแล้วขั้นตอนการจดบันทึกข้อมูล (Recording) จะมีลักษณะเช่นเดียวกับระบบที่มิได้ใช้คอมพิวเตอร์ แต่ในบางกรณีขั้นตอนดังกล่าวอาจกระทำโดยคอมพิวเตอร์ตามโปรแกรมที่กำหนดไว้ เช่น ในกรณีที่สะสมข้อมูลจากระบบการประมวลผลงานอื่นๆ เมื่อถึงจุด ๆ หนึ่ง หรือ ณ ปริมาณหนึ่งที่กำหนดไว้ คอมพิวเตอร์ก็จะส่งข้อมูล ณ จุดนั้น หรือ ณ ปริมาณนั้น ไปสู่ระบบอื่นเพื่อประมวลผลต่อไปก็ได้

กระบวนการแปลงข้อมูล (Converting) ไปสู่ input media กระทำได้หลายวิธี ได้แก่ การใช้บัตรเจาะรู (Punched Cards) แถบกระดาษ (Paper Tape) ในสมัยเดิม ตลอดจนวิธีอื่น ๆ ที่แปลงข้อมูลเข้าไปบรรจุลงบนจานหรือเทปแม่เหล็กโดยตรง วิธีการเช่นนี้มักจะปฏิบัติโดยเจ้าหน้าที่ปฏิบัติการ (Operators) โดยส่งข้อมูลผ่านเครื่องส่งข้อมูล (Terminals) ซึ่งเชื่อมตรงต่อเครื่องคอมพิวเตอร์เล็ก ซึ่งจะมีโปรแกรมคอยตรวจสอบความถูกต้องและครบถ้วนของข้อมูล ก่อนที่จะส่งต่อไปยังเครื่องคอมพิวเตอร์ใหญ่ (Main Computer) ต่อไป

วิธีการแปลงข้อมูลที่กล่าวข้างต้น เป็นวิธีการเปลี่ยนข้อมูลดิบให้อยู่ในรูปที่คอมพิวเตอร์สามารถอ่านได้ก่อนที่จะส่งเข้าไปในคอมพิวเตอร์ อีกวิธีหนึ่งได้แก่ การจัดทำข้อมูลดิบให้อยู่ในรูปที่คอมพิวเตอร์สามารถอ่านได้ทันทีโดยไม่ต้องผ่านกระบวนการแปล ได้แก่ การเคลือบตัวอักษรหรือตัวเลขด้วยหมึกแม่เหล็ก (Magnetic Ink Character Recognition หรือ NICR) และการอ่านด้วยแสง (Optical Character Recognition หรือ OCR) เป็นต้น

ข้อมูลอาจถูกอ่านด้วยคอมพิวเตอร์ใหญ่โดยตรง หรือถูกส่งผ่านด้วยข่ายงานสื่อสารพิเศษ เช่น สายโทรศัพท์ หรือข่ายงานโทรคมนาคมทั่วไป ให้เข้าไปสู่คอมพิวเตอร์ศูนย์กลางก็ได้ การส่งข้อมูลลักษณะพิเศษนี้กระทำได้ทั้งในระบบ Off-line และ On-line

2) การประมวลผล (Processing)

การประมวลผล ในที่นี้มีความหมายเฉพาะการทำงานภายในเครื่องคอมพิวเตอร์ ซึ่งแบ่งออกเป็น 4 ประเภท ดังนี้

ก. การสอบทานข้อมูล (Editing) หมายถึง การใช้โปรแกรมตรวจสอบข้อมูลในขณะที่ข้อมูลถูกส่งเข้ามาบันทึกในแฟ้มแม่เหล็ก ปกติจะได้แก่ การตรวจสอบความถูกต้อง (Validity Checks) และความสมเหตุสมผล (Reasonableness Checks) ของข้อมูล รวมทั้งการเปรียบเทียบ (Matching) ข้อมูลนำเข้ากับข้อมูลที่มีอยู่แล้วในแฟ้มคอมพิวเตอร์

ข. การคำนวณ (Calculating) การรวมค่า (Summarizing) และการจัดหมวดหมู่ (Categorizing) การคำนวณ หมายถึง การเทียบค่า (Matching) ข้อมูล 2 ชุด แล้วสร้างค่าที่สามขึ้นมา โดยปกติแล้วจะเป็นการเทียบค่าระหว่างข้อมูลถาวร (Standing Data) ที่บรรจุไว้ในแฟ้มข้อมูลหลัก (Master File)

อย่างถาวร เช่น ราคา คูณกับ ข้อมูลเคลื่อนไหวที่จะถูกส่งเข้ามา (Transaction Data) เช่น จำนวนซึ่งเป็นข้อมูล input และทำการประมวลผลเพียงครั้งเดียวเท่านั้น สำหรับการรวมค่า หมายถึง การสะสมรายการทุกรายการที่เกิดขึ้น ปกติจะเป็นการสะสมรายการที่ได้จากการคำนวณ แล้วสร้างยอดรวมขึ้นมา ส่วนการจัดหมวดหมู่ หมายถึง การวิเคราะห์ยอดรวมที่ได้จากการรวมค่า เช่น การจำแนกอายุหนี้ตามระยะเวลาครบกำหนดชำระ เป็นต้น โดยปกติการจัดหมวดหมู่มักจะอ้างอิงรหัสที่กำกับเข้ามาพร้อมกับข้อมูลนำเข้าแต่ละรายการ

ค. การสร้างข้อมูลโดยอัตโนมัติ (Initiating Transactions) เครื่องคอมพิวเตอร์สามารถสร้างข้อมูลโดยอัตโนมัติตามโปรแกรมที่กำหนดไว้ได้ 2 วิธี คือ วิธีแรกโดยการกำหนดเงื่อนไขไว้ในการประมวลผล เมื่อได้ทำการประมวลผลรายการต่าง ๆ ไปแล้วจนกระทั่งถึงจุดที่ตรงกับเงื่อนไขที่กำหนดไว้ คอมพิวเตอร์ก็จะผลิตข้อมูลชุดใหม่ขึ้นมา อีกวิธีหนึ่งคือ โดยการส่งสัญญาณอย่างใดอย่างหนึ่งเข้าไปให้คอมพิวเตอร์สร้างข้อมูลโดยอัตโนมัติ

ง. การปรับปรุงแฟ้มข้อมูล (Updating Master or Pipeline Files) แฟ้มข้อมูลหลัก (Master Files) มีความคล้ายคลึงกับบัญชี (Ledgers) ในระบบที่มิได้ใช้คอมพิวเตอร์ และหมายถึงแฟ้มที่จัดเก็บข้อมูลทางการเงิน หรือข้อมูลอ้างอิงที่มีความสำคัญต่อการประมวลผลมากกว่าหนึ่งครั้งขึ้นไป สำหรับแฟ้มข้อมูลชั่วคราว (Pipeline Files) เป็นแฟ้มชั่วคราว (Temporary Files) มีความคล้ายคลึงกับบัญชีพัก (Suspense Accounts) ในระบบที่มิได้ใช้คอมพิวเตอร์ และโดยปกติจะเป็นแฟ้มสำหรับจัดเก็บข้อมูลเคลื่อนไหว (Transaction Data) การปรับปรุงแฟ้มข้อมูล (Updating) จึงหมายถึงการบันทึกข้อมูลลงบนแฟ้มข้อมูล หรือถ่ายข้อมูลจากแฟ้มข้อมูลนั้น วิธีการปรับปรุงแฟ้มข้อมูลจะขึ้นอยู่กับการจัดโครงสร้างแฟ้มข้อมูล ตัวอย่างเช่น แฟ้มข้อมูลที่เป็นม้วนเทปจะทำการปรับปรุงโดยการอ่านแฟ้มข้อมูลหลักเดิม (Old Master File) กับแฟ้มข้อมูลปัจจุบัน (Current Transaction File) โดยการอ่านแบบเรียงลำดับ (Sequential) แล้วสร้างแฟ้มข้อมูลหลักแฟ้มใหม่ (New Master File) ส่วนแฟ้มข้อมูลที่เป็นจานแม่เหล็กจะทำการปรับปรุงได้ด้วยวิธีเดียวกัน แต่มีข้อได้เปรียบกว่า เพราะการปรับปรุงแฟ้มข้อมูลชนิดจานแม่เหล็กจะสามารถเข้าไปถึง และเปลี่ยนแปลงข้อมูลเฉพาะตำแหน่งที่ต้องการปรับปรุงได้โดยตรงโดยไม่ต้องอ่านและบันทึกใหม่ตลอดแฟ้มข้อมูล

3) การแสดงผลลัพธ์ (Output)

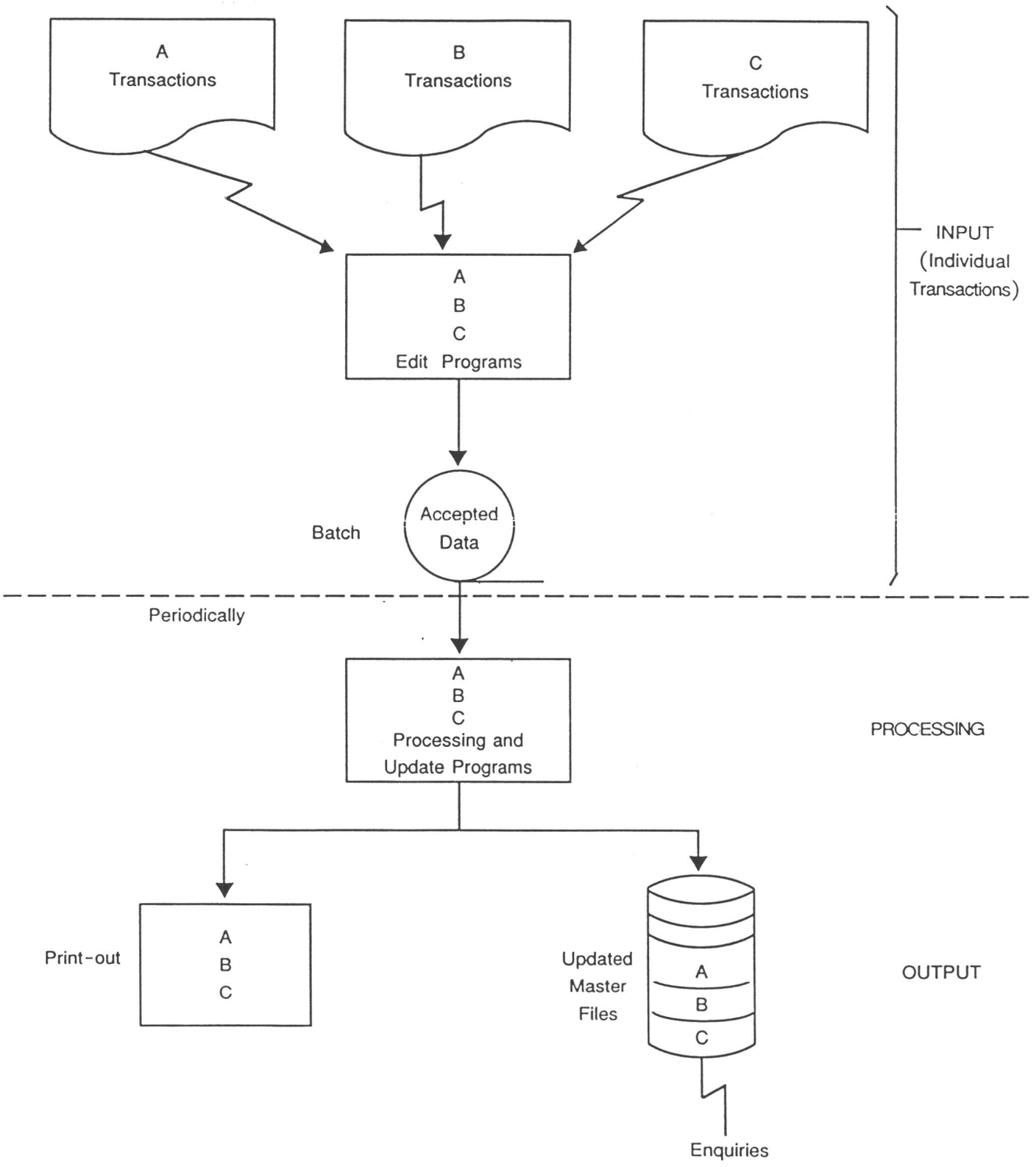
ผลลัพธ์จากการประมวลผล ในที่นี้มีความหมายรวมถึงแฟ้มข้อมูลหลักที่ปรับปรุงแล้ว (Updated Master Files) ตลอดจนผลลัพธ์ในรูปแบบอื่น ๆ เช่น รายงานต่าง ๆ เอกสารแบบพิมพ์ทางการบัญชี หรือบางครั้งอยู่ในรูปของบัตรเจาะรู แถบกระดาษ หรือไมโครฟิล์ม เป็นต้น

2.2.2 ลักษณะของการประมวลผล

1) การนำข้อมูลเข้าและการแสดงผลลัพธ์ระบบ On-line (Online Input and Output)

ระบบ On-line จำเป็นจะต้องมีเครื่องส่งข้อมูลนำเข้า (Input Devices) ซึ่งอาจมากกว่าหนึ่งเครื่องก็ได้ โดยเครื่องมือดังกล่าวสามารถส่งข้อมูลนำเข้าให้เข้าไปสู่คอมพิวเตอร์ได้ทันทีและต่อเนื่องและสามารถที่จะสอบถามและแสดงข้อมูลที่บันทึกไว้ในแฟ้มข้อมูลหลักได้โดยทันทีและต่อเนื่องเช่นเดียวกัน

แผนผังของระบบ On-line แสดงได้ตามแผนภาพที่ 17.2



แผนภาพที่ 17.2 On - line System

การใช้ระบบ On-line มีผลกระทบต่อการนำข้อมูลเข้าและการแสดงผลลัพธ์เท่านั้น ส่วนการประมวลผลยังคงมีลักษณะเช่นเดียวกับการใช้ Batch System ความแตกต่างที่สำคัญสำหรับ การแสดงผลลัพธ์คือ สามารถแสดงข้อมูลในแฟ้มข้อมูลถาวรให้ปรากฏแก่ผู้ใช้ได้ทันทีที่ต้องการ

ฉะนั้น การเปลี่ยนแปลงที่สำคัญจะอยู่ที่การนำข้อมูลเข้า ซึ่งมีด้วยกัน 2 ประการ คือ

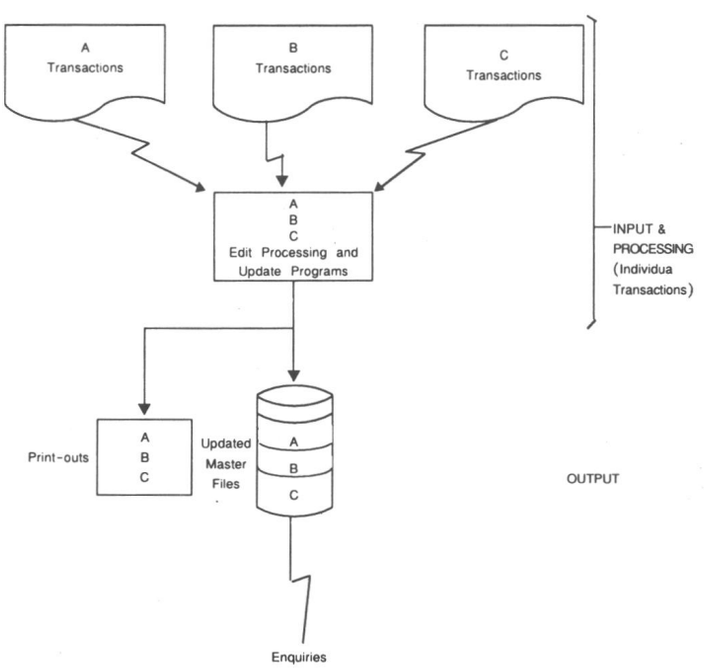
ก. จะมีการนำข้อมูลเข้าทีละรายการ ไม่จำเป็นต้องเป็นชุดหรือกลุ่มข้อมูลเดียวกัน และข้อมูลต่างจำพวกกันก็สามารถนำเข้าติดต่อกันไปได้ ส่วนการบันทึกข้อมูลลงบนแฟ้มแม่เหล็กในคอมพิวเตอร์จะเป็นแบบ Batch System

ข. จำเป็นต้องใช้ Software ที่สลับซับซ้อนในการจัดการข้อมูลนำเข้ามาและการป้อนคำถามต่าง ๆ เนื่องจากมีการนำเข้าข้อมูลทั้งแบบต่อเนื่อง และแบบสุ่มโดยผ่านเครื่องส่งข้อมูลหลายเครื่อง

2) การประมวลผลข้อมูลระบบ Real-time

ระบบ Real-time หมายถึงการประมวลผลและแสดงผลข้อมูลทันทีที่มีการนำข้อมูลเข้า ผลกระทบที่สำคัญของการใช้ระบบ Real-time อยู่ที่ขั้นตอนการประมวลผล ข้อแตกต่างที่สำคัญระหว่างระบบ Real-time กับระบบอื่น ๆ ได้แก่ การที่ระบบ Real-time สามารถทำการประมวลผลทีละรายการได้ทุกขั้นตอนตั้งแต่ต้นจนจบ ในระบบอื่น ๆ โปรแกรมที่ใช้ในการประมวลผลจะถูกป้อนเข้าคอมพิวเตอร์เป็นลำดับแรก หลังจากนั้นชุดข้อมูลที่สมบูรณ์ (Complete Batch) จะถูกส่งเข้าไปแล้วทำการประมวลผล แต่ในระบบ Real-time โปรแกรมต่าง ๆ จะเก็บไว้ในคอมพิวเตอร์ในสภาพพร้อมที่จะประมวลผลได้ทุกขณะ เมื่อมีข้อมูลเข้ามาก็จะทำการประมวลผลได้ทันที

แผนผังของระบบ Real-time แสดงได้ตามแผนภาพที่ 17.3



แผนภาพที่ 17.3 Real - time

3) ระบบฐานข้อมูล (Database)

ระบบฐานข้อมูลเป็นวิธีการจัดเก็บข้อมูลต่าง ๆให้อยู่ในรูปแบบที่เหมาะสมสำหรับการใช้งานร่วมกันได้หลายงาน ข้อมูลซึ่งปกติจะถูกจัดเก็บให้เหมาะกับการใช้งานแต่ละระบบ โดยเฉพาะในแฟ้มข้อมูลที่มีความแตกต่างกันทางตรรกวิทยา จะถูกรวบรวมจัดเก็บเสียใหม่ให้อยู่ในระบบฐานข้อมูลเดียวกัน กล่าวอีกนัยหนึ่งก็คือ ระบบฐานข้อมูล หมายถึง การบันทึกแสดงความสัมพันธ์เชิงตรรกวิทยาระหว่างข้อมูลที่เป็นอิสระจากกัน คุณสมบัติที่สำคัญของระบบฐานข้อมูลคือ ลดความซ้ำซ้อนของการบันทึกข้อมูลเดียวกันที่ใช้งานหลายงานให้สามารถใช้ประโยชน์ร่วมกันได้ การแสดงความสัมพันธ์ระหว่างข้อมูลที่ใช้ร่วมกันอาจทำได้โดยใช้ดัชนี (Indexes หรือ Pointers) ระบบฐานข้อมูลนี้อาจนำมาใช้ได้ทั้งในการประมวลผลระบบ Real-time หรือ On-line หรือ Batch System

ผลกระทบที่สำคัญของการใช้ระบบฐานข้อมูลอยู่ที่ขั้นตอนการอ่านข้อมูลจากฐานข้อมูลเพื่อทำการประมวลผลหรือเพื่อแสดงผลลัพธ์ และขั้นตอนการปรับปรุง (Update) ข้อมูลในฐานข้อมูล กระบวนการในการอ่านและปรับปรุงข้อมูลในระบบฐานข้อมูลแตกต่างไปจากระบบที่มิได้ใช้ฐานข้อมูล เนื่องมาจากความแตกต่างของวิธีการจัดโครงสร้างข้อมูลในระบบฐานข้อมูล และความแตกต่างอันเนื่องมาจากวิธีการของแต่ละระบบงานในการดึงข้อมูลจากฐานข้อมูลมาทำการประมวลผล

ในระบบที่มิได้ใช้ฐานข้อมูล แฟ้มข้อมูลแต่ละแฟ้มจะถูกออกแบบให้ใช้ได้กับโปรแกรมของระบบงาน (Application Program) เฉพาะระบบงานระบบใดระบบหนึ่ง แฟ้มข้อมูลที่ใช้สำหรับระบบงานที่ต่างกันจึงไม่เหมือนกัน ดังนั้นในการเขียนโปรแกรมของระบบงานแต่ละระบบ จึงจำเป็นต้องอธิบายรายละเอียดของลักษณะการจัดเก็บข้อมูล (Records) ในแฟ้มข้อมูลที่จะนำมาประมวลผล ในภาษา COBOL เรียกวิธีการเช่นนี้ว่า File Description (FD)

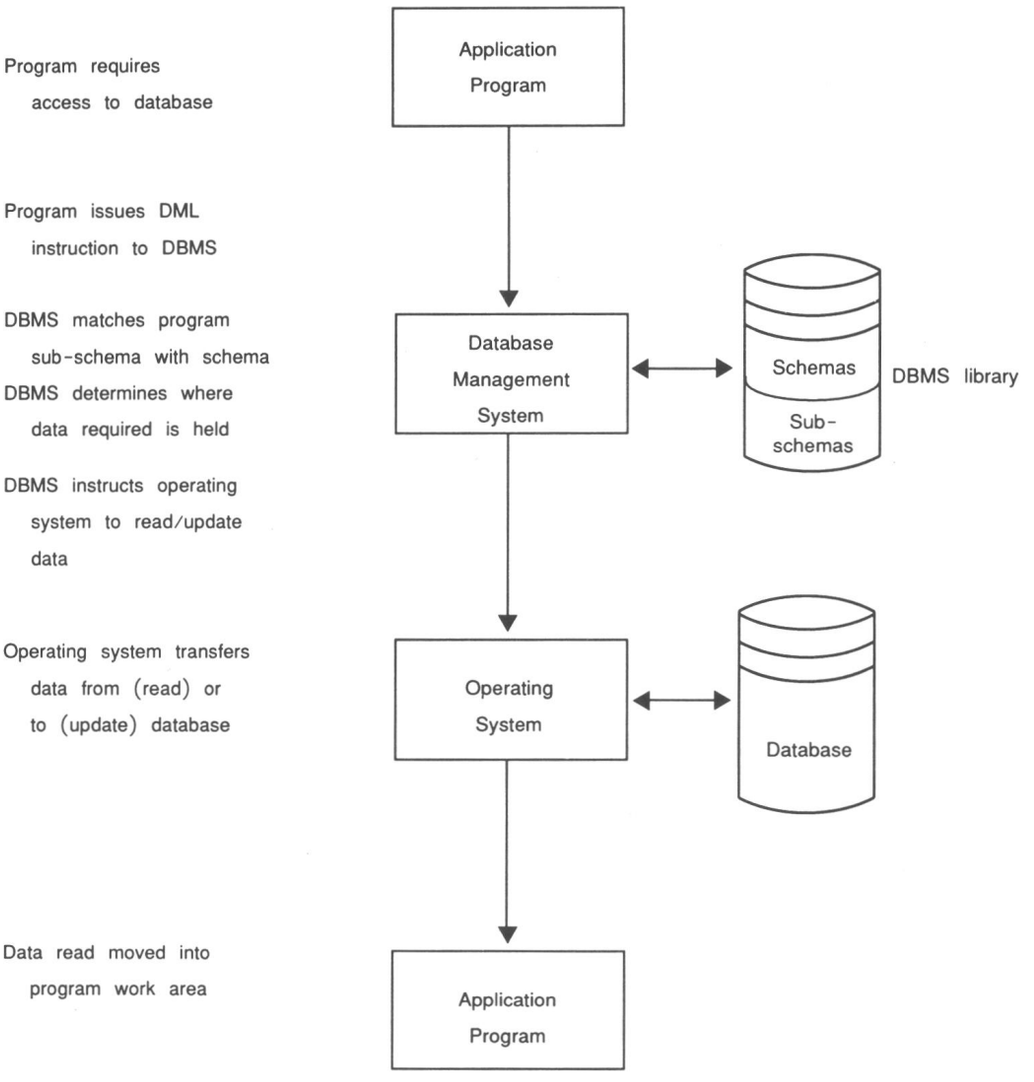
ในระบบฐานข้อมูล คำอธิบายลักษณะของข้อมูลที่จัดเก็บไว้ในฐานข้อมูลจะอยู่ต่างหากจากโปรแกรมของระบบงาน โดยจัดเก็บไว้ในห้องสมุดของฐานข้อมูล (Database Library) คำอธิบายลักษณะของข้อมูลในห้องสมุดนี้จะต้องมีองค์ประกอบ 2 ส่วน คือ องค์ประกอบแรก ได้แก่ คำอธิบายลักษณะทางกายภาพ (Physical Nature) ของข้อมูล ซึ่งรวมถึงตำแหน่งที่ตั้ง ลักษณะและความสัมพันธ์กับข้อมูลอื่นที่เกี่ยวข้อง องค์ประกอบส่วนที่สอง ด้วยเหตุที่โปรแกรมของระบบงานแต่ละระบบงานจะใช้ข้อมูลแต่เพียงบางส่วนในระบบฐานข้อมูลเท่านั้น ดังนั้นจึงจำเป็นต้องให้คำอธิบายด้วยว่าข้อมูลใดใช้กับระบบงานใด

The Conference on Data System Languages หรือ CODASYL ได้บัญญัติคำที่ใช้เรียกองค์ประกอบทั้ง 2 ส่วนข้างต้นไว้ คือ Schema หมายถึง คำอธิบายลักษณะของข้อมูลทั้งหมดในระบบฐานข้อมูล และ Sub-schema หมายถึง คำอธิบายบ่งชี้ว่าข้อมูลใดใช้กับโปรแกรมของระบบงานใด นอกจาก CODASYL แล้ว IBM ได้ใช้คำว่า Data Base Description (DBD) แทน Schema และคำว่า Program Specification Block (PSB) แทน Sub-Schema

โปรแกรมของระบบงานจะต้องให้ข้อมูลเกี่ยวกับ Sub-schema ที่เกี่ยวข้องกับโปรแกรมนั้น ดังนั้นจึงจำเป็นต้องระบุ Sub-schema ในห้องสมุดฐานข้อมูล รวมทั้งใช้ Schema แสดงลักษณะของข้อมูลที่อยู่ในฐานข้อมูล จึงจะสามารถอ่านหรือบันทึกข้อมูลในฐานข้อมูลได้ กระบวนการที่เกี่ยวข้องกับโปรแกรมของ

ระบบงาน Sub-schema และ Schema ตลอดจนการอ่านและเปลี่ยนแปลงฐานข้อมูลจะถูกควบคุมโดย Software ที่เรียกว่า Database Management System (DBMS) ซึ่งเขียนขึ้นโดยภาษาเฉพาะ เรียกว่า Data Management Language (DML)

วิธีการอ่านและปรับปรุงฐานข้อมูลแสดงได้ตามแผนภาพที่ 17.4



แผนภาพที่ 17.4 Database - reading and updating

อย่างไรก็ตาม แม้ว่าการใช้ข้อมูลร่วมกันได้หลายโปรแกรมหรือหลายระบบงานจะเป็นคุณลักษณะที่สำคัญของระบบฐานข้อมูล แต่ในระบบที่มิได้ใช้ฐานข้อมูลก็อาจมีการใช้ข้อมูลร่วมกันหลายโปรแกรมงานก็ได้ โดยออกแบบโปรแกรมเป็นพิเศษเพื่อให้ใช้ข้อมูลของโปรแกรมในระบบงานอื่นได้ ด้วยเหตุนี้จึงได้เกิดการคิดค้นระบบสารบรรณข้อมูล (Data Dictionary Directory หรือ DDD) ขึ้น ซึ่งอาจทำได้ด้วยมือ (Manual) หรือใช้โปรแกรมก็ได้ วัตถุประสงค์ของระบบสารบรรณข้อมูลก็เพื่อที่จะบันทึกข้อมูลทุกรายการในระบบตลอดจนอธิบายคุณลักษณะและวิธีการใช้งาน ระบบสารบรรณข้อมูลนี้สามารถช่วยเพิ่มประสิทธิภาพระบบฐานข้อมูล กรณีที่มีความยุ่งยากซับซ้อนได้อย่างมาก ระบบสารบรรณข้อมูลที่นำมาใช้ร่วมกับระบบฐานข้อมูลมักจะทำงานด้วยโปรแกรมมากกว่าทำด้วยมือ ซึ่งการเขียนโปรแกรมของระบบสารบรรณข้อมูลสามารถรวมเข้าด้วยกับ DBMS อย่างได้ผล

รายละเอียดเกี่ยวกับข้อมูลที่จะจัดเก็บไว้ในระบบสารบรรณข้อมูล มีดังนี้

- คำอธิบายข้อมูล (ได้แก่ ชื่อและเนื้อหา)
- ความสัมพันธ์กับข้อมูลอื่น
- หน่วยงานที่กำเนิดข้อมูลและเอกสารเบื้องต้น
- โปรแกรมและรายการที่จะต้องใช้ข้อมูล และใช้ด้วยเหตุผลใด (เช่น เพิ่มเติม แก้ไข ลบ และอ่าน)
- การแสดงผลลัพธ์
- วิธีการสอบทานข้อมูล (Edit Test) (ได้แก่ สอบทานรูปแบบความสมเหตุสมผลและความถูกต้องตรงกัน)
- รูปประโยค (Picture Statement) (ตัวเลข หรือตัวเลขแบบอักษร)
- วิธีจัดเก็บในฐานข้อมูล (ธรรมดาหรือมีรหัส)
- ที่อยู่ทางตรรกวิทยา (Logical Address) และตำแหน่งทางกายภาพ (Physical Location)

4) ระบบการประมวลผลแบบกระจาย (Distributed Processing)

ระบบการประมวลผลแบบกระจาย เป็นระบบการประมวลผลที่พัฒนาขึ้นใหม่ โดยที่แต่เดิมนั้นระบบการประมวลผลทั้งหมดจะกระทำ ณ คอมพิวเตอร์ขนาดใหญ่ที่เป็นศูนย์กลางเพียงแห่งเดียว แต่ในระบบการประมวลผลแบบกระจายนี้ หากการประมวลผลใดเกี่ยวข้องกับศูนย์งานใดโดยเฉพาะ ก็จะทำการประมวลผลด้วยคอมพิวเตอร์ขนาดเล็ก ณ ศูนย์งานนั้นเป็นเอกเทศ ณ ที่คอมพิวเตอร์ขนาดเล็กจะประกอบด้วยอุปกรณ์รับส่งข้อมูล ซึ่งเครื่องรับ-ส่งข้อมูลดังกล่าวสามารถที่จะรับแล้วส่งข้อมูลไปประมวลผลได้ ทั้งที่คอมพิวเตอร์ศูนย์กลาง และ ณ ศูนย์งานต่าง ๆ ที่มีคอมพิวเตอร์ขนาดเล็ก โดยอาศัยข่ายงานสื่อสารโทรคมนาคม หรือโดยวิธีการอื่นที่เหมาะสม เมื่อพิจารณาถึงปริมาณงาน ระยะทาง และค่าใช้จ่าย

3. การบันทึกระบบงาน (Recording the System)

3.1 คุณประโยชน์ของการจัดทำผังงาน

เมื่อผู้ตรวจสอบได้ทำการศึกษาระบบงานจนถี่ถ้วนเป็นที่พอใจแล้ว ก็จำเป็นต้องจดบันทึกระบบงานไว้เพื่อประโยชน์ในการประเมินการควบคุมภายใน การจดบันทึกระบบงานมักจะทำเป็นผังงาน (Flowchart) มากกว่าจดบันทึกเป็นคำอธิบาย (Narrative) ทั้งนี้เนื่องจากระบบและระเบียบของการควบคุมส่วนใหญ่มักจะสอดคล้องกับรูปแบบและเนื้อหาของผังงาน รวมทั้งช่วยให้เกิดความเข้าใจและตรวจทานได้ง่าย นอกจากนั้น การจัดทำผังงานยังเป็นมาตรฐานการปฏิบัติงานที่ดี ที่ช่วยให้ผู้ตรวจสอบครั้งต่อไปเข้าใจและสามารถปฏิบัติงานต่อไปได้โดยง่าย ที่สำคัญคือ ระบบคอมพิวเตอร์มีลักษณะที่ซับซ้อนกว่าระบบงานปกติ การจัดทำผังงานจึงเป็นประโยชน์อย่างยิ่งในการอธิบายและทำความเข้าใจกับระบบที่ซับซ้อนนั้น

3.2 เทคนิคการจัดทำผังงาน

หลักการที่สำคัญของเทคนิคในการจัดทำผังงาน คือ การจัดทำเส้นทางเดินของงาน (Flowline) เพื่อแสดงเส้นทางของขบวนการปฏิบัติงานและเอกสารที่เกี่ยวข้อง เส้นทางเดินของงานแต่ละระบบงานจะมีจุดเริ่มต้นตั้งแต่การรับรายการเข้ามา และสิ้นสุดที่รายการดังกล่าวได้ถูกบันทึกไว้ในสมุดบัญชีเรียบร้อยแล้ว และได้ส่งกลับหรือส่งออกไปจากแผนกที่ประมวลผลรายการนั้น

องค์ประกอบที่สำคัญในการจัดทำผังงาน มีดังนี้

- สัญลักษณ์มาตรฐานที่แสดงความหมายในตัว
- การจัดเรียงลำดับ
- ให้ความสำคัญแก่จำนวนสำเนาเอกสารทุกฉบับ เนื่องจากเป็นหลักฐานที่สำคัญทางการบัญชี
- ตำแหน่งของพนักงานผู้ปฏิบัติหน้าที่ในแต่ละขั้นตอน และควรระบุชื่อด้วย
- คำอธิบายประกอบควรลดให้น้อยที่สุด หรือมีอย่างสั้น ๆ หากจำเป็นต้องอธิบายรายละเอียดมากควรทำเป็นภาคผนวก

3.3 การจัดทำผังงานในระบบคอมพิวเตอร์

ลักษณะสำคัญของการจัดทำผังงานในระบบคอมพิวเตอร์ คือ การแสดงรวมวิธีการปฏิบัติงานทั้งที่ใช้คอมพิวเตอร์ และมิได้ใช้คอมพิวเตอร์เข้าไว้ในผังงานเดียวกัน ทั้งนี้จำเป็นต้องมีสัญลักษณ์เฉพาะ เพื่อแสดงว่าเป็นการปฏิบัติงานด้วยคอมพิวเตอร์ เช่น สัญลักษณ์แสดงว่าเป็นเทปหรือจานแม่เหล็ก เป็นต้น

ลักษณะที่สำคัญอีกประการหนึ่งของการจัดทำผังงานในระบบคอมพิวเตอร์ คือ การแสดงผังงานและคำอธิบายอย่างกระทัดรัด แต่เป็นที่เข้าใจได้ง่าย ซึ่งนอกจากจะให้เป็นที่เข้าใจได้แก่บุคคลที่ไม่ทราบเทคนิคการตรวจสอบมาก่อนเลยแล้ว ยังจะต้องแสดงให้เห็นจุดสำคัญที่ผู้ตรวจสอบควรให้ความสนใจอย่างเข้มงวดด้วย

ปัจจัยที่ควรพิจารณาในการจัดทำผังงานในระบบคอมพิวเตอร์มีดังนี้

3.3.1 ผังงานเบื้องต้น (Overview Flowcharts)

ในขั้นแรกผู้ตรวจสอบควรที่จะได้ตระเตรียมหรือจัดทำร่างผังงานเบื้องต้นสำหรับระบบงานสำคัญที่ใช้คอมพิวเตอร์ ก่อนที่จะจัดทำผังงานที่มีรายละเอียดสมบูรณ์ผังงานเบื้องต้นนี้จะแสดงขอบเขตและโครงสร้างทั้งหมดของการประมวลผล และจะทำให้ทราบผลกระทบของระบบคอมพิวเตอร์ที่มีต่อวิธีการตรวจสอบ

องค์ประกอบสำคัญที่ควรปรากฏในผังงานเบื้องต้น ได้แก่ การนำข้อมูลเข้า แฟ้มข้อมูลหลัก (Master Files) และการแสดงผลลัพธ์จากการประมวลผล ซึ่งอาจจะเป็นผลลัพธ์ปกติที่ได้จากการประมวลผลและรายงานพิเศษ (Exception Reports) สำหรับระบบงานที่มีความซับซ้อนมาก ควรจะแบ่งเส้นทางข้อมูลออกเป็นระบบย่อย ๆ และระบุจุดสำคัญ ๆ ที่มีการผลิตรายงานหรือจัดทำแฟ้มข้อมูล

3.3.2 การจัดทำโปรแกรม (Programmed Operations)

ในการจัดทำผังงาน ผู้ตรวจสอบจำเป็นที่จะต้องจดบันทึกวิธีการสร้างและใช้โปรแกรมหรือไม่ ขึ้นอยู่กับการวินิจฉัยความสำคัญ การจดบันทึกการจัดทำโปรแกรมนี้จะรวมถึงการจดบันทึกขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ตลอดจนการทำงานหรือขั้นตอนอื่น ๆ ที่จำเป็น และมีความสำคัญต่อการทำความเข้าใจเส้นทางของผังงานทั้งหมด

การจดบันทึกการจัดทำโปรแกรม จะใช้สัญลักษณ์เช่นเดียวกับการจดบันทึกวิธีการปฏิบัติงานและการควบคุมแบบ Manual อย่างไรก็ตามโดยปกติแล้วมักจำเป็นต้องอธิบายรายละเอียดการทำงานของโปรแกรมที่ใช้ในการปฏิบัติการ และการควบคุมที่พิเศษ

3.3.3 การแก้ไขข้อมูลถาวร (Standing Data Amendments)

วิธีการแก้ไขข้อมูลถาวรยากที่จะแสดงรวมไว้ในผังงานของระบบงาน เพราะมีข้อยุ่งยากในการเกี่ยวข้องกับแฟ้มข้อมูลหลัก (Master Files) ฉะนั้นจึงควรแยกแสดงผังงานหรือคำอธิบายการแก้ไขข้อมูลถาวรต่างหากจากผังงานของระบบงาน

3.3.4 วิธีปฏิบัติเมื่อข้อมูลผิดพลาด (Rejection Procedures)

คอมพิวเตอร์จะปฏิเสธข้อมูลที่ไม่ถูกต้องในขั้นตอนของการสอบทาน (Edit) และการปรับปรุง (Update) ข้อมูล ธุรกิจที่ใช้คอมพิวเตอร์มักจะกำหนดมาตรฐานและวิธีการปฏิบัติในการตรวจสอบ แก้ไข และปฏิเสธข้อมูล ซึ่งการกำหนดมาตรฐานและวิธีการปฏิบัติดังกล่าวปกติจะอยู่ในรูปของผังงานหรือคำอธิบายอยู่แล้ว ในการจัดทำผังงานของระบบงาน ผู้ตรวจสอบควรอ้างถึงผังงานของวิธีปฏิบัติเมื่อข้อมูลผิดพลาดไว้ด้วย

3.3.5 การควบคุมเป็นครั้งคราว (Periodic Controls)

วิธีการควบคุมบางประการที่มีการปฏิบัติเป็นครั้งคราวหรือเป็นระยะ โดยแยกออกจากการประมวลผลตามปกติ เช่น การกระทบยอดบัญชี เป็นต้น ควรบันทึกไว้ต่างหากจากผังงานของระบบงาน แต่ให้อ้างอิงกันได้

3.3.6 การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Control)

โดยปกติการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ ยากที่จะแสดงรวมไว้ในผังเดียวกับผังงานของระบบบัญชี เพราะจะทำให้ผังงานของระบบบัญชีมีความยุ่งยากซับซ้อนมากยิ่งขึ้น ฉะนั้นควรแยกการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ แสดงเป็นผังงานต่างหากจากผังงานของระบบบัญชี หรือจัดทำเป็นคำอธิบายโดยย่อ (Narrative Form)

3.4 เอกสารประกอบ (Documentation)

เอกสารประกอบการดำเนินงานด้านคอมพิวเตอร์ จะเป็นประโยชน์และเป็นสื่อที่สำคัญยิ่งของผู้ตรวจสอบในการศึกษาและบันทึกระบบงาน ทั้งนี้เนื่องจากจะมีรายละเอียดและความถูกต้องแน่นอนของการปฏิบัติงานอยู่โดยครบถ้วน โดยทั่วไปเอกสารประกอบการดำเนินงานด้านคอมพิวเตอร์ที่มีความสำคัญต่อผู้ตรวจสอบแบ่งออกเป็น 2 ประเภท ได้แก่ เอกสารประกอบระบบงาน (Systems Documentation) และเอกสารมาตรฐานของระบบงาน (Standards Documentation)

3.4.1 เอกสารประกอบระบบงาน (Systems Documentation)

เอกสารประกอบระบบงานจะประกอบด้วยคำอธิบายทั่วไป (General Description) และรายละเอียด (Detailed Description) ของระบบงาน ทั้งที่เป็นการปฏิบัติงานด้วยบุคคล (Manual) และที่เป็นขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) โดยปกติคำอธิบายทั่วไปมักจะหมายถึงคำอธิบายเกี่ยวกับโครงสร้างของระบบงาน (Outline Systems Description) ซึ่งจะเป็นคำอธิบายในรูปลักษณะที่ช่วยให้เกิดความเข้าใจระบบงานทั้งหมดได้โดยง่าย ทั้งในส่วนของขั้นตอนการปฏิบัติงานโดยบุคคล และขั้นตอนการทำงานของโปรแกรม ตลอดจนแสดงความสัมพันธ์ภายในระหว่างส่วนต่าง ๆ ของระบบงาน

เพื่อช่วยเหลือให้การปฏิบัติงานเป็นไปอย่างชัดเจนและไม่สับสน ปกติจะมีการจัดทำคู่มือสำหรับผู้ปฏิบัติงานในแผนกผู้ใช้ (User Department) และสำหรับส่วนที่ทำหน้าที่ควบคุมในแผนกคอมพิวเตอร์ ในคู่มือดังกล่าวจะบรรจุขั้นตอนการปฏิบัติงานโดยลำดับและอย่างมีรายละเอียดของการรวบรวมข้อมูล การนำข้อมูลเข้าการที่เครื่องคอมพิวเตอร์ปฏิเสธข้อมูล และการแสดงผลลัพธ์ คู่มือดังกล่าวนี้เป็นแหล่งข้อมูลที่เป็นประโยชน์อย่างยิ่งสำหรับการศึกษาและบันทึกระบบงาน

สำหรับขั้นตอนการทำงานของโปรแกรม จะมีเอกสารประกอบที่เกี่ยวกับขั้นตอนการทำงานของโปรแกรมในรายละเอียดที่ต่างระดับกันไป ได้แก่ เอกสารคำอธิบายระบบงาน (System Description) ซึ่งจะให้รายละเอียดของโปรแกรมเฉพาะที่ใช้แต่ละงาน (Application) และเอกสารที่อธิบายแต่รายละเอียดของโปรแกรมล้วน ๆ เอกสารทั้งสองแบบที่กล่าวนี้จะเป็นประโยชน์สำหรับผู้ตรวจสอบ และเป็นแหล่งข้อมูลในการทำความเข้าใจขั้นตอนการทำงานของโปรแกรมโดยเฉพาะในระบบงานที่ซับซ้อน เอกสารประกอบในระดับที่แสดงรายละเอียดมากจะแสดงแผนผังของโปรแกรมและคำสั่งต่าง ๆ ในโปรแกรมประกอบไว้ด้วย

3.4.2 เอกสารมาตรฐานของระบบงาน (Standards Documentation)

กระบวนการออกแบบ พัฒนา แก้ไข และปฏิบัติการทางคอมพิวเตอร์ควรจัดทำเป็นมาตรฐานไว้ เพื่อช่วยให้ผู้ปฏิบัติงานมีคู่มือที่เป็นมาตรฐานสำหรับการดำเนินการทางด้านคอมพิวเตอร์ สำหรับคู่มือการปฏิบัติการทางคอมพิวเตอร์นั้นจะระบุหน้าที่ที่แน่นอนของเจ้าหน้าที่ปฏิบัติการ (Operating Staff) กับบรรณารักษ์ (Librarian) การใช้คำสั่งต่าง ๆ ในการปฏิบัติการกับเครื่องคอมพิวเตอร์จะต้องมีมาตรฐานกำหนดไว้ คู่มือหรือเอกสารมาตรฐานดังกล่าวจะเป็นประโยชน์สำหรับผู้ตรวจสอบในการศึกษาและบันทึกรูปแบบของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Control)

4. การทบทวนการศึกษาและบันทึกระบบงาน (Transaction Reviews)

ภายหลังจากที่ได้จัดทำผังของระบบงาน หรือจดบันทึกระบบงานแล้ว ผู้ตรวจสอบควรจะเลือกติดตามรายการ (Trace) อย่างน้อยหนึ่งรายการที่ผ่านเข้ามาสู่ระบบงานทุกๆส่วนของระบบงาน เพื่อทดสอบความถูกต้องหรือยืนยันความเข้าใจจากการศึกษาและจดบันทึกระบบงานของผู้ตรวจสอบ

การทบทวนการศึกษาและบันทึกระบบงานในลักษณะที่กล่าวนี้ ควรจะกระทำให้ครอบคลุมทุกส่วนของผังงาน รวมทั้งการตรวจสอบหลักฐานการปฏิบัติงาน และการสอบถามผู้ปฏิบัติงาน เสมือนหนึ่งผู้ตรวจสอบได้กระทำการติดตามผลการปฏิบัติงานของพนักงานและทดลองปฏิบัติซ้ำ (Reperformance) ภายในขอบเขตที่สามารถกระทำได้ ในขณะที่ทำการทบทวนการศึกษาและบันทึกระบบงาน ผู้ตรวจสอบควรระมัดระวังผลกระทบจากขั้นตอนการปฏิบัติงานบางขั้นตอน ซึ่งหากพิจารณาในแง่นัยสำคัญของขอบเขตการตรวจสอบแล้ว ไม่จำเป็นต้องบันทึกไว้ในผังงานก็ได้

ในกรณีที่ผลจากการทบทวนการศึกษาและบันทึกระบบงานยืนยันว่า ความเข้าใจของผู้ตรวจสอบเกี่ยวกับระบบงานนั้นถูกต้อง และได้จดบันทึกไว้โดยครบถ้วนแล้ว ก็เป็นอันเสร็จสิ้นการศึกษาและบันทึกระบบงาน แต่ถ้าผลออกมายังไม่ถูกต้องหรือไม่ครบถ้วน ผู้ตรวจสอบจำเป็นต้องค้นหาข้อมูลเพิ่มเติมและแก้ไขผังงานนั้นเสียให้ถูกต้องครบถ้วนต่อไป

การทบทวนการศึกษาและบันทึกระบบงาน หรือการทดสอบรายการในระบบคอมพิวเตอร์มีข้อที่ควรคำนึง 2 ประการ คือ

1) ในบางครั้งเป็นการยากที่จะทดสอบรายการใดรายการหนึ่งโดยเฉพาะ โดยใช้ยอดสรุปหรือยอดการวิเคราะห์ของคอมพิวเตอร์ ในกรณีเช่นนี้ควรจะทดสอบรายการนั้นโดยใช้ batch หรือใช้รายงานของคอมพิวเตอร์ และทดสอบยอดรวมโดยตรวจสอบยอดรวมครั้งหลังสุดกับการปฏิบัติงานครั้งหลังสุด

2) ในทางปฏิบัติบางครั้งเป็นการยากที่จะจำแนกหรือคัดเลือกรายการบางรายการเพื่อทดสอบยืนยันว่า การประมวลผลตามขั้นตอนการทำงานของโปรแกรมนั้นเป็นไปอย่างเหมาะสม ตัวอย่างเช่น การเลือกรายการพิเศษ (Exceptional Transactions) มาทดสอบว่าได้ปรากฏรายการนั้นในรายการพิเศษ (Exception Reports) หรือไม่ ซึ่งเป็นเรื่องยากที่จะทดสอบได้ ในกรณีเช่นนี้ควรใช้การทดสอบเอกสารเบื้องต้นก็จะเป็นการเพียงพอแล้ว

ถ้าผู้ตรวจสอบได้รับความมั่นใจว่า เอกสารประกอบระบบงานมีรายละเอียดของขั้นตอนการทำงานของโปรแกรมที่ใช้ในการปฏิบัติงานจริงอย่างเพียงพอแล้ว ผู้ตรวจสอบก็อาจเชื่อถือได้ว่าการตรวจสอบเอกสารประกอบโปรแกรมเพียงพอแล้ว โดยไม่จำเป็นต้องทดสอบรายการต่อไป

ในทางปฏิบัติเป็นไปไม่ได้ที่จะใช้วิธีการทดสอบรายการสำหรับขอบเขตการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Control) ทั้งนี้ก็เพราะเส้นทางของข้อมูลแยกต่างหากจากระบบการบัญชี ผู้ตรวจสอบจึงควรที่จะใช้วิธีการตรวจสอบเอกสารหลักฐานและการสังเกตวิธีการปฏิบัติงานในขณะที่ทำการประเมินระบบการควบคุม

5. สรุป

ในการศึกษาและบันทึกระบบงานที่มีประสิทธิภาพ ผู้ตรวจสอบจำเป็นที่จะต้องเข้าใจและมีพื้นฐานเกี่ยวกับหลักการของคอมพิวเตอร์และวิธีการประมวลผล อันได้แก่ การนำข้อมูลเข้า การประมวลผล และการแสดงผลลัพธ์ สำหรับการประมวลผลนั้นรวมถึงการสอบทานข้อมูล (Editing) การคำนวณ การรวมค่าและการจัดหมวดหมู่หรือวิเคราะห์ ตลอดจนการสร้างข้อมูลโดยอัตโนมัติ และการปรับปรุงแฟ้มข้อมูล นอกจากนั้นผู้ตรวจสอบจำเป็นต้องมีความเข้าใจเป็นพิเศษเกี่ยวกับการนำข้อมูลเข้าและการแสดงผลลัพธ์ระบบ On-line การประมวลผลระบบ Real-time และโครงสร้างระบบฐานข้อมูล (Database)

การบันทึกระบบงานจะสะดวกและเป็นประโยชน์อย่างยิ่ง หากจัดทำเป็นผังระบบงาน (Flowcharts) โดยรวมการปฏิบัติงานทั้งส่วนของคอมพิวเตอร์และส่วนที่มิใช่คอมพิวเตอร์เข้าไว้ในผังงานเดียวกัน หลังจากนั้นผู้ตรวจสอบจะต้องทำการทดสอบระบบงานเพื่อยืนยันความเข้าใจและความถูกต้องของการศึกษาและบันทึกระบบงานโดยคัดเลือกรายการเพื่อติดตามเส้นทางที่ผ่านเข้ามาสู่ระบบงานนั้น ๆ ถ้าผู้ตรวจสอบได้ตรวจสอบเอกสารประกอบระบบงาน และมีความพอใจกับรายละเอียดที่ปรากฏในเอกสารประกอบนั้นแล้ว ก็พึงถือได้ว่าการศึกษาและบันทึกระบบงานเพียงพอแล้วโดยไม่จำเป็นต้องทดสอบระบบงาน



18

การตรวจสอบเพื่อประเมินระบบการควบคุมภายใน

การตรวจสอบเพื่อประเมินระบบการควบคุมภายใน

1. การตรวจสอบทั่วไป

1.1 ขอบเขตของการประเมิน

ผู้ตรวจสอบจำเป็นต้องเข้าไปเกี่ยวข้องกับระบบการควบคุมภายในของธนาคารพาณิชย์ ด้วยวัตถุประสงค์ที่สำคัญ ดังนี้

1) ผู้ตรวจสอบจำเป็นต้องตัดสินใจว่าจะสามารถให้ความเชื่อถือต่อระบบการควบคุมภายในได้มากน้อยเพียงไร เพื่อจะสามารถกำหนดขอบเขตและช่วงเวลาการตรวจสอบได้อย่างเหมาะสม

2) เพื่อชี้ให้ผู้บริหารของธนาคารพาณิชย์ทราบถึงข้อบกพร่องของการควบคุมภายในอย่างสำคัญ พร้อมทั้งเสนอแนะวิธีการแก้ไขเพื่อให้ความคุ้มครองการบันทึกข้อมูลทางการบัญชีและรักษาความปลอดภัยแก่ทรัพย์สิน

โดยทั่วไปการควบคุมภายในมีความหมายครอบคลุมถึงวิธีการ การดำเนินการและการจัดโครงสร้างใด ๆ เพื่อรักษาความปลอดภัยแก่ทรัพย์สิน และเพื่อความถูกต้องเชื่อถือได้ของการบันทึกบัญชี ตลอดจนเพื่อส่งเสริมประสิทธิภาพในการปฏิบัติงานและการดำเนินนโยบายของฝ่ายจัดการ ด้วยความหมายดังกล่าวจึงอาจแบ่งการควบคุมภายในออกเป็น 2 ประเภท ได้แก่ การควบคุมภายในทางการบัญชี (Internal Accounting Controls) และการควบคุมการปฏิบัติงาน (Operational Controls) อย่างไรก็ตามโดยปกติเมื่อกล่าวถึงการควบคุมภายในทางการบัญชี มักจะรวมนัยของการควบคุมการปฏิบัติงานไว้ด้วย ซึ่งในที่นี้การควบคุมภายในจะหมายถึงการควบคุมภายในทางการบัญชี

1.2 การควบคุมขั้นพื้นฐานและกฎเกณฑ์การควบคุม

ในการประเมินระบบการควบคุมภายใน ผู้ตรวจสอบจะต้องทำความเข้าใจคำที่มีความหมาย 2 คำ คือ การควบคุมขั้นพื้นฐาน (Basic Controls) และกฎเกณฑ์การควบคุม (Disciplines) การควบคุมขั้นพื้นฐานหมายถึง การควบคุมทั่ว ๆ ไปเพื่อความมั่นคงว่าเฉพาะรายการที่ได้รับอนุมัติอย่างถูกต้องแล้วเท่านั้น ที่ได้รับการประมวลผลและบันทึกอย่างถูกต้องและครบถ้วน ส่วนกฎเกณฑ์การควบคุม หมายถึง ระบบการควบคุมเพื่อความมั่นใจว่าได้มีการปฏิบัติตามการควบคุมขั้นพื้นฐานอย่างเหมาะสมและต่อเนื่อง

การทำความเข้าใจความหมายของทั้งสองคำข้างต้นมีความสำคัญ เนื่องจากขอบเขตของการให้ความเชื่อถือต่อระบบการควบคุมภายในอยู่ที่ความมั่นใจของผู้ตรวจสอบว่าธนาคารพาณิชย์ได้มีการปฏิบัติตามการควบคุมขั้นพื้นฐานอย่างเหมาะสมและต่อเนื่องมากน้อยเพียงไร หรือไม่ ในกรณีที่ไม่มีกฎเกณฑ์การควบคุมใช้อยู่หรือมีใช้อยู่น้อย โดยเฉพาะอย่างยิ่งในส่วนงานที่มีพนักงานจำกัด ผู้ตรวจสอบที่ไม่อาจมั่นใจได้ว่าส่วนงานนั้นได้มีการปฏิบัติตามการควบคุมขั้นพื้นฐานอย่างเหมาะสมและต่อเนื่อง ในกรณีเช่นนี้ผู้ตรวจสอบจำเป็นต้องขยายการตรวจสอบรายการทางบัญชีและการเงินเพิ่มมากขึ้น หรือหากจำเป็นหรือสมควรก็จะต้องทดสอบขั้นตอนการควบคุมขั้นพื้นฐานนั้นด้วย

2. การตรวจสอบในระบบคอมพิวเตอร์

2.1 ลักษณะของการควบคุมในระบบคอมพิวเตอร์

การควบคุมในระบบคอมพิวเตอร์มีวัตถุประสงค์เช่นเดียวกับการควบคุมในระบบที่มิได้ใช้คอมพิวเตอร์ นั่นคือ การควบคุมเพื่อความมั่นใจว่าเฉพาะรายการที่ได้รับอนุมัติแล้วเท่านั้นที่ได้รับการประมวลผลอย่างสมบูรณ์และถูกต้อง การควบคุมบางอย่างในระบบคอมพิวเตอร์ที่กระทำโดยบุคคลหรือด้วยมือ เช่น การควบคุมในแผนกผู้ใช้ซึ่งเรียกว่า การควบคุมทางด้านผู้ใช้ (User Controls) ยังคงมีลักษณะคล้ายคลึงกับการควบคุมในระบบที่มิได้ใช้คอมพิวเตอร์ อย่างไรก็ตามการทำงานด้วยระบบคอมพิวเตอร์ได้ก่อให้เกิดความเปลี่ยนแปลงในด้านการควบคุมและการประมวลผลข้อมูล ซึ่งความเปลี่ยนแปลงดังกล่าวจะมากน้อยเพียงใด ขึ้นอยู่กับขอบเขตของการประมวลผลข้อมูลด้วยคอมพิวเตอร์ในแต่ละระบบ

หลักการที่เปลี่ยนแปลงไป มีดังนี้

1) วิธีการหรือขั้นตอนการควบคุมและการบัญชีส่วนใหญ่ ซึ่งแต่ก่อนเคยปฏิบัติด้วยบุคคล จะถูกแทนที่ในทุกขั้นตอนด้วยโปรแกรมคอมพิวเตอร์ ดังนั้นในที่นี้ผู้ตรวจสอบจะต้องเข้าไปเกี่ยวข้องกับสิ่งที่เรียกว่า ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures)

2) กระบวนการดำเนินการเกี่ยวกับขั้นตอนการทำงานของโปรแกรมจะเป็นไปอย่างเหมาะสมและต่อเนื่อง ก็ด้วยการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) อย่างมีประสิทธิภาพ การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ ในที่นี้หมายถึง การควบคุมซึ่งส่วนใหญ่กระทำในศูนย์คอมพิวเตอร์ อันได้แก่ การพัฒนา การรักษาความปลอดภัย และการใช้โปรแกรมคอมพิวเตอร์ ถ้าหากเป็นระบบที่มิได้ใช้คอมพิวเตอร์จะพิสูจน์ความถูกต้องของการควบคุมและการบัญชีได้ ก็โดยทดสอบผลลัพธ์จากการดำเนินงานแต่ละรายการ แต่ในระบบคอมพิวเตอร์การทดสอบด้วยมือคนโดยครบถ้วนทุกรายการนั้นมิใช่สิ่งที่จำเป็น เพราะสามารถให้ความเชื่อถือและไว้วางใจผลลัพธ์จากการประมวลผลได้ โดยอาศัยความเพียงพอของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ที่มีประสิทธิภาพ

3) ด้วยเหตุที่ลดการตรวจสอบความถูกต้องของผลลัพธ์จากการประมวลผล จึงจำเป็นต้องมีมาตรการพิเศษเพื่อความมั่นใจในความถูกต้องสมบูรณ์ของข้อมูลในการประมวลผล มาตรการพิเศษนี้ได้แก่ การควบคุมความถูกต้องของข้อมูลหลัก (Standing Data) ที่บรรจุอย่างถาวรในแฟ้มข้อมูลหลัก (Master Files) วิธีการควบคุมได้แก่ การตรวจสอบความถูกต้องของข้อมูลหลักในแฟ้มข้อมูล และการป้องกันการเข้าถึงและเปลี่ยนแปลงแฟ้มข้อมูลโดยมิได้รับอนุญาต การป้องกันแฟ้มข้อมูลนี้เรียกว่า การควบคุมความปลอดภัยของแฟ้มข้อมูล (Data File Security Controls) ซึ่งเป็นส่วนหนึ่งของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls)

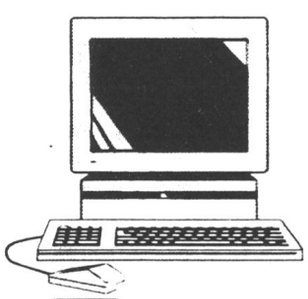
2.2 การควบคุมทางด้านผู้ใช้ (User Controls)

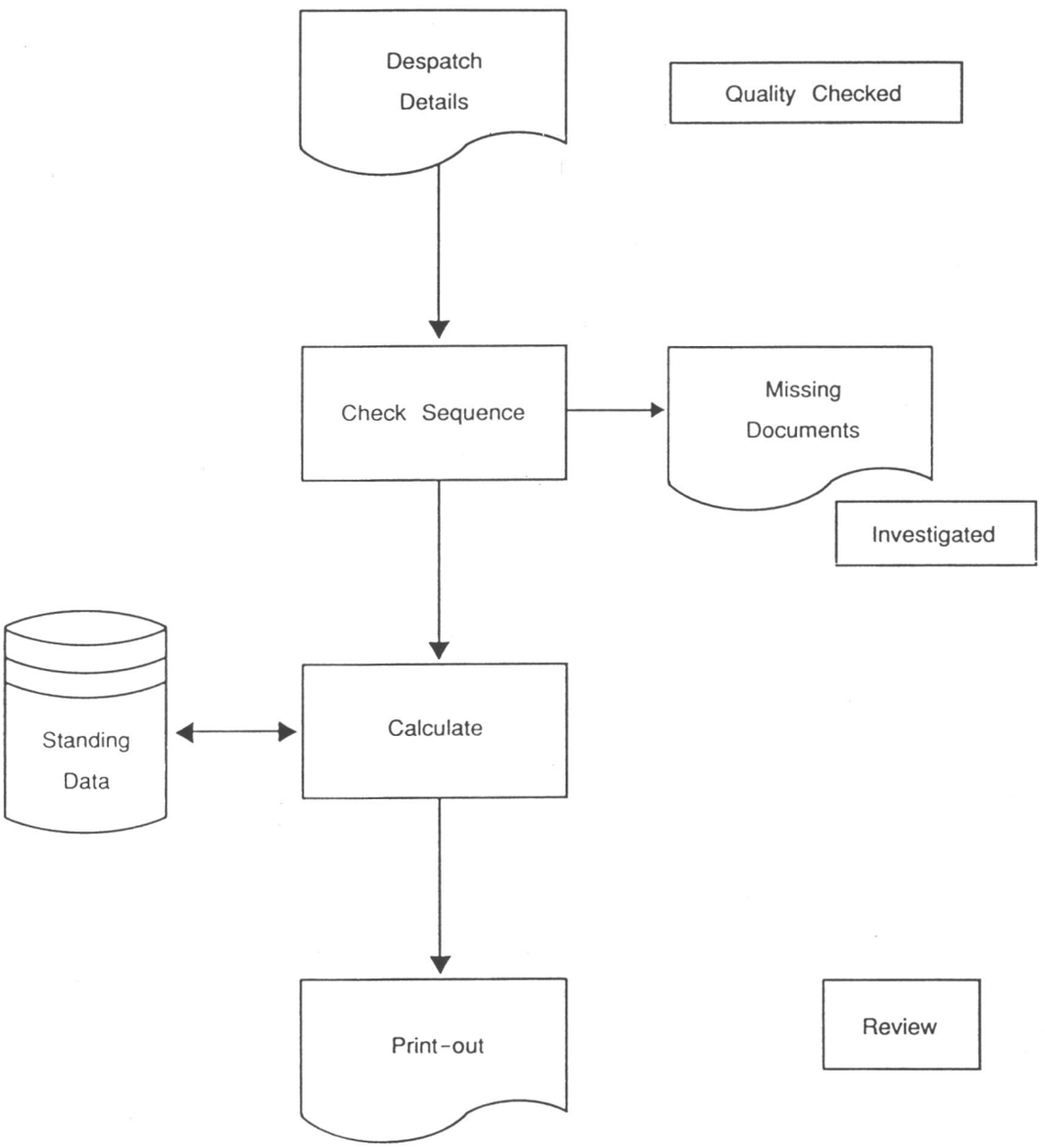
การควบคุมทางด้านผู้ใช้ หมายถึง การควบคุมข้อมูลที่ทำการประมวลผลโดยบุคคล (Manual Controls) ผู้ใช้ในที่นี้มีความหมายถึงพนักงานที่ไม่เกี่ยวข้องกับการดำเนินงานด้านคอมพิวเตอร์ การควบคุมทางด้านผู้ใช้จึงเป็นการควบคุมในแผนกของผู้ใช้ และบางกรณีจะรวมถึงการควบคุมบางส่วนในศูนย์คอมพิวเตอร์ด้วย

การควบคุมทางด้านผู้ใช้ประกอบด้วย การควบคุมที่เกี่ยวข้องและไม่เกี่ยวข้องกับการประมวลผลด้วยคอมพิวเตอร์ การควบคุมที่เกี่ยวข้องกับการประมวลผลด้วยคอมพิวเตอร์ ได้แก่ การกำหนดไว้ในขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ให้รายงานข้อผิดพลาดสูญหาย (missing) หรือข้อผิดปกติ (exceptional) ของข้อมูลที่ทำการประมวลผลเพื่อตรวจสอบข้อเท็จจริงต่อไป ส่วนการควบคุมที่ไม่เกี่ยวข้องกับการประมวลผล ได้แก่ การตรวจสอบคุณภาพและเงื่อนไขของข้อมูลเบื้องต้น หรือการตรวจสอบว่าข้อมูลทุกรายการได้รับอนุมัติการบันทึกรายการอย่างถูกต้องแล้ว เป็นต้น นอกจากที่กล่าวแล้วการควบคุมทางด้านผู้ใช้ชนิดอื่น ๆ ได้แก่ การตรวจสอบที่มีวัตถุประสงค์จำเพาะเพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรม เช่น การตรวจสอบข้อมูลเบื้องต้น (Source Data) กับรายงานการแก้ไขข้อมูลที่เป็น Standing Data

เทคนิคการควบคุมทางด้านผู้ใช้โดยทั่วไปมีความคล้ายคลึงกับการควบคุมในระบบที่มิได้ใช้คอมพิวเตอร์ ข้อแตกต่างที่สำคัญอยู่ที่เป็นการตรวจสอบจากผลลัพธ์ที่ผลิตโดยคอมพิวเตอร์ (Computer Output) มิใช่รายงานที่จัดทำด้วยมือคน (Manually- produced Reports) ข้อแตกต่างประการอื่นได้แก่ วิธีการควบคุมค่อนข้างจะมีระเบียบแบบแผนแน่นอน (formalised) เช่น การแก้ไขรายการที่ผิดพลาด เป็นต้น การควบคุมทางด้านผู้ใช้ยังรวมถึงเทคนิคในการตรวจสอบผลลัพธ์จากคอมพิวเตอร์ เปรียบเทียบกับข้อมูลเบื้องต้น หรือกับยอดรวมที่กำหนดไว้ก่อน (Pre-determined Totals) หรือเทคนิคการตรวจสอบรายงานกระทบยอดของคอมพิวเตอร์ ตลอดจนรายงานข้อมูลที่ผิดพลาดหรือที่ผิดปกติ เป็นต้น

แผนภาพที่ 18.1 แสดงให้เห็นถึงการควบคุมทางด้านผู้ใช้ทั้ง 3 แบบ ได้แก่ การนับจำนวนของข้อมูลนำเข้าหรือตรวจสอบคุณภาพของข้อมูลเบื้องต้น ซึ่งเป็นการควบคุมที่ไม่เกี่ยวข้องกับการประมวลผล การตรวจสอบเอกสารหลักฐานที่สูญหายไปหรือไม่ครบ ซึ่งเป็นการควบคุมที่เกี่ยวข้องกับการประมวลผล และจะควบคุมได้ผลก็ต่อเมื่อได้กำหนดไว้ในขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) แล้ว และการตรวจสอบรายงานที่ได้จากคอมพิวเตอร์ ซึ่งจะเป็นการตรวจสอบขั้นตอนการทำงานของโปรแกรมด้วยส่วนหนึ่ง





แผนภาพที่ 18.1 การควบคุมทางด้านผู้ใช้

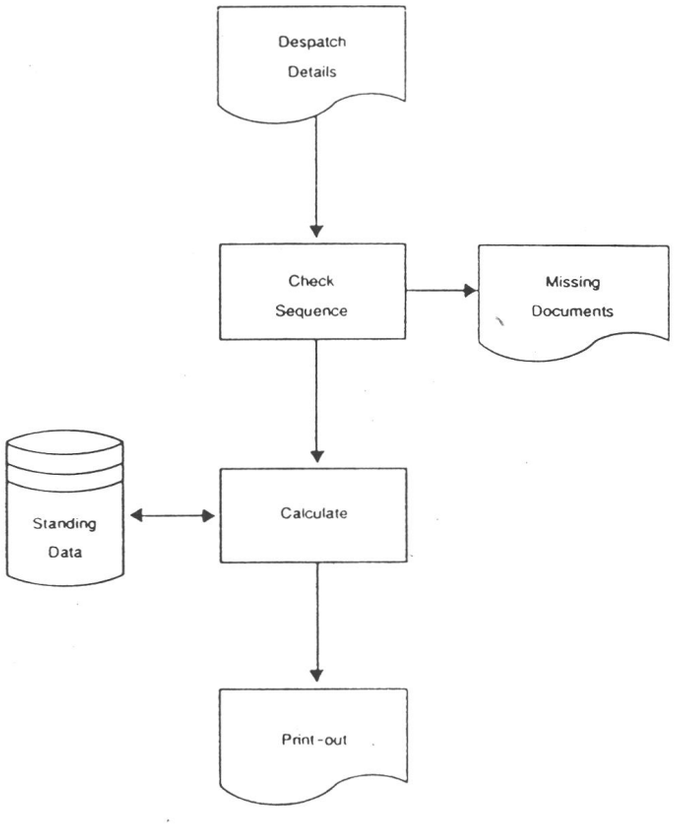
2.3 ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures)

ขั้นตอนการทำงานของโปรแกรมแบ่งออกเป็น 2 ประเภท ดังนี้

1) ขั้นตอนการทำงานของโปรแกรมซึ่งใช้แทนที่การควบคุมโดยบุคคล ได้แก่ ขั้นตอนของโปรแกรมที่ทำหน้าที่ตรวจสอบความสมบูรณ์ ความถูกต้อง และการได้รับอนุมัติข้อมูลที่ทำการประมวลผล รวมถึงการทำหน้าที่บรรณาธิการข้อมูล (Edit Tests) การรวมค่าข้อมูลทดสอบกับยอดรวมที่ใช้ในการควบคุม การรวมค่ารายการต่าง ๆ ในแฟ้มข้อมูลหลัก แล้วกระทบยอดกับยอดรวมของแฟ้มข้อมูล ตลอดจนการจำแนกและรายงานข้อมูลที่ผิดพลาด ข้อมูลผิดปกติ และข้อมูลที่สูญหาย

2) ขั้นตอนการทำงานของโปรแกรมซึ่งใช้แทนที่การปฏิบัติงานทางบัญชีโดยบุคคล ได้แก่ การคำนวณและสร้างเอกสารสำคัญ การปรับปรุงแฟ้มข้อมูล และการสร้างข้อมูลต่าง ๆ ภายในคอมพิวเตอร์ เป็นต้น

แผนภาพที่ 18.2 จะแสดงให้เห็นขั้นตอนการทำงานของโปรแกรมทั้ง 2 ประเภทที่กล่าวข้างต้น คือ การตรวจสอบลำดับ (Check Sequence) เป็นขั้นตอนการทำงานของโปรแกรมซึ่งแทนที่การควบคุมโดยบุคคล และการคำนวณ (Calculate) เป็นขั้นตอนการทำงานของโปรแกรมซึ่งแทนที่การปฏิบัติงานด้านบัญชีโดยบุคคล



แผนภาพที่ 18.2 ขั้นตอนการทำงานของโปรแกรม

2.4 การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Control)

การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ เป็นการควบคุมทั่วไป (General Controls) ซึ่งส่วนใหญ่จะเป็นการควบคุมภายในศูนย์คอมพิวเตอร์ การควบคุมดังกล่าวแบ่งออกได้เป็น 3 ประเภท ตามวัตถุประสงค์ของการควบคุม ดังนี้

2.4.1 การควบคุมการพัฒนาระบบงาน (Implementation Controls)

หมายถึง การควบคุมเพื่อความมั่นใจว่าขั้นตอนการทำงานของโปรแกรมที่เหมาะสมได้บรรจุไว้ในโปรแกรมอย่างครบถ้วนและอย่างมีประสิทธิภาพ ทั้งในขณะที่ได้เริ่มปฏิบัติงานตามโปรแกรมนั้น และเมื่อมีการแก้ไขเปลี่ยนแปลงในระยะต่อไป การควบคุมชนิดนี้รวมถึงการควบคุมการออกแบบ และการนำออกใช้งานของระบบงานใหม่ การเปลี่ยนแปลงแก้ไขโปรแกรมและเอกสารต่าง ๆ ที่เกี่ยวข้อง

2.4.2 การควบคุมความปลอดภัยของโปรแกรม (Program Security Controls)

หมายถึง การควบคุมเพื่อป้องกันมิให้มีการเปลี่ยนแปลงแก้ไขโปรแกรม โดยมิได้รับอนุญาต และรวมถึงการควบคุมเพื่อรักษาความปลอดภัยของโปรแกรม ทั้งในขณะที่อยู่ระหว่างการประมวลผล และขณะที่เก็บรักษาไว้ในห้องสมุดโปรแกรม (Library)

2.4.3 การควบคุมการปฏิบัติงานกับคอมพิวเตอร์ (Computer Operations Controls)

หมายถึง การควบคุมให้มีการประมวลผลเป็นไปตามขั้นตอนการทำงานของโปรแกรมโดยไม่ผิดเพี้ยน และการควบคุมการใช้งาน (set up and run) โปรแกรมและแฟ้มข้อมูลให้เป็นไปตามข้อปฏิบัติที่กำหนดไว้

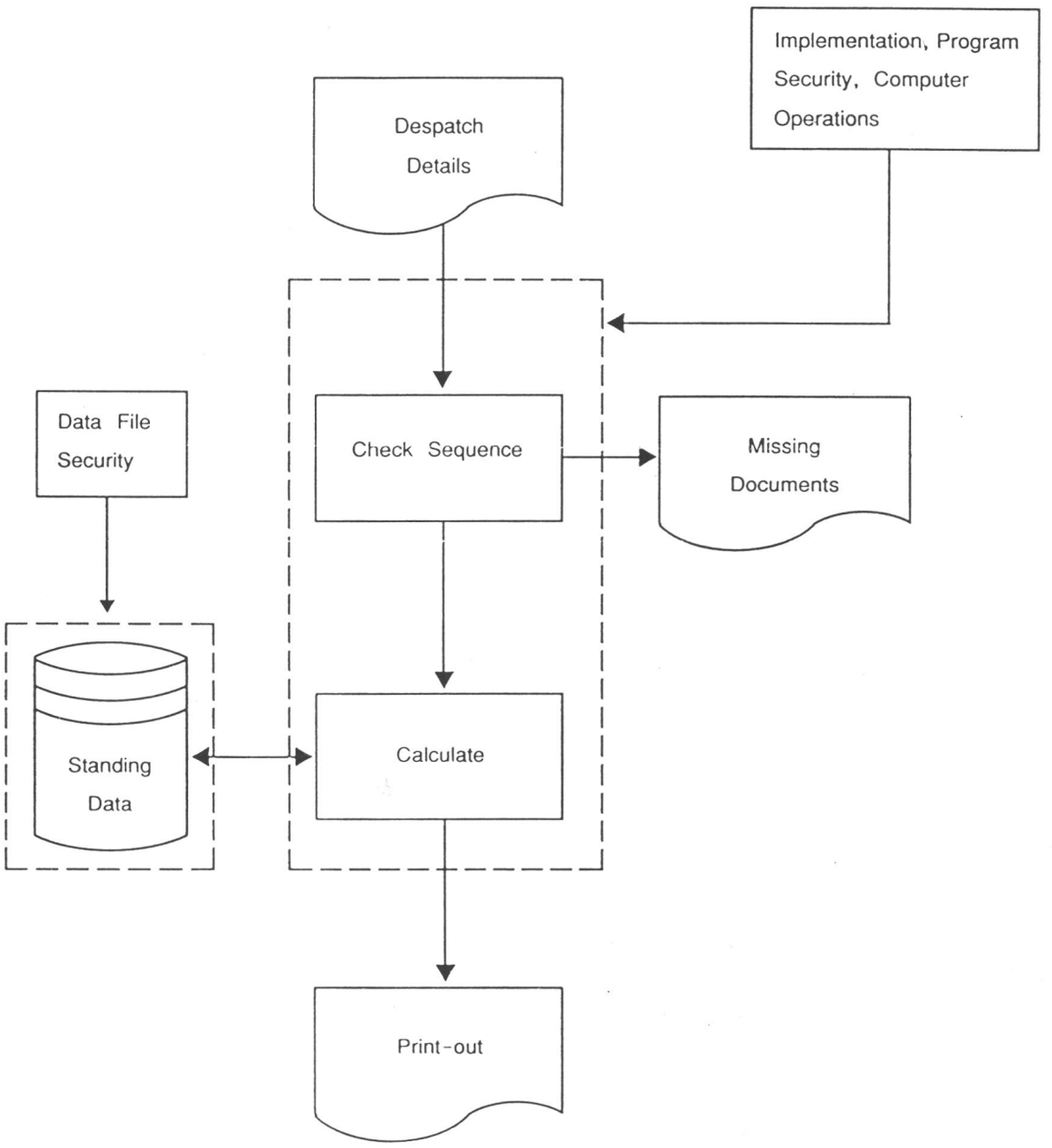
2.4.4 การควบคุมความปลอดภัยของแฟ้มข้อมูล (Data File Security Controls)

หมายถึง การควบคุมเพื่อป้องกันมิให้มีการเปลี่ยนแปลงแก้ไขแฟ้มข้อมูลโดยมิได้รับอนุญาต และรวมถึงการควบคุมเพื่อรักษาแฟ้มข้อมูลทั้งในขณะที่อยู่ระหว่างการประมวลผล โดยเฉพาะอย่างยิ่งป้องกันการแทรกแซงโดยมิได้รับอนุญาตจากสถานีข้อมูลที่อยู่ห่างไกล และในขณะที่เก็บรักษาไว้ในห้องสมุดแฟ้มข้อมูล

การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ เป็นการควบคุมที่ผสมผสานกัน 2 วิธี คือ การควบคุมด้วยบุคคล (Manual Controls) และการควบคุมโดยใช้โปรแกรมของระบบ (System Software) โปรแกรมของระบบในที่นี้หมายถึง โปรแกรมที่ใช้ในการปฏิบัติการ (Operating System) มิใช่โปรแกรมที่ใช้ในการประมวลข้อมูลทางการบัญชี ผู้ตรวจสอบสามารถจะอาศัยและให้ความเชื่อถือต่อโปรแกรมของระบบเพื่อประโยชน์ในการตรวจสอบได้ แต่ทั้งนี้จะต้องพิจารณาวิธีการเก็บรักษาและควบคุมโปรแกรมของระบบให้รอบคอบด้วย

โดยทั่วไปการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ จะเป็นอย่างเดียวกันหรือใช้กับทุกระบบงานที่พัฒนาและประมวลผล ณ ศูนย์คอมพิวเตอร์เดียวกัน

แผนภาพที่ 18.3 แสดงให้เห็นตัวอย่างการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ การควบคุมการปฏิบัติการกับคอมพิวเตอร์ และการรักษาความปลอดภัยโปรแกรม จะให้ความคุ้มครองขั้นตอนการปฏิบัติงานของโปรแกรม (Programmed Procedures) อันได้แก่ การตรวจสอบลำดับและการคำนวณ ส่วนการควบคุมความปลอดภัยของแฟ้มข้อมูลจะคุ้มครองแฟ้มข้อมูลที่เป็นข้อมูลถาวร (Standing Data)



แผนภาพที่ 18.3 Integrity Controls

2.5 กฎเกณฑ์การควบคุม (Disciplines)

กฎเกณฑ์สำหรับการควบคุมในระบบคอมพิวเตอร์ไม่แตกต่างไปจากระบบที่มิได้ใช้คอมพิวเตอร์ ทั้งนี้ได้แบ่งหลักการสำคัญเป็น 3 ข้อ ดังนี้

2.5.1 การกำกับ (Supervisory Controls)

หมายถึง การกำกับควบคุมดูแลให้มีการปฏิบัติตามการควบคุมพื้นฐาน (Basic Controls) อย่างสม่ำเสมอ ได้แก่ การให้มีเจ้าหน้าที่ผู้รับผิดชอบคอยตรวจสอบข้อมูลที่คอมพิวเตอร์รายงานว่าผิดพลาด (Rejection) ทุกครั้ง หรือการทดสอบโปรแกรมและการแก้ไขโปรแกรมจะต้องได้รับการตรวจสอบและอนุมัติจากผู้บริหารศูนย์คอมพิวเตอร์ก่อน เป็นต้น

2.5.2 การแบ่งแยกหน้าที่ (Segregation of Duties)

หมายถึง การจัดหน้าที่การปฏิบัติงานให้สามารถสอบยันซึ่งกันและกันได้ ตัวอย่างเช่น บุคคลผู้มีหน้าที่ควบคุมข้อมูลจะต้องไม่เกี่ยวข้องกับการปฏิบัติงานกับเครื่องคอมพิวเตอร์ หรือบุคคลผู้พัฒนาและทดสอบระบบงานจะต้องไม่เข้าไปเกี่ยวข้องกับการประมวลผลในระบบงานนั้น

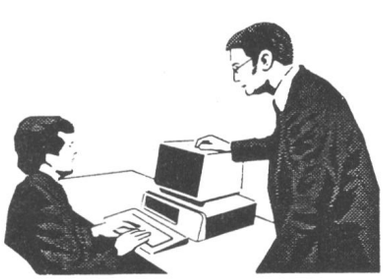
2.5.3 การพิทักษ์ทรัพย์สิน (Custodial Controls)

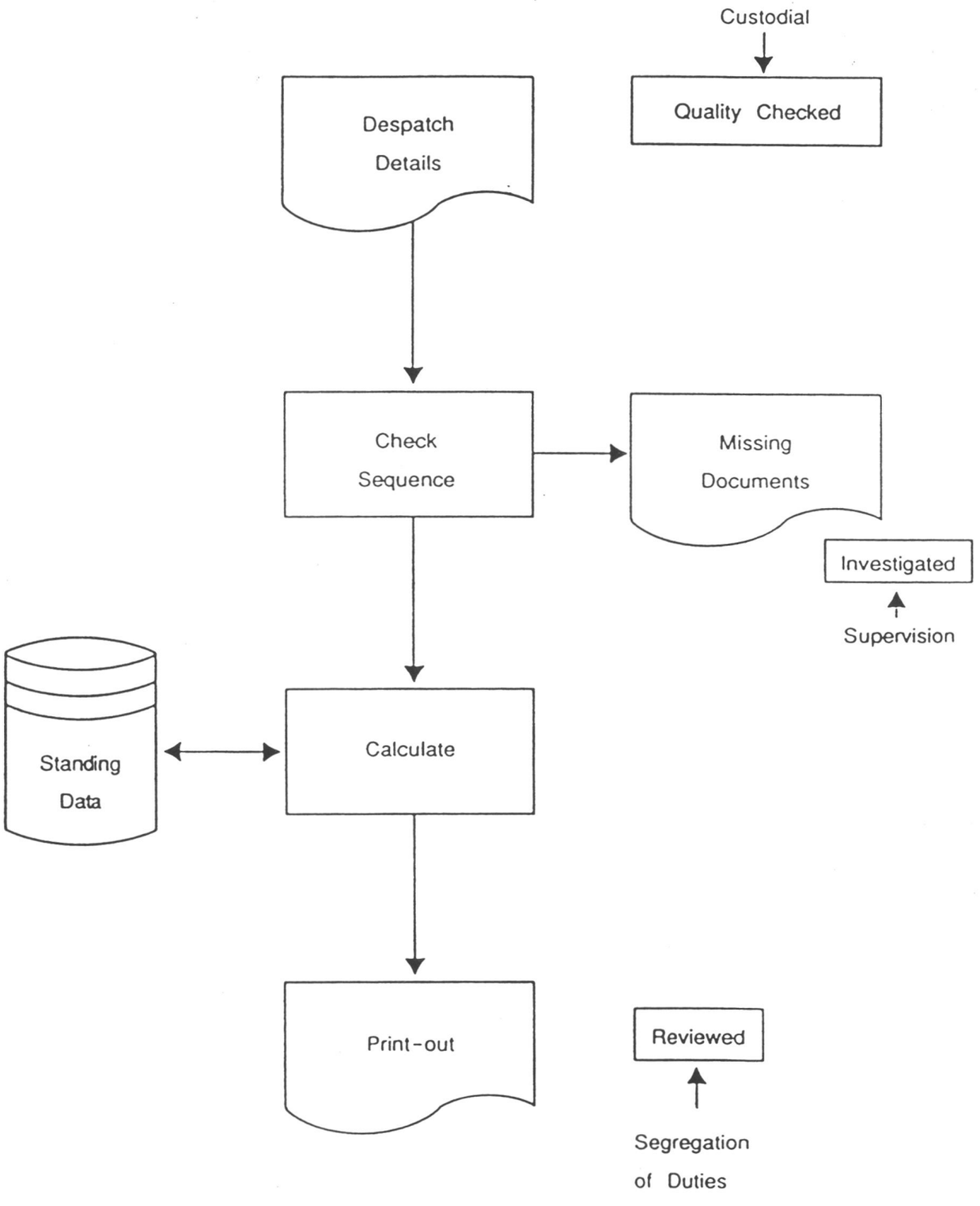
หมายถึง การควบคุมที่เกี่ยวข้องกับทรัพย์สิน ได้แก่ การควบคุมดังนี้

1) แบ่งแยกหน้าที่การบันทึกบัญชีต่างหากจากการเก็บรักษาทรัพย์สิน ตัวอย่างเช่น จัดให้มีการตรวจสอบการเก็บรักษาแฟ้มข้อมูลโดยบุคคลผู้ไม่มีหน้าที่ในการเก็บรักษา เป็นต้น

2) จัดให้มีการควบคุมทางกายภาพเพื่อป้องกันการแทรกแซงการเก็บรักษาทรัพย์สินโดยมิได้รับอนุญาต

แผนภาพที่ 18.4 แสดงให้เห็นตัวอย่างของกฎเกณฑ์การควบคุม โดยเฉพาะทางด้านแผนกผู้ใช้ บุคคลผู้มีหน้าที่ในการตรวจสอบเอกสารขั้นต้น (Quality Checked) จะไม่มีหน้าที่ในการเก็บรักษาทรัพย์สิน หน้าที่ในการตรวจสอบเอกสารที่ผิดพลาดสูญหาย (Missing Documents) เป็นหน้าที่ในการกำกับ (Supervisory Controls) และบุคคลผู้มีหน้าที่ตรวจสอบรายงานจากคอมพิวเตอร์ (Reviewed) จะต้องไม่มีหน้าที่เกี่ยวข้องกับการปฏิบัติการทางคอมพิวเตอร์





แผนภาพที่ 18.4 กฎเกณฑ์การควบคุม

2.6 การเลือกให้ความเชื่อถือต่อระบบการควบคุม

การพิจารณาเลือกให้ความเชื่อถือต่อระบบการควบคุมใด ๆ ก็ตาม ผู้ตรวจสอบจะต้องมีหลักการในการเลือกที่สำคัญคือ ระบบการควบคุมที่จะให้ความเชื่อถือนั้นเป็นระบบการควบคุมที่ประกันความสมบูรณ์ครบถ้วน และความถูกต้องของการบันทึกข้อมูลทางบัญชีได้อย่างมั่นใจ ดังนั้นโดยปกติผู้ตรวจสอบจะต้องเข้าไปเกี่ยวข้องหรือประเมินการควบคุมใน 3 ขอบเขตที่สำคัญ ได้แก่ การควบคุมทางด้านผู้ใช้ (User Controls) ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) และการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls)

ในระบบคอมพิวเตอร์ที่ค่อนข้างง่ายหรือไม่ซับซ้อน ผู้ตรวจสอบอาจไม่จำเป็นต้องเข้าไปประเมินหรือให้ความเชื่อถือต่อการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ ถ้าหากได้ประเมินแล้วว่าการควบคุมเกี่ยวกับขั้นตอนการทำงานของโปรแกรมมีประสิทธิภาพอย่างเพียงพอ อย่างไรก็ตามกรณีเช่นนี้ไม่เกิดขึ้นได้บ่อยครั้งนัก ฉะนั้นผู้ตรวจสอบยังจำเป็นต้องเข้าไปประเมินการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์อยู่นั่นเอง

2.7 ช่วงเวลาที่เหมาะสมในการประเมิน

ช่วงเวลาที่เหมาะสมสำหรับการประเมินผลการควบคุมภายในในระบบคอมพิวเตอร์ ควรจะเป็นช่วงเวลาก่อนหน้าที่ระบบงานใด ๆ จะถูกใช้ปฏิบัติงานจริง ทั้งนี้ก็เพราะ

1) การเปลี่ยนแปลงใด ๆ ในระบบงานคอมพิวเตอร์ภายหลังที่ใช้งานจริง แล้วกระทำได้ยาก ผู้ตรวจสอบควรจะให้คำแนะนำแก้ไขในระหว่างที่ระบบงานอยู่ระหว่างการพัฒนาเพื่อมิให้เกิดปัญหาภายหลัง

2) ผู้ตรวจสอบควรที่จะได้ทราบและทดสอบลักษณะและขอบเขตของขั้นตอนการทำงานของโปรแกรมด้วยตนเอง เพื่อที่จะสามารถวางแผนและกำหนดเทคนิคหรือวิธีการตรวจสอบหลังจากที่ได้ใช้โปรแกรมนั้นปฏิบัติงานจริงแล้วต่อไปได้อย่างเหมาะสม

3) ผู้ตรวจสอบสามารถที่จะกำหนดเพิ่มเติมเข้าไปในระบบงานถึงความต้องการพิเศษที่จำเป็นสำหรับการตรวจสอบ เช่น รายงานบางอย่าง หรือข้อมูลบางประเภท เป็นต้น

อย่างไรก็ตาม ถ้าหากผู้ตรวจสอบไม่สามารถจะเข้าไปในช่วงเวลาก่อนหน้าที่จะใช้ระบบงานจริงได้ ซึ่งเป็นผลให้การแนะนำเพื่อแก้ไขระบบงานกระทำได้ยาก ผู้ตรวจสอบควรพิจารณาทางเลือกอื่นที่เป็นไปได้และเหมาะสมในการให้คำแนะนำ เช่น ให้เพิ่มการควบคุมทางด้านผู้ใช้ซึ่งกระทำด้วยบุคคลให้เข้มงวดยิ่งขึ้น เป็นต้น

3. แบบสอบถามการควบคุมภายใน (The Internal Control Questionnaire)

3.1 ลักษณะของแบบสอบถาม

แบบสอบถามสำหรับการควบคุมภายในควรมีลักษณะดังนี้

1) เป็นแบบสอบถามเพื่อประเมินผลระบบการควบคุม มิใช่เพื่อรวบรวมหรือบันทึกรายละเอียดของระบบงาน ทั้งนี้เพราะรายละเอียดของระบบงานได้ทำการศึกษาและบันทึกไว้เรียบร้อยแล้วก่อนหน้านี้

2) มีลักษณะร่วม คือ สามารถใช้ประเมินผลการควบคุมได้ทั้งในส่วนของการควบคุมขั้นพื้นฐานและกฎเกณฑ์การควบคุม และทั้งในระบบคอมพิวเตอร์ล้วน ๆ ระบบงานที่มิได้ใช้คอมพิวเตอร์และระบบงานกึ่งคอมพิวเตอร์

3) จัดแยกประเภทและเรียงลำดับเรื่องที่จะประเมินผลออกเป็นสัดส่วนอย่างมีระเบียบ

3.2 เป้าหมายของการควบคุม

หลักการสำคัญของการสร้างแบบสอบถามคือ ให้สอดคล้องกับวัตถุประสงค์ของการควบคุมระบบงานแต่ละระบบย่อมมีเป้าหมายของการควบคุมที่แตกต่างกัน ผู้ตรวจสอบจำเป็นที่จะต้องทำความเข้าใจเป้าหมายของการควบคุมของแต่ละระบบงาน รวมทั้งเข้าใจความสัมพันธ์ระหว่างเป้าหมายต่าง ๆ นั้น การควบคุมที่หย่อนยานสำหรับระบบงานหนึ่งอาจส่งผลให้ระบบงานอื่นที่สัมพันธ์กันพลอยไม่น่าเชื่อถือไปด้วย

3.3 การใช้แบบสอบถาม

3.3.1 จำแนกความสำคัญของเป้าหมายในการควบคุม

ในการใช้แบบสอบถาม ก่อนอื่นผู้ตรวจสอบจะต้องพิจารณาความสำคัญของเป้าหมายในการควบคุมแต่ละระบบงาน ในบางกรณีผู้ตรวจสอบอาจไม่จำเป็นต้องประเมินการควบคุมด้านใดด้านหนึ่งหากเข้าข่ายประการใดประการหนึ่งต่อไปนี้

1) การดำเนินกิจกรรมส่วนนั้นไม่มีผลกระทบต่อเป้าหมายของการควบคุมและไม่มีผลอันใดต่อนัยสำคัญของรายงานทางการเงิน

2) แม้ว่าการดำเนินกิจกรรมส่วนนั้นจะมีผลกระทบต่อนัยสำคัญของรายงานทางการเงิน แต่ผู้ตรวจสอบสามารถใช้วิธีการตรวจสอบอย่างอื่นได้ประสิทธิภาพมากกว่าโดยไม่จำเป็นต้องประเมินการควบคุมภายใน เช่น ขยายการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) เป็นต้น

3.3.2 การตอบแบบสอบถาม

1) คำถามทุกคำถามควรให้ได้รับคำตอบอย่างครบถ้วน ซึ่งจะแสดงให้เห็นว่าการควบคุมนั้นมีหรือไม่มี

2) ขณะที่ตอบคำถามควรจะอ้างอิงถึงระบบงานที่ได้ศึกษาและบันทึกไว้

3) คำถามที่ตอบรับว่ามีการควบคุมใช้อยู่ ควรทดสอบข้อเท็จจริงต่อไป

3.3.3 การประเมินคำตอบในแบบสอบถาม

กรณีที่ได้รับคำตอบที่แสดงว่าไม่มีการควบคุมใช้อยู่ ให้พิจารณา ดังนี้

1) ให้พิจารณาว่ามีการควบคุมอย่างอื่นที่ชดเชยกันอยู่หรือไม่ ถ้ามีให้อ้างอิงถึงกัน

2) ถ้าไม่มีการควบคุมที่ชดเชยกันได้ พึงสันนิษฐานไว้ก่อนว่าจุดอ่อนที่เกิดขึ้นจะมีผลกระทบต่อความถูกต้องของระบบงาน และส่งผลต่อการตรวจสอบต่อไป

3.3.4 ขั้นตอนการบันทึกข้อบกพร่องของการควบคุม

1) ถ้าคำตอบที่ได้รับแสดงว่าไม่มีการควบคุมที่สำคัญ ให้บันทึกจุดอ่อนและรายละเอียดของข้อบกพร่องทั้งหมด

2) ถ้าคำตอบที่ได้รับแสดงว่าแม้จะไม่มีการควบคุมที่สำคัญ แต่ก็มีการควบคุมอย่างอื่นที่ชดเชยกันได้ ให้บันทึกด้วยว่าเหตุใดความผิดพลาดที่มีนัยสำคัญจะไม่เกิดขึ้น

3) การบันทึกข้อบกพร่องทั้งหมดที่กระทบกระเทือนถึงข้อมูลถาวร (Standing Data)

4) ควรบันทึกข้อบกพร่องทั้งหมดที่เกี่ยวข้องกับการพัฒนาโปรแกรมการควบคุมและรักษาความปลอดภัยของโปรแกรม และการปฏิบัติการคอมพิวเตอร์

4. สรุป

การประเมินระบบการควบคุมภายในที่มีประสิทธิภาพ ผู้ตรวจสอบจะต้องเข้าใจลักษณะของการควบคุมในระบบคอมพิวเตอร์ นอกเหนือจากการควบคุมด้วยบุคคล (Manual Controls) ซึ่งในที่นี้หมายถึงการควบคุมทางด้านผู้ใช้ (User Controls) แล้ว ยังได้แก่ การควบคุมซึ่งเป็นลักษณะเฉพาะของระบบคอมพิวเตอร์ ได้แก่ ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) และการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ขั้นตอนการทำงานของโปรแกรม หมายถึง ลำดับขั้น (Steps) ในโปรแกรม ซึ่งจะช่วยควบคุมข้อมูลที่ทำการประมวลผลไปด้วย ส่วนการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ หมายถึง กระบวนการควบคุมโปรแกรมและแฟ้มข้อมูล และรวมถึงการควบคุมการพัฒนาและรักษาความปลอดภัยโปรแกรมและแฟ้มข้อมูล ตลอดจนการควบคุมและรักษาความปลอดภัยด้านการปฏิบัติการคอมพิวเตอร์ การควบคุมในแบบต่างๆที่กล่าวมานี้แต่ละประเภทยังประกอบด้วย การควบคุมขั้นพื้นฐาน (Basic Controls) และกฎเกณฑ์การควบคุม (Disciplines) กฎเกณฑ์การควบคุมจะมีลักษณะเช่นเดียวกับระบบที่มิได้ใช้คอมพิวเตอร์ กล่าวคือ แบ่งออกเป็น 3 ชนิด ได้แก่ การกำกับ (Supervisory Controls) การแบ่งแยกหน้าที่ (Segregation of Duties) และการพิทักษ์ทรัพย์สิน (Custodial Controls) กฎเกณฑ์การควบคุมซึ่งปกติจะเป็นการควบคุมด้วยบุคคลนี้ ควรจะมีใช้อยู่ทั้งในแผนกผู้ใช้และในศูนย์คอมพิวเตอร์

เครื่องมือที่ใช้ในการประเมินระบบการควบคุม ได้แก่ แบบสอบถามการควบคุมภายใน ซึ่งผู้ตรวจสอบจะต้องเข้าใจลักษณะการควบคุมและวัตถุประสงค์ของการควบคุมการดำเนินงานแต่ละด้านเสียก่อน จึงจะสามารถสร้างแบบสอบถามที่มีประสิทธิภาพได้



19

การประเมินผลระบบการควบคุม

การควบคุมด้านการปฏิบัติงานและด้านโปรแกรม

1. แนวความคิดเกี่ยวกับการออกแบบระบบการควบคุม (Design Concepts)

1.1 โครงสร้างของการควบคุม (Control Structure)

1.1.1 การควบคุมงานแต่ละอย่าง หมายถึง การควบคุมการปฏิบัติงานทุกขั้นตอน ซึ่งเริ่มตั้งแต่มีรายการทางบัญชีเกิดขึ้น จนกระทั่งถึงขั้นออกรายงานให้ฝ่ายบริหาร หรือรายงานผลลัพธ์อื่น ๆ และในกรณีพิเศษอาจจะรวมถึงการควบคุมการนำส่งรายงานไปจุดหมายปลายทาง และการติดตามผลรายงานที่ผิดปกติ

1.1.2 เนื่องจากมีการนำคอมพิวเตอร์มาใช้ในระบบงานมากขึ้น จึงจำเป็นต้องวางระบบการควบคุมการปฏิบัติงานภายในแผนกคอมพิวเตอร์และยิ่งไปกว่านั้นอาจจะต้องกำหนดการควบคุมไว้ในโปรแกรมคอมพิวเตอร์ด้วย เพื่อให้การปฏิบัติข้อมูลมีประสิทธิภาพและเชื่อถือได้ ดังนั้นจึงควรกำหนดไว้ให้เป็นส่วนหนึ่งของระบบงาน ซึ่งจะขาดเสียมิได้ แทนที่จะเกิดขึ้นโดยการบังคับจากแหล่งภายนอก เช่น ผู้สอบบัญชี

1.1.3 เมื่อออกแบบระบบการควบคุมเรียบร้อยแล้ว จะต้องพิจารณาว่าทำอย่างไรจึงจะบรรลุเป้าหมายที่วางไว้ สิ่งที่ควรคำนึงถึงคือ วิธีการหรือเทคนิคที่ใช้ในการควบคุมมีมาก และแตกต่างกันในแง่ของความยุ่งยากซับซ้อน ประสิทธิผล และค่าใช้จ่าย และอีกประการหนึ่งคือ เราอาจจะละเลยการควบคุมบางจุดไปได้โดยไปกำหนดการควบคุมที่เหมาะสมไว้ในขั้นตอนอื่นของการปฏิบัติข้อมูล ไม่จำเป็นต้องออกแบบไว้ให้ครบทุกจุด ทั้งนี้เพราะระบบการควบคุมที่มีประสิทธิภาพมิได้ขึ้นอยู่กับการควบคุมที่จุดหนึ่งจุดใดโดยเฉพาะ

1.2 มาตรฐานในการกำหนดการควบคุม (Controls and Standard of Accuracy)

ในขณะที่ออกแบบระบบการควบคุม จะต้องแน่ใจว่าไม่ได้ละเลยการควบคุมที่สำคัญ และขณะเดียวกันได้ลดการควบคุมที่ไม่จำเป็น โดยพิจารณาถึงวัตถุประสงค์ที่แท้จริงของการควบคุมแต่ละอย่าง และพิจารณาเปรียบเทียบระหว่างค่าใช้จ่ายในการดำเนินการ กับความเสียหายที่อาจจะเกิดขึ้นหากไม่มีการควบคุมดังกล่าว

1.3 ข้อมูลที่ควรจะควบคุม (Types of data to be controlled)

1.3.1 ข้อมูลถาวร (Standing data) และมักจะใช้เป็นประจำทุกครั้งที่มีการปฏิบัติข้อมูล เช่น เลขที่บัญชี เป็นต้น จะก่อให้เกิดข้อผิดพลาดได้มากกว่าข้อมูลรายวัน (transaction data) เพราะฉะนั้นจึงควรกำหนดมาตรฐานในการควบคุมให้สูงกว่าข้อมูลรายวัน

1.3.2 ข้อมูลที่เป็นจำนวนเงิน เช่น จำนวนเงินที่ลูกค้านำเข้าบัญชีมีความสำคัญมากกว่าข้อมูลที่ใช้สำหรับอ้างอิง เช่น เลขที่ของรายการที่เกิดขึ้นในวันนั้น ฉะนั้นจึงควรกำหนดมาตรฐานในการควบคุมให้สูงกว่าข้อมูลอ้างอิง

2. การควบคุมด้านการปฏิบัติงานและด้านโปรแกรม

หมายถึง การควบคุมและวิธีปฏิบัติที่กำหนดขึ้น เพื่อให้แน่ใจว่าข้อมูลที่ส่งเข้าไปในคอมพิวเตอร์ได้รับการประมวลและบันทึกไว้ในแฟ้มข้อมูลอย่างครบถ้วนและถูกต้อง ซึ่งอาจจะแยกพิจารณาได้ตามหัวข้อต่อไปนี้

- ความครบถ้วนของข้อมูลที่จะนำไปใช้ประมวลผล และการบันทึกข้อมูลที่มีการเปลี่ยนแปลง (Completeness of input and updating)
- ความถูกต้องของข้อมูลที่จะนำไปใช้ประมวลผล และการบันทึกข้อมูลลงในแฟ้มข้อมูล (Accuracy of input and updating)
- ข้อมูลที่คอมพิวเตอร์สร้างขึ้นตามเงื่อนไขเฉพาะที่กำหนดไว้ในโปรแกรม (Computer-generated data)
- การรับรองความถูกต้องของข้อมูลที่ส่งเข้าไปประมวลผล (Validity of data processed)
- การคำนวณ การสรุปผล และการแยกประเภทข้อมูล (Calculation, Summarization and categorization procedures)
- การตรวจตราความถูกต้องของข้อมูลในแฟ้มข้อมูล (Maintenance of data on files)
- การสร้างแฟ้มข้อมูล (File creation)

3. ความครบถ้วนของข้อมูลที่จะนำไปใช้ประมวลผล และการบันทึกข้อมูลที่มีการเปลี่ยนแปลง

หมายถึง การควบคุมให้ข้อมูลรายวันทั้งหมดที่เกิดขึ้นเข้าไปในคอมพิวเตอร์ และบันทึกไว้ในแฟ้มข้อมูลตามที่ต้องการจนครบถ้วน ต่างจากการควบคุมความถูกต้องของข้อมูลที่จะใช้ประมวลผล และการบันทึกข้อมูลที่มีการเปลี่ยนแปลงลงในแฟ้มข้อมูล ซึ่งหมายถึง การควบคุมความถูกต้องของรายละเอียดประกอบข้อมูลแต่ละราย

3.1 การเลือกวิธีการควบคุมหลัก

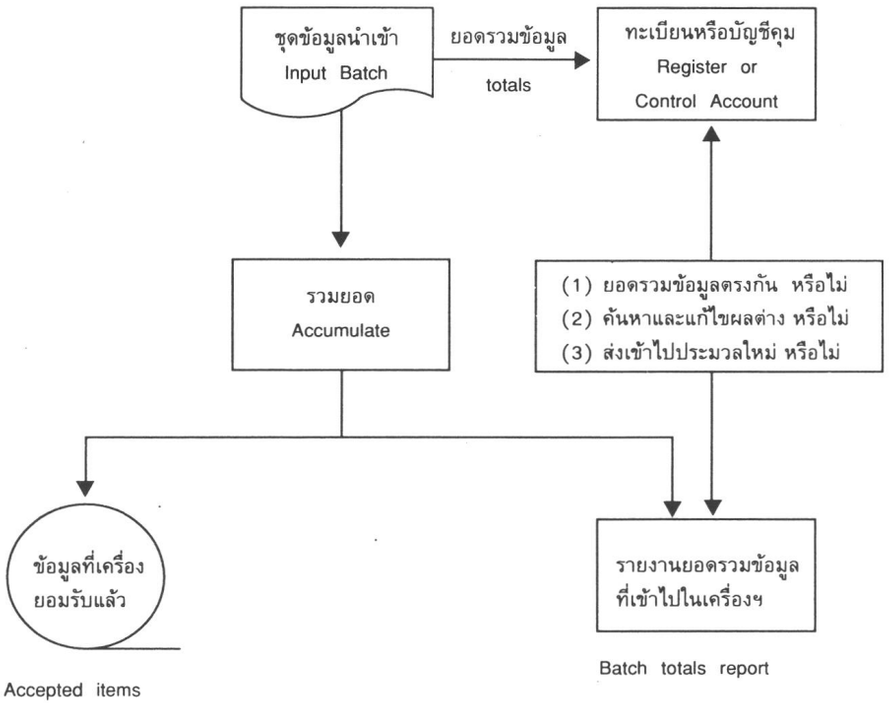
ผู้ตรวจสอบจะพบอยู่เสมอว่า วิธีการควบคุมความครบถ้วนของข้อมูลที่จะนำไปประมวลผลแต่ละประเภทมีมากกว่า 1 วิธี แต่ผู้ตรวจสอบอาจจะเลือกวิธีที่ผู้ตรวจสอบเห็นว่ามีประสิทธิภาพมากที่สุด และสามารถสอบยันความถูกต้องได้โดยตนเองเพียงวิธีเดียวก็ได้ สุดแล้วแต่ความเหมาะสม

3.2 เทคนิคที่ใช้ในการควบคุม

(1) Batch totals

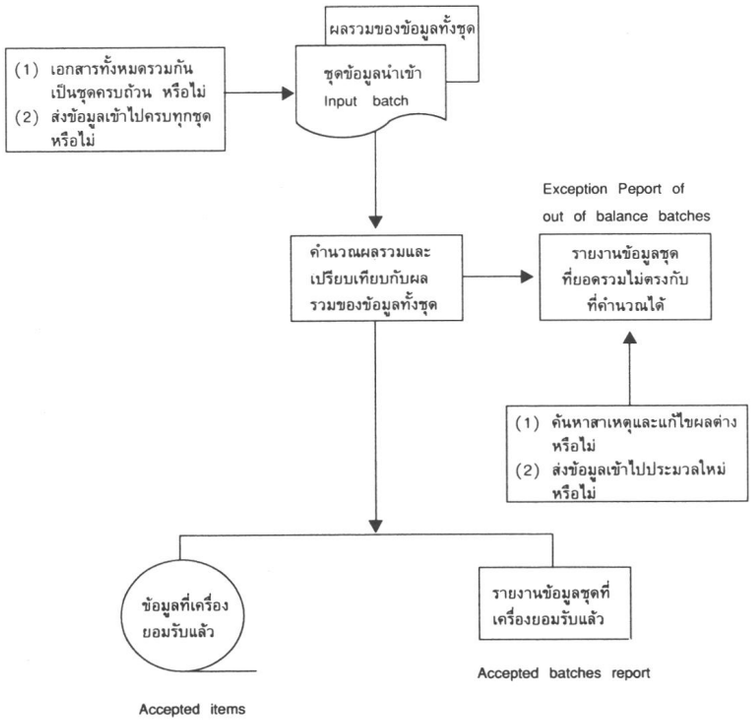
หมายถึง วิธีการควบคุมความครบถ้วนของข้อมูลแบบง่าย ๆ ในระบบการประมวลข้อมูลแบบ Batch ซึ่งมีอยู่ 2 วิธี คือ

(1.1) บวกยอดข้อมูลทั้งชุด (Batch) แล้วบันทึกไว้ในทะเบียน นำข้อมูลทั้งชุดส่งเข้าไปประมวลผลในคอมพิวเตอร์ และให้พิมพ์รายงานผลรวมข้อมูล จากนั้นให้เปรียบเทียบผลรวมข้อมูลในรายงานกับยอดรวมข้อมูลที่บันทึกไว้ในทะเบียน



แผนภาพที่ 19.1 แสดงเทคนิคที่ใช้ในการควบคุมแบบ Batch Total โดยรวมยอดจากทะเบียน

(1.2) บวกยอดของข้อมูลทั้งชุด (Batch) แล้วนำเข้าไปประมวลพร้อมกับคอมพิวเตอร์ จะคำนวณผลรวมของข้อมูลทั้งชุด (Batch total) และเปรียบเทียบผลรวมที่คำนวณได้กับยอดรวมของข้อมูลนำเข้า (Input total) ที่ใส่ไปพร้อมกับข้อมูล จากนั้นคอมพิวเตอร์จะพิมพ์ผลรวมข้อมูลที่คำนวณได้ให้ ไม่ว่าจะเกิดผลต่างหรือไม่ก็ตาม แต่ในกรณีที่เกิดผลต่างคอมพิวเตอร์จะไม่ยอมให้ข้อมูลชุดนั้นผ่านเข้าไปในเครื่องฯ (Rejected)



แผนภาพที่ 19.2 แสดงเทคนิคที่ใช้ในการควบคุมแบบ Batch Total โดยใช้เครื่องควบคุม

การควบคุมความครบถ้วนของข้อมูลที่จะนำไปใช้ประมวลผล และการบันทึกข้อมูลลงในแฟ้มข้อมูลแบบ Batch total โดยการนับจำนวนของเอกสารประกอบข้อมูล (Document count) ปกติ ถือว่าเพียงพอแล้ว แต่ถ้าหากในเอกสารดังกล่าวแต่ละใบมีข้อมูลที่จะต้องนำเข้ามากกว่า 1 รายการ ก็จะต้องใช้จำนวนรายการที่นับได้แทนเอกสาร ในทางปฏิบัติจะนับเฉพาะรายการที่สำคัญ (Important data field) เช่น จำนวนเงินหรือปริมาณ

การใช้วิธีการควบคุมข้อมูลแบบ Batch totals ให้มีประสิทธิภาพมากที่สุด จะต้องมีการควบคุมเพื่อให้แน่ใจว่า

(ก) เอกสารทั้งหมดรวมกันเข้าเป็นชุดครบถ้วน

(ข) ส่งเอกสารทุกชุดเข้าไปปฏิบัติจนครบ

ซึ่งจะทำได้โดยการเช็คสอบลำดับเลขที่ของเอกสารหรือเลขที่ของ Batches

กรณีที่ธนาคารใช้วิธีการควบคุมข้อมูลที่จะนำไปใช้ประมวลผล และมีการบันทึกข้อมูลแบบ Batch ควรสอบถามคำถามดังนี้

1. มีการควบคุมอย่างเหมาะสม เพื่อให้แน่ใจว่า
   (ก) เอกสารหลักฐานประกอบข้อมูลครบถ้วนทุกราย
   (ข) เอกสารหลักฐานทั้งหมดรวมอยู่เป็น Batch
   (ค) Batch ทั้งหมดถูกส่งไปประมวลผลจนครบถ้วน

2. มีการคุมยอดข้อมูลที่จะนำไปใช้ประมวลผลเพื่อความครบถ้วนของข้อมูลโดยวิธีใดวิธีหนึ่งดังนี้ หรือไม่
   (ก) ใช้คอมพิวเตอร์เปรียบเทียบยอดข้อมูลที่ป้อนเข้าสู่ระบบคอมพิวเตอร์กับยอดรวมของข้อมูลแต่ละรายการที่คอมพิวเตอร์ยอมรับ และมีรายงานผลการเปรียบเทียบจากคอมพิวเตอร์ (Print-out) เป็นหลักฐาน หรือไม่
   (ข) ใช้พนักงานเปรียบเทียบยอดข้อมูลที่ป้อนเข้าสู่ระบบคอมพิวเตอร์กับยอดรวมของข้อมูลแต่ละรายการที่คอมพิวเตอร์ยอมรับในรายงานที่คอมพิวเตอร์พิมพ์ออกมา

3. กำหนดวิธีปฏิบัติเกี่ยวกับเรื่องต่อไปนี้ไว้เพียงพอ หรือไม่
   (ก) การค้นหาสาเหตุและการแก้ไขผลต่างที่ได้จากการพิสูจน์ยอดข้อมูลนำเข้า (Input Reconciliations)
   (ข) การส่งข้อมูลชุดที่เครื่องไม่ยอมรับเข้าไปประมวลใหม่

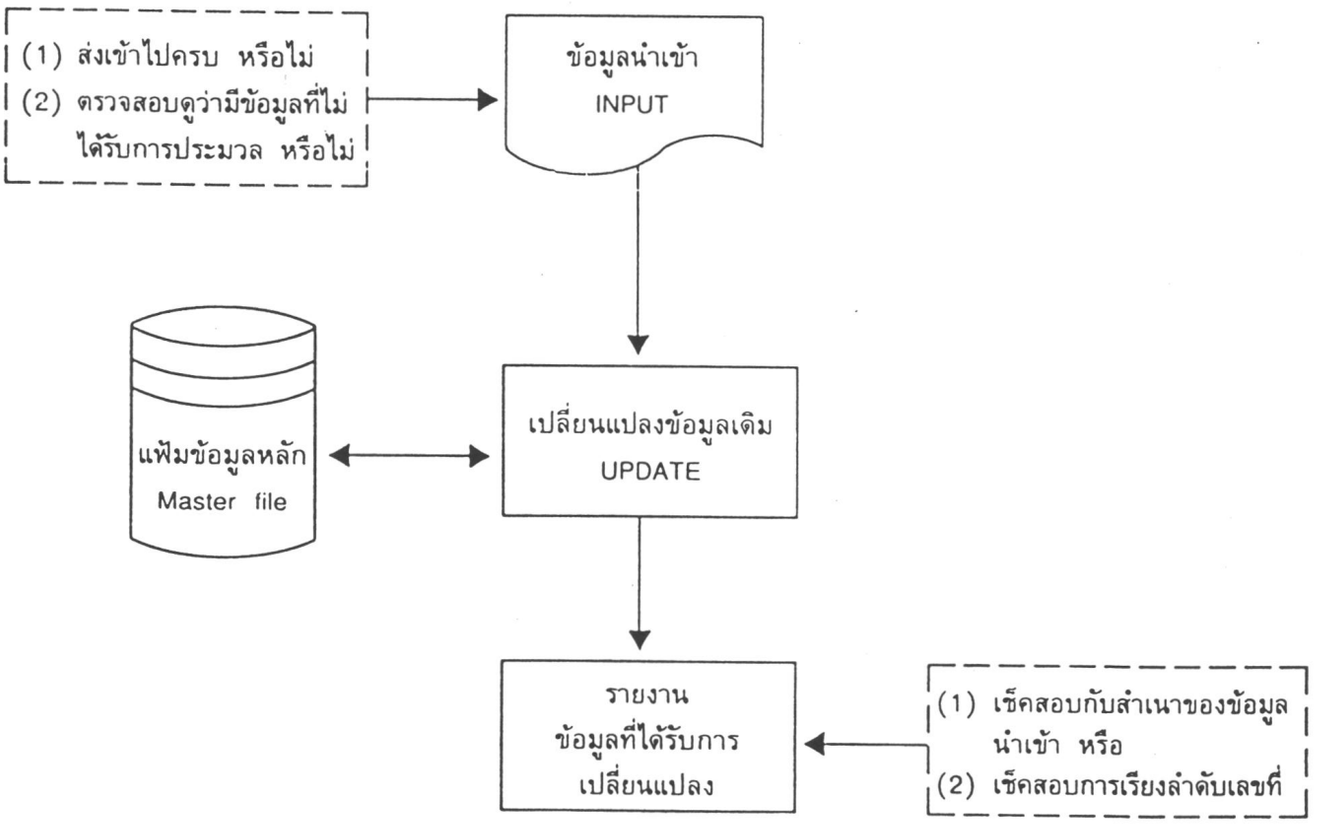
(2) **การเช็คสอบรายงานจากคอมพิวเตอร์** (Checking of print out)

หมายถึง วิธีการควบคุมความครบถ้วนของข้อมูลโดยการเช็คสอบรายงานคอมพิวเตอร์ ซึ่งแสดงรายละเอียดของข้อมูลที่คอมพิวเตอร์ประมวลผล (Listing of items processed by computer) กับเอกสารหลักฐานที่เป็นข้อมูลที่จะใช้ประมวลผล (Input documents) แต่ละราย เพื่อให้แน่ใจว่าได้ส่งเอกสารหลักฐานที่เป็นข้อมูลที่จะใช้ประมวลผลมีความครบถ้วน ซึ่งปกติจะเช็คสอบได้จาก

(ก) สำเนาของเอกสารหลักฐานทั้งหมดที่ส่งไปรับการประมวลผล ซึ่งเก็บไว้ที่แผนกผู้จัดทำเอกสารดังกล่าว (เช็คสอบรายงานคอมพิวเตอร์กับสำเนาของเอกสารหลักฐานที่นำส่ง)

(ข) การเรียงลำดับหมายเลขของเอกสารหลักฐานที่ส่งมารับการประมวลผล หรือการตรวจนับจำนวนเอกสาร (Document counts)

Checking of print out แม้จะเป็นวิธีการควบคุมข้อมูลที่มีประสิทธิภาพ แต่ก็สิ้นเปลืองเวลาและเสียค่าใช้จ่ายสูง ฉะนั้นจึงเหมาะสำหรับใช้ในการควบคุมความครบถ้วนของข้อมูลที่นำเข้าประมวลผล และเปลี่ยนแปลงข้อมูลถาวร (Standing data) และรายการปรับปรุงทางบัญชีที่สำคัญ เช่น การตัดบัญชี การควบคุม วิธีนี้เหมาะสำหรับการประมวลข้อมูลแบบ Batch และ On-line



แผนภาพที่ 19.3 แสดงการเช็คสอบรายงานจากคอมพิวเตอร์

ในกรณีที่ใช้วิธี Checking of print-outs ควบคุมความครบถ้วนของการนำเข้าข้อมูลและเปลี่ยนแปลงข้อมูลเดิม (Update) ควรสอบถามคำถามดังต่อไปนี้

1. มีการควบคุมอย่างเพียงพอ เพื่อให้แน่ใจว่าได้ส่งเอกสารไปรับการประมวลผลครบถ้วน (เช่น การเช็คสอบกับสำเนาเอกสารหลักฐานของแผนกผู้ใช้ข้อมูล การเช็คสอบลำดับเลขที่รายการในรายงานคอมพิวเตอร์) หรือไม่

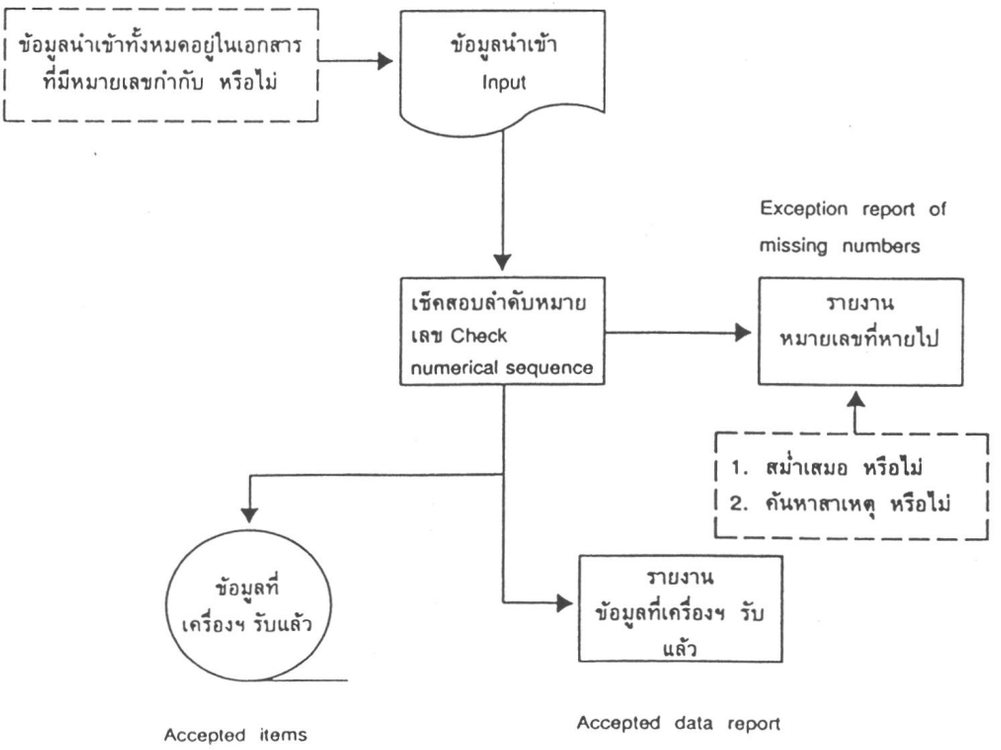
2. มีการเช็คสอบเอกสารเบื้องต้น (Source document) อย่างสม่ำเสมอ (เช่น เดือนละครั้ง) เพื่อดูว่ามีเอกสารใบไหนบ้างที่ไม่ได้ส่งไปรับการประมวลผล หรือไม่

3. โปรแกรมที่ใช้ในการออกแบบรายงานคอมพิวเตอร์ (Print-outs) เหมาะสม เช่น มีรายละเอียดของข้อมูลที่ได้รับการบันทึกไว้ในแฟ้มข้อมูลแล้ว หรือไม่

4. มีวิธีปฏิบัติอย่างเหมาะสมในการค้นหาสาเหตุและแก้ไขผลต่างที่ได้จากการเช็คสอบรายงานหรือไม่

(3) **การเช็คสอบลำดับของหมายเลขข้อมูลนำเข้า**
(Computer Sequence Check)

หมายถึง วิธีการควบคุมความครบถ้วนของข้อมูลโดยใช้คอมพิวเตอร์เช็คสอบลำดับหมายเลขข้อมูลนำเข้า และจัดทำรายงานหมายเลขที่หายไปและซ้ำกัน เพื่อค้นหาสาเหตุต่อไป เหมาะสมสำหรับการประมวลข้อมูลแบบ batch, on-line และ real time



แผนภาพที่ 19.4 แสดงการเช็คสอบลำดับของหมายเลขข้อมูลนำเข้า

เพื่อให้การใช้วิธีนี้มีประสิทธิภาพ ควรจัดให้มีการควบคุมทางด้านการปฏิบัติและด้านโปรแกรม ดังนี้

(3.1) จะต้องกำหนดวิธีปฏิบัติเพื่อควบคุมให้ข้อมูลที่จะนำเข้าทั้งหมดอยู่ในแบบฟอร์มมาตรฐานที่มีหมายเลขกำกับเรียงตามลำดับ (Standard serially numbered form) และควรจะมีการควบคุมการใช้แบบฟอร์มทั้งนี้ก็เพื่อจำกัดหมายเลขแบบฟอร์มชุดที่ใช้อยู่ในขณะใดขณะหนึ่ง

(3.2) โปรแกรมที่ใช้เช็คสอบลำดับหมายเลขต้องเหมาะสม (logically sound) ในการพิจารณาถึงความเหมาะสมควรคำนึงถึงเรื่องต่อไปนี้

(ก) สามารถเช็คสอบข้อมูลชุดซึ่งมิได้เรียงกันตามปกติ (Changes in sequence) โดยการใส่ Parameter cards ระบุหมายเลขชุดที่จะตรวจสอบ หรือสร้าง File ตารางหมายเลขทั้งหมด (Table of all numbers) หรือสั่งให้คอมพิวเตอร์ออกรายงาน Changes in sequences เมื่อตรวจพบว่ามีหมายเลขใดขาดหายไป

(ข) สามารถเช็คสอบลำดับหมายเลขข้อมูลมากกว่า 1 ชุดพร้อมกัน โดยใช้เทคนิคเช่นเดียวกับข้อ (ก)

(ค) กรณีที่ใช้ Parameter card เพื่อระบุหมายเลขแรกและหมายเลขสุดท้ายของชุด จะต้องตรวจสอบได้ว่าหมายเลขอันดับแรกใน Parameter card นั้นเรียงต่อจากหมายเลขสุดท้ายของชุดก่อน

(ง) สามารถตรวจพบและจัดทำรายงานแสดงหมายเลขที่ซ้ำกันทั้งในกรณีที่ใช้ Table of number file และในกรณีที่ใช้ parameter cards ซึ่งในกรณีหลังจะมีข้อจำกัดคือสามารถค้นพบเฉพาะหมายเลขซ้ำที่ปรากฏตาม Parameter เท่านั้น

(3.3) จะต้องจัดทำรายงานหมายเลขข้อมูลที่หายไปและซ้ำกันเป็นประจำ เพื่อให้สามารถติดตามและแก้ไขข้อผิดพลาดได้ทันท่วงที มิฉะนั้นแล้วอาจจะไม่พบข้อผิดพลาดได้

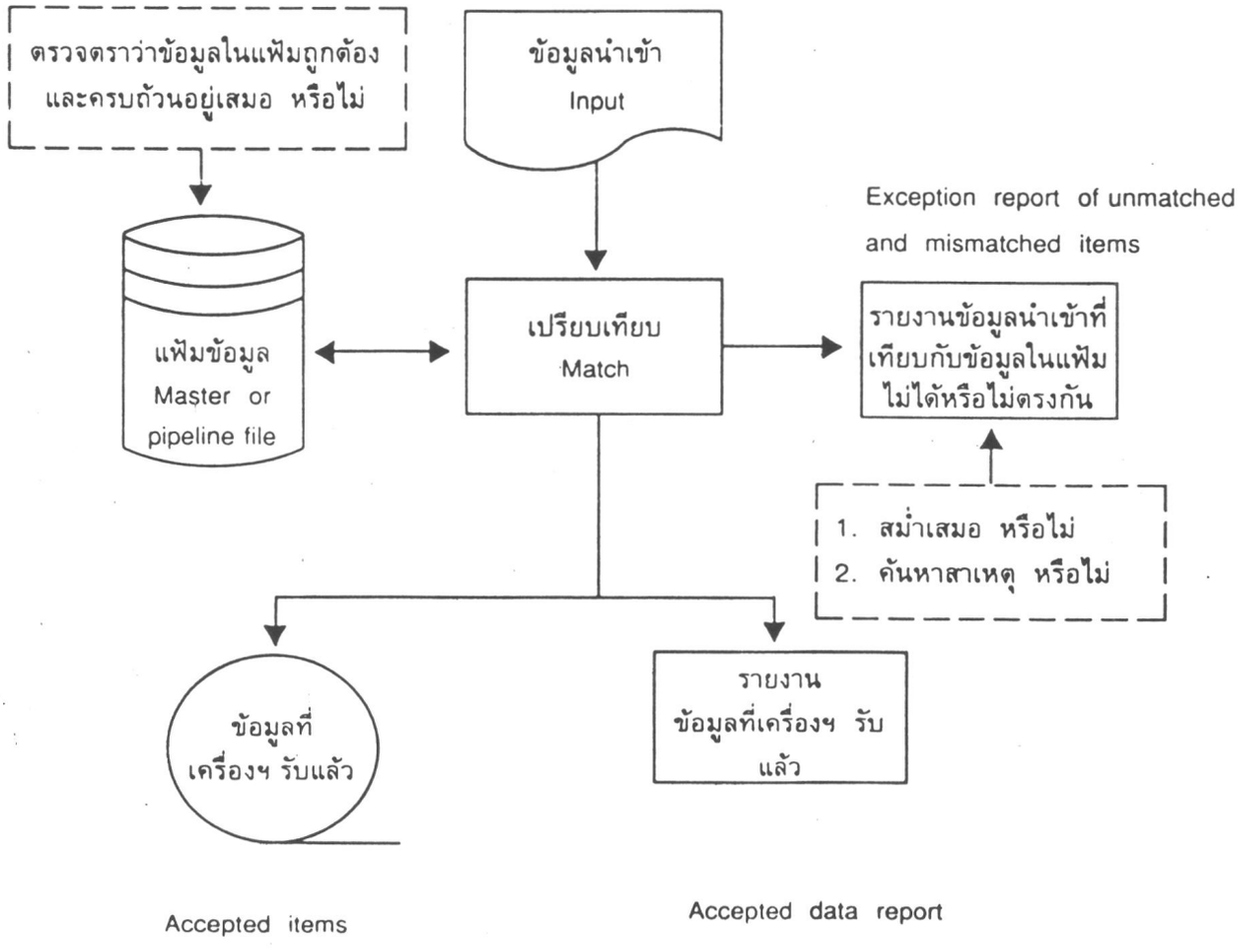
(3.4) จะต้องกำหนดวิธีปฏิบัติในการค้นหาสาเหตุของหมายเลขที่หายไปและซ้ำกัน การควบคุมงานค้นหาสาเหตุของข้อมูลที่หายไป หรือซ้ำกันจะทำได้ง่ายขึ้นถ้าหากมีการจัดทำรายงานแสดงรายการที่ยังคงอยู่ระหว่างการติดตามรวบรวมไว้ (Cumulative List of outstanding items)

เมื่อใช้วิธี Computer sequence check ควบคุมความครบถ้วนของข้อมูลที่จะนำไปประมวลผลและข้อมูลที่มีการเปลี่ยนแปลง (update) ควรสอบถามคำถามเกี่ยวกับการควบคุมดังนี้

1. มีวิธีการเช็คสอบอย่างเพียงพอ เพื่อให้แน่ใจว่าข้อมูลนำเข้าทั้งหมดบันทึกอยู่ในเอกสารที่มีหมายเลขกำกับเรียงตามลำดับ หรือไม่
2. โปรแกรมที่ใช้ในการเช็คสอบลำดับหมายเลขเหมาะสม (สามารถใช้เช็คสอบข้อมูลชุดที่มิได้เรียงตามปกติ และเช็คสอบได้มากกว่า 1 ชุดพร้อมกัน) หรือไม่
3. จัดทำรายงานเอกสารหลักฐานที่หายไปเป็นประจำ (เช่น รายสัปดาห์) หรือไม่
4. วิธีปฏิบัติในการค้นหาสาเหตุเอกสารหลักฐานที่หายไปเหมาะสมหรือไม่

(4) Computer Matching

หมายถึง วิธีควบคุมความครบถ้วนของข้อมูลโดยให้คอมพิวเตอร์เปรียบเทียบ (Matching) ข้อมูลในเอกสารหลักฐานกับข้อมูลที่เก็บอยู่ในแฟ้มข้อมูลในเครื่องคอมพิวเตอร์ (master หรือ pipeline files) ว่ามีลักษณะครบถ้วนตรงกัน หรือไม่ ถ้ามีข้อมูลคู่ใดไม่ตรงกันให้จัดทำรายงาน (outstanding items report) เพื่อค้นหาสาเหตุต่อไป เช่น ให้คอมพิวเตอร์เปรียบเทียบรายละเอียดข้อมูลในการฝาก-ถอนของลูกค้า กับข้อมูลที่เกี่ยวกับตัวลูกค้าที่อยู่ในแฟ้มข้อมูลหลัก (Master File) แล้วค้นหาและจัดทำรายงานแสดงข้อมูลรายการที่ขาดหายไปจับคู่ไม่ได้ และข้อมูลรายที่ซ้ำกัน วิธีการควบคุมความสมบูรณ์ของข้อมูลแบบ Matching นี้เหมาะสำหรับการประมวลผลข้อมูลแบบ on-line และ real-time มากกว่าแบบ Batch เพราะโอกาสที่จะใช้เครื่องคอมพิวเตอร์เทียบข้อมูลนำเข้ากับข้อมูลใน master file มีมากกว่าในระหว่างที่ทำการตรวจสอบข้อมูล (editing)



แผนภาพที่ 19.5 แสดงวิธีการควบคุมความครบถ้วนของข้อมูลโดยใช้คอมพิวเตอร์เปรียบเทียบ

เพื่อให้การใช้วิธีนี้มีประสิทธิภาพ ควรจัดให้มีการควบคุมด้านการปฏิบัติงานและโปรแกรม ดังนี้

(4.1) จะต้องมีการควบคุม file ที่เก็บรายละเอียดข้อมูลที่ใช้เป็นหลักในการเปรียบเทียบกับข้อมูลนำเข้าอย่างเหมาะสม ซึ่งปกติได้แก่ การทดสอบความถูกต้องของยอดรวมข้อมูลใน file กับยอดรวมในบัญชีคุม (control account) อย่างสม่ำเสมอ

(4.2) การปรับปรุงข้อมูลทุกรายการใน file จะต้องมีการขออนุมัติตามความเหมาะสม

(4.3) โปรแกรมที่ใช้สำหรับ matching ต้องเหมาะสม (logically sound) และโดยทั่วไปควรจะเปรียบเทียบข้อมูลแต่ละรายการได้มากกว่า 1 field เช่น สามารถเปรียบเทียบเลขที่บัญชีและเลขที่เช็คของลูกค้าได้

(4.4) จะต้องมีการปฏิบัติที่เหมาะสมเกี่ยวกับการติดตามรายการค้าง และรายการที่จับคู่ไม่ได้ และควรจัดทำรายงานที่แสดงรายละเอียดรายการคงค้างรวบรวมไว้ทุกรายการ (cumulative list of outstanding items)

เมื่อจะใช้ Computer matching ควบคุมการนำเข้าข้อมูล และเปลี่ยนแปลงข้อมูลเดิม ควรสอบถามคำถามต่อไปนี้

1. มีการควบคุม file ที่ใช้เก็บรายละเอียดของรายการฝาก-ถอนของลูกค้า เพื่อให้แน่ใจว่าข้อมูลใน file ถูกต้องและครบถ้วน การแก้ไขข้อมูลทุกรายการต้องได้รับการอนุมัติหรือไม่
2. โปรแกรมที่ใช้สำหรับเปรียบเทียบข้อมูลเหมาะสม หรือไม่
3. มีการจัดทำรายงานแสดงข้อมูลที่มีปัญหาในการนำเข้าประมวลผลที่ค้างนานเกินสมควร (เช่น เกินกว่า 1 เดือน) เป็นประจำ หรือไม่
4. มีการตรวจสอบข้อมูลที่จับคู่ไม่ได้เป็นประจำ (เช่น ทุกเดือน) เพื่อหาสาเหตุของรายการที่ค้างนานเกินเวลาสมควร หรือไม่

(5) Updating

ในบางกรณีการควบคุมความครบถ้วนของข้อมูลนำเข้าก็จะรวมถึงการควบคุมความครบถ้วนของการ Update ด้วย โดยเฉพาะในระบบการประมวลข้อมูลแบบ Batch จะมีการควบคุมข้อมูลนำเข้าแบบ checking of print-outs และ batch totals เพื่อเช็คสอบรายละเอียดและยอดรวมของข้อมูลนำเข้าทั้งหมดที่ปรากฏในรายงานคอมพิวเตอร์ที่จัดทำขึ้นหลังจากมีการ update ข้อมูลเข้าไปไว้ใน file แล้ว ข้อมูลเหล่านี้จะไม่มีการแปลงสภาพก่อนที่จะนำไปทำการ update นั่นคือ ข้อมูลที่จะนำไป update ต้องมีสภาพเหมือนกับข้อมูลนำเข้า หากมีการแปลงสภาพข้อมูลก่อน เช่น มีการคำนวณ ก็ควรกำหนดให้มีการควบคุมเป็นพิเศษ

ในระบบประมวลข้อมูลแบบ Batch การควบคุมพิเศษเกี่ยวกับการ update โดยทั่วไปหมายถึงวิธีการควบคุมทางด้านโปรแกรม ดังต่อไปนี้

ก. ในระหว่างที่คอมพิวเตอร์ทำการเช็คสอบลำดับของข้อมูลหรือเปรียบเทียบข้อมูล (matching) หรือควบคุมข้อมูลนำเข้าในลักษณะอื่น ๆ ควรจะสะสมยอดรวมของข้อมูลที่ผ่านการตรวจสอบความถูกต้องแล้ว (control total of accepted items) และบันทึกยอดรวมทั้งสิ้นไว้ใน file ส่วนที่เป็น control record ซึ่งเป็น field ที่สำคัญมากสำหรับใช้ในการตรวจสอบความครบถ้วนของการ update ข้อมูล

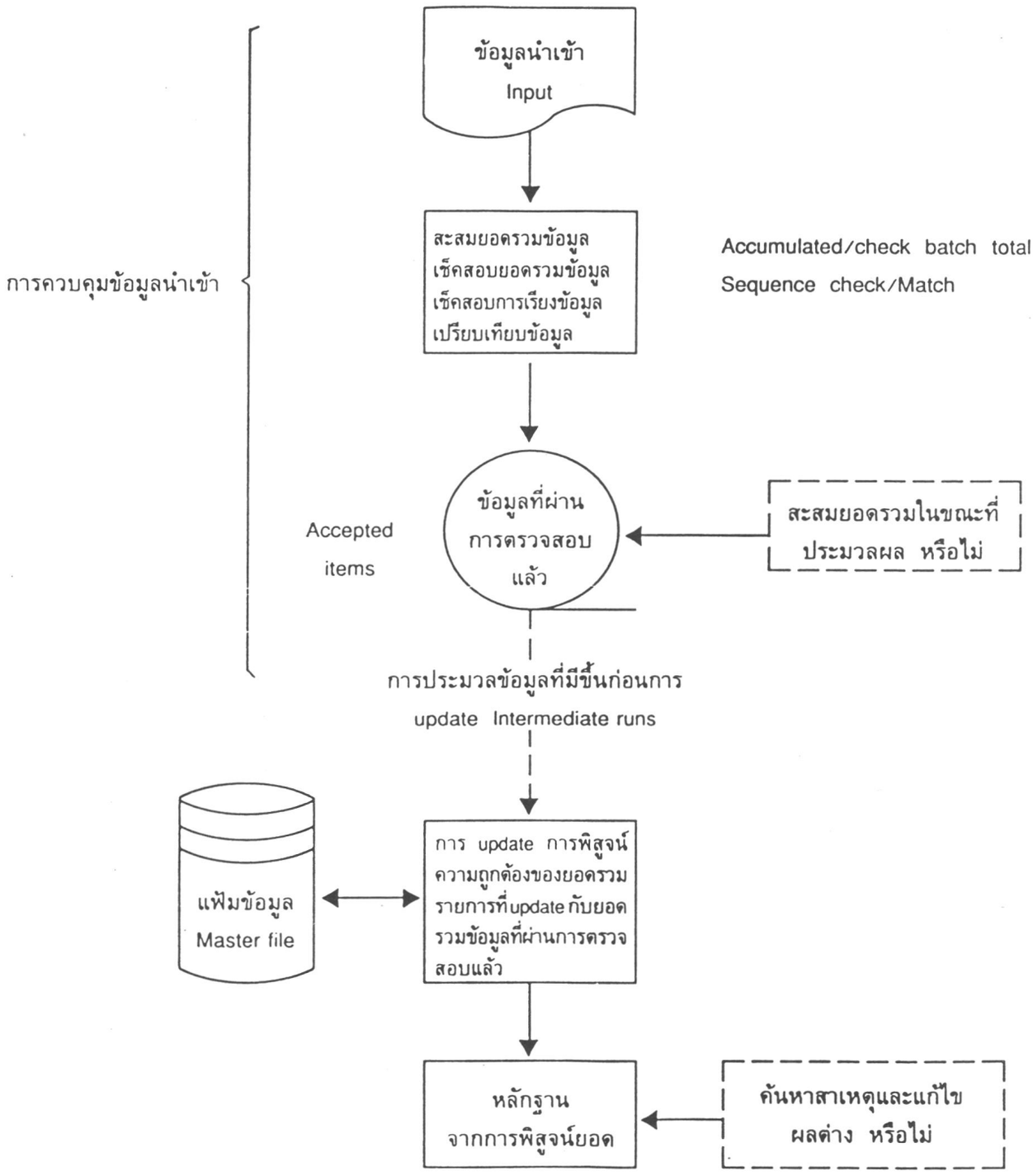
ข. ในระหว่างการประมวลข้อมูลแต่ละขั้นก่อนถึงการ update ผลลัพธ์ใน master file ควรกำหนดให้คอมพิวเตอร์สะสมยอดรวมของข้อมูลขณะที่อ่านเข้าไปแต่ละครั้ง แล้วให้ตรวจสอบผลรวมสะสมของข้อมูลกับผลรวมที่บันทึกไว้ใน control record

ค. เมื่อมีการคำนวณเกิดขึ้น ควรจะควบคุมยอดรวมของข้อมูลผลลัพธ์ที่ได้ใหม่ (new control total for product field) เช่นเดียวกับข้อ ก. และข้อ ข. การสะสมยอดรวมข้อมูลใหม่นี้ควรกระทำในขณะที่คอมพิวเตอร์กำลังทำการประมวลข้อมูลอยู่

ง. เมื่อมีการรวมข้อมูล (summarization) เพื่อสรุปยอดในแต่ละสัปดาห์หรือแต่ละเดือนก่อนจะทำการ update ใน master file ควรจะมีการควบคุมข้อมูลเช่นเดียวกับข้อ ค.

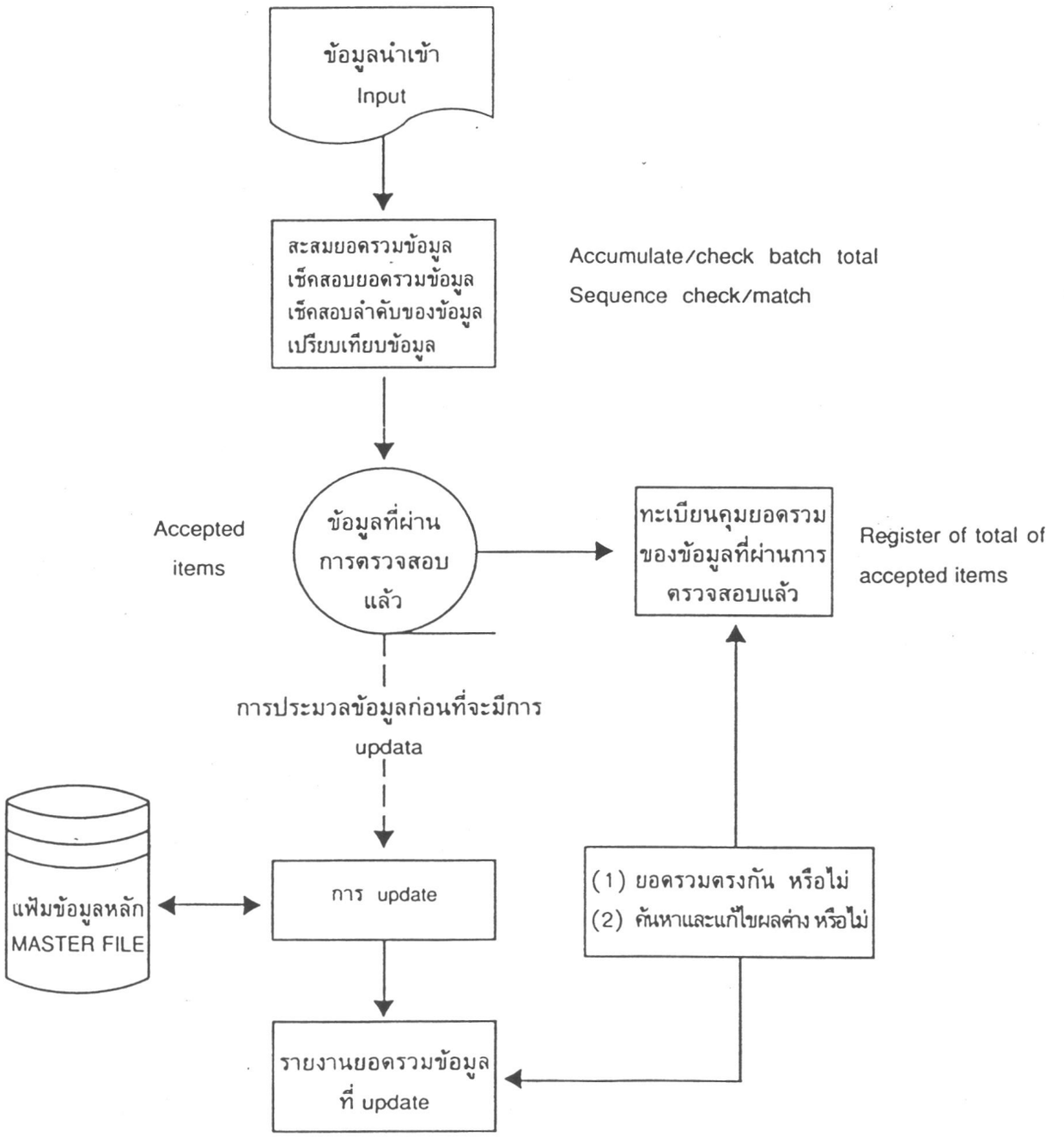
วิธีปฏิบัติที่เหมาะสมก็คือ ให้คอมพิวเตอร์พิมพ์ผลรวมข้อมูลหลังจากการประมวลแต่ละครั้ง ก่อนหน้าที่จะนำผลลัพธ์สุดท้ายไป update ใน master file และให้บุคคลเป็นผู้ตรวจสอบความถูกต้องของยอดรวมนี้ อย่างไรก็ตามเราอาจจะอาศัยคอมพิวเตอร์ทำหน้าที่พิสูจน์ความถูกต้องของยอดรวมข้อมูล (reconciliation) ที่ได้จากการประมวลในแต่ละขั้น (RUN-TO-RUN) โดยไม่จำเป็นต้องให้บุคคลเช็คสอบอีก สิ่งที่สำคัญคือจะต้องให้คอมพิวเตอร์พิมพ์หลักฐานของการพิสูจน์ยอด (evidence of reconciliation) อย่างเหมาะสม ซึ่งโดยปกติก็คือผลรวมข้อมูลที่ใช้ในการพิสูจน์ยอดนั่นเอง





แผนภาพที่ 19.6 แสดงการใช้คอมพิวเตอร์ทำหน้าที่พิสูจน์ความถูกต้องของยอดรวมข้อมูล

เมื่อจะประเมินผลการควบคุมการ update ข้อมูล ผู้ตรวจสอบมักจะสอบถามให้แน่ใจว่าการควบคุมที่มีอยู่นั้นได้รวมการตรวจสอบโดยบุคคล (Manual checking) ไว้ด้วย ทั้งนี้เพราะผู้ตรวจสอบมีความเชื่อมั่นในการควบคุมโดยบุคคลมากกว่า เนื่องจากการตรวจสอบหลักฐานที่ได้จากการปฏิบัติการควบคุมได้ง่ายกว่า ดังนั้นใน Internal control questionnaire จึงมีคำถามว่าการพิสูจน์ความถูกต้องของยอดรวมข้อมูลกระทำโดยบุคคลหรือคอมพิวเตอร์



แผนภาพที่ 19.7 Report of Updated totals

ในระบบ Real time และ On-line ซึ่งการประมวลข้อมูลเป็นแบบเฉพาะรายการมากกว่าจะเป็นการประมวลข้อมูลรวมกันเป็นชุด (batches) ดังนั้นการปฏิบัติข้อมูลแต่ละชนิดจึงต้องใช้โปรแกรมที่แตกต่างกัน ระหว่างที่ทำการประมวลข้อมูลคอมพิวเตอร์จะแยกผลรวมสะสมของข้อมูลแต่ละพวกไว้พอครบช่วงเวลาหนึ่งเช่นสิ้นวัน คอมพิวเตอร์จะปรับ (reorganized) รายการข้อมูลใน master file ให้ถูกต้องใหม่ ซึ่งจำนวนรายการเคลื่อนไหวทั้งหมดนับจากการกระทบยอดครั้งก่อน จะต้องตรงกับผลรวมสะสมของข้อมูลที่เกิดขึ้น

กรณีที่การเก็บข้อมูลเป็นแบบ Data Base การกระทบยอดรวมของรายการที่ update อาจทำได้โดยการตรวจสอบจำนวนข้อมูลที่เพิ่มขึ้น หรือล้างออกจาก Data Base ฉะนั้นในโปรแกรมจะต้องมีส่วนที่แสดงถึงความสัมพันธ์ของข้อมูลแต่ละกลุ่ม เช่น ในการตรวจสอบความถูกต้องของรายการ update ข้อมูลในบัญชีลูกหนี้ อาจจะทำได้โดยการแยกกันตรวจสอบความถูกต้องของจำนวน INVOICES, CREDIT NOTES เงินสด และรายการปรับปรุงต่าง ๆ ควรตรวจสอบความสัมพันธ์ของกลุ่มข้อมูลเหล่านี้เป็นครั้งคราว โดยการตรวจสอบความถูกต้องของข้อมูลแต่ละกลุ่ม

ในแบบสอบถามการควบคุมภายใน นอกจากจะสอบถามเกี่ยวกับความสมบูรณ์ของการ update แล้วยังจะต้องถามต่อถึงความสมบูรณ์ของข้อมูลนำเข้าด้วย

1. มีการกำหนดให้คอมพิวเตอร์สะสมยอดข้อมูลที่ผ่านการตรวจสอบความถูกต้องในขณะที่ทำการตรวจสอบการเรียงลำดับข้อมูล (Sequence check) หรือไม่ และ

   (ก) ยอดรวมของข้อมูลที่ผ่านการตรวจสอบตรงกับยอดรวมของข้อมูลที่นำไป update ในแฟ้มข้อมูล หรือไม่

   (ข) กรณีมีการนำข้อมูลที่ผ่านการตรวจสอบแล้วไปประมวลผลอย่างอื่นก่อน (รวมทั้งการสรุปหรือเปลี่ยนแปลงยอดรวมข้อมูล) ยังสามารถควบคุมให้ข้อมูลเหล่านั้นเข้าไป update แฟ้มข้อมูลครบถ้วนหรือไม่

2. การตรวจสอบความถูกต้องของยอดรวมข้อมูลในข้อ 1. กระทำโดย

   (ก) บุคคล

   (ข) คอมพิวเตอร์ และมีรายงานผลการตรวจสอบ (check printed out) หรือไม่

3. มีวิธีการในการค้นหาและแก้ไขผลต่างที่เกิดขึ้นจากการตรวจสอบความถูกต้องของการ update

ในกรณีที่ใช้วิธีการควบคุม INPUT แบบ Batch control คำถามเกี่ยวกับการ update ในข้อ 1 จะเปลี่ยนแปลงไปเล็กน้อย ดังนี้

ยอดรวมของชุดข้อมูลนำเข้า (input batch totals) ทั้งหมด

(ก) ตรงกับยอดรวมของข้อมูลที่นำไปบันทึกกับแฟ้มข้อมูล หรือไม่

(ข) เมื่อนำข้อมูลนำเข้าทั้งหมดไปประมวลผลอย่างอื่นก่อน (รวมทั้งการสรุปหรือเปลี่ยนแปลงยอดรวมข้อมูล) ยังสามารถควบคุมให้ข้อมูลเหล่านั้นเข้าไป update แฟ้มข้อมูลครบถ้วน หรือไม่

ทั้งนี้ก็เพื่อให้แน่ใจว่าได้ใช้ยอดรวมของข้อมูลนำเข้าเป็นตัวควบคุมการ input และการ update

(6) Rejections

ข้อมูลที่นำเข้าไปในคอมพิวเตอร์มักจะรวมข้อมูลที่ไม่ถูกต้องไว้ด้วย และเมื่อมีรายการที่ผิดพลาดเกิดขึ้นในระหว่างทำการประมวลข้อมูลอยู่ ก็ยากที่จะค้นหาและแก้ไขข้อผิดพลาดนั้น ปกติจะสามารถค้นพบรายการที่ผิดพลาดในระหว่างที่ทำการตรวจสอบความถูกต้องของข้อมูลนำเข้า และในระหว่างที่ทำการ update หากข้อมูลที่เตรียมไว้ไม่ตรงกับข้อมูลที่เก็บไว้ใน master file เมื่อค้นพบข้อมูลที่ผิดพลาดแล้วอาจจะยกเลิกข้อมูลนั้นไป หรือโอนไปพักไว้ในแฟ้มข้อมูลชั่วคราว (Suspense file)

ควรกำหนดวิธีการในการค้นหาสาเหตุ แก้ไข และส่งข้อมูลที่ยกเลิกหรือที่พักไว้ในแฟ้มชั่วคราวเข้าไปในคอมพิวเตอร์ใหม่ และจำเป็นต้องปรับปรุงยอดคุมข้อมูล (control totals) ก่อนหน้านั้น

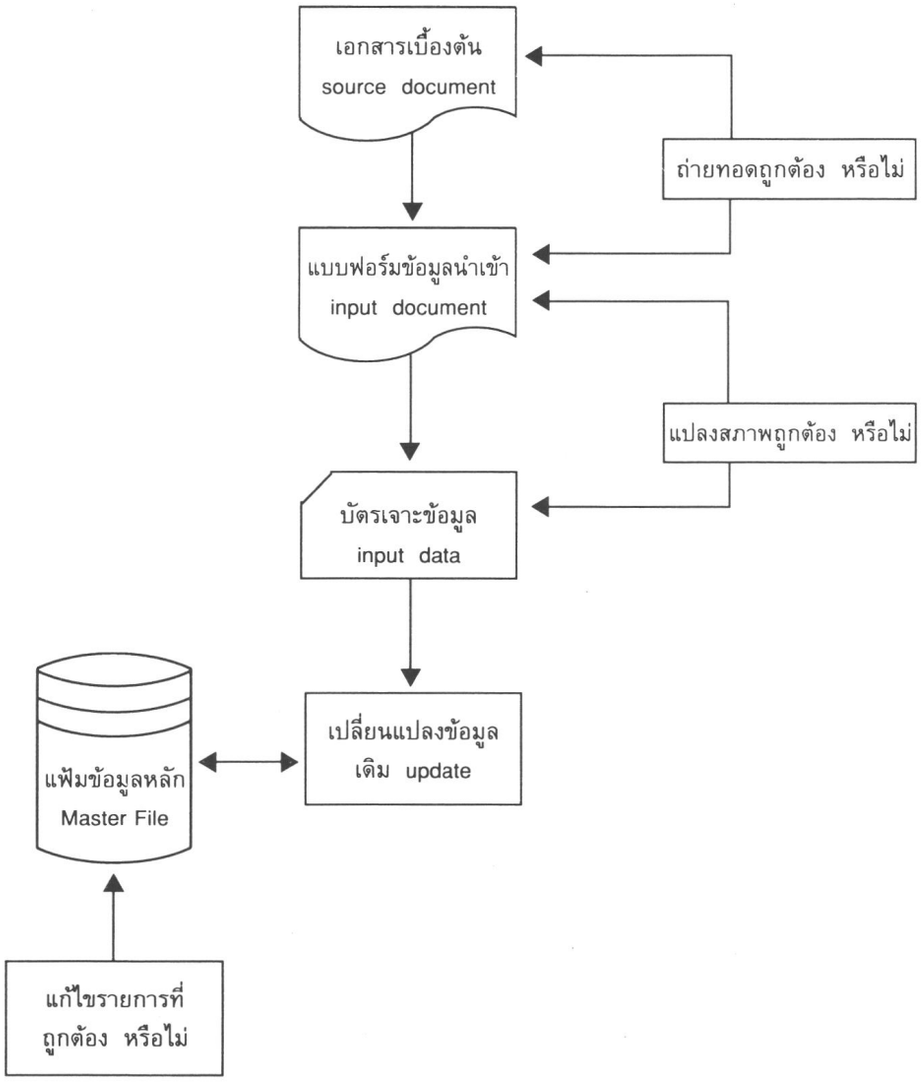
การแก้ไขข้อมูลที่ไม่ถูกต้องโดยเร่งด่วน เป็นสิ่งจำเป็นสำหรับการประมวลข้อมูลแบบ on-line เพราะมีการเปรียบเทียบข้อมูลนำเข้ากับข้อมูลที่อยู่ใน master file ตลอดเวลา ฉะนั้นหากยังคงรายการที่ผิดพลาดไว้ข้อมูลใน master file ก็จะไม่ตรงกับปัจจุบัน (up-to-date) เมื่อมีข้อมูลรายการต่อ ๆ ไปเข้ามาก็จะใช้เช็คสอบความถูกต้องไม่ได้ เช่น การเปรียบเทียบยอดเงินที่ถอนกับยอดคงเหลือในบัญชีเงินเกินบัญชีของลูกค้า ซึ่งเป็นเรื่องที่สำคัญมาก การแก้ไขข้อมูลที่ผิดพลาดโดยเร่งด่วน เป็นสิ่งที่สำคัญมากสำหรับการเก็บข้อมูลแบบ Data Base เพราะมีผู้ใช้ข้อมูลร่วมกันมาก และอาจจะไม่มีใครรู้ว่ามีรายการผิดพลาดค้างอยู่

ผู้ตรวจสอบโดยทั่วไปมักจะให้ความเชื่อถือวิธีการค้นหาข้อมูลที่ไม่ถูกต้อง ซึ่งใช้หลักของการควบคุมข้อมูลแบบ batch totals ทั้งนี้เพราะหากใช้ checking of print-outs, computer sequence check หรือ computer matching แล้ว ข้อมูลที่ค้นพบก็คือ ข้อมูลที่ไม่ได้นำเข้า ข้อมูลที่หายไป หรือข้อมูลที่เทียบกับข้อมูลใน master file ไม่ได้ ซึ่งก็ไม่ได้หมายความว่าจะเป็นข้อมูลที่ไม่ถูกต้องทั้งหมด นอกจากนั้นวิธีการค้นหาข้อมูลที่ไม่ถูกต้องยังขึ้นอยู่กับว่า การตรวจสอบ batch totals กระทำโดยบุคคลหรือคอมพิวเตอร์ ถ้าตรวจสอบด้วยบุคคล หากมีรายการไม่ถูกต้องและแก้ไขยอดคุมแล้ว จะต้องบันทึกรายการข้อมูลที่ไม่ถูกต้องไว้ในทะเบียนเมื่อได้ปรับปรุงยอดคุม (control totals) แล้ว แต่ถ้าใช้คอมพิวเตอร์ตรวจสอบก็จะไม่มียอดคุมข้อมูล (previously-established total) และหลักฐานในการปรับปรุงข้อมูล ดังนั้นในกรณีเช่นนี้จึงจำเป็นต้องตรวจสอบวิธีปฏิบัติเกี่ยวกับการค้นหาข้อมูลที่ไม่ถูกต้อง

ในแบบสอบถามการควบคุมภายใน คำถามที่เกี่ยวข้องกับ batch totals จะรวมถึงการกำหนดวิธีการในการส่งข้อมูลที่ไม่ถูกต้องเข้าไปประมวลใหม่ด้วย ปกติผู้ตรวจสอบจะให้ความสนใจข้อมูลที่ไม่ถูกต้องซึ่งค้นพบในระหว่างการ update ดังนั้นเมื่อมีคำถามเกี่ยวกับการ update ผู้ตรวจสอบจะพิจารณาถึงวิธีปฏิบัติเกี่ยวกับข้อมูลที่ไม่ถูกต้องด้วย เช่น การกำหนดวิธีการในการค้นหาสาเหตุ และแก้ไขรายการที่ผิดปกติที่พบจากการตรวจสอบความถูกต้องของการ update

4. ความถูกต้องของข้อมูลที่จะนำไปใช้ประมวลผลและการบันทึกข้อมูลลงในแฟ้มข้อมูล

การนำเข้าข้อมูลเริ่มตั้งแต่การถ่ายทอดข้อมูลดิบ (Source data) ไปลงในสลิปแบบฟอร์มข้อมูลนำเข้า (input document) และหลังจากนั้นก็จะแปลงข้อมูลลงในบัตรเจาะให้เป็นภาษาที่เครื่องเข้าใจได้ (machine-readable form) แต่ถ้าเป็นการเจาะ (Key) ข้อมูลเข้าไปในเทปหรือจานแม่เหล็ก (disc) หรืออ่านเข้าไปในคอมพิวเตอร์โดยตรง ก็จะไม่มีขั้นตอนการเจาะข้อมูลลงบัตร ดังนั้นเพื่อให้การนำเข้าและบันทึกข้อมูลเป็นไปอย่างถูกต้อง จึงควรควบคุมข้อมูลใน data fields ที่สำคัญ ๆ ทั้งหมด และควรเน้นการควบคุมที่ขั้นตอนการแปลงสภาพข้อมูล มากกว่าในขณะที่ทำการประมวลข้อมูล เพราะในทันทีที่ข้อมูลเข้าไปในคอมพิวเตอร์แล้ว การทำลายข้อมูลนั้นทิ้งไปไม่ใช่เป็นสิ่งที่ทำได้ง่าย ๆ



แผนภาพที่ 19.8 แสดงความถูกต้องของข้อมูลที่จะนำไปใช้ประมวลผลและการบันทึกข้อมูลลงในแฟ้มข้อมูล

Data fields ที่ต้องการคุม

สิ่งที่สำคัญอันดับแรกสำหรับผู้ตรวจสอบคือ การกำหนด data fields ที่จำเป็นต้องมีการควบคุม และขนาดของการควบคุม เพราะในทางปฏิบัติแล้วไม่สามารถควบคุม data fields ทั้งหมดได้อย่างเต็มที่ การเลือก data fields ที่สมควรมีการควบคุมอย่างเข้มงวดไม่ใช่เป็นเรื่องง่าย เพราะข้อมูลที่สำคัญมีทั้งข้อมูลทางการเงินซึ่งจะต้องนำไปใช้ในการคำนวณจำนวนเงิน เช่น จำนวนชั่วโมง หรือปริมาตร และข้อมูลประกอบที่ใช้ในการอ้างอิง (reference data fields) เช่น เลขที่ วันที่ และสัญลักษณ์

เลขที่อ้างอิง (Reference Number)

เลขที่บัญชีเงินฝากที่ถูกต้องเป็นสิ่งที่สำคัญ เพราะจะทำให้แน่ใจว่าได้ Update ข้อมูลในบัญชีที่ถูกต้องแล้ว หมายเลขรหัสของบัญชีเงินฝากแต่ละประเภทจะเป็นประโยชน์ต่อการคำนวณดอกเบี้ยเงินฝาก

วันที่ (Date)

การบันทึกวันที่อย่างถูกต้องเป็นสิ่งที่สำคัญ เพราะวันที่ซึ่งเป็นข้อมูลถาวร (Standing data) อาจจะใช้ในการกำหนดให้คอมพิวเตอร์ประมวลข้อมูลทางการบัญชีได้ ตัวอย่างเช่น วันที่ที่ใช้ในการคำนวณดอกเบี้ยเงินให้กู้ยืม และเงินฝาก เป็นต้น

สัญลักษณ์ (Indicators)

สัญลักษณ์ คือ ส่วนของข้อมูล (field) ที่จะชี้ให้เห็นว่าควรใช้โปรแกรมอะไรในการปฏิบัติข้อมูลนั้น บ่อยครั้งที่ใช้สัญลักษณ์แทนเครื่องหมายบวกและลบของข้อมูล ดังนั้นหากนำเข้าและบันทึกสัญลักษณ์ผิดพลาดก็จะก่อให้เกิดผลลัพธ์ตรงกันข้ามกับที่ต้องการ ตัวอย่างเช่น ในระบบเงินเดือนและค่าจ้าง ลูกจ้างรายที่เริ่มเข้าทำงานหรือออกจากงาน ควรจะใช้แบบฟอร์มข้อมูลที่เหมือนกัน แต่จะมีสัญลักษณ์เป็นเครื่องชี้ความแตกต่างของสภาพการจ้างงาน สัญลักษณ์ยังมีความสำคัญในแง่ของการควบคุม เช่น หลักทรัพย์ประเภทที่ต้องควบคุมดูแลเป็นพิเศษ เมื่อจะบันทึกข้อมูลเข้าไปเก็บไว้ในคอมพิวเตอร์ ควรจะใส่สัญลักษณ์ไว้ด้วย เพื่อเตือนให้ใช้โปรแกรมตรวจนับยอดคงเหลือให้ถี่ขึ้น

เทคนิคที่ใช้ในการควบคุม (Control Techniques)

ก. ใช้วิธีการควบคุมแบบเดียวกับการนำเข้าและบันทึกให้ครบถ้วน (Use of Completeness Controls)

เทคนิคที่ใช้ในการควบคุมความถูกต้องของการนำเข้า และบันทึกข้อมูลบางอย่าง ก็เหมือนกับการควบคุมข้อมูลให้ครบถ้วน ซึ่งได้แก่ การใช้ Checking of print-outs ตรวจสอบความถูกต้องของข้อมูล ในแต่ละ fields การใช้ batch totals ตรวจสอบจำนวน fields และการใช้ Computer matching ตรวจสอบ ความถูกต้องของ fields

ข. Edit Checks

เทคนิคตามข้อ ก. ยกเว้น Checking of print-outs ไม่สามารถใช้ควบคุมความถูกต้องของ data fields ที่สำคัญ ๆ ทั้งหมดได้ ดังนั้นจะต้องใช้วิธีการทางโปรแกรมช่วยตรวจสอบ data fields ที่เหลือ วิธีการนี้เรียกว่า "edit checks" ซึ่งจะใช้ในระหว่างที่นำข้อมูลเข้าคอมพิวเตอร์ ในขณะที่ออกแบบโปรแกรม (program specification stage) จึงควรพิจารณาถึงจุดที่จะมีการตรวจสอบและขอบเขตของการตรวจสอบ

การตรวจสอบแบบนี้ใช้มากในระบบ on-line และ real time ซึ่งข้อมูลที่นำเข้ามีโอกาสจะ match กับข้อมูลใน master file เป็นจำนวนมาก และยังขยายไปถึงระยะการจัดเก็บข้อมูลแบบ data base อีกด้วย เช่น การนำข้อมูลในใบส่งของ (Sales invoices) ไป match กับยอดขายในอดีตที่ผ่านมาของลูกค้ารายที่ต้องการ

Edit Checks มีหลายแบบ ได้แก่

(1) Format Checks เป็นการตรวจสอบโครงสร้างของข้อมูลที่นำเข้าเพื่อให้แน่ใจว่าทุก fields ประกอบด้วยตัวอักษรหรือตัวเลขถูกต้อง การเช็คสอบวิธีนี้จะเป็นประโยชน์ในด้านการปฏิบัติงานข้อมูล และอาจจะช่วยให้ผู้ตรวจสอบมั่นใจว่าข้อมูลที่นำเข้านั้นมีวันที่และสัญลักษณ์ตามที่ต้องการ

(2) Existence Checks เป็นการตรวจสอบเลขที่อ้างอิง (Reference numbers) ของข้อมูลนำเข้ากับตารางหมายเลขอ้างอิงที่ถูกต้อง (lists of valid numbers) ซึ่งบรรจุไว้ก่อนแล้วในแฟ้มข้อมูลหรือในโปรแกรมประโยชน์ที่จะได้รับจากวิธีนี้คือ ช่วยให้มั่นใจได้ว่าข้อมูลที่นำเข้าใช้รหัสบัญชีที่ถูกต้อง

(3) Check digit verification เป็นเทคนิคการตรวจสอบความถูกต้องของเลขที่บัญชีหรือเลขที่อ้างอิงนั้น ๆ (reference numbers) โดยการใช้โปรแกรมคอมพิวเตอร์ทดสอบความถูกต้องทางด้านคณิตศาสตร์ เพื่อค้นหาหมายเลขบัญชีที่ผิดพลาด

Edit Checks จะช่วยให้ค้นพบข้อผิดพลาดได้อย่างรวดเร็ว ณ จุดเริ่มต้นของขบวนการปฏิบัติข้อมูล (processing cycle) ซึ่งหากไม่ได้ใช้ Edit Checks แต่เริ่มแรกเราก็จะค้นพบว่ามีข้อมูลที่ผิดพลาดเมื่อทำการ update เพราะข้อมูลนั้นมีลักษณะไม่ตรงกับข้อมูลที่เก็บไว้ใน master file ในระบบการปฏิบัติข้อมูลแบบ on-line การตรวจสอบความถูกต้องของเลขที่บัญชีกระทำได้รวดเร็วและมีประสิทธิภาพ โดยการ match ข้อมูลนำเข้าแต่ละรายกับข้อมูลใน master file โดยตรง ดังนั้นการทำ Edit checks แต่เริ่มแรกจึงไม่ค่อยมีความสำคัญนัก

ค. Reasonableness checks และ dependency checks

(1) Reasonableness Checks เป็นการตรวจสอบความเหมาะสมของข้อมูลนำเข้าเมื่อเทียบกับข้อมูลมาตรฐานหรือข้อมูลครั้งก่อน (Standard or previous input) มาตรฐานนี้อาจจะกำหนดไว้ในแฟ้มข้อมูลหรือโปรแกรม ตัวอย่างเช่น ชั่วโมงทำงานและอัตราดอกเบี้ย

ในกรณีที่ไม่สามารถกำหนดมาตรฐานได้ อาจจะใช้ข้อมูลของครั้งก่อน (previous input) เปรียบเทียบกับข้อมูลที่นำเข้า เช่น อัตราแลกเปลี่ยนครั้งหลังสุด เป็นต้น

(2) Dependency Checks เป็นการตรวจสอบความถูกต้องของข้อมูลนำเข้า โดยเช็คสอบว่ามีเนื้อหาสาระของ data fields ที่ต้องการรวมอยู่ในข้อมูลที่นำเข้า หรือไม่ เช่น เงินให้กู้ยืมชนิดผ่อนชำระควรจะมีวันที่เริ่มต้นชำระไว้ด้วย เป็นต้น

ง. การตรวจสอบความถูกต้องของการแปลงสภาพข้อมูลและข้อมูลผลลัพธ์ (Verification of Conversion and Scrutiny of Output)

การตรวจสอบการแปลงสภาพข้อมูลนำเข้าในระบบคอมพิวเตอร์หลาย ๆ แห่งยังคงใช้วิธีการแปลงสภาพข้อมูลซ้ำสองอยู่โดยทั่วไป เช่น การเตรียมข้อมูลแบบเจาะลงบัตร หรือม้วนเทปกระดาษ แต่อย่างไรก็ตามวิธีตรวจสอบแบบนี้เริ่มเป็นที่นิยมน้อยลง เพราะสามารถใช้วิธี Edit checks ได้สะดวกและประหยัดกว่า การตรวจสอบการแปลงสภาพอีกวิธีหนึ่งก็คือ การตรวจสอบข้อมูลผลลัพธ์เพื่อดูว่าการนำเข้าและบันทึกข้อมูลถูกต้องเพียงใด แต่ควรจะใช้วิธีนี้กับข้อมูลที่มีความสำคัญน้อยเท่านั้น เช่น ข้อมูลที่ใช้ในการวิเคราะห์ยอดเงินฝากรายภาค เป็นต้น

การเลือกวิธีการควบคุมที่ดี

ในทางปฏิบัติ ผู้ตรวจสอบจะพบว่าการควบคุมความถูกต้องของการนำเข้าและการบันทึกข้อมูลกระทำรวม ๆ กันหลายวิธี ดังนั้นผู้ตรวจสอบจะต้องตรวจดูว่าวิธีใดที่ดีและไว้ใจได้ โดยทั่วไปผู้ตรวจสอบจะเริ่มตรวจดูว่าวิธีการควบคุมทั้งหมดที่ใช้อยู่มีครบและเรียงตามลำดับตามที่กล่าวมาแล้วข้างต้นหรือไม่ ผู้ตรวจสอบจะเริ่มประเมินผลวิธีการควบคุมการนำเข้าและบันทึกข้อมูลให้ครบถ้วนก่อน เพื่อให้แน่ใจว่าการนำเข้าและบันทึกข้อมูลถูกต้อง แต่การควบคุมวิธีนี้ตามที่กล่าวแล้วไม่สามารถใช้ควบคุมความถูกต้องของ data fields ได้ ผู้ตรวจสอบจึงควรประเมินผลของการควบคุมแบบ edit checks และการควบคุมทางด้านโปรแกรมอื่น ๆ ต่อไป หลังจากนั้นถ้ายังมี data fields ที่สำคัญไม่ได้รับการควบคุมอีก ผู้ตรวจสอบก็จะไปประเมินวิธีการควบคุมแบบ Verification of Conversion ต่อไป แต่อย่างไรก็ตามผู้ตรวจสอบจะต้องนึกอยู่เสมอว่า ไม่มีการควบคุมวิธีใดที่จะสามารถใช้ควบคุมความถูกต้องของ data fields ทั้งหมดได้

เนื่องจากวิธีการควบคุมความถูกต้องของข้อมูลมีหลายวิธี จึงไม่สามารถจะแสดงไว้ในแบบสอบถามการควบคุมภายในทั้งหมดได้ จึงขอยกตัวอย่างแต่เพียงบางส่วนดังนี้

1. มีวิธีการควบคุมความถูกต้องในการนำเข้าและบันทึกข้อมูลใน fields ต่อไปนี้ หรือไม่ (ตัวอย่างวิธีควบคุม เช่น batch totals, edit checks, reporting of non-matched items)

ก. จำนวนเงิน

ข. เลขที่บัญชีของลูกค้า

ค. วันที่

2. มีวิธีการปฏิบัติอย่างเพียงพอหรือไม่ เกี่ยวกับ

ก. การพิสูจน์ยอดรวมข้อมูล (agreement of totals)

ข. การค้นหาและแก้ไขผลต่างและรายการพิเศษ (differences or exceptions)

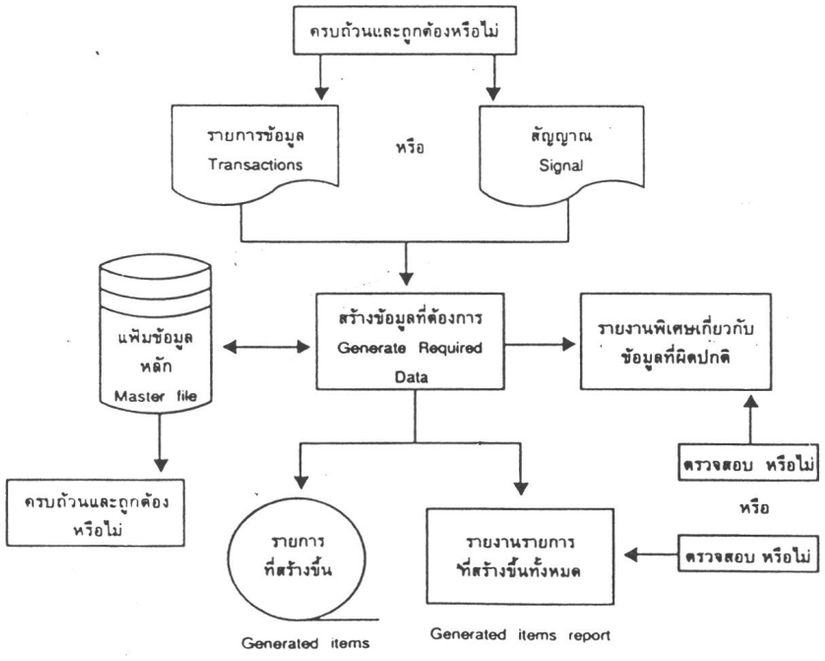
ในกรณีที่เป็นการ update ข้อมูลใน master file จะมีคำถามว่า "โปรแกรมที่ใช้ในการ update บัญชีรายตัวเหมาะสม หรือไม่"

5. Computer-generated data

เราสามารถจะเขียนโปรแกรมสั่งให้คอมพิวเตอร์สร้างข้อมูล (initiated data) ขึ้นมาเองภายใต้เงื่อนไขพิเศษต่อไปนี้

ก. ในการปฏิบัติข้อมูลรายการหนึ่งอาจจะก่อให้เกิดเงื่อนไขที่พิเศษขึ้น เช่น การปฏิบัติข้อมูลรายการเบิกวัสดุคงคลัง ทำให้ยอดวัสดุคงคลังเหลือน้อยกว่าระดับต่ำสุดที่ควรจะมี ดังนั้นจึงต้องจัดทำคำสั่งซื้อวัสดุเพิ่มขึ้น (purchase order) ในกรณีเช่นนี้คอมพิวเตอร์จะทราบและปฏิบัติตามเงื่อนไขได้เมื่อเปรียบเทียบยอดวัสดุคงเหลือกับ standing data ที่เก็บไว้ในเครื่อง เช่น ระดับวัสดุคงคลังต่ำสุด (minimum stock level) การสร้างข้อมูลโดยวิธีนี้เป็นสิ่งธรรมดาที่สุดสำหรับการจัดเก็บข้อมูลแบบ database

ข. การใส่ข้อมูลเข้าไปในคอมพิวเตอร์เพื่อกำหนดเงื่อนไขในการสร้างข้อมูลขึ้น เช่น การใส่วันที่เข้าไปในคอมพิวเตอร์เพื่อให้คำนวณดอกเบี้ยเงินเบิกเกินบัญชี การใส่ข้อมูลเกี่ยวกับขั้นตอนการปฏิบัติงานของคอมพิวเตอร์ การใส่รหัส (requisition code) สั่งให้คอมพิวเตอร์จัดทำรายละเอียดข้อมูลที่ต้องการ เพื่อให้คอมพิวเตอร์สร้างรายการข้อมูลออกมาครบถ้วนและถูกต้อง จำเป็นต้องมีการควบคุมตามที่แสดงไว้ในรูปภาพต่อไปนี้



แผนภาพที่ 19.9 การสร้างข้อมูลอย่างอัตโนมัติโดยคอมพิวเตอร์

(1) ควรจะมีการควบคุมความครบถ้วนและถูกต้องของสัญญาณ (signal) เช่น วันที่หรือขั้นตอนการปฏิบัติข้อมูลที่ต้องกระทำ ซึ่งใช้ในการสร้างข้อมูล

(2) ขั้นตอนในโปรแกรมที่ใช้สร้างข้อมูลจะต้องเหมาะสม

(3) ควรจัดให้มีการควบคุมการแก้ไขและการดูแลรักษา Standing data ที่เก็บไว้ในแฟ้มข้อมูลหรือฐานที่จะใช้ในการสร้างข้อมูล

(4) ควรมอบหมายให้บุคคลตรวจสอบความถูกต้องของข้อมูลที่คอมพิวเตอร์สร้างขึ้น

หลังจากที่คอมพิวเตอร์สร้างข้อมูลขึ้นมาแล้ว ก็จะทำการ update ข้อมูลเหล่านั้นเข้าไปเก็บไว้ในแฟ้มข้อมูล (FILE) ด้วยเหตุนี้จึงจำเป็นต้องจัดให้มีการควบคุมเช่นเดียวกับที่กล่าวมาแล้วในเรื่องการ update ข้อมูล ยอดรวมของข้อมูลที่ update ในแฟ้มข้อมูลจะต้องเท่ากับยอดรวมของข้อมูลที่สะสมไว้ในระหว่างการสร้างข้อมูล

คำถามที่แสดงไว้ข้างล่างนี้จะเป็นประโยชน์ในการประเมินผลการควบคุมการสร้างข้อมูล

1. โปรแกรมที่ใช้ในการสร้างข้อมูลและสะสมยอดรวมข้อมูลที่สร้างขึ้น (Control Record) เหมาะสม หรือไม่ (ตัวอย่างเช่น การนับจำนวนข้อมูลที่สร้างขึ้น)

2. มีการควบคุมความถูกต้องของข้อมูลที่สร้างขึ้น (ตัวอย่างเช่น การตรวจสอบความเหมาะสมและการใช้บุคคลตรวจสอบข้อมูลที่สร้างขึ้น) หรือไม่

3. กำหนดให้เจ้าหน้าที่ผู้มีอำนาจรับผิดชอบเป็นผู้ตรวจสอบความถูกต้องของรายการในแฟ้มข้อมูลซึ่งเกิดจากการที่คอมพิวเตอร์สร้างขึ้น หรือไม่

4. ตรวจสอบยอดรวมข้อมูลที่คอมพิวเตอร์สร้างขึ้นกับยอดรวมของข้อมูลที่เพิ่มขึ้น หรือลดลงในแฟ้มข้อมูล หรือไม่ การตรวจสอบกระทำโดย

4.1) บุคคล

4.2) คอมพิวเตอร์ และมีหลักฐานการตรวจสอบพิมพ์ออกมาจากเครื่อง หรือไม่

5. กำหนดวิธีการค้นหาสาเหตุและแก้ไขผลต่างที่เกิดจากการกระทบยอดข้อมูลที่ update หรือไม่

6. การรับรองความถูกต้องของข้อมูลที่ส่งเข้าไปประมวลผล (Validity of data processed)

ผู้ตรวจสอบจะต้องพิจารณาดูว่ามีการควบคุมทางด้านนี้หรือไม่ ทั้งนี้เพื่อให้แน่ใจว่าข้อมูลที่ส่งเข้าไปประมวลผลทุกรายได้รับการรับรองหรือเช็คสอบ (authorized or checked) แล้ว วิธีการเช็คสอบก็คงคล้าย ๆ กับที่ใช้ในระบบงานซึ่งไม่ใช้คอมพิวเตอร์ เมื่อผู้ตรวจสอบต้องการประเมินผลการควบคุมด้านนี้ ก็ควรจะสอบถามวิธีปฏิบัติเกี่ยวกับการเช็คสอบความเป็นจริงของข้อมูล

ลักษณะที่สำคัญของการรับรองความถูกต้องของข้อมูล มีดังนี้

ก) การรับรอง (authorized) ข้อมูล ควรทำก่อนที่จะนำข้อมูลเข้า (INPUT) คอมพิวเตอร์ ดีกว่าจะทำในตอนที่ได้รับผลลัพธ์ (Accounting output) จากคอมพิวเตอร์แล้ว

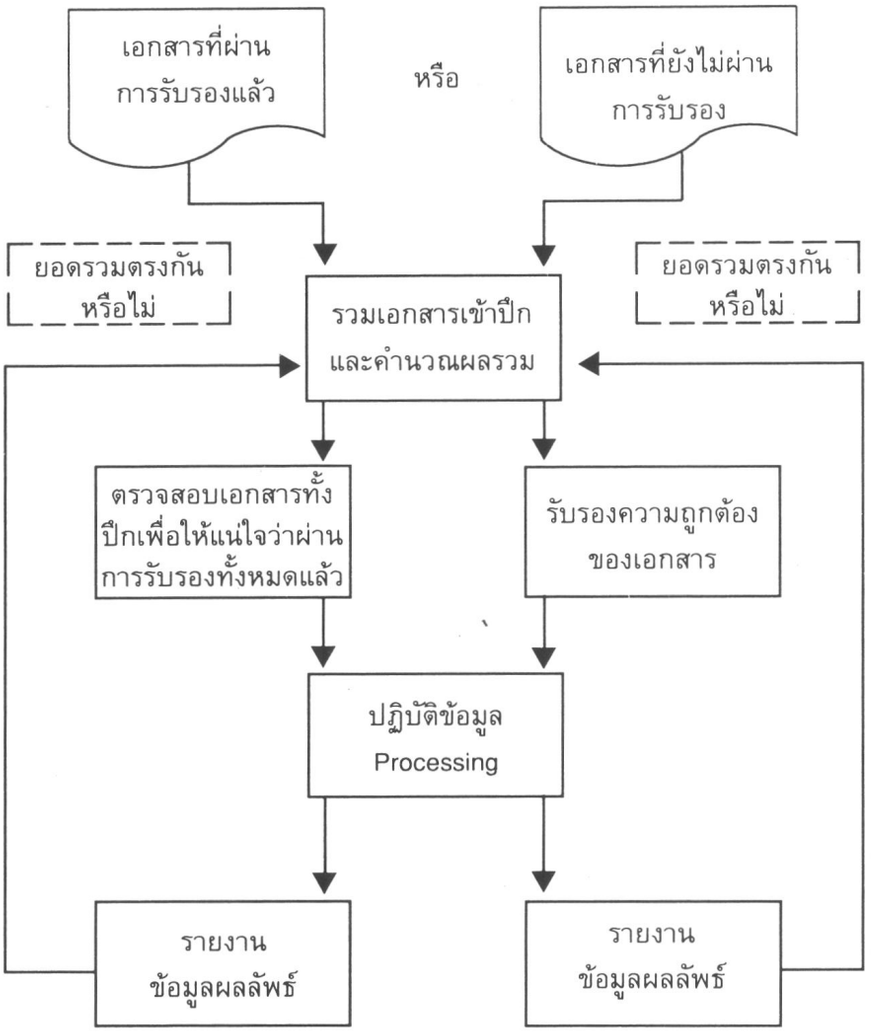
ข) แทนที่จะทำตามแบบข้อ ก. อาจจะกำหนดในโปรแกรมคอมพิวเตอร์ให้ค้นหา และจัดทำรายงานข้อมูลรายที่ต้องการให้บุคคลเช็คสอบความถูกต้อง เช่น จำนวนชั่วโมงล่วงเวลาที่มากเกินกำหนด

ค) ในบางกรณีการใช้โปรแกรมเช็คสอบความถูกต้อง (Validity) ของข้อมูลอย่างเดียวก็เพียงพอแล้ว ไม่จำเป็นต้องใช้บุคคลตรวจสอบอีก เช่น การกระทบ (matching) จำนวนชั่วโมงทำงานของลูกจ้างกับแฟ้มบัญชีลูกจ้าง (employee's master file) และการไม่ยอมรับ (rejecting) ข้อมูลรายที่ซ้ำกัน

การกำหนดเวลาและการรับรองความถูกต้องของข้อมูล (Timing of authorization)

การรับรองความถูกต้องของข้อมูลควรกระทำก่อนหน้าที่จะนำข้อมูลเข้าคอมพิวเตอร์ ดีกว่าที่จะกระทำหลังจากที่ได้รับผลลัพธ์จากคอมพิวเตอร์แล้ว ข้อมูลที่จะต้องผ่านการรับรองมีทั้งข้อมูลถาวร (standing data) และข้อมูลรายครั้ง (Transaction data) เช่น ควรจะรับรองความถูกต้องของอัตราดอกเบี้ยเงินให้กู้ยืม หรือวงเงินเบิกเกินบัญชี เมื่อจะบันทึกเก็บไว้ในแฟ้มข้อมูล หลังจากนั้นก็ไม่ต้องตรวจสอบความถูกต้องของรายการนั้นอีก สิ่งที่สำคัญคือ จะต้องมั่นใจว่าไม่มีการเปลี่ยนแปลงแก้ไขหลังจากผ่านการรับรอง ในบางกรณีเมื่อทำการควบคุมความครบถ้วนและถูกต้องของการนำเข้าและบันทึกข้อมูล จะพบว่ามีข้อมูลที่ไม่ผ่านการรับรอง (unauthorized data) เช่น การเช็คสอบข้อมูลผลลัพธ์ (processed output) กับข้อมูลนำเข้าที่ผ่านการรับรองแล้วรายต่อราย หรือเปรียบเทียบ (match) ข้อมูลนำเข้ากับข้อมูลในแฟ้มที่ผ่านการรับรองแล้ว จึงจำเป็นต้องมีวิธีการของการรับรองความถูกต้องของข้อมูลที่รัดกุมพอสมควร ซึ่งแสดงได้ตามรูป





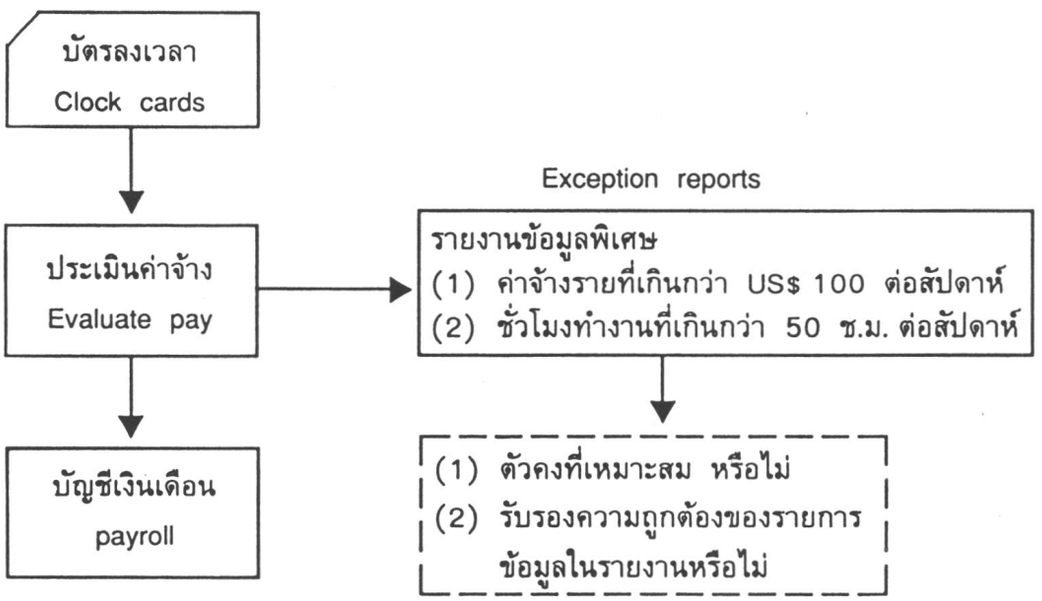
แผนภาพที่ 19.10 แสดงการกำหนดเวลาและการรับรองความถูกต้องของข้อมูล

เพื่อให้เป็นไปตามวัตถุประสงค์ของการควบคุมความถูกต้องของการนำเข้า และบันทึกข้อมูล ควรจะสอบถามดูว่าในกรณีที่การรับรองข้อมูลเกิดขึ้นก่อนการควบคุมความครบถ้วนและถูกต้องของข้อมูลนำเข้า มีการควบคุมอื่นเพียงพอที่จะแน่ใจได้ว่า

(ก) ไม่มีการแก้ไขเปลี่ยนแปลงข้อมูลที่ผ่านมารับรองความถูกต้องแล้วระหว่างการปฏิบัติข้อมูลขั้นต่อไป
(ข) ไม่มีการเติมข้อมูลที่ไม่ผ่านการรับรองเพิ่มเข้าไป
(ค) ไม่ได้ละเลยหรือหลงลืมไม่ใช้ข้อมูลที่ผ่านการรับรองแล้วในการประมวลผล

การเลือกรับรองความถูกต้องข้อมูล (Selective authorization)

การเลือกข้อมูลให้บุคคลรับรองความถูกต้อง ขึ้นอยู่กับการเขียนโปรแกรมสั่งให้คอมพิวเตอร์เลือกข้อมูลโดยการเปรียบเทียบข้อมูลนำเข้ากับตัวคงที่ (constant) ในโปรแกรม เช่น เทียบชั่วโมงทำงานจริงกับมาตรฐาน แล้วให้รายงานชั่วโมงทำงานล่วงเวลาที่เกินไป ตามที่แสดงในรูป



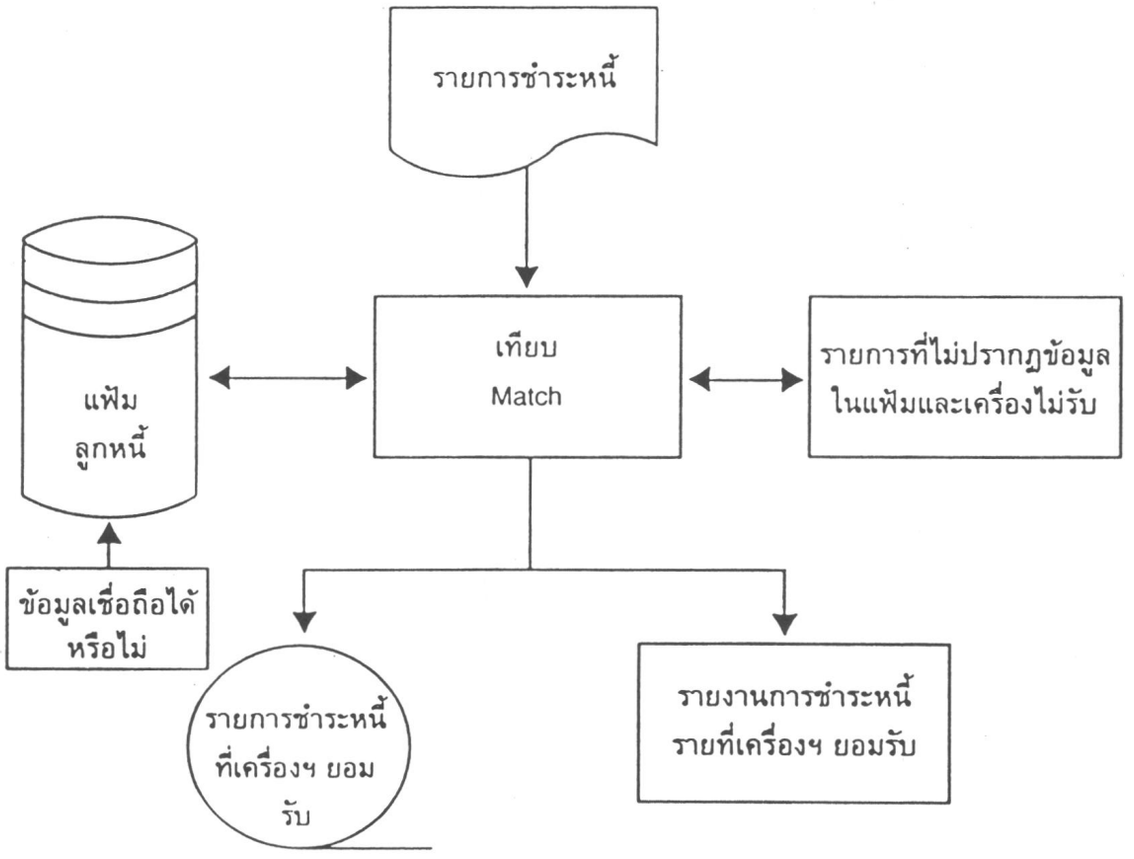
แผนภาพที่ 19.11 แสดงการรับรองความถูกต้องของข้อมูล



การเช็คสอบความถูกต้องของข้อมูลโดยใช้โปรแกรม

(Programmed Checking of Validity)

นอกจากจะใช้คอมพิวเตอร์เลือกข้อมูลแล้ว ยังสามารถใช้ทดสอบความถูกต้องของข้อมูลได้อย่างแม่นยำ โดยการเขียนโปรแกรมสั่งให้เปรียบเทียบข้อมูลนำเข้า (match) กับข้อมูลที่เก็บไว้ใน master file เช่น การเทียบจำนวนชั่วโมงทำงานของพนักงานกับแฟ้มข้อมูลพนักงาน (employee's master file) แล้วไม่รับ (reject) ข้อมูลรายที่ซ้ำกัน เพื่อให้การเช็คสอบนี้มีประสิทธิภาพควรมีการควบคุมข้อมูลในแฟ้มที่ใช้เทียบกับข้อมูลนำเข้า และวิธีการเทียบข้อมูล (matching process) จะต้องเหมาะสม ตามแสดงในภาพ



แผนภาพที่ 19.12 แสดงการเช็คสอบความถูกต้องของข้อมูลโดยใช้โปรแกรม

7. การคำนวณ สรุปผล และแยกประเภทข้อมูล (Calculating, Summarizing and Categorizing)

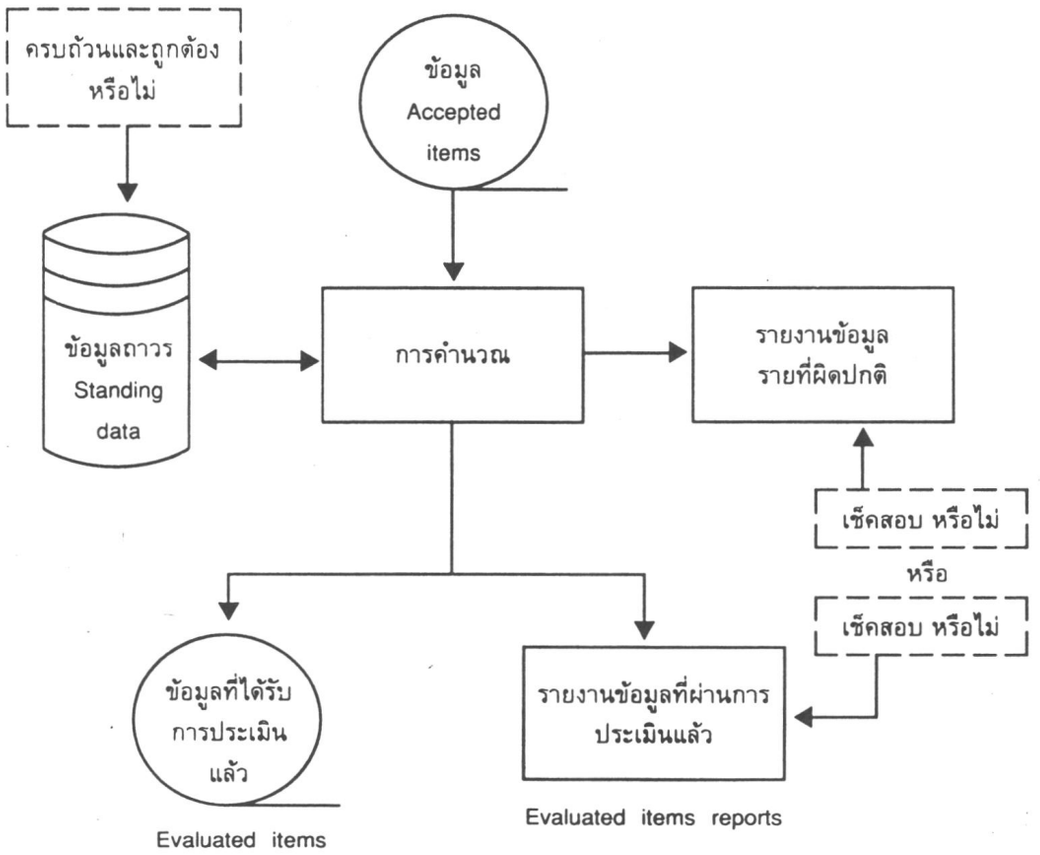
7.1 การคำนวณ

การคำนวณข้อมูลแตกต่างจากการสร้างข้อมูล (computer-generated data) เพราะการคำนวณต้องอาศัยข้อมูลที่นำเข้ามา (Data input) ส่วนการสร้างข้อมูลเกิดจากการกำหนดเงื่อนไขพิเศษ ฉะนั้นจึงต้องมีการควบคุมความถูกต้องของการนำเข้าข้อมูล และเพื่อให้การคำนวณเป็นไปอย่างมีประสิทธิภาพควรกำหนดให้มีสิ่งต่อไปนี้

(ก) ควบคุมการแก้ไขและปรับปรุงข้อมูลถาวร (standing data) ในแฟ้มข้อมูล เช่น อัตราค่าแรง ทั้งนี้ เพราะไม่สามารถเช็คสอบความถูกต้องของข้อมูลประเภทนี้ในเอกสารการลงบัญชี (accounting documents) ดังเช่น ระบบที่ใช้บุคคล (manual system)

(ข) โปรแกรมที่ใช้ในการคำนวณต้องเหมาะสม

(ค) ควรจะมีการเช็คสอบความถูกต้องของการคำนวณ ซึ่งโดยปกติจะใช้บุคคลตรวจสอบรายการผิดปกติ (exceptions) เช่น ค่าจ้างที่สูงเกินไปในรายงานคอมพิวเตอร์ หรือตรวจสอบผลลัพธ์ของการคำนวณ



แผนภาพที่ 19.13 แสดงการคำนวนสรุปผลและแยกประเภทข้อมูล

เพื่อให้เป็นไปตามวัตถุประสงค์ของการควบคุมความถูกต้องของการคำนวณควรจะสอบถามคำถามดังต่อไปนี้ (ตัวอย่างที่ใช้เป็นเรื่องของการคำนวณเงินค่าจ้าง)

ให้ลอกรายละเอียด standing data fields ที่ใช้ในการจัดเตรียมเงินเดือน เช่น อัตราค่าจ้าง การหักเงินเดือน หมายเลขประจำตัวลูกจ้าง อัตรารายได้พิเศษ และแฟ้มข้อมูลที่ใช้บันทึก

(1) มีการควบคุมอย่างเหมาะสมเกี่ยวกับ

(ก) การสร้างแฟ้มข้อมูลขึ้นใหม่เพื่อบรรจุข้อมูลตามรายละเอียดข้างต้น
(ข) การอนุมัติในการแก้ไขข้อมูล
(ค) ความครบถ้วนของการแก้ไขข้อมูลในแฟ้ม
(ง) ความถูกต้องของการแก้ไขข้อมูลในแฟ้ม
(จ) การปรับปรุงข้อมูลในแฟ้มให้ถูกต้องอยู่เสมอ

(2) มีการควบคุมความถูกต้องของการคำนวณค่าแรงขั้นต่ำ รายการหักค่าแรง และค่าแรงสุทธิ ดังนี้

(ก) โปรแกรมที่ใช้ในการคำนวณเหมาะสมหรือไม่
(ข) มีการควบคุมความถูกต้องของผลการคำนวณ เช่น รายงานค่าแรงรายที่ผิดปกติ

7.2 การสรุปผลและแยกประเภทข้อมูล (Summarizing and Categorizing)

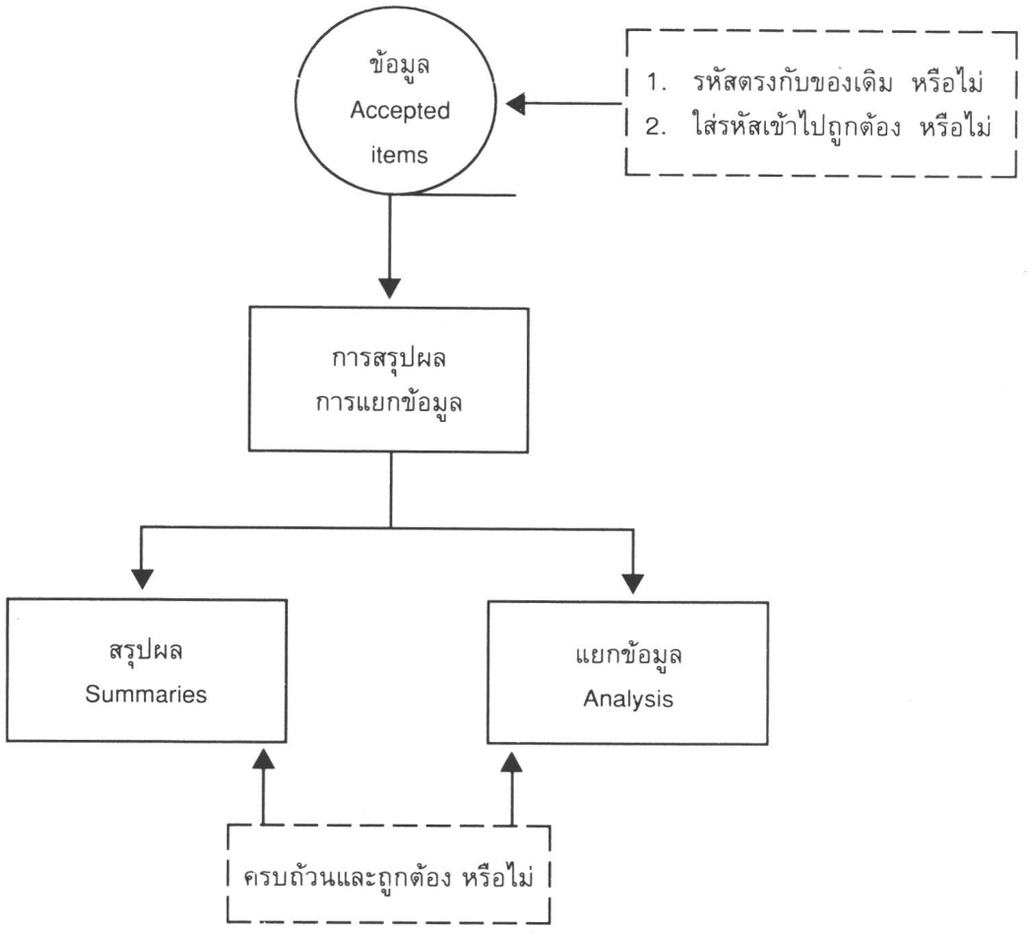
การสรุปผลและแยกประเภทข้อมูลให้มีประสิทธิภาพ ควรกำหนดให้มีสิ่งต่อไปนี้

(ก) รหัส (codes) ที่ใช้สรุปผลและแยกประเภทข้อมูลจะต้องถูกต้องและถูกนำเข้าไปในคอมพิวเตอร์อย่างถูกต้อง

(ข) จะต้องมีการควบคุมการสรุปผลข้อมูลอย่างเหมาะสม เช่นเดียวกับการควบคุมความครบถ้วนและถูกต้องของการ update ข้อมูล

(ค) โปรแกรมที่ใช้ในการแยกประเภทข้อมูลเหมาะสม





แผนภาพที่ 19.14 แสดงการสรุปผลและแยกประเภทข้อมูล

คำถามที่ใช้สำหรับประเมินผลการควบคุมความถูกต้องของการสรุปผลและแยกประเภทข้อมูลที่จะบันทึกในบัญชีคุม (general ledger) มีดังนี้

1. เช็คสอบรหัสของรายการที่ใช้ในการบันทึกบัญชีคุม หรือไม่

2. มีการควบคุมการบันทึกรหัสในคอมพิวเตอร์อย่างเหมาะสม (เช่น ใช้โปรแกรมตรวจสอบความถูกต้องของรหัส) หรือไม่

3. มีการควบคุมให้คอมพิวเตอร์สรุปผลและแยกประเภทข้อมูลครบถ้วนและถูกต้อง (เช่น การใช้บุคคลหรือโปรแกรมตรวจสอบรายงานผลลัพธ์) หรือไม่

4. โปรแกรมที่ใช้ในการสรุปผลและแยกประเภทข้อมูลเหมาะสม หรือไม่

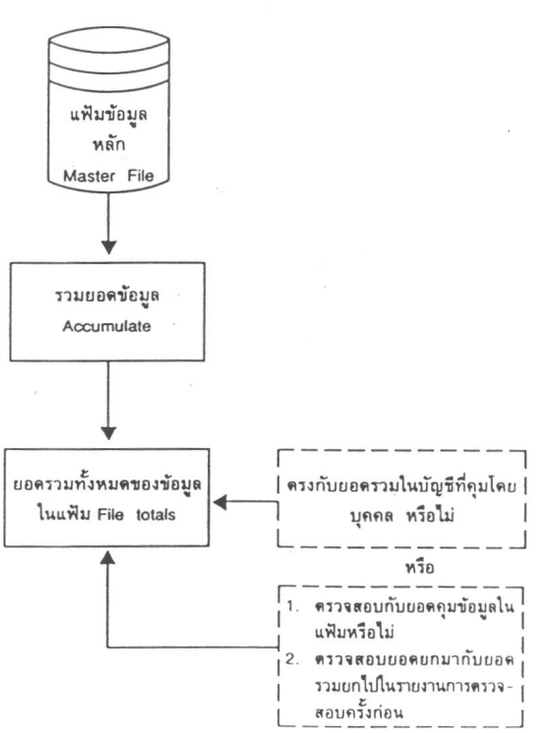
5. ในกรณีที่ใช้บุคคลทำการสรุปผลหรือแยกประเภทข้อมูลเพิ่มเติมต่อไปอีกมีการควบคุมเกี่ยวกับความถูกต้องและครบถ้วนของข้อมูล หรือไม่

8. การตรวจตราความถูกต้องของข้อมูลที่อยู่ในแฟ้มข้อมูล (Maintenance of Data on Files)

การตรวจตราความถูกต้องของข้อมูล เป็นวิธีการควบคุมความถูกต้องของข้อมูลที่อยู่ใน files จนกว่าข้อมูลนั้นจะถูกล้างออกไป วิธีการตรวจตราความถูกต้องของข้อมูลประเภท Transaction data จะเหมือนกันทั้งในระบบงานที่ใช้และไม่ใช้คอมพิวเตอร์ แต่จะต่างกันสำหรับการตรวจตราข้อมูลประเภท standing data เพราะในระบบงานที่ไม่ใช้คอมพิวเตอร์การตรวจสอบความถูกต้องของ standing data จะกระทำทุกครั้งที่นำข้อมูลไปใช้งาน ส่วนระบบที่ใช้คอมพิวเตอร์การตรวจสอบความถูกต้องของ standing data จะกระทำเฉพาะครั้งแรกที่นำข้อมูลเข้าไปในคอมพิวเตอร์ และเมื่อมีการแก้ไขภายหลัง

แต่เดิมการตรวจตราความถูกต้องของข้อมูลมีวัตถุประสงค์เพื่อค้นหาความผิดพลาด อันเนื่องมาจากการลักลอบแก้ไขข้อมูลที่เก็บไว้ใน file ซึ่งปัจจุบันมีน้อยมาก เพราะฉะนั้นเหตุผลที่สำคัญของการตรวจตราความถูกต้องของข้อมูลจึงเปลี่ยนไป เป็นการป้องกันการแก้ไขข้อมูลใน file โดยมิได้รับอนุญาต โดยเฉพาะการแก้ไข standing data จากประสบการณ์ในอดีตพบว่า แม้จะมีการควบคุมความถูกต้องของการนำเข้าและบันทึกข้อมูลใน file แล้วก็ตาม คนก็ยังสามารถสร้างข้อมูลที่ไม่ถูกต้องไว้ใน file ได้ ถ้าหากปราศจากการตรวจตราข้อมูลตามปกติ นอกจากนั้นการตรวจตราข้อมูลยังช่วยให้มั่นใจว่าการ update ข้อมูลของแฟ้มถูกต้องทุกครั้ง

วิธีการตรวจตราความถูกต้องของข้อมูลที่มีประสิทธิภาพมากที่สุดคือ การตรวจสอบยอดรวมของข้อมูลทั้งหมดใน file กับยอดรวมในบัญชีคุม (independently maintained control account) รายการที่ปรากฏในบัญชีคุมได้มาจากยอดรวมของเอกสารในปึก (Batch total) ก่อนที่จะนำไปถ่ายทอดลงแฟ้มข้อมูล การตรวจสอบยอดรวมของข้อมูลใน file อาจจะใช้โปรแกรมคอมพิวเตอร์ตรวจสอบก็ได้ แต่จะต้องเช็คสอบดูว่ายอดยกมาในรายงานการตรวจสอบยอดรวมข้อมูลปัจจุบันตรงกับยอดยกไปในรายงานครั้งก่อนหรือไม่ ทั้งนี้เพราะโปรแกรมคอมพิวเตอร์ที่ใช้ไม่สามารถจะค้นหาข้อผิดพลาดเช่นนี้ได้ วิธีการตรวจสอบยอดรวมข้อมูลใน file แสดงได้ตามรูปภาพ



แผนภาพที่ 19.15 แสดงการตรวจตราความถูกต้องของข้อมูลที่อยู่ในแฟ้มข้อมูล

ความถี่ในการตรวจสอบความถูกต้องของยอดรวมข้อมูลในแฟ้ม ขึ้นอยู่กับลักษณะของการปฏิบัติข้อมูล ถ้าหากการ update ข้อมูลเป็นแบบ sequential การตรวจสอบยอดรวมข้อมูลจะสามารถกระทำได้ทุกครั้งที่มีการ update เพราะขณะที่คอมพิวเตอร์อ่านข้อมูลก็จะทำการรวมยอดข้อมูลที่อ่านไปด้วยพร้อมกัน แต่ถ้าเป็นการปฏิบัติข้อมูลแบบ real time การตรวจสอบยอดรวมข้อมูลใน file จะไม่สามารถกระทำได้บ่อยครั้ง เพราะจะต้องรอจัดระเบียบข้อมูลใน file ก่อน หรือใช้โปรแกรมพิเศษเพื่อการตรวจสอบนี้โดยเฉพาะ ซึ่งวิธีหลังนี้ใช้สำหรับระบบการจัดเก็บข้อมูลใน file แบบ data base

8.1 การตรวจตราความถูกต้องของ Transaction Data

วิธีการตรวจสอบตามที่กล่าวข้างต้นเพียงพอแล้วที่จะใช้ตรวจตราความถูกต้องของ transaction data ที่อยู่ใน file กรณีที่การตรวจสอบไม่สมบูรณ์ เช่น ไม่มีการเช็คสอบยอดข้อมูลคงเหลือยกมาจากการตรวจสอบครั้งก่อน หากผู้ตรวจสอบพบว่าระบบการควบคุมความปลอดภัยของ file เพื่อป้องกันการนำ file ไปใช้โดยมิได้รับอนุญาต มีประสิทธิภาพดีแล้ว ก็ถือได้ว่าการตรวจสอบนี้เพียงพอแล้ว

คำถามเพื่อวัตถุประสงค์ของการควบคุมเกี่ยวกับการตรวจตราความถูกต้องของข้อมูลใน file หลังจากมีการนำเข้าและบันทึกข้อมูลแล้ว มีดังนี้

1. ตรวจสอบยอดรวมของข้อมูลใน file กับ

   (ก) บัญชีคุมข้อมูลซึ่งจัดทำโดยแผนกผู้ใช้ข้อมูล หรือ
   (ข) ยอดคุมข้อมูล (control record) ที่อยู่ใน file และมีหลักฐานการตรวจสอบพิมพ์ออกมาจากคอมพิวเตอร์ หรือไม่

2. กรณีที่ใช้คอมพิวเตอร์ในการตรวจสอบความถูกต้องของข้อมูล

   (ก) ตรวจสอบยอดข้อมูลคงเหลือยกมา หรือไม่
   (ข) ถ้าไม่มีการตรวจสอบยอดข้อมูลคงเหลือยกมา มีการควบคุมความปลอดภัย เพื่อป้องกันมิให้มีการเปลี่ยนแปลงข้อมูลใน file โดยมิได้รับอนุญาต หรือไม่

3. มีการค้นหาสาเหตุของผลต่างซึ่งเกิดจากการตรวจสอบข้อมูลในข้อ 1 และ 2 (ก) ก่อนที่จะทำการปรับปรุงแก้ไข หรือไม่

8.2 การตรวจตราความถูกต้องของ Standing Data

การตรวจสอบข้อมูลที่สำคัญ (important data fields) เช่น อัตราดอกเบี้ยควรจะใช้วิธีการตรวจสอบตามที่กล่าวข้างต้น และควรจะตรวจสอบจำนวนบัญชีหรือข้อมูลใน file เป็นประจำ โดยเฉพาะบัญชีเงินฝากของลูกค้า เพราะอาจมีการเพิ่มบัญชีเงินฝากของลูกค้าเข้าไปใน file โดยไม่ผ่านขั้นตอนตามปกติ เพื่อถอนเงินในภายหลัง ซึ่งเป็นสิ่งที่จำเป็นที่ต้องใช้ในการตรวจสอบข้อมูล standing data

ถึงแม้ว่าการตรวจสอบข้อมูล standing data ใน file เป็นสิ่งที่จำเป็นก็ตาม ผู้ตรวจสอบจะพบว่าระบบคอมพิวเตอร์หลาย ๆ แห่งไม่มีการตรวจสอบชนิดนี้ แต่อาจจะใช้การควบคุมความปลอดภัยของ file และการเช็คสอบเป็นประจำแทน การเช็คสอบกระทำโดยตรวจสอบความถูกต้องของ standing data กับ source data ความถี่ของการตรวจสอบขึ้นอยู่กับความสำคัญของข้อมูลและการควบคุมอื่น ๆ ที่มี ในกรณีที่ไม่มีการควบคุมอื่นควรจะตรวจสอบข้อมูลในแฟ้มทั้งหมด 3 เดือนครั้ง หรือปีละ 4 ครั้ง

คำถามที่เกี่ยวข้องกับการตรวจตราความถูกต้องของ standing data มีดังนี้

1. การควบคุมความถูกต้องของ standing data ในแฟ้มข้อมูลทางบัญชีที่สำคัญ ๆ ใช้วิธีผสมดังต่อไปนี้หรือไม่

   (ก) การควบคุมความปลอดภัยของแฟ้มข้อมูล
   (ข) การตรวจสอบยอดรวมข้อมูลในบัญชีคุม กับยอดรวมข้อมูลที่คอมพิวเตอร์คำนวณได้และพิมพ์ออกมา โดยแผนกผู้ใช้ข้อมูลเป็นประจำทุกเดือน
   (ค) การตรวจสอบรายละเอียดข้อมูลในแฟ้มกับข้อมูลดิบ (source data) โดยแผนกผู้ใช้ข้อมูลเป็นประจำทุกเดือน

2. มีการตรวจสอบ file เป็นประจำเพื่อค้นหา standing data ที่ยังไม่ได้ปรับปรุงให้ถูกต้องหรือไม่

3. มีวิธีการปฏิบัติอย่างเหมาะสมเกี่ยวกับ

   (ก) การค้นหาสาเหตุของความแตกต่างที่ได้มาจากการตรวจสอบในข้อ 1 ก่อนที่จะทำการแก้ไขใด ๆ
   (ข) การค้นหาสาเหตุและการแก้ไข standing data ในข้อ 2

9. การสร้างแฟ้มข้อมูล (File Creation)

เมื่อเกิดการเปลี่ยนระบบจากการปฏิบัติงานโดยใช้บุคคลทั้งหมด มาเป็นการปฏิบัติงานด้วยคอมพิวเตอร์หรือมีการเปลี่ยนแปลงระบบคอมพิวเตอร์ที่มีอยู่เดิม จะมีการสร้าง file ใหม่ ๆ ขึ้น ฉะนั้นผู้ตรวจสอบจะต้องตรวจสอบให้แน่ใจว่า transaction data และ standing data ที่ส่งเข้าไปใน file ตั้งแต่เริ่มแรกถูกต้องและครบถ้วน ซึ่งโดยปกติได้แก่ การตรวจสอบความเหมาะสมของการควบคุมที่สำคัญ ๆ ต่อไปนี้

9.1 การควบคุม Transaction Data

การควบคุมที่เหมาะสมจะช่วยป้องกันและเปิดเผยข้อผิดพลาดในการถ่ายทอดข้อมูลเดิมไปเก็บไว้ในแฟ้มข้อมูลที่สร้างขึ้นใหม่ (opening transaction data) ตัวอย่างเช่น การเปรียบเทียบยอดรวมข้อมูลทั้งหมดในแฟ้มบัญชีลูกหนี้กับบัญชีคุม (control account) และการส่งใบยืนยันยอดหนี้คงเหลือ (statements) ไปให้ลูกหนี้ การควบคุมทั้งสองวิธีนี้จะทำให้ค้นพบข้อผิดพลาดในการถ่ายทอดข้อมูล (incorrect allocations)

ในกรณีที่ผู้ตรวจสอบพบว่าการควบคุมไม่เหมาะสม จะต้องหาวิธีการตรวจสอบอื่น ๆ เพื่อตรวจสอบให้แน่ใจว่าการควบคุมที่ไม่เหมาะสมดังกล่าวไม่ได้ก่อให้เกิดข้อผิดพลาดอย่างร้ายแรงต่องบการเงิน ซึ่งโดยปกติได้แก่ การทดสอบการควบคุมในการถ่ายทอดข้อมูล เช่น การเช็คสอบความถูกต้องของข้อมูลผลลัพธ์โดยละเอียด

9.2 การควบคุม Standing Data

การควบคุมที่ใช้ในระบบงานใหม่ จะไม่สามารถป้องกันข้อผิดพลาดในการถ่ายทอด standing data เข้าไปเก็บไว้ในแฟ้มข้อมูลที่สร้างขึ้นใหม่ ทั้งนี้เพราะ standing data จะได้รับการเช็คสอบความถูกต้องเฉพาะครั้งแรกที่เข้าไปบันทึกเก็บไว้ในคอมพิวเตอร์ หลังจากนั้นความถูกต้องของ standing data จะขึ้นอยู่กับการตรวจตราเป็นประจำ (maintenance controls) ดังนั้นผู้ตรวจสอบจะต้องตรวจสอบให้แน่ใจว่า ในงวดบัญชีที่มีการสร้างแฟ้มข้อมูลขึ้นใหม่นั้นได้บรรจุ standing data ไว้ในแฟ้มครบถ้วนและถูกต้อง โดยผู้ตรวจสอบจะทดสอบผลของการควบคุมในการสร้างแฟ้มข้อมูล เช่น ตรวจสอบความถูกต้องของผลลัพธ์ของข้อมูลโดยละเอียด

คำถามที่ผู้ตรวจสอบควรใช้เมื่อทำการตรวจสอบ standing data ในงวดการบัญชีที่มีการสร้างแฟ้มข้อมูลขึ้นใหม่ คือ "เมื่อสร้างแฟ้มข้อมูลขึ้นใหม่ มีการควบคุมความครบถ้วนและถูกต้องของข้อมูล field ที่มีความสำคัญทางการบัญชี หรือไม่"

นอกจากนี้การควบคุมที่มีอยู่ในระบบงานใหม่อาจจะสามารถป้องกันข้อผิดพลาดในการบรรจุstanding data ลงในแฟ้มข้อมูลใหม่ได้

ระเบียบในการควบคุมการปฏิบัติงาน (Disciplines Over User Controls)

ระเบียบที่กำหนดขึ้นมีวัตถุประสงค์เพื่อคุ้มครองความปลอดภัยของทรัพย์สิน และให้แน่ใจว่าการควบคุมที่ใช้เป็นไปตามมาตรฐานและโดยสม่ำเสมอ ทั้งนี้โดยการกำหนดหรือมอบหมายให้เจ้าหน้าที่ที่รับผิดชอบเป็นผู้ตรวจสอบและรับรองผลของการควบคุมดังกล่าว โดยทั่วไปควรจะมีการแบ่งแยกหน้าที่ของเจ้าหน้าที่ผู้ตรวจสอบการควบคุมการปฏิบัติงานดังนี้

(1) บุคคลที่ทำหน้าที่ตรวจสอบการควบคุมการปฏิบัติงาน ไม่ควรเป็นบุคคลที่มีหน้าที่เกี่ยวกับการออกแบบระบบงาน เขียนโปรแกรม และปฏิบัติข้อมูล ยกเว้นการควบคุมความถูกต้องของข้อมูล (data control section)

(2) บุคคลที่ทำหน้าที่ตรวจสอบการควบคุม standing data ไม่ควรมีส่วนเกี่ยวข้องกับการควบคุม transaction data

(3) ควรแยกบุคคลที่ทำหน้าที่ตรวจสอบการควบคุมเกี่ยวกับการนำเข้า และการบันทึกข้อมูล ออกจากบุคคลที่ทำหน้าที่ตรวจตราความถูกต้องของบัญชีคุมยอด (control account)

(4) บุคคลที่ทำหน้าที่ตรวจสอบความถูกต้องของบัญชีย่อย (subsidiary records) กับบัญชีคุมยอด (control account) ไม่ควรเป็นบุคคลเดียวกับที่ทำหน้าที่ควบคุมความถูกต้องของบัญชีคุมยอด

20

การประเมินการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (1)

การประเมินการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (1)

1. คำนำ

การประเมินการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ ได้แก่ การประเมินการควบคุมการพัฒนาและการแก้ไขโปรแกรม การรักษาความปลอดภัยเกี่ยวกับตัวโปรแกรม ทั้งในระหว่างการใช้งานและไม่ได้ใช้งาน รวมทั้งการควบคุมทั่ว ๆ ไปภายในศูนย์คอมพิวเตอร์ โดยจะพิจารณาในแง่ของการตรวจสอบมากกว่าในแง่ของการสร้างระบบควบคุม

2. วิธีประเมินผล

การประเมินผลส่วนใหญ่จะอาศัยแบบสอบถามการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Controls) และเป้าหมายของการควบคุม (Control Objectives) ในแต่ละเรื่อง เพื่อไม่ให้การสอบถามในแต่ละด้านเยิ่นเย้อจนเกินไป ควรแยกการสอบถามไม่ให้ปะปนกัน และข้อมูลที่ได้จากการสอบถามด้านใดด้านหนึ่งที่สามารถนำมาใช้ประโยชน์ในการประเมินการควบคุมอีกด้านหนึ่งได้ ก็ไม่จำเป็นต้องสอบถามซ้ำอีก

ในกรณีที่พบว่า Control Objectives ไม่เป็นที่น่าเชื่อถือ ผู้ตรวจสอบควรประเมิน Integrity Controls ให้บ่อยขึ้น เพื่อค้นหาจุดอ่อนที่ทำให้ขาดประสิทธิภาพในการปฏิบัติงาน นำเสนอต่อผู้บริหารของธนาคารให้ดำเนินการปรับปรุงแก้ไขและจะพบอยู่เสมอว่าระบบการควบคุมของธนาคารที่เติบโตมาจากการควบคุมด้านผู้ใช้ข้อมูล (User Controls) มักจะต้องมีการปรับปรุงหันมาใช้ Integrity Controls ในเรื่องต่อไปนี้มากขึ้น

1) การควบคุมการพัฒนาโปรแกรม
2) การรักษาความปลอดภัยเกี่ยวกับตัวโปรแกรม
3) การควบคุมการใช้เครื่องคอมพิวเตอร์
4) การควบคุมและการรักษาความปลอดภัยแฟ้มข้อมูล
5) System Software

3. การจัดองค์การในศูนย์คอมพิวเตอร์ (Organization of the Computer Department)

โครงสร้างการจัดองค์การในศูนย์คอมพิวเตอร์ เป็นปัจจัยที่มีความสำคัญประการหนึ่งในการประเมิน Integrity Controls การจัดระบบงานและพนักงานในศูนย์คอมพิวเตอร์ส่วนใหญ่มักจะขึ้นอยู่กับปริมาณงานที่ประมวลผลด้วยคอมพิวเตอร์ จำนวนพนักงานในศูนย์คอมพิวเตอร์ และเทคนิคการควบคุมต่าง ๆ ที่นำมาใช้ ศูนย์คอมพิวเตอร์

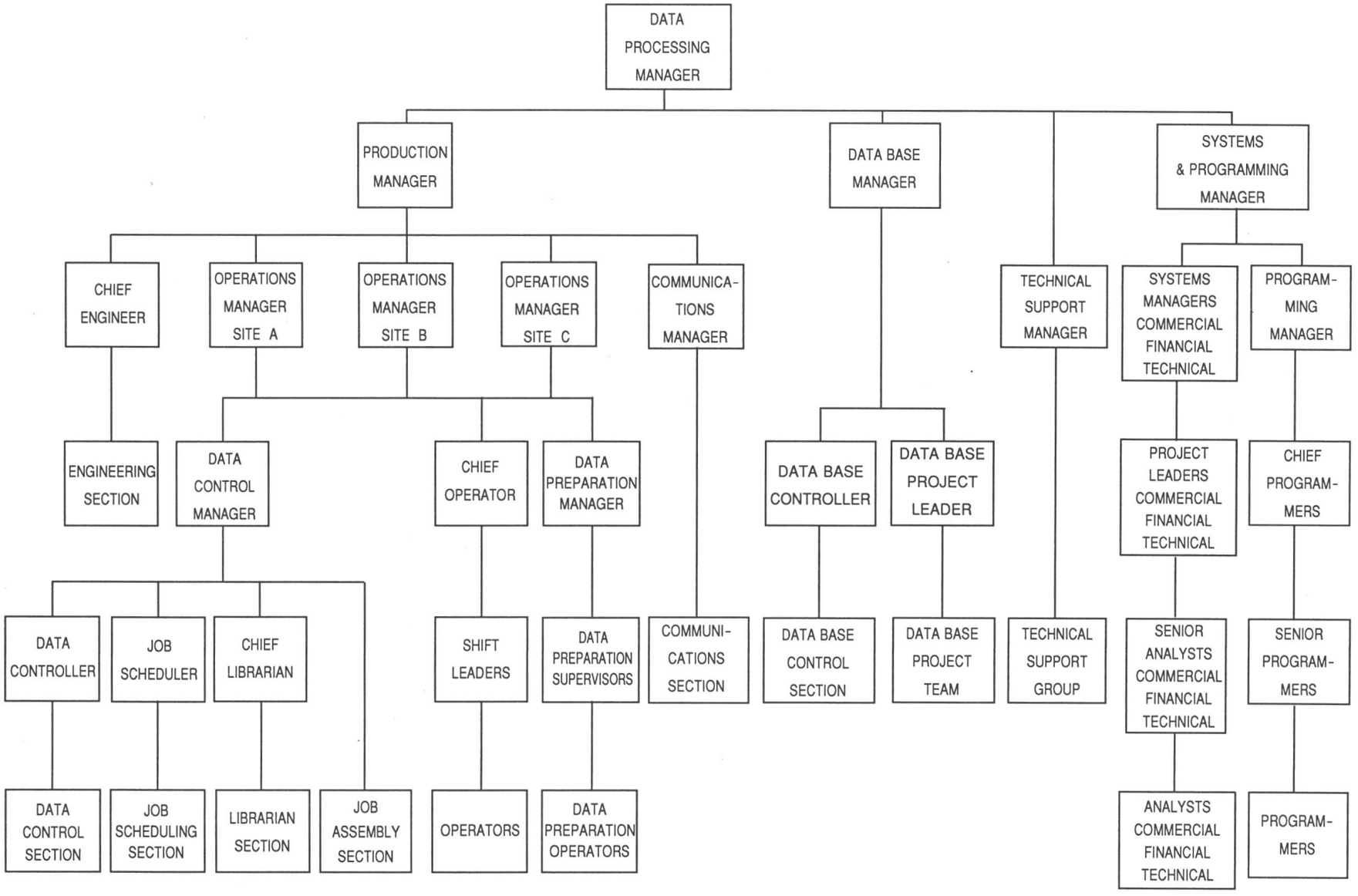
ที่มีขนาดใหญ่ย่อมจะมีโอกาสนำเอาระบบ Integrity Controls ที่ดีพอสนองความต้องการมาใช้ได้มากกว่า เพราะสามารถใช้โปรแกรมเข้าช่วยควบคุมและจัดระเบียบการควบคุมต่าง ๆ ให้เหมาะสมได้ง่าย

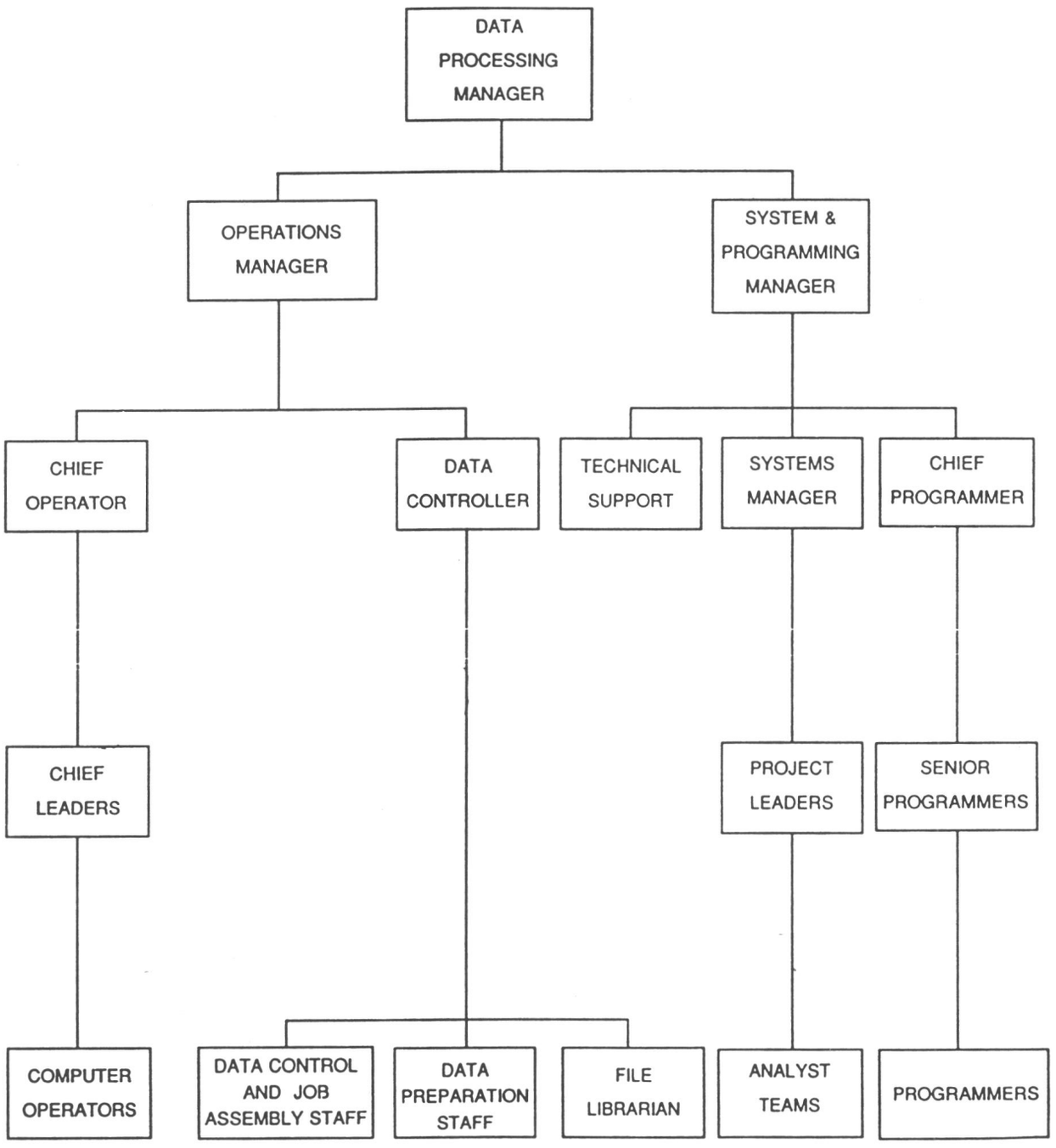
ในศูนย์คอมพิวเตอร์ขนาดใหญ่อาจมีพนักงานถึง 200 คน จะมีการแบ่งแยกหน้าที่กันในด้านการปฏิบัติการประมวลผลด้านการพัฒนาระบบงาน และด้านการควบคุมแฟ้มข้อมูล นอกจากนี้ยังมีการแบ่งแยกหน้าที่ย่อยลงไปอีกในแต่ละด้าน เช่น หน่วยพัฒนาระบบ หน่วยสนับสนุนด้านเทคนิค หน่วยบริหารงาน Data Base และหน่วยควบคุมและเก็บรักษาโปรแกรมงานและแฟ้มข้อมูล ดังนั้นการพิจารณาการจัดองค์การควรคำนึงถึงหน้าที่เป็นหลัก เช่น งานด้านการปฏิบัติการ พนักงานที่ปฏิบัติงานด้านนี้จะมีหน้าที่เกี่ยวกับการปฏิบัติงานการประมวลผล การกำหนดเวลาการปฏิบัติงาน การกำหนดชื่อเครื่องจักรที่ใช้ร่วมกับระบบคอมพิวเตอร์เพื่อใช้ควบคุมการประมวลผลในแต่ละงาน (job set-up) การควบคุมข้อมูลและติดต่อกับผู้ใช้ข้อมูล และการจัดเตรียมข้อมูล เป็นต้น Integrity Controls ที่ใช้อยู่ในศูนย์คอมพิวเตอร์ขนาดนี้ส่วนใหญ่จะอาศัยโปรแกรมและจัดระเบียบที่ใช้ในการควบคุม (Disciplines) ทั้งในด้านการแบ่งแยกหน้าที่ และด้านการควบคุมดูแล (Supervision)

สำหรับศูนย์คอมพิวเตอร์ขนาดกลางอาจจะมีพนักงานประมาณ 50 คน แบ่งแยกหน้าที่เป็นฝ่ายปฏิบัติการประมวลผล กับฝ่ายพัฒนาระบบงาน และอาจมีหน่วยงานย่อย ๆ ที่สนับสนุนด้านเทคนิคอยู่ด้วยก็ได้ แต่การแบ่งแยกความรับผิดชอบในแต่ละหน้าที่จะน้อยกว่าในศูนย์คอมพิวเตอร์ขนาดใหญ่ เช่น อาจมีหัวหน้าศูนย์หรือหัวหน้างาน (Supervisor) เพียงคนเดียว รับผิดชอบในงานด้านการปฏิบัติการประมวลผล ด้านการควบคุมข้อมูล และด้านเก็บรักษาโปรแกรมและแฟ้มข้อมูล เจ้าหน้าที่ผู้ปฏิบัติงานในแต่ละด้านจะถูกจำกัดขอบเขตในการปฏิบัติงานน้อยกว่าศูนย์คอมพิวเตอร์ขนาดใหญ่ จึงควรตรวจสอบว่ามี Integrity Controls เพียงพอหรือไม่ โดยพิจารณาได้จาก Software Procedures การจัดระเบียบในการควบคุม การมอบหมาย และการกระจายหน้าที่ในการควบคุมดูแลการปฏิบัติงาน ซึ่งอาจมีความรัดกุมน้อยกว่าศูนย์คอมพิวเตอร์ขนาดใหญ่

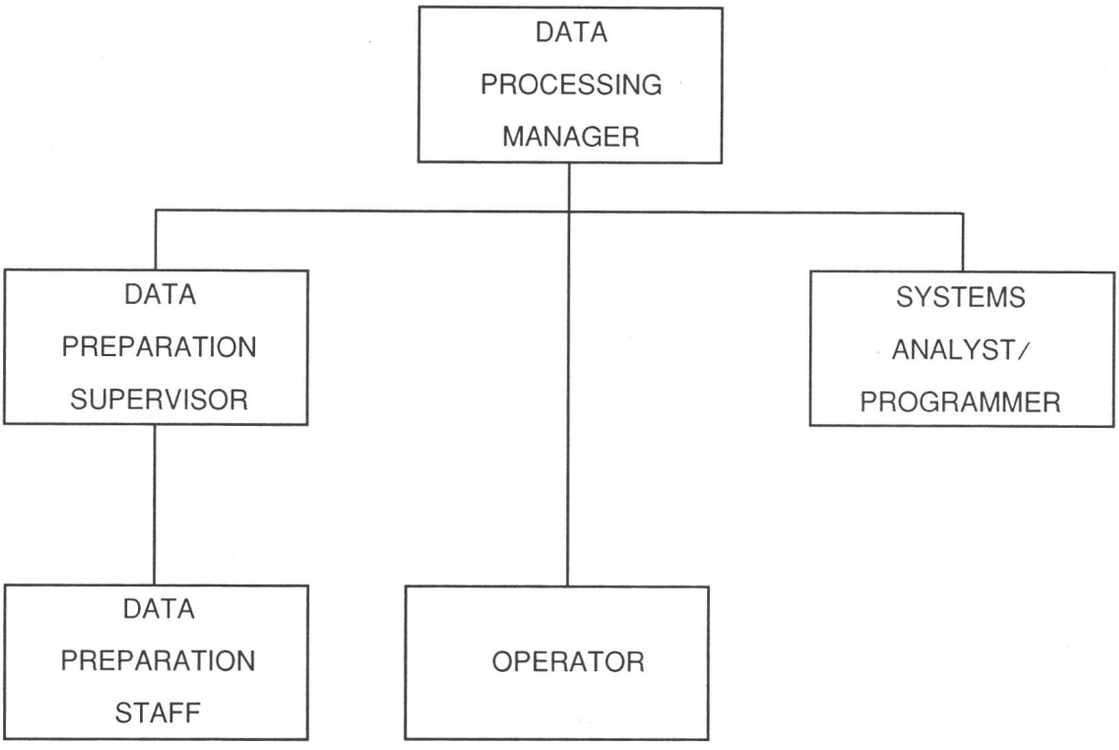


แผนภาพที่ 20.1 แสดงแผนผังการจัดองค์การของศูนย์คอมพิวเตอร์ขนาดใหญ่





แผนภาพที่ 20.2 แสดงผังการจัดองค์การศูนย์คอมพิวเตอร์ขนาดกลาง



แผนภาพที่ 20.3 แสดงผังการจัดองค์การของศูนย์คอมพิวเตอร์ขนาดเล็ก

ในศูนย์คอมพิวเตอร์ขนาดเล็กอาจมีพนักงานเพียง 5 คน จึงเป็นการยากที่จะแบ่งแยกหน้าที่ให้ชัดเจนได้ ส่วนใหญ่หัวหน้าศูนย์คอมพิวเตอร์จะเป็นผู้รับผิดชอบควบคุมดูแลหน้าที่ต่าง ๆ เสียเอง และมอบหมายให้ผู้อื่นควบคุมดูแลการปฏิบัติงานเพียงเล็กน้อย จึงไม่ควรจะเชื่อถือ Integrity Controls ให้มากนัก เพราะมักจะไม่มีการจัดระเบียบในการควบคุมไว้ แต่อย่างไรก็ดีธนาคารที่ใช้ศูนย์คอมพิวเตอร์ขนาดเล็กส่วนใหญ่จะใช้วิธีควบคุมทางด้านผู้ใช้ข้อมูล (User Controls) ทดแทน

4. การควบคุมการพัฒนาโปรแกรม (Implementation Controls)

การควบคุมการพัฒนาโปรแกรม เป็นการพิจารณาความเหมาะสมของกระบวนการพัฒนาโปรแกรมและประสิทธิภาพในการใช้โปรแกรมที่ได้รับอนุมัติให้ใช้งาน (Production Programs) ในการประมวลผล

Production Programs หมายถึง โปรแกรมงานต่าง ๆ (Application Programs) ที่ได้รับอนุมัติให้ใช้ในการประมวลข้อมูลทางการบัญชี ซึ่งอาจอยู่ในรูปของโปรแกรมที่ถูกแปลงรหัสแล้วพร้อมที่จะประมวลผล (Executable Program) และโปรแกรมที่อยู่ในรูปของภาษาเขียนดั้งเดิมของผู้เขียนโปรแกรม ซึ่งใช้ประมวลผลยังไม่ได้ (Source Program) เช่น อยู่ในรูปของภาษา COBOL

Application Program หมายถึง โปรแกรมที่ใช้ในการประมวลผลงานใดงานหนึ่งโดยเฉพาะ ไม่รวมถึงโปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์ (Operating System)

การประเมินการควบคุมการพัฒนาโปรแกรมอาจแยกพิจารณาได้ 2 กรณี คือ กรณีของระบบงานใหม่และกรณีแก้ไขโปรแกรม

4.1 กรณีระบบงานใหม่ (New Systems)

สาเหตุที่ทำให้ผู้ตรวจสอบอาจไม่เชื่อถือการควบคุมการพัฒนาโปรแกรมในตอนที่เริ่มนำระบบงานใหม่มาใช้ โดยเฉพาะระบบงานที่ค่อนข้างใหญ่และมีความสลับซับซ้อนมากมีอยู่หลายประการ ในบางครั้งผู้ตรวจสอบอาจจำเป็นต้องทดสอบการทำงานของโปรแกรมที่ใช้ประมวลผลในตอนที่นำระบบงานใหม่มาปฏิบัติงานด้วย อย่างไรก็ตามผู้ตรวจสอบภายในของธนาคารมักมีส่วนร่วมในการพัฒนาโปรแกรม เพื่อช่วยกำหนดรูปแบบข้อมูลที่ใช้ในการทดสอบ (Audit Test Data) และสามารถให้คำแนะนำแก้ไขข้อบกพร่องได้ก่อนที่จะนำโปรแกรมออกใช้งาน ดังนั้นผู้ตรวจสอบควรประเมินผลการควบคุมการพัฒนาโปรแกรมของระบบงานใหม่ ๆ ทุกงาน แม้จะไม่ตั้งใจเชื่อถือการควบคุมดังกล่าวในระยะที่เริ่มนำระบบงานใหม่มาใช้ก็ตาม

การควบคุมการพัฒนาโปรแกรมใช้งานสามารถแบ่งออกได้ 3 ขั้นตอน คือ การวางระบบงาน (System Design) การทดสอบโปรแกรมและระบบงาน (Program and System Testing) และการ catalog โปรแกรม ซึ่งในแต่ละขั้นตอนจะมีความสำคัญและสัมพันธ์กันเพียงใดนั้น ขึ้นอยู่กับชนิดของโปรแกรมซึ่งมีอยู่ 2 ประเภท คือ ประเภท Purpose-built และประเภท Package

โปรแกรมประเภท Purpose-built คือ โปรแกรมที่ออกแบบขึ้นมาใช้เฉพาะงาน ซึ่งอาจพัฒนาและปรับปรุงให้ตรงกับความต้องการของผู้ใช้โดยศูนย์คอมพิวเตอร์ของธนาคารเอง หรือจ้างบุคคลภายนอกให้ดำเนินการพัฒนาให้ การพัฒนาโปรแกรมประเภทนี้ทุกขั้นตอนค่อนข้างจะมีความสำคัญมากกว่าการควบคุมการวางระบบใหม่โดยบุคคลภายนอก

โปรแกรมประเภท Package คือ โปรแกรมที่พัฒนาโดยบริษัทผู้ผลิตคอมพิวเตอร์ หรือ Software House เพื่อใช้กับงานทั่ว ๆ ไป เช่น โปรแกรมเงินเดือน ซึ่งค่อนข้างจะมีมาตรฐานอยู่ในระดับเดียวกันทุกกิจการ ผู้ใช้ (User) เพียงแต่กำหนดตัวแปร (Parameters) ที่เกี่ยวข้องให้กับโปรแกรม ก็สามารถประมวลผลให้อยู่ในรูปแบบที่ต้องการได้ ผู้ตรวจสอบเพียงแต่คอยดูแล Package โปรแกรมที่นำมาใช้ว่าสามารถเข้ากับระบบงานส่วนอื่นได้หรือไม่ โดยไม่จำเป็นต้องเข้าไปเกี่ยวข้องกับการวางระบบงาน (System Design) การทดสอบโปรแกรมและระบบงาน (Program and System Testing) ให้มากนัก ถ้า Package โปรแกรมดังกล่าวมีใช้กันอยู่อย่างแพร่หลายทั่วไป

การปฏิบัติงานของธนาคารตั้งแต่เริ่มศึกษาความเป็นไปได้ในการนำระบบคอมพิวเตอร์มาใช้จนกระทั่งนำระบบคอมพิวเตอร์ออกปฏิบัติงานจนสำเร็จนั้น เป็นช่วงที่มีความสำคัญและต้องใช้เวลามาก เนื่องจากต้องมีการพิจารณาเพื่อกำหนดระเบียบการปฏิบัติงานต่าง ๆ ทั้งด้านศูนย์คอมพิวเตอร์และด้านผู้ใช้ข้อมูลคอมพิวเตอร์

ทำโปรแกรมงานต่าง ๆ ให้เป็นไปตามความต้องการของผู้ใช้ ซึ่งงานเหล่านี้จะต่อเนื่องกันไปเรื่อย ๆ ผู้ตรวจสอบจะต้องชี้ให้เห็นถึงความสำคัญของวิธีปฏิบัติงานในแต่ละด้าน เพื่อให้ Programmed Procedures ที่นำมาใช้นั้นเหมาะสมและเชื่อถือได้ โดยกำหนดวิธีการเกี่ยวกับ

- การวางระบบงานและการจัดทำโปรแกรม
- การทดสอบโปรแกรมและระบบงาน
- การ Catalog โปรแกรม

(1) การวางระบบงานและการจัดทำโปรแกรม

(System Design and Program Preparation)

อาจพิจารณาได้จากความเหมาะสมของ Programmed Procedures ที่ใช้ การวางระบบงานและการเขียนโปรแกรม สำหรับการกำหนดลักษณะของระบบงานมีอยู่ 2 แบบ คือ แบบกว้าง ๆ และแบบละเอียด

คำอธิบายระบบงานแบบกว้าง (Outline System Descriptions) ควรเขียนให้ผู้ใช้ข้อมูลเข้าใจและเห็นด้วยกับ Program Procedures ที่จะนำออกใช้ เช่นเดียวกับคำอธิบายระบบงานโดยละเอียด (Detailed System Descriptions) ซึ่งจะต้องพยายามทำความเข้าใจกับผู้รับผิดชอบในการตรวจสอบการพัฒนาระบบงานในขั้นรายละเอียดด้วย สำหรับศูนย์คอมพิวเตอร์ขนาดใหญ่ หัวหน้าศูนย์ฯหรือหัวหน้าโครงการจะเป็นผู้รับผิดชอบ และไม่ควรปฏิบัติงานด้านอื่นต่อไปจนกว่า Outline System Descriptions จะถูกตรวจสอบและได้รับการอนุมัติจากผู้ใช้ข้อมูลและศูนย์คอมพิวเตอร์ หากเป็นระบบ Data Base จะต้องให้ผู้บริหารงาน Data Base ร่วมพิจารณาระบบงานใหม่ที่วางไว้ด้วย เพื่อขจัดความขัดแย้งระหว่างผู้ใช้ข้อมูลชนิดเดียวกัน

สำหรับคำอธิบายระบบงานโดยละเอียด ควรเขียนให้ผู้เขียนโปรแกรมเข้าใจ สามารถเขียนโปรแกรมได้อย่างมีประสิทธิภาพและชัดเจน หัวหน้างานที่มีหน้าที่ควบคุมดูแลการเขียนโปรแกรมสามารถใช้คำอธิบายนี้ตรวจสอบตรรก (Logic) ที่ใช้ในการเขียนโปรแกรม และควบคุมงานเขียนโปรแกรมได้เป็นอย่างดี นอกจากนี้ผู้ใช้ข้อมูลจำเป็นต้องอาศัยคำอธิบายระบบงานโดยละเอียดนี้ เพื่อทำความเข้าใจการทำงานของโปรแกรม เพื่อประสิทธิภาพในการวางระบบควบคุมทางด้านผู้ใช้ข้อมูล (User Controls) ด้วย และก่อนที่จะนำรายละเอียดไปใช้เขียนโปรแกรม ควรให้ผู้ใช้ข้อมูลและศูนย์คอมพิวเตอร์ตรวจสอบและอนุมัติให้ใช้เสียก่อน

คุณภาพของคำอธิบายระบบงานทั้งสองแบบที่กล่าวข้างต้น ต้องมีความสำคัญต่อการแก้ไขโปรแกรมมาก หากไม่มีรายละเอียดระบุไว้ในระบบงานอย่างเพียงพอ การแก้ไขโปรแกรมจะยุ่งยากและขาดประสิทธิภาพ

คำถามที่ใช้สอบถามเกี่ยวกับระบบงาน มีดังนี้

1) คำอธิบายระบบงานและการแก้ไขระบบงานที่ทำขึ้นมาเป็นไปตามหลักเกณฑ์ต่อไปนี้หรือไม่

1.1) ช่วยให้ผู้ใช้ข้อมูลเข้าใจและยอมรับ Program Procedures

1.2) มีการควบคุมการวางระบบและจัดทำโปรแกรมโดยฝ่ายที่รับผิดชอบในการประมวลข้อมูล

2) คำอธิบายระบบงานที่กล่าวตามข้อ 1 มีการตรวจสอบและได้รับอนุมัติจากพนักงานชั้นบริหารที่มีหน้าที่รับผิดชอบดังต่อไปนี้หรือไม่

2.1) ผู้ใช้ข้อมูล
2.2) ฝ่ายที่รับผิดชอบในการประมวลข้อมูล

(2) การทดสอบโปรแกรมและระบบงาน

(Program and System Testing)

การทดสอบโดยปกติมี 3 ขั้นตอน คือ การทดสอบโปรแกรม (Program Testing) การทดสอบโปรแกรมทั้งระบบ (System Testing) และการทดลองปฏิบัติงานคู่ขนาน หรือทดลองปฏิบัติจริง (Parallel or Pilot Running)

2.1) การทดสอบโปรแกรม (Program Testing)

การทดสอบโปรแกรม คือ การเช็คสอบตรรก (Logic) ในแต่ละโปรแกรมโดยใช้วิธีทดสอบแบบ Desk Checking ซึ่งได้แก่ การตรวจสอบรหัสต่าง ๆ ที่ใช้ในโปรแกรมให้ตรงกับข้อกำหนดและตรวจสอบ Logical Paths ต่าง ๆ ในโปรแกรมด้วย ซึ่งจะเชื่อมโยงกับเทคนิคที่ผู้ตรวจสอบใช้ทดสอบและวิเคราะห์รหัสโปรแกรมการทดสอบแบบ Desk Checking นี้ควรมอบหมายให้ผู้เขียนโปรแกรมเป็นผู้ทดสอบ ไม่ควรให้ผู้ออกแบบรหัส ผู้เขียนรหัส และผู้แปลงรหัส เป็นผู้ทดสอบ

2.2) การทดสอบโปรแกรมทั้งระบบ (System Testing)

การทดสอบโปรแกรมทั้งระบบ ได้แก่ การเช็คสอบตรรก (Logic) ของโปรแกรมต่าง ๆ ที่นำมาเชื่อมต่อกัน (Link) ทั้งระบบ โดยใช้เทคนิคการทดสอบข้อมูล (Test Data) ซึ่งจำเป็นต้องสร้างข้อมูลสำหรับการทดสอบให้แตกต่างไปจากข้อมูลที่ใช้ตามปกติบ้าง เพื่อทดสอบการทำงานของโปรแกรมเมื่อพบรายการที่ผิดปกติ การจัดทำข้อมูลสำหรับทดสอบในกรณีนี้คณะผู้เขียนโปรแกรมกับผู้วิเคราะห์ระบบงาน ควรร่วมกันจัดทำโดยมีฝ่ายผู้ใช้ข้อมูลเป็นที่ปรึกษา การพิจารณาผลการทดสอบควรทำด้วยความระมัดระวัง หากพบตรรก (Logic) ที่ ผิดพลาดจะต้องแก้ไขและทดสอบใหม่จนกว่าจะถูกต้อง โดยดำเนินการตามระเบียบปฏิบัติในการปรับปรุงแก้ไขโปรแกรม หากมีปัญหาเกิดขึ้นในการทดสอบ และต้องติดตามดูแลแก้ไขจนแล้วเสร็จ สำหรับผู้ที่ปฏิบัติงานทดสอบไม่ควรเป็นผู้เขียนโปรแกรม

2.3) การทดลองปฏิบัติงานคู่ขนานหรือทดลองปฏิบัติงานจริง (Parellel of Pilot Running)

การทดลองปฏิบัติงานคู่ขนาน (Parallel running) คือ การทดสอบระบบงานใหม่ที่จะนำมาใช้ โดยทดลองปฏิบัติงานควบคู่ไปกับระบบงานเดิม แล้วนำผลการปฏิบัติงานทั้งสองระบบมาตรวจสอบข้อแตกต่างที่เกิดขึ้น แต่ค่อนข้างยุ่งยาก เพราะมีปัญหาเกี่ยวกับค่าใช้จ่ายในการปฏิบัติงานซ้ำซ้อน และผลการ

ปฏิบัติงานทั้งสองระบบก็ยากแก่การเปรียบเทียบ ดังนั้นจึงนิยมใช้วิธีทดลองปฏิบัติงานจริงแบบ Pilot running โดยค่อย ๆ ทะยอยนำระบบใหม่เข้ามาปฏิบัติงานแทนระบบงานเดิมไปทีละส่วนจนครบทั้งระบบ

วิธีปฏิบัติทั้งสองวิธีนี้เป็นการทดสอบความสมบูรณ์ของการปฏิบัติงานในระบบงานใหม่ทั้งด้านผู้ใช้ข้อมูลและด้านประมวลผล ซึ่งต่างกับ System Testing เพราะการทดลองปฏิบัติงานคู่ขนาน หรือการทดลองปฏิบัติงานจริงนี้ เป็นการทดสอบความสามารถของระบบใหม่ด้วยการปฏิบัติงานจริง มิใช่การทดสอบข้อมูลที่ไม่ได้ใช้ปฏิบัติงานจริง หรือทดสอบเฉพาะรายการแต่ละชนิดเท่านั้น จึงควรมีคณะกรรมการรับผิดชอบโดยตรงร่วมกับตัวแทนฝ่ายผู้ใช้ข้อมูลที่มาช่วยสร้างแฟ้มข้อมูล และฝึกอบรมการใช้ข้อมูล และไม่ควรยอมรับระบบใหม่ที่นำมาใช้งานทั้งระบบจนกว่าการทดลองปฏิบัติงานจะเสร็จสิ้นทั้งระบบ สำหรับงานบางประเภทที่ต้องใช้เวลาทดลองปฏิบัติงานตั้งแต่ 3 เดือนขึ้นไปจึงจะเสร็จงานอาจใช้วิธีเลียนแบบ (Simulated) งานที่ทำก็ได้ อย่างไรก็ดีควรหาวิธีที่สามารถทดสอบงานที่ปฏิบัติทั้งเดือนได้อย่างน้อยเดือนละครั้ง เป็นการทดสอบงานซ้ำเพื่อความแน่ใจในการทดสอบงานประจำวันหรือประจำสัปดาห์

ความสำคัญของการทดสอบโปรแกรมและระบบงาน ขึ้นอยู่กับบทบาทของหน่วยงานที่เกี่ยวข้อง และข้อกำหนดในการทดสอบทุกขั้นตอน เพื่อความเหมาะสมในทางปฏิบัติ ทุกฝ่ายที่เกี่ยวข้อง คือ พนักงานของศูนย์คอมพิวเตอร์ ผู้ใช้ข้อมูล และคณะกรรมการที่รับผิดชอบงานด้านคอมพิวเตอร์ ควรร่วมกันหาข้อสรุปในการตัดสินใจรับรองผลการทดสอบโปรแกรมและระบบงานใหม่ที่จะนำมาใช้งาน

การสอบถามเกี่ยวกับการทดสอบโปรแกรมและระบบงาน อาจใช้คำถามดังนี้

1) ในการจัดทำโปรแกรมมีการทดสอบในเรื่องต่อไปนี้อย่างเพียงพอหรือไม่

   1.1) วิธีการ (เช่น การทดสอบด้วยข้อมูล การปฏิบัติงานคู่ขนาน)
   1.2) ขอบเขต (เช่น ปริมาณงานที่ทดสอบ)

2) มีบุคคลอื่นที่มิใช่ผู้เขียนโปรแกรมเป็นผู้ตรวจสอบการทดสอบโปรแกรมและระบบงาน หรือไม่

(3) การ Catalog โปรแกรม

วิธีการ catalog โปรแกรมในระบบงานใหม่ จะเหมือนกับการ catalog โปรแกรมในกรณีที่มีการแก้ไขโปรแกรม ซึ่งอยู่ในเรื่องการแก้ไขโปรแกรมในหัวข้อถัดไป

4.2 การแก้ไขโปรแกรม (Program Changes)

ก่อนที่จะเชื่อถือการควบคุมการแก้ไขโปรแกรมในระบบงานใหม่ที่จะนำมาใช้งาน ควรดำเนินการทดสอบจนพอใจเพื่อให้แน่ใจว่าธนาคารมีการควบคุมการแก้ไขโปรแกรมอย่างเหมาะสม มีการขออนุมัติแก้ไขโปรแกรมตามระเบียบที่วางไว้อย่างมีประสิทธิภาพ และการแก้ไขดังกล่าวจะต้องไม่มีผลกระทบต่อขั้นตอนในการทำงานของโปรแกรม

ในกรณีที่ผลการทดสอบการควบคุมการแก้ไขโปรแกรมดังกล่าวไม่เป็นที่น่าพอใจ จะต้องขยายการทดสอบให้มากขึ้น โดยตรวจสอบขั้นตอนในการจัดทำโปรแกรมในบางส่วนจนพอใจ แต่วิธีนี้อาจนำไปใช้กับระบบงานขนาดใหญ่ไม่ได้ และในกรณีที่ไม่อาจเชื่อถือในวิธีการการควบคุมจะต้องประเมินผลเพื่อตั้งเป็นข้อสังเกตให้ธนาคารทราบ

สำหรับการควบคุมในการปรับปรุงแก้ไขโปรแกรมที่ใช้งานแล้ว จะมีลักษณะเหมือนกับการแก้ไขโปรแกรมในระบบงานใหม่ที่จะนำมาใช้งาน ดังนั้นจึงจำเป็นต้องมีหลักการในการตรวจรับงาน (Acceptance) การออกแบบและการทดสอบในการแก้ไขโปรแกรมอย่างเหมาะสม และมีมาตรฐานในระดับสูงเช่นเดียวกับกรณีที่เป็นระบบงานใหม่ โดยมีการขออนุมัติแก้ไขก่อนที่จะดำเนินการแก้ไขด้วยความระมัดระวัง เพื่อให้แน่ใจว่าการแก้ไขโปรแกรมดังกล่าวจะไม่มีผลกระทบกระเทือนต่อระบบงานอื่น โดยเฉพาะอย่างยิ่งในกรณีที่มีการใช้ข้อมูลร่วมกันในระบบ Data Base เช่น การลบข้อมูลที่ถูก update เข้าสู่ระบบ Data Base จะต้องตรวจสอบส่วนที่เกี่ยวข้องกับระบบงานอื่นด้วยความระมัดระวัง และถือเป็นการตรวจสอบงานด้าน Data Base ด้วย

นอกจากนี้การแก้ไขโปรแกรมในระบบงานเก่าที่ใช้งานแล้ว ควรมีกระบวนการที่ช่วยให้แน่ใจว่าโปรแกรมส่วนที่ถูกแก้ไขทำงานได้ผลตรงตามวัตถุประสงค์ มีความถูกต้อง มีความสมบูรณ์ และมีประสิทธิภาพในการแก้ไข ซึ่งเป็นหลักในการพิจารณาถึงความเชื่อถือการควบคุมในการแก้ไขโปรแกรมของธนาคาร โดยอาจ ละเว้นการควบคุมอื่นที่ไม่จำเป็นได้บางส่วน

กรณีที่เป็นระบบงานใหม่ควรมีกระบวนการที่จะช่วยให้เกิดความเชื่อมั่นในการแก้ไขโปรแกรม ดังนี้

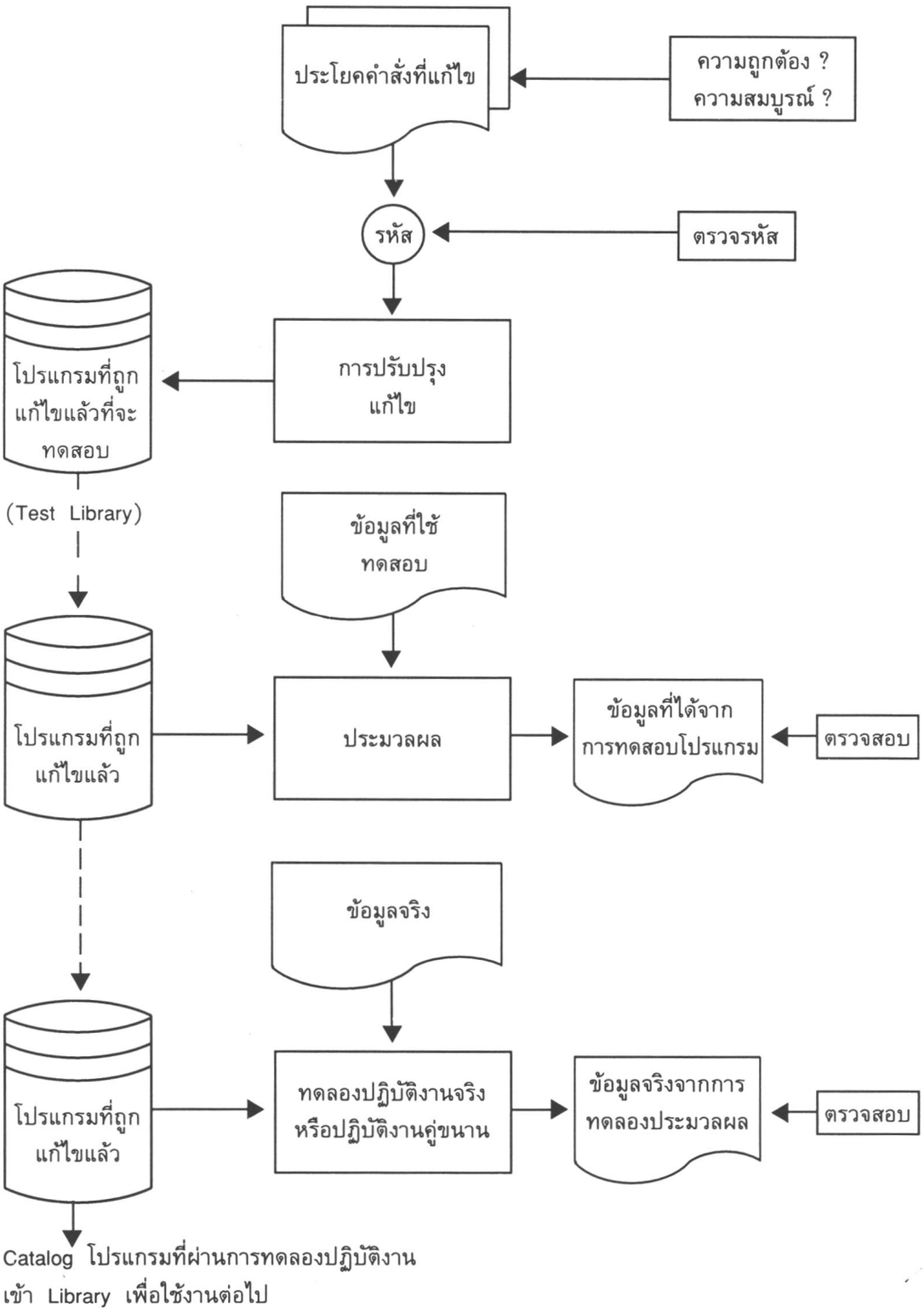
(1) การปฏิบัติตามระเบียบในการแก้ไขโปรแกรม
(2) ความสมบูรณ์ในการแก้ไขโปรแกรม
(3) การทดสอบโปรแกรมที่มีการแก้ไข
(4) การ catalog โปรแกรมที่มีการแก้ไข

การปฏิบัติตามระเบียบในการแก้ไขโปรแกรม

โดยปกติจะมีระเบียบกำหนดให้ผู้ใช้ข้อมูลและเจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ ต้องยื่นคำขอแก้ไขโปรแกรมไปยังผู้วิเคราะห์ระบบงาน เพื่อกำหนดแนวทางในการแก้ไขให้ผู้เขียนโปรแกรมนำไปใช้ในการแก้ไขโปรแกรม รวมทั้งรหัสต่าง ๆ และเอกสารที่เกี่ยวข้อง โดยให้ผู้บริหารระดับสูงที่มีหน้าที่รับผิดชอบตามลำดับขั้นพิจารณาอนุมัติการแก้ไข และพิจารณาการควบคุมอื่น ๆ ก่อนดำเนินการ



กระบวนการแก้ไขโปรแกรม



แผนภาพที่ 20.4 กระบวนการแก้ไขโปรแกรม

คำถามที่ควรสอบถามเพื่อประเมินผลการปฏิบัติตามระเบียบในการแก้ไขโปรแกรม มีดังนี้

มีการขออนุมัติแก้ไขโปรแกรม(ยกเว้นการแก้ไขปัญหาฉุกเฉินเฉพาะหน้า)ตามระเบียบทุกครั้งหรือไม่

ความสมบูรณ์ในการแก้ไขโปรแกรม

เพื่อให้แน่ใจว่าได้มีการดำเนินการตามคำขออนุมัติแก้ไขโปรแกรมทุกรายการ จึงจำเป็นต้องจดบันทึกการแก้ไขไว้ทุกครั้ง โดยใช้แบบฟอร์มชนิดพิมพ์เลขที่คำขอเรียงกันไว้ล่วงหน้าเพื่อใช้เก็บไว้เป็นหลักฐานเรียงกันตามลำดับ หรือจะใช้ทะเบียนบันทึกการแก้ไขก็ได้ และมีพนักงานของศูนย์คอมพิวเตอร์เป็นผู้รับผิดชอบ

คำถามที่จะใช้ประเมินความสมบูรณ์ในการแก้ไขโปรแกรม มีดังนี้

1) มีการจดบันทึกการแก้ไขโปรแกรมไว้ในทะเบียนทุกครั้ง หรือไม่
2) มีการทบทวนสาเหตุที่ทำให้การแก้ไขโปรแกรมล่าช้า หรือไม่

การทดสอบโปรแกรมที่มีการแก้ไข

การทดสอบโปรแกรมที่มีการแก้ไขคงใช้หลักการทดสอบเช่นเดียวกับกรณีระบบงานใหม่ที่มีการทดสอบโปรแกรมและระบบงาน รวมทั้งการปฏิบัติงานคู่ขนาน หรือการทดลองปฏิบัติงานจริงซึ่งได้กล่าวมาแล้ว แต่เอกสารเกี่ยวกับการแก้ไขโปรแกรมควรมีคุณภาพ เพื่อเป็นพื้นฐานในการออกแบบเปลี่ยนแปลงแก้ไข หากเอกสารเหล่านี้ไม่สมบูรณ์อาจทำให้การออกแบบแก้ไขโปรแกรมไม่เป็นไปตามวัตถุประสงค์ การทดสอบจะมากน้อยเพียงใดขึ้นอยู่กับขอบเขตของการแก้ไข เช่น ในกรณีที่แก้ไขเฉพาะรูปแบบของรายงานการตรวจรหัสและใช้แฟ้มข้อมูลง่าย ๆ ทดสอบโปรแกรมที่ใช้พิมพ์รายงาน หากการแก้ไขมีผลกระทบต่อการคำนวณ เช่น มีการแก้ไขรายการหักเงินเดือน หรือมีการจ่ายโบนัสเป็นกรณีพิเศษ อาจต้องทดสอบระบบงานโดยใช้ข้อมูลทดสอบหลาย ๆ แบบทดสอบโปรแกรมทั้งระบบ เพื่อป้องกันผลกระทบที่อาจก่อให้เกิดความเสียหายซึ่งอาจมองไม่เห็น สำหรับการแก้ไขโปรแกรมในส่วนที่สำคัญ หรือมีผลกระทบต่อโปรแกรมทั้งระบบ อาจจำเป็นต้องทดสอบปฏิบัติงานแบบคู่ขนานหรือทดลองปฏิบัติงานจริง เหมือนกับนำระบบงานใหม่มาใช้งานเพื่อพิสูจน์ผลของการแก้ไขโปรแกรม ถ้าการแก้ไขมีผลกระทบต่อการควบคุมทางด้านผู้ใช้ข้อมูล จะต้องทดสอบการทำงานของผู้ใช้ข้อมูลที่มีการแก้ไขเปลี่ยนแปลงในส่วนที่สำคัญด้วย

การสอบถามเพื่อประเมินผลการทดสอบโปรแกรมที่มีการแก้ไข มีดังนี้

1) เพื่อให้การออกแบบและการแก้ไขโปรแกรมมีหลักการที่ดี ธนาคารมีการปฏิบัติดังต่อไปนี้หรือไม่
   1.1) มีเอกสารเกี่ยวกับระบบงานและโปรแกรมอย่างเพียงพอ
   1.2) การเขียนโปรแกรมเป็นไปตามมาตรฐานที่เหมาะสม

2) ในการทดสอบโปรแกรม

(ก) วิธีการ (เช่น การทดสอบข้อมูล) และ

(ข) ขอบเขต (เช่น ปริมาณการทดสอบ)

ที่กำหนดไว้เหมาะสมกับการปฏิบัติงานเกี่ยวกับ

2.1) การแก้ไขโปรแกรม หรือไม่

2.2) การปฏิบัติงานอื่น ๆ นอกจากการแก้ไขโปรแกรม หรือไม่

3) มีบุคคลอื่นที่มิใช่ผู้แก้ไขโปรแกรมเป็นผู้ทดสอบการทำงานของโปรแกรมที่ถูกแก้ไข หรือไม่

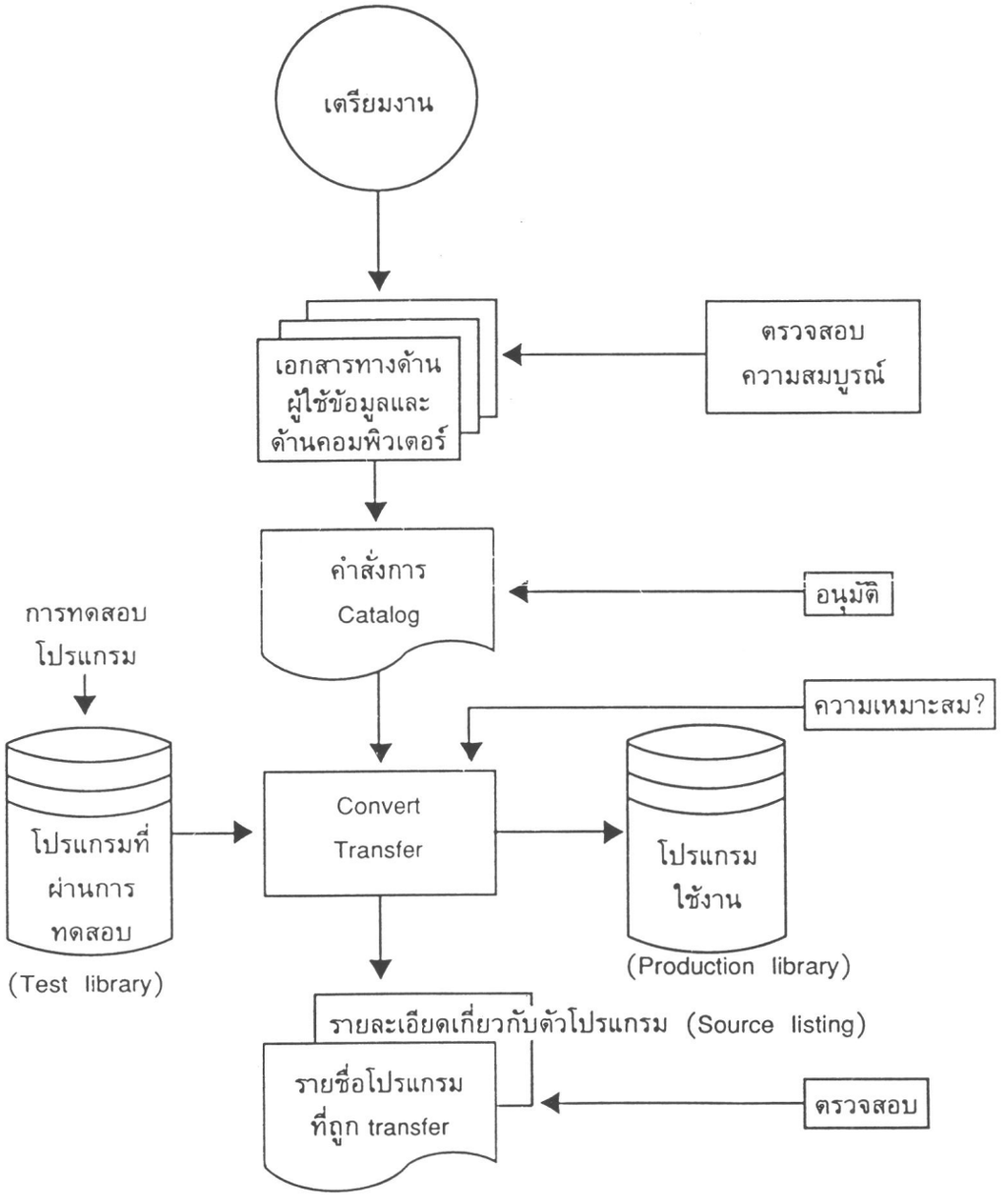
การ Catalog โปรแกรมที่มีการแก้ไข

การ Catalog คือ กระบวนการปฏิบัติงานทั้งด้าน Manual และ Software เพื่อนำโปรแกรมที่ผ่านการทดสอบการทำงานแล้วเข้าสู่ Library สำหรับใช้ปฏิบัติงานจริง

เพื่อให้การทดสอบโปรแกรม ตลอดจนเอกสารต่าง ๆ มีความสมบูรณ์และเป็นที่น่าพอใจ จำเป็นต้องมีคู่มือปฏิบัติงานเกี่ยวกับการทดสอบโปรแกรมการจัดทำเอกสารและการนำระบบงานใหม่มาใช้ หรือการแก้ไขระบบงาน ทั้งด้านผู้ใช้ข้อมูลและศูนย์คอมพิวเตอร์ นอกจากนี้ยังจำเป็นต้องมีคู่มือชนิดที่ต้องถือเป็นระเบียบปฏิบัติอย่างเคร่งครัด เพื่อให้การโอนงานในระบบงานใหม่หรือโปรแกรมที่มีการแก้ไขมีจุดตัดตอน (Cut-off Point) ที่เหมาะสมทุกขั้นตอน นับตั้งแต่ขั้นทดสอบโปรแกรมหรือขั้นปฏิบัติงานจริง ซึ่งผู้ใช้ข้อมูลและศูนย์คอมพิวเตอร์จะตัดสินใจร่วมกันในระหว่างการประชุมคณะกรรมการที่รับผิดชอบงานด้านคอมพิวเตอร์ ทั้งนี้เพื่อให้ผู้ที่เกี่ยวข้องทุกฝ่ายสามารถนำระบบงานชนิดใหม่เข้ามาปฏิบัติงานทดแทนระบบเก่าได้ถูกต้องตามลำดับ ส่วนการพิจารณาตัดสินใจนำโปรแกรมใหม่เข้าสู่ระบบเพื่อใช้งานนั้น ขึ้นอยู่กับความสมบูรณ์ของการทดสอบระบบงาน การปฏิบัติงานคู่ขนาน และเอกสารที่เกี่ยวกับการปฏิบัติงานทางด้านคอมพิวเตอร์ เช่น เอกสารเกี่ยวกับโปรแกรม การใช้เครื่อง และผู้ใช้ข้อมูล เป็นสำคัญ



การ Catalog โปรแกรม



แผนภาพที่ 20.5 การ catalog โปรแกรม

ในการ Catalog โปรแกรม และการใช้ Compiler และ Linkage Editor แปลงรูป Source Program ให้เป็นภาษาเครื่องจักรที่ใช้ประมวลผลได้ทันทีนั้น หากมีการทดสอบโปรแกรมในระบบ On-line จะต้องมีการป้องกันมิให้มีการเปลี่ยนสภาพของ Test Program ที่อยู่ใน Program Library File ไปเป็นโปรแกรมใช้งาน (Production Program) โดยมิได้รับอนุญาต ตามปกติโปรแกรมที่ถูกแก้ไขจะถูกลบทิ้ง แต่ส่วนใหญ่นิยมเก็บสำรองไว้เป็น Back-up File ในบางกรณีอาจใช้วิธีโอนโปรแกรมทั้งชนิด Source Program และ Executable Program จาก Test Library เข้าสู่ Production Library จึงจำเป็นต้องควบคุม Source Program เช่นเดียวกับ Executable Program ด้วย เมื่อมีการแก้ไขจะแก้ไขจาก Source Program เพื่อป้องกันข้อผิดพลาด ในระบบเก่าที่เก็บโปรแกรมไว้ในห้องเก็บ จำเป็นต้องใช้ Control Manual เข้าช่วย เพื่อให้แน่ใจว่าโปรแกรมชุดเก่าที่ถูกแก้ไขถูกทำลายหรือถูกเก็บเป็น Back-up และไม่นำมาใช้ประมวลผลอีกต่อไป

รายละเอียดที่คอมพิวเตอร์พิมพ์ให้จากการ Catalog จะประกอบด้วยรายชื่อโปรแกรมจาก Test Library ที่โอนเข้าสู่ Production Library และรายละเอียดของ Source program (Source Listing) ที่นำไปใช้เป็น Production Program ควรตรวจสอบโดยละเอียด เพื่อให้แน่ใจว่าไม่มีการแก้ไขนอกเหนือไปจากคำขออนุมัติและการแก้ไขเป็นไปด้วยความเหมาะสม

โดยปกติผู้ตรวจสอบจะปล่อยให้เป็นหน้าที่ของธนาคาร ที่จะต้องแก้ไข Software ที่ผิดพลาดที่ได้จากการทดสอบเอง

คำถามเพื่อประเมินผลการควบคุมภายในเกี่ยวกับการ Catalog มีดังนี้

1) มีเจ้าหน้าที่ของฝ่ายผู้ใช้ข้อมูลตรวจสอบการใช้งาน และอนุมัติในเรื่องต่าง ๆ ดังต่อไปนี้ หรือไม่

   1.1) ระเบียบการควบคุมและการปฏิบัติงานทางด้านผู้ใช้ข้อมูล
   1.2) ผลการทดสอบและความสำเร็จในการทดสอบ
   1.3) วันที่โอน Test Program ไปเป็น Production Program

2) เจ้าหน้าที่ผู้รับผิดชอบในการประมวลผลตรวจสอบการใช้งานและอนุมัติในเรื่องต่าง ๆ ดังต่อไปนี้ หรือไม่

   2.1) ความสมบูรณ์ การแก้ไขความถูกต้องอยู่เสมอ และมาตรฐานของเอกสารเกี่ยวกับโปรแกรมและระบบงาน
   2.2) ประโยคคำสั่งเกี่ยวกับ Job Set-up ที่ใช้ประมวลผล
   2.3) ผลการทดสอบและความสำเร็จในการทดสอบ
   2.4) การนำ Test Program ไปใช้เป็น Production Program

3) System Software Procedures ในเรื่องต่าง ๆ ดังต่อไปนี้มีความเหมาะสม หรือไม่

3.1) การทดสอบและการเปลี่ยนรูป Source program ให้เป็นภาษาเครื่องจักรที่ใช้ประมวลผลได้ทันที (โดยให้ compiler และ Linkage Editor)

3.2) การนำโปรแกรมชุดที่แก้ไขถูกต้องแล้วไปเป็น Production Program (เช่น มีการตรวจสอบหมายเลขโปรแกรมที่สร้างขึ้นมา)

3.3) การขออนุมัติแก้ไข Test Program ที่จะใช้เป็น Production Program

3.4) มีการกำหนดรูปแบบให้เหมือนกันทุกโปรแกรม (ไม่ว่าจะเป็นโปรแกรมชนิด Source, Object และ Executable)

4) ให้ทบทวนคำตอบที่ได้จากการสอบถามในเรื่อง System Software เพื่อพิจารณาว่ามีการควบคุม การพัฒนา และรักษาความปลอดภัย System Software อย่างเพียงพอ หรือไม่

5) มีเอกสารหลักฐานเกี่ยวกับ System Software Procedures อย่างเพียงพอ หรือไม่ และเอกสารเหล่านี้มีบุคคลอื่นนอกจากผู้มีหน้าที่ด้าน System Software หรือผู้ปฏิบัติงานในห้องคอมพิวเตอร์เป็นผู้ตรวจสอบหรือไม่

6) มีการควบคุมคู่มือปฏิบัติงานเกี่ยวกับการ Catalog อย่างเพียงพอหรือไม่

7) มีพนักงานชั้นบริหารตรวจสอบและอนุมัติผลการปฏิบัติงานตามข้อ 5 และข้อ 6 หรือไม่

การแก้ไขโปรแกรมอย่างฉุกเฉิน

ในบางครั้งการแก้ไข Production Program อาจจำเป็นต้องปฏิบัติแตกต่างไปจากกระบวนการที่กล่าวไว้ข้างต้นก็ได้ เช่น ในกรณีถึงกำหนดประมวลผลหรือมีปัญหาเกิดขึ้นในเวลากลางคืน และมีพนักงานอยู่ปฏิบัติงานในช่วงนั้นน้อย จึงจำเป็นต้องมีการควบคุมเพื่อติดตามการอนุมัติการแก้ไข การทดสอบ และกระบวนการพัฒนาโปรแกรมอย่างใกล้ชิด

การสอบถามเกี่ยวกับการแก้ไขโปรแกรมอย่างฉุกเฉิน มีดังนี้

1) ในกรณีที่มีการแก้ไข Production Program อย่างฉุกเฉิน โดยละเว้นขั้นตอนที่ปฏิบัติกันตามปกตินั้น มีกระบวนการที่ช่วยให้แน่ใจว่าการแก้ไขนั้นถูกต้อง และได้รับความเห็นชอบหรือไม่

2) มีการตรวจสอบกระบวนการที่กล่าวตามข้อ 1 และมีการอนุมัติโดยพนักงานที่มีหน้าที่รับผิดชอบ หรือไม่

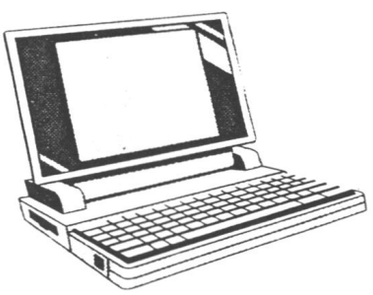
5. การควบคุมและการรักษาความปลอดภัยเกี่ยวกับตัวโปรแกรม (Program Security Controls)

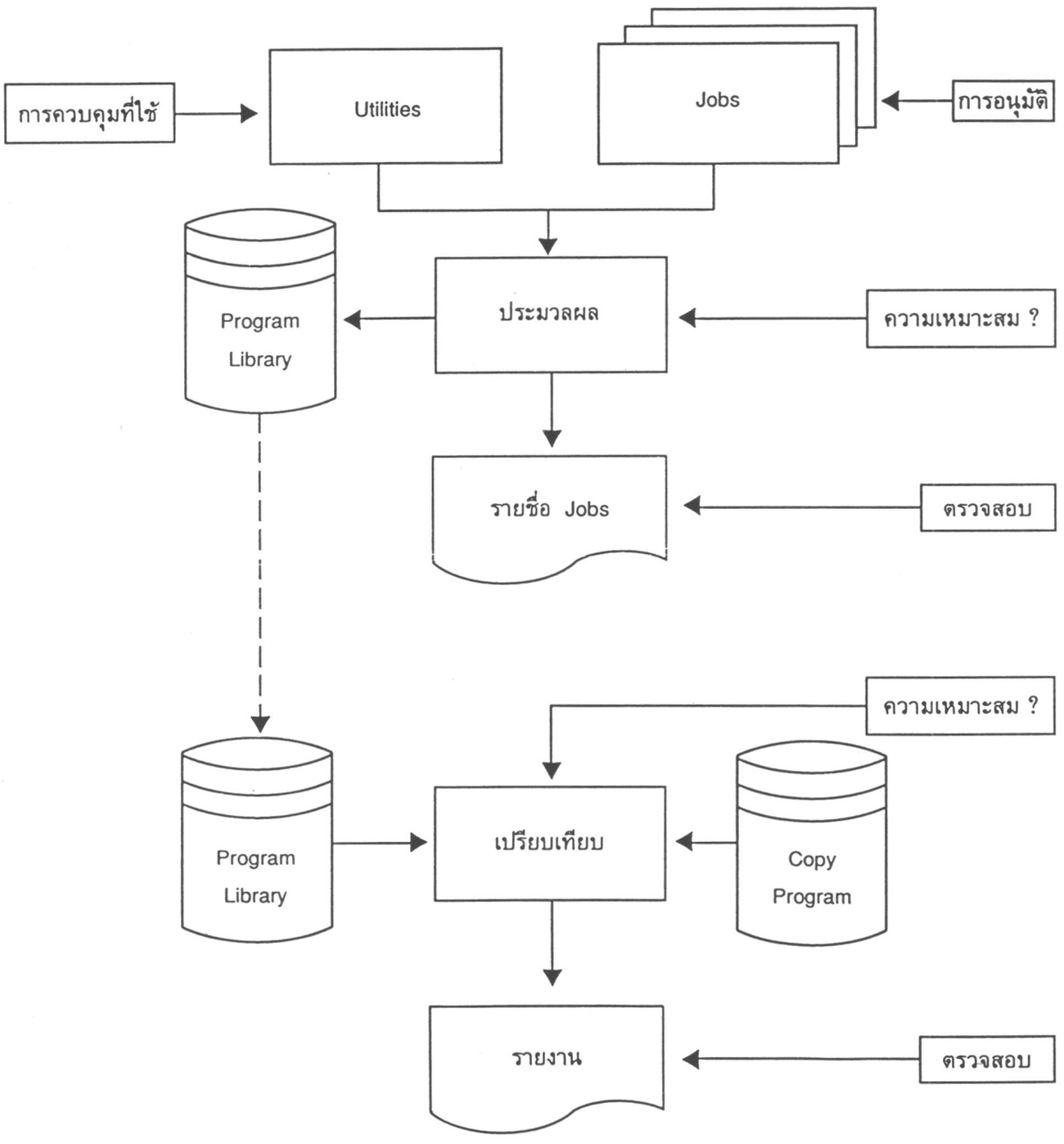
การควบคุมรักษาความปลอดภัยเกี่ยวกับตัวโปรแกรม ได้แก่ การควบคุมมิให้สามารถแก้ไข Production Program ที่ใช้ในการประมวลข้อมูลทางบัญชีโดยมิได้รับอนุญาต แต่ไม่รวมถึงการแก้ไขโปรแกรมที่อยู่ในระหว่างการพัฒนา ทั้งนี้ควรตระหนักอยู่เสมอว่า โปรแกรมที่ถูกแก้ไขโดยมิได้รับอนุญาตอาจเป็นประโยชน์ต่อผู้แก้ไขไม่มากก็น้อย เช่น ในระบบเงินเดือนและระบบจ่ายเงินสด จึงจำเป็นต้องตรวจสอบเพื่อให้แน่ใจว่า การควบคุมรักษาความปลอดภัยของธนาคารมีความเหมาะสมและเชื่อถือได้เพียงใด จนเป็นที่พอใจแต่ไม่จำเป็นต้องขยายการทดสอบไปถึงกระบวนการจัดทำโปรแกรม

โปรแกรมที่มีการควบคุมรักษาความปลอดภัยมีสองชนิด คือ โปรแกรมชนิดที่อยู่ระหว่างการใช้งาน บรรจุอยู่ในระบบคอมพิวเตอร์พร้อมที่จะประมวลผล และชนิดเก็บไว้ที่อื่นไม่บรรจุอยู่ในระบบคอมพิวเตอร์ ซึ่งตามปกติจะเก็บไว้ในห้องเก็บโปรแกรม และแฟ้มข้อมูลต่าง ๆ ที่ยังไม่ได้ใช้งาน

5.1 การควบคุมรักษาความปลอดภัยโปรแกรมที่อยู่ในระหว่างการใช้งาน

การแก้ไขโปรแกรมโดยไม่ได้รับอนุญาต ส่วนใหญ่จะใช้วิธีแจ้งว่าเป็น Job ที่ต้องใช้คอมพิวเตอร์ปฏิบัติงานเพื่อวัตถุประสงค์บางอย่างตามคำสั่งของผู้ใช้ข้อมูล หรือพนักงานในศูนย์คอมพิวเตอร์ โดยเฉพาะ Job ที่มีการ Compile จาก Source program ให้เป็น Executable program อาจมีการแก้ไขโปรแกรมโดยไม่ขออนุญาตรวมอยู่ด้วย จึงควรตรวจสอบการปฏิบัติงานทุก Job โดยตรวจจากรายงานแสดงการปฏิบัติงานในแต่ละ Job ที่คอมพิวเตอร์พิมพ์มาให้เปรียบเทียบกับตารางกำหนดการปฏิบัติงาน (Job Schedules) เพื่อดูว่ามีการนำเอา Production Program อื่นนอกจากที่กำหนดไว้ในตารางมาใช้ประมวลผลหรือไม่ นอกจากนี้ควรควบคุมการใช้ Utilities Program ที่ใช้ในการแก้ไข Executable Programs ด้วย





แผนภาพที่ 20.6 แสดงการควบคุมรักษาความปลอดภัยโปรแกรมที่อยู่ในระหว่างการใช้งาน

สำหรับคอมพิวเตอร์ขนาดเล็กจะไม่มีการพิมพ์รายชื่อ Job ที่เข้าประมวลผล จะตรวจสอบได้จากเวลาที่มีการอนุมัติ Job ตั้งแต่ขั้นเริ่มพัฒนางาน จนถึงขั้นส่งงานให้ Operator รับผิดชอบในการปฏิบัติงานประมวลผล อย่างไรก็ดีจะต้องไม่มีการแก้ไข Job ภายหลังการ Set-up งานอีก เพื่อให้แน่ใจว่าไม่มี Job ที่ไม่ได้รับอนุญาตให้ใช้ถูกเพิ่มเติมเข้าไปอีก ควรตรวจสอบรายงานการปฏิบัติงานใน Job ต่าง ๆ ของหัวหน้า Operator ด้วย นอกจากนี้อาจเลือกใช้วิธีกำหนดให้พนักงานชั้นบริหารควบคุมดูแลการประมวลผลทุก Job และการแก้ไข Production program อย่างใกล้ชิดด้วยตนเองตลอดเวลา

ในกรณีที่ไม่สามารถใช้วิธีการควบคุมตามที่กล่าวไว้ อาจใช้วิธีเปรียบเทียบ Production Program กับโปรแกรมชุดสำเนาที่เก็บแยกไว้ในห้องเก็บโปรแกรม หรือสถานที่อื่นนอกศูนย์คอมพิวเตอร์ โดยปกติผู้ตรวจสอบภายในจะเป็นผู้ควบคุมดูแลการเปรียบเทียบโปรแกรม และในกรณีที่การป้องกันการแก้ไขโปรแกรมมีความสำคัญต่อการปฏิบัติงานบางอย่างของธนาคารมาก อาจต้องทำการเปรียบเทียบทุกวันก่อนการประมวลผล

สำหรับคอมพิวเตอร์ขนาดเล็ก ผู้ที่มีหน้าที่รับผิดชอบอาจต้องดำเนินการทดสอบข้อมูลด้วยตนเองเป็นครั้งคราว เพื่อป้องกันการแก้ไขโปรแกรมโดยไม่ได้รับอนุญาต

โปรแกรมที่ใช้ในการประมวลผลควรมีรหัสลับ (Pass words) ควบคุมการใช้โปรแกรม ทั้งในกรณีที่ใช้ในการประมวลข้อมูลและแก้ไขโปรแกรม โดยเฉพาะในกรณีที่ใช้เครื่อง Terminal แก้ไขโปรแกรม ซึ่งวิธีการควบคุมและกระบวนการแก้ไขโปรแกรมขึ้นอยู่กับชนิดของเครื่อง Terminal และรหัสลับที่ใช้

ควรห้ามใช้ Production Program โดยมิได้รับอนุญาตในช่วงที่ไม่ได้ทำการประมวลผลจริง และควรควบคุมอย่างเคร่งครัด การควบคุมดังกล่าวอาจรวมถึงการนำโปรแกรมออกจากเครื่องคอมพิวเตอร์ไปเก็บไว้ใน Library หรือควบคุม Operator ในช่วงเวลาที่ไม่ได้ประมวลผลจริงด้วย

คำถามที่ใช้ในการสอบถามมีดังนี้

1) มีการควบคุมมิให้มีการแก้ไข production program ในขณะที่นำออกไปใช้งานโดยมิได้รับอนุญาตดังต่อไปนี้ หรือไม่
   1.1) มีเจ้าหน้าที่ตรวจสอบรายงานการปฏิบัติงานในแต่ละ Job ที่คอมพิวเตอร์พิมพ์มาให้ หรือไม่
   ถ้ามี ให้ตอบคำถามในข้อ 2 ถึงข้อ 4
   1.2) มีเจ้าหน้าที่อนุมัติการปฏิบัติงานในแต่ละ Job ก่อนดำเนินการประมวลผล หรือไม่
   ถ้ามี ให้ตอบคำถามในข้อ 5 และข้อ 6
   1.3) มีการเปรียบเทียบ Production Program กับโปรแกรมชุดสำเนา ซึ่งเก็บแยกไว้ต่างหากสำหรับการควบคุม หรือไม่ (Program Comparisons)
   ถ้ามี ให้ตอบคำถามในข้อ 7 ถึงข้อ 10
   1.4) มีการใช้รหัสลับป้องกัน Production Program หรือไม่

2) System Software Procedures ที่ใช้สามารถรายงานการใช้ Production Program ได้ทุกโปรแกรม หรือไม่

3) ให้ดูคำถามเกี่ยวกับ System Software เพื่อทบทวนความเพียงพอในการควบคุมการพัฒนาและแก้ไขโปรแกรมก่อนใช้งาน และการควบคุมรักษาความปลอดภัย System Software ที่เป็น Production แล้ว

4) มีกระบวนการตรวจสอบรายงานแสดงการปฏิบัติงานประมวลผลในแต่ละ Job ที่เพียงพอหรือไม่

5) ในการอนุมัติให้ปฏิบัติงานในแต่ละ Job มีเอกสารอื่นที่จะใช้เป็นหลักฐานยืนยันการอนุมัติหรือไม่ (เช่น ตารางงานประมวลผล (Processing Schedules) ที่ผ่านการอนุมัติแล้ว)

6) มีการควบคุมดังต่อไปนี้อย่างเพียงพอ หรือไม่

   6.1) การควบคุมการแก้ไขโปรแกรมโดยมิได้รับอนุญาตหลังจากที่ได้รับอนุมัติให้ปฏิบัติงานตาม Job

   6.2) การควบคุมการเพิ่ม Job ที่ไม่ได้รับอนุมัติให้ประมวลผล

7) การเปรียบเทียบโปรแกรม (Program Comparisons) ใช้วิธีไม่บอกให้ทราบล่วงหน้า (Surprise Basis) หรือไม่

8) System Software Procedures ที่ใช้ในการเปรียบเทียบโปรแกรมเหมาะสม หรือไม่

9) ให้ดูคำถามเกี่ยวกับ System Software เพื่อทบทวนถึงความเพียงพอในการควบคุมการพัฒนาและแก้ไขโปรแกรมก่อนใช้งาน และการควบคุมรักษาความปลอดภัย System Software ที่เป็น Production แล้ว

10) มีวิธีการตรวจสอบเพื่อหาข้อแตกต่างที่เหมาะสม หรือไม่

11) มีบุคคลอื่นที่ไม่ได้ทำหน้าที่ภายในห้องคอมพิวเตอร์ออกแบบระบบงานและเขียนโปรแกรมปฏิบัติงานดังต่อไปนี้ หรือไม่

   11.1) ตรวจสอบการประมวลผลในแต่ละ Job

   11.2) อนุมัติ Job ก่อนนำเข้าประมวลผล

   11.3) ตรวจสอบหาข้อแตกต่างจากการเปรียบเทียบโปรแกรม

12) มีพนักงานชั้นบริหารของธนาคารรับผิดชอบตรวจสอบและอนุมัติผลการปฏิบัติงานดังต่อไปนี้ หรือไม่

   12.1) การตรวจสอบการประมวลผลในแต่ละ Job

   12.2) การอนุมัติ Job ก่อนนำเข้าประมวลผล

   12.3) การตรวจสอบหาข้อแตกต่างจากการเปรียบเทียบโปรแกรม

13) มีการควบคุมโปรแกรมประเภท Non-Production ในช่วงที่ไม่ได้ประมวลผลจริงหรือไม่ (เช่น การเคลื่อนย้ายโปรแกรมไปเก็บไว้ในห้องเก็บโปรแกรม หรือการปฏิบัติงานของ Operator ในช่วงที่ไม่ได้ประมวลผลจริง)

5.2 การควบคุมและเก็บรักษา Utility Programs

เนื่องจาก Utility Programs ที่ได้มาจากผู้ผลิตคอมพิวเตอร์หรือบริษัทผู้ผลิต System Software ว่าหน่วยนี้สามารถแก้ไข Executable Program ได้โดยตรง จึงควรมีเจ้าหน้าที่รับผิดชอบในการเก็บรักษา สำหรับ Utility Programs ที่ไม่ใช้ในการปฏิบัติงานประจำ ควรส่งคืนบริษัทผู้ผลิตหรือมอบหมายให้เจ้าหน้าที่ชั้นบริหารระดับสูงด้าน System Software เป็นผู้รับผิดชอบในการเก็บรักษา และอนุญาตให้ใช้เฉพาะการปรับปรุงแก้ไข Operating System ที่ใช้ควบคุมให้คอมพิวเตอร์ปฏิบัติงานตามโปรแกรมใช้งานเท่านั้น ซึ่งสามารถตรวจสอบการอนุมัติใช้ Utility Programs ได้จาก System Log นอกจากนี้ผู้ตรวจสอบภายในยังสามารถใช้ Utility Programs ในการเปรียบเทียบ Executable Program และ Source Program ด้วย

เพื่อป้องกัน Operator แก้ไข Production Program ควรแบ่งแยกหน้าที่กันโดยเด็ดขาด และไม่ให้ Operator ทราบรายละเอียดเกี่ยวกับตัวโปรแกรม นอกจากนี้จะต้องป้องกันผู้ที่มีหน้าที่รับผิดชอบในการพัฒนาปรับปรุง แก้ไขโปรแกรมที่ยังไม่ได้นำมาใช้งานไม่ให้สามารถแก้ไข Production Program ได้ การแบ่งแยกหน้าที่เป็นเรื่องที่สำคัญที่ต้องกระทำอยู่ตลอดเวลา รวมทั้งในช่วงที่มีการปฏิบัติงานนอกเวลาทำการด้วย

คำถามที่ใช้สอบถามมีดังนี้

1) มีการกำหนดตัวผู้มีอำนาจใช้ Utility Programs ที่สามารถแก้ไข Production Programs หรือไม่

2) มีรายงานการใช้ Utility Programs ให้ผู้ที่มีหน้าที่รับผิดชอบในการประมวลผลตรวจสอบหรือไม่

3) มีการห้าม Operator ผู้ที่มีหน้าที่รับผิดชอบในการเก็บรักษาคำสั่งเกี่ยวกับ Job Control ผู้ปฏิบัติงานอื่นในห้องคอมพิวเตอร์ และผู้รับผิดชอบในการประมวลผลจริง ไม่ให้เกี่ยวข้องกับเรื่องต่าง ๆ ดังต่อ ไปนี้ หรือไม่

   3.1) เขียนและปรับปรุงแก้ไข Production Programs และ System Software
   3.2) นำ Source Listings, Flowcharts ผังแสดงตำแหน่งข้อมูลที่เก็บไว้ในแฟ้มข้อมูล (File Layouts) และเอกสารที่เกี่ยวกับโปรแกรมไปใช้งาน

4) มีการห้ามผู้วิเคราะห์ระบบ (System Analysts) และผู้เขียนโปรแกรมทั้ง Production Program และ System Software ไม่ให้เข้าไปในห้องคอมพิวเตอร์ หรือไม่

5) ข้อห้ามตามข้อ 3) และข้อ 4) ใช้บังคับนอกเวลาทำการ (เช่น วันหยุดสุดสัปดาห์) และในช่วงที่ได้ประมวลผลจริง (เช่น ในช่วงทดสอบโปรแกรม) ด้วย หรือไม่

5.3 การควบคุมรักษาโปรแกรมที่ไม่ได้ใช้งาน

โปรแกรมที่ไม่ได้ใช้งานควรควบคุมและเก็บรักษาไว้ในห้องเก็บโดยเฉพาะ (Physical Library) การนำออกใช้งานควรมีการขออนุมัติและส่งคืนทันทีที่ใช้งานเสร็จ สำหรับสำเนาโปรแกรมชุดสำรอง (Back-up Copies of Program) และเอกสารเกี่ยวกับโปรแกรม ควรมีการป้องกันเพื่อหลีกเลี่ยงบุคคลอื่นที่ไม่มีสิทธิใช้ทราบรายละเอียดภายในโปรแกรม การควบคุม Back-up Copies of Program นี้มีความสำคัญมาก โดยเฉพาะในกรณีที่ใช้วิธีการควบคุมโดยการเปรียบเทียบโปรแกรม ควรเก็บรักษาโปรแกรมดังกล่าวใน Library หรือสถานที่อื่นนอกศูนย์คอมพิวเตอร์ และมีเจ้าหน้าที่รับผิดชอบในการใช้งานโดยตรง



21

การประเมินการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (2)

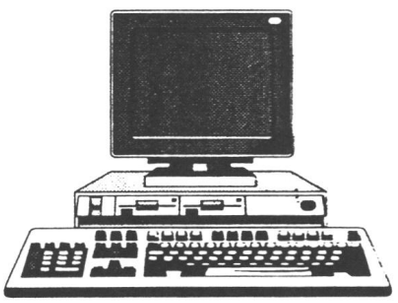
การประเมินการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (2)

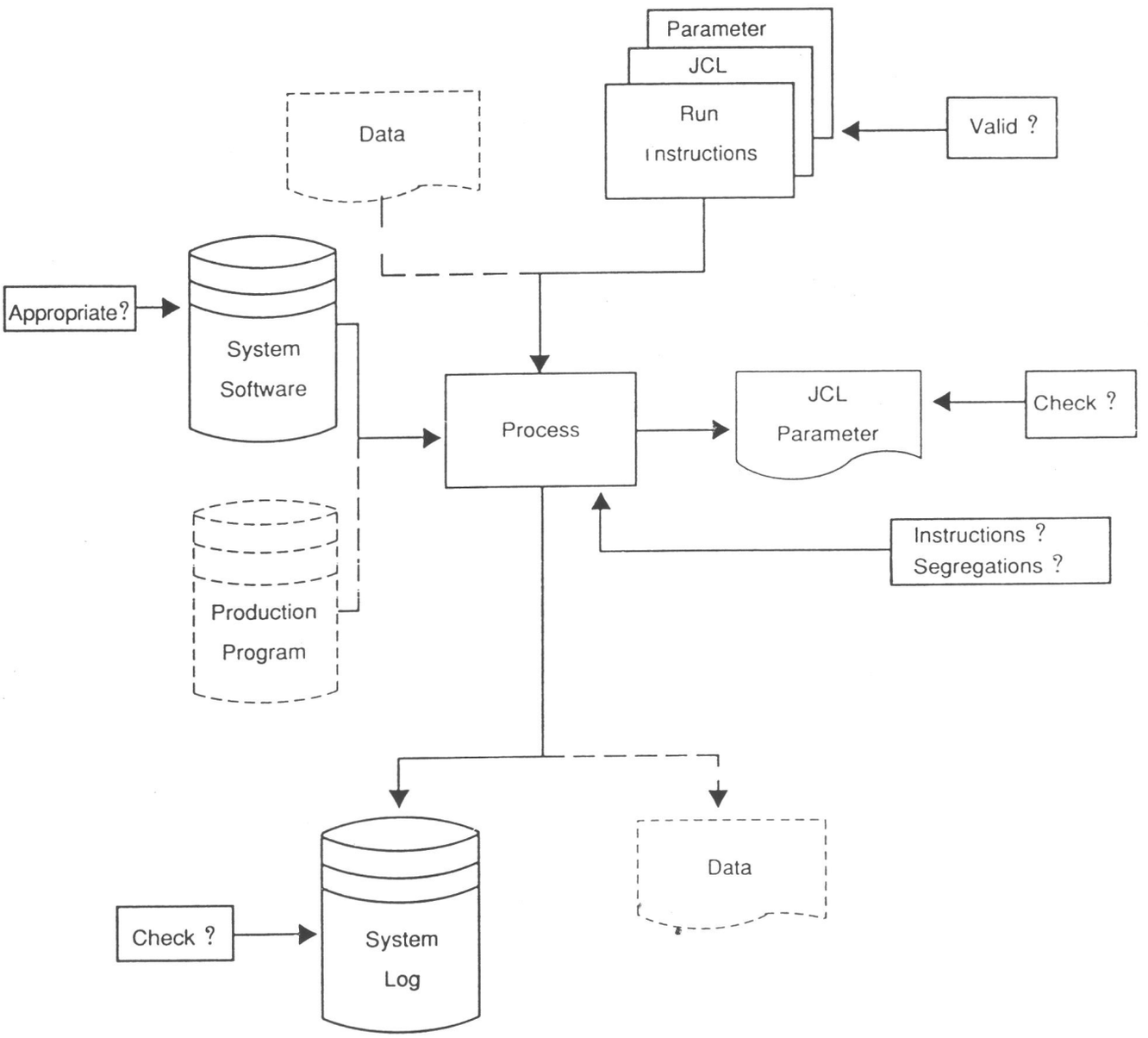
1. คำนำ

ในที่นี้จะกล่าวถึงรายละเอียดของการควบคุมที่จำเป็น และเทคนิคต่าง ๆ ที่ใช้ในการควบคุมการใช้เครื่องคอมพิวเตอร์ (Computer Operations Controls) ตลอดจนการรักษาความปลอดภัยของแฟ้มข้อมูล (Data File) และโปรแกรมควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ (System Software) และจะได้กล่าวถึงวิธีการประเมินผลการควบคุมและรักษาความปลอดภัยดังกล่าวจากการใช้แบบสอบถามการควบคุมภายใน

2. การควบคุมการใช้เครื่องคอมพิวเตอร์ (Computer Operation Controls)

การควบคุมการใช้เครื่องคอมพิวเตอร์ กำหนดขึ้นเพื่อความมั่นใจว่าขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ที่ใช้ในการประมวลผลข้อมูลมีความถูกต้องแน่นอนและสม่ำเสมอ รวมทั้งการควบคุมการปฏิบัติงานทั้งหมดในศูนย์คอมพิวเตอร์ เช่น การควบคุมวัสดุที่จำเป็นต้องใช้เป็นประจำ การควบคุมการใช้แฟ้มข้อมูลในการประมวลผลให้ถูกต้อง และการควบคุมการแก้ไขรายการที่ผิดพลาด การปฏิบัติงานและการควบคุมที่ได้กล่าวข้างต้นจะได้กล่าวเป็นลำดับไปภายใต้หัวข้อ Job Set-up โปรแกรมควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ และการใช้เครื่องคอมพิวเตอร์ (Operations Software and Computer Operating) การใช้แฟ้มข้อมูลที่ถูกต้อง (Use of Correct Data File) และการแก้ไขข้อผิดพลาด (Recovery from Processing Failure) การควบคุมการทำงานของเครื่องคอมพิวเตอร์แสดงไว้ตามแผนภาพ





แผนภาพที่ 21.1 การควบคุมการใช้คอมพิวเตอร์ (Computer Operations Controls)

2.1 Job Set-up

หมายถึง การกำหนดชื่อเพื่อกำกับอุปกรณ์ต่าง ๆ ที่จำเป็นต้องใช้ในการประมวลผล ซึ่งได้แก่ อุปกรณ์ (Devices) ที่ใช้สำหรับโปรแกรมและข้อมูล คำสั่งที่ใช้ควบคุมการประมวลผลในแต่ละงาน (Job Control Statement) คำสั่งที่ใช้ในการเดินเครื่องคอมพิวเตอร์ (Run Instructions) และการ์ดตัวแปรที่ใช้ในการประมวลผล (Parameter Cards) ในระบบคอมพิวเตอร์ที่ก้าวหน้า ความจำเป็นในการใช้อุปกรณ์ดังกล่าวลดน้อยลง เนื่องจากมี Program Library สำหรับเก็บโปรแกรมที่ใช้ประมวลผล และแฟ้มข้อมูลส่วนใหญ่จะพัฒนาให้อยู่ในรูปของระบบ On-line

Job Control Statement หรือ Job Control Language (JCL) เป็นคำสั่งที่กำหนดให้เครื่องคอมพิวเตอร์ใช้โปรแกรมและแฟ้มข้อมูลในการประมวลผลให้เป็นไปตามลำดับความต้องการของผู้ใช้เครื่องคอมพิวเตอร์ โดยปกติคำสั่งเหล่านี้จะอยู่ในรูปของการ์ดที่เจาะไว้ (Punched Card) แต่ในระบบคอมพิวเตอร์ที่ก้าวหน้ามาก สามารถนำเข้าเครื่องไปเก็บไว้ในจานแม่เหล็ก (Disk) เพื่อใช้งานแบบ On-line โดยเรียก Job Control Statement มาทำงานได้ เพียงแต่ใช้การ์ดรหัสเพียงแผ่นเดียวเรียกเข้าไป หรือโดยกดรหัสผ่านเครื่อง Terminal

สำหรับ Run Instructions จะประกอบด้วยคำสั่ง 2 ประเภท คือ Program Operating Instructions และ Processing Instructions คำสั่งประเภทแรกเป็นคำสั่งที่ผู้ควบคุมเครื่องคอมพิวเตอร์ (Operator) จะต้องปฏิบัติตามขั้นตอนที่กำหนดในโปรแกรมทั้งก่อนการทำงาน ระหว่างการทำงาน และเมื่อสิ้นสุดการทำงานแต่ละโปรแกรม ส่วนคำสั่งประเภทหลังเป็นคำสั่งที่ให้รายละเอียดของชุดโปรแกรมทั้งหมด ซึ่งได้แก่ โปรแกรมแฟ้มข้อมูล แบบฟอร์ม และสิ่งพิมพ์ต่าง ๆ ที่จะต้องใช้ในงานนั้น นอกจากนี้ Run Instructions จะรวมถึง Standard Operation Instructions ที่กำหนดให้ใช้เป็นมาตรฐานในการปฏิบัติงานประมวลผลโดยทั่วไปทุกงานด้วย

การ์ดตัวแปรที่ใช้ในการประมวลผล (Parameter Cards) เป็นการ์ดที่ระบุข้อมูลที่จำเป็นต้องเปลี่ยนแปลงไปเป็นปกติ เช่น วันที่ ซึ่งจำเป็นต้องใช้ในการสร้างข้อมูลบนเช็คสั่งจ่าย หรือใช้ในการแยกเช็ค หรือจำแนกอายุลูกหนี้ เป็นต้น นอกจากนั้นตัวแปร (Parameter) ยังใช้เพื่อบ่งบอกการทำงานตามขั้นตอนของโปรแกรมตามรอบระยะเวลาที่กำหนด เช่น การพิมพ์รายละเอียดของบัญชีลูกค้ารายตัว (Customer Statements) เป็นต้น

การควบคุมการใช้เครื่องคอมพิวเตอร์ (Computer Operations Control) จำเป็นต้องให้ความสำคัญต่อ Job Set-up เพื่อความมั่นใจว่าการจัดทำ Job Control Statement และตัวแปร (Parameters) มีความเหมาะสมอย่างเพียงพอ โดยปกติแล้วการจัดเตรียมอุปกรณ์ (Devices) ที่จะใช้ในการประมวลผลมีความสำคัญค่อนข้างน้อย เพราะจำเป็นที่จะตรวจสอบความถูกต้องของโปรแกรมและแฟ้มข้อมูลที่จะใช้เสียก่อนที่จะเริ่มทำการประมวลผล อย่างไรก็ตามข้อผิดพลาดอันเนื่องมาจากตัวแปร (Parameter) และ Job Control Statement มักจะไม่ปรากฏให้เป็นที่สังเกตได้ โดยปกติในกรณีที่ไม่สามารถตรวจสอบกับผลลัพธ์จากการประมวลผลได้ การใช้ Job Control Statement ที่ไม่ถูกต้องจะทำให้โปรแกรมทำงานผิดขั้นตอนหรือผิดพลาดไปเลย นอกจากนั้น Job Control Statement อาจแทรกเป็นส่วนหนึ่งของโปรแกรมประมวลผลก็ได้ด้วยเหตุผลเหล่านี้ การควบคุม Job Set-up จึงเป็นสิ่งสำคัญ

เพื่อให้แน่ใจว่า Job Control Statement และ Parameter ที่จะใช้ในการประมวลผลมีความถูกต้อง ควรกำหนดให้มีการตรวจสอบและขออนุมัติก่อนนำออกใช้งาน

การจัดทำคำสั่งเกี่ยวกับ Job Set-up ควรกระทำในขั้นตอนการพัฒนาระบบงานในครั้งแรก และเมื่อมีการแก้ไขโปรแกรมจะต้องปรับปรุงแก้ไขคำสั่งเหล่านี้ให้ถูกต้องอยู่เสมอด้วย โดยมีพนักงานผู้มีหน้าที่รับผิดชอบตรวจสอบก่อนที่จะดำเนินการ Catalog โปรแกรม

ควรกำหนดให้มีการอนุมัติแก้ไข Job Control Statement ทุกครั้ง และมีการป้องกันไม่ให้รายละเอียดของคำสั่งเหล่านั้น และ Parameter รั่วไหลไปสู่ผู้ที่ไม่มีอำนาจแก้ไข การแก้ไข Parameter ที่เกี่ยวข้องกับข้อมูลทางการบัญชีจะต้องได้รับการรับรองจากผู้บริหารของฝ่ายผู้ใช้ข้อมูลก่อน รายละเอียดในการแก้ไขและการอนุมัติให้ดำเนินการแก้ไขจะต้องเก็บรักษาไว้ในที่เดียวกับชุดคำสั่งที่แก้ไข พนักงานผู้มีหน้าที่รับผิดชอบงานด้านนี้จะต้องตรวจสอบความสมบูรณ์ และความถูกต้องของชุดคำสั่ง โดยเฉพาะจุดที่มีการแก้ไขเป็นครั้งคราว

ทุกครั้งที่มีการประมวลผล เครื่องคอมพิวเตอร์จะพิมพ์รายละเอียดของ Job Control Statement และ Parameter ด้วย ควรให้พนักงานอื่นที่ไม่มีหน้าที่รับผิดชอบหรือมีอำนาจในการใช้ Job Set-up ในการปฏิบัติงาน นำรายละเอียดเหล่านี้ไปตรวจสอบกับชุดจริง สำหรับ Parameter ที่มีความสำคัญ เช่น อัตราแลก-เปลี่ยนเงินตราหรืออัตราดอกเบี้ย จะต้องให้ผู้ใช้ข้อมูลที่เกี่ยวข้องตรวจสอบความถูกต้องเสียก่อน

เรื่องที่ควรซักถามเพื่อประเมินระบบควบคุมภายในส่วนที่เกี่ยวกับ Job Set-up มีดังนี้

1) Job Set-up Instruction (เช่น รายละเอียดของ JCL Parameter และวิธีการใช้เครื่องคอมพิวเตอร์ปฏิบัติงานทุกขั้นตอน) เพียงพอสำหรับ
   - งานแต่ละงาน (Each Application) หรือไม่
   - โปรแกรมควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ (System Software) หรือไม่

2) การแก้ไขคำสั่งเหล่านี้ทุกชนิดต้องขออนุมัติจากผู้บริหาร หรือไม่

3) มีการควบคุมเพื่อให้แน่ใจว่าคำสั่งต่าง ๆ เหล่านี้มีความสมบูรณ์และถูกต้องอยู่เสมอ (เช่น ความเป็นอิสระในการตรวจสอบที่กระทำเป็นครั้งคราว) อย่างเพียงพอหรือไม่

4) มีการควบคุมการใช้ Job Control Statement และ Parameter ในการประมวลผลเพื่อให้เป็นไปตามข้อกำหนดที่วางไว้อย่างเพียงพอหรือไม่ (เช่น มีการตรวจสอบการใช้ Job Control Statement และ Parameter จากรายงานที่เครื่องคอมพิวเตอร์พิมพ์ให้เป็นครั้งคราว)

5) มีบุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องกับ Job Set-up หรือเป็นผู้ควบคุมการทำงานของเครื่องคอมพิวเตอร์ตรวจสอบการใช้ Job Control Statement และ Parameter หรือไม่

6) มีพนักงานชั้นบริหารผู้มีหน้าที่รับผิดชอบสอบทานและรับทราบผลการปฏิบัติงานในข้อ (4) หรือไม่

2.2 โปรแกรมควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ และการใช้เครื่องคอมพิวเตอร์ (Operations Software and Computer Operating)

การบริหารและการควบคุมกิจกรรมในการประมวลผลด้วยคอมพิวเตอร์จำเป็นต้องใช้บุคคลและโปรแกรมคอมพิวเตอร์ดำเนินการ แต่ในระบบคอมพิวเตอร์ที่ก้าวหน้ามาก ๆ จะใช้โปรแกรมคอมพิวเตอร์ให้ทำหน้าที่เหล่านี้มากขึ้น งานในหน้าที่ต่าง ๆ ที่กระทำโดยบุคคลจะลดลง สิ่งสำคัญที่ควรพิจารณาเกี่ยวกับการควบคุมคือ โปรแกรมควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ (System Software) ที่ใช้จะต้องเชื่อถือได้ วิธีการปฏิบัติงานด้วยมือหรือโดยบุคคลจะต้องไม่มีข้อผิดพลาด หรือมีปัญหาที่อาจมีผลกระทบต่อการประมวลผล

โปรแกรมควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ (System Software) หรือ Operating System ประกอบด้วยโปรแกรมย่อย ๆ หลายชุด (module) ซึ่งอาจมีชื่อเรียกแตกต่างกันในแต่ละบริษัทผู้ผลิต เช่น Control Module, Supervisor, Monitor และ Executive เป็นต้น Operating System คือ โปรแกรมที่เก็บไว้ในเครื่องคอมพิวเตอร์ตลอดเวลาที่เครื่องคอมพิวเตอร์ทำงานเพื่อทำหน้าที่ควบคุมการทำงานของโปรแกรมที่ผู้ใช้เครื่องต้องการ ประมวลผล (Application Program) Operating System ส่วนใหญ่จะประกอบด้วย Subsidiary Program Module หลายชุด แต่ละชุดจะทำหน้าที่ต่างกัน เช่น ควบคุมการใช้แฟ้มข้อมูล ควบคุมการประมวลผลหลายโปรแกรมในเวลาเดียวกัน (Multi-programming) ควบคุมการทำงานของอุปกรณ์ที่ใช้ร่วมกันในระบบคอมพิวเตอร์ (Spooling Systems) และควบคุมการประมวลผลในส่วนที่เกี่ยวกับข้อมูล เป็นต้น โดยมี Control Program ชุดหนึ่งคอยควบคุมดูแลการทำงานของ Subsidiary Program Module เหล่านี้อยู่ตลอดเวลา

ในระบบคอมพิวเตอร์ที่ก้าวหน้าอาจต้องใช้ระบบงานและโปรแกรม (System Software) อื่น ๆ เพิ่มเติม ซึ่งจะต้องนำมาเชื่อมต่อกับ Operation System เพื่อช่วยกันควบคุมดูแลการประมวลผล ตัวอย่างเช่น ในระบบ On-line จะต้องใช้โปรแกรมควบคุมการสื่อสารข้อมูล (Data Communication Software) ระหว่างเครื่อง Terminal กับหน่วยความจำที่ศูนย์คอมพิวเตอร์ หรือในระบบฐานข้อมูล (Data Base) จะต้องใช้ DBMS ช่วยอำนวยความสะดวกในการใช้ข้อมูลในระบบนี้ด้วย เป็นต้น

สำหรับการควบคุมการทำงานของระบบคอมพิวเตอร์ด้วยมือหรือโดยบุคคล จะมากน้อยเพียงใดขึ้นอยู่กับขนาดของโปรแกรมที่ใช้ควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ (System Software) และขนาดของเครื่องคอมพิวเตอร์ที่ใช้ ด้วยการกำหนดหน้าที่และระเบียบการปฏิบัติงานสำหรับผู้ควบคุมการทำงานของเครื่องคอมพิวเตอร์ (Operator) การป้องกันข้อผิดพลาดโดยจัดให้มีการแบ่งแยกหน้าที่กันตามความเหมาะสม และอาจใช้วิธีสอบทานการปฏิบัติงานของ Operator เพื่อหาข้อผิดพลาด

การปฏิบัติงานของ Operator ควรอยู่ในกรอบของระเบียบที่ได้กำหนดให้ถือปฏิบัติในเรื่องที่เกี่ยวกับการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ระเบียบเหล่านี้รวมถึงการแก้ไขปัญหาที่เกิดจากเครื่องจักรและโปรแกรมทำงานผิดพลาด และการบันทึกรายละเอียดในการปฏิบัติงาน ขั้นตอนในการปฏิบัติงานของ Operator จะประกอบด้วยคำสั่งหรือระเบียบในการปฏิบัติงาน 2 ชนิด คือ คำสั่งหรือระเบียบในการปฏิบัติงานโดยทั่วไป (Standing Instruction) และวิธีการใช้เครื่องคอมพิวเตอร์ในแต่ละงาน (Run Instructions) ผู้บริหารที่มีหน้าที่

ต้องรับผิดชอบในการปฏิบัติงานด้านคอมพิวเตอร์ เช่น ผู้จัดการฝ่ายควบคุมการปฏิบัติงานด้านคอมพิวเตอร์ (Operation Manager) การตรวจสอบคำสั่งหรือระเบียบดังกล่าวทุกระยะ เพื่อสอบยันความสมบูรณ์และถูกต้องของคำสั่ง หรือระเบียบที่ใช้ในการปฏิบัติงาน และควรรวบรวมปัญหาที่เกี่ยวกับคำสั่งหรือระเบียบในการปฏิบัติงานเหล่านี้ไว้ด้วย เพื่อจะได้ปรับปรุงวิธีการประมวลผลให้ดีขึ้น

ในกรณีที่เครื่องคอมพิวเตอร์มีขนาดใหญ่ ควรใช้ Operator มากกว่าหนึ่งคนควบคุมเครื่องคอมพิวเตอร์ขณะทำการประมวลผล เพื่อช่วยเหลือและสับเปลี่ยนหน้าที่กัน และมีหัวหน้าผู้ควบคุมเครื่องคอมพิวเตอร์ (Chief Operator) หรือหัวหน้าผลัด (Chief Leader) คอยควบคุมการทำงานของ Operator ด้วย สำหรับศูนย์คอมพิวเตอร์ที่มีเครื่องคอมพิวเตอร์ขนาดเล็ก มักจะไม่ค่อยมีการแบ่งหน้าที่ในการทำงานของ Operator จึงจำเป็นต้องเน้นหนักไปทางด้านการตรวจสอบการปฏิบัติงานของ Operator เป็นส่วนใหญ่

การตรวจสอบการปฏิบัติงานของ Operator จะถี่เพียงใดนั้น จะขึ้นอยู่กับรายงานการปฏิบัติงานที่เครื่องคอมพิวเตอร์ทำขึ้น หรือโดยบุคคลที่มีหน้าที่บันทึกรายละเอียดในการปฏิบัติงาน โดยปกติโปรแกรมที่ทำหน้าที่ควบคุมการทำงานของระบบคอมพิวเตอร์ (System Software) จะบันทึกการทำงานของเครื่องคอมพิวเตอร์ทั้งหมดไว้ในแฟ้มข้อมูลสำหรับบันทึกรายละเอียดในการปฏิบัติงานโดยเฉพาะ ซึ่งเรียกว่า System Log ซึ่งสามารถนำมาพิมพ์เป็นรายงานสำหรับตรวจสอบการปฏิบัติในเรื่องต่าง ๆ ได้ เช่น กรณีเครื่องคอมพิวเตอร์ทำงานผิดปกติ การประมวลผลซ้ำ (re-runs) การปฏิบัติงานในช่วงสุดท้ายก่อนจบงานผิดปกติหรือผิดขั้นตอนในการปฏิบัติงาน และผลการปฏิบัติงานของ Operator เป็นต้น อย่างไรก็ดีรายละเอียดต่าง ๆ ที่บันทึกใน Log เหล่านี้มีปริมาณมาก และเป็นเรื่องทางเทคนิคซึ่งไม่สามารถตรวจสอบได้หมด ดังนั้นผู้ตรวจสอบอาจซื้อหาโปรแกรมจากผู้ผลิตโปรแกรมที่สามารถวิเคราะห์รายการที่เกิดขึ้นเพื่อช่วยในการตรวจสอบก็ได้

ในศูนย์คอมพิวเตอร์ที่ใช้เครื่องคอมพิวเตอร์ขนาดเล็กส่วนใหญ่จะไม่มี Log บันทึกรายละเอียดการทำงานของเครื่องคอมพิวเตอร์ ให้ตรวจสอบการทำงานที่ผิดปกติ จึงต้องตรวจสอบจากทะเบียนบันทึกที่ทำขึ้นโดยบุคคลผู้ปฏิบัติงาน หรือด้วยมือ หรือตรวจสอบจากรายงานที่คอมพิวเตอร์ทำขึ้นส่วนหนึ่ง และรายงานที่ทำด้วยมืออีกส่วนหนึ่ง ตัวอย่างเช่น คอมพิวเตอร์จะบันทึกรายละเอียดของระยะเวลาที่ประมวลผลแต่ละงาน และในขณะเดียวกัน Operator จะต้องบันทึกรายละเอียดในการปฏิบัติงานลงในแบบฟอร์มที่กำหนดไว้ และหากมีการปฏิบัติที่ผิดปกติจะต้องบันทึกรายละเอียดไว้ด้วย แต่รายละเอียดที่บันทึกด้วยมือนี้จะเชื่อถือได้ต่อเมื่อมีการแบ่งแยกหน้าที่ในการทำงาน มีการควบคุมในห้องคอมพิวเตอร์ในขณะปฏิบัติงานประมวลผลอย่างเพียงพอ

นอกจากนี้ควรมีพนักงานชั้นบริหารหรือบุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องกับ Job Set-up หรือมีหน้าที่ใช้เครื่องคอมพิวเตอร์ปฏิบัติงานประมวลผลเป็นผู้ตรวจสอบ System Log โดยเพ่งเล็งเฉพาะกรณีที่ Operator ละเลยไม่ใช้โปรแกรมตรวจสอบการปฏิบัติงานที่สำคัญ เช่น ละเลยไม่ตรวจสอบอายุการเก็บแฟ้มข้อมูลที่ใช้ประมวลผล ผู้ตรวจสอบควรตรวจสอบความสมบูรณ์และความต่อเนื่องของ System Log ในแต่ละงวด โดยอาศัยการกำหนดเลขที่เรียงตามลำดับก่อนหลังไว้ล่วงหน้าในแบบฟอร์มที่จะใช้บันทึกการปฏิบัติงาน

การซักถามเพื่อประเมินผลการควบคุมภายในเกี่ยวกับการปฏิบัติงานประมวลผล มีดังนี้

1) โปรแกรมที่ใช้ควบคุมการทำงานของระบบคอมพิวเตอร์ (Operations Software)

1.1) วิธีการใช้ System Software (หรือ Supervisor Program) มีความเหมาะสมกับ Production Program ที่ใช้ในการประมวลผล หรือไม่

1.2) ให้ดูคำถามในเรื่อง System Software เพื่อพิจารณาว่ามีการควบคุมการใช้และมีการรักษาความปลอดภัยเกี่ยวกับ System Software หรือไม่

2) การปฏิบัติงานในห้องคอมพิวเตอร์ (Computer Operating)

2.1) มีการกำหนดคำสั่งหรือระเบียบในการปฏิบัติงานของ Operator อย่างเพียงพอหรือไม่

2.2) การแก้ไขคำสั่งหรือระเบียบการปฏิบัติงานทุกชนิด ผู้บริหารต้องลงนามอนุมัติหรือไม่

2.3) มีการควบคุมคำสั่งหรือระเบียบให้ถูกต้องครบถ้วน และทันเวลาอยู่เสมอหรือไม่ (เช่น มีการตรวจสอบคำสั่งหรือระเบียบโดยผู้จัดการฝ่ายปฏิบัติการด้านคอมพิวเตอร์ทุกระยะ)

2.4) มีการควบคุมการปฏิบัติงานของ Operator ให้เป็นไปตามขั้นตอนที่ได้กำหนดไว้หรือไม่ และการควบคุมดังกล่าวขัดต่อการปฏิบัติงานในเรื่องต่อไปนี้หรือไม่

ก) การควบคุมดูแลภายในห้องเครื่องคอมพิวเตอร์ ถ้าไม่ขัดกันให้ตอบคำถามในข้อที่ (3.1) ด้วย

ข) การตรวจสอบบันทึกรายละเอียดในการปฏิบัติงานประมวลผล ถ้าไม่ขัดกันให้ตอบคำถามในข้อ (4.1) - (4.6)

3) การควบคุมดูแล (Supervision)

3.1) มีหัวหน้างาน (Supervisor) ควบคุมดูแลอยู่ในห้องคอมพิวเตอร์ตลอดเวลาทำงานตามปกติ และในกรณีพิเศษด้วยหรือไม่

4) การบันทึกรายละเอียดในการปฏิบัติงานประมวลผล (Record of Processing)

4.1) การปฏิบัติงานในส่วนใดบ้างที่เครื่องคอมพิวเตอร์บันทึกรายละเอียดในการทำงานไว้

ก) จะเชื่อถือ System Software ที่ใช้ได้ หรือไม่ว่าจะบันทึกเหตุการณ์ที่ผิดปกติ (เช่น เครื่องจักรทำงานผิดพลาด การทำงานซ้ำกันหลายครั้ง (re-run) และความผิดปกติในช่วงจะจบงาน) และการปฏิบัติงานของ Operator ไว้โดยอัตโนมัติ

ข) มีการควบคุมระบบงานที่เริ่มนำออกใช้ การรักษาความปลอดภัยเกี่ยวกับ System Software อย่างเพียงพอหรือไม่ (ดูคำถามในส่วนที่เกี่ยวกับ System Software ประกอบ)

4.2 มีการควบคุมการปฏิบัติงานโดยบุคคลหรือด้วยมือ เพียงพอที่จะช่วยให้แน่ใจว่ามีการบันทึกเหตุการณ์ที่ผิดปกติ และการปฏิบัติงานของ Operator ไว้ครบถ้วนหรือไม่ (เช่น มี Operations Supervisor เป็นผู้ตรวจสอบบันทึกการปฏิบัติงาน)

4.3 มีการควบคุมที่ทำให้แน่ใจว่าการตรวจสอบบันทึกการทำงานจะครบถ้วนสมบูรณ์หรือไม่ (เช่น มีการให้หมายเลขลงในแบบฟอร์มที่จะใช้บันทึกไว้ล่วงหน้า หรือให้บันทึกลง Run Sheet ที่มีเลขหน้าเรียงตามลำดับอยู่แล้ว เป็นต้น)

4.4 มีการตรวจสอบและค้นหาสาเหตุของรายการผิดปกติที่เกิดขึ้น หรือการปฏิบัติงานของ Operator ที่เกี่ยวข้องกับเหตุการณ์ที่ผิดปกติจนเป็นที่พอใจหรือไม่

4.5 การตรวจสอบในข้อที่ (4.4) ข้างต้นกระทำโดยบุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องกับการใช้เครื่องคอมพิวเตอร์หรือไม่

4.6 มีเจ้าหน้าที่ที่รับผิดชอบเป็นผู้ทบทวนและรับทราบผลการสอบสาเหตุของข้อผิดพลาดในข้อที่ (4.4) หรือไม่

2.3 การใช้แฟ้มข้อมูลให้ถูกต้อง

ในบทที่ 4 ซึ่งเป็นเรื่องที่เกี่ยวกับการประเมินผลการควบคุมทางด้านผู้ให้ข้อมูล ได้เคยกล่าวถึงวิธีการควบคุมการบันทึกข้อมูลที่เปลี่ยนแปลงให้ถูกต้องทันเวลาอยู่เสมอ (Update) และการบำรุงรักษาแฟ้มข้อมูลไปบ้างแล้ว ส่วนในหัวข้อนี้จะกล่าวถึงวิธีการควบคุมการใช้แฟ้มข้อมูลที่ใช้ในการประมวลผล ซึ่งจำเป็นต้องมีวิธีการควบคุมโดยเฉพาะ เพื่อให้การใช้แฟ้มข้อมูลเป็นไปอย่างถูกต้อง

โดยปกติการควบคุมแฟ้มข้อมูลจะเริ่มจากการควบคุมโดยบุคคลหรือด้วยมือ นับตั้งแต่การนำแฟ้มข้อมูลออกจากห้องเก็บแฟ้มข้อมูลไปจนถึงการใช้ Job Set-up ซึ่งผู้ตรวจสอบมักจะเชื่อว่า System Software สามารถทำงานได้ถูกต้อง และแฟ้มข้อมูลที่นำไปใส่ไว้ในเครื่องคอมพิวเตอร์นั้นถูกต้องแล้ว โดยแฟ้มข้อมูลแต่ละแฟ้มจะมี Header Label บรรจุข้อมูลสำหรับอ้างอิง เช่น ชื่อแฟ้ม ข้อมูล และ Version Number แสดงว่าเป็นแฟ้มข้อมูลชุดใด สำหรับแฟ้มข้อมูลที่มีขนาดใหญ่ต้องใช้อุปกรณ์มากกว่าหนึ่งหน่วย จะต้องมีเลขลำดับแสดงความต่อเนื่องของแฟ้มข้อมูล เมื่อแฟ้มข้อมูลถูกนำไปใส่ (Load) ไว้ในเครื่องเพื่อใช้ประมวลผล จะต้องมีการตรวจสอบรายละเอียดใน Header Label นอกจากนี้การประมวลผลในระบบ Batch ซึ่งมีการกำหนดอายุในการเก็บแฟ้มข้อมูล (Retention Period) จะต้องกำหนดให้ System Software ตรวจสอบอายุการใช้งานที่อยู่ใน Header Label ก่อนจะใช้ประมวลผลเพื่อสร้างแฟ้มข้อมูลชุดใหม่ หาก Operator ละเลยวิธีการควบคุมดังกล่าว ควรสอบทานการปฏิบัติงานโดยอาศัยคำถามดังต่อไปนี้

1) ขั้นตอนในการทำงานมีความเหมาะสม และช่วยให้แน่ใจว่า

ก) มีการใช้แฟ้มข้อมูลถูกต้องหรือไม่ (เช่น ใช้โปรแกรมตรวจสอบชื่อแฟ้มข้อมูลและหมายเลขประจำแฟ้มข้อมูล และวันที่สร้างแฟ้มข้อมูล เป็นต้น)

ข) ในกรณีที่แฟ้มข้อมูลเป็นแบบ Multivolume โดยบันทึกอยู่ในอุปกรณ์หลายหน่วย การใช้แฟ้มข้อมูลในแต่ละครั้งครบถ้วนทุกหน่วย หรือไม่

2) System Software ส่วนใดที่ทำให้แน่ใจว่าการใช้แฟ้มข้อมูลเป็นไปอย่างถูกต้อง

ก) ขั้นตอนการทำงานของโปรแกรมที่ใช้มีความเหมาะสมเพียงใด (เช่น ชี้ให้เห็นความแตกต่างของแฟ้มข้อมูลหลักในแต่ละรุ่น)

ข) มีการควบคุมระบบงานที่เริ่มนำออกใช้ และการรักษาความปลอดภัยเกี่ยวกับ System Software อย่างเพียงพอหรือไม่ (ดูคำถามในส่วนที่เกี่ยวกับ System Software ประกอบ)

3) มีการตรวจสอบรายงานที่ System Software พิมพ์ออกมาโดยบุคคลอื่นที่ไม่เกี่ยวข้องกับการใช้เครื่องคอมพิวเตอร์ หรือ System Software หรือไม่

4) มีเจ้าหน้าที่ที่รับผิดชอบเป็นผู้ทบทวนและรับทราบผลการปฏิบัติงานตามข้อ 1) และข้อ 3) หรือไม่

2.4 การแก้ไขความเสียหายที่เกิดขึ้นจากการประมวลผลให้คืนสู่สภาพเดิม

ควรมีการตระเตรียมวิธีการแก้ไขข้อผิดพลาด หรือมีความเสียหายที่อาจเกิดขึ้นกับโปรแกรมที่ได้รับอนุมัติให้ใช้ประมวลผล (Production Program) โปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์ (System Software) และแฟ้มข้อมูล โดยไม่ทำให้ระบบงานนั้น ๆ ต้องเปลี่ยนแปลง สำหรับคำถามที่ใช้สอบถามเพื่อประโยชน์ในการตรวจสอบ ได้แก่

1) มีการตระเตรียมวิธีการแก้ไขข้อผิดพลาดหรือความเสียหายที่เกิดขึ้น โดยไม่ทำให้ระบบงานต้องเปลี่ยนแปลงในเรื่องต่าง ๆ ดังต่อไปนี้หรือไม่

ก) Production Program

ข) System Software

ค) แฟ้มข้อมูล

2) มีเจ้าหน้าที่ที่รับผิดชอบตรวจทานและรับทราบการแก้ไขความเสียหายหรือไม่

3. การควบคุมและการรักษาความปลอดภัยแฟ้มข้อมูล

การควบคุมและรักษาความปลอดภัยแฟ้มข้อมูล (Data Files Security Controls) มีวัตถุประสงค์เพื่อป้องกันการแก้ไขแฟ้มข้อมูลโดยไม่ได้รับอนุญาต โดยผู้ตรวจสอบจะต้องพิจารณาในการให้ความเชื่อถือ ทั้งด้านการควบคุม การบำรุงรักษาแฟ้มข้อมูล และการตรวจจับการแก้ไขแฟ้มข้อมูลโดยไม่ได้รับอนุญาต ซึ่งผู้ตรวจสอบ

จะต้องให้ความสนใจต่อการควบคุม การรักษาความปลอดภัยแฟ้มข้อมูลในส่วนที่เป็นข้อมูลถาวรที่ไม่ค่อยมีการเปลี่ยนแปลง (Standing Data) มากกว่าข้อมูลแต่ละรายการ (Transaction Data) ทั้งนี้เพราะในกรณีที่การกระทบยอด Standing Data เฉพาะ Field ที่สำคัญของข้อมูลทางบัญชี การตรวจสอบข้อมูลตามรอบระยะเวลาที่กำหนดไว้ในแต่ละครั้งอาจไม่เพียงพอที่จะช่วยให้ทราบถึงการเปลี่ยนแปลงการแก้ไขแฟ้มข้อมูลโดยไม่ได้รับอนุญาตได้ทันเวลา และในกรณีที่การจัดองค์ประกอบของแฟ้มข้อมูลเป็นระบบฐานข้อมูล (Data Base) วิธีการตรวจสอบโดยการกระทบยอดจะน้อยลงไปอีก ย่อมเปิดโอกาสให้มีการแก้ไขข้อมูลโดยไม่ได้รับอนุญาตมากขึ้น โดยเฉพาะอย่างยิ่งในกรณีที่แฟ้มข้อมูลถูกใช้ในระบบ On-line

ด้วยเหตุนี้ผู้ตรวจสอบจึงต้องมีส่วนเกี่ยวข้องกับการควบคุมการรักษาความปลอดภัยของแฟ้มข้อมูลเพื่อไม่ให้มีการแก้ไขแฟ้มข้อมูลโดยไม่ได้รับอนุญาต เพื่อให้ธนาคารที่ทำการตรวจสอบมีการควบคุมที่เหมาะสมเพื่อป้องกันการบันทึกข้อมูลอื่นทับข้อมูลที่อยู่ในแฟ้มข้อมูลโดยไม่ตั้งใจหรือถูกทำลาย และเพื่อป้องกันการคัดลอกข้อมูลโดยทำเป็นแฟ้มข้อมูลชุดสำเนา ซึ่งอาจทำให้ธนาคารเสียหาย

การควบคุมแฟ้มข้อมูลจะต้องกระทำทั้งขณะที่ใช้งานและเลิกใช้งาน โดยจะต้องกำหนดว่ามีแฟ้มข้อมูลใดบ้างที่ Operator หรือผู้ใช้ข้อมูลทางเครื่อง Terminal จำเป็นต้องใช้ปฏิบัติงานเช่นเดียวกับโปรแกรมที่ใช้งานสำหรับแฟ้มข้อมูลที่ใช้อาจเป็นเทปหรือจานแม่เหล็ก หากเป็นการประมวลผลแบบ Batch System แฟ้มข้อมูลเหล่านี้จะถูกนำมาบรรจุไว้ในเครื่องคอมพิวเตอร์เพื่อทำการประมวลผล เมื่อเสร็จงานจะนำออกจากเครื่องคอมพิวเตอร์เพื่อนำไปเก็บไว้รอการประมวลผลในครั้งต่อไป ในระบบ On-line และระบบ Real-time แฟ้มข้อมูลจะถูกบรรจุอยู่ในเครื่องตลอดเวลา เพื่อให้ผู้ใช้ข้อมูลสามารถสอบถามและแก้ไขข้อมูลได้ตามความต้องการ นอกจากนี้ยังมีการจัดองค์ประกอบของแฟ้มข้อมูลแบบใหม่ ๆ เกิดขึ้นอยู่เสมอ เช่น ระบบฐานข้อมูล (Data Base) เป็นต้น

3.1 การควบคุมแฟ้มข้อมูลระหว่างการใช้งาน

การควบคุมการเปลี่ยนแปลงแก้ไขแฟ้มข้อมูลโดยไม่ได้รับอนุญาตในระบบ Batch จะมีข้อจำกัดในการควบคุม Operator ในช่วงระยะเวลาที่ทำการประมวลผล หากเป็นระบบ On-line และระบบ Real-time จะต้องมีการป้องกันการใช้ข้อมูลผ่านทางเครื่อง Terminal เพิ่มขึ้นด้วย การควบคุมแฟ้มข้อมูลที่อยู่ระหว่างการใช้งานควรกระทำทั้งในขณะประมวลผลจริง และในขณะที่มีการปรับปรุงแก้ไข หรือทดสอบโปรแกรม ซึ่งเป็นช่วงที่ไม่ได้ทำการประมวลผลจริง

(1) การควบคุมการใช้แฟ้มข้อมูลของ Operator ในระหว่างการประมวลผล

การควบคุม Operator ในระหว่างการประมวลผล เพื่อป้องกันการใช้แฟ้มข้อมูลในส่วนที่ไม่ได้รับอนุญาต รวมทั้งการตรวจสอบการใช้ข้อมูลในการปฏิบัติงานที่ประมวลผลจะมีวิธีการเช่นเดียวกับการควบคุมโปรแกรมดังที่เคยกล่าวมาแล้ว

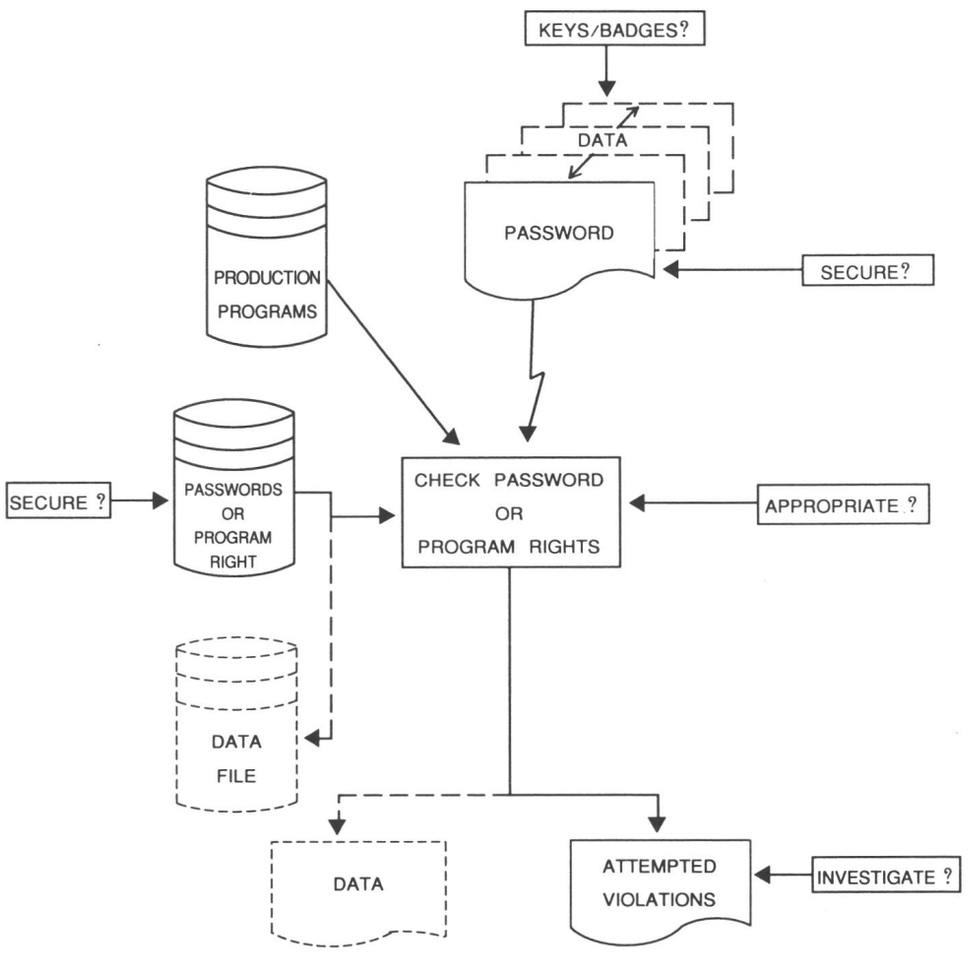
ในกรณีที่ระบบคอมพิวเตอร์ของธนาคารมีคุณสมบัติที่สามารถแก้ไขข้อมูลในแฟ้มข้อมูลได้โดยตรงจะต้องจัดให้มีวิธีการควบคุมคล้ายกับการควบคุมการปรับปรุงแก้ไขโปรแกรมซึ่งได้เคยกล่าวมาแล้วเช่นเดียวกันในระบบฐานข้อมูล (Data Base) หากมีความจำเป็นที่ไม่อาจจะใช้ DBMS (Data Base Management System)

ซึ่งเป็นโปรแกรมควบคุมการใช้ข้อมูลในระบบนี้จะด้วยเหตุใดก็ตาม เช่น อยู่ระหว่างการปรับปรุงแก้ไขหรือบำรุงรักษา DBMS จะต้องเพิ่มความระมัดระวังการใช้ข้อมูลที่อยู่ในระบบฐานข้อมูลให้มากขึ้น นอกจากนี้การแก้ไขข้อมูลในระบบฐานข้อมูลจะทำได้ถูกต้อง หากผู้แก้ไขทราบโครงสร้างและความสัมพันธ์ระหว่างข้อมูลตามหลักการของระบบนี้เป็นอย่างดี จึงควรควบคุมการใช้ข้อมูลและเอกสารที่สำคัญของระบบฐานข้อมูลอย่างรัดกุม

(2) การควบคุมการใช้แฟ้มข้อมูลผ่านทางเครื่อง Terminal

ในกรณีที่มีการใช้เครื่อง Terminal เช่น ในระบบ On-line และในระบบ Real-time จะต้องป้องกันการแก้ไขข้อมูลที่อยู่ในแฟ้มข้อมูลโดยไม่ได้รับอนุญาตอย่างรัดกุม โดยเฉพาะในช่วงนอกเวลาทำงานตามปกติ

การแก้ไขข้อมูลโดยไม่ได้รับอนุญาตอาจกระทำได้ทั้งข้อมูลที่เกิดขึ้นในแต่ละรายการ (Transaction Data) หรือข้อมูลถาวรที่มีการเปลี่ยนแปลงน้อย (Standing Data) เช่น อาจมีรายการฝากถอนซึ่งเป็น Transaction Data ที่ถูกแก้ไขโดยไม่ได้รับอนุญาต และมีผลกระทบต่อยอดเงินฝากของลูกค้าปะปนอยู่ในแฟ้มข้อมูล หรือวงเงินเบิกเกินบัญชีซึ่งเป็น Standing Data อาจถูกแก้ไขโดยไม่ได้รับอนุญาตปะปนอยู่ในแฟ้มข้อมูลได้เช่นเดียวกัน



แผนภาพที่ 21.2 การควบคุมการใช้แฟ้มข้อมูลผ่านทางเครื่อง Terminal

การควบคุมการใช้ข้อมูลที่เก็บไว้ในแฟ้มข้อมูลเป็นเรื่องที่สำคัญมาก เพราะถ้าเปิดโอกาสให้สามารถแก้ไขข้อมูลที่อยู่ในแฟ้มข้อมูลโดยไม่ได้รับอนุญาตได้ง่าย จะทำให้คุณค่าในการควบคุมลดน้อยลง โดยผู้ที่แก้ไขข้อมูลโดยไม่ได้รับอนุญาตจะแก้ไขข้อมูลให้ถูกต้องก่อนที่จะมีการตรวจสอบ

การใช้แฟ้มข้อมูลผ่านทางเครื่อง Terminal ในระบบ On-line ควรมีโปรแกรมควบคุมการใช้แฟ้มข้อมูล และมีการรักษาความปลอดภัยเกี่ยวกับการใช้เครื่อง Terminal ที่เหมาะสมและรัดกุม เพื่อให้พนักงานที่ได้รับมอบหมายให้ใช้เครื่อง Terminal เท่านั้นที่สามารถใช้ข้อมูลหรือนำข้อมูลเข้าไปเก็บไว้ในแฟ้มข้อมูลได้

(3) การใช้รหัสลับควบคุมการใช้แฟ้มข้อมูลผ่านทางเครื่อง Terminal

โดยปกติโปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์ (System Software) จะมีวิธีการควบคุมและป้องกันการใช้เครื่อง Terminal โดยกำหนดให้ผู้ที่จะใช้เครื่อง Terminal ติดต่อกับเครื่องได้ต้องป้อนรหัสประจำตัวผู้ใช้ผ่านเครื่อง Terminal ไปยังเครื่องคอมพิวเตอร์เพื่อตรวจสอบรหัส (Password) ก่อนอนุญาตให้ใช้เครื่อง

การใช้รหัสลับควบคุมการใช้เครื่อง Terminal อาจใช้วิธีการง่าย ๆ โดยยินยอมให้ผู้ที่ได้รับอนุญาตมีรหัสลับสามารถนำข้อมูลจากศูนย์คอมพิวเตอร์มาพิมพ์ และหรือแสดงทางจอภาพทางเครื่อง Terminal ได้ตามความจำเป็นในการปฏิบัติงาน หรืออาจสร้างระบบให้ซับซ้อนยิ่งขึ้นโดยสร้างรหัสลับไว้หลายชุด แต่ละชุดจะใช้ข้อมูลได้เฉพาะส่วนที่ได้กำหนดไว้เท่านั้น ตัวอย่างเช่น ธนาคารอาจกำหนดรหัสลับในการใช้แฟ้มข้อมูลเกี่ยวกับลูกหนี้ไว้สองชุด ชุดที่มอบไว้ประจำตัวพนักงานคนแรกอาจใช้ข้อมูลได้เฉพาะส่วนที่เป็นชื่อและที่อยู่ของลูกค้า และมีพนักงานอีกคนหนึ่งถือรหัสที่สามารถใช้ข้อมูลเกี่ยวกับวงเงินของลูกหนี้แต่ละรายได้ นอกจากนี้หากมีการลักลอบใช้เครื่อง Terminal ข้อมูลในการใช้เครื่องที่ผิดปกติหรือแตกต่างไปจากข้อกำหนด จะถูกบันทึกไว้และพิมพ์เป็นรายงานให้ทราบ ซึ่งจะต้องสืบหาแหล่งการลักลอบนั้นทันที

การสร้างรหัสลับควรใช้ความระมัดระวังให้มาก โดยเฉพาะการสร้างรหัสลับในกรณีที่มีหลักการเหตุผลคล้าย ๆ กัน ตัวอย่างเช่น การใช้เครื่องหมายนำหน้ารหัสที่เหมือนกัน มีตัวเลขต่อท้ายเรียงตามลำดับ และตัวเลขเหล่านี้จะมีค่าเพิ่มขึ้นอย่างคงที่ เช่น LOAN010 LOAN020 LOAN030 ซึ่งรหัสแต่ละตัวนี้สามารถที่จะเรียกข้อมูลแต่ละประเภทเกี่ยวกับบัญชีลูกหนี้ที่อยู่ในแฟ้มข้อมูลออกมาใช้ได้ ผู้ถือรหัสคนใดคนหนึ่งใน 3 คนนี้อาจเอารหัสของคนอื่นและทดลองใช้จนสามารถนำข้อมูลที่ตนเองไม่มีสิทธิ์มาใช้ได้โดยง่าย หรืออาจทราบรหัสของผู้อื่น หากผู้ถือรหัสบางคนใช้รหัสของงานผิดพลาดกลายเป็นรหัสของผู้อื่น และใช้ข้อมูลในส่วนที่ไม่ได้ตั้งใจก็ได้

เพื่อความเหมาะสมในการควบคุมการสร้าง การบำรุงรักษา และการใช้รหัสลับ การมอบหมายให้เป็นหน้าที่ของเจ้าหน้าที่ที่ไม่มีส่วนเกี่ยวข้องในการใช้เครื่องคอมพิวเตอร์และเครื่อง Terminal ซึ่งปกติผู้ตรวจสอบภายในจะเป็นผู้ตรวจสอบการปฏิบัติงานของเจ้าหน้าที่ที่กล่าวอีกชั้นหนึ่ง

นอกจากนี้ควรมีวิธีการควบคุมอื่น ๆ ที่จำเป็นเพื่อป้องกันรหัสลับไม่ให้ตกไปอยู่ในมือของบุคคลที่ไม่ได้รับมอบหมาย เช่น ระมัดระวังไม่ให้เครื่อง Terminal พิมพ์รายละเอียดของรหัสลับออกมาในขณะที่นำข้อมูลเกี่ยวกับรหัสลับเข้าไปเก็บไว้ในเครื่องคอมพิวเตอร์ สำหรับตารางรหัสลับ (Password Table) ที่เก็บไว้ในเครื่องคอมพิวเตอร์ควรเปลี่ยนรูปเป็นรหัสที่ไม่สามารถเข้าใจได้อีกขั้นหนึ่งและควรเปลี่ยนแปลงรหัสลับที่ใช้เป็นครั้งคราว

(4) การควบคุมการใช้แฟ้มข้อมูลโดยอาศัยวิธีการรักษาความปลอดภัยทางด้านตัวเครื่อง Terminal

การควบคุมการใช้เครื่อง Terminal ทางด้าน Physical Security ได้แก่ การใช้กุญแจหรืออุปกรณ์อื่น (Badge) ในการปิด/เปิดเครื่อง Terminal โดยเฉพาะในกรณีที่ไม่ได้ติดตั้งเครื่อง Terminal ไว้ในห้องเป็นสัดส่วน และมีการควบคุมที่รัดกุมอยู่ตลอดเวลา ในบางครั้งจะพบว่ามีการควบคุมการใช้เครื่อง Terminal ในช่วงนอกเวลาทำงานตามปกติอย่างรัดกุม แต่ในช่วงเวลาทำงานตามปกติระหว่างวันจะไม่มีการควบคุมที่ดีพอ ดังนั้นจึงควรมีการบันทึกการใช้กุญแจหรือ Badge ในการปิด/เปิดเครื่อง Terminal และชื่อผู้ใช้ทุกครั้ง แต่อย่างไรก็ดีควรระมัดระวังกุญแจหรือ Badge ชุดอื่นที่อาจใช้ข้อมูลที่เก็บไว้ในแฟ้มข้อมูลหลัก หรือข้อมูลในบางส่วนของแฟ้มข้อมูลอื่นนอกจากที่ได้กำหนดไว้

(5) การควบคุมโปรแกรมที่ใช้ประมวลผลในการเข้าไปใช้แฟ้มข้อมูล

ในระบบฐานข้อมูล (Data Base) นอกจากจะมีการควบคุม Operator และเครื่อง Terminal ตามที่ได้กล่าวมาแล้ว จะต้องควบคุมโปรแกรมที่ใช้ประมวลผล (Production Program) ในการเข้าไปใช้แฟ้มข้อมูลหรือปรับปรุงแก้ไขเพิ่มเติม (Modify) ข้อมูลในระบบนี้ด้วย ทั้งนี้เพราะโปรแกรมที่ใช้ประมวลผลในแต่ละงานในระบบ Data Base จะมีความสัมพันธ์กับลักษณะปลีกย่อยโดยเฉพาะของข้อมูล (Sub-scheme) ที่ได้ออกแบบไว้ในหน่วยเก็บข้อมูลของระบบ ซึ่งเรียกว่า Database Library ดังนั้นจึงจำเป็นต้องตั้งข้อกำหนดในการใช้ข้อมูลในแต่ละ Field ของโปรแกรมที่จะใช้ประมวลผลให้ชัดเจน ตัวอย่างเช่น ยินยอมให้โปรแกรมที่ใช้งานบางโปรแกรมอ่านข้อมูลใน Field ที่สำคัญได้อย่างเดียว หรือมีโปรแกรมใดบ้างที่สามารถเปลี่ยนแปลงหรือล้างรายการเดิมออกได้

สิ่งสำคัญในระบบ Data Base กับ Sub-scheme ทั้งนี้เพราะโปรแกรมที่ใช้ประมวลผลต้องอาศัย Sub-scheme ช่วยในการเข้าไปใช้ข้อมูลในระบบซึ่งมีอยู่มากมาย ดังนั้น การควบคุม Sub-scheme จึงเป็นเรื่องสำคัญ เพราะสามารถป้องกันบุคคลอื่นที่ไม่ได้รับมอบหมายเข้าไปใช้ข้อมูลในระบบนี้ได้ โดยปกติการควบคุมรายละเอียดของ Sub-scheme จะเป็นหน้าที่ของฝ่ายจัดการด้วย Data Base โดยควบคุมรายงานต่าง ๆ และคอยตรวจสอบการลักลอบ หรือพยายามใช้ข้อมูลโดยผู้ที่ไม่ได้รับมอบหมาย

สำหรับคำถามที่ใช้ในการถามเกี่ยวกับการควบคุม และป้องกันแฟ้มข้อมูลที่อยู่ในระหว่างการใช้งานมีดังนี้

1) การป้องกันแฟ้มข้อมูลโดยอาศัยโปรแกรมและขั้นตอนในการปฏิบัติงานของระบบงานและโปรแกรมมีความเหมาะสมสามารถชี้ให้เห็นและหยุดยั้งความพยายามของผู้ที่จะเข้าไปใช้ข้อมูลโดยไม่ได้รับอนุญาตได้หรือไม่
2) ทบทวนคำถามในส่วนที่เกี่ยวกับ System Software เพื่อพิจารณาว่ามีการควบคุมการพัฒนาและการรักษาความปลอดภัย System Software เพียงพอหรือไม่
3) มีขั้นตอนในการตรวจสอบรายงานเกี่ยวกับความพยายามที่จะใช้แฟ้มข้อมูลโดยไม่ได้รับอนุญาตอย่างเพียงพอหรือไม่
4) มีการควบคุม Password ในกรณีดังต่อไปนี้อย่างเพียงพอหรือไม่
   ก) การสร้าง Password

ข) การใช้ Password

ค) การรักษาความปลอดภัย Password

5) มีการควบคุมตามข้อ (4) ตลอดเวลาที่มีการใช้เครื่อง Terminal ติดต่อกับแฟ้มข้อมูลในระบบ On-line หรือไม่ (เช่น ในระหว่างการทดสอบ - Testing)

6) มีการควบคุมที่เกี่ยวกับกุญแจและ Badge ที่ใช้ปิดเปิดเครื่อง Terminal ในกรณีต่อไปนี้อย่างเพียงพอหรือไม่

ก) กุญแจและ Badge ที่จัดหามาใช้

ข) การใช้กุญแจและ Badge

ค) การรักษาความปลอดภัยกุญแจและ Badge

7) มีการตรวจสอบโดยบุคคลอื่นที่ไม่มีหน้าที่ที่เกี่ยวข้องกับการควบคุมเครื่องคอมพิวเตอร์และเครื่อง Terminal ในกรณีต่อไปนี้หรือไม่

ก) การตรวจสอบเพื่อค้นหาสาเหตุในการพยายามเข้าใช้แฟ้มข้อมูลโดยไม่ได้รับอนุญาตตามข้อ (3)

ข) การสร้าง การใช้ และการรักษาความปลอดภัยของ Password ตามข้อ (4)

ค) การจัดหา การใช้ และการรักษาความปลอดภัยของกุญแจและ Badge ตามข้อ (6)

8) มีเจ้าหน้าที่ผู้รับผิดชอบตรวจทานและรับทราบผลของการปฏิบัติงานในกรณีต่อไปนี้หรือไม่

ก) การตรวจสอบเพื่อค้นหาสาเหตุในการพยายามเข้าใช้แฟ้มข้อมูล โดยไม่ได้รับอนุญาตตามข้อ (3)

ข) การสร้าง การใช้ และการรักษาความปลอดภัยของ Password ตามข้อ (4)

ค) การจัดหา การใช้และการรักษาความปลอดภัยของกุญแจและ Badge ตามข้อ (6)

3.2 การควบคุมแฟ้มข้อมูลที่ยังไม่ได้นำมาใช้งาน

แฟ้มข้อมูลที่ยังไม่ได้นำมาใช้งาน (Off-line Files) อาจเสียหายได้ หากมีการนำไปใช้งานผิดวัตถุประสงค์ที่มิได้มีการมอบหมาย จึงควรมีการป้องกันการนำแฟ้มข้อมูลไปใช้โดยไม่ได้รับอนุญาต และมีการบันทึกรายละเอียดในการใช้แฟ้มข้อมูลไว้เป็นหลักฐาน ดังนี้

(1) การรักษาความปลอดภัยสำหรับแฟ้มข้อมูลที่ยังไม่ได้นำมาใช้งาน

เพื่อความปลอดภัยของแฟ้มข้อมูลที่ยังไม่ได้นำมาใช้ที่อาจถูกนำไปใช้โดยไม่ได้รับอนุญาต ควรมีสถานที่เก็บที่แยกต่างหากจากห้องคอมพิวเตอร์ มี Librarian เป็นผู้รับผิดชอบและควบคุมแฟ้มข้อมูลเหล่านี้เกี่ยวกับการนำออกไปใช้งาน การรับคืน และการรักษาความปลอดภัยโดยเฉพาะอยู่ตลอดเวลา ถ้าหากสถานที่เก็บรักษาแฟ้มข้อมูลไม่ใหญ่นัก ไม่สามารถที่จะจัดให้พนักงานคนหนึ่งทำหน้าที่นี้แบบเต็มเวลาทำงานเป็น Full-time Librarian ได้ ควรมอบหมายให้พนักงานชุดหนึ่งช่วยกันทำหน้าที่ควบคุมดูแลการใช้แฟ้มข้อมูลที่เก็บไว้ใน Library

การใช้แฟ้มข้อมูลในการประมวลผลจะถูกต้องตามที่ได้รับมอบหมายหากการจัดทำตารางประมวลผล (Processing Schedule) มีรายละเอียดเกี่ยวกับแฟ้มข้อมูลที่ใช้ประมวลผลในแต่ละงาน (Application) เป็นอย่างดี โดยมีเจ้าหน้าที่ที่รับผิดชอบเป็นผู้รับรองเพื่อให้ Librarian ที่ทำหน้าที่ควบคุมแฟ้มข้อมูลใช้ในการจัดเตรียมแฟ้มข้อมูลตามตารางประมวลผลซึ่งได้รับการอนุมัติให้ใช้แล้ว ส่วนแฟ้มข้อมูลที่ไม่ปรากฏในตารางประมวลผลที่จำเป็นต้องใช้งาน จะต้องขออนุมัติเป็นกรณีพิเศษเป็นคราว ๆ ไป

แฟ้มข้อมูลที่นำไปใช้ในการประมวลผลจะต้องไม่นำออกไปนอกบริเวณพื้นที่ของหน่วยงานปฏิบัติการด้านคอมพิวเตอร์ (Operation-Area) โดยมีผู้จัดการฝ่ายปฏิบัติการด้านคอมพิวเตอร์ (Operations Manager) หรือหัวหน้าผู้ควบคุมเครื่องคอมพิวเตอร์ (Chief Operator) เป็นผู้รับผิดชอบในการควบคุมตัวแฟ้มข้อมูล (Physical Control) ที่นำออกไปใช้ นอกจากนี้การติดตามและจดบันทึกการนำแฟ้มข้อมูลออกไปใช้งานเพื่อป้องกันการนำแฟ้มข้อมูลไปใช้นานเกินกว่าเวลาที่ควรจะเป็นด้วย

(2) การบันทึกรายละเอียดในการใช้แฟ้มข้อมูลที่เก็บไว้ใช้งาน (Library Records)

อุปกรณ์ที่ใช้เก็บข้อมูล (Device) ที่สามารถเคลื่อนที่ได้ ควรมีหมายเลขกำกับไว้อย่างถาวร การบันทึกรายละเอียดของแฟ้มข้อมูลจะเป็นประโยชน์ต่อการจัดทำบัญชีและการควบคุมแฟ้มข้อมูลที่นำออกไปใช้งานและแฟ้มข้อมูลที่ถูกสร้างขึ้นมาใหม่ระหว่างการประมวลผลซึ่งสามารถทำได้ทั้งวิธีบันทึกด้วยมือหรือใช้SystemSoftware

ในกรณีที่ใช้วิธีบันทึกด้วยมือจะมีแบบฟอร์มสำหรับบันทึกชื่อครั้งที่ถูกสร้าง (Version Number) และวันที่สร้างแฟ้มข้อมูลปะติดกับอุปกรณ์ที่เป็นแฟ้มข้อมูล และบันทึกรายละเอียดเหล่านี้ลงในทะเบียนด้วย การนำอุปกรณ์ออกไปใช้งานต้องให้ Librarian ผู้ควบคุมอุปกรณ์ที่กล่าวบันทึกรายละเอียดในการใช้งานตามที่ปรากฏในตารางประมวลผล (Processing Schedule) ลงในทะเบียนเสียก่อน เนื่องจากแฟ้มข้อมูลที่เก็บอยู่ใน Library บางชนิดจะเป็นข้อมูลที่ไม่มีการเปลี่ยนแปลงหรือมีการแก้ไขน้อยเป็นข้อมูลถาวร (Standing Data) และบางชนิดเป็นข้อมูลที่มีการเปลี่ยนแปลงอยู่เสมอ ดังนั้น ก่อนจะล้างแฟ้มข้อมูลเพื่อนำไปใช้งานอื่น Librarian จะต้องแน่ใจว่าเป็นแฟ้มข้อมูลที่ไม่ได้ใช้งานอีกต่อไปเท่านั้น และควรตรวจสอบทะเบียนเก็บแฟ้มข้อมูลทุกวัน จะได้ทราบว่ามีอุปกรณ์ชุดใดบ้างที่เก็บไว้นานเกินความจำเป็น เพื่อจะได้ติดตามต่อไป

ประโยชน์ของการจัดทำบัญชีอุปกรณ์แฟ้มข้อมูลอีกประการหนึ่งก็คือ สามารถนำรายละเอียดไปใช้ในการเปรียบเทียบช่วยให้ทราบว่ามีแฟ้มข้อมูลที่อยู่ในระหว่างการประมวลผลที่สร้างขึ้นมาใหม่ตาม Processing Schedule หรือตามที่ปรากฏอยู่ในรายการที่เป็น System Log อยู่เท่าใด ซึ่งมีความสำคัญมาก โดยเฉพาะอย่างยิ่ง ในกรณีที่ไม่มีพนักงานทำหน้าที่เป็น Librarian โดยตรง

ในกรณีที่ใช้เครื่องคอมพิวเตอร์บันทึกรายละเอียดของแฟ้มข้อมูลโดยใช้ System Software บันทึกรายละเอียดของแฟ้มข้อมูล เช่น ชื่อ ครั้งที่สร้าง วันที่สร้าง ลงภายในแฟ้มข้อมูลขณะที่ทำการประมวลผลเพื่อใช้เป็นข้อมูลอ้างอิงประจำแฟ้มข้อมูล และ System Software จะนำข้อมูลอ้างอิงนี้ไปจัดทำตารางประมวลผล (Processing Schedule) สามารถระบุถึงแฟ้มข้อมูลที่ต้องใช้ได้ ภายหลังจากเสร็จสิ้นการประมวลผล เครื่องคอมพิวเตอร์จะแก้ไขหรือบันทึกรายละเอียดเกี่ยวกับแฟ้มข้อมูลให้ถูกต้องตามข้อเท็จจริง เพื่อให้ Librarian ใช้

ตรวจสอบแฟ้มข้อมูลที่ส่งกลับคืนมา นอกจากนี้ Librarian ควรตรวจสอบตารางการใช้แฟ้มข้อมูลในการประมวลผลที่ System Software สร้างขึ้นมาด้วย เพื่อให้แน่ใจว่าการใช้แฟ้มข้อมูลในการประมวลผลได้กระทำอย่างถูกต้องตาม Processing Schedule

คำถามที่ใช้ในการสอบถามเกี่ยวกับการควบคุมแฟ้มข้อมูลที่ยังไม่ได้นำมาใช้งาน มีดังนี้

1) แฟ้มข้อมูลในขณะที่ไม่ได้นำออกมาใช้ถูกเก็บไว้อย่างปลอดภัยหรือไม่
2) การนำแฟ้มข้อมูลออกไปใช้ต้องขออนุมัติจากผู้ที่ได้รับมอบหมายให้ควบคุมดูแลหรือไม่
3) มีการบันทึกรายละเอียด เพื่อให้ทราบว่ามีแฟ้มข้อมูลอะไรบ้างที่ถูกนำออกไปใช้หรือไม่
4) มีระเบียบในการติดตามแฟ้มข้อมูลที่นำออกไปใช้คืนมาได้ทันท่วงทีหรือไม่ (เช่น โดยการตรวจทานจากบันทึกเพื่อหาสาเหตุที่ไม่มีการส่งแฟ้มข้อมูลกลับคืนมาเก็บไว้)
5) มีบุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องกับหน้าที่ต่อไปนี้ปฏิบัติงานหรือตรวจสอบการปฏิบัติงานตามข้อ (3) และข้อ (4) หรือไม่
   ก) การควบคุมการปฏิบัติงานด้านเครื่องคอมพิวเตอร์ (Computer Operations)
   ข) การออกแบบระบบงานและการเขียนโปรแกรม
6) มีเจ้าหน้าที่ที่รับผิดชอบได้ทำการตรวจทานและรับทราบผลการปฏิบัติงานตามข้อ (3) และข้อ (4) หรือไม่
7) ถ้าการบันทึกรายละเอียดตามข้อ 3) ทำด้วยคอมพิวเตอร์แล้ว System Software ที่ใช้มีความเหมาะสมสามารถบันทึกรายละเอียดได้ถูกต้องหรือไม่
8) ให้ทบทวนคำถามในส่วนที่เกี่ยวกับ System Software เพื่อพิจารณาว่ามีการควบคุมการพัฒนาและการรักษาความปลอดภัย System Software อย่างเพียงพอหรือไม่
9) มีการควบคุมตามข้อ (1) ถึงข้อ (3) ในช่วงเวลาที่มีการทำงานนอกเหนือจากการทำงานตามปกติ เช่น วันหยุดสุดสัปดาห์ และในช่วงเวลาที่มีการทำงานพิเศษในเวลาปกติ เช่น ระหว่างที่มีการทดสอบโปรแกรม หรือไม่

4. โปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์

System Software ที่จะกล่าวในข้อนี้ หมายถึง โปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์ซึ่งทำหน้าที่โดยทั่วไป ดังนี้

1) Cataloguing
2) Reporting of Job Processed
3) Program Comparison
4) Supervision of Application Programs
5) File Handling DBMS
6) Data Communications
7) Reporting of Operations

8) File Set-up

9) Password Protection

10) Library Records

ผู้ตรวจสอบจะเชื่อถือการทำงานของโปรแกรมได้เพียงใดนั้น อาจพิจารณาได้จากการพัฒนาและการเก็บรักษาโปรแกรมว่ามีความเหมาะสมเพียงใด

4.1 การพัฒนาโปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์

การควบคุมการพัฒนาและการปรับปรุงแก้ไขโปรแกรมการทำงานของระบบคอมพิวเตอร์มีลักษณะคล้ายกับการควบคุมการพัฒนาและการปรับปรุงแก้ไขโปรแกรมที่ใช้ประมวลผลในแต่ละงานของผู้ใช้ข้อมูล (Application Program) ที่ได้เคยกล่าวมาแล้วในบทก่อน ๆ ซึ่งสามารถนำวิธีการตรวจสอบมาใช้ได้เป็นอย่างดีทั้ง System Software ที่ซื้อมาจากบุคคลภายนอกหรือธนาคารพัฒนาขึ้นเอง

ในกรณีที่มีการพัฒนาหรือมีการปรับปรุงแก้ไขโปรแกรมขึ้นมาใหม่ จะต้องทดสอบการทำงานของ System Software ชุดใหม่นี้ก่อนใช้งานจริง เพื่อให้แน่ใจว่าสามารถทำงานร่วมกับ Application Program ได้อย่างถูกต้อง โดยตรวจสอบจากผลการทำงานของ Application Program ที่ใช้อยู่ในขณะนั้น หากมีข้อผิดพลาดเกิดขึ้นก็อาจพิสูจน์ได้ว่า System Software และ Application Program ยังทำงานไม่สอดคล้องกัน ซึ่งในบางครั้งอาจต้องปรับปรุงแก้ไข Application Program ที่ใช้งานอยู่เดิมทั้งหมดก็ได้ เช่น ในกรณีที่มีการนำระบบ Data Base มาใช้แทนการจัดเก็บข้อมูลในระบบเดิมจะต้องนำ Data Base Management System (DBMS) มาใช้ด้วย

การสอบทาน System Generated Output ซึ่งเป็นรายละเอียดในการจัดทำโปรแกรมที่ใช้ควบคุมการทำงานของระบบคอมพิวเตอร์ที่คอมพิวเตอร์พิมพ์ให้ จะช่วยให้ทราบรายละเอียดของโปรแกรมในส่วนที่ไม่ได้เกี่ยวข้องกับ Application Program ตัวอย่างเช่น การจัดทำรายงานการใช้เครื่องคอมพิวเตอร์และการจัดแฟ้มข้อมูล (File Set-up) หน้าที่ของ System Software และทางเลือกต่าง ๆ ได้เป็นอย่างดี

สำหรับการควบคุมสำเนารายละเอียดในการทดสอบโปรแกรม (Test Software) ที่เก็บไว้ใน Library ของศูนย์คอมพิวเตอร์ การดำเนินการติดตามและตรวจสอบเช่นเดียวกับการ Catalog โปรแกรมใช้งาน (Application Program)

4.2 การรักษาความปลอดภัยโปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์

การรักษาความปลอดภัยโปรแกรมควบคุมการทำงานของระบบคอมพิวเตอร์มีลักษณะคล้ายกับการรักษาความปลอดภัย Application Program ที่ได้กล่าวไว้แล้ว ซึ่งสรุปได้ว่าจะต้องแน่ใจว่าจะไม่มีการแก้ไข System Software โดยไม่ได้รับอนุญาตทั้งในขณะใช้งานและไม่ได้ใช้งาน

คำถามที่ใช้สอบถามในเรื่องนี้ให้ใช้คำถามของ Application Program และการควบคุมภายในที่เกี่ยวข้อง มาประยุกต์ใช้ตามความสามารถ

5. การบริหารระบบ Data Base

เนื่องจากระบบ Data Base มีขนาดใหญ่และมีความซับซ้อนมาก จึงจำเป็นต้องมีเจ้าหน้าที่รับผิดชอบโดยตรง เรียกว่า Data Base Administrator (DBA) ทำหน้าที่ออกแบบและบำรุงรักษา Scheme, Sub-scheme และ DBMS ตลอดจนติดต่อประสานงานกับผู้ใช้ พนักงานอื่นในศูนย์คอมพิวเตอร์และผู้ขายบริการเกี่ยวกับงานคอมพิวเตอร์จากภายนอก การควบคุมงาน Data Base ของ DBA มีดังนี้

1) สอบทานระบบงานใหม่เพื่อให้สามารถทำงานร่วมกับระบบ Data Base ได้อย่างเหมาะสม
2) สอบทานการเปลี่ยนแปลงแก้ไขโปรแกรมที่มีผลกระทบต่อ Data Base
3) ควบคุม Scheme และ Sub-scheme

นอกจากนี้ DBA อาจต้องรับผิดชอบในการควบคุมการบำรุงรักษาข้อมูลใน Data Base ด้วย

การประมวลผลและการจัดเก็บข้อมูลในแบบเดิม ความรับผิดชอบในการปฏิบัติงานและการควบคุมจะถูกแบ่งแยกตามหน้าที่ของพนักงานแต่ละคน แต่ในระบบ Data Base จะมี DBA เข้ามาร่วมรับผิดชอบด้วยตามความเหมาะสม และต้องจำกัดขอบเขตการทำงานของ DBA ไม่ให้เกี่ยวข้องกับการทำงานในห้องคอมพิวเตอร์และการสร้างข้อมูลทุกชนิด

6. สรุป

การควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Controls) ส่วนใหญ่ได้แก่ การควบคุมภายในฝ่ายคอมพิวเตอร์ให้แน่ใจว่า

1) การควบคุมการพัฒนาและการปรับปรุงแก้ไขโปรแกรมและระบบงาน (Implementation Controls) การเขียนโปรแกรมมีความเหมาะสม
2) มีการรักษาความปลอดภัยโปรแกรม (Program Security Controls) ที่รัดกุม สามารถป้องกันการเปลี่ยนแปลงแก้ไขโปรแกรมโดยไม่ได้รับอนุญาตได้
3) มีการควบคุมการปฏิบัติงานประมวลผลตามโปรแกรมที่กำหนดไว้อย่างสม่ำเสมอ (Computer Operations Controls)
4) มีการรักษาความปลอดภัยแฟ้มข้อมูล (Data File Security Controls) ที่รัดกุม สามารถป้องกันการใช้แฟ้มข้อมูลโดยไม่ได้รับอนุญาตได้

แม้ว่าผู้ตรวจสอบจะไม่เชื่อถือในการควบคุมที่ใช้อยู่ในขณะนั้นก็ตาม ผู้ตรวจสอบควรประเมินการควบคุมในศูนย์คอมพิวเตอร์เป็นครั้งคราว เพื่อชี้ให้เห็นจุดอ่อนในการบริหารด้านคอมพิวเตอร์ที่ได้ตรวจพบต่อผู้บริหารของธนาคาร ทั้งนี้เพราะจุดอ่อนในการบริหารงานด้านคอมพิวเตอร์จะเป็นสิ่งที่ทำให้การดำเนินงานของธนาคารโดยส่วนรวมขาดประสิทธิภาพ

22

การตรวจสอบระบบการควบคุม

การตรวจสอบระบบการควบคุม

1. การตรวจสอบทั่วไป

1.1 วัตถุประสงค์และขอบเขตของการตรวจสอบ

ผู้ตรวจสอบจะต้องใช้วิธีการตรวจสอบที่เหมาะสม เพื่อให้ได้หลักฐานและความมั่นใจว่าธนาคารพาณิชย์ได้ปฏิบัติตามระบบการควบคุมภายในอย่างเหมาะสมและต่อเนื่องตลอดงวดการบัญชีที่ตรวจสอบ การตรวจสอบเช่นนี้เรียกว่า การตรวจสอบระบบการควบคุม (Functional Tests หรือ Compliance Tests หรือ Procedural Tests)

โดยปกติผู้ตรวจสอบจะทำการตรวจสอบระบบการควบคุมภายหลังจากที่ประเมินคำตอบจากแบบสอบถามแล้วว่าสามารถให้ความเชื่อถือต่อระบบการควบคุมนั้นได้ ทั้งนี้เพื่อลดขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Tests) ลง อย่างไรก็ตามผู้ตรวจสอบอาจไม่ทำการตรวจสอบระบบการควบคุมก็ได้ หากพิจารณาเห็นว่าการขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินจะช่วยให้คำตอบหรือยืนยันการปฏิบัติตามระบบการควบคุมภายในได้ด้วยเป็นอย่างดี

ผู้ตรวจสอบมักจะเข้มงวดและเชื่อถือการปฏิบัติตามระเบียบข้อบังคับ หรือความมีกฎเกณฑ์การควบคุม (Disciplines) มากกว่าการควบคุมขั้นพื้นฐาน (Basic Controls) เพราะหากธนาคารมีระเบียบข้อบังคับการควบคุมภายในใช้อยู่ ก็เป็นหลักประกันประการหนึ่งว่าธนาคารได้เอาใจใส่เข้มงวดการควบคุมภายใน ผู้ตรวจสอบจึงควรให้ความสนใจและตรวจสอบกฎเกณฑ์การควบคุมเป็นอันดับแรก

1.2 การจัดทำเอกสารประกอบการตรวจสอบ

ผู้ตรวจสอบจะต้องทำบันทึกการตรวจสอบเพื่อรวบรวมและพิจารณาการปฏิบัติตามระบบการควบคุมของธนาคาร ขั้นตอนและบันทึกการตรวจสอบระบบการควบคุม อย่างน้อยควรจะมีดังนี้

1) รายละเอียดวิธีการตรวจสอบ
2) การอ้างอิงแสดงความสัมพันธ์ระหว่างการตรวจสอบแต่ละขั้นกับคำถามในแบบสอบถาม เพื่อความมั่นใจว่าได้ตรวจสอบระบบการควบคุมครบถ้วนและได้ตรวจสอบตรงต่อการควบคุม
3) กำหนดระดับการตรวจสอบ
4) ช่วงเวลาของข้อมูลที่ทำการตรวจสอบ
5) หลักฐานที่ได้ตรวจสอบ
6) รายละเอียดของข้อขัดข้อง (Breakdown) หรือข้อน่าสังเกตที่พบระหว่างการตรวจสอบและสาเหตุ
7) วันที่ตรวจสอบแล้วเสร็จแต่ละขั้นตอน และลายมือชื่อผู้ตรวจสอบ

กระดาษทำการสำหรับบันทึกการตรวจสอบระบบการควบคุมมีรายละเอียดปรากฏตามแผนภาพที่ 22.1 ส่วนวิธีการตรวจสอบที่เป็นมาตรฐานสำหรับการตรวจสอบระบบการควบคุมปรากฏตามภาคผนวก ก.

1.3 ประเภทการตรวจสอบ

การตรวจสอบระบบการควบคุมประกอบด้วยการตรวจสอบ 2 ประเภทร่วมกัน ดังนี้

1.3.1 การตรวจสอบหลักฐาน (Examination of Evidence)

คือ การตรวจสอบการบันทึกรายการ เอกสาร และรายงานกระทบยอดว่าได้ปฏิบัติตามระเบียบข้อบังคับ หรือมีการควบคุมที่ดีหรือไม่ เช่น มีการลงนามกำกับรายการและเอกสารที่สำคัญโดยผู้มีอำนาจหน้าที่อย่างครบถ้วน

แผ่นที่_____
จากจำนวน_____

กระดาษทำการ
บันทึกการตรวจสอบระบบการควบคุม

ธนาคาร_____
การตรวจสอบเพียงวันที่_____ การควบคุม_____

Ref. แบบสอบถาม	รายละเอียดการตรวจสอบ หรือ เหตุผลที่ไม่ตรวจสอบ	ระดับการตรวจสอบ (ร้อยละ)	ช่วงเวลาของข้อมูลที่ตรวจสอบ	หลักฐานการตรวจสอบ (Ref. กระดาษทำการ)	ข้อสังเกต	ผู้ตรวจสอบและวันที่ตรวจสอบ

แผนภาพที่ 22.1 กระดาษทำการ "บันทึกการตรวจสอบระบบการควบคุม"

1.3.2 การสอบทานการปฏิบัติงาน (Reperformance)

คือ การทดสอบปฏิบัติงานซ้ำรอยของพนักงานธนาคาร เช่น คำนวณวิเคราะห์และกระทบยอด เป็นต้น หากพบข้อผิดพลาดหรือข้อบกพร่องจากการสอบทานการปฏิบัติงาน ผู้ตรวจสอบก็ไม่อาจให้ความเชื่อถือต่อการตรวจสอบหลักฐานที่ปฏิบัติไปแล้วได้

การควบคุมใดที่ผู้ตรวจสอบไม่อาจใช้วิธีการตรวจสอบโดยการตรวจสอบหลักฐาน และสอบทานการปฏิบัติงานได้ ผู้ตรวจสอบอาจใช้วิธีการสอบถามหรือสังเกตการณ์การปฏิบัติงานจริง (Observation) อย่างไรก็ตามวิธีการนี้มีข้อบกพร่อง เพราะไม่อาจวางใจได้ว่าในช่วงเวลาอื่นนอกเหนือจากช่วงเวลาที่สังเกตการณ์ได้มีการปฏิบัติตามระบบการควบคุม หรือมีการควบคุมที่ดีหรือไม่ กรณีเช่นนี้ผู้ตรวจสอบอาจใช้วิธีขอคำยืนยันจากธนาคารก็ได้

2. การตรวจสอบในระบบคอมพิวเตอร์

2.1 ลักษณะของการตรวจสอบ

การตรวจสอบระบบการควบคุมในระบบคอมพิวเตอร์ มีวัตถุประสงค์เช่นเดียวกับการตรวจสอบในระบบเดิมที่มิได้ใช้คอมพิวเตอร์ แต่โดยที่การควบคุมในระบบคอมพิวเตอร์มีความแตกต่างไปจากเดิม เทคนิคและขอบเขตการตรวจสอบระบบการควบคุมจึงแตกต่างไปด้วย

ก่อนที่จะตัดสินใจตรวจสอบระบบการควบคุมในระบบคอมพิวเตอร์ ผู้ตรวจสอบพึงระลึกว่ามีวิธีการตรวจสอบอย่างอื่นอย่างน้อย 2 วิธี ซึ่งผู้ตรวจสอบอาจเลือกวิธีใดวิธีหนึ่งมาใช้ก็ได้ และได้ผลการตรวจสอบระบบการควบคุมอย่างมีประสิทธิภาพด้วยเช่นกัน หรือไม่จำเป็นต้องตรวจสอบระบบการควบคุมก็ได้ คือ

1) การใช้โปรแกรมคอมพิวเตอร์ (Computer Program) ช่วยในการตรวจสอบ ทบทวน และแยกประเภทข้อมูลที่ประมวลผลจำนวนมาก การใช้โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบ เป็นการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) ที่มีประสิทธิภาพมากเช่นกัน

2) การเพิ่มระดับและขยายการทดสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) แทนการตรวจสอบระบบการควบคุมในเรื่องของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ผู้ตรวจสอบอาจจำกัดการตรวจสอบความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ได้ โดยการเพิ่มการตรวจสอบระบบและตัวโปรแกรม หรือเมื่อได้พิจารณาแล้วว่าได้มีการควบคุมทางด้านผู้ใช้ (User Controls) อย่างได้ผล

2.2 เทคนิคการตรวจสอบ

เทคนิคการตรวจสอบจะแยกกล่าวตามหัวข้อการควบคุมต่อไปนี้

- กฎเกณฑ์การควบคุม (Disciplines)
- การควบคุมทางด้านผู้ใช้ (User Controls)
- การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls)
- การควบคุมโดยขั้นตอนการทำงานของโปรแกรม (Programmed Procedures)

2.2.1 การตรวจสอบกฎเกณฑ์การควบคุม

โดยที่กล่าวมาแล้วในบทที่ 3 ว่า กฎเกณฑ์การควบคุมประกอบด้วย การกำกับ (Supervisory Controls) การแบ่งแยกหน้าที่ (Segregation of Duties) และการควบคุมทรัพย์สิน (Custodial Controls) การตรวจสอบระบบการควบคุมทั้ง 3 แบบทำได้ดังนี้

1) การกำกับ

การตรวจสอบว่าได้มีการกำกับ (Supervisory Controls) ใช้อยู่หรือไม่ วิธีที่สำคัญคือตรวจสอบจากหลักฐาน (Examination of Evidence) ได้แก่ การตรวจสอบการลงนามของผู้มีหน้าที่กำกับ เช่น ในการควบคุมทางด้านผู้ใช้ ได้มีการสอบสวนและลงลายมือชื่อกำกับรายการที่เครื่องไม่ยอมรับ (Rejection Reports) หรือรายการที่มีข้อสังเกตผิดปกติ (Exception Reports) หรือไม่ หรือการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ได้มีการลงลายมือชื่อโดยผู้มีอำนาจในแบบฟอร์มขอแก้ไขโปรแกรม (Program Change Form) หรือไม่ นอกจากนั้นยังตรวจสอบได้จากหลักฐานบันทึกโต้ตอบภายใน ซึ่งอาจระบุวิธีการหรือการอนุมัติให้ทำลายหรือยกเลิกรายการบันทึกหรือเอกสารที่ผิดพลาดหรือที่ไม่น่าพอใจ ในกรณีที่เห็นสมควรผู้ตรวจสอบควรขอตรวจสอบเอกสารหลักฐานต่าง ๆ ที่ผ่านมือผู้มีอำนาจหน้าที่กำกับว่าครบถ้วนเพียงพอหรือไม่ เช่น ในการทดสอบโปรแกรมได้ส่งรายละเอียดของข้อมูลตัวอย่างที่ทำการทดสอบกับผลของการทดสอบให้ผู้มีอำนาจหน้าที่กำกับตรวจสอบโดยครบถ้วนหรือไม่ ผู้ตรวจสอบควรเข้าไปสังเกตการณ์วิธีการควบคุมรายการหรือข้อมูลขณะประมวลผล และการจัดทำรายงานต่าง ๆ ในขณะใดขณะหนึ่งด้วย

การตรวจสอบการกำกับโดยใช้วิธีสอบทานการปฏิบัติงาน (Reperformance) อาจไม่ได้ผลเต็มที่นัก หรือไม่อาจทำได้เนื่องจากผู้ตรวจสอบไม่อาจที่จะรู้หรือไม่มีประสบการณ์ในการควบคุมแบบนี้ หรืออาจเป็นเพราะการกำกับบางอย่างขึ้นอยู่กับการตัดสินใจของผู้มีอำนาจหน้าที่กำกับ จึงไม่ปรากฏหลักฐานให้สอบทานการปฏิบัติงานได้

การตรวจสอบการกำกับควรใช้ข้อมูลเดียวกันกับการตรวจสอบการควบคุมแบบอื่น ๆ เพราะจะให้ประสิทธิภาพในการตรวจสอบเป็นอย่างมาก ข้อบกพร่องที่พบจากการตรวจสอบการควบคุมอื่น ๆ ในข้อมูลหรือหลักฐานการตรวจสอบเดียวกัน จะยืนยันให้เห็นว่าการกำกับไม่มีประสิทธิภาพเพียงพอ

2) การแบ่งแยกหน้าที่และการควบคุมทรัพย์สิน

การตรวจสอบการแบ่งแยกหน้าที่และการควบคุมทรัพย์สิน ทำได้โดยการตรวจสอบลายมือชื่อและการลงนามกำกับในเอกสารและรายการ ตลอดจนใช้วิธีสังเกตการณ์และขอคำยืนยันยอด โดยปกติแล้วไม่อาจใช้วิธีการสอบทานการปฏิบัติงานเพื่อตรวจสอบการควบคุมทั้ง 2 ประเภทนี้อย่างได้ผล

ตัวอย่างการตรวจสอบการควบคุมทางด้านผู้ใช้ (User Controls) ได้แก่ การตรวจสอบการลงนามและลายมือชื่อกำกับรายงานการกระทบยอดและรายงานข้อผิดสังเกต เพื่อพิสูจน์ว่าผู้ที่ทำหน้าที่ควบคุมทางด้านผู้ใช้มิใช่บุคคลเดียวกันกับผู้ปฏิบัติการคอมพิวเตอร์ ผู้ตรวจสอบควรพิสูจน์การแบ่งแยกหน้าที่ทั้งในด้านการออกแบบระบบงาน การจัดทำโปรแกรม และการปฏิบัติการคอมพิวเตอร์ ผู้ตรวจสอบควรเข้าไปสังเกตการณ์การปฏิบัติงานในแผนกต่าง ๆ ที่เกี่ยวข้อง เพื่อตรวจสอบว่าได้มีการปฏิบัติงานโดยอิสระจากกันจริง

ในการควบคุมทรัพย์สินซึ่งเป็นส่วนหนึ่งของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ผู้ตรวจสอบจะต้องตรวจสอบดูว่าระเบียบคำสั่งที่ใช้บังคับแก่พนักงานผู้เกี่ยวข้องมีความเหมาะสมเพียงใด และควรเข้าไปสังเกตการณ์มาตรการรักษาความปลอดภัยว่าได้มีการปฏิบัติตามหรือไม่ นอกจากนั้นควรตรวจสอบบุคคลผู้ปฏิบัติหน้าที่ว่าตรงกับคำสั่งแต่งตั้งหรือไม่ โดยเฉพาะอย่างยิ่งในส่วนของการแบ่งแยกหน้าที่ เช่น ระหว่างผู้พัฒนาระบบงานกับผู้รักษาระบบงาน ผู้ปฏิบัติการคอมพิวเตอร์กับผู้เก็บรักษาแฟ้มข้อมูล เป็นต้น ผู้ตรวจสอบควรตรวจสอบผังการจัดองค์การ (Organization Charts) ของศูนย์คอมพิวเตอร์และรายละเอียดตำแหน่งงาน (Job Description) เพื่อพิสูจน์ว่าได้มีการแบ่งแยกหน้าที่อย่างชัดเจนทั้งในระหว่างการปฏิบัติงานปกติ และการปฏิบัติงานนอกเวลาทำการ นอกจากนั้นควรพิสูจน์ข้อเท็จจริงดังกล่าวโดยการเข้าไปสังเกตการณ์ศูนย์คอมพิวเตอร์และห้องปฏิบัติการขณะใดขณะหนึ่งด้วย และควรตรวจสอบตารางการปฏิบัติงาน (Work Schedules) รายงานเวลาใช้คอมพิวเตอร์ (Time Report) รายละเอียดการปฏิบัติงานของผู้ปฏิบัติการคอมพิวเตอร์ที่พิมพ์โดยเครื่อง (Operator Logs) ตลอดจนเอกสารอื่น ๆ ในลักษณะที่กล่าวเพื่อตรวจสอบว่าการปฏิบัติงานจริงสอดคล้องกับวิธีการที่กำหนดไว้

2.2.2 การตรวจสอบการควบคุมทางด้านผู้ใช้

การตรวจสอบระบบการควบคุมทางด้านผู้ใช้ โดยปกติสามารถใช้ได้ทั้งวิธีตรวจสอบหลักฐานและวิธีสอบทานการปฏิบัติงาน ผู้ตรวจสอบจะไม่ประสบปัญหายุ่งยากในการตรวจสอบด้านนี้นัก เพราะเอกสารหลักฐานเกี่ยวกับการควบคุมสามารถมองเห็นได้ อย่างไรก็ตามการตรวจสอบการปฏิบัติงานที่มีปริมาณสูงนั้น หากใช้วิธีสอบทานการปฏิบัติงานก็ไม่สู้จะเหมาะสม

2.2.3 การตรวจสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์

ผู้ตรวจสอบจะต้องตรวจสอบระบบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ซึ่งปกติจะเป็นการตรวจสอบด้วยมือ (Manually) และสุ่มตัวอย่างทดสอบการทำงานของโปรแกรมระบบคอมพิวเตอร์ (System Software Procedures) ผู้ตรวจสอบจะต้องเลือกและตัดสินใจว่าจะเลือกใช้โปรแกรมระบบโปรแกรมใด และจำนวนมากน้อยเพียงไร เพื่อทำการทดสอบและยืนยันการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ โดยเฉพาะการควบคุมการพัฒนาและใช้โปรแกรมระบบและการรักษาความปลอดภัยแก่โปรแกรมระบบ

การตรวจสอบระบบการควบคุมในส่วนของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์โดยการตรวจสอบด้วยมือ ได้แก่ การตรวจสอบหลักฐานการสอบทานการปฏิบัติงานและการสังเกตการณ์ การตรวจสอบส่วนใหญ่คล้ายคลึงกับการตรวจสอบทางด้านผู้ใช้ ได้แก่ การตรวจสอบจากรายงานคอมพิวเตอร์ และการตรวจสอบบางด้านจะคล้ายคลึงกับการตรวจสอบในระบบที่มิได้ใช้คอมพิวเตอร์ เช่น การตรวจสอบการควบคุมการแก้ไขเปลี่ยนแปลงโปรแกรม เป็นต้น การตรวจสอบหลักฐานเป็นการตรวจสอบที่สำคัญเพราะไม่อาจใช้วิธีการสอบทานการปฏิบัติงานได้เสมอไป ฉะนั้นผู้ตรวจสอบจึงควรตรวจสอบเอกสารประกอบระบบงาน (System Descriptions) และคู่มือปฏิบัติการคอมพิวเตอร์ (Operating Instructions) อย่างถี่ถ้วนถึงความเพียงพอและความสมบูรณ์ของเอกสารดังกล่าว

การตรวจสอบโปรแกรมของระบบมีวิธีการตรวจสอบที่สามารถนำมาใช้ได้หลายวิธี ขึ้นอยู่กับลักษณะของการปฏิบัติงานที่จะตรวจสอบ ตัวอย่าง เช่น การตรวจสอบ Cataloguing Procedures ก็อาจใช้ข้อมูลตัวอย่างทดสอบ (Audit Test Data) หรือใช้วิธีวิเคราะห์รหัสโปรแกรม (Program Code Analysis) เพื่อพิสูจน์ว่าโปรแกรมใหม่ ๆ หรือโปรแกรมที่แก้ไขใหม่ได้ Catalogued เป็นที่เรียบร้อยและน่าพอใจหรือไม่ นอกจากที่กล่าวแล้วยังอาจพัฒนาโปรแกรมคอมพิวเตอร์ (Computer Program) ขึ้นมาช่วยในการตรวจสอบโปรแกรมของระบบได้ ดังนี้

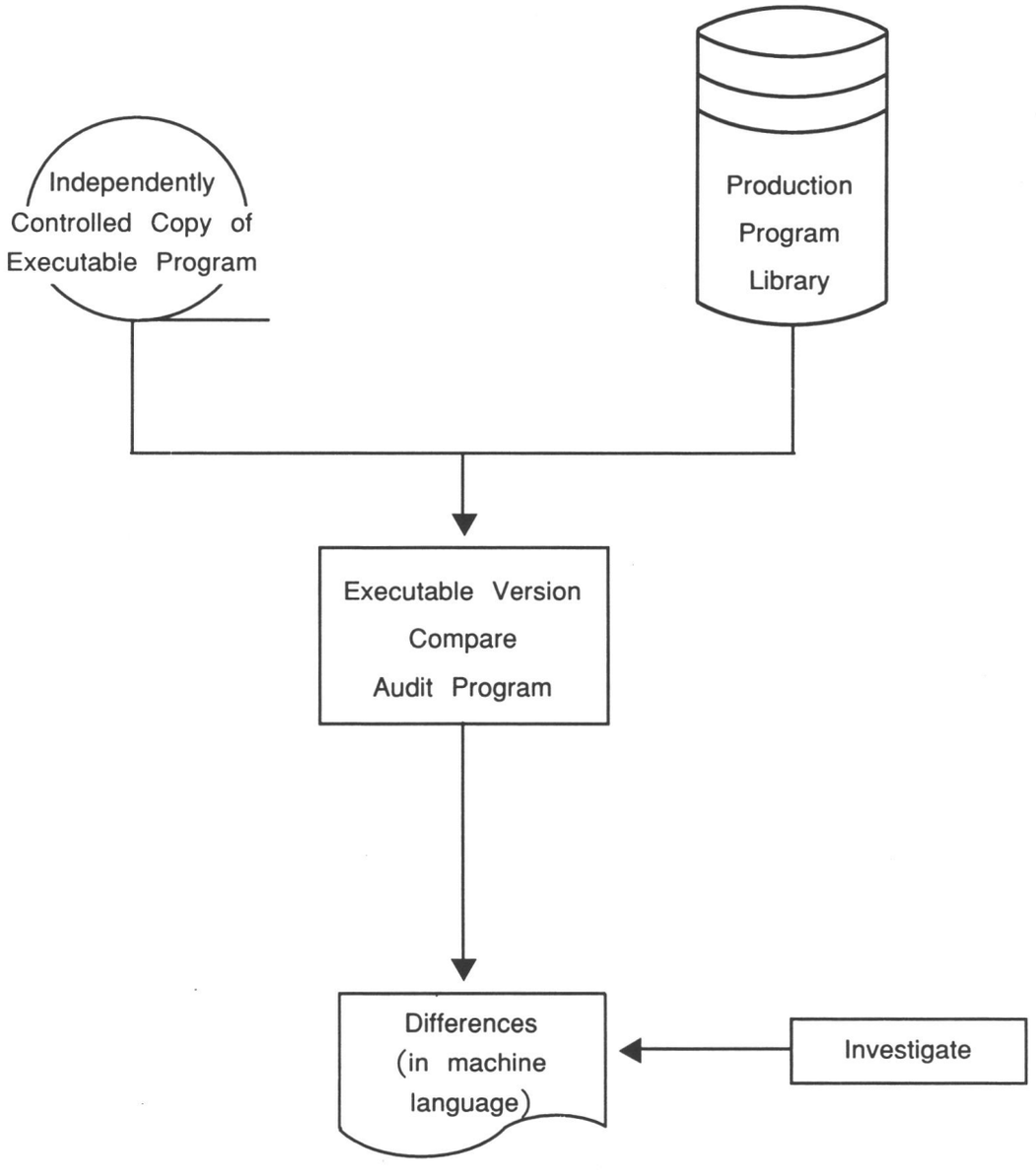
1) โปรแกรมที่ใช้ตรวจสอบว่าได้มีการเปลี่ยนแปลงแก้ไขโปรแกรมของระบบโดยได้รับอนุญาต หรือโดยถูกต้องหรือไม่ ทั้งนี้โดยการนำโปรแกรมของระบบที่ใช้ปฏิบัติงานขณะนั้นมาเปรียบเทียบกับโปรแกรมสำเนาที่เก็บไว้ภายใต้การควบคุมอย่างอิสระ แล้วรายงานข้อแตกต่างที่เกิดขึ้น (แผนภาพที่ 22.2 และ 22.3)

2) โปรแกรมที่ใช้วิเคราะห์และรายงานข้อมูลที่เก็บไว้ใน System Log ซึ่งผู้ตรวจสอบจะนำมาเปรียบเทียบกับรายงานที่ธนาคารพาณิชย์จัดทำให้เพื่อหาข้อแตกต่างได้ (แผนภาพที่ 22.4)

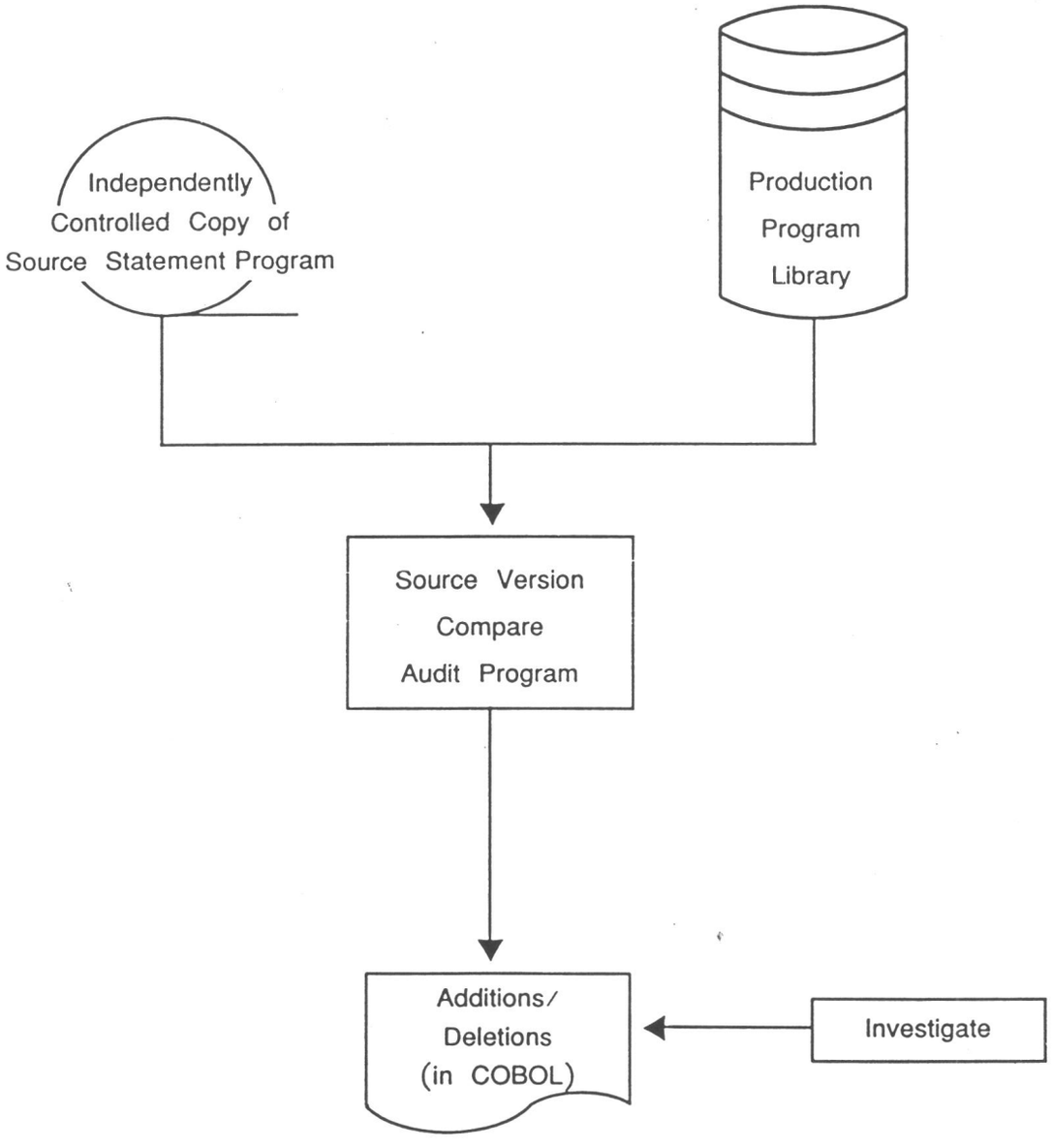
การทดสอบโปรแกรมของระบบที่ใช้ในการคุ้มครองรหัสลับเฉพาะผู้มีหน้าที่ในการปฏิบัติการ (Password Protection) อาจทำได้โดยผู้ตรวจสอบทดลองใช้รหัสลับที่มิได้รับอนุญาตผ่านเข้าไปทางเครื่องเทอร์มินอล อย่างไรก็ตามก่อนที่จะใช้เทคนิคใด ๆ ผู้ตรวจสอบพึงระมัดระวังผลกระทบที่มีต่อการประมวลผลด้วย

2.2.4 การตรวจสอบขั้นตอนการทำงานของโปรแกรม

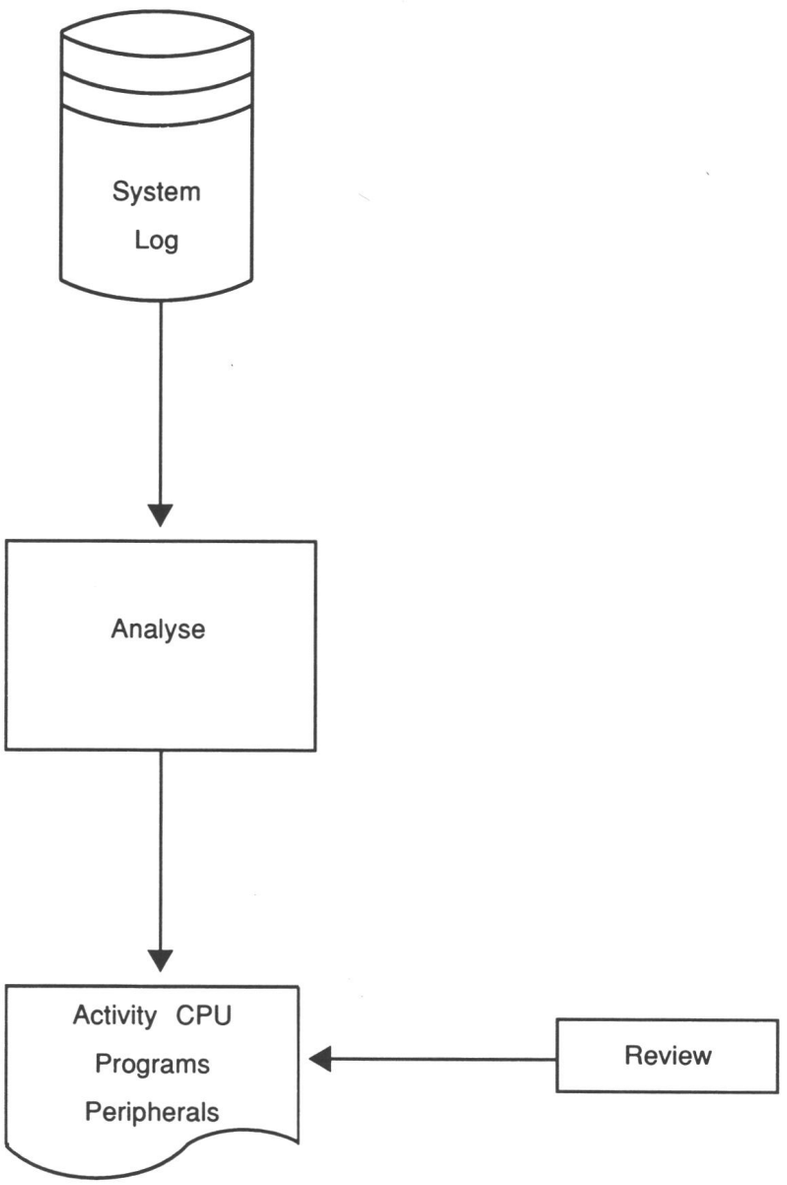
ในขณะที่ผู้ตรวจสอบดำเนินการตรวจสอบระบบการควบคุมในด้านการควบคุมการพัฒนาและใช้ระบบงาน (Implementation Controls) โดยวิธีสอบทานการปฏิบัติงาน (Reperformance) นั้น ก็เท่ากับเป็นการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ด้วยส่วนหนึ่ง นอกจากนั้นการตรวจสอบขั้นตอนการทำงานของโปรแกรมยังแทรกอยู่ส่วนหนึ่งของการตรวจสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ นั่นคือ การตรวจสอบว่าได้มีการจัดสร้างและใช้ขั้นตอนของโปรแกรมอย่างเหมาะสม และโดยต่อเนื่อง อย่างไรก็ตามผู้ตรวจสอบก็ควรที่จะตรวจสอบขั้นตอนการทำงานของโปรแกรมโดยเฉพาะด้วยเพื่อความสมบูรณ์ของการตรวจสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ และเพื่อให้ได้หลักฐานว่าได้มีการควบคุมดังกล่าวโดยต่อเนื่อง



แผนภาพที่ 22.2 การตรวจสอบโปรแกรมปฏิบัติงาน (Executable Program)



แผนภาพที่ 22.3 การตรวจสอบโปรแกรมจากต้นฉบับ (Source Statement Programs)



แผนภาพที่ 22.4 **การวิเคราะห์** System Log

การตรวจสอบขั้นตอนการทำงานของโปรแกรม ปกติจะใช้วิธีสอบทานการปฏิบัติงาน เพราะเป็นการยากหรือไม่เหมาะสมที่จะตรวจสอบจากหลักฐาน อย่างไรก็ตามหลักฐานบางอย่าง เช่น รายงานข้อผิดพลาดจากรายการที่ประมวลผลก็อาจใช้เป็นหลักฐานเบื้องต้นยืนยันว่าการควบคุมโดยขั้นตอนการปฏิบัติงานของโปรแกรมได้มีใช้อยู่ และโดยต่อเนื่องหรือไม่ การตรวจสอบจากหลักฐานนี้ปกติจะกระทำเป็นส่วนหนึ่งของการตรวจสอบการควบคุมทางด้านผู้ใช้ (User Controls)

เทคนิคสำคัญของการตรวจสอบขั้นตอนการทำงานของโปรแกรม ประกอบด้วย การทดสอบด้วยมือ (Manual Tests) การใช้ข้อมูลตัวอย่างตรวจสอบ (Audit Test Data) การวิเคราะห์รหัสโปรแกรม (Program Code Analysis) และการใช้โปรแกรมตรวจสอบ (Computer Audit Programs) การเลือกที่จะใช้เทคนิคใดก็ตามขึ้นอยู่กับว่าจะมีหลักฐานที่มองเห็นได้ให้ตรวจสอบหรือไม่

1) การขาดหลักฐานที่มองเห็นได้

โดยปกติรายงานที่คอมพิวเตอร์พิมพ์ออกมาให้นั้นจะไม่มีรายละเอียด ซึ่งเป็นลักษณะอย่างหนึ่งของการประมวลผลด้วยคอมพิวเตอร์ ด้วยเหตุที่ขาดรายละเอียดหรือขาดรายงานบางอย่างไป ผู้ตรวจสอบจึงไม่อาจใช้วิธีการตรวจสอบหลักฐานในการตรวจสอบขั้นตอนการทำงานของโปรแกรมได้ ความยุ่งยากที่เกิดขึ้นมี 2 แบบ คือ แบบแรก คอมพิวเตอร์อาจจะพิมพ์ยอดรวมและยอดประกอบยอดรวม แต่มิได้ให้รายละเอียดประกอบส่วนแบบที่ 2 หลักฐานที่ได้ไม่แน่ชัดเพียงพอ เช่น กรณีที่คอมพิวเตอร์พิมพ์รายงานที่มีข้อสังเกต (Exception Reports) หรือรายงานเกี่ยวกับรายการที่เครื่องไม่ยอมรับ (Rejected Items) ผู้ตรวจสอบไม่อาจเชื่อมั่นได้ว่ารายการที่มีข้อสังเกตหรือที่คอมพิวเตอร์ไม่ยอมรับได้พิมพ์ออกมาโดยครบถ้วนหรือไม่ ข้อยุ่งยากทั้ง 2 แบบนี้เรียกว่าการขาดร่องรอยการตรวจสอบ อย่างไรก็ตามการขาดร่องรอยการตรวจสอบมิได้หมายความว่ามีข้อบกพร่องในระบบการควบคุม ผู้ตรวจสอบจำเป็นต้องเปลี่ยนแปลงเทคนิคการตรวจสอบให้สอดคล้องกับร่องรอยการตรวจสอบที่ขาดหายไปด้วย

2) การทดสอบด้วยมือ (Manual Tests)

การตรวจสอบขั้นตอนการทำงานของโปรแกรมโดยการทดสอบด้วยมือ สามารถทำได้ในกรณีที่หลักฐานมีปรากฏอย่างครบถ้วน เช่น รายการบัญชี (Statements) ของลูกหนี้ ได้แสดงรายละเอียดความเคลื่อนไหวทุกรายการ ซึ่งสามารถทำให้ทดสอบการผ่านบัญชีได้ เป็นต้น การทดสอบยังอาจทำได้โดยปฏิบัติงานด้วยมือซ้ำกับการทำงานด้วยขั้นตอนการทำงานของโปรแกรมแล้วเปรียบเทียบผลลัพธ์ที่ได้

ในกรณีที่หลักฐานมีปรากฏไม่ครบถ้วน ผู้ตรวจสอบสามารถที่จะสร้างหลักฐานเพื่อการตรวจสอบได้ด้วยวิธีต่อไปนี้

ก. นำข้อมูลที่ประมวลผลแล้วมารวบรวมปรับปรุงใหม่ให้อยู่ในสภาพเดียวกับขณะที่ใช้ขั้นตอนการทำงานของโปรแกรมทำการประมวลผล

ข. รวบรวมและตรวจสอบจากข้อมูลปัจจุบันก่อนที่จะทำการประมวลผลด้วยคอมพิวเตอร์ ตัวอย่าง เช่น ทดสอบยอดรวมของ Batches เป็นต้น

ค. เลือกข้อมูลจำนวนหนึ่งจากข้อมูลทั้งหมดมาทำการประมวลผลด้วยมือต่างหาก แล้วเปรียบเทียบกับผลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์

ง. เลือกทดสอบเงื่อนไขของขั้นตอนการทำงานของโปรแกรม ซึ่งหากมีประสิทธิภาพเพียงพอและมีความเหมาะสมแล้ว จะรายงานข้อผิดพลาดที่ตรงตามเงื่อนไขนั้นออกมา เช่น ดึงเอกสารบางอย่างไว้ไม่ส่งเข้าไปประมวลผล หรือแก้ตัวเลขให้ผิดพลาด เป็นต้น ซึ่งขั้นตอนการทำงานของโปรแกรมดังกล่าวจะต้องรายงานข้อผิดพลาดออกมา

จ. ขอให้คอมพิวเตอร์พิมพ์รายงานพิเศษให้ในกรณีที่ไม่มีหลักฐานที่มองเห็นได้เลย และไม่สามารถใช้วิธีสร้างหลักฐานเพื่อการตรวจสอบอย่างใดอย่างหนึ่งได้ การทดสอบด้วยมือก็ไม่สามารถทำได้ จึงควรเปลี่ยนไปใช้วิธีการตรวจสอบอย่างอื่นแทน

3) การสร้างข้อมูลตัวอย่างทดสอบ (Audit Test Data)

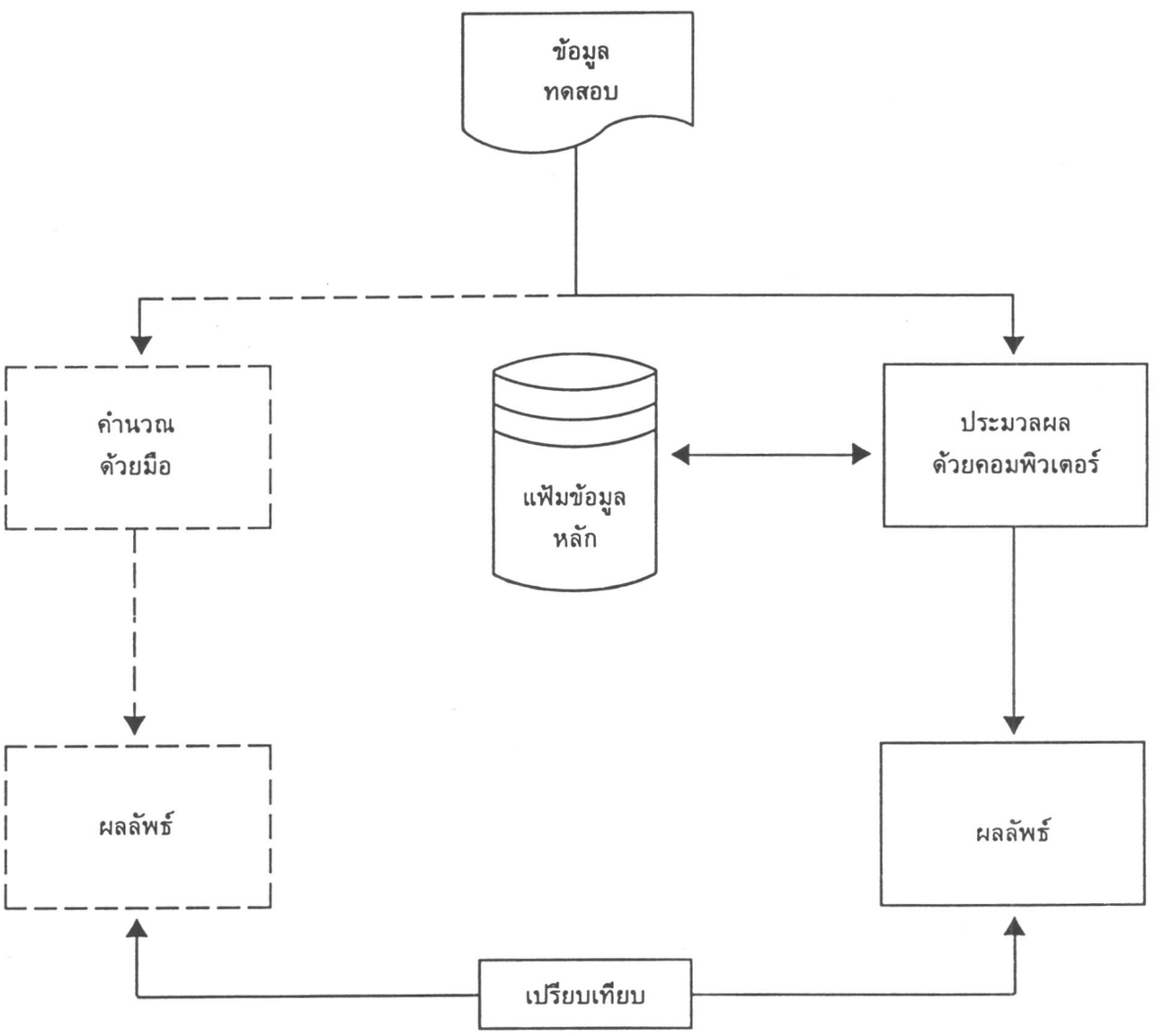
เป็นวิธีการสร้างข้อมูลขึ้นมาชุดหนึ่ง แล้วคำนวณผลลัพธ์ที่จะได้ไว้ล่วงหน้า หลังจากนั้นส่งข้อมูลตัวอย่างดังกล่าวไปทดสอบกับขั้นตอนการทำงานของโปรแกรมเปรียบเทียบผลลัพธ์ที่ได้จากคอมพิวเตอร์กับผลลัพธ์ที่ทราบล่วงหน้านั้น เทคนิคนี้มีความเหมาะสมมากในกรณีที่ไม่มีหลักฐานที่มองเห็นได้ให้ตรวจสอบเลย และการทดสอบด้วยมือไม่ได้ผล

เทคนิคการใช้วิธีการสร้างข้อมูลตัวอย่างทดสอบปรากฏตามแผนภาพที่ 22.5

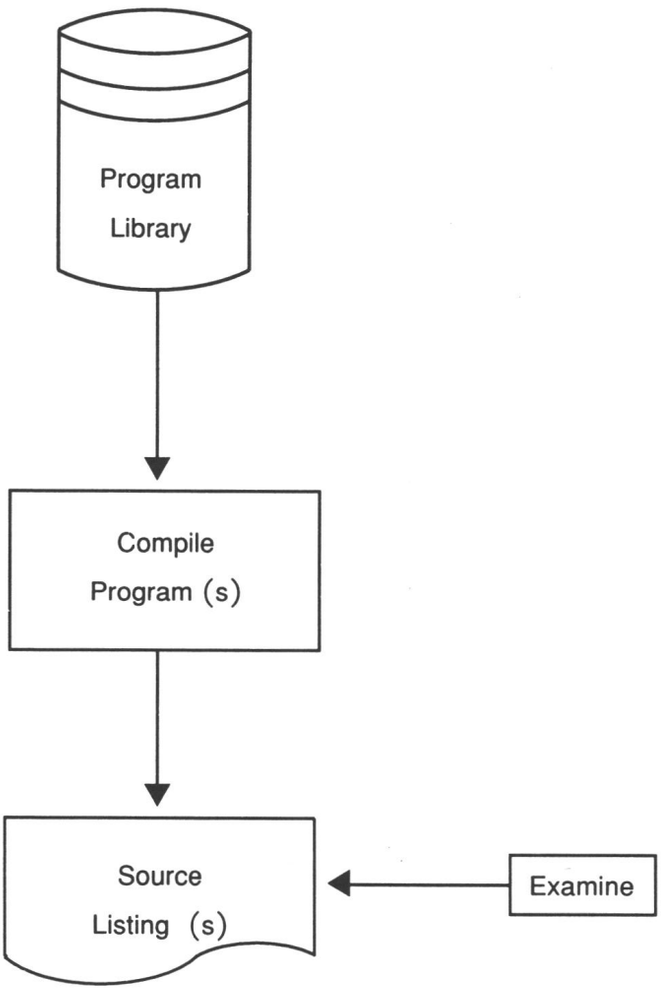
4) การวิเคราะห์รหัสโปรแกรม (Program Code Analysis)

หมายถึง การตรวจสอบโปรแกรมปฏิบัติการ (Operational Programs) จากโปรแกรมต้นฉบับที่คอมพิวเตอร์พิมพ์ออกมาให้ (Source Listing) เพื่อพิสูจน์ว่าขั้นตอนการทำงานของโปรแกรมที่เกี่ยวข้องได้ถูกใช้และให้รหัสอย่างถูกต้องหรือไม่ เทคนิคการตรวจสอบเช่นนี้ต้องการความรู้และทักษะทางด้านโปรแกรมอย่างสูง ผู้ตรวจสอบจะต้องตรวจสอบว่ารหัสที่ปรากฏในโปรแกรมต้นฉบับ (Source Listing) ไม่แตกต่างจากโปรแกรมปฏิบัติการที่ใช้ในการประมวลผลจริง เทคนิคการวิเคราะห์รหัสโปรแกรมปรากฏตามแผนภาพที่ 22.6





แผนภาพที่ 22.5 การสร้างข้อมูลตัวอย่างทดสอบ (Audit Test Data)



แผนภาพที่ 22.6 การวิเคราะห์รหัสโปรแกรม (Program Code Analysis)

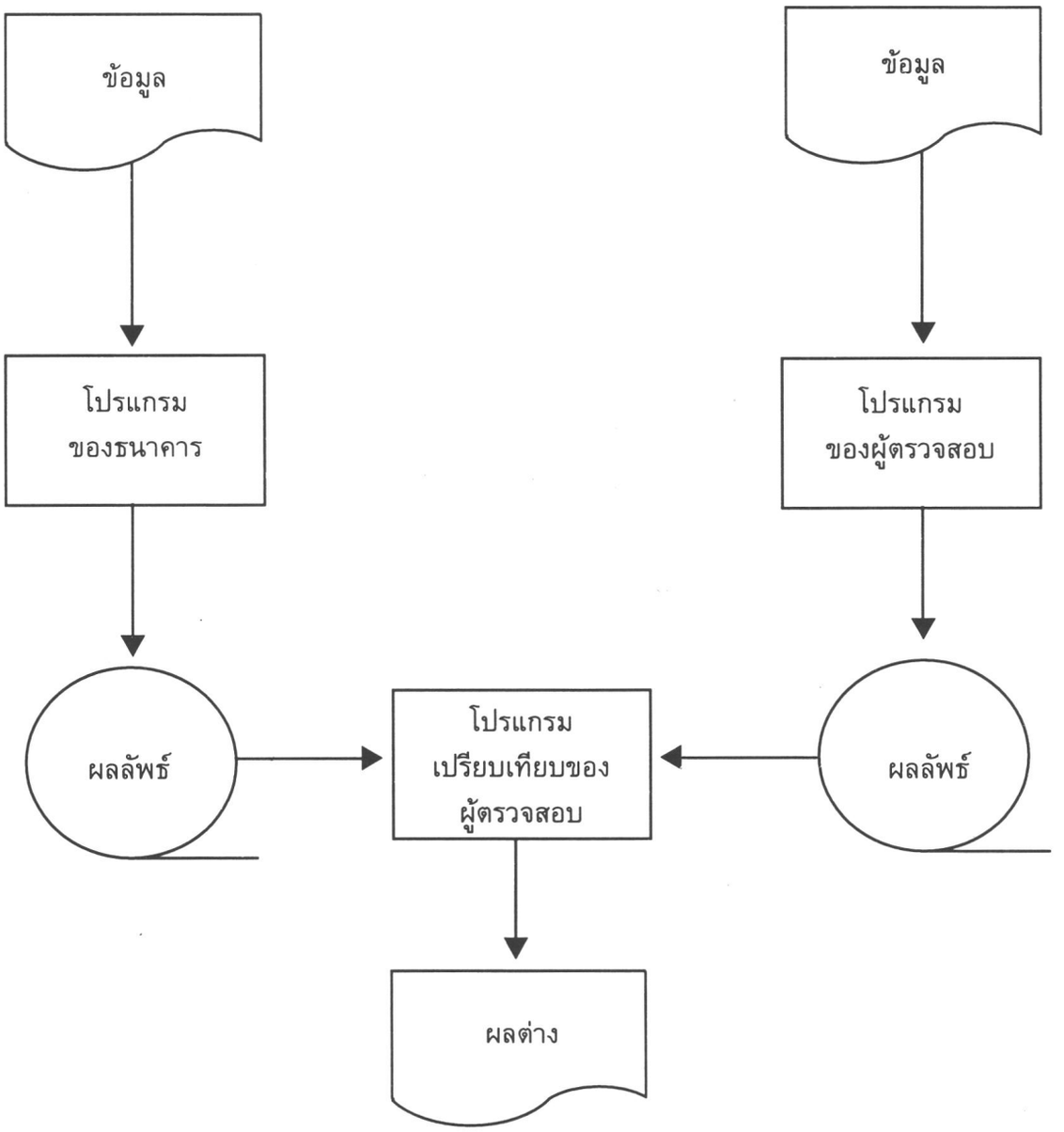
5) การตรวจสอบโดยใช้โปรแกรมคอมพิวเตอร์ (Computer Program)

โดยปกติผู้ตรวจสอบจะสร้างโปรแกรมคอมพิวเตอร์ของผู้ตรวจสอบขึ้นมา เพื่อช่วยในการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) แต่ก็อาจสร้างโปรแกรมขึ้นมาเพื่อช่วยในการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ซึ่งเรียกว่าการทดสอบโดยแบบจำลอง (Simulation) ด้วยก็ได้ โดยหลักพื้นฐานแล้วไม่มีความแตกต่างกันสำหรับการใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) กับการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ข้อแตกต่างที่สำคัญคือ ในการใช้โปรแกรมคอมพิวเตอร์เพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรมของธนาคาร ซึ่งเป็นการทดสอบโดยแบบจำลองนั้นมีวัตถุประสงค์เพื่อตรวจสอบว่าโปรแกรมของธนาคารได้ประมวลผลโดยถูกต้องหรือไม่ โดยตรวจสอบตัวเลขหรือผลการคำนวณโปรแกรมของธนาคาร แต่ในกรณีที่สร้างโปรแกรมคอมพิวเตอร์เพื่อตรวจสอบความถูกต้องของรายการทางการเงิน โปรแกรมของผู้ตรวจสอบจะถูกใช้เพื่อสร้างและตระเตรียมข้อมูลจากแฟ้มข้อมูลต่าง ๆ ของธนาคารที่เกี่ยวข้อง เพื่อเป็นข้อมูลสำหรับใช้ในการตรวจสอบต่อไป

ปัญหาในทางปฏิบัติของการใช้โปรแกรมของผู้ตรวจสอบเพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรมของธนาคาร คือ การย่นย่อ (Short-out) โปรแกรมที่สลับซับซ้อนของธนาคารเพื่อตรวจสอบค่อนข้างยากลำบาก บางครั้งอาจทำให้ผู้ตรวจสอบได้รับตัวเลขที่แตกต่างไปจากการประมวลผลของธนาคาร และอาจต้องเสียเวลาในการแก้ไขโปรแกรมหรือเสียเวลาในการกระทบยอด ด้วยเหตุนี้เทคนิคการใช้โปรแกรมคอมพิวเตอร์เพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรม จึงไม่อาจกล่าวได้ว่ามีประสิทธิภาพดีเสมอไป โดยเฉพาะเมื่อได้มีการทดสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) แล้ว และเห็นว่าการควบคุมดังกล่าวเชื่อถือได้ เพียงแต่ให้มีการสอบทาน (Reperformance) ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) เท่านั้นก็เพียงพอแล้ว อย่างไรก็ตามในบางส่วนที่ผู้ตรวจสอบไม่อาจจะเชื่อถือการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ได้ การใช้โปรแกรมของผู้ตรวจสอบเพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรมก็เป็นทางเลือกที่ดี



เพื่อขยายขอบเขตของการตรวจสอบระบบการควบคุม (Functional Tests) ผู้ตรวจสอบอาจจะแทรกจุดทดสอบลงไปในโปรแกรมตรวจสอบด้วย เช่น การตรวจสอบยอดคงเหลือของลูกหนี้แต่ละครั้งก่อนที่จะปล่อยเงินกู้ครั้งต่อไปมิให้เกินกว่าวงเงินในสัญญา ซึ่งจะช่วยป้องกันมิให้เกิดหนี้สูญรายใหญ่ขึ้น เป็นต้น การตรวจสอบดังกล่าว อาจช่วยให้เพิ่มข้อแนะนำที่ดีในการแก้ไขการปฏิบัติงานและระบบงานของธนาคาร อันเป็นคุณลักษณะอย่างหนึ่งของการตรวจสอบระบบปฏิบัติงานของธนาคาร (Operational Examination)



แผนภาพที่ 22.7 การทดสอบข้อมูลโดยใช้โปรแกรมจำลอง (Simulation)

2.3 ระดับการทดสอบ (Levels of Test)

การกำหนดกฎเกณฑ์ของระดับการทดสอบระบบการควบคุมให้เป็นมาตรฐานตายตัวลงไปเป็นสิ่งที่เป็นไปไม่ได้ ผู้ตรวจสอบจึงควรต้องพิจารณาเป็นกรณี ๆ ไป โดยขึ้นอยู่กับการควบคุม (Basic Control or Discipline) ว่ามีอยู่มากหรือน้อยเพียงไร ซึ่งโดยทั่วไปแล้วถ้าระเบียบหรือการควบคุมมีอยู่มาก ปริมาณหรือระดับการทดสอบก็ควรจะต้องมากขึ้นด้วย และโดยปกติระดับของการตรวจสอบโดยวิธีสอบทานการปฏิบัติงาน (Reperformance) จะต่ำกว่าระดับการตรวจสอบหลักฐาน (Examination of Evidence) แนวทางในการกำหนดระดับการทดสอบของการควบคุม มีดังนี้

2.3.1 การตรวจสอบการควบคุมทางด้านผู้ใช้ (User Controls)

ปกติจะกำหนดระดับของการทดสอบเช่นเดียวกับการตรวจสอบในระบบที่มิได้ใช้คอมพิวเตอร์ที่มีการปฏิบัติการและการควบคุมที่เหมือนกัน

2.3.2 การตรวจสอบความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls)

1) การควบคุมการใช้ระบบงาน (Implementation Controls)

ในกรณีที่ธนาคารพัฒนาระบบงานใหม่ ผู้ตรวจสอบจะต้องตรวจสอบด้วยว่าธนาคารได้มีระเบียบข้อบังคับเพื่อการควบคุมการใช้ระบบงานใหม่ (Disciplines) ที่มีประสิทธิภาพเพียงพอ และได้มีการปฏิบัติตามระเบียบนั้นอย่างเคร่งครัด ถ้าผลการตรวจสอบการปฏิบัติตามระเบียบเป็นที่พอใจ ผู้ตรวจสอบเพียงแต่ทดสอบการควบคุมพื้นฐาน (Basic Control) ของขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ของแต่ละระบบงานก็ย่อมเป็นการเพียงพอ ในการเลือกตัวอย่างทดสอบควรจะได้พิจารณาถึงความสำคัญของระบบงานและการประมวลผล โดยเฉพาะผลที่จะเกิดขึ้นหากระบบงานหรือการประมวลผลนั้นมิได้ดำเนินไปอย่างถูกต้อง

ระดับของการทดสอบการแก้ไขโปรแกรม (Program Changes) อาจเปรียบเทียบได้กับการตรวจสอบในระบบที่มิได้ใช้คอมพิวเตอร์ ซึ่งมีลักษณะของการควบคุมที่คล้ายคลึงกัน และวิธีการตรวจสอบก็คล้ายคลึงกันในทุก ๆ ระบบงาน อย่างไรก็ตามควรจะเลือกตรวจสอบการเปลี่ยนแปลงแก้ไขโปรแกรมที่เกี่ยวข้องกับขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) มากกว่าการเปลี่ยนแปลงในสิ่งเล็ก ๆ น้อย ๆ ซึ่งมีผลกระทบเพียงด้านการปฏิบัติการ (Operational Effect) เท่านั้น เช่น การเปลี่ยนแปลงรูปแบบของรายงาน เป็นต้น

2) การควบคุมและรักษาความปลอดภัยโปรแกรม ระบบปฏิบัติการ และแฟ้มข้อมูล

การควบคุมในขอบเขตนี้จำเป็นต้องปฏิบัติอยู่ตลอดเวลา ลักษณะเฉพาะของการควบคุมประเภทนี้คือ มิได้มีความสัมพันธ์กับปริมาณข้อมูลที่ประมวลผล แต่มีความสัมพันธ์กับปริมาณและการใช้โปรแกรมในการประมวลผล จึงควรเลือกระดับการทดสอบให้สัมพันธ์กับปริมาณและการใช้โปรแกรมด้วย

3) โปรแกรมของระบบคอมพิวเตอร์ (System Software)

ลักษณะและขอบเขตของการทดสอบความเหมาะสมของโปรแกรมของระบบคอมพิวเตอร์

ขึ้นอยู่กับการตัดสินใจวินิจฉัยของผู้ตรวจสอบ ปัจจัยที่ควรพิจารณาคือ ระดับความเชื่อถือได้ของการควบคุมการใช้งาน (Implementation Controls) และการรักษาความปลอดภัยต่อโปรแกรมของระบบ (Security of System Software) ตลอดจนผลที่มีต่อการตรวจสอบด้านอื่นๆ

2.3.3 การตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures)

ลักษณะและขอบเขตของการทดสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) เพิ่มเติม ขึ้นอยู่กับการตัดสินใจวินิจฉัยของผู้ตรวจสอบเช่นกัน ปัจจัยที่ควรพิจารณามีดังนี้

1) ระดับความเชื่อถือได้ของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ถ้าผู้ตรวจสอบไม่อาจเชื่อถือต่อการควบคุมการใช้งาน (Implementation Controls) ผู้ตรวจสอบก็จะต้องเพิ่มระดับการทดสอบขั้นตอนการทำงานของโปรแกรม โดยการเพิ่มจำนวนโปรแกรมที่ตรวจสอบ ถ้าผู้ตรวจสอบไม่อาจให้ความเชื่อถือต่อการรักษาความปลอดภัยโปรแกรม หรือการควบคุมการปฏิบัติการคอมพิวเตอร์ ผู้ตรวจสอบก็ควรพิจารณาขยายช่วงเวลาของข้อมูลที่ผ่านโปรแกรมที่ตรวจสอบให้มากยิ่งขึ้น

2) ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ที่เลือกทดสอบควรเป็นโปรแกรมที่มีผลกระทบต่อนัยสำคัญ (Material Effect) ของรายงานแสดงฐานะและการดำเนินงานของธนาคาร

3) ในการกำหนดระดับการทดสอบ ผู้ตรวจสอบควรพิจารณาลักษณะและขนาดของรายการที่ทำการประมวลผล และความเสี่ยงที่จะเกิดข้อผิดพลาดอันมีนัยสำคัญ (Material Error) ระบบเกี่ยวกับการจ่ายเงิน บัญชีเงินสดและลูกหนี้ มักจะมีแนวโน้มที่เสี่ยงต่อการทุจริตอย่างมาก

4) ในระบบงานใดซึ่งผลลัพธ์จากการประมวลผลได้มีการสอบทานใหม่ทั้งหมดอีกครั้งหนึ่ง โอกาสที่จะเกิดข้อผิดพลาดเนื่องจากโปรแกรมย่อมน้อยกว่าระบบซึ่งผลลัพธ์จากการประมวลผลไม่อาจจะสอบทานใหม่ด้วยมือได้

2.3.4 ข้อควรพิจารณาอื่น

ข้อควรพิจารณาอื่นในการเลือกระดับการทดสอบ มีดังนี้

1) ปฏิกิริยาของผู้ตรวจสอบที่มีต่อข้อบกพร่องในการควบคุม

ผู้ตรวจสอบควรจะเลือกระดับการทดสอบได้เหมาะสมกับข้อบกพร่องของการควบคุมที่พบจากการประเมินระบบการควบคุมภายใน ตัวอย่างเช่น ในกรณีที่ขาดการควบคุมแบบกำกับ (Supervisory Controls) แต่พอจะสันนิษฐานได้ว่ามีการแบ่งแยกหน้าที่ (Segregation of Duties) อย่างเหมาะสม ผู้ตรวจสอบก็อาจเพิ่มระดับการตรวจสอบหลักฐาน (Examination of Evidence) เพื่อความมั่นใจว่าได้มีการปฏิบัติตามการควบคุมขั้นพื้นฐาน (Basic Controls) อย่างต่อเนื่องตลอดงวดการบัญชีที่ตรวจสอบ ในทางกลับกันในกรณีที่การแบ่งแยกหน้าที่ไม่เหมาะสม แต่มีการควบคุมแบบกำกับที่ดีพอ ผู้ตรวจสอบอาจเพิ่มระดับการสอบทานการปฏิบัติงาน (Reperformance) เพื่อความมั่นใจว่าได้มีการปฏิบัติตามการควบคุมขั้นพื้นฐาน (Basic Controls) โดยต่อเนื่องเช่นกัน

2) ความสำคัญของข้อผิดพลาดที่อาจเกิดขึ้น

ความล้มเหลว (Breakdown) หรือการขาดระบบควบคุมใด ๆ จะให้ผลที่แตกต่างกันแล้วแต่ลักษณะของการควบคุมนั้น ๆ ตัวอย่างเช่น การขาดการควบคุมข้อมูลถาวร (Standing Data) ย่อมจะมีความสำคัญกว่าการขาดการควบคุมข้อมูลเคลื่อนไหว (Transaction Data) ฉะนั้นจึงควรจะใช้ระดับการทดสอบที่สูงกว่า หรือหากไม่มีการควบคุมความถูกต้องสมบูรณ์ครบถ้วน (Completeness) ย่อมจะมีความสำคัญมากกว่าการขาดการควบคุมด้านความถูกต้อง (Accuracy หรือ Validity) ของข้อมูลเคลื่อนไหวแต่ละข้อมูล ทั้งนี้เพราะรายการที่ควรจะรวมอยู่ในผลลัพธ์จากการประมวลผล แต่ขาดหายไปในระหว่างการประมวลผล ยากแก่การตรวจพบในระหว่างตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) ฉะนั้นระดับการทดสอบความถูกต้องสมบูรณ์จึงควรอยู่ในระดับสูงขณะที่ทำการตรวจสอบระบบการควบคุม (Functional Test)

3) ความสลับซับซ้อนของรายการบัญชีและประสบการณ์การตรวจสอบ

ถ้าข้อมูลที่นำเข้าประมวลผลด้วยคอมพิวเตอร์มีหลายประเภท และมีความแตกต่างกันอย่างมาก หรือรายการหรือการคำนวณมีความสลับซับซ้อน ระดับการทดสอบก็ควรมีประสิทธิภาพพอที่จะครอบคลุมความแตกต่างกันในทุกแง่มุมได้ทั้งหมด ในทำนองเดียวกันถ้าจากการตรวจสอบที่ผ่านมาได้พบข้อบกพร่องจากการประมวลผลระดับของการทดสอบก็ควรจำเป็นต้องเพิ่มให้ครอบคลุมข้อบกพร่องทุกด้านที่เคยเกิดขึ้น

3. สรุป

ในระบบคอมพิวเตอร์วัตถุประสงค์ของการตรวจสอบระบบการควบคุม (Functional Tests) ยังคงเช่นเดียวกับการตรวจสอบในระบบที่มิได้ใช้คอมพิวเตอร์ คือ การหาหลักฐานว่าได้มีการปฏิบัติตามขบวนการการควบคุมภายในตามที่ระบุในแบบสอบถาม (Internal Control Questionnaire) หรือไม่ แต่ด้วยเหตุที่มีการเปลี่ยนแปลงการควบคุมในระบบคอมพิวเตอร์เทคนิคและขอบเขตของการตรวจสอบจึงแตกต่างไปจากระบบธรรมดา

ก่อนที่จะตัดสินใจตรวจสอบระบบการควบคุม (Functional Tests) ผู้ตรวจสอบพึงระลึกว่าประสิทธิภาพการตรวจสอบในบางครั้งก็อาจจะดีกว่าก็ได้ หากเลือกวิธีการตรวจสอบอย่างใดอย่างหนึ่งซึ่งเป็นลักษณะเฉพาะของระบบคอมพิวเตอร์ คือ การใช้โปรแกรมคอมพิวเตอร์เพื่อตรวจสอบข้อมูลที่ประมวลผลจำนวนมาก ซึ่งเป็นวิธีการหนึ่งที่จะช่วยเพิ่มประสิทธิภาพของการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) อีกทางหนึ่งด้วย หรืออีกทางเลือกหนึ่งคือ เพิ่มการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) หรือตรวจสอบโปรแกรมของระบบ (System Softwares) โดยไม่จำเป็นต้องประเมินหรือตัดสินใจให้ความเชื่อถือการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Controls)

การทดสอบการควบคุมทางด้านผู้ใช้ (User Controls) และการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Controls) ซึ่งกระทำด้วยมือ จะมีลักษณะเหมือนการตรวจสอบในระบบที่มิได้ใช้คอมพิวเตอร์ แต่การทดสอบความเหมาะสมของโปรแกรมของระบบ (System Software) และขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) มักจะต้องใช้เทคนิคที่แตกต่างออกไป ซึ่งได้แก่ ทั้งการสร้างข้อมูลตัวอย่างทดสอบ (Audit Test Data) การวิเคราะห์รหัสโปรแกรม (Program Code Analysis) และการใช้โปรแกรมคอมพิวเตอร์ (Computer Programs)

23

การประเมินผลกระทบของข้อบกพร่อง ในระบบการควบคุมภายใน

การประเมินผลกระทบของข้อบกพร่องในระบบการควบคุมภายใน

1. คำนำ

การตัดสินใจให้ความเชื่อถือต่อระบบการควบคุมภายในได้มากน้อยเพียงใด ผู้ตรวจสอบจะต้องค้นหาข้อบกพร่องที่อาจเกิดขึ้น แล้วพิจารณาว่าข้อบกพร่องนั้นจะกระทบกระเทือนขั้นตอนการตรวจสอบในลำดับต่อไปอย่างไรหรือไม่ ข้อบกพร่องที่เกิดขึ้นอาจมีสาเหตุมาจากการขาดการควบคุมที่สำคัญ หรือความล้มเหลวในการดำเนินการตามระบบการควบคุมที่กำหนดไว้ ความล้มเหลวของกิจกรรมการควบคุมนั้นแบ่งออกเป็น 2 ลักษณะ คือ ความล้มเหลวชั่วคราวเนื่องจากขาดช่วงการปฏิบัติ (Departure) ซึ่งความล้มเหลวนี้เป็นไปโดยเจตนา เช่น เกิดจากการลาหยุดของพนักงาน เป็นต้น ส่วนความล้มเหลวอีกลักษณะหนึ่งมีลักษณะถาวร (Breakdown) เนื่องจากเกิดความเปลี่ยนแปลงโดยคาดไม่ถึงในระบบการควบคุม

ข้อบกพร่องที่มีสาเหตุมาจากการขาดการควบคุมที่สำคัญสามารถตรวจสอบพบได้ในขณะที่ประเมินผลการควบคุมภายในโดยใช้แบบสอบถาม ส่วนความล้มเหลวของกิจกรรมการควบคุมภายในจะตรวจสอบพบในขณะที่ทำการตรวจสอบระบบการควบคุม (Functional Tests)

ในขณะที่ทำการตรวจสอบระบบการควบคุม (Functional Tests) หากพบว่าความล้มเหลวของกิจกรรมการควบคุมที่เกิดขึ้น ผู้ตรวจสอบจะต้องติดตามให้แน่ใจว่าความล้มเหลวนั้นได้รับการแก้ไข หรือได้สร้างระบบการควบคุมใหม่ขึ้นมาทดแทนหรือไม่ หากไม่พบการแก้ไขหรือมีระบบการควบคุมที่ทดแทนกันได้ ผู้ตรวจสอบก็สามารถยุติการตรวจสอบระบบการควบคุมได้ เพราะบรรลุเป้าหมายของการตรวจสอบแล้ว คือ ไม่มีระบบการควบคุมที่ดีพอ

2. การประเมินผลกระทบของข้อบกพร่อง

ผู้ตรวจสอบจะต้องประเมินข้อบกพร่องที่เกิดขึ้น ไม่ว่าข้อบกพร่องจะเกิดขึ้นโดยเจตนาหรือไม่ก็ตามว่ามีผลกระทบอย่างไรต่อรายงานแสดงฐานะการเงินและผลการดำเนินงาน โดยทั่วไปข้อบกพร่องของการควบคุมภายในจะก่อให้เกิดข้อผิดพลาด (Error) อย่างสำคัญในลักษณะต่าง ๆ ดังนี้

1) แสดงมูลค่าของสินทรัพย์หรือหนี้สินในงบดุลสูงหรือต่ำเกินไป ซึ่งมีผลต่อเนื่องถึงบัญชีกำไรและขาดทุน หรือ

2) ไม่แสดงรายการทุจริตที่เกิดขึ้นเนื่องจากความเสียหายได้ถูกตัดออกจากบัญชีกำไรและขาดทุนแล้วหรือ

3) จำแนกรายการบัญชีผิดพลาดทำให้การแสดงรายการในงบดุลและบัญชีกำไรและขาดทุนไม่เหมาะสม

ผู้ตรวจสอบจะต้องทำการประเมินหลังจากที่อาศัยและพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องแล้วว่าข้อบกพร่องที่เกิดขึ้นจะก่อให้เกิดข้อผิดพลาดอันมีนัยสำคัญต่อรายการแสดงฐานะการเงินและผลการดำเนินงานหรือไม่ ถ้าผู้ตรวจสอบมีความเห็นว่าข้อผิดพลาดอันมีนัยสำคัญจะไม่เกิดขึ้นก็ไม่จำเป็นต้องเปลี่ยนแปลงวิธีการตรวจสอบ เพราะผู้ตรวจสอบไม่จำต้องให้ความสนใจต่อข้อผิดพลาดที่ไม่มีนัยสำคัญ แต่หากประเมินแล้วว่าข้อผิดพลาดอันมีนัยสำคัญจะเกิดขึ้น ผู้ตรวจสอบจะต้องทราบขอบเขตของข้อผิดพลาดนั้น และเปลี่ยนแปลงหรือเพิ่มวิธีการตรวจสอบเพื่อให้ผลการตรวจสอบเป็นที่พอใจมากที่สุด

3. หลักเกณฑ์ในการพิจารณาข้อผิดพลาดอันมีนัยสำคัญ

หลักเกณฑ์ทั่วไปในการพิจารณาข้อผิดพลาดอันมีนัยสำคัญ มีดังนี้

1) สินทรัพย์หรือหนี้สินรายการที่มีข้อผิดพลาดเกิดขึ้นนั้นมีนัยสำคัญหรือไม่ต่องบการเงิน

2) ข้อผิดพลาดนั้นได้กระทบกระเทือนการควบคุมด้านอื่นที่เกี่ยวข้อง จนทำให้เกิดข้อผิดพลาดที่มีนัยสำคัญหรือไม่

3) ข้อบกพร่องของการควบคุมข้อมูลถาวร (Standing Data) จะทำให้เกิดผลกระทบที่สำคัญกว่าข้อบกพร่องของการควบคุมข้อมูลเคลื่อนไหว (Transaction Data)

4) ข้อบกพร่องในการควบคุมความครบถ้วนสมบูรณ์ (Completeness) จะเกิดผลกระทบที่รุนแรงมากกว่าข้อบกพร่องในการควบคุมความถูกต้อง (Accuracy or Validation) ของแต่ละรายการ (Individual Transaction)

5) ข้อบกพร่องของขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) มีความสำคัญกว่าข้อบกพร่องในการควบคุมทางด้านผู้ใช้ (User Controls) โดยเฉพาะอย่างยิ่งในกรณีที่มีปริมาณข้อมูลจำนวนมากผ่านเข้าไปในขั้นตอนการทำงานของโปรแกรม และ (หรือ) ผลลัพธ์จากขั้นตอนการทำงานของโปรแกรมมิได้รับการตรวจสอบ หรือพินิจพิจารณาโดยบุคคล (Manual Scrutiny) อีกครั้งหนึ่ง

6) ข้อบกพร่องของการควบคุมภายใน ซึ่งเป็นความล้มเหลวของระบบการควบคุมโดยมิได้คาดฝัน (Breakdown) ได้รับการแก้ไขโดยทันกาลก่อนสิ้นสุดปีบัญชีหรือไม่ อย่างไรก็ตามแม้ว่าข้อบกพร่องนั้นจะได้รับการแก้ไขแล้วก็ตาม ผู้ตรวจสอบยังจำเป็นต้องขยายการตรวจสอบเพื่อความมั่นใจว่า การทุจริตหรือความเสียหายที่สำคัญมิได้เกิดขึ้นในระหว่างปีบัญชีที่เกี่ยวข้อง

ในขอบเขตใดที่ผู้ตรวจสอบประเมินแล้วว่า การควบคุมการพัฒนาและรักษาความปลอดภัยโปรแกรม และการควบคุมการปฏิบัติการคอมพิวเตอร์ยังไม่เพียงพอ ผู้ตรวจสอบจะต้องตรวจทานขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ในส่วนที่เกี่ยวข้องกับความเสี่ยงภัย แล้วประเมินว่าข้อผิดพลาดที่มีนัยสำคัญจะเกิดขึ้นหรือไม่

ในกรณีที่ผลการทดสอบของผู้ตรวจสอบ (โดยใช้การทดสอบด้วยมือ การสร้างข้อมูลทดสอบ การวิเคราะห์รหัสโปรแกรม หรือการใช้โปรแกรมคอมพิวเตอร์) ปรากฏว่าการปฏิบัติตามขั้นตอนการทำงานของโปรแกรมยังไม่เหมาะสม ผู้ตรวจสอบจะต้องสอบหาสาเหตุที่เกิดขึ้น ซึ่งสาเหตุอาจเนื่องมาจากกำหนดขั้นตอนการทำงานที่ไม่เหมาะสมไว้ในโปรแกรม (อันเป็นข้อบกพร่องของการควบคุมการพัฒนาและรักษาความปลอดภัยโปรแกรม) หรือการใช้โปรแกรมไม่เหมาะสม (ซึ่งเป็นข้อบกพร่องของการควบคุมการปฏิบัติการคอมพิวเตอร์) เมื่อผู้ตรวจสอบได้ทราบสาเหตุแล้วก็จะต้องประเมินผลกระทบอันเนื่องมาจากขั้นตอนการทำงานของโปรแกรมที่ผิดพลาดนั้น และขั้นตอนการทำงานของโปรแกรมอื่น ๆ ที่เกี่ยวข้อง นั่นคือ ผู้ตรวจสอบจะต้องตรวจสอบลึกลงไปในขั้นตอนการทำงานของโปรแกรม และการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ให้มากขึ้น เพื่อประมวลว่าข้อบกพร่องของการควบคุมความสมบูรณ์ถูกต้องดังกล่าวได้เกิดขึ้นหรือไม่ และเกี่ยวข้องกับข้อบกพร่องของขั้นตอนการทำงานของโปรแกรมอย่างไร และถ้าพบว่ามีข้อบกพร่องเกิดขึ้น ผู้ตรวจสอบก็จะต้องประเมินด้วยว่าข้อผิดพลาดที่มีนัยสำคัญจะเกิดขึ้นเนื่องจากข้อบกพร่องนั้นหรือไม่เช่นกัน

ในกรณีที่ผู้ตรวจสอบพบว่าการควบคุมข้อมูลถาวร (Standing Data) หรือการควบคุมความปลอดภัยของแฟ้มข้อมูลยังไม่เพียงพอ ผู้ตรวจสอบก็จะต้องตรวจสอบแฟ้มข้อมูลที่เกิดความเสี่ยงภัยนั้น แล้วประเมินว่าข้อบกพร่องของการควบคุมดังกล่าวจะทำให้เกิดข้อผิดพลาดที่มีนัยสำคัญหรือไม่ อย่างไร

ในการประเมินผลกระทบของความล้มเหลวอันคาดไม่ถึงของการควบคุมในระบบคอมพิวเตอร์ (Break-down) ผู้ตรวจสอบพึงระลึกว่าข้อบกพร่องของขั้นตอนการทำงานของโปรแกรมมิได้เกิดขึ้นอย่างลอย ๆ แต่แสดงให้เห็นข้อบกพร่องของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ด้วย

4. ผลกระทบต่อวิธีการตรวจสอบ

โดยทั่วไปผลกระทบที่มีต่อวิธีการตรวจสอบอันเนื่องมาจากข้อบกพร่องที่ทำให้เกิดข้อผิดพลาดอันมีนัยสำคัญของการควบคุมภายใน จะขึ้นอยู่กับลักษณะและนัยสำคัญของสินทรัพย์หรือหนี้สินที่มีข้อผิดพลาดนั้น ตลอดจนโอกาสที่จะเกิดข้อผิดพลาดอันมีนัยสำคัญขึ้น

เมื่อผู้ตรวจสอบพบว่าข้อผิดพลาดอันมีนัยสำคัญมีโอกาสที่จะเกิดขึ้นได้ ผู้ตรวจสอบจำเป็นต้องสอบทานการปฏิบัติงานทั้งหมด (Overall Review) เพื่อค้นหาข้อผิดพลาดอันมีนัยสำคัญ เช่น ตรวจสอบการรวบยอดของข้อมูลที่ประมวลผลเดือนต่อเดือน แล้วเปรียบเทียบกับงบประมาณหรืองวดการบัญชีที่ผ่านมาหรือกับดัชนีการปฏิบัติงาน (Performance Indicators) เป็นต้น แต่ถ้าข้อมูลที่ต้องการตรวจสอบดังกล่าวจัดเก็บไว้ในแฟ้มข้อมูลคอมพิวเตอร์ ผู้ตรวจสอบก็อาจใช้โปรแกรมการตรวจสอบ (Computer Audit Programs) เข้าช่วยในการค้นหาข้อผิดพลาดก็ได้ การใช้โปรแกรมตรวจสอบกระทำได้ทั้งการตรวจสอบการควบคุมทางด้านผู้ใช้ (User Controls) และการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures)

ผลจากการสอบทานการปฏิบัติงาน (Overall Review) หากปรากฏว่าข้อผิดพลาดอันมีนัยสำคัญอาจเกิดขึ้นในยอดคงเหลือของบัญชีหนึ่งบัญชีใด ผู้ตรวจสอบจะต้องตรวจสอบรายการทุกรายการของบัญชีนั้น หรือ

ส่วนใดส่วนหนึ่งของบัญชีอันเป็นที่ต้องสงสัย และหากพบว่าการทุจริตที่เป็นนัยสำคัญได้เกิดขึ้นแล้ว ผู้ตรวจสอบจำเป็นต้องตรวจสอบรายการที่เกิดขึ้นในระยะเวลาบัญชีที่ตรวจสอบให้มากยิ่งขึ้น นั่นคือ ต้องขยายการตรวจสอบความถูกต้องของรายการทางการเงินเพิ่มขึ้น

5. การบันทึกข้อบกพร่องในการควบคุม

ผู้ตรวจสอบจะต้องบันทึกข้อบกพร่องในการควบคุมภายใน โดยใช้แบบฟอร์ม "บันทึกข้อบกพร่องในการควบคุมภายใน" (Record of Control Weaknesses "RCW") ตามตัวอย่างในแผนภาพที่ 23.1 โดยมีลำดับขั้นและวิธีการบันทึกดังนี้



แผนภาพที่ 23.1 ตัวอย่างบันทึกข้อบกพร่องของระบบการควบคุมภายใน

แผ่นที่.....
จากจำนวน.....

ธนาคาร.....
บันทึกข้อบกพร่องของระบบการควบคุมภายใน
การตรวจสอบเพียงวันที่.....

อ้างถึงแบบสอบถามการควบคุมภายใน
เรื่อง.....

ลักษณะของข้อบกพร่องและผลกระทบที่อาจเกิดขึ้นต่องบการเงิน	คำชี้แจงของเจ้าหน้าที่ธนาคารที่เกี่ยวข้อง	โอกาสที่จะเกิดข้อผิดพลาดอันมีนัยสำคัญ		ผลกระทบต่อลักษณะ ขอบเขต และระยะเวลาการตรวจสอบ		การแก้ไขข้อบกพร่อง	
		มี/ไม่มี	ความเห็น	การแก้ไขวิธีการตรวจสอบที่จำเป็น	Ref. แผนการตรวจสอบ	วันที่	วิธีการ
(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
ไม่มีการควบคุมอัตราค่าเสื่อมราคาที่ใช้ในการคำนวณค่าเสื่อมราคาประจำเดือน ทำให้ค่าเสื่อมราคาที่ปรากฏในบัญชีกำไรขาดทุนอาจผิดพลาดและการแสดงทรัพย์สินในงบดุลพลอยผิดพลาดไปด้วย	(ระบุชื่อและตำแหน่ง) นาย.....ยอมรับว่าการควบคุมบกพร่อง แต่จะตรวจพบข้อผิดพลาดว่ามีนัยสำคัญหรือไม่ เมื่อสอบทานรายงานบัญชีเพื่อการจัดการ	มี	ไม่มีระเบียบการปฏิบัติที่แน่นอนในการป้องกันข้อผิดพลาดและค่าเสื่อมราคาเป็นรายการที่มีนัยสำคัญในบัญชีกำไรขาดทุน	ใช้โปรแกรมการตรวจสอบคำนวณค่าเสื่อมราคาและค่าเสื่อมราคาสะสมสินทรัพย์ทุกรายการ	ม/34		

1) ระบุข้อบกพร่องที่เกิดขึ้นและผลกระทบที่อาจมีต่องบการเงิน (แบบฟอร์มช่องที่ 1 และ 2)

2) หากไม่พบว่ามีการควบคุมอื่นที่ชดเชยกันได้ ให้นำข้อบกพร่องดังกล่าวซักถามความเห็นจากเจ้าหน้าที่ที่เกี่ยวข้องของธนาคาร เพื่อความมั่นใจและให้ได้ข้อเท็จจริงที่เกิดขึ้น (แบบฟอร์มช่องที่ 3)

3) ประเมินว่าโอกาสที่ข้อผิดพลาดอันมีนัยสำคัญจะเกิดขึ้นหรือไม่ พร้อมทั้งให้เหตุผลในการประเมิน (แบบฟอร์มช่องที่ 4 และ 5)

4) บันทึกผลกระทบที่มีต่อวิธีการตรวจสอบของผู้ตรวจสอบ (แบบฟอร์มช่องที่ 6 และ 7)

5) บันทึกการแก้ไขข้อบกพร่องของธนาคาร (แบบฟอร์มช่องที่ 8 และ 9)

6. ข้อบกพร่องที่พบบ่อยครั้งในระบบคอมพิวเตอร์

ข้อบกพร่องในระบบคอมพิวเตอร์มักเกิดขึ้น เนื่องจากขาดการวางแผนการควบคุมที่ดีพอ นับตั้งแต่ระยะเริ่มต้นของการพัฒนาระบบงาน โดยเฉพาะอย่างยิ่งการควบคุมด้วยบุคคล (Manual Controls) มักจะถูกละเลยหรือมิได้เตรียมการไว้ล่วงหน้าจนกว่าจะได้ใช้ระบบงานจริง

ข้อบกพร่องที่พบบ่อยครั้งมีดังนี้

1) ขาดการควบคุมการบำรุงรักษา (Maintenance) ข้อมูลถาวร (Standing Data)

2) ขาดการควบคุมข้อมูลอ้างอิง (Reference Data) ที่จำเป็น

3) วิธีปฏิบัติเกี่ยวกับการกำกับและอนุมัติ (Authorization Procedures) ไม่มีประสิทธิภาพหรือไม่ได้รับการปฏิบัติตาม โดยเฉพาะอย่างยิ่งในการแก้ไขปรับปรุงข้อมูลนำเข้าที่ผิดพลาด หรือที่ปฏิเสธโดยคอมพิวเตอร์

4) ขาดการควบคุมแบบ Supervisory Controls ที่สำคัญ

5) ขาดการตรวจสอบความถูกต้องของข้อมูลที่เครื่องคอมพิวเตอร์สร้างขึ้นโดยอัตโนมัติ (Computer-generated Data) ทั้งการตรวจสอบความสมเหตุสมผล (Reasonableness Checks) และการตรวจสอบโดยบุคคล

6) การกำหนดความสมเหตุสมผลและการตรวจสอบซึ่งกันและกัน (Dependency Checks) ภายในโปรแกรมไม่สอดคล้องกับความเป็นจริงหรือไม่ถูกหลักการ ทำให้การปฏิเสธข้อมูลและ (หรือ) การรายงานข้อมูลผิดพลาดมากหรือน้อยเกินไป

7) การจัดแบ่งอำนาจหน้าที่การปฏิบัติงานในศูนย์คอมพิวเตอร์สับสน

8) ขาดการบันทึกที่เหมาะสม (Readily Digestible Reports) ของการใช้เครื่องคอมพิวเตอร์

9) ไม่มีการควบคุมการปรับปรุงแก้ไข (Modifications) ห้องสมุดโปรแกรม (Program Libraries)

10) ไม่มีการควบคุมและรักษาความปลอดภัยแฟ้มข้อมูล

11) ไม่มีการควบคุมเพื่อความมั่นใจว่าข้อปฏิบัติที่กำหนดเกี่ยวกับการปฏิบัติการคอมพิวเตอร์ และการใช้แฟ้มข้อมูลได้รับการปฏิบัติตามโดยไม่บกพร่อง โดยเฉพาะการปฏิบัติงานในตอนเย็นหรือในวันหยุด

12) ขาดการเอาใจใส่ต่อรายงานข้อผิดพลาด (Exceptional Reports) โดยทันทีทันใด

13) สะสมความไม่เอาใจใส่หรือไม่สอบสวนข้อมูลที่เครื่องคอมพิวเตอร์ไม่ยอมรับ

14) สะสมรายการที่น่าสงสัยหรือรายการตกค้าง (Suspense Items) ไว้ในแฟ้มข้อมูล

15) การติดตามรายการที่เป็นจุดเด่นอย่างสำคัญและรายการที่เกินกำหนดไม่ทันกาล

16) การกระทบยอดเนื่องจากการประมวลผลล่าช้าไม่ทันกาล

17) รอบระยะเวลาการตรวจสอบข้อมูลถาวร (Standing Data) มักจะถูกจัดให้อยู่ลำดับความสำคัญต่ำ

18) ข้อกำหนดเกี่ยวกับการปฏิบัติการคอมพิวเตอร์มักไม่เป็นผล เช่น ผู้เขียนโปรแกรมทำการทดสอบโปรแกรมกับเครื่องคอมพิวเตอร์โดยมิได้รับอนุญาต

19) ขาดการตรวจสอบและรับรองบันทึกการใช้เครื่องคอมพิวเตอร์โดยสม่ำเสมอ

20) ข้อกำหนดเกี่ยวกับการเข้าถึง (access to) แฟ้มข้อมูลมักไม่เป็นผล เช่น พนักงานปฏิบัติการคอมพิวเตอร์ (Operators) เข้าถึงห้องสมุดแฟ้มข้อมูล (File Libraries) ได้โดยไม่จำเป็นต้องได้รับอนุมัติอย่างถูกต้องเสียก่อน

21) การแก้ไขห้องสมุดโปรแกรมปฏิบัติการ (Operational Program Libraries) กระทำโดยปราศจากการควบคุมตามปกติหรือไม่มีการอนุมัติ

ข้อบกพร่องที่กล่าวจากข้อ 12 ถึงข้อ 21 มักจะพบในระหว่างที่ทำการตรวจสอบระบบการควบคุม (Functional Tests)

7. การทุจริตในระบบคอมพิวเตอร์

การทุจริตในระบบคอมพิวเตอร์ (Computer Fraud) แบ่งโดยแนวกว้างออกเป็น 3 ขอบเขต ดังนี้

7.1 การเบียดบังสินทรัพย์ (Defalcation)

หมายถึง การใช้วิธีการประมวลผลด้วยคอมพิวเตอร์ (Computer Processing) เพื่อช่วยให้ได้รับสินทรัพย์ของธนาคารไปโดยมิชอบ การปฏิบัติดังกล่าวอาจทำได้ 2 วิธี คือ

7.1.1 การทุจริตโดยขั้นตอนของโปรแกรม (Fraudulent Program Steps)

การทุจริตโดยอาศัยขั้นตอนของโปรแกรมเป็นกรณีที่เกิดขึ้นได้น้อย ทั้งนี้เพราะมีระบบงานเพียงไม่กี่ระบบที่ผู้เขียนโปรแกรมจะสามารถแทรกขั้นตอนการทุจริตไว้ในโปรแกรมเพื่อรับประโยชน์ส่วนตัวโดยทันทีได้

เช่น ระบบการจ่ายเงินเดือน เป็นต้น นอกจากนั้นยังอาจเป็นเพราะผู้เขียนโปรแกรมไม่สามารถรู้ระบบงานที่เป็นจริงได้อย่างลึกซึ้งทั้งหมดก็ได้

การป้องกันการทุจริตโดยขั้นตอนของโปรแกรม อาจทำได้โดยการแบ่งแยกหน้าที่กันอย่างเหมาะสม โดยที่ผู้เขียนโปรแกรมไม่ทราบวิธีการควบคุมโดยบุคคลในส่วนต่าง ๆ ของระบบงาน รวมทั้งการควบคุมทางด้านผู้ใช้ นอกจากนั้นควรทดสอบระบบงานใหม่ การเปลี่ยนแปลงโปรแกรม และการควบคุมการเข้าถึงโปรแกรมอย่างเข้มงวด หรือใช้วิธีป้องกันโดยใช้เทคนิคการสร้างโปรแกรมเป็นชิ้นส่วน (Moduler Programming Techniques) ซึ่งจะไม่มีผู้เขียนโปรแกรมคนใดคนหนึ่งทราบระบบคอมพิวเตอร์ทั้งระบบได้

7.1.2 การประมวลผลข้อมูลโดยมิชอบ (Processing Unauthorized Data)

เป็นวิธีการทุจริตที่ง่ายที่สุดในระบบคอมพิวเตอร์ ซึ่งอาจทำได้โดยป้อนข้อมูลนำเข้าโดยมิได้รับอนุมัติอย่างถูกต้อง ยักย้ายถ่ายเทแฟ้มข้อมูล ใช้เครื่องพิมพ์ผลลัพธ์โดยเจตนาให้ผิดพลาด และปิดบังอำพรางผลลัพธ์ วิธีป้องกันที่ดีที่สุดคือ กำหนดหรือจัดแบ่งระดับ และระยะเวลาการอนุมัติให้ปรับปรุงและแก้ไขข้อมูลถาวร (Standing Data) ทุกประเภทอย่างเหมาะสม ควบคุมการบำรุงรักษาข้อมูลในแฟ้มข้อมูลอย่างสม่ำเสมอ ควบคุมการเข้าถึงแฟ้มข้อมูลในระบบ On-line อย่างเข้มงวด และจัดแบ่งหน้าที่การปฏิบัติงานให้เหมาะสม นอกจากนั้นเพื่อการป้องกันที่ดียิ่งขึ้น การแบ่งแยกหน้าที่ความรับผิดชอบในการอนุมัติข้อมูลที่เป็นข้อมูลเคลื่อนไหว (Transaction Data) ออกจากข้อมูลถาวร (Standing Data)

7.2 การเสนอรายงานเท็จ (Misrepresentation)

หมายถึง การใช้วิธีการประมวลผลด้วยคอมพิวเตอร์เพื่อตบแต่ง หรือสร้างข้อมูลทางการเงินจากรายการที่มิได้รับอนุมัติอย่างถูกต้อง การปฏิบัติเช่นนี้ได้ต้องอาศัยการสมรู้ร่วมคิดอย่างสำคัญ แต่ผู้ตรวจสอบก็สามารถตรวจสอบพบได้โดยอาศัยวิธีการตรวจสอบต่าง ๆดังที่ได้กล่าวกันมาแล้ว อย่างไรก็ตามการทุจริตด้วยวิธีนี้ก็สามารถกระทำได้ง่าย ทั้งนี้ก็เพราะธรรมชาติของการประมวลผลด้วยคอมพิวเตอร์นั้น มีสมรรถภาพที่จะประมวลผลข้อมูลจำนวนมหาศาลได้ โดยไม่จำเป็นต้องใช้พนักงานจำนวนมากแต่อย่างใด

7.3 ปฏิบัติการด้านกายภาพ (Physical Action)

หมายถึง การทุจริตโดยทำลายระบบการรักษาความปลอดภัย หรือทำลายข้อมูลและโปรแกรม หรือขโมยอุปกรณ์ หรือทรัพย์สินในระบบคอมพิวเตอร์ เป็นต้น

8. สรุป

เป็นบทบาทและหน้าที่ที่สำคัญในการตรวจสอบ ซึ่งผู้ตรวจสอบจะต้องประเมินข้อบกพร่องต่าง ๆ ที่เกิดขึ้นในระบบการควบคุมภายในว่า ข้อบกพร่องนั้นจะก่อให้เกิดข้อผิดพลาดอันมีนัยสำคัญต่อรายงานแสดงฐานะการเงินและผลการดำเนินงานหรือไม่ และหากข้อผิดพลาดอันมีนัยสำคัญมีโอกาสที่จะเกิดขึ้นได้ ผู้ตรวจสอบจะต้องทราบขอบเขตของข้อผิดพลาดอันนั้น

24

การตรวจสอบความถูกต้องของรายการทางการเงิน

การตรวจสอบความถูกต้องของรายการทางการเงิน

1. การตรวจสอบทั่วไป

1.1 วัตถุประสงค์และขอบเขตของการตรวจสอบ

การตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures หรือ Verification Procedures หรือ Substantive Tests) คือ การตรวจสอบความถูกต้องของยอดคงเหลือตามบัญชี รวมทั้งข้อมูลอื่นในงบการเงิน และข้อสังเกตที่พบเป็นการตรวจสอบขั้นสุดท้ายก่อนแสดงความเห็นในการตรวจสอบ นอกจากนี้การตรวจสอบความถูกต้องของรายการทางการเงินยังช่วยให้การตรวจสอบระบบควบคุมภายใน (Functional Test) มีความสมบูรณ์ขึ้นด้วย เพราะสามารถใช้ผลการตรวจสอบเป็นหลักฐานยืนยันว่ามีการปฏิบัติตามระเบียบควบคุมภายในหรือไม่ได้เป็นอย่างดี

1.2 ความสำคัญของการควบคุมภายในต่อการตรวจสอบความถูกต้องของรายการทางการเงิน

ปัจจัยที่สำคัญที่สุดในการกำหนดวิธีการ ช่วงเวลาข้อมูล และขอบเขตของการตรวจสอบความถูกต้องของรายการทางการเงินคือ นัยสำคัญ (Materiality) ของยอดคงเหลือตามบัญชี และความเชื่อถือต่อการควบคุมภายใน หากการควบคุมภายในเป็นที่น่าพอใจจะช่วยให้สามารถกำหนดขอบเขตและดำเนินการตรวจสอบความถูกต้องของรายการทางการเงินได้อย่างเหมาะสมได้ตั้งแต่ระยะแรกของการตรวจสอบแต่ในทางตรงข้ามหากพบว่าการควบคุมภายในไม่เป็นที่น่าพอใจ จะต้องขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินมากขึ้นและปริมาณงานตรวจสอบส่วนใหญ่จะตกไปอยู่ในช่วงท้ายของการตรวจสอบ

1.3 ความเชื่อถือต่อการควบคุมภายใน

ในการกำหนดวิธีการช่วงเวลาข้อมูล และขอบเขตของการตรวจสอบความถูกต้องของรายการทางการเงินจะต้องพิจารณาถึงความเชื่อถือต่อการควบคุมภายในเสียก่อนโดยอาศัยข้อสรุปที่ได้จากการประเมินผลการควบคุมภายใน การตรวจสอบระบบควบคุมภายใน และผลกระทบของข้อบกพร่องในการควบคุมภายใน

ในกรณีที่ไม่ได้ทำการตรวจสอบระบบควบคุมภายใน อาจใช้วิธีสอบถามระบบควบคุมภายในที่ใช้อยู่ในขณะนั้นมาพิจารณาวิธีการและขอบเขตในการตรวจสอบความถูกต้องของรายการทางการเงิน แล้วนำผลการตรวจสอบยันกับการปฏิบัติงานภายใต้ระบบการควบคุมนั้น

นอกจากนี้ในการเข้าตรวจสอบแต่ละครั้งควรตรวจสอบงานประจำที่ใช้ในการควบคุมภายในด้วย เช่น การกระทบยอดบัญชีต่าง ๆ เป็นต้น

1.4 การขยายขอบเขตการตรวจสอบ

เมื่อพบว่าการควบคุมภายในของธนาคารไม่เป็นที่น่าพอใจเชื่อถือไม่ได้ จะต้องขยายขอบเขตของการตรวจสอบความถูกต้องของรายการทางการเงินให้มากขึ้น ซึ่งจะกล่าวโดยละเอียดในภายหลัง

1.5 เอกสารประกอบการตรวจสอบความถูกต้องของรายการทางการเงิน

ในการปฏิบัติงานตรวจสอบควรมีการจดบันทึกการทำงานไว้ด้วย เพื่อให้แน่ใจว่าได้มีการปฏิบัติงานครบถ้วนตามแผนที่วางไว้ และเพื่อให้ผู้ตรวจทานงานตรวจสอบสามารถตัดสินข้อสรุปที่ได้จากการตรวจสอบความถูกต้องของรายการทางการเงินได้ใกล้เคียงกับข้อเท็จจริง สิ่งที่ควรกำหนดให้ปฏิบัติในแผนการตรวจสอบมีดังนี้

1) รายละเอียดในการตรวจสอบ
2) ขั้นตอนในการตรวจสอบ
3) หลักฐานที่ตรวจพบโดยละเอียด
4) รายงานข้อบกพร่องในการปฏิบัติงานของธนาคารและการแก้ไขโดยละเอียด
5) เครื่องหมายแสดงว่างานแล้วเสร็จ (โดยปกติเป็นลายมือชื่อผู้ตรวจสอบ) และวันที่งานแล้วเสร็จ

2. การตรวจสอบในระบบคอมพิวเตอร์

วัตถุประสงค์ในการตรวจสอบและความสำคัญของระบบการควบคุมภายในที่มีต่อการตรวจสอบความถูกต้องของรายการทางการเงินในระบบที่ใช้คอมพิวเตอร์ยังคงเหมือนระบบเดิมที่ไม่ใช้คอมพิวเตอร์ แต่วิธีการตรวจสอบอาจแตกต่างกันบ้างเล็กน้อย ในระบบคอมพิวเตอร์จำเป็นต้องใช้โปรแกรมคอมพิวเตอร์อ่านข้อมูลที่เก็บไว้ในแฟ้มข้อมูลและการควบคุมในระบบคอมพิวเตอร์จะแตกต่างไปจากระบบเดิมด้วย

3. วิธีการตรวจสอบความถูกต้องของรายการทางการเงิน

3.1 ประเภทของการตรวจสอบความถูกต้องของรายการทางการเงิน

การตรวจสอบความถูกต้องของรายการทางการเงินมี 2 ประเภท

- การทดสอบความถูกต้องของรายการทางการเงิน (Validation Tests)
- วิธีการตรวจสอบอื่น ๆ

การทดสอบความถูกต้องของรายการทางการเงินคือการทดสอบความถูกต้องของรายการประกอบยอดคงเหลือตามบัญชีหรือข้อมูลทางการเงินอื่น ๆ ที่ต้องการทราบความเป็นจริงโดยตรง ส่วนวิธีการตรวจสอบอื่น ๆ เป็นการทดสอบเพิ่มเติมในด้านทั่ว ๆ ไป เช่นการวิเคราะห์เปรียบเทียบ และการสอบทานเพื่อเป็นหลักฐานช่วยแสดงความถูกต้องและสมบูรณ์ของข้อมูลตามบัญชี รวมทั้งข้อสังเกตอื่น ๆ

3.1.1 การทดสอบความถูกต้องของรายการทางการเงิน

วิธีการทดสอบความถูกต้องของรายการทางการเงินจะเปลี่ยนไปตามลักษณะของบัญชีที่ตรวจสอบ ซึ่งอาจเลือกใช้วิธีการสอบยัน (Confirmation) การสำรวจหรือการตรวจนับ (Inspection) การสอบทานระบบการปฏิบัติงาน (Reperformance) และการตรวจสอบเอกสารประกอบการลงบัญชี (Vouching) แล้วแต่กรณี

1) การสอบยัน (Confirmation)

การสอบยัน คือ การสอบทานข้อเท็จจริงหรือสภาพของรายการที่ประกอบเป็นยอดคงเหลือตามบัญชีจากบุคคลที่สาม ซึ่งเป็นบุคคลที่มิได้ตกอยู่ภายใต้อิทธิพลของผู้ที่ถูกตรวจสอบ ย่อมมีน้ำหนักเพียงพอที่จะพิสูจน์ข้อเท็จจริงได้ และสามารถใช้เป็นหลักฐานในการทดสอบยอดคงเหลือตามบัญชีได้เป็นอย่างดี เช่น การยืนยันยอดลูกหนี้ เป็นต้น

2) การสำรวจหรือการตรวจนับ (Inspection)

การสำรวจหรือการตรวจนับ คือการตรวจนับและ/หรือการสำรวจทรัพย์สินตามรายการบัญชีโดยการเข้าไปสังเกตการตรวจนับของฝ่ายบริหาร และบางครั้งผู้ตรวจสอบอาจดำเนินการตรวจนับเอง เช่น การตรวจนับเงินสด เป็นต้น

3) การสอบทานระบบการปฏิบัติงาน (Reperformance)

ในบางกรณียอดคงเหลือของบัญชีบางประเภทอาจได้มาจากการคำนวณหรือคำนวณสะสมกันมา เช่น การกันสำรองหนี้สูญ และดอกเบี้ยต่าง ๆ การตรวจสอบความถูกต้องของบัญชีเหล่านี้จำเป็นต้องอาศัยวิธีการและดำเนินการคำนวณโดยละเอียดเช่นเดียวกับผู้ปฏิบัติงานเพื่อพิจารณาความถูกต้องของวิธีการคำนวณที่ใช้ รวมทั้งประเมินวิธีการปฏิบัติงานว่าเหมาะสมเพียงใดด้วยตัวอย่างเช่น การกันสำรองหนี้สูญ ผู้ตรวจสอบควรประเมินความเหมาะสมของวิธีการกันสำรองและดำเนินการคำนวณตามสูตรที่กำหนดไว้ ประกอบกับความสามารถในการเรียกเก็บหนี้ เพื่อประโยชน์ในการพิจารณาทบทวนการกันสำรองหนี้สูญต่อไป

4) การตรวจสอบเอกสารประกอบการลงบัญชี (Vouching)

การตรวจสอบเอกสารประกอบการลงบัญชีคือการตรวจสอบความถูกต้องของเอกสารที่ใช้เป็นหลักฐานในการบันทึกรายการบัญชี เพื่อให้แน่ใจว่าเอกสารเหล่านี้ได้จัดทำขึ้นถูกต้องตามระเบียบ และมีการเช็คสอบทุกขั้นตอน (โดยการทดสอบตามความเหมาะสม) นอกจากนี้ยังอาจตรวจพบสิ่งผิดปกติในเอกสารด้วย เช่น ที่อยู่ของลูกหนี้ที่น่าสงสัย เป็นต้น

5) การกระทบยอดและการวิเคราะห์บัญชี (Reconcilation and Account Analysis)

การกระทบยอดคือ การพิสูจน์หาข้อแตกต่างระหว่างตัวเลข 2 จำนวน เช่น การกระทบยอดคงเหลือของบัญชีเงินฝากที่ธนาคารอื่นตามบัญชีของธนาคารกับ statement ที่ธนาคารอื่นที่เกี่ยวข้องแจ้งให้ทราบ หรือการกระทบยอดบัญชีระหว่างกันของสำนักงานใหญ่กับสาขาเพื่อทดสอบความถูกต้องของรายการทางการเงินและนำผลการกระทบยอดไปปรับปรุงรายการตามความเหมาะสม

การตรวจสอบความถูกต้องของรายการทางการเงิน
เงินให้สินเชื่อ

ธนาคาร_____ วันที่ตรวจสอบ_____

แผนการตรวจสอบ	หมายเลข กระดาษทำการ	ข้อบกพร่อง มี/ไม่มี	ลายมือชื่อผู้ตรวจสอบ และวันที่แล้วเสร็จ

แผนภาพที่ 24.1 กระดาษทำการ การตรวจสอบความถูกต้องของรายการทางการเงิน

การวิเคราะห์บัญชี คือ การจัดประเภทและสรุปรายการบัญชีเพื่อให้เข้าใจง่าย การวิเคราะห์บัญชีมี 2 ประเภท ประเภทแรกเป็นการสรุปกิจกรรมที่เกิดขึ้นในงวดที่ตรวจสอบใช้กับบัญชีสินทรัพย์เกี่ยวกับที่ทำการและเครื่องมือเครื่องใช้สำนักงาน ซึ่งรายการที่เกิดขึ้นตั้งแต่ต้นงวดจนถึงสิ้นงวดยังคงค้างเป็นส่วนประกอบสำคัญของยอดคงเหลือตามบัญชี ส่วนประเภทหลังเป็นการวิเคราะห์องค์ประกอบที่สำคัญของยอดคงเหลือ เช่น บัญชีลูกหนี้ซึ่งมีอยู่มากรายการตลอดงวดการบัญชีที่ตรวจสอบ โดยวิเคราะห์ระยะเวลาที่ค้างชำระหรือรายละเอียดเกี่ยวกับตัวลูกหนี้การวิเคราะห์บัญชีทั้ง 2 ประเภทเป็นประโยชน์ต่อการตรวจสอบความถูกต้องมากช่วยให้เข้าใจลักษณะพื้นฐานของรายการประกอบยอดคงเหลือตามบัญชีได้เป็นอย่างดี

3.1.2 วิธีการตรวจสอบอื่น ๆ

วิธีการตรวจสอบอื่น ๆ ที่อาจนำมาใช้ในการตรวจสอบความถูกต้องของรายการทางการเงินมี 2 วิธีคือการวิเคราะห์ความผันแปร (Analysis of Fluctuations) และการวิเคราะห์ทางโน้มและอัตราส่วนทางการเงิน (Analysis of Financial Trends and Ratios)

1) การวิเคราะห์ความผันแปร (Analysis of Fluctuations)

การวิเคราะห์ความผันแปรของยอดคงเหลือตามบัญชีเป็นการเปรียบเทียบตัวเลขที่มีการเปลี่ยนแปลงไปอย่างผิดปกติ ไม่เป็นไปตามงบประมาณ หรือต่างไปจากปีก่อนอย่างคาดไม่ถึงเป็นการประเมินความสัมพันธ์ของข้อมูลทางการเงินอย่างมีเหตุผลช่วยให้รอบรู้งานที่ตรวจสอบมากขึ้น ซึ่งจะทำให้การทดสอบความถูกต้องของรายการทางการเงินสมบูรณ์ขึ้น และอาจช่วยให้พบรายการที่ผิดปกติได้ เช่น อาจช่วยให้พบค่าใช้จ่ายเกี่ยวกับการบำรุงรักษาซ่อมแซมที่สูงเกินควรซุกซ่อนอยู่ในบัญชีสินทรัพย์เกี่ยวกับที่ทำการและเครื่องมือเครื่องใช้สำนักงาน

2) การวิเคราะห์ทางโน้มและอัตราส่วนทางการเงิน (Analysis of Financial Trends and Ratios)

การวิเคราะห์ทางโน้มและอัตราส่วนทางการเงินเป็นการพิจารณาฐานะและการดำเนินงานโดยอาศัยดัชนีเป็นหลัก เช่นอัตรากำไร (Gross Profit Percentages) อัตราเงินกองทุน (Working Capital Ratios) อัตราส่วนเหล่านี้จะสัมพันธ์และสอดคล้องกันอย่างสมเหตุผลเป็นเครื่องชี้ให้เห็นสิ่งผิดปกติ ช่วยให้สามารถเปลี่ยนแปลงวิธีการ ช่วงเวลาข้อมูลและขอบเขตในการทดสอบความถูกต้องของรายการทางการเงินได้อย่างเหมาะสมโดยปกติการวิเคราะห์ทางโน้มและอัตราส่วนทางการเงินมักจะทำควบคู่กับการวิเคราะห์ความผันแปรของงบการเงินเพื่อหาความสัมพันธ์ร่วมกัน

3.2 การนำวิธีการตรวจสอบมาใช้ปฏิบัติงาน

วิธีการตรวจสอบความถูกต้องของรายการทางการเงินที่กล่าวมาข้างต้น มีความสำคัญต่อขอบเขตของการตรวจสอบอย่างยิ่ง วิธีการตรวจสอบที่เหมาะสมโดยส่วนรวม จะช่วยให้การตรวจสอบงานแต่ละชนิดละเอียดและมีประสิทธิภาพสูงการตรวจสอบตามขั้นตอนที่วางไว้แต่ละขั้นตอนจะทำให้ผู้ตรวจสอบมีความเข้าใจ และมั่นใจในการตรวจสอบมากขึ้นตามลำดับหากผลการตรวจสอบขั้นต้นอย่างกว้าง ๆ เป็นที่น่าพอใจ ก็อาจจำกัดระดับการตรวจสอบไม่ให้ลึกจนเกินไป แต่ในทางตรงกันข้ามหากการตรวจสอบในขั้นต้นยังไม่เป็นที่น่าพอใจ จะต้องขยายขอบเขตการตรวจสอบเพิ่มขึ้น

ดังนั้น จึงควรศึกษาและวิเคราะห์รายการทางการเงินก่อนลงมือทดสอบความถูกต้องของรายการทางการเงินเช่นควรวิเคราะห์อัตราส่วนต่าง ๆ ที่เกี่ยวกับการให้สินเชื่อก่อนลงมือตรวจสอบด้านสินเชื่อ เป็นต้น

4. ผลกระทบของคอมพิวเตอร์ต่อวิธีการตรวจสอบความถูกต้องของรายการทางการเงิน

ข้อแตกต่างที่สำคัญที่สุดในการตรวจสอบความถูกต้องของรายการทางการเงินในระบบคอมพิวเตอร์กับระบบเดิมที่ไม่ใช้คอมพิวเตอร์ คือ ในระบบคอมพิวเตอร์จำเป็นต้องใช้โปรแกรมคอมพิวเตอร์ช่วยอ่านข้อมูลแทนระบบเดิมที่ต้องใช้คนตรวจสอบ

4.1 การใช้โปรแกรมคอมพิวเตอร์ (The Use of Computer Programs)

เนื่องจากข้อมูลเกี่ยวกับรายการบัญชีในระบบคอมพิวเตอร์จะเก็บไว้ในแฟ้มเก็บข้อมูลขนาดใหญ่จึงจำเป็นต้องใช้โปรแกรมคอมพิวเตอร์เข้าช่วยค้นหาข้อมูลให้ ซึ่งจะได้ผลรวดเร็วและถูกต้องกว่าการตรวจสอบแบบเดิมโดยไม่ใช้คอมพิวเตอร์ เช่น ภายในเวลา 5 นาทีคอมพิวเตอร์ขนาดกลางจะอ่านข้อมูลและจัดประเภทรายการได้ประมาณ 5,000 บัญชี ซึ่งเร็วกว่าพนักงานตรวจสอบมาก ประโยชน์ประการที่สองในการใช้โปรแกรมคอมพิวเตอร์ตรวจสอบก็คือ สามารถตรวจสอบข้อมูลได้มากขึ้น แทนที่จะใช้เทคนิคในการทดสอบเข้าช่วยตามวิธีการตรวจสอบแบบเก่าซึ่งเป็นวิธีการที่แก้ข้อขัดแย้งระหว่างปริมาณงานที่ควรตรวจสอบกับปริมาณงานที่สามารถตรวจสอบได้จริง แต่ในกรณีที่ใช้โปรแกรมคอมพิวเตอร์จะสามารถอ่านข้อมูลในแฟ้มข้อมูลได้ทั้งหมดช่วยให้ทราบว่าควรทดสอบอะไรบ้าง ประโยชน์ประการที่สามคือ ใช้กระดาษทำงานน้อยลง โดยให้คอมพิวเตอร์พิมพ์เฉพาะผลการทดสอบและคัดเลือกรายการทดสอบบางรายการเท่านั้น ประโยชน์ที่สำคัญที่สุดประการสุดท้ายคือสามารถลดงานตรวจสอบแต่ละรายการลงได้มากทำให้มีเวลาตรวจสอบงานด้านอื่นที่มีปัญหาได้มากขึ้น

4.1.1 ขอบเขตการใช้โปรแกรมคอมพิวเตอร์ช่วยงานตรวจสอบ

โปรแกรมคอมพิวเตอร์สามารถช่วยงานตรวจสอบความถูกต้องของรายการทางการเงินได้ ดังนี้

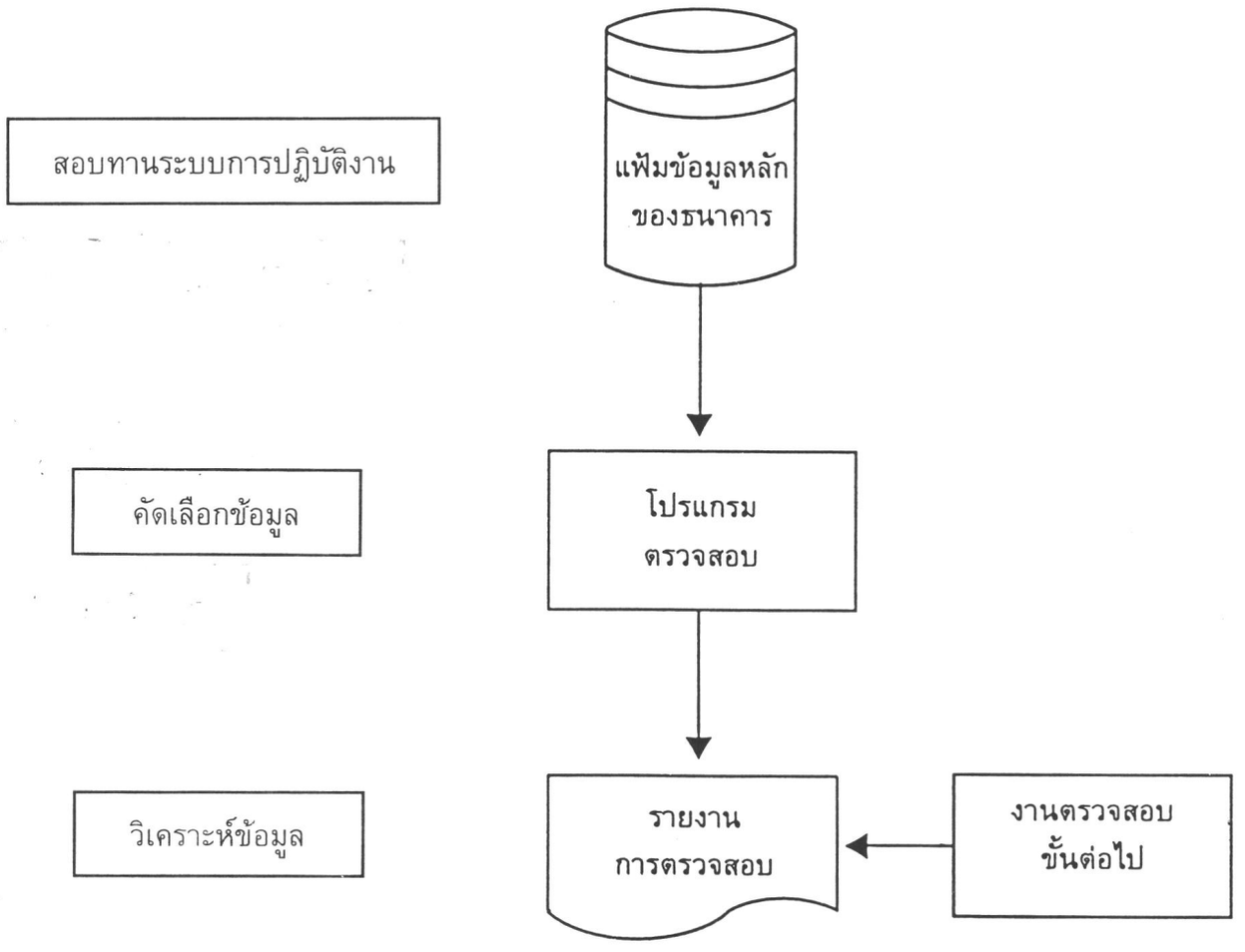
- สอบทานระบบการปฏิบัติงาน (Reperformance) เช่น สอบทานการบวกยอดคงเหลือและการคำนวณต่าง ๆ
- คัดเลือก (Selection) รายการเพื่อนำไปใช้ในการสอบยัน (Confirmation) สำรวจหรือตรวจนับทรัพย์สิน (Inspection) และอาจใช้โปรแกรมคอมพิวเตอร์เข้าช่วยสอบยันข้อมูลที่ถูกคัดเลือกด้วย
- วิเคราะห์บัญชี (Additional Account Analysis) เช่น วิเคราะห์บัญชีลูกหนี้และวงเงินให้สินเชื่อ

1) การสอบทานระบบการปฏิบัติงาน

การสอบทานระบบการปฏิบัติงานเป็นงานที่มีปริมาณงานสูงต้องสอบยอดสะสม คำนวณและวิเคราะห์ทุกรายการ การตรวจสอบในระบบเดิมจึงจำเป็นต้องใช้วิธีสุ่มตัวอย่างทดแทน แต่ในกรณีที่ใช้โปรแกรมคอมพิวเตอร์เข้าช่วยจะสามารถตรวจสอบได้โดยละเอียด ซึ่งเป็นประโยชน์ต่อการวิเคราะห์มาก

2) การคัดเลือกข้อมูล

การคัดเลือกรายการด้วยโปรแกรมคอมพิวเตอร์เพื่อนำไปใช้สอบยัน สำรวจหรือตรวจนับทรัพย์สิน ย่อมสะดวกกว่าระบบเดิมซึ่งผู้ตรวจสอบต้องลงมือคัดเลือกรายการด้วยตนเองทั้งนี้เพราะสามารถใช้โปรแกรมคอมพิวเตอร์อ่านข้อมูลทั้งหมดเพื่อทำการคัดเลือกและสุ่มตัวอย่างจึงสามารถปรับปรุงวิธีการคัดเลือกได้ตามความต้องการ ทั้งในเชิงสถิติหรือตามวิธีการของระบบงานที่วางไว้ทั้งยังสามารถจำแนกรายการที่คัดเลือกออกเป็นพวก ๆ ได้อีกด้วย เช่น คัดยอดเดบิตที่มีจำนวนเกิน 1,000 บาท ไว้พวกหนึ่ง และคัดยอดเครดิตที่เกิน 500 บาท ไว้อีกพวกหนึ่ง เป็นต้น



แผนภาพที่ 24.2 การใช้โปรแกรมคอมพิวเตอร์ตรวจสอบความถูกต้องของรายการทางการเงิน

ไว้อีกพวกหนึ่ง เป็นต้น

3) การวิเคราะห์บัญชี

ประโยชน์ที่ได้รับจากการใช้โปรแกรมคอมพิวเตอร์เข้าช่วยตรวจสอบที่สำคัญอีกประการหนึ่ง คือ ข้อมูลการวิเคราะห์บัญชีและตัวอย่างข้อมูลที่น่าสังเกต การตรวจสอบข้อมูลที่มีอยู่ทั้งหมดในแฟ้มข้อมูล และการวิเคราะห์ที่ดีจะช่วยให้ทราบขอบเขตของปัญหาที่จะตรวจสอบในขั้นต่อไป

การใช้โปรแกรมคอมพิวเตอร์เข้าช่วยตรวจสอบความถูกต้องของรายการทางการเงินจะมีประสิทธิภาพสูงกว่าการตรวจสอบแบบเก่า เพราะสามารถใช้ผลการอ่านข้อมูลในแฟ้มข้อมูลเป็นหลักในการทดสอบได้ แต่ถ้าปรากฏว่าการคัดเลือกข้อมูลและการวิเคราะห์ยังขาดนัยสำคัญ จะต้องลงมือดำเนินการตรวจสอบในขั้นต่อไปโดยอาศัยข้อมูลที่ได้จากคอมพิวเตอร์ เช่น สำรวจตรวจนับทรัพย์สินเพื่อความสมบูรณ์ในการตรวจสอบความถูกต้องของรายการทางการเงิน

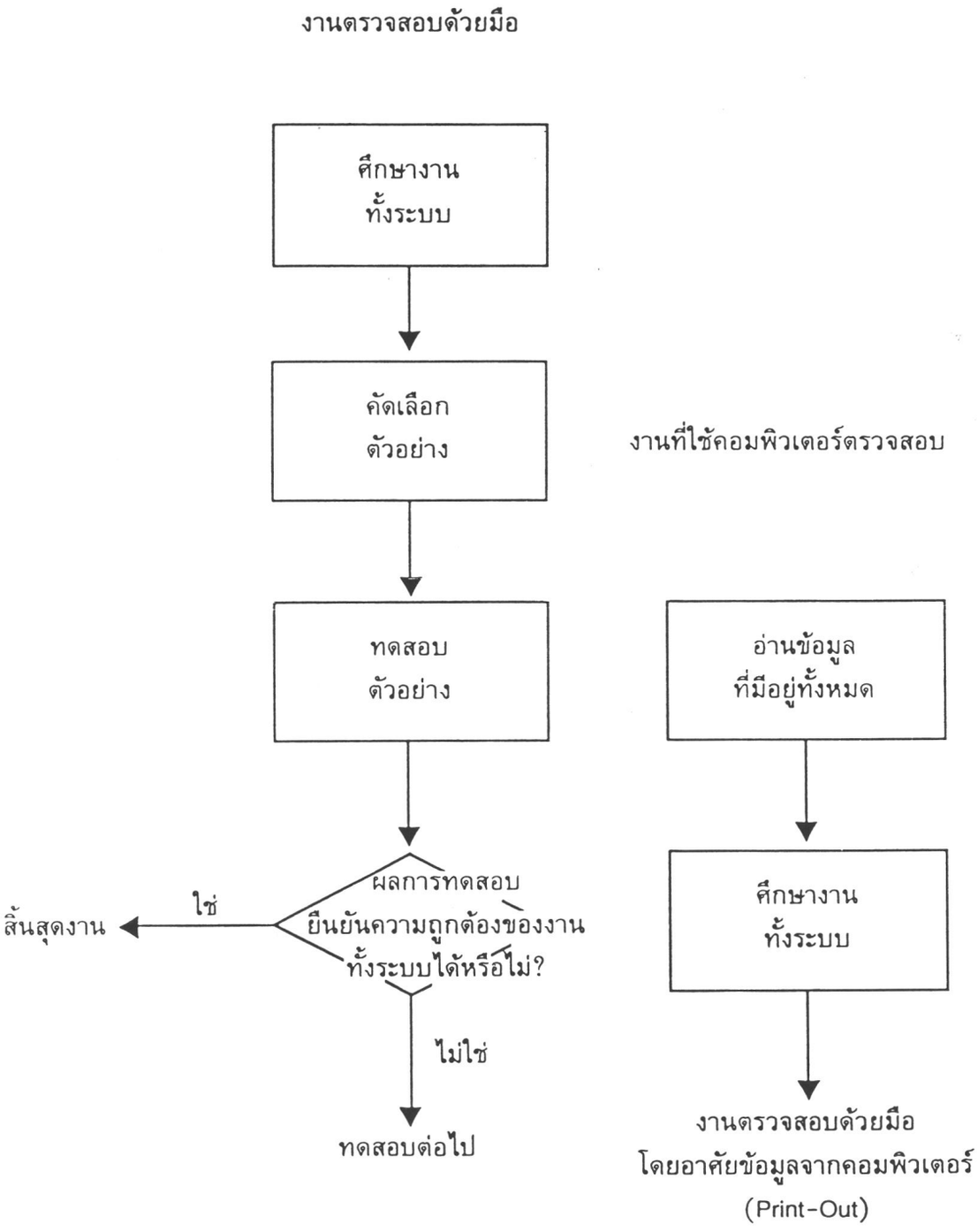
4.1.2 วิธีการใช้โปรแกรมคอมพิวเตอร์เข้าช่วยตรวจสอบ

ในการใช้โปรแกรมคอมพิวเตอร์จำเป็นต้องสร้างโปรแกรมสำหรับตรวจสอบความถูกต้องของรายการทางการเงินขึ้นมาก่อน ต่อจากนั้นจะต้องชี้แจงให้ผู้ตรวจสอบเข้าใจการทำงานของโปรแกรมเป็นการประสานงานตรวจสอบระหว่างคอมพิวเตอร์กับผู้ตรวจสอบ เพื่อหลีกเลี่ยงงานที่ไม่มีความจำเป็นหรือมองข้ามงานที่สำคัญไป

4.1.3 การตรวจสอบโดยอาศัยข้อมูลที่ได้จากคอมพิวเตอร์

ในการใช้โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบ ไม่ควรมองข้ามความสำคัญของงานตรวจสอบด้วยมือซึ่งเป็นงานที่มีคุณภาพสูงในการแปลความหมายของข้อมูลที่ได้จากคอมพิวเตอร์ ตลอดจนการพิจารณาตัดสินใจและดำเนินการตรวจสอบในขั้นต่อไปตามความจำเป็น เพื่อให้สอดคล้องกับแผนการตรวจสอบ





แผนภาพที่ 24.3 ประสิทธิภาพของการตรวจสอบความถูกต้องของรายการทางการเงิน
โดยการตรวจสอบด้วยมือและใช้โปรแกรมคอมพิวเตอร์

4.1.4 ตัวอย่างการใช้โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบ

ประโยชน์ที่จะได้รับจากการใช้คอมพิวเตอร์ ขึ้นอยู่กับวัตถุประสงค์ในการตรวจสอบข้อมูลที่เก็บไว้ในแฟ้มข้อมูลที่ตรวจสอบ และความสามารถในการเขียนโปรแกรมให้ทำงานได้ตามความต้องการ งานที่ต้องใช้คอมพิวเตอร์ช่วยตรวจสอบ ได้แก่

- การบวกยอดสะสม การบวกยอดเดบิต เครดิต ตรวจสอบบัญชีที่มียอดคงเหลือเป็นศูนย์ และยอดสุทธิต่าง ๆ
- การจัดลำดับยอดคงเหลือหรือรายการบัญชี และคัดเลือกตัวอย่างเพื่อใช้ในการตรวจสอบความถูกต้องในขั้นต่อไป
- ตรวจสอบยอดย่อย ๆ ที่ประกอบยอดคงเหลือ เปรียบเทียบกับยอดที่ปรากฏตามรายงานที่ไม่ลงตัว
- เก็บรายละเอียด บวกยอด และออกรายงานสำหรับรายการที่เกิดขึ้นภายหลังวันตัดยอดข้อมูล (cut-off date) ที่เก็บไว้ในแฟ้มข้อมูล

นอกจากนี้ยังอาจใช้โปรแกรมคอมพิวเตอร์วิเคราะห์และตรวจสอบงานที่ใช้คอมพิวเตอร์เป็นงาน ๆ ไปได้อีกด้วย ซึ่งจะมีลักษณะแตกต่างกันตามชนิดของงาน

ตัวอย่างงานที่ใช้คอมพิวเตอร์ช่วยตรวจสอบ

เงินกู้ยืม

- จับคู่ (matching) การชำระหนี้ตามงวดที่กำหนดกับงวดที่ชำระจริง หายอดหนี้คงเหลือ และเก็บรายการชำระหนี้ที่ไม่เป็นไปตามกำหนด
- เก็บรายการที่ผิดปกติ
- กระทบยอดตามบัญชีกับ statement ของธนาคารหรือสถาบันที่ให้กู้ยืมแจ้งมาให้ทราบ

สินเชื่อ

- วิเคราะห์ระยะเวลาที่ลูกหนี้ค้างชำระ
- วิเคราะห์สินเชื่อที่เกินวงเงิน
- เก็บยอดลูกหนี้ที่ไม่มีวงเงิน
- เก็บยอดลูกหนี้รายที่เป็นพนักงานหรือผู้ถือหุ้นของธนาคาร
- เก็บยอดลูกหนี้รายที่หลักประกันไม่คุ้มยอดหนี้
- เก็บรายการผิดปกติ เช่น การชำระหนี้จำนวนสูงในวันสิ้นงวดหรือสิ้นเดือน
- เก็บข้อมูลผิดปกติ เช่น ลูกหนี้รายที่อัตราดอกเบี้ยสูงหรือต่ำกว่าปกติ
- คัดเลือกลูกหนี้รายที่จะขอคำยืนยันและพิมพ์ใบขอคำยืนยันส่งให้ลูกหนี้
- วิเคราะห์และคำนวณการปฏิบัติตามกฎหมาย

อาคารที่ทำการและเครื่องมือเครื่องใช้สำนักงาน

- คำนวณค่าเสื่อมราคาเปรียบเทียบกับตัวเลขที่ธนาคารบันทึกบัญชีไว้
- เก็บรายการตัวอาคารหรือเครื่องมือเครื่องใช้สำนักงานที่คิดค่าเสื่อมราคาหมดแล้ว
- เก็บรายการที่ใช้อัตราค่าเสื่อมราคาผิดปกติ
- วิเคราะห์อายุการใช้งาน โดยพิจารณาจากรายละเอียดที่ได้จากการสำรวจตรวจนับครั้งหลังสุด
- เก็บรายการที่ไม่มีใบสำคัญแสดงสิทธิการเป็นเจ้าของ

รายได้และค่าใช้จ่าย

- เปรียบเทียบรายได้และค่าใช้จ่ายที่เกิดขึ้นจริงกับงบประมาณที่ตั้งไว้ หรือรายได้และค่าใช้จ่ายในปีก่อน ๆ

4.2 การอาศัยวิธีการควบคุมที่เชื่อถือได้เข้าช่วยงานตรวจสอบ

ในการตรวจสอบความถูกต้องของรายการทางการเงินในระบบที่ใช้คอมพิวเตอร์ควรคำนึงถึงความเชื่อถือในวิธีการควบคุมที่ใช้ด้วย ทั้งนี้เพราะในระบบคอมพิวเตอร์สามารถใช้วิธีการควบคุมที่เชื่อถือได้เข้ามาช่วยได้ดีกว่าการปฏิบัติงานแบบเก่าที่ใช้พนักงานซึ่งมักจะไม่เป็นไปตามระเบียบปฏิบัติที่วางไว้ ทำให้ผู้ตรวจสอบต้องเพิ่มประสิทธิภาพในการตรวจสอบมากขึ้น เช่น การควบคุมอำนาจอนุมัติเงินเบิกเกินบัญชีที่เกินวงเงินในระบบคอมพิวเตอร์แบบ On-line สามารถที่จะเขียนโปรแกรมควบคุมการอนุมัติการเบิกเกินวงเงินจำนวนสูงเกินอำนาจพนักงานที่ได้รับมอบหมายได้

4.3 ประโยชน์ในการปรับปรุงวิธีการวิเคราะห์บัญชี

ประโยชน์ที่ได้รับจากการใช้คอมพิวเตอร์ในการประมวลผลอีกประการหนึ่ง คือ รายงานการวิเคราะห์และรายการที่น่าสังเกตซึ่งช่วยเพิ่มประสิทธิภาพในการวิเคราะห์บัญชีมากกว่าการปฏิบัติงานในระบบเดิมที่ไม่ใช้คอมพิวเตอร์รายงานที่ได้จากคอมพิวเตอร์เหล่านี้จะช่วยให้ข้อมูลที่จะใช้ในการวิเคราะห์บัญชีมากขึ้น ไม่จำกัดเฉพาะยอดคงเหลือตามบัญชีเหมือนแบบเก่า และเข้าใจลักษณะพื้นฐานของรายการประกอบยอดคงเหลือตามบัญชีมากขึ้นด้วย

ในกรณีที่ต้องใช้รายงานการวิเคราะห์ และรายการที่น่าสังเกตที่ได้จากคอมพิวเตอร์ของธนาคารประกอบการตรวจสอบความถูกต้องของรายการทางการเงิน จะต้องแก้ไขว่าโปรแกรมต่าง ๆ ที่สร้างรายการดังกล่าวขึ้นมาสามารถทำงานได้ตรงตามวัตถุประสงค์ ข้อมูลมีความสมบูรณ์ถูกต้อง โดยทดสอบวิธีการปฏิบัติงานด้วยคอมพิวเตอร์ของธนาคารอย่างใกล้ชิด และถือเอาการทดสอบดังกล่าวเป็นส่วนหนึ่งของการตรวจสอบความถูกต้องของรายการทางการเงินด้วย หรือเพื่อความมั่นใจในระยะต้น ๆ อาจใช้วิธีการทดสอบการควบคุมภายในที่เกี่ยวข้องด้วยและทำการทดสอบการปฏิบัติงานสำคัญ ๆ อยู่เสมอ

4.4 การตรวจสอบยอดคงเหลือตามงบทดลอง

ในการตรวจสอบยอดคงเหลือตามงบทดลองในระบบที่ไม่ใช้คอมพิวเตอร์ทำบัญชี จำเป็นต้องตรวจกับบัญชีแยกประเภท แต่ในระบบที่ใช้คอมพิวเตอร์ไม่จำเป็นต้องใช้วิธีการตรวจสอบดังกล่าวทั้งนี้เพราะเป็นข้อมูลที่มาจากแฟ้มข้อมูลเดียวกัน ซึ่งมีการบวกยอดสะสมและคุมยอดให้ลงตัวอยู่แล้ว แต่ในกรณีที่โปรแกรมตรวจสอบไม่ได้เช็คสอบการรวมยอดบัญชี จะต้องทำการเช็คสอบยอดด้วยมือ

4.5 การตรวจตัดยอด (Cut-off Tests)

การประมวลผลด้วยคอมพิวเตอร์ที่อำนวยความสะดวก และสร้างประสิทธิภาพในการตรวจตัดยอด ได้แก่ การประมวลผลแบบ Batch Systems โดยอาศัยการตัดยอดรายการที่นำเข้าประมวลผลเป็นหลักเช่น ธนาคารอาจนำเงินให้กู้ยืมชนิดผ่อนชำระเข้าประมวลผลด้วยคอมพิวเตอร์ทุกวันอังคารของสัปดาห์ โดยตัดยอดเพียงวันศุกร์ของสัปดาห์ก่อน สิ่งที่จะต้องระมัดระวังในการตรวจสอบคือ วันที่ตัดยอดกับวันที่ออกรายงานคอมพิวเตอร์ซึ่งอาจแตกต่างกันและเกิดความเข้าใจผิดได้ง่าย

4.6 การกระทบยอด (Reconciliations)

การกระทบยอดในระบบประมวลผลด้วยคอมพิวเตอร์ ถือเป็นงานปกติที่จะต้องทำทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงข้อมูลที่เก็บไว้ในแฟ้มข้อมูลเพื่อคุมยอดข้อมูลให้ถูกต้องอยู่เสมอ ซึ่งผู้ตรวจสอบสามารถนำผลการกระทบยอดด้วยคอมพิวเตอร์นี้มาใช้ประโยชน์ในการตรวจสอบระบบควบคุมภายใน (Functional Tests) ได้สะดวกกว่าการบันทึกบัญชีแบบเดิมที่ไม่ได้ใช้คอมพิวเตอร์

4.7 การสร้างข้อมูลตัวอย่างทดสอบ (Use of audit test data)

ในการตรวจสอบความถูกต้องของรายการทางการเงิน ในบางครั้งอาจจำเป็นต้องสร้างข้อมูลสำหรับทดสอบความสมบูรณ์และถูกต้องของรายงานการวิเคราะห์และรายงานที่น่าสังเกตที่คอมพิวเตอร์ของธนาคารพิมพ์มาให้ด้วยตนเอง ทั้งนี้เพื่อประโยชน์ในการตรวจสอบระบบการควบคุมภายใน (Functional Tests) เพิ่มประสิทธิภาพในการตรวจสอบความถูกต้องของรายการทางการเงิน และช่วยเสริมการตรวจสอบรายงานต่าง ๆ ให้มีความละเอียดถี่ถ้วนมากขึ้น

5. เวลาที่ควรลงมือตรวจสอบความถูกต้องของรายการทางการเงิน

ระยะเวลาที่ควรลงมือตรวจสอบความถูกต้องของรายการทางการเงิน ขึ้นอยู่กับการตัดสินใจของผู้ตรวจสอบ ซึ่งอาจพิจารณาให้สอดคล้องกับการตรวจสอบระบบการควบคุมภายใน (Functional Tests) แล้วแต่กรณี ตามปกติมักจะตรวจสอบหลักการควบคุมภายในและการแบ่งแยกหน้าที่ก่อนในระยะต้น ๆ ของการตรวจสอบ เพื่อให้แน่ใจว่าข้อมูลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์น่าเชื่อถือเพียงใดเสียก่อนสำหรับการตรวจสอบความถูกต้องของยอดคงเหลือตามบัญชีอาจทำได้ตลอดเวลา สุดแล้วแต่ความเหมาะสมเพราะสามารถใช้โปรแกรมคอมพิวเตอร์เข้าช่วยตรวจสอบได้

6. ขอบเขตของการตรวจสอบความถูกต้องของรายการทางการเงิน

6.1 แนวทางทั่วไป

ผู้ตรวจสอบควรจำกัดขอบเขตการตรวจสอบให้เป็นไปตามวัตถุประสงค์ในการตรวจสอบความถูกต้องของรายการทางการเงินให้มากที่สุดเท่าที่จะทำได้ หลักเกณฑ์ในการกำหนดขอบเขตการตรวจสอบขึ้นอยู่กับน้ำหนักความสำคัญของปัจจัยดังต่อไปนี้

- ระดับความเชื่อถือต่อการควบคุมภายในของธนาคาร
- ความสำคัญของรายการบัญชีที่เกี่ยวข้องโดยส่วนรวม
- ลักษณะ จำนวน และขนาดของรายการที่ประกอบเป็นยอดคงเหลือตามบัญชี
- ความสัมพันธ์ของบัญชีที่ตรวจสอบกับบัญชีอื่น หรือข้อมูลอื่นที่จำเป็นต่อการตรวจสอบ
- รายการที่น่าสังเกตจากการตรวจสอบความถูกต้องของรายการทางการเงิน

อย่างไรก็ตามปัจจัยที่ได้รับผลกระทบโดยตรงเนื่องจากระบบคอมพิวเตอร์ มีดังนี้

6.1.1 ความเชื่อถือต่อการควบคุมภายใน

ปัจจัยสำคัญที่ใช้ในการพิจารณาขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินในส่วนที่เกี่ยวกับการควบคุมในระบบ Computer-based Accounting Systems มี 2 ประการ คือ

- ข้อมูลที่ใช้ในการวิเคราะห์รายการบัญชีที่ได้จากการตรวจสอบด้านอื่น ๆ
- ประสิทธิภาพการควบคุมภายในของระบบคอมพิวเตอร์ในการบำรุงรักษา และการเปลี่ยนแปลงหรือปรับปรุงข้อมูลที่เก็บไว้ในแฟ้มข้อมูล

ในกรณีที่ไม่ได้ใช้คอมพิวเตอร์เข้าช่วยตรวจสอบความถูกต้องของรายการทางการเงิน ก็ให้ถือปัจจัยทั้ง 2 ประการข้างต้นเป็นหลักเช่นเดียวกับกรณีที่ใช้คอมพิวเตอร์เช็คสอบการคำนวณ คัดเลือกข้อมูลเพื่อประโยชน์ในการตรวจสอบขั้นต่อไป

6.1.2 ลักษณะ จำนวน และขนาดของรายการที่ประกอบเป็นยอดคงเหลือตามบัญชี

โดยปกติผู้ตรวจสอบมักสนใจตรวจสอบยอดคงเหลือตามบัญชีที่มีจำนวนเงินสูงการพิจารณาตัดสินใจใช้โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบรายการต่าง ๆ ทั้งหมด และวิเคราะห์บัญชี มีหลักการพิจารณาดังนี้

1) หากเป็นบัญชีที่มีรายการบัญชีมาก ๆ และจำนวนเงินแต่ละรายการมีเพียงเล็กน้อยในกรณีที่ไม่ใช้โปรแกรมคอมพิวเตอร์จะต้องใช้ผลการตรวจสอบระบบการควบคุมภายใน (Functional Tests) และสถิติประกอบผลการสุ่มตัวอย่างทดสอบความถูกต้องของรายการทางการเงินบางรายการเป็นหลักในการพิจารณาความเชื่อถือในการปฏิบัติงานส่วนในระบบคอมพิวเตอร์อาจใช้โปรแกรมตรวจสอบและแยกแยะรายการต่าง ๆ ได้โดยละเอียด

2) สำหรับบัญชีที่มีรายการน้อย แต่จำนวนเงินสูงแทบทุกรายการ ไม่จำเป็นต้องใช้โปรแกรมคอมพิวเตอร์เข้าช่วยตรวจสอบ เพราะสามารถตรวจสอบแต่ละรายการได้โดยละเอียดอยู่แล้ว

6.1.3 ความสัมพันธ์ของบัญชีที่ตรวจสอบกับบัญชีหรือข้อมูลอื่น

ในการกำหนดขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน ควรคำนึงถึงสิ่งต่าง ๆ ดังต่อไปนี้ด้วย

- ข้อมูลที่ได้จากการทดสอบที่เกี่ยวข้องกับบัญชีที่ตรวจสอบ เช่น ดอกเบี้ยรับกับบัญชีลูกหนี้ เป็นต้น
- ข้อมูลจากแหล่งอื่นที่ได้รับในระหว่างการตรวจสอบ เช่น ราคาหลักทรัพย์ที่ธนาคารลงทุนมีแนวโน้มตกต่ำหรือสูงขึ้นเพียงใด เป็นต้น

6.1.4 รายการที่น่าสังเกต

ในการตรวจสอบความถูกต้องของรายการทางการเงินหากพบว่ามีรายการที่น่าสังเกต (เช่น ข้อผิดพลาดหรือผิดแผกไปจากระบบที่วางไว้) จะต้องหาสาเหตุให้พบและพิจารณาผลกระทบที่มีต่อระบบการควบคุมภายในและความถูกต้องของยอดคงเหลือตามบัญชีที่เกี่ยวข้องสิ่งที่ควรจำก็คือ รายการที่น่าสังเกตดังกล่าวแม้จะเกิดขึ้นเพียงรายการเดียวโดด ๆ ไม่เกี่ยวกับรายการใด ก็สามารถที่จะชี้ให้เห็นข้อบกพร่องในการควบคุมภายในที่ร้ายแรงได้โดยเฉพาะอย่างยิ่งในกรณีที่เป็นข้อผิดพลาดเกี่ยวกับโปรแกรมใช้งานหรืองบการเงิน หากปรากฏให้เห็นจะต้องขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินเพิ่มขึ้นตามความจำเป็น

สิ่งที่ควรพิจารณาเกี่ยวกับรายการที่น่าสังเกต

- รายการผิดปกติที่น่าสังเกตเป็นรายการประเภทใด
- ควรเพิ่มระดับการทดสอบมากน้อยเพียงใดจึงจะทราบว่ารายการเหล่านี้เป็นรายการที่ผิดปกติจริงหรือไม่
- มีวิธีการตรวจสอบความถูกต้องของรายการทางการเงินอื่น ๆ ที่สามารถนำมาใช้ตรวจสอบซ้ำอีกครั้งหนึ่งหรือไม่
- สาเหตุที่แท้จริงของรายการที่น่าสังเกตเกิดจากการใช้หลักในการพิจารณาตัดสินใจเกี่ยวกับวิธีการตรวจสอบหรือการกำหนดขอบเขตในการตรวจสอบไม่ถูกต้อง เช่น ไม่ได้ชี้ให้เห็นจุดอ่อนของการควบคุมในระยะแรก ๆ ให้ทราบหรือไม่
- รายการที่น่าสังเกตให้ข้อมูลเกี่ยวกับข้อผิดพลาดทางการเงินที่สำคัญซึ่งไม่สามารถเปลี่ยนแปลงวิธีการตรวจสอบ หรือขยายขอบเขตการตรวจสอบ เป็นการยืนยันความถูกต้องเพื่อประโยชน์ในการจัดทำรายงานการตรวจสอบหรือไม่

ผู้ตรวจสอบควรทำบันทึกรายการที่น่าสังเกตที่สำคัญแจ้งให้ธนาคารทราบ เพื่อสอบหาสาเหตุและดำเนินการแก้ไขให้ถูกต้องต่อไปโดยเร็ว

6.2 การขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน

6.2.1 วิธีการโดยทั่วไป

ตามที่เคยได้กล่าวมาแล้วว่า หากการตรวจสอบตามขอบเขตที่กำหนดไว้ไม่สามารถทำให้ผู้ตรวจสอบพอใจ หรือเชื่อถือการควบคุมภายในของธนาคารได้ จะต้องขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน ดังนี้

1) เปลี่ยนแปลงวิธีการตรวจสอบใหม่ หรือใช้วิธีการตรวจสอบที่ลึกกว่าเดิม เช่น ตรวจสอบและหาเอกสารหลักฐานมาสนับสนุนให้มากขึ้น หรือตรวจสอบการบวกเลขอย่างระมัดระวังมากขึ้น

2) ทำการทดสอบลักษณะรายการที่น่าสังเกตให้มากขึ้น เช่นสอบทานความถูกต้องของรายการประกอบยอดคงเหลือตามบัญชี หรือตรวจสอบความสมบูรณ์ในการบันทึกรายการ โดยการตรวจสอบเอกสารประกอบการลงบัญชีให้มากขึ้น

ก่อนเปลี่ยนแปลงวิธีการตรวจสอบผู้ตรวจสอบควรพิจารณาวัตถุประสงค์และวิธีที่จะบรรลุวัตถุประสงค์อย่างมีประสิทธิภาพด้วยความระมัดระวัง ซึ่งจะเป็นประโยชน์ต่อการตรวจสอบด้านอื่นด้วยเช่น การศึกษาดัชนีที่ใช้ในการปฏิบัติงานต่าง ๆ ก่อนพิจารณาตัดสินใจ

ในกรณีที่อาจขยายขอบเขตการตรวจสอบเฉพาะบัญชีสินทรัพย์และหนี้สิน หรืออาจต้องขยายขอบเขตการตรวจสอบความถูกต้องเฉพาะรายการที่เกี่ยวข้องกับบัญชีรายได้และรายจ่ายเพียงด้านใดด้านหนึ่งเท่านั้น จะต้องพิจารณาผลกระทบต่อบัญชีหรืองบการเงินที่ไม่ได้ขยายการตรวจสอบด้วยเช่น บัญชีกำไรขาดทุนย่อมมีผลกระทบต่องบดุลซึ่งจะมีผลต่อการตรวจสอบด้านอื่นด้วย ดังนั้นหากปรากฏว่าการขยายขอบเขตการตรวจสอบด้านใดจะมีผลทำให้การตรวจสอบด้านอื่นไม่เป็นที่น่าพอใจ จะต้องชี้ให้เห็นอย่างชัดเจนเพื่อจะได้วางแผนให้เป็นที่น่าพอใจตามวัตถุประสงค์ที่วางไว้

การขยายการตรวจสอบความถูกต้องของรายการที่เกี่ยวกับบัญชีรายได้รายจ่ายมี 2 วิธี

1) หากผู้ตรวจสอบต้องการตรวจสอบความถูกต้องของจำนวนเงินตามบัญชีรายได้หรือรายจ่ายบัญชีใดบัญชีหนึ่งโดยเฉพาะเช่น บัญชีค่าโฆษณา ค่าจ้าง หรือเงินเดือน ควรวิเคราะห์ค้นหารายการที่ก่อปัญหาให้พบ เพื่อขจัดข้อผิดพลาดให้หมดสิ้น

2) แทนที่จะถือเอาบัญชีใดบัญชีหนึ่งเป็นหลักในการตรวจสอบ ผู้ตรวจสอบอาจสนใจที่จะตรวจสอบรายการบางประเภทโดยเฉพาะ (เช่นอาจมีจุดอ่อนในการควบคุมการจ่ายเงินบางประเภท เป็นต้น) ดังนั้นจึงควรกำหนดว่ามีบัญชีรายได้และรายจ่ายประเภทใดบ้างอยู่ในข่ายที่ได้รับผลกระทบกระเทือนเนื่องจากมีจุดอ่อนในการควบคุมเพื่อคัดเลือกรายการเหล่านั้นมาตรวจสอบอย่างระมัดระวังเพื่อขจัดข้อผิดพลาดให้หมดไป

แต่อย่างไรก็ดีการขยายการตรวจสอบความถูกต้องของบัญชีรายได้และรายจ่ายตามที่กล่าวข้างต้นเป็นการแก้ปัญหาเกี่ยวกับจุดอ่อนในการควบคุมเรื่องใดเรื่องหนึ่งโดยเฉพาะเท่านั้นไม่เหมาะที่จะนำไปใช้คัดเลือกรายการทุกประเภทเพื่อใช้ในการตรวจสอบ (ที่เรียกว่า Vouching Tests) ทั้งนี้เพราะจะมีผลกระทบต่อบัญชีรายได้และรายจ่ายอย่างมหาศาล

6.2.2 การขยายขอบเขตการตรวจสอบในระบบคอมพิวเตอร์

การขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินตามที่กล่าวมาแล้วเป็นวิธีการทั่ว ๆ ไปในกรณีที่ผู้ตรวจสอบขาดความเชื่อถือการควบคุมภายใน ส่วนที่ตรวจสอบซึ่งอาจดัดแปลงวิธีการได้ตามความเหมาะสม แต่อย่างไรก็ดีผู้ตรวจสอบอาจตัดสินใจขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินเพิ่มขึ้น เพื่อเพิ่มประสิทธิภาพการทดสอบการควบคุมภายในที่เกี่ยวข้อง แม้จะพอใจวิธีการควบคุมเหล่านั้นอยู่แล้วก็ตาม ในทางปฏิบัติจะพบว่าระบบการควบคุมส่วนใหญ่ย่อมมีข้อดีและข้อเสียในการควบคุมผู้ใช้ข้อมูลและการควบคุมการจัดทำข้อมูลปะปนกันอยู่เช่นเดียวกับวิธีการทดสอบที่ใช้มักจะปะปนกันจนแยกไม่ออกระหว่างการตรวจสอบระบบการควบคุม (Functional Tests) กับการขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน

การขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน ประกอบด้วย

1) การสอบทานระบบการปฏิบัติงาน (Reperformance) เช่น การคำนวณดอกเบี้ยและค่าธรรมเนียมต่าง ๆ
2) ค้นหาข้อบกพร่องหรือสิ่งผิดปกติอย่างถี่ถ้วน (scrutiny) เช่น ค้นหาลูกค้ารายที่ธนาคารคิดดอกเบี้ยหรือค่าธรรมเนียมในอัตราที่สูงหรือต่ำกว่าปกติ
3) วิเคราะห์บัญชี (Account Analysis) เช่น การดำรงสินทรัพย์ของธนาคารนับแต่การตรวจสอบครั้งก่อน

งานการตรวจสอบความถูกต้องของรายการทางการเงินดังกล่าว สามารถใช้คอมพิวเตอร์เข้าช่วยในการอ่านข้อมูล และวิเคราะห์ได้อย่างมีประสิทธิภาพและรวดเร็วกว่าการใช้พนักงาน ซึ่งควรประหยัดแรงงานไว้ใช้ทดสอบความถูกต้องของข้อมูลตามความจำเป็นต่อไป

7. การใช้รหัสและโปรแกรมสำหรับการตรวจสอบ (Resident Code)

7.1 คำจำกัดความและวัตถุประสงค์ของ Resident Code

Resident Code หรือ Resident Program หรือ Embedded Code คือ โปรแกรมที่ผู้ตรวจสอบเขียนขึ้นมาเพื่อทำงานตามขั้นตอนที่ต้องการตรวจสอบ (เป็น Program Steps) แล้วนำไปแทรกกับโปรแกรมที่ใช้ในการประมวลผลตามปกติของธนาคารหรือผู้ตรวจสอบอาจสร้างรหัสของตนเองแทรกลงไปในโปรแกรมใช้งานจริงของธนาคารก็ได้ นอกจากนี้ผู้ตรวจสอบอาจใช้วิธีเขียนโปรแกรมตรวจสอบเพื่อใช้ประมวลผลตามจุดที่ต้องการตรวจสอบ และถือเป็นส่วนหนึ่งของโปรแกรมที่ใช้ในการปฏิบัติงานของธนาคารด้วย

วัตถุประสงค์หลักของ Resident Code คือ ทำหน้าที่ตรวจสอบรายการที่ใช้ในการประมวลผลในขณะนั้น (Live Transaction) โดยคัดเลือกและบันทึกรายการที่อยู่ภายใต้หลักเกณฑ์ที่ใช้ในการคัดเลือกลงสู่แฟ้มข้อมูลที่จะนำไปใช้ในการตรวจสอบต่อไป

รายการที่คัดเลือกและแฟ้มเก็บรายการที่คัดเลือกมีดังนี้

- รายการที่อยู่ภายใต้หลักเกณฑ์ที่ใช้ในการคัดเลือก ที่ผ่านการตรวจสอบจาก Resident Code ทั้งที่ถูกต้องและไม่ถูกต้องทุกรายการ แฟ้มข้อมูลที่เก็บรายการประเภทนี้เรียกว่า System Control Audit Review File (SCARF)
- รายการที่ถูกคัดเลือกโดยวิธีสุ่มตัวอย่างจาก Resident Code แฟ้มข้อมูลที่เก็บรายการประเภทนี้เรียกว่า Sample Audit Review File (SARF)

7.2 ประโยชน์ของ Resident Code

ประโยชน์ของ Resident Code ในที่นี้ได้แก่การตรวจสอบความถูกต้อง และ/หรือความเที่ยงตรง (Validity and/or Accuracy) ของข้อมูลนำเข้าหรือข้อมูลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ ช่วยให้ผู้ตรวจสอบไม่ต้องอาศัยความเชื่อถือที่ต้องฝากไว้กับการควบคุมผู้ใช้ข้อมูล (User) และการออกแบบโปรแกรมมากจนเกินไปนอกจากนี้ยังสามารถใช้ Resident Code ตรวจสอบโปรแกรมที่ใช้ในการประมวลผลด้วย เช่น ใช้ Resident Code ตรวจสอบข้อมูลนำเข้าที่ผิดปกติ ตรวจสอบการคำนวณดอกเบี้ยหรือรายการผิดปกติอื่น ๆ ที่ปรากฏในรายงานที่น่าสังเกต (Exception Report)

7.3 วิธีการใช้ Resident Code

การใช้ Resident Code อาจทำได้ดังนี้

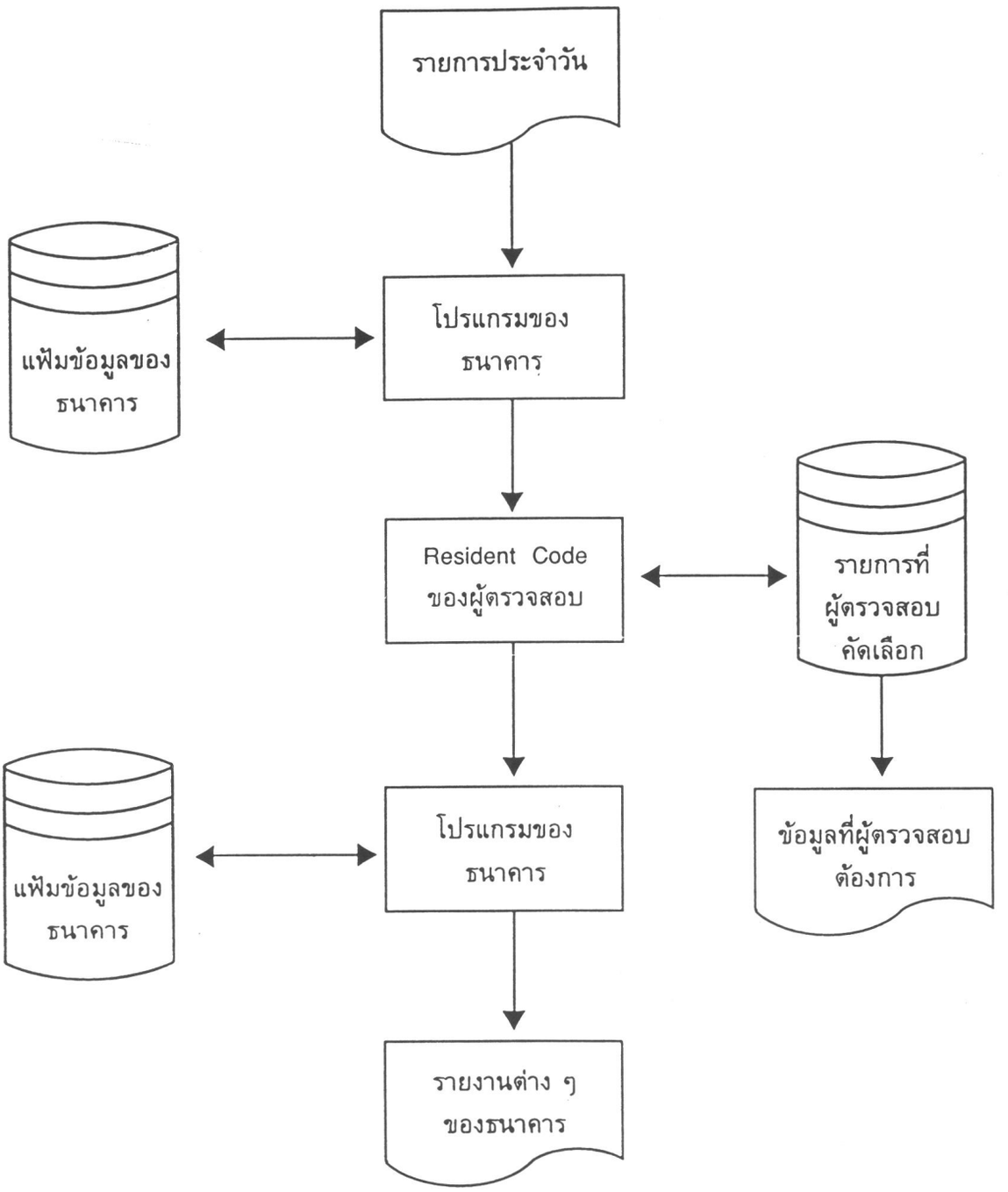
1) มอบหมายให้ผู้ตรวจสอบภายในทำหน้าที่ตรวจสอบ parameters การ "On" และ "off" ซึ่งแสดงภาวะการทำงานของ Resident Code ในระหว่างการปฏิบัติงานประจำวันแทนผู้ตรวจสอบ

2) ให้ธนาคารเก็บแฟ้มข้อมูลหรือรายงานที่ได้จากการประมวลผลด้วย Resident Code จัดส่งมาให้ผู้ตรวจสอบ หรือเก็บไว้ที่ธนาคารรอการตรวจสอบครั้งต่อไป

3) ในกรณีที่การควบคุมภายในของธนาคารยังมีจุดอ่อนเพื่อความปลอดภัยของ Resident Code ควรนำวิธีการควบคุมอื่น ๆ ที่รัดกุมมาใช้ โดยการขอสำเนาโปรแกรมที่เกี่ยวข้องกับ Resident Code มาเก็บไว้ 1 ชุด สำหรับใช้เปรียบเทียบกับโปรแกรมที่ใช้งานจริงเพื่อหาข้อแตกต่างที่ผิดสังเกตอยู่ทุกระยะ

8. Snapshot

Snapshot เป็นเทคนิคที่ขยายตัวมาจาก Resident Code เพื่อประโยชน์ในการพัฒนาและบำรุงรักษาโปรแกรมโดยวิธีสร้างรหัสพิเศษใส่ลงในโปรแกรมเพื่อตรวจสอบการทำงานของโปรแกรมที่ใช้งานในบางช่วงตามต้องการ



แผนภาพที่ 24.4 การใช้รหัสคำสั่งคงที่ (Resident Code)

9. การใช้โปรแกรมตรวจสอบโดยวิธีสอบถาม (Interactive Enquiry Software)

การตรวจสอบตามวิธีนี้ส่วนใหญ่ใช้กับระบบ On-line ระบบ Real-time และระบบ Data Base โดยสร้างโปรแกรมสำหรับตรวจสอบความถูกต้องของข้อมูล และการทำงานของโปรแกรมที่ใช้ในการปฏิบัติงาน

10. สรุป

1) วัตถุประสงค์ของการตรวจสอบความถูกต้องของรายการทางการเงินและความสำคัญของการควบคุมภายในที่มีต่อการตรวจสอบความถูกต้องของรายการทางการเงินในระบบที่ใช้คอมพิวเตอร์ และในระบบเดิมที่ไม่ได้ใช้คอมพิวเตอร์ยังคงเหมือนกัน แต่ในระบบคอมพิวเตอร์สามารถใช้โปรแกรมคอมพิวเตอร์เข้าช่วยตรวจสอบข้อมูลที่เก็บไว้ในแฟ้มเก็บข้อมูลได้สะดวกและรวดเร็ว และลักษณะการควบคุมในระบบคอมพิวเตอร์ก็ต่างไปจากระบบเดิม นอกจากนี้ยังมีข้อแตกต่างกันบางประเภทเกี่ยวกับวิธีการตรวจสอบความถูกต้องของรายการทางการเงิน

2) การใช้โปรแกรมคอมพิวเตอร์เข้าช่วยตรวจสอบงานในระบบคอมพิวเตอร์ จะได้ประโยชน์ที่สำคัญ 2 ประการ คือ สามารถตรวจสอบข้อมูลที่ต้องการตรวจสอบได้โดยละเอียดทุกรายการ และสามารถสร้างข้อมูลเสริมการตรวจสอบได้เป็นอย่างดีทำให้มีประสิทธิภาพในการตรวจสอบมากกว่าการตรวจสอบแบบเดิมที่ไม่ได้ใช้คอมพิวเตอร์

3) ลักษณะการควบคุมในระบบคอมพิวเตอร์ที่ต่างไปจากระบบเดิมมีผลทำให้วิธีการตรวจสอบความถูกต้องของรายการทางการเงินต้องเปลี่ยนแปลงไปบ้าง ทั้งนี้เพราะการควบคุมในระบบเดิมที่ไม่ได้ใช้คอมพิวเตอร์ส่วนใหญ่จะวางระเบียบการควบคุมไว้คร่าว ๆ ไม่มีแบบแผนที่แน่นอนเหมือนระบบคอมพิวเตอร์ จึงจำเป็นต้องมีการตรวจสอบการควบคุมการปฏิบัติงานและถือเป็นส่วนหนึ่งของการตรวจสอบความถูกต้องของรายการทางการเงินด้วย ซึ่งต่างกับระบบคอมพิวเตอร์ที่มีการควบคุมการปฏิบัติงานทุกขั้นตอนโดยละเอียด มีการวิเคราะห์รายการทางการเงิน และมี Exception Reports แสดงสิ่งผิดปกติที่เกิดขึ้นทุกขั้นตอนของการปฏิบัติงานซึ่งดีกว่าระบบเดิมที่ไม่ใช้คอมพิวเตอร์ ทำให้สามารถลดวิธีการตรวจสอบความถูกต้องของรายการทางการเงินที่ไม่จำเป็นลงได้บางส่วน

4) ระยะเวลาในการตรวจสอบความถูกต้องของรายการทางการเงินในระบบคอมพิวเตอร์แต่ละช่วงอาจเลื่อนกำหนดให้เร็วขึ้นกว่าเดิมเพราะสามารถตรวจสอบได้ตลอดเวลา

5) ในการกำหนดขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินระบบคอมพิวเตอร์ ควรพิจารณาลดระดับการทดสอบที่เคยใช้กับระบบเดิมที่ไม่ใช้คอมพิวเตอร์ให้น้อยลงเนื่องจากข้อมูลบางชนิดที่ได้จากการประมวลผลด้วยคอมพิวเตอร์สามารถเชื่อถือได้เพราะมีระบบการควบคุมภายในที่ดี และมีโปรแกรมคอมพิวเตอร์ตรวจสอบความถูกต้องของข้อมูลทุกรายการอยู่แล้ว แต่เพื่อให้เป็นที่น่าพอใจว่าข้อมูลต่าง ๆ ที่อยู่ในแฟ้มเก็บข้อมูลมีความสมบูรณ์อย่างแท้จริง ผู้ตรวจสอบอาจใช้โปรแกรมคอมพิวเตอร์คัดเลือกรายการออกมาตรวจสอบให้แน่ใจด้วยตนเองก็ได้

6) การใช้โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบข้อมูลที่ใช้ในการประมวลผลจำนวนมาก ๆ ได้โดยใช้ Resident Code เช่น การสร้างโปรแกรมสำหรับตรวจสอบการทำงานของโปรแกรมที่ธนาคารใช้อยู่ก็ได้ นอกจากนี้ยังอาจใช้ Interaction Enquiry Software ตรวจสอบข้อมูลในระบบ On-line, Real-time และระบบ Data Base ที่ทันสมัยได้อีกด้วย

25

การใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบ

การใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบ

1. ลักษณะโปรแกรมคอมพิวเตอร์

โปรแกรมคอมพิวเตอร์ที่ใช้ในการตรวจสอบโดยทั่วไปมีหลายชนิด ผู้ตรวจสอบอาจลงมือเขียนโปรแกรมด้วยตนเอง หรือให้ผู้อื่นเขียนโปรแกรมให้ตามความต้องการ เพื่อใช้ตรวจสอบเฉพาะงาน ไม่สามารถนำไปใช้ตรวจสอบงานอื่นได้ เรียกว่า "one off" program ส่วนอีกชนิดหนึ่งเป็นโปรแกรมเบ็ดเสร็จ (package program) ซึ่งผู้ตรวจสอบนิยมใช้กันมาก เพราะสามารถดัดแปลงใช้ตรวจสอบได้ทั่วไป

1.1 โปรแกรมชนิดที่เขียนขึ้นเอง (Writing Programs)

โดยปกติผู้ตรวจสอบจะพยายามหลีกเลี่ยงการออกแบบและการเขียนโปรแกรมด้วยตนเอง เพราะค่าใช้จ่ายสูง นับตั้งแต่การฝึกเขียนโปรแกรม การเขียนโปรแกรม และการทดสอบโปรแกรม นอกจากนี้ยังมีปัญหาในการนำโปรแกรมเข้าประมวลผล เนื่องจากธนาคารมักจัดลำดับความสำคัญในการนำโปรแกรมตรวจสอบเข้าประมวลผลไว้ในลำดับต่ำ ผู้ตรวจสอบส่วนใหญ่จึงพยายามไม่ใช้โปรแกรมชนิดนี้ (ชนิด "one off')

1.2 โปรแกรมตรวจสอบเฉพาะงาน (Specifying Programs)

เพื่อตัดปัญหาทางเทคนิค ผู้ตรวจสอบอาจเลือกใช้วิธีให้ธนาคารที่ถูกตรวจสอบช่วยเขียนโปรแกรมให้ตามที่ตนต้องการ แต่ผู้ตรวจสอบจะรู้สึกขาดความเป็นอิสระ ซึ่งที่จริงแล้ววิธีนี้มีลักษณะคล้ายกับการขอรายละเอียดประกอบการตรวจสอบนั่นเอง อย่างไรก็ดีผู้ตรวจสอบจะต้องนำโปรแกรมเหล่านี้มาทดสอบเงื่อนไขและการทำงานให้ถูกต้องก่อนใช้งานจริง

1.3 โปรแกรมเบ็ดเสร็จ (Package Programs)

โปรแกรมคอมพิวเตอร์ที่ใช้กับงานตรวจสอบ ส่วนใหญ่จะมีลักษณะการทำงานคล้ายกัน ซึ่งเน้นหนักไปในเชิงเปรียบเทียบข้อมูลใน field ต่าง ๆ ที่อยู่ในแฟ้มข้อมูล หากใช้โปรแกรมชนิด "one off" จะมีปัญหาเกี่ยวกับการแก้ไขโปรแกรมเพื่อนำไปใช้กับคอมพิวเตอร์แต่ละเครื่อง และปัญหาเกี่ยวกับเงื่อนไขในการปฏิบัติงานตรวจสอบที่แตกต่างกันด้วย ดังนั้นจึงมีบริษัทต่าง ๆ ผลิตโปรแกรมเบ็ดเสร็จ (Package Programs) สำหรับงานตรวจสอบทั่วไปออกจำหน่ายมากมาย เพื่อแก้ปัญหาที่เกิดขึ้นกับโปรแกรมชนิด "one off" ซึ่งผู้ตรวจสอบสามารถเลือกใช้ได้ตามความเหมาะสม วิธีการใช้ง่ายและสะดวก เพียงแต่ระบุอุปกรณ์คอมพิวเตอร์ (Computer Configurations) แฟ้มเก็บข้อมูลที่ต้องการใช้ และคัดเลือกเงื่อนไขการทำงานตามที่ต้องการ เพื่อให้ package program ทำงานเหมือนกับ specification program

การใช้ package program จะช่วยแก้ปัญหาปลีกย่อยเกี่ยวกับการเขียนโปรแกรมและทดสอบโปรแกรม สะดวกต่อการใช้ และเสียค่าใช้จ่ายน้อยกว่าการพัฒนาโปรแกรมด้วยตนเอง

2. ประเภทของโปรแกรม

โปรแกรมคอมพิวเตอร์ที่ใช้ตรวจสอบมีหลายประเภท สรุปได้ดังนี้

1) File Interrogation Programs ใช้ตรวจสอบแฟ้มข้อมูลต่าง ๆ เช่น master files, pipeline files และ transaction data files File Interrogation Program เป็นโปรแกรมตรวจสอบชนิดแรกที่พัฒนาและใช้ได้ดีมาหลายปี ในปัจจุบันอาจมีลักษณะเปลี่ยนแปลงไปบ้าง

2) Comparison Programs ใช้เปรียบเทียบความแตกต่างของโปรแกรมที่เป็น source form และ executable form

3) Flowcharting Programs ใช้สร้างแผนภูมิแสดงเงื่อนไขการทำงาน (Logic) ของ source programs และรายละเอียดเกี่ยวกับ verb และ data name ที่ใช้ในโปรแกรมที่ถูกตรวจสอบ

4) Interactive Enquity Programs ใช้ตรวจสอบค้นหาข้อมูลที่อยู่ในแฟ้มข้อมูลในระบบ on-line

5) Log Analysis Programs ใช้วิเคราะห์บันทึกการปฏิบัติงานที่คอมพิวเตอร์บันทึกไว้ใน log

6) Resident Code ใช้ตรวจสอบข้อมูลที่ใช้อยู่ในปัจจุบัน (Live Transaction)

7) Test Data Generation ใช้สร้างแฟ้มข้อมูลสำหรับใช้ทดสอบ

3. โปรแกรมตรวจสอบประเภท File Interrogation Package

โปรแกรมประเภทนี้มี 2 ชนิด คือ แบบ “ตายตัว” และแบบ “ยืดหยุ่น”

3.1 File Interrogation Package แบบตายตัว (Fixed)

โปรแกรมชนิดนี้ถูกออกแบบให้เหมาะสมกับผู้ตรวจสอบที่มีความรู้ความชำนาญด้านเทคนิคเพียงเล็กน้อย ทำงานเชื่อถือได้ และใช้สะดวก ไม่ต้องเขียนข้อมูลเพิ่มเติมลงไปอีก เพราะงานที่ต้องทำส่วนใหญ่ถูกบันทึกไว้ในโปรแกรมแล้ว ไม่ว่าจะเป็นอุปกรณ์ของเครื่องคอมพิวเตอร์ (Computer Configurations) แฟ้มข้อมูลที่ต้องใช้ บริษัทผู้ขาย package program จะกำหนดไว้ตายตัวในโปรแกรม แต่ไม่สะดวกที่จะนำไปใช้ที่อื่น บางกรณีอาจเป็นแบบ built-in operating system สามารถทำงานโดยอิสระด้วยตนเองไม่ต้องเชื่อมต่อ (link) กับ operating system ซึ่งเป็นระบบบริหารการทำงานของระบบคอมพิวเตอร์ บางแบบอาจเปลี่ยนรูปแบบของข้อมูล (reformat) ที่อยู่ในแฟ้มข้อมูลที่ตรวจสอบ เพื่อให้เหมาะกับลักษณะตายตัวที่กำหนดมาในโปรแกรมด้วย

วิธีใช้โปรแกรมเริ่มต้นจากการเติมข้อความลงในแบบสอบถามที่ผู้ผลิต package program จัดมาให้ แล้วนำข้อมูลตามแบบสอบถามป้อนสู่ระบบคอมพิวเตอร์ เพื่อสร้างโปรแกรมที่ต้องการใช้ตรวจสอบ โปรแกรมเหล่านี้อาจอยู่ในรูปของ object program หรือ source program ที่ใช้ภาษาระดับสูงใกล้เคียงกับภาษามนุษย์ (High Level Language) เช่น ภาษา COBOL หรือ RPG II ก็ได้ ในกรณีที่เป็น source program จะต้องนำไปเปลี่ยนรูปให้เป็นภาษาเครื่องจักร (compile) เสียก่อนที่จะนำไปใช้งาน และเรียกโปรแกรมเหล่านี้ว่า program generators, procompilers หรือ preprocessors ซึ่งมีความยืดหยุ่นพอสมควร สามารถดัดแปลงเพิ่มเติมรหัสบางตัวเพื่อให้ทำงานเพิ่มเติมได้โดยง่าย

สิ่งที่น่าสนใจอีกประการหนึ่งของโปรแกรมชนิดนี้ก็คือ ความสะดวกต่อการใช้งานในกรณีที่องค์ประกอบเกี่ยวกับตัวเครื่องคอมพิวเตอร์ (Configuration) และลักษณะการจัดเก็บข้อมูลในแฟ้มข้อมูล (File Organization) ของธนาคารที่ตรวจสอบแต่ละแห่งมีลักษณะคล้ายกัน แต่การ process งานบางชนิดอาจถูกจำกัดไปด้วย ซึ่งปัญหานี้อาจขจัดได้ด้วยวิธีเปิดโอกาสให้ผู้ตรวจสอบสามารถสร้างรหัสบางส่วนได้ด้วยตนเอง เพื่อเพิ่มประสิทธิภาพในการใช้งาน

3.2 File Interrogation Package แบบยืดหยุ่นได้ (Flexible)

โปรแกรมชนิดนี้มีความยืดหยุ่น สามารถเปลี่ยนแปลงให้เข้ากับสถานการณ์ได้โดยมีข้อจำกัดเพียงเล็กน้อย ผู้ตรวจสอบสามารถนำโปรแกรมหลักที่ซื้อมาแก้ไขให้ทำงานได้ตามความต้องการ

โปรแกรมแบบยืดหยุ่นแบ่งออกเป็น 3 ส่วน ดังนี้

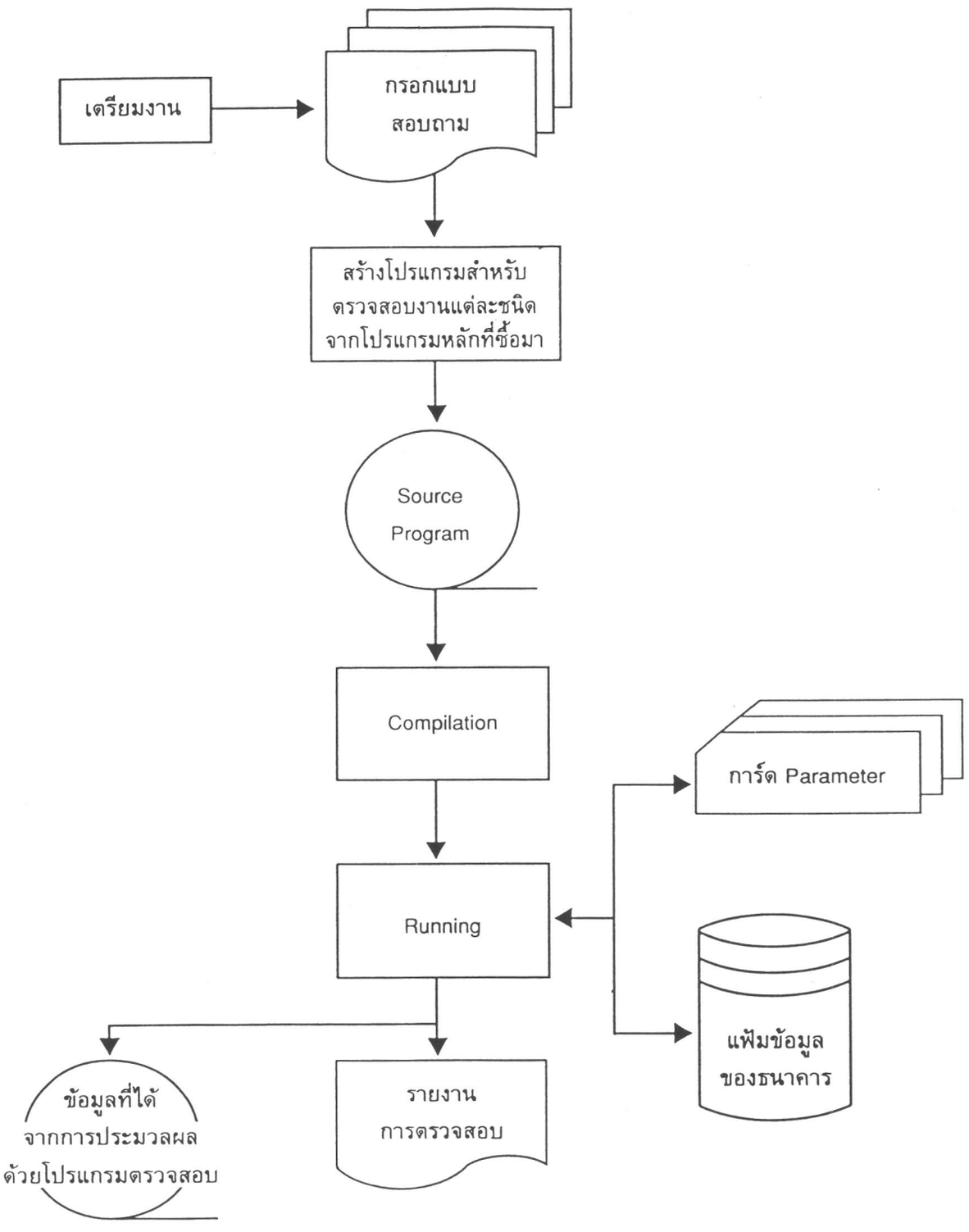
1) ส่วนแรกเป็นเรื่องเกี่ยวกับตัวเครื่องคอมพิวเตอร์ (Computer Environment) ที่ใช้ในการประมวลผลและแฟ้มข้อมูลที่จะตรวจสอบ สำหรับรายละเอียดเกี่ยวกับตัวเครื่องที่จะระบุไว้ในโปรแกรมสามารถใช้ coding sheet ตามมาตรฐานของภาษา COBOL ได้

2) ส่วนที่สองเป็นเรื่องเกี่ยวกับวิธีการประมวลผลตามความต้องการของผู้ตรวจสอบ โดยมีรหัสมาตรฐานสำหรับงานตรวจสอบที่ใช้กันทั่วไปให้ผู้ตรวจสอบเลือกใช้ตามความเหมาะสม และเก็บรวบรวมคำสั่งเหล่านี้มาสร้าง modules สำหรับใช้ในการตรวจสอบ นอกจากนี้ผู้ตรวจสอบยังสามารถใช้รหัสของตนเองเพิ่มเติมเข้าไปได้หากโปรแกรมหลักที่ซื้อมาไม่มีคำสั่งที่ต้องการใช้ในการตรวจสอบ

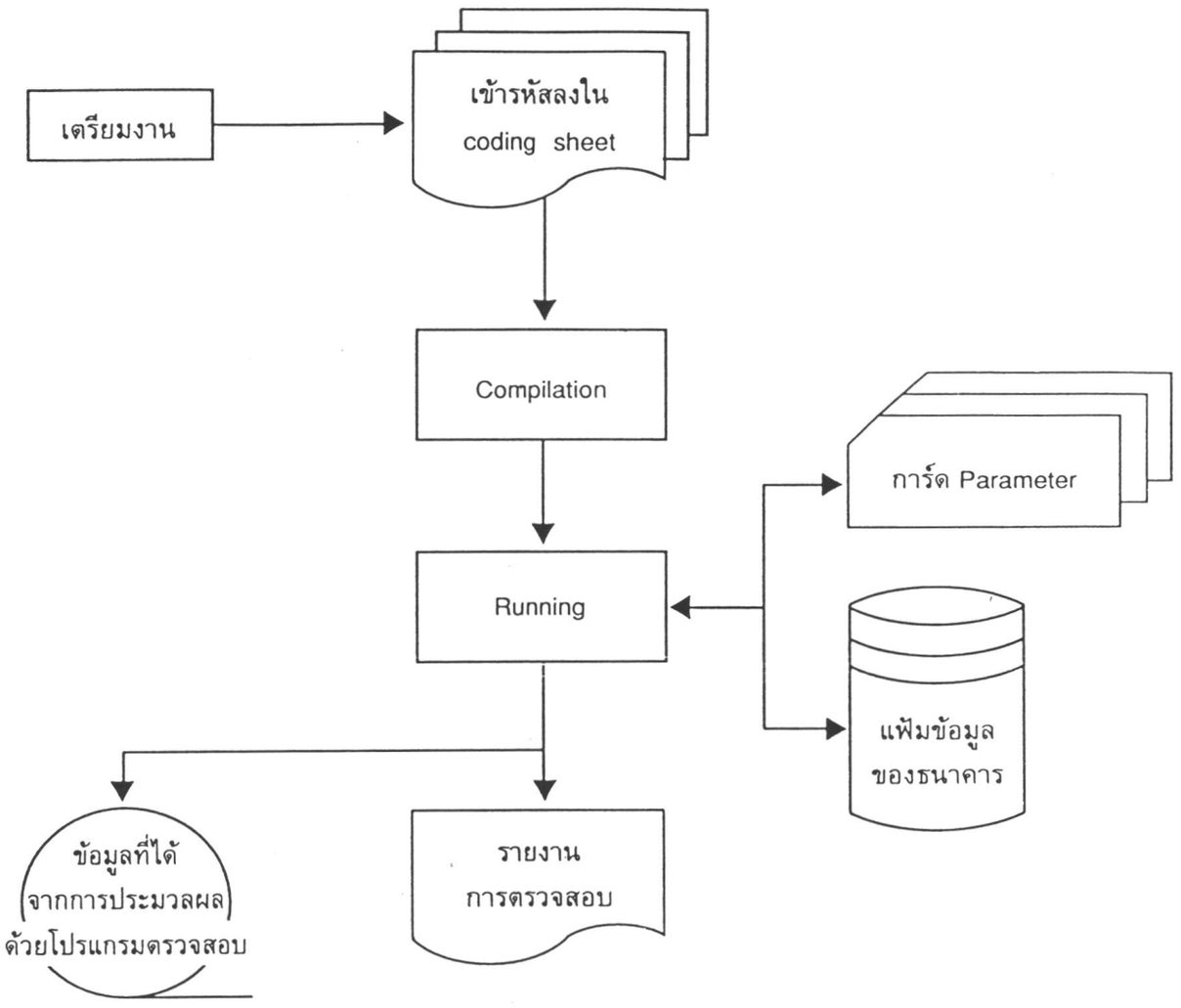
3) ส่วนที่สามเป็นงาน routine ทั่ว ๆ ไป เช่น การอ่านข้อมูล การพิมพ์รายงาน ซึ่งสามารถดัดแปลงแก้ไขได้เช่นเดียวกัน

โปรแกรมลักษณะนี้สามารถใช้กับระบบคอมพิวเตอร์ทั่ว ๆ ไปได้อย่างกว้างขวาง แม้อุปกรณ์และตัวเครื่องคอมพิวเตอร์ ตลอดจนแฟ้มเก็บข้อมูลของธนาคารที่ตรวจสอบแต่ละแห่งจะมีลักษณะต่างกันก็ตาม ทั้งนี้ควรคำนึงถึงความรู้ความชำนาญทางเทคนิคในการใช้โปรแกรมประเภทนี้ด้วย





แผนภาพที่ 25.1 File Interrogation Package (fixed)



แผนภาพที่ 25.2 File Interrogation Program (Flexible)

4. ความสะดวกในการใช้ Computer Audit Package

การใช้ Computer audit package ควรพิจารณาความสะดวกในการใช้งาน ซึ่งมีองค์ประกอบหลายประการเกี่ยวกับตัวเครื่องคอมพิวเตอร์ (Configuration) แฟ้มข้อมูล (Files) และลักษณะการทำงานของ package (Tasks) ดังนี้

4.1 องค์ประกอบเกี่ยวกับตัวเครื่องคอมพิวเตอร์ (Configuration)

การจัดหา package มาใช้งานควรพิจารณาความสะดวกในการนำ package ไปใช้กับคอมพิวเตอร์แต่ละรุ่นด้วย เพราะคอมพิวเตอร์แต่ละรุ่นจะมีวิธีการจัดเก็บข้อมูล (Data Storage and Handling) ไม่เหมือนกัน ซึ่งเป็นปัญหาในการปฏิบัติมาก โดยเฉพาะ package แบบตายตัว (Fixed) ที่ดัดแปลงแก้ไขได้เพียงเล็กน้อย แม้โปรแกรมแบบนี้จะแก้ปัญหาด้วยการแบ่ง configuration และ operating system ออกเป็นพวกๆ เพื่อให้สามารถใช้กับคอมพิวเตอร์รุ่นต่าง ๆ ได้แล้วก็ตาม

นอกจากนี้ควรพิจารณาภาษาที่ใช้ด้วย package ส่วนใหญ่จะใช้ภาษา COBOL ทำให้ไม่สามารถใช้กับคอมพิวเตอร์ขนาดเล็กซึ่งใช้ภาษา RPG II เป็นส่วนใหญ่

4.2 องค์ประกอบเกี่ยวกับแฟ้มข้อมูล (Files)

เนื่องจาก package ส่วนใหญ่สามารถใช้กับแฟ้มข้อมูลที่เป็นเทปและ disc ชนิด fixed length records ได้ดี แต่ยังมี package บางชนิดที่ไม่สามารถใช้กับ variable length records และ single bit fields ได้ ทั้งยังมีปัญหาในกรณีที่เป็นระบบ database ซึ่งอาจต้องแก้ปัญหาดังกล่าวด้วยการใช้ software ของธนาคารที่ตรวจสอบเข้าช่วยเปลี่ยนรูปแบบข้อมูล (re-formatting) หรือเข้าไปสู่ระบบ database หรือใช้ข้อมูลที่บันทึกอยู่ในรูปแบบเก่า ๆ (conventional form) ได้ นอกจากที่กล่าวควรพิจารณาความสามารถในการใช้ข้อมูลได้มากกว่า 1 แฟ้มด้วย

4.3 ลักษณะการทำงานของ package (Tasks)

สิ่งควรพิจารณาอีกประการหนึ่งคือ ความสามารถในการประมวลผลของ package ในแง่ของงานตรวจสอบ ซึ่งได้กล่าวโดยละเอียดในเรื่อง Validation Procedures ในที่นี้ขอสรุปเฉพาะเรื่องการรวมยอดข้อมูล การคัดเลือกตัวอย่าง และรายงานที่ได้จากการประมวลผลด้วย package ที่ใช้ในการตรวจสอบ

4.3.1 การรวมยอดข้อมูล (Totals)

วัตถุประสงค์ในการรวมยอดข้อมูล

1) เพื่อรวมยอดที่อยู่ในแฟ้มข้อมูลทุกรายการเป็นยอดเดียว เช่น การรวมยอดบัญชีลูกหนี้

2) เพื่อประโยชน์ในการวิเคราะห์รายการ เช่น การคัดลูกหนี้ออกเป็นพวก ๆ ตามระยะเวลาที่ค้างชำระสำหรับวิเคราะห์การจัดชั้น

3) เพื่อรวมยอดข้อมูลที่ต้องการทราบ เช่น ยอดลูกหนี้ที่เกินวงเงินเป็นที่น่าสังเกตว่าข้อมูลที่ต้องการรวมยอดส่วนใหญ่จะเป็นข้อมูลที่เป็น field หลักของรายการ แต่ในบางครั้งอาจเป็นข้อมูลใน field

ที่ไม่สำคัญก็ได้ การรวมยอดข้อมูลตามที่กล่าวในข้อแรกนั้น ส่วนใหญ่จะอาศัยคำสั่งง่าย ๆ ในการบวกยอดสะสม (Accumulation) ที่มีอยู่ในโปรแกรม สำหรับจำนวนยอดที่จะบวกมากน้อยเพียงใดนั้นสุดแล้วแต่ความต้องการของผู้ตรวจสอบ นอกจากนี้โปรแกรมดังกล่าวยังสามารถออกยอดย่อย (sub-totals) ของข้อมูลแต่ละกลุ่มได้อีกด้วย

สำหรับข้อมูลที่ต้องการทราบยอดหรือข้อมูลที่ต้องการวิเคราะห์ ส่วนใหญ่จะมีการเปรียบเทียบข้อมูล ซึ่งอาจเป็นการเปรียบเทียบเพียงครั้งเดียวหรือหลายครั้ง ดังนี้

1) เปรียบเทียบข้อมูลระหว่าง field เพียง 2 field ของแต่ละ record เช่น เปรียบเทียบยอดหนี้คงค้างกับวงเงิน

2) เปรียบเทียบข้อมูลที่อยู่ใน field ของแต่ละ record กับค่าคงที่ (constant) ที่ผู้ตรวจสอบกำหนดไว้ เช่น เปรียบเทียบยอดหนี้คงค้างของลูกหนี้แต่ละรายกับร้อยละ 25 ของเงินกองทุนของธนาคาร

3) เปรียบเทียบข้อมูลที่อยู่ใน field ของแต่ละ record กับตัวเลขที่ได้จากการคำนวณในโปรแกรมตรวจสอบ เช่น เปรียบเทียบจำนวนดอกเบี้ยเงินฝากที่จ่ายให้ลูกค้า กับจำนวนดอกเบี้ยที่ผู้ตรวจสอบคำนวณใหม่ด้วยโปรแกรมตรวจสอบ

4) เปรียบเทียบข้อมูลที่อยู่ใน field กับค่า constant เพื่อนำข้อมูลที่ได้จากการเปรียบเทียบมาคำนวณด้วยโปรแกรมตรวจสอบ เช่น เปรียบเทียบจำนวนหุ้นของผู้ถือหุ้นแต่ละรายกับร้อยละ 5 ของจำนวนหุ้นทั้งหมดของธนาคาร เพื่อนำผู้ถือหุ้นรายที่ถือหุ้นเกินกว่าอัตราดังกล่าวมาคำนวณอัตราการถือหุ้น

ในบางกรณีอาจต้องเปรียบเทียบ field และค่า constant พร้อมกันหลายตัว เช่น อาจเปรียบเทียบยอดลูกหนี้คงค้างกับ field ต่าง ๆ และค่า constant หลายตัวพร้อมกันคราวเดียว

การเปรียบเทียบข้อมูลใน field ต่าง ๆ ตามที่กล่าวมาแล้ว ควรพิจารณาถึงการถ่วงน้ำหนัก (weight) ให้กับ field บางประเภทด้วย เช่น การเปรียบเทียบยอดหนี้คงค้างกับวงเงิน อาจถ่วงน้ำหนักด้วยมูลค่าหลักประกันกับส่วนที่เกินวงเงิน

การดำเนินการเปรียบเทียบข้อมูลบางชนิด อาจต้องมีการคำนวณก่อนหรือหลังการเปรียบเทียบ ซึ่งจะมีจำนวนมากน้อยเพียงใดสุดแล้วแต่ความต้องการของผู้ตรวจสอบ ทั้งนี้ขึ้นอยู่กับลักษณะโปรแกรมที่ใช้ด้วย ถ้าเป็นโปรแกรมแบบตายตัว (Fixed) จำนวนการเปรียบเทียบอาจถูกจำกัดตามความสามารถของโปรแกรม ต่างกับโปรแกรมแบบยืดหยุ่น (Flexible) ที่ไม่จำกัดการเปรียบเทียบ และสามารถสอดแทรกวิธีการเปรียบเทียบอื่น ๆ ที่ไม่มีในโปรแกรมเพิ่มเติมเข้าไปได้

โดยปกติผู้ตรวจสอบมักต้องการบวกยอดสะสม (Accumulate) ไว้ทุกรายการทุกครั้งที่มีการเปรียบเทียบ คัดเลือกตัวอย่างและพิมพ์รายงาน แต่อาจไม่มีการบวกยอดสะสมหากมีการเปรียบเทียบเพียงเล็กน้อย วิธีการบวกยอดสะสมดังกล่าวส่วนใหญ่จะเป็นคำสั่งตายตัวอยู่ในโปรแกรมเช่นเดียวกับการคัดเลือกตัวอย่างและการพิมพ์รายงาน ซึ่งสามารถ “กระตุ้น” (Trigger) ให้ทำงานได้ตามความต้องการ การทำงานของโปรแกรมโดยปกติจะดำเนินตามขั้นตอนดังนี้

1) คำนวณก่อนการเปรียบเทียบ (ถ้าต้องการ)
2) ดำเนินการตรวจสอบโดยการเปรียบเทียบ
3) คำนวณหลังการเปรียบเทียบ (ถ้าต้องการ)
4) กระตุ้นให้คำสั่งบวกยอดสะสม คัดเลือกตัวอย่าง และพิมพ์รายงานที่อยู่ในโปรแกรมทำงานตามต้องการ คำสั่งในโปรแกรมตามที่กล่าวมานี้สามารถใช้ซ้ำกันได้หลายเที่ยว สุดแล้วแต่ความต้องการ

4.3.2 การคัดเลือกตัวอย่าง (Samples)

ใน package บางชนิดมีคำสั่ง routine สำหรับคัดเลือกตัวอย่างข้อมูลเชิงสถิติให้ด้วย เพื่อช่วยคัดเลือกข้อมูลที่จะนำไปใช้ตรวจสอบในขั้นต่อไป เช่น คัดเลือกบัญชีเงินฝากเพื่อตรวจสอบการคำนวณดอกเบี้ย แต่ในกรณีที่ผู้ตรวจสอบต้องการตัวอย่างรายการเพื่อเป็นหลักฐานประกอบยอดคงเหลือ อาจใช้วิธีการดังต่อไปนี้

1) คัดเลือกโดยวิธีสุ่มตัวอย่างไปตามจุดต่าง ๆ ของแฟ้มข้อมูล

2) คัดเลือกกระจายไปตามจำนวนเงินแต่ละระดับ เช่น ยอดเดบิต ตั้งแต่ 100,000 บาทขึ้นไป หรือยอดเครดิตตั้งแต่ 20,000 บาทขึ้นไป

3) คัดเลือกตามช่วงรายการ เช่น คัดเลือกจาก record ที่หนึ่งร้อย แล้วเว้นช่วงไปอีก 100 record เท่า ๆ กัน

4) คัดเลือกตัวอย่างจากรายการทุกประเภท แต่คุมจำนวนที่คัดเลือกในแต่ละประเภทไม่ให้เกินจำนวนสูงสุดที่กำหนดไว้ เช่น คัดเอาเฉพาะ 10 รายการแรกของข้อมูลที่คัดเลือกแต่ละประเภท

ตัวอย่างที่ได้รับการคัดเลือกตามวิธีดังกล่าวข้างต้นนี้ สามารถบันทึกลงในแฟ้มข้อมูลเพื่อนำไปเรียงลำดับรายการ (Sort) และพิมพ์รายงานหรือนำไปประมวลผลต่อไปได้ นอกจากนี้ยังใช้เป็นข้อมูลให้ธนาคารใช้ในการสอบสวนตามความจำเป็นอีกด้วย

4.3.3 การพิมพ์รายงาน (Print-out)

รูปแบบของรายงานแสดงข้อมูลต่าง ๆ ที่ได้จากการประมวลผลด้วยโปรแกรมตรวจสอบเป็นสิ่งสำคัญประการหนึ่ง เพราะรายงานต่าง ๆ เหล่านี้จะถูกนำไปใช้ประโยชน์ในการตรวจสอบ และอาจถือเป็นส่วนหนึ่งของกระดาษทำการ (Working Papers) ด้วย ดังนั้นจึงควรมีรายละเอียดเกี่ยวกับการบวกยอดทั้งจำนวนเงินและจำนวน record รวมทั้งอัตราร้อยละของรายการที่ทดสอบต่อจำนวนรายการที่มีอยู่ทั้งสิ้น แต่ package ส่วนใหญ่จะไม่มีการหาอัตราร้อยละดังกล่าวได้ แม้จะมีความสำคัญต่อผลการทดสอบเพียงใดก็ตาม

ควรพิมพ์รายละเอียดประกอบรายการที่เกี่ยวข้อง พร้อมทั้งเหตุผลในการคัดเลือกข้อมูล แต่ไม่ควรพิมพ์คำย่อหรือรหัสลงในรายงาน เพราะยุ่งยากต่อการถอดรหัสหรือแปลความหมาย การเรียงลำดับรายการ (Sort) ให้เรียบร้อยก่อนพิมพ์ จะช่วยให้อ่านรายงานได้ง่ายขึ้น นอกจากนี้การจัดรูปแบบของรายงาน การออกยอดและรายละเอียดต่าง ๆ การจัดลำดับการพิมพ์ให้เหมาะสมกับวัตถุประสงค์ในการตรวจสอบด้วย

5. ขั้นตอนการใช้โปรแกรมคอมพิวเตอร์

การกำหนดขั้นตอนในการใช้โปรแกรมไว้อย่างมีแบบแผน จะช่วยให้การใช้โปรแกรมคุ้มกับค่าใช้จ่าย และถูกต้องตามวัตถุประสงค์ สามารถตั้งงบประมาณ ดำเนินการอนุมัติ และควบคุมงบประมาณเกี่ยวกับค่าใช้จ่ายได้อย่างเหมาะสม ขั้นตอนการนำโปรแกรมมาใช้งานที่สำคัญส่วนใหญ่จะอยู่ในปีแรก ส่วนการใช้งานในปีที่ 2 และปีถัดไปจะมีลักษณะคล้ายกัน

5.1 การใช้โปรแกรมในปีแรก

5.1.1 การเสนอใช้โปรแกรม

ในขณะที่มีการประเมินระบบการควบคุมภายใน หรือในขณะวางแผนการตรวจสอบขั้นต้นเกี่ยวกับความถูกต้องของรายการทางการเงิน ควรพิจารณาข้อเสนอในการใช้โปรแกรมเข้าช่วยตรวจสอบด้วย เพื่อให้มีเวลาตระเตรียมและจัดหาโปรแกรมมาใช้งานให้ได้ประโยชน์เต็มที่

5.1.2 ข้อกำหนดเกี่ยวกับคุณสมบัติของโปรแกรม (Specification)

เมื่อได้พิจารณาตัดสินใจใช้โปรแกรมแล้ว ควรกำหนดคุณสมบัติของโปรแกรมที่ต้องการใช้ โดยกำหนดวัตถุประสงค์ ลักษณะและเงื่อนไขในการทำงานของโปรแกรม และงบประมาณที่ต้องใช้เพื่อขออนุมัติจัดหาโปรแกรม

5.1.3 การเตรียมงาน

ในกรณีที่เป็นโปรแกรมชนิด program generators จะต้องกรอกข้อความลงในแบบสอบถามที่ผู้ผลิตจัดมาให้ครบถ้วน แต่ถ้าเป็น COBOL-based programs จะต้องกรอกรหัสลงใน coding sheets และต้องจัดทำ parameter cards ด้วย เพื่อป้อนเข้าคอมพิวเตอร์ซึ่งอาจเปลี่ยนแปลงได้เช่นเดียวกับวันที่ประมวล

5.1.4 การเปลี่ยนแปลงรูปคำสั่งเป็นภาษาเครื่องจักร (Compilation)

หลังจากนั้นจึงนำแบบสอบถามและ coding sheet มาเจาะบัตรหรือบันทึกลงในอุปกรณ์อื่นและสอบทานให้ถูกต้อง แล้วจึงทำการ compile เพื่อแปลคำสั่งให้เป็นภาษาเครื่องจักร ผู้ตรวจสอบจะต้องควบคุมอย่างใกล้ชิดเพื่อให้แน่ใจว่า source statements ถูกป้อนเข้าคอมพิวเตอร์ครบถ้วน ซึ่งสามารถตรวจสอบได้โดยการนับจำนวนบรรทัดที่ปรากฏใน compilation listing โดยปกติการ compile ในครั้งแรก ๆ มักจะมีข้อผิดพลาดที่จะต้องแก้ไขให้ถูกต้องอยู่บ้าง ดังนั้นอาจต้องอาศัยผู้เชี่ยวชาญด้านโปรแกรมเข้าช่วยบ้าง

5.1.5 การทดสอบโปรแกรม

ทุกครั้งที่มีการนำโปรแกรมใหม่ออกใช้ หรือมีการแก้ไขโปรแกรมจะต้องทดสอบการทำงานก่อนใช้งานจริงเสมอ เพื่อให้แน่ใจว่าโปรแกรมดังกล่าวสามารถทำงานได้ตามวัตถุประสงค์ ซึ่งส่วนใหญ่จะอาศัยแฟ้มข้อมูลชุดสำเนาของธนาคารมาทำการทดสอบโปรแกรมบางชนิดสามารถหยุดการอ่านข้อมูลและประมวลผลได้เป็น

ช่วง ๆ หากพบว่ามีข้อมูลบางยอดแตกต่างกับยอดที่ได้จากการประมวลผลด้วยโปรแกรมของธนาคาร จะต้องพิมพ์รายการที่ประมวลผลทุกรายการ เพื่อนำไปเปรียบเทียบกับตัวเลขข้อมูลที่คำนวณไว้ล่วงหน้า ส่วนในกรณีที่แฟ้มข้อมูลที่ใช้ทดสอบมีลักษณะไม่ตรงกับเงื่อนไขการทำงานของโปรแกรมอาจต้องสร้างข้อมูลขึ้นมาทดสอบเฉพาะกรณีก็ได้

5.1.6 การดำเนินการประมวลผล (Execution)

ในขณะที่ผู้ตรวจสอบดำเนินการประมวลผลด้วยโปรแกรมที่ใช้งานได้จริงเพื่อตรวจสอบข้อมูลจริง ควรห้ามมิให้ operator หยุดเครื่องคอมพิวเตอร์โดยพลการในระหว่างการประมวลผล

5.1.7 การควบคุมโปรแกรมที่ใช้ตรวจสอบ (Control Over Program)

การตรวจสอบด้วยโปรแกรมตามปกติจะใช้วิธีการประมวลผลรวดเดียวตั้งแต่ต้นจนจบ คือ นำโปรแกรมเข้าเครื่องคอมพิวเตอร์เพื่อเปลี่ยนรูปคำสั่งให้เป็นภาษาเครื่องจักรและใช้ประมวลผลทันที ("input, compile, load and go") โดยไม่มีการบันทึกหรือคัดลอกโปรแกรมลงสู่อุปกรณ์ที่เป็นสื่อกลางอื่น ๆ (Catalogue) เก็บไว้ใน program library ของธนาคาร ทั้งนี้เพื่อหลีกเลี่ยงปัญหาในการลักลอบแก้ไขโปรแกรมตรวจสอบให้น้อยที่สุด นอกจากนี้ผู้ตรวจสอบควรควบคุมดูแลการใช้คำสั่งควบคุมการเดินเครื่องคอมพิวเตอร์ (JCL) ที่ใช้ในการประมวลผลเพื่อการตรวจสอบอย่างระมัดระวังด้วย เพื่อให้แน่ใจว่าได้มีการใช้โปรแกรมที่ถูกต้องในการตรวจสอบ และเพื่อให้แน่ใจว่าไม่มีคำสั่งอื่น ๆ สอดแทรกลงใน JCL ซึ่งอาจทำให้ผลการตรวจสอบที่ได้จากการประมวลผลผิดไปจากความเป็นจริง

ก่อนที่ผู้ตรวจสอบจะให้ความเชื่อถือในระบบการควบคุมการเดินเครื่องคอมพิวเตอร์ของธนาคาร ควรทดสอบการควบคุมของธนาคารเสียก่อน ในกรณีที่ไม่ได้ทดสอบหรือปรากฏว่ามีข้อสังเกตเกี่ยวกับการปฏิบัติงานด้านนี้เกิดขึ้น ผู้ตรวจสอบควรเข้าไปสังเกตการณ์และเช็คสอบการหยุดเครื่องของ operator ทุกครั้ง หรืออาจใช้วิธีถ่ายสำเนาแฟ้มข้อมูลแล้วนำไปประมวลผลที่อื่น

5.1.8 การใช้แฟ้มข้อมูลที่แท้จริงในการตรวจสอบ (Correct File)

ในการเช็คสอบยอดคุมกับแฟ้มข้อมูลของธนาคาร ผู้ตรวจสอบจะต้องแน่ใจว่าแฟ้มข้อมูลที่ใช้ในการตรวจสอบเป็นแฟ้มข้อมูลที่แท้จริงที่ได้จากโปรแกรมตรวจสอบ และต้องแน่ใจว่ายอดคุมนั้นสามารถพิสูจน์ได้ว่าเป็นแฟ้มข้อมูลใช้งานชุดหลังสุด และมีการแก้ไขยอดคุมอยู่เสมอเมื่อมีการแก้ไขข้อมูลทุกรายการ หากไม่แน่ใจในยอดคุมควรเช็คสอบรหัสประจำแฟ้มข้อมูล (file labels) เพื่อป้องกันการใช้แฟ้มข้อมูลผิดพลาด หรือสังเกตการสร้างแฟ้มข้อมูลและถ่ายสำเนาไว้สำหรับใช้กับโปรแกรมตรวจสอบต่อไป

5.1.9 แผนการตรวจสอบ (Audit Program)

ในแผนการตรวจสอบควรมีรายละเอียดเกี่ยวกับวัตถุประสงค์ในการตรวจสอบ การสร้างข้อมูลและการใช้ข้อมูลที่ได้จากการประมวลผลการตรวจสอบด้วยคอมพิวเตอร์ นอกจากนี้ควรกำหนดให้มีการติดตามวิธีการบริหารงานของธนาคาร รวมทั้งแฟ้มข้อมูลใช้งาน ข้อมูลที่ใช้กับโปรแกรมตรวจสอบ การจัดตัวแปรต่าง ๆ (Parameter Cards) รวมทั้งวิธีการหยุดเครื่องคอมพิวเตอร์ และวิธีการจัดทำรายงานที่ได้จากการประมวลผล

5.1.10 รายงานผลการใช้โปรแกรมตรวจสอบ (Completion Report)

หลังจากการใช้โปรแกรมตรวจสอบในครั้งแรกได้สิ้นสุดลงแล้ว ควรจัดทำรายงานผลการใช้โปรแกรม เพื่อสรุปผลและเสนอแนะสิ่งที่น่าสนใจจากการใช้โปรแกรมตรวจสอบ รวมทั้งการเปรียบเทียบค่าใช้จ่ายที่เกิดขึ้นจริงกับงบประมาณที่ตั้งไว้

5.1.11 การจัดเก็บโปรแกรมและคำสั่งอื่น ๆ ที่ใช้ในการควบคุม (Storage)

การจัดเก็บโปรแกรมการ์ด parameter cards และ JCL ควรบันทึกลงในอุปกรณ์ที่เหมาะสม และไม่ควรเก็บอุปกรณ์เหล่านี้ไว้ใน library ของธนาคารที่ตรวจพบ

5.1.12 การจัดทำ Work Plan

Work plan ที่จัดทำขึ้นควรมีลักษณะคล้ายกับแผนการตรวจสอบ โดยแบ่งงานตามความเหมาะสมและความสามารถของผู้ตรวจสอบ

5.2 การใช้โปรแกรมในการตรวจสอบครั้งถัดไป

โดยปกติโปรแกรมที่เขียนขึ้นใช้งาน ส่วนใหญ่สามารถนำไปใช้ตรวจสอบในครั้งถัดไปได้โดยไม่ต้องมีการแก้ไข แต่ในบางกรณีอาจต้องมีการเปลี่ยนแปลงบ้าง เนื่องจากมีการเปลี่ยนระบบคอมพิวเตอร์ การเปลี่ยนแปลงลักษณะการเก็บข้อมูลในแฟ้มเก็บข้อมูลหลัก การเปลี่ยน JCL หรือคำสั่งที่ operator ใช้ควบคุมการทำงานของระบบคอมพิวเตอร์ นอกจากนี้ยังอาจมีการเปลี่ยนแปลงข้อมูลบางอย่างใน parameter cards เช่น วันที่ และจำนวนตัวเลข เป็นต้น การแก้ไขดังกล่าวควรมอบหมายให้ผู้ตรวจสอบอาวุโสเป็นผู้ดำเนินการ

6. สรุป

- โปรแกรมตรวจสอบที่นิยมใช้กันมาก ได้แก่ โปรแกรมประเภท file interrogation package ซึ่งเป็นโปรแกรมตรวจสอบเอนกประสงค์ สามารถใช้ตรวจสอบงานที่คล้าย ๆ กันได้ แม้ระบบคอมพิวเตอร์ของธนาคารแต่ละแห่งจะมีลักษณะต่างกัน

- สำหรับประโยชน์ที่จะได้รับจากการใช้โปรแกรมตรวจสอบนั้น ขึ้นอยู่กับประสบการณ์ของผู้ตรวจสอบ ระบบคอมพิวเตอร์ที่ใช้ แฟ้มข้อมูลที่ตรวจสอบ งานที่ตรวจสอบ และข้อมูลที่ได้จากการประมวลผลด้วยโปรแกรมตรวจสอบ

- ควรกำหนดขั้นตอนในการแก้ไขโปรแกรมตรวจสอบไว้เป็นบรรทัดฐาน เพื่อควบคุมการใช้โปรแกรมให้เป็นไปตามวัตถุประสงค์ และค่าใช้จ่ายในการใช้โปรแกรมด้วย

26

การตรวจสอบศูนย์บริการคอมพิวเตอร์

การตรวจสอบศูนย์บริการคอมพิวเตอร์

1. คำนำ

ธนาคารพาณิชย์และองค์กรบางแห่งได้เริ่มหันมาใช้บริการด้านการประมวลผลจากศูนย์บริการคอมพิวเตอร์ภายนอก แทนที่จะซื้อเครื่องคอมพิวเตอร์ไว้ประมวลเอง ทั้งนี้เพราะมีเหตุผลหลายประการด้วยกัน อาทิ เช่น อาจเป็นการประหยัดกว่าที่จะพัฒนาและประมวลผลเอง หรืออาจเป็นความรู้สึกของฝ่ายบริหารที่ว่า การใช้คอมพิวเตอร์ให้ได้ผลดีมากที่สุดนั้นควรจะปล่อยให้เป็นหน้าที่ของผู้เชี่ยวชาญด้านคอมพิวเตอร์โดยเฉพาะ นอกจากนั้นในบางกรณีศูนย์บริการคอมพิวเตอร์สามารถประมวลผลได้อย่างมีประสิทธิภาพมากกว่า โดยการใช้โปรแกรมสำเร็จรูป (Application Packages)

ความแตกต่างที่เกิดขึ้นเมื่อทำการประมวลผล ณ ศูนย์บริการคอมพิวเตอร์ คือ การประมวลผลได้กระทำขึ้น ณ สถานที่อื่นซึ่งมิใช่ที่ทำการธนาคารพาณิชย์ และโดยสถาบันอื่นซึ่งผู้ปฏิบัติงานมิใช่พนักงานของธนาคาร ธนาคารพาณิชย์ผู้ใช้บริการจะมีฐานะเป็นเพียงผู้ใช้ (User) โดยที่การประมวลผลมิได้อยู่ภายใต้การควบคุมของธนาคาร ความแตกต่างดังกล่าวมีผลกระทบต่อการควบคุมภายในและวิธีการตรวจสอบของผู้ตรวจสอบ และย่อมหมายถึงการที่ธนาคารพาณิชย์จะต้องทำความตกลงในเรื่องขอบเขตและวิธีการปฏิบัติงานกับศูนย์บริการคอมพิวเตอร์ให้รอบคอบด้วย

2. ลักษณะทั่วไปของการประมวลผล ณ ศูนย์บริการคอมพิวเตอร์ (General Characteristics)

ลักษณะทั่วไปของการประมวลผล ณ ศูนย์บริการคอมพิวเตอร์ไม่มีความแตกต่างจากการประมวลผล ณ ศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ กล่าวคือ ระบบงาน ณ ศูนย์บริการคอมพิวเตอร์อาจเป็นได้ทั้งระบบ Batch ระบบ On-line และระบบ Real-time ซึ่งตามปกติแล้วระบบ Real-time มักจะมีโปรแกรมที่เตรียมพร้อมสำหรับใช้ในการแก้ปัญหากรณีต่าง ๆ (Problem Solving Program) คอยให้บริการได้ทุกขณะ และผู้ใช้ข้อมูลที่อยู่ห่างไกลออกไปสามารถใช้เครื่องเทอร์มินอลประมวลผลได้ โดยผ่านอุปกรณ์อำนวยความสะดวกด้านการจัดสรรเวลาการใช้เครื่องคอมพิวเตอร์ (Time Sharing Facilities)

3. ผลกระทบที่มีต่อการตรวจสอบ (Impact on the Examination)

3.1 การควบคุมภายใน (Internal Control)

โดยทั่วไปข้อกำหนด ตลอดจนเทคนิคต่าง ๆ ของการควบคุมภายในด้านการประมวลผลข้อมูลทางบัญชี ณ ศูนย์บริการคอมพิวเตอร์นั้นจะคล้ายคลึงกับที่ปฏิบัติกันอยู่ในศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ ข้อแตกต่างที่สำคัญก็คือ ในกรณีที่ทำการประมวลผล ณ ศูนย์บริการคอมพิวเตอร์นั้น ธนาคารพาณิชย์ไม่สามารถมั่นใจได้ว่ามีการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) อย่างครบถ้วน

เพราะการปฏิบัติงานและการควบคุมต่าง ๆ มิได้อยู่ภายใต้การควบคุมดูแลของธนาคาร ฉะนั้นผู้ตรวจสอบจึงควรคำนึงถึงปัญหานี้ด้วยเมื่อจะประเมินขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) และการควบคุมด้านการบำรุงรักษาและแก้ไขเปลี่ยนแปลง (Maintenance Controls)

3.1.1 ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures)

เนื่องจากธนาคารพาณิชย์ซึ่งในที่นี้มีฐานะเป็นผู้ใช้ (User) ไม่สามารถวางใจการพัฒนาโปรแกรม (Implementation) การรักษาความปลอดภัยของโปรแกรม (Program Security) และการควบคุมการใช้เครื่องคอมพิวเตอร์ (Computer Operation Control) ได้อย่างเต็มที่ ดังนั้นธนาคารพาณิชย์จึงจำเป็นต้องให้ความสนใจวิธีการควบคุมต่าง ๆ ทางด้านผู้ใช้ (User Controls) เพิ่มขึ้น โดยเฉพาะการควบคุมที่สามารถตรวจสอบได้ว่ามีการปฏิบัติตามขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ที่ได้กำหนดไว้

ถ้าธนาคารพาณิชย์ปรารถนาจะตรวจสอบว่า จุดการควบคุมที่กำหนดไว้ในขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ทำหน้าที่การควบคุมอย่างได้ผล เช่น การระบุรายการที่ขาดหายไปและโดยที่ขาดหลักฐานที่มองเห็นได้ ธนาคารพาณิชย์จำเป็นต้องทำการสอบทานการทำงานตามขั้นตอนต่าง ๆ อย่างสม่ำเสมอ โดยการใช้ข้อมูลจริง หรือข้อมูลที่สร้างขึ้นเพื่อใช้ทดสอบ (Test Data) ซึ่งทราบผลลัพธ์อยู่แล้วมาใช้ตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลนั้น

ในกรณีที่ต้องการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ส่วนที่เกี่ยวข้องกับการบัญชี เช่น การคำนวณ ธนาคารพาณิชย์ก็อาจตรวจสอบจากยอดรวมของคอมพิวเตอร์ (Computer-produced Output) แต่ในกรณีที่ไม่ปรากฏหลักฐานให้ตรวจสอบได้ ก็อาจใช้วิธีตรวจสอบเช่นเดียวกับการตรวจสอบชุดการควบคุมข้างต้น

3.1.2 การควบคุมการบำรุงรักษาและแก้ไขเปลี่ยนแปลง (Maintenance Controls)

เนื่องจากธนาคารพาณิชย์ไม่อาจวางใจต่อการควบคุมและรักษาความปลอดภัยของแฟ้มข้อมูลของศูนย์บริการคอมพิวเตอร์ได้ จึงจำเป็นต้องกำหนดมาตรการควบคุมการบำรุงรักษาและแก้ไขเปลี่ยนแปลงข้อมูลที่บันทึกไว้ในแฟ้มข้อมูลหลัก (Master Files) ให้รัดกุม ในกรณีที่เป็นข้อมูลเคลื่อนไหว (Transaction Data) ธนาคารพาณิชย์ควรจัดให้มีบัญชีคุมยอดไว้ต่างหาก (Independent Control Account) แล้วตรวจสอบอย่างระมัดระวังต่อข้อผิดพลาดที่พบจากการประมวลผล เช่น จากข้อทักท้วงของลูกค้า เป็นต้น ในกรณีที่เป็นข้อมูลถาวร (Standing Data) ก็ยิ่งมีความจำเป็นอย่างมากที่จะต้องควบคุมข้อมูลที่สำคัญเหล่านั้นทุกรายการ โดยใช้บัญชีคุมยอดต่างหากเช่นกัน การควบคุมดังที่กล่าวนี้ควรจะได้วางแผนไว้เสียตั้งแต่ขณะที่ออกแบบระบบงาน และควรตรวจสอบความถูกต้องของข้อมูลในแฟ้มข้อมูลกับเอกสารขั้นต้น (Source Records) ที่ธนาคารพาณิชย์เก็บรักษาไว้ให้บ่อยครั้ง ซึ่งในบางกรณีจำเป็นต้องขอให้ทางศูนย์บริการคอมพิวเตอร์จัดพิมพ์รายละเอียดข้อมูลที่บันทึกอยู่ในแฟ้มข้อมูลเป็นกรณีพิเศษ เพื่อใช้ในการตรวจสอบ นอกจากนี้ควรกำหนดไว้ในโปรแกรมให้พิมพ์รายการแก้ไขข้อมูลที่เป็นข้อมูลถาวร (Standing Data) ไว้ในรายงานด้วย

3.1.3 การควบคุมรายงาน (Receipt of Print-outs)

ลักษณะสำคัญซึ่งเป็นข้อแตกต่างประการหนึ่งของการใช้บริการกับศูนย์บริการคอมพิวเตอร์คือ ผู้ใช้บริการไม่สามารถควบคุมการจัดส่งรายการต่าง ๆ ที่ผลิตโดยศูนย์บริการคอมพิวเตอร์ได้ จึงมักเป็นเหตุให้ไม่ได้รับรายงาน หรือได้รับไม่ครบถ้วนบ่อย ๆ ผู้ใช้ข้อมูลจึงจำเป็นต้องมีวิธีควบคุมต่างหากที่ใช้ควบคุมการรับรายงานประเภทต่าง ๆ ทั้งที่เป็นรายงานตามปกติและรายงานพิเศษ โดยใช้ทะเบียนคุมหรือวิธีการอื่น ๆ ที่เห็นว่าเหมาะสม

3.2 วิธีการตรวจสอบ

โดยทั่วไปหลักการและวิธีการตรวจสอบศูนย์บริการคอมพิวเตอร์มีความคล้ายคลึงกับหลักการและวิธีการตรวจสอบศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ อย่างไรก็ตามยังมีบางสิ่งบางอย่างที่ผู้ตรวจสอบควรให้ความสนใจเป็นพิเศษ ดังนี้

3.2.1 การประเมินการควบคุมภายใน (Evaluation of Internal Control)

โดยทั่วไปเทคนิคการควบคุม ณ ศูนย์บริการคอมพิวเตอร์มักจะไม่แตกต่างจากการควบคุมศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ แบบสอบถามการควบคุมภายในเพียงดัดแปลงเล็กน้อยก็สามารถใช้ด้วยกันได้ รวมทั้งการสอบหาวิธีการควบคุมอย่างอื่นที่ใช้แทนกันได้ในขอบเขตการควบคุมที่ขาดหายไป วิธีประเมินการควบคุมภายในของศูนย์บริการคอมพิวเตอร์ ผู้ตรวจสอบจึงอาจใช้เทคนิคและวิธีการเช่นเดียวกับการตรวจสอบศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ นอกจากนั้นผู้ตรวจสอบยังอาจใช้ข้อมูลหรือสอบทานกระดาษทำการและรายงานของผู้สอบบัญชีของศูนย์บริการคอมพิวเตอร์เพื่อประกอบการตรวจสอบด้วยก็ได้

3.2.2 การตรวจสอบระบบการควบคุม (Functional Tests)

การตรวจสอบระบบการควบคุมของศูนย์บริการคอมพิวเตอร์ก็มีเทคนิคคล้ายคลึงกับการตรวจสอบระบบการควบคุม ณ ศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ แต่ผู้ตรวจสอบจะพบว่าการขยายขอบเขตการทดสอบการควบคุมขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) เป็นวิธีหนึ่งที่อาจใช้ตรวจสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Control) อย่างมีประสิทธิภาพมาก นอกจากนั้นผู้ตรวจสอบควรใช้การทดสอบข้อมูลจริงในระหว่างที่ข้อมูลนั้นประมวลผลงานจริง ("Live" Audit Test Data) เพราะสามารถทำการตรวจสอบได้โดยอิสระ ไม่ต้องยุ่งเกี่ยวกับพนักงานควบคุมเครื่องคอมพิวเตอร์

3.2.3 การตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures)

ในบางครั้งเป็นการยากที่จะให้ความไว้วางใจการควบคุมตามขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ที่ใช้อยู่ ณ ศูนย์บริการคอมพิวเตอร์ได้ ผู้ตรวจสอบจึงอาจใช้วิธีตรวจสอบความถูกต้องของรายการทางการเงินด้วยโปรแกรมคอมพิวเตอร์ทำการตรวจสอบความถูกต้องของรายการต่าง ๆ ที่ประมวลผลเพื่อยืนยันการควบคุมภายในต่าง ๆ ของศูนย์บริการคอมพิวเตอร์

อย่างไรก็ตามอาจเป็นการไม่สะดวกที่ผู้ตรวจสอบจะนำโปรแกรมคอมพิวเตอร์ไปใช้ ณ ศูนย์บริการคอมพิวเตอร์ ทั้งนี้อาจเป็นเพราะไม่มีเวลาเหมาะสมจะใช้เครื่องคอมพิวเตอร์หรือข้อมูลที่ผู้ตรวจสอบต้องการตรวจสอบได้บันทึกรวมไว้กับข้อมูลของผู้ใช้บริการศูนย์บริการคอมพิวเตอร์รายอื่น และทางศูนย์บริการ

คอมพิวเตอร์พิจารณาว่าอาจเกิดการเสียหายต่อข้อมูลที่เก็บไว้ได้ ดังนั้น ผู้ตรวจสอบจึงควรขอให้ธนาคารพาณิชย์สั่งให้ศูนย์บริการคอมพิวเตอร์จัดทำแฟ้มข้อมูลสำเนาสำหรับผู้ตรวจสอบ ซึ่งการตรวจสอบอาจปฏิบัติ ณ ศูนย์บริการคอมพิวเตอร์นอกเวลาทำการ หรือ ณ สถานที่อื่นที่เหมาะสมก็ได้

4. การคัดเลือกศูนย์บริการคอมพิวเตอร์

4.1 มาตรการในการคัดเลือกศูนย์บริการคอมพิวเตอร์

เป็นเรื่องยากสำหรับธนาคารพาณิชย์ในการเลือกศูนย์บริการคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งเมื่อเริ่มนำเอาวิธีประมวลผลด้วยคอมพิวเตอร์มาใช้เป็นครั้งแรกก่อนอื่นก็ควรจะพิจารณาเลือกศูนย์บริการคอมพิวเตอร์สัก 6-8 แห่ง ที่พอจะมีชื่อเสียงดีทั้งในด้านการดำเนินงานและการให้บริการ และควรจะอยู่ไม่ไกลจากธนาคารพาณิชย์มากนัก

ภายหลังจากที่ได้ตัดสินใจเลือกศูนย์บริการคอมพิวเตอร์ไว้ในขั้นต้นจำนวนหนึ่งแล้ว ธนาคารพาณิชย์ตัดสินใจเลือกขั้นสุดท้ายเพื่อลดจำนวนให้เหลือที่ตรงกับความต้องการเพียง 3 หรือ 4 แห่ง โดยทำการสัมภาษณ์บรรดาเจ้าหน้าที่ของศูนย์บริการคอมพิวเตอร์แต่ละแห่ง และรวบรวมข้อมูลในเรื่องต่อไปนี้

1) ผู้เป็นเจ้าของกิจการและความมั่นคงทางการเงิน
2) ชื่อเสียงและประสิทธิภาพในการบริหารงาน
3) ความสามารถจัดหาบริการตามที่ต้องการให้ได้ ตัวอย่างเช่น ประมวลผลในระบบ Batch หรือระบบ On-line (วิธีที่เหมาะสมที่สุดที่ควรใช้ในการประมวลผลอาจจะกำหนดไว้ก่อนจากการศึกษาความเหมาะสม (Feasibility Study) ในตอนแรก)
4) ความเข้าใจในปัญหาและการจัดการธุรกิจการธนาคารพาณิชย์
5) มีโปรแกรมสำเร็จรูป (Package) ที่เหมาะสมตรงกับงานไว้ให้เลือกใช้
6) สถานที่ตั้ง
7) แผนการพัฒนางานของศูนย์บริการคอมพิวเตอร์
8) อัตราค่าบริการและวิธีการคิดค่าบริการ

ธนาคารพาณิชย์จะต้องซักถามจนเป็นที่พอใจว่า ในกรณีที่เกิดเหตุการณ์ผันผวนซึ่งมีผลกระทบต่อวงการธุรกิจ ศูนย์บริการคอมพิวเตอร์ยังคงสามารถให้บริการได้ต่อไป เพราะการที่ศูนย์บริการคอมพิวเตอร์ไม่สามารถดำเนินการต่อไปได้นั้น ย่อมก่อให้เกิดผลเสียหายต่อธนาคารพาณิชย์อย่างร้ายแรง

ธนาคารพาณิชย์ควรให้ศูนย์บริการคอมพิวเตอร์แต่ละแห่งที่เลือกไว้ยื่นข้อเสนอเป็นลายลักษณ์อักษรในเรื่องข้อกำหนดต่าง ๆ ของบริการ โดยมีรายละเอียดในเรื่องงานที่จะประมวลผลให้ (Applications)

ปริมาณของรายการ (Volume of Transactions) ขนาดของแฟ้มข้อมูล วิธีการเก็บและบันทึกข้อมูล (Method of Data Capture) ความถี่ของการประมวลผล กำหนดเวลาล่าสุดที่จะทำงานเสร็จ (Operational Deadlines) และรายงานที่ต้องการ พร้อมกันนี้ธนาคารพาณิชย์ก็ควรจัดทำแบบสอบถามส่งให้ศูนย์บริการคอมพิวเตอร์กรอกเพื่อขอทราบรายละเอียดในเรื่องต่อไปนี้

1) การจัดแบ่งผังงานและคุณวุฒิของเจ้าหน้าที่ของศูนย์บริการคอมพิวเตอร์
2) รายละเอียดอุปกรณ์ต่าง ๆ ที่ใช้ ตลอดจนแผนงานการพัฒนาในอนาคตที่อาจมีผลกระทบต่อผู้ใช้บริการ
3) วิธีการติดต่อประสานงานในการทำงานทั้งในขณะที่พัฒนาระบบงาน และขณะประมวลผลตามปกติ
4) การรักษาความลับและความปลอดภัยของแฟ้มข้อมูล รายงานและโปรแกรม
5) หลักเกณฑ์การคิดค่าใช้จ่ายในช่วงพัฒนาระบบงาน และค่าใช้จ่ายในการประมวลผล ตลอดจนค่าบริการอื่น ๆ พร้อมรายละเอียด
6) เงื่อนไขและข้อตกลงทั้งหมดที่พึงกำหนดไว้ในสัญญาของทั้งสองฝ่าย รวมถึงมาตรการในการรักษาความปลอดภัยและหลักประกันต่าง ๆ เช่น วิธีการและกำหนดเวลาในการส่งรายงานจากศูนย์บริการคอมพิวเตอร์ไปยังผู้ใช้ข้อมูล เป็นต้น

4.2 การประเมินข้อเสนอของศูนย์บริการคอมพิวเตอร์

ศูนย์บริการคอมพิวเตอร์จำเป็นต้องใช้เวลาประมาณ 2-4 สัปดาห์ ในการเตรียมข้อเสนอต่าง ๆ ในช่วงนี้ธนาคารพาณิชย์ก็ควรพิจารณาหามาตรการที่ใช้ในการคัดเลือกไว้ให้ครบถ้วน ตลอดจนเรื่องต่าง ๆ ที่เห็นว่ามีความสำคัญควรเพิ่มเติมไว้ในแต่ละข้อ ในขั้นนี้ธนาคารพาณิชย์ที่ยังไม่มีประสบการณ์ในด้านการประมวลผลด้วยคอมพิวเตอร์ ก็ควรจะหาที่ปรึกษาเพื่อขอคำแนะนำในเรื่องราคาค่าบริการที่เสนอมา และเงื่อนไขต่าง ๆ ตามสัญญา

ควรประเมินข้อเสนอของศูนย์บริการคอมพิวเตอร์แต่ละแห่งอย่างรอบคอบเพื่อที่จะได้คัดเลือกศูนย์บริการคอมพิวเตอร์ที่น่าจะมีคุณสมบัติตามที่กำหนดไว้มากที่สุด ทั้งในด้านประสิทธิภาพและราคา ธนาคารพาณิชย์อาจขอเข้าชมกิจการของศูนย์บริการคอมพิวเตอร์เพื่อดูประสิทธิภาพในการปฏิบัติงานทั่ว ๆ ไป และติดต่อสอบถามบรรดาลูกค้าของศูนย์บริการคอมพิวเตอร์นั้น ๆ ในเรื่องความถูกต้องของงาน การตรงต่อเวลา และการให้ความร่วมมือดีเพียงใด เพื่อเป็นการยืนยันไปในตัว

4.3 การทำสัญญา

ก่อนที่ธนาคารพาณิชย์จะตกลงทำสัญญากับศูนย์บริการคอมพิวเตอร์ ก็ควรจะทำความตกลงกันให้แน่นอนในเรื่องค่าบริการที่จะต้องจ่ายตามปกติและในกรณีพิเศษ ทั้งในช่วงพัฒนาระบบงานและช่วงการประมวล

ผล นอกจากนี้ควรทำความตกลงในเรื่องหน้าที่และความรับผิดชอบในการติดต่อประสานงานกันระหว่างเจ้าหน้าที่ของธนาคารพาณิชย์กับเจ้าหน้าที่ของศูนย์บริการทางคอมพิวเตอร์เสียให้เรียบร้อย

เรื่องอื่น ๆ ที่ควรกำหนดไว้ในสัญญามีดังนี้

1) การแบ่งความรับผิดชอบระหว่างศูนย์บริการคอมพิวเตอร์กับธนาคารพาณิชย์ในงานที่เกี่ยวข้องทั้งหมด เช่น ใครจะเป็นผู้ขนส่งเอกสารในการประมวลผล (Input) และรายงานต่าง ๆ (Output)

2) มาตรการต่าง ๆ ในด้านการรักษาความปลอดภัยและความลับของข้อมูลและแฟ้มข้อมูลต่าง ๆ ตลอดจนการทำชุดแฟ้มข้อมูลสำรอง (Generations) ที่จะต้องเก็บรักษาไว้ และสถานที่เก็บ

3) การเตรียมการในกรณีที่อุปกรณ์คอมพิวเตอร์ต่าง ๆของศูนย์บริการคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ ด้วยเหตุไฟไหม้หรือภัยพิบัติอื่น ๆ

4) กรรมสิทธิของโปรแกรมกรณีที่ธนาคารพาณิชย์มิได้ใช้โปรแกรมสำเร็จของศูนย์บริการคอมพิวเตอร์ โดยปกติแล้วโปรแกรมที่เขียนโดยเจ้าหน้าที่ธนาคารพาณิชย์ หรือโดยเจ้าหน้าที่ของศูนย์บริการคอมพิวเตอร์ แต่ในนามของธนาคารพาณิชย์จะตกเป็นกรรมสิทธิของธนาคารพาณิชย์ เรื่องกรรมสิทธิในโปรแกรมมีความสำคัญในกรณีที่ธนาคารพาณิชย์ต้องการทำการประมวลผล ณ สถานที่อื่น ไม่ว่าด้วยเหตุผลประการใด รวมทั้งกรณีหมดอายุสัญญาการใช้บริการด้วย

5) ข้อตกลงในเรื่องค่าเสียหายหรือการชดใช้วิธีอื่นกรณีที่มีการผิดสัญญา เช่น ในกรณีที่ศูนย์บริการคอมพิวเตอร์ประมวลผลให้ไม่ทันตามกำหนด ควรมีการกำหนดมาตรการชี้ขาดไว้ล่วงหน้าสำหรับข้อขัดแย้งต่าง ๆ ที่อาจเกิดขึ้น

5. การปฏิบัติงานร่วมกับศูนย์บริการคอมพิวเตอร์

นอกเหนือไปจากการทำสัญญาอย่างเป็นทางการแล้ว การสร้างความสัมพันธ์เหมาะสมในการปฏิบัติงานร่วมกับศูนย์บริการคอมพิวเตอร์ ก็เป็นสิ่งที่มีความสำคัญอีกประการหนึ่งด้วยเช่นกัน เรื่องต่าง ๆ ที่ควรจะทำความตกลงกัน ได้แก่ การติดต่อประสานงานในระหว่างกัน การพัฒนาระบบและโปรแกรมโดยศูนย์บริการคอมพิวเตอร์ และการปฏิบัติงานของแต่ละฝ่าย

5.1 การติดต่อประสานงานระหว่างกัน

แม้จะเป็นที่คาดหวังกันไว้ว่า ทั้งศูนย์บริการคอมพิวเตอร์กับธนาคารพาณิชย์จะพัฒนาความสัมพันธ์อันดีในการทำงานร่วมกันก็ตาม ทั้งสองฝ่ายก็ยังคงเป็นองค์กรแยกต่างหากจากกัน และการติดต่อกันก็ต้องทำอย่างเป็นทางการอยู่ดี แต่ละฝ่ายควรมอบหมายให้เจ้าหน้าที่ของตนเป็นผู้รับผิดชอบในการติดต่อระหว่างกันไว้โดยแน่ชัด

ซึ่งอาจกำหนดไว้ในสัญญาก็ได้ และควรจะให้เจ้าหน้าที่ผู้นั้นทำการติดต่อหรือร่วมประชุมด้วยทุกครั้ง ทั้งในขณะพัฒนาระบบงานหรือเมื่อทำการประมวลผลแล้ว

การติดต่อใด ๆ ระหว่างกันไม่ควรจะกระทำในลักษณะที่กำกวมไม่ชัดเจน การติดต่อโดยวาจาแต่ละครั้งควรจะได้รับการยืนยันเป็นหนังสือโดยเร็ว เพื่อเป็นการประกันว่าเมื่อเกิดข้อขัดแย้งก็สามารถหาข้อเท็จจริงมายืนยันได้

5.2 การพัฒนาระบบงาน (Development work)

ธนาคารพาณิชย์อาจตัดสินใจที่จะพัฒนาโปรแกรมที่ใช้ในงานของตนขึ้นเป็นพิเศษ ซึ่งสามารถจัดทำได้โดยเจ้าหน้าที่ของธนาคารพาณิชย์ หรือโดยเจ้าหน้าที่ของศูนย์บริการคอมพิวเตอร์ นอกจากนี้อาจเลือกใช้โปรแกรมสำเร็จรูป (Package) ที่ศูนย์บริการคอมพิวเตอร์จัดหามา ซึ่งพิจารณาแล้วว่าเหมาะสม โปรแกรมส่วนมากจำเป็นต้องแก้ไขให้ตรงกับความต้องการใช้งานเสียก่อน ดังนั้นจึงต้องมีการประชุมและตกลงกันในรายละเอียดในการพัฒนาระบบงานอย่างสม่ำเสมอ ไม่ว่าจะใช้โปรแกรมของใครก็ตาม นอกจากนี้ในเรื่องกรรมสิทธิ์ของโปรแกรมที่ใช้ในการประมวลผล ก็ควรจะได้พิจารณาและทำความตกลงกันให้เรียบร้อยแล้วแนบข้อตกลงดังกล่าวไว้กับสัญญาการใช้บริการด้วย เรื่องที่ควรพิจารณาตกลงกันมี ดังนี้

1) วิธีการคิดค่าบริการในงานแต่ละงาน เช่น คิดค่าบริการแยกตามระบบงานด้วยวิธีจ่ายครั้งเดียว (Separate Fixed Price Contract) หรือคิดตามเวลาและวัสดุที่ใช้ไป (Time and Material Basis)

2) ศูนย์บริการคอมพิวเตอร์ควรเป็นผู้จัดทำคู่มือการปฏิบัติงาน (Procedures Manuals) พร้อมทั้งจัดพิมพ์แบบฟอร์มในการเตรียมข้อมูล ตลอดจนคำอธิบายรายงานต่าง ๆ ให้ด้วย

3) วิธีปฏิบัติในการกำหนด (Specifying) ยกเลิก (Signing off) และเปลี่ยนแปลงแก้ไข (Modifying) ระบบงาน เช่น เมื่อธนาคารพาณิชย์ได้กำหนดระบบงานขึ้นมาแล้ว ศูนย์บริการคอมพิวเตอร์จะทำรายละเอียดของระบบงานซึ่งมักจะทำในรูปผังระบบงาน (Flow Chart) และอธิบายวิธีการประมวลผล ธนาคารพาณิชย์จะต้องตรวจดูว่ารายละเอียดของระบบงานนั้น ๆ ตรงกับความต้องการโดยครบถ้วนหรือไม่ การยกเลิกระบบงานใด ๆ ต้องได้รับความเห็นชอบจากธนาคารพาณิชย์ก่อนเสมอ การเปลี่ยนแปลงสภาพการทำงานใด ๆ ของธนาคารพาณิชย์ อาจทำให้ต้องเปลี่ยนแปลงแก้ไขระบบงานซึ่งได้พัฒนาใช้แล้ว วิธีการเปลี่ยนแปลงแก้ไขก็จำเป็นต้องกำหนดหรือให้ยกเลิกโดยวิธีการเช่นเดียวกับข้างต้น และควรจะประเมินผลกระทบของการเปลี่ยนแปลงแก้ไขที่อาจมีต่อการปฏิบัติงานในทุก ๆ ด้าน การแก้ไขเปลี่ยนแปลงโปรแกรมใดบ่อย ๆ อาจทำให้ต้องแก้ไขเปลี่ยนแปลงโปรแกรมอื่นในชุดเดียวกันด้วย

4) ขั้นตอนการอนุมัติให้ใช้ระบบงานและโปรแกรม ควรผ่านช่วงการทดลองปฏิบัติงานโดยคอมพิวเตอร์ควบคู่ไปกับระบบงานเดิม (Parallel Running) ให้ได้ผลเป็นที่พอใจของธนาคารพาณิชย์เสียก่อน

5) วิธีการสร้างและตรวจสอบแฟ้มข้อมูลหลัก (Master Files) ถ้าศูนย์บริการคอมพิวเตอร์เป็นผู้สร้างแฟ้มข้อมูลขึ้นจากสมุดแยกประเภท หรือข้อมูลที่ธนาคารพาณิชย์ส่งมาให้ ก็ควรพิมพ์รายงาน (Print-out) ให้ธนาคารพาณิชย์ใช้ตรวจสอบความถูกต้องครบถ้วนของข้อมูลที่บันทึกไว้ในแฟ้มข้อมูลด้วย

5.3 การปฏิบัติงาน (Operational work)

ตามปกติศูนย์บริการคอมพิวเตอร์และธนาคารพาณิชย์มักจะอยู่ห่างไกลกัน ดังนั้นจึงจำเป็นต้องกำหนดแบ่งแยกหน้าที่และความรับผิดชอบในขั้นตอนการปฏิบัติงานต่าง ๆ ไว้อย่างชัดเจน เรื่องที่สำคัญ ๆ ที่ควรพิจารณามีดังนี้

1) กำหนดเวลาและวิธีการในการส่งข้อมูล (Input Data) ไปยังศูนย์บริการคอมพิวเตอร์ ในกรณีที่ธนาคารพาณิชย์จำเป็นต้องส่งเอกสารต้นฉบับ (Original Vouchers) ออกนอกที่ทำการก็ควรทำสำเนาโดยถ่ายเอกสารไว้หรือบันทึกไมโครฟิล์ม

2) ความถี่ (Frequency) และขอบเขต (Scope) ในการประมวลผล ตลอดจนกำหนดเวลาแล้วเสร็จซึ่งย่อมขึ้นกับเวลาที่ได้รับข้อมูล (Input)

3) ภาระหน้าที่และความรับผิดชอบในการดูแลให้มีการปฏิบัติตามการควบคุมด้านต่าง ๆ

4) การแก้ไขข้อมูลที่ประมวลผลไม่ได้ หรือประมวลผลไม่ถูกต้องเพื่อนำเข้าประมวลผลใหม่ ควรทำความตกลงกันไว้ล่วงหน้าว่ากรณีใดบ้างที่ศูนย์บริการคอมพิวเตอร์จะคิดค่าบริการในการนำงานเข้าประมวลผลใหม่

5) ควรมีการตกลงกันถึงการประมวลผลและการคิดค่าบริการในกรณีต่อไปนี้
   (1) ศูนย์บริการคอมพิวเตอร์ได้รับข้อมูลล่าช้า
   (2) การทำงานในวันหยุดประจำสัปดาห์ วันหยุดธนาคาร หรือวันหยุดราชการ
   (3) การทำงานตามโปรแกรมต่าง ๆ (Running of Programs)

ในกรณีดังกล่าวศูนย์บริการคอมพิวเตอร์มีวิธีคิดค่าบริการตั้งแต่แบบเหมาจ่าย (Global Charges) สำหรับงานทั้งหมดที่ทำในช่วงระยะเวลาใดเวลาหนึ่งตามที่ตกลงกันไปจนถึงแบบใช้สูตรยุ่งยาก โดยคิดตามจำนวนรายการที่ประมวลผล จำนวนบรรทัดที่พิมพ์ จำนวนการใช้แฟ้มข้อมูล และปัจจัย (Factors) ตัวอื่น ๆ ที่สามารถจะนำมาคำนวณได้ ดังนั้นจึงจำเป็นต้องทำความตกลงกันไว้ถึงเงื่อนไขพิเศษต่าง ๆ ในการคิดค่าบริการตามกรณีเหล่านั้นไว้ด้วย

6) การตรวจทานการคิดค่าบริการทั้งในกรณีปกติและพิเศษ ศูนย์บริการคอมพิวเตอร์ควรจัดหารายละเอียดของงานที่ประมวลผลไว้อย่างพอเพียง เพื่อให้ผู้ใช้ข้อมูลสามารถเข้าใจและตรวจทานการคิดค่าบริการได้

6. สรุป

ลักษณะเฉพาะของการประมวลผล ณ ศูนย์บริการคอมพิวเตอร์ที่ธนาคารพาณิชย์และผู้ตรวจสอบควรทราบก็คือ การประมวลผลได้กระทำ ณ สถานที่อื่นซึ่งอยู่ไกลออกไป โดยองค์กรอื่นซึ่งผู้ปฏิบัติงานไม่ได้เป็นลูกจ้างของธนาคารพาณิชย์ และไม่อยู่ภายใต้การควบคุมดูแลของธนาคารพาณิชย์

โดยทั่วไปข้อกำหนดและเทคนิคของการควบคุมภายในต่าง ๆ ณ ศูนย์บริการคอมพิวเตอร์มีลักษณะเช่นเดียวกับการควบคุม ณ ศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ ข้อแตกต่างที่สำคัญคือ ธนาคารพาณิชย์ไม่อาจไว้วางใจในวิธีการควบคุมต่าง ๆ ที่ใช้ปฏิบัติอยู่ ณ ศูนย์บริการคอมพิวเตอร์นั้นได้เต็มที่ เนื่องจากมิได้ทำการควบคุมด้วยตนเอง ผู้ตรวจสอบจึงต้องคำนึงถึงปัญหานี้ด้วยเมื่อทำการประเมินการควบคุมภายใน

หลักการและวิธีการตรวจสอบต่าง ๆ ที่ใช้กับศูนย์บริการคอมพิวเตอร์ ก็คล้ายกับหลักการและวิธีการที่ใช้กับศูนย์คอมพิวเตอร์ของธนาคารพาณิชย์ แต่อย่างไรก็ตามผู้ตรวจสอบก็ควรให้ความสนใจเป็นพิเศษในการประเมินการควบคุมภายใน การตรวจสอบระบบการควบคุม (Functional Test) และการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures)

ธนาคารพาณิชย์ต้องใช้ความรอบคอบทั้งในการคัดเลือกและการปฏิบัติงานร่วมกับศูนย์บริการคอมพิวเตอร์ และผู้ตรวจสอบควรจะสอบถามเพื่อให้ข้อสังเกตในเรื่องเหล่านี้ด้วย



27

ตัวอย่างคำถามอีกรูปแบบหนึ่งที่ใช้เป็นเทคนิค ในการประเมินการควบคุมภายใน สำหรับการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

ตัวอย่างคำถามอีกรูปแบบหนึ่งที่ใช้เป็นเทคนิคในการประเมินการควบคุมภายในสำหรับการตรวจสอบองค์กรที่ใช้คอมพิวเตอร์

ตัวอย่างคำถามข้างล่างเป็นคำถามที่สำคัญ ๆ ที่ผู้สอบบัญชีอาจจะนำมาใช้ในการประเมินระบบการควบคุมภายใน สำหรับระบบบัญชีที่ใช้คอมพิวเตอร์ คำถามเหล่านี้อาจจะไม่สมบูรณ์ แต่อาจจะนำมาถือเป็นแนวในการสร้างคำถามเพื่อการประเมินการควบคุมภายในสำหรับระบบบัญชีที่ใช้คอมพิวเตอร์ในการแสดงตัวอย่างคำถามดังปรากฏมีข้อควรระลึกดังต่อไปนี้

ก. ในที่นี้ได้สมมุติว่าคำถามในการประเมินการควบคุมภายในสำหรับวิธีการบัญชีนี้ไม่ใช่เป็นส่วนหนึ่งของการประมวลผลโดยคอมพิวเตอร์จะแยกทำต่างหาก เช่น คำถามเพื่อการประเมินการควบคุมในการจ่ายค่าแรง โดยปกติมักจะพิจารณาคำถามเกี่ยวกับการควบคุมภายใน ทั้งในส่วนทั่วไปและส่วนที่เกี่ยวกับการประมวลข้อมูลโดยคอมพิวเตอร์ไปพร้อม ๆ กัน เพื่อสามารถทำความเข้าใจเกี่ยวกับระบบที่ใช้อยู่ได้โดยถูกต้อง และเพื่อสามารถประเมินความสำคัญของการควบคุมแต่ละอย่าง

ข. คำถามที่นำมาแสดงเป็นตัวอย่างนี้ เป็นคำถามเพื่อให้ได้รับข้อมูลเกี่ยวกับประเภทของการควบคุม ในกรณีที่เหมาะสมอาจจะมีคำถามเพิ่มเติมเมื่อทราบว่าใครเป็นผู้ทำหน้าที่ควบคุม และการควบคุมเช่นว่านั้นมีหลักฐานอะไรแสดงบ้าง ซึ่งคำถามเพิ่มเติมเหล่านี้มิได้นำมาแสดง ณ ที่นี้

ค. คำถามเกี่ยวกับการประเมินการควบคุมภายในในระบบบัญชีที่ใช้คอมพิวเตอร์มักจะรวมคำถามเกี่ยวกับยี่ห้อ ชนิด และขนาดของคอมพิวเตอร์ที่ใช้ พร้อมด้วยอุปกรณ์ประกอบ คำถามเหล่านี้โดยปกติไม่กระทบกระเทือนการประเมินการควบคุมภายใน และมิได้รวมอยู่ ณ ที่นี้

ในการประเมินระบบการควบคุมภายใน ไม่ได้ให้ความสำคัญเกี่ยวกับการแบ่งแยกหน้าที่ระหว่างแผนกผู้ใช้ข้อมูลและแผนกคอมพิวเตอร์ และการแบ่งแยกหน้าที่ระหว่างหน่วยงานสำคัญในแผนกคอมพิวเตอร์ เช่น แบ่งเป็นหน่วยงานพัฒนาระบบ หน่วยปฏิบัติการประมวลผล หน่วยเก็บรักษาแฟ้มข้อมูลและโปรแกรมคำสั่ง และหน่วยควบคุม คำถามที่จะใช้ในการประเมินการควบคุมภายใน ก็ดำเนินตามแนวความคิดนี้ ดังนั้น

- ในการประเมินการควบคุมภายในเกี่ยวกับการบริหารและการพัฒนาระบบ จะต้องระมัดระวังที่จะต้องแยกระหว่างจุดอ่อนที่สำคัญในระบบ และการมีประสิทธิภาพในการดำเนินงาน
- ในการประเมินการควบคุมเฉพาะระบบงานซึ่งมีเทคนิคการควบคุมต่าง ๆ ใช้อยู่ คำถามในขั้นแรกจะถามว่ามีการควบคุมด้วยมือหรือไม่ ถ้าคำตอบที่ได้รับบอกว่ามีการควบคุมเช่นนั้นอยู่ คำถามต่อไปที่เกี่ยวกับการควบคุมในเรื่องเดียวกันโดยโปรแกรมคำสั่งก็อาจจะไม่จำเป็น

นอกจากนี้ภายหลังคำถามบางคำถามได้มีข้อความต่อท้าย เพื่อบอกว่าคำถามเช่นนั้นมีความสำคัญเมื่อใด ตลอดจนความสำคัญเกี่ยวกับการควบคุมว่าทำด้วยมือหรือโดยโปรแกรมคำสั่ง

1. การควบคุมภายในเกี่ยวกับการบริหาร

(คำถามในส่วนนี้เกี่ยวกับระบบคอมพิวเตอร์เป็นส่วนรวม)

การแบ่งแยกความรับผิดชอบ

1. หัวหน้าแผนกคอมพิวเตอร์รับผิดชอบขึ้นตรงต่อเจ้าหน้าที่ในระดับสูงตามที่กำหนดไว้อย่างเหมาะสมในกิจการนั้นหรือไม่

2. การปฏิบัติงานในหน้าที่ต่าง ๆ ดังต่อไปนี้ กระทำโดยหน่วยงานที่แยกออกจากกันหรือไม่ :
   - การพัฒนาระบบ
   - การจัดเตรียมข้อมูล
   - การควบคุมการทำงานของเครื่อง
   - การเก็บรักษาแฟ้มต่าง ๆ
   - การควบคุม

3. มีการจัดทำผังการจัดสายงานและรายละเอียดการปฏิบัติงานในแต่ละหน้าที่หรือไม่

4. มีการจำกัดขอบเขตในเรื่องเหล่านี้หรือไม่
   ก. การเข้าไปเกี่ยวข้องกับเอกสารซึ่งเป็นแหล่งกำเนิดข้อมูล ควรจะจำกัดเฉพาะพนักงานผู้มีหน้าที่ควบคุม และเจ้าหน้าที่จากหน่วยงานจัดเตรียมข้อมูล
   ข. พนักงานในแผนกคอมพิวเตอร์ไม่ควรเข้าไปเกี่ยวข้องกับบันทึกทางการเงินที่ทำด้วยมือ
   ค. ห้ามการเข้าไปในห้องเครื่องในระหว่างการประมวลผล นอกจากเจ้าหน้าที่ผู้ควบคุมการทำงานของเครื่อง
   ง. การเข้าไปเกี่ยวข้องกับแฟ้มข้อมูลและโปรแกรมคำสั่ง จะจำกัดเฉพาะผู้มีหน้าที่ควบคุมการทำงานของเครื่อง และ librarian ผู้เก็บรักษาแฟ้มข้อมูลและโปรแกรมคำสั่งเหล่านั้นเท่านั้น
   จ. พนักงานผู้ควบคุมการทำงานของเครื่อง และผู้เขียนโปรแกรมคำสั่ง ไม่มีหน้าที่ในการเปลี่ยน-แปลงข้อมูลนำเข้า (Input Data)
   ฉ. พนักงานในหน่วยควบคุมและ librarian ไม่มีหน้าที่อื่นใดอีกภายในแผนกคอมพิวเตอร์
   ช. พนักงานในแผนกคอมพิวเตอร์ไม่มีหน้าที่ก่อให้เกิดรายการและเปลี่ยนแปลงข้อมูลใน master file
   ซ. ห้ามมิให้ใครเข้าไปในห้องคอมพิวเตอร์โดยไม่ได้รับอนุญาต (ให้บอกวิธีการในการควบคุมด้วย)

5. ข้อจำกัดดังกล่าวในข้อ 4 ได้นำมาใช้อยู่เสมอหรือไม่

การควบคุมพนักงานผู้ควบคุมการทำงานของเครื่อง

6. การปฏิบัติงานของพนักงานผู้ควบคุมการทำงานของเครื่อง มีการควบคุมโดย
   ก. คู่มือในการบริหาร
   ข. ตารางกำหนดเวลาการทำงาน

ค. คำสั่งเกี่ยวกับการประมวลผลในแต่ละครั้ง
ง. รายงานการใช้เครื่องคอมพิวเตอร์ (เช่น รายงานที่พิมพ์โดยเครื่อง)
จ. กำหนดให้มีพนักงานผู้ควบคุมการทำงานของเครื่องปฏิบัติงานร่วมกันอย่างน้อย 2 คน ในหนึ่งผลัด
ฉ. มีการสับเปลี่ยนหน้าที่
ช. ด้วยวิธีการอื่น ๆ (ระบุ)

7. ในการพิมพ์รายงานโดยเครื่องมีการ แสดงการขัดจังหวะการทำงานของเครื่องโดยผู้ควบคุมการทำงานของเครื่องหรือไม่

8. รายงานการใช้เครื่อง รวมทั้งรายงานการใช้เครื่องที่พิมพ์โดยเครื่องคอมพิวเตอร์ ได้รับการตรวจสอบโดยเจ้าหน้าที่ในระดับรับผิดชอบหรือไม่

- ในกรณีที่การควบคุมภายในเฉพาะระบบงานต้องพึ่งพาการปฏิบัติงาน เพื่อทำหน้าที่นี้โดยพนักงานผู้ควบคุมการทำงานของเครื่อง การควบคุมในเรื่องนี้เป็นสิ่งสำคัญ

การควบคุมแฟ้มข้อมูล

9. มีการทำทะเบียนแฟ้มต่าง ๆ หรือไม่ ถ้ามีระบุ
10. มีการบันทึกการเคลื่อนไหวของแฟ้มหรือไม่ (การนำไปใช้ การส่งคืน) ถ้ามีระบุ
11. ใครมีอำนาจเบิกแฟ้มเหล่านี้มาใช้ได้บ้าง
12. แฟ้มที่สำคัญ ๆ (เช่น โปรแกรมคำสั่ง บันทึกเกี่ยวกับระบบ ฯลฯ) มีการเก็บสำรองไว้นอกสถานที่ด้วยหรือไม่

วิธีการในการระบุความแตกต่างของแฟ้มข้อมูล

13. มีวิธีการระบุความแตกต่างของแฟ้มต่าง ๆ อย่างพอเพียง โดย
    ก. มีรหัสอ้างอิงที่มองเห็นได้ง่าย
    ข. มีดัชนีปรากฏในส่วนบนของแฟ้ม ซึ่งสามารถตรวจสอบได้ว่าเป็นแฟ้มที่ถูกต้องในการนำมาใช้
    ค. ด้วยวิธีอื่น ๆ ระบุ

วิธีการในการสร้างแฟ้มข้อมูลใหม่

14. มีวิธีการที่เพียงพอในการสร้างแฟ้มข้อมูลใหม่ โดย
    ก. มีการกำหนดระยะเวลาที่จะต้องเก็บข้อมูลในแฟ้ม ในสื่อที่รับข้อมูลและเอกสาร
    ข. มีระบบการสร้างแฟ้มข้อมูล

ค. มีการคัดลอกข้อมูลในแฟ้มแม่เหล็กเป็นระยะๆที่เหมาะสม

ง. วิธีการอื่น ๆ ระบุ

มาตรการป้องกันไฟและมาตรการฉุกเฉิน

15. ก. มีการป้องกันไฟอย่างพอเพียงหรือไม่ ระบุ

ข. มีมาตรการสำหรับการประมวลผลในกรณีฉุกเฉินอย่างเพียงพอหรือไม่ หากการทำงานของเครื่องต้องหยุดชะงักลง ระบุ

ค. ในกรณีที่มีมาตรการเหล่านี้ ได้เคยมีการทดสอบมาตรการเหล่านี้บ้างหรือไม่

2. การควบคุมการพัฒนาระบบ

ข้อสังเกต 1. คำถามในส่วนนี้เกี่ยวกับระบบคอมพิวเตอร์เป็นส่วนรวม

2. ในการใช้ระบบคอมพิวเตอร์ มักจะมีการกำหนดมาตรฐานสำหรับการควบคุมและวิธีการในการพัฒนาระบบ ผู้สอบบัญชีควรจะสอบถามเกี่ยวกับเรื่องนี้ เพราะมิฉะนั้นจะกระทบกระเทือนถึงคุณภาพของการทำงาน ของระบบงานคอมพิวเตอร์โดยทั่วไป

วิธีการที่เป็นมาตรฐานและการบันทึกการพัฒนาระบบ

16. การบันทึกเกี่ยวกับระบบงานได้ครอบคลุมถึงสิ่งต่อไปนี้หรือไม่

ก. คำอธิบายเกี่ยวกับระบบ

ข. ผังระบบงาน

ค. คำอธิบายเกี่ยวกับข้อมูลนำเข้าและข้อมูลส่งออก

ง. รูปแบบของการบันทึกข้อมูลในแฟ้มต่างๆ

จ. วิธีการควบคุม

ฉ. รายละเอียดเกี่ยวกับโปรแกรมคำสั่ง

ช. ข้อมูลทดสอบและผลของการทดสอบ

ซ. คำสั่งเกี่ยวกับการแจกจ่ายข้อมูลส่งออก

ฌ. คำสั่งเกี่ยวกับการทำงานของเครื่อง

ฎ. คู่มือการปฏิบัติงาน

17. มีวิธีการเช่นใดที่จะทำให้มั่นใจว่าการบันทึกดังกล่าวข้างต้น

ก. ได้มีการจัดทำอย่างถูกต้อง

ข. ได้มีการเปลี่ยนแปลงเมื่อมีการเปลี่ยนแปลงในระบบและโปรแกรมคำสั่ง

การทดสอบระบบและโปรแกรมคำสั่ง

18. ได้มีการทดสอบโปรแกรมคำสั่งอย่างเพียงพอหรือไม่ โดย
    ก. การทดลองปฏิบัติการ
    ข. ทดลองการประมวลผลด้วยข้อมูลทดสอบ
    ค. การปฏิบัติงานตามคำสั่งในการทำงานของเครื่อง โดยผู้จัดทำโปรแกรมคำสั่งมิได้อยู่ในที่นั้น
    ง. ด้วยวิธีการอื่น ๆ ระบุ
19. ให้มีการทดสอบระบบอย่างเพียงพอหรือไม่ โดย
    ก. โดยการประมวลผลข้อมูลทดสอบ
    ข. โดยการทดลองปฏิบัติการ
    ค. โดยการปฏิบัติงานควบคู่กับระบบเดิม
    ง. มีการทดสอบวิธีการควบคุมต่าง ๆ ในแผนกผู้ใช้ข้อมูลทั้งหมดที่เกี่ยวข้องกับระบบ
    จ. วิธีอื่น ๆ ระบุ
20. ใครเป็นผู้ประเมินผลการทดสอบ และมีการทำรายงานอะไรบ้าง

การแปลงสภาพข้อมูล

21. มีการตรวจทานข้อมูลใน master file ก่อนที่จะมีการเริ่มใช้ระบบหรือไม่

วิธีการในการยอมรับและการอนุมัติระบบ

22. มีการตรวจทานงานพัฒนาระบบที่ได้ทำเสร็จไปแล้ว มีการให้ความเห็นชอบและอนุมัติให้ดำเนินการต่อไป โดยเจ้าหน้าที่ผู้รับผิดชอบ ทั้งจากแผนกผู้ใช้ข้อมูลและแผนกคอมพิวเตอร์ในขั้นตอนต่าง ๆ ของการพัฒนาระบบดังต่อไปนี้หรือไม่
    ก. เมื่อการทำรายงานเกี่ยวกับโครงร่างของระบบเสร็จสิ้นลง
    ข. เมื่อได้มีการกำหนดรายละเอียดต่าง ๆ ของระบบเสร็จสิ้นแล้ว
    ค. เมื่อได้มีการทดสอบโปรแกรมคำสั่งและระบบเรียบร้อยแล้ว
    ง. เมื่อมีการยอมรับระบบใหม่ให้นำมาดำเนินการได้

การเปลี่ยนแปลงระบบและโปรแกรมคำสั่ง

23. การเปลี่ยนแปลงในระบบการปฏิบัติงานและโปรแกรมคำสั่งต้องได้รับการอนุมัติหรือไม่
24. การเปลี่ยนแปลงทั้งหลายมีการ
    ก. จัดทำบันทึกเกี่ยวกับการเปลี่ยนแปลง
    ข. มีการทดสอบ

ค. ในลักษณะเดียวกันการนำระบบใหม่หรือโปรแกรมคำสั่งใหม่มาใช้หรือไม่

25. มีวิธีการเช่นใดที่จะทำให้มั่นใจว่ามีการแจ้งเกี่ยวกับการเปลี่ยนแปลงนี้ให้ทุกฝ่ายที่เกี่ยวข้อง รวมทั้งแผนกผู้ใช้ข้อมูลได้ทราบ

3. การควบคุมเฉพาะระบบงาน (Application control)

ข้อสังเกต 1. คำถามในส่วนนี้จะเกี่ยวข้องกับการประมวลผลในแต่ละระบบงาน

2. คำถามในส่วนนี้ควรจะใช้กับข้อมูลนำเข้า รายงาน และ master file ของแต่ละระบบงาน

ก. การควบคุมข้อมูลนำเข้า

การจัดให้มีการควบคุม

26. การควบคุมเพื่อให้มั่นใจว่าการประมวลผลสมบูรณ์และถูกต้องได้จัดให้มีในขั้นต้น

ก. ก่อนที่จะรวมเอกสารเข้าเป็น Batch โดยวิธีการดังนี้

(1) วิธีการควบคุมอื่นที่ทำไว้แล้ว - ระบุ

(2) โดยการตรวจการเรียงลำดับของเอกสารที่เกี่ยวข้องด้วยมือ

(3) โดยการเก็บสำเนาเอกสารไว้

(4) โดยวิธีอื่น ระบุ

ข. โดยการทำด้วยมือภายหลังที่รวมเอกสารเป็น Batch โดย

(1) วิธีการควบคุมด้วยยอดรวม ระบุ

(2) โดยวิธีอื่น ระบุ

ค. โดยคอมพิวเตอร์ โดย

(1) การควบคุมด้วยยอดรวม ระบุ

(2) โดยการตรวจสอบการเรียงลำดับของรหัส

(3) โดยวิธีอื่น ระบุ

ข้อสังเกต 1. คำถามข้อ 26 นี้จะใช้ได้กับข้อมูลในเอกสารที่เป็นข้อมูลเกี่ยวกับการเงิน เป็นสิ่งสำคัญที่จะต้องแยกระหว่างการควบคุมที่จะทำให้การประมวลผลสมบูรณ์ และการควบคุมที่จะทำให้การประมวลผลถูกต้อง

2. ในคำถาม 26 ข. เป็นสิ่งสำคัญที่จะต้องแยกว่าการควบคุมได้ทำในขั้นแรกใน แผนกผู้ใช้หรือแผนกคอมพิวเตอร์ ถ้าหากทำในขั้นแรกในแผนกคอมพิวเตอร์ การควบคุมในด้านการบริหารเป็นสิ่งสำคัญ

3. ถ้าการควบคุมในขั้นแรกกระทำโดยคอมพิวเตอร์ (ตามคำถาม 26 ค.) การควบคุมในการพัฒนาระบบและการบริหารเป็นสิ่งสำคัญ

27. มีการควบคุมเช่นใดบ้างในการตรวจสอบความถูกต้องของข้อมูลเพื่อการอ้างอิงที่สำคัญ (เช่น วิธีการตรวจทานความถูกต้องของรหัสโดยวิธี Check digit และการเปรียบเทียบกับข้อมูลใน master file)

การตรวจทานความถูกต้องในการแปลงสภาพ

28. ก. มีการตรวจทานความถูกต้องในการแปลงสภาพข้อมูลให้อยู่ในสื่อที่เครื่องสามารถรับรู้ได้ โดยบุคคลที่มิได้เกี่ยวข้องกับการแปลงสภาพนั้นหรือไม่
ข. มีวิธีอีกอย่างไรที่จะทำให้มั่นใจได้ว่า ความผิดพลาดทั้งหมดจะได้รับการแก้ไข

ข้อสังเกต ถ้าการควบคุมในขั้นแรกกระทำภายหลังที่ได้มีการแปลงสภาพข้อมูลแล้ว การควบคุมนี้สำคัญมาก

การอนุมัติข้อมูลนำเข้า

29. มีการอนุมัติข้อมูลนำเข้าอย่างพอเพียงหรือไม่

30. ถ้าหากมีการอนุมัติเอกสารก่อนที่จะมีการควบคุม มีการตรวจทานการอนุมัติอีกหรือไม่ภายหลังที่มีการควบคุมแล้ว (เพื่อมิให้มีการนำเอกสารที่มิได้มีการอนุมัติเข้ามาเพิ่ม)

31. มีการใช้โปรแกรมคำสั่งเพื่อให้เครื่องทำหน้าที่อนุมัติรายการที่สำคัญหรือไม่ (เช่น จัดให้มีการตรวจข้อจำกัดหรือความเหมาะสมของรายการโดยเครื่อง)

ข้อสังเกต ถ้ามีการกำหนดให้เครื่องคอมพิวเตอร์ทำหน้าที่อนุมัติข้อมูลได้ การควบคุมเกี่ยวกับการพัฒนาระบบและการบริหารเป็นสิ่งสำคัญ

ข. การควบคุมการประมวลผล

การปฏิเสธไม่ยอมรับข้อมูลนำเข้า

32. ขอรายละเอียดเกี่ยวกับเหตุผลที่ข้อมูลอาจจะถูกปฏิเสธไม่ยอมรับเข้าประมวลผลโดยเครื่อง

33. วิธีการในการสอบสวนข้อผิดพลาด แก้ไขข้อผิดพลาด และส่งข้อมูลกลับเข้าไปประมวลผลใหม่ ตลอดรายการบันทึกเหตุการณ์ดังกล่าวมีเช่นใด

34. มีวิธีการเช่นใดที่จะทำให้มั่นใจว่ารายการที่เครื่องปฏิเสธไม่รับเข้าประมวลผลนี้ได้มีการแก้ไข และนำกลับเข้าสู่การประมวลผลใหม่อย่างทันท่วงที (เช่น โดยการทำบันทึกเกี่ยวกับรายการค้างเหล่านี้ และการตรวจทานบันทึกนี้โดยหน่วยงานอิสระ)

ข้อสังเกต คำถามในลักษณะเดียวกันนี้อาจจะใช้คำถามเกี่ยวกับรายการที่ค้างอยู่ใน suspense file

การพิมพ์ข้อมูลเพื่อการควบคุมในระหว่างการประมวลผล

35. ก. ถ้ามีการควบคุมก่อนการประมวลผล (ตามคำถามข้อ 26 ก-ค) มีการใช้วิธีการควบคุมนี้เพื่อตรวจทานความถูกต้องของข้อมูลส่งออกทางการบัญชีหรือไม่ ระบุ
    ข. หากไม่มีการใช้การควบคุมดังกล่าวเพื่อตรวจทานการประมวลผลจนถึงบางขั้นตอนหรือไม่ โดยตรวจทานกับผลการประมวลข้อมูลเมื่อเสร็จการประมวลในแต่ละขั้น ระบุ

36. ถ้ามีการควบคุมโดยคอมพิวเตอร์เพื่อตรวจสอบข้อมูลส่งออกกับข้อมูลนำเข้าหรือกับผลการประมวล-ข้อมูลในขั้นตอนอื่น
    ก. มีการพิมพ์ผลการประมวลข้อมูลในระหว่างทำการประมวลข้อมูลเพื่อนำไปตรวจทานกับข้อมูลส่งออก เมื่อการประมวลข้อมูลเสร็จสิ้นลงหรือไม่ ระบุ
    ข. ถ้ามีการปฏิบัติดังกล่าวในข้อ ก. มีการควบคุมอย่างเพียงพอโดยโปรแกรมคำสั่ง อันจะทำให้มั่นใจถึงความสมบูรณ์และความถูกต้องของข้อมูลในแต่ละขั้นตอนของการประมวลผลหรือไม่ ระบุ

ข้อสังเกต หากต้องการให้ได้รับความมั่นใจจากการควบคุมโดยโปรแกรมคำสั่ง การควบคุมในการพัฒนาระบบและการควบคุมทางด้านบริหารเป็นสิ่งสำคัญ

ค. การควบคุมข้อมูลส่งออก

ข้อความทั่วไป

37. รายงานที่พิมพ์ออกมานั้นมีจุดประสงค์เพื่อนำไปใช้ในทางใดบ้าง (เช่น เพื่อก่อให้เกิดรายการหรือเพื่อสนับสนุนรายการในบัญชีเพื่อวัตถุประสงค์ในการควบคุม)
38. ในรายงานที่พิมพ์ออกมานั้นมีข้อมูลเพียงพอเพื่อกระทำการดังต่อไปนี้หรือไม่
    ก. ติดตามจากเอกสารแหล่งข้อมูลมายังรายงาน
    ข. ตรวจทานการคำนวณและยอดรวมที่คำนวณโดยเครื่องคอมพิวเตอร์

ข้อสังเกต คำถามนี้มีจุดประสงค์ที่จะดูว่ามี audit trail หรือไม่ แม้ว่าการไม่มี audit trail จะมิได้เป็นเครื่องบ่งชี้ว่ามีจุดอ่อนในการควบคุมภายในก็ตาม

ข้อมูลส่งออกที่มีความสัมพันธ์โดยตรงกับข้อมูลนำเข้า

39. ก. มีการตรวจทานยอดรวมและรายละเอียดของข้อมูลส่งออกด้วยมือกับยอดที่ใช้ในการควบคุม ซึ่งได้จัดทำขึ้นก่อนการประมวลผล หรือกับยอดที่ได้ในระหว่างการประมวลผลหรือไม่

ข. ถ้าไม่มีการกระทำดังกล่าวในข้อ ก. มีการควบคุมโดยโปรแกรมคำสั่งอย่างเพียงพอ เพื่อให้มั่นใจในความสมบูรณ์และความถูกต้องของข้อมูลส่งออกในรายงานต่าง ๆ หรือไม่ ระบุ

ข้อมูลส่งออกที่ไม่มีความสัมพันธ์กับข้อมูลนำเข้าโดยตรง

40. ก. มีการตรวจทานยอดรวมและรายละเอียดของข้อมูลส่งออกด้วยมือกับข้อมูลอื่น ๆ จากภายนอกหรือไม่ ระบุ

ข. ถ้าไม่มีการตรวจทานดังกล่าวในข้อ ก. มีการควบคุมโดยโปรแกรมคำสั่งอย่างเพียงพอ เพื่อให้มั่นใจในความสมบูรณ์และความถูกต้องของข้อมูลส่งออกในรายงานต่าง ๆ หรือไม่ ระบุ

รายงานรายการผิดปกติต่างๆ

41. มีการตรวจทานรายงานนี้ด้วยมือว่าครบถ้วนหรือไม่ ถ้ามีระบุรายละเอียด

42. มีการควบคุมโดยโปรแกรมคำสั่งอย่างเพียงพอ เพื่อให้มั่นใจในความสมบูรณ์ (ในกรณีที่เหมาะสม) และความถูกต้องของข้อมูลในรายงานหรือไม่

43. วิธีการในการสอบสวนและดำเนินการเกี่ยวกับข้อผิดพลาดและการบันทึกการดำเนินการดังกล่าวมีเช่นใด

การแจกจ่ายข้อมูลส่งออก

44. ถ้าหากการได้รับข้อมูลส่งออกมิได้มีการควบคุมโดยแผนกผู้ใช้ข้อมูล มีวิธีการเช่นใดบ้างในระบบที่จะทำให้มั่นใจได้ว่าแผนกผู้ใช้ข้อมูลได้รับรายงานทั้งหมดโดยไม่ขาดตกบกพร่อง

ข้อสังเกต

1. ในคำถามข้อ 39 ก. และ 40 ก. เป็นสิ่งสำคัญที่จะต้องแยกระหว่างการตรวจทานที่กระทำในแผนกผู้ใช้ข้อมูล และที่ทำในแผนกคอมพิวเตอร์ ถ้าการตรวจทานนี้กระทำภายในแผนกคอมพิวเตอร์ การควบคุม ภายในทางด้านบริหารเป็นสิ่งสำคัญ
2. ถ้าจะให้ความเชื่อมั่นในการควบคุมโดยโปรแกรมคำสั่ง (ตามคำถาม 39 ข. 40 ข. และ 42) การควบคุมในด้านการพัฒนาระบบและการควบคุมทางด้านการบริหารเป็นสิ่งสำคัญ

ง. การควบคุมเกี่ยวกับ Master File

การเปลี่ยนแปลงข้อมูลที่มีลักษณะถาวร

45. ก. วิธีการในการอนุมัติการเปลี่ยนแปลงมีเช่นใด
    ข. การอนุมัติเพียงพอหรือไม่

46. ขั้นตอนต่าง ๆ ในการเปลี่ยนแปลงข้อมูลมีการตรวจทานอย่างละเอียดหรือไม่ ด้วยวิธีใด

47. มีวิธีการในระบบอย่างไรที่จะให้มั่นใจได้ว่า ได้มีการเปลี่ยนแปลงข้อมูลที่มีลักษณะถาวรอย่างครบถ้วน
    ก. โดยการควบคุมยอดรวม
    ข. โดยการเก็บสำเนาเอกสารเป็นหลักฐาน
    ค. โดยวิธีการอื่น ระบุ

การเก็บรักษาข้อมูลที่มีลักษณะถาวร

48. มีการตรวจสอบข้อมูลเหล่านี้อย่างไร บ่อยเพียงไร
    ก. โดยการพิมพ์รายละเอียดเพื่อตรวจสอบกับข้อมูลภายนอก
    ข. โดยการพิมพ์ยอดรวมเพื่อกระทบกับยอดรวมที่ทำโดยบุคคลอื่นอย่างเป็นอิสระ หรือกระทบกับยอดรวมที่เครื่องทำออกมา
    ค. โดยการกระทบยอดรวมโดยคอมพิวเตอร์
    ง. โดยวิธีการอื่น ระบุ

การเก็บรักษาข้อมูลรายการ

49. มีการตรวจทานยอดรวมข้อมูลรายการในแฟ้มอย่างไร บ่อยเพียงใด
    ก. โดยการพิมพ์ยอดรวมเพื่อกระทบกับยอดรวมที่ทำขึ้นโดยบุคคลอื่นอย่างเป็นอิสระ หรือกับยอดรวมของคอมพิวเตอร์
    ข. โดยการกระทบยอดรวมโดยคอมพิวเตอร์
    ค. โดยวิธีการอื่น ๆ ระบุ

50. มีการพิมพ์ยอดคงเหลือของรายการต่าง ๆ และตรวจทานกับข้อมูลข้างนอกหน่วยงานคอมพิวเตอร์หรือไม่ ระบุ

28

แนวการตรวจสอบการดำเนินงานและการควบคุมภายในด้านคอมพิวเตอร์ในภาคปฏิบัติ

(เป็นการตรวจสอบด้าน General Controls ของคอมพิวเตอร์โดยรวม)

แนวการตรวจสอบการดำเนินงานและการควบคุมภายในด้านคอมพิวเตอร์

(Data center) ในภาคปฏิบัติ

(ตามมาตรฐานการดำเนินงานด้านคอมพิวเตอร์)

ได้อธิบายจุดอ่อนหรือข้อบกพร่อง ตลอดจนการดำเนินงานด้านคอมพิวเตอร์ที่ไม่เหมาะสม และอาจก่อให้เกิดความเสียหายต่อสถาบันการเงิน พร้อมทั้งการปรับปรุงแก้ไขอันควรไว้ในข้อสังเกตของผู้ตรวจสอบ

การตรวจสอบภายในและการตรวจสอบของผู้สอบบัญชี

การตรวจสอบภายใน	*มีข้อสังเกต
1. สถาบันการเงินมอบอำนาจให้ผู้ตรวจสอบภายใน (1) เพียงพอที่จะทำให้งานตรวจสอบมีประสิทธิภาพ (2) สามารถกำหนดวิธีการควบคุมภายใน และจัดให้มีข้อมูลสำหรับใช้เป็นหลักฐานในการควบคุมและตรวจสอบได้อย่างเพียงพอทุกระบบงาน 2. มีการจัดสรรงบประมาณสำหรับการตรวจสอบคอมพิวเตอร์ 3. คณะกรรมการสถาบันการเงิน (1) เป็นผู้พิจารณาแผนงานและเป้าหมายการตรวจสอบประจำปี (2) ติดตามผลการปฏิบัติงานของผู้ตรวจสอบภายใน โดยเปรียบเทียบผลการปฏิบัติงานจริงกับแผนงานและเป้าหมายการตรวจสอบประจำปี (3) เป็นผู้พิจารณาหลักเกณฑ์ที่ใช้ในการคัดเลือกงานตรวจสอบ (4) รับทราบผลการตรวจสอบคอมพิวเตอร์ 4. ผู้ตรวจสอบภายใน (1) เข้าร่วมประชุมพิจารณาจัดหาเครื่องคอมพิวเตอร์ และ/หรือระบบงานและโปรแกรม (2) เข้าร่วมพัฒนาระบบงานและโปรแกรม (3) มีหน้าที่เสนอรายงานการตรวจสอบผ่านคณะกรรมการธนาคาร	

การตรวจสอบภายใน	*มีข้อสังเกต
5. มีระเบียบให้หน่วยงานที่มีส่วนเกี่ยวข้องกับการใช้คอมพิวเตอร์มีหน้าที่แจ้งปัญหาการปฏิบัติงานให้ผู้ตรวจสอบภายในทราบ 6. มีระเบียบปฏิบัติกรณีหน่วยงานที่ถูกตรวจสอบมีข้อโต้แย้งและไม่ปรับปรุงแก้ไขข้อบกพร่องตามคำแนะนำของผู้ตรวจสอบภายใน 7. มีระเบียบกำหนดวิธีการยุติปัญหากรณีหน่วยงานที่ถูกตรวจสอบมีข้อโต้แย้งผู้ตรวจ-สอบภายใน 8. มีนโยบายไม่ต้องการให้ผู้ตรวจสอบภายในปฏิบัติงานในกิจกรรมที่อาจมีการตรวจ-สอบ 9. การปฏิบัติงานของผู้ตรวจสอบภายในอยู่ภายใต้การควบคุมดูแลของคณะกรรมการสถาบันการเงินโดยตรง 10. มีการกำหนดคุณสมบัติของผู้ตรวจสอบภายในด้านคอมพิวเตอร์ 11. ผู้ตรวจสอบภายใน (1) มีวุฒิการศึกษาตามคุณสมบัติที่กำหนด (2) มีประสบการณ์ตามคุณสมบัติที่กำหนด 12. มีโครงการให้การศึกษาแก่ผู้ตรวจสอบภายในทางด้าน (1) ปรัชญาการตรวจสอบและเทคนิคการตรวจสอบ (2) การเขียนโปรแกรม การออกแบบระบบงาน และการบริหารโครงการ (3) การปฏิบัติงานในห้องคอมพิวเตอร์และการสื่อสารข้อมูล (4) เทคนิคอื่น ๆ 13. มีการจัดหลักสูตรการบังคับบัญชาหรือหลักสูตรการบริหารงานสำหรับผู้ตรวจสอบภายในระดับต่าง ๆ 14. ในการจัดแผนงานตรวจสอบประจำปี ผู้ตรวจสอบภายในคำนึงถึงกิจกรรมที่เกี่ยวข้องกับงานคอมพิวเตอร์ทุกด้าน 15. ผู้ตรวจสอบภายในสามารถปฏิบัติงานได้ตามเป้าหมายที่กำหนดไว้ทุกปี	

การตรวจสอบภายใน	*มีข้อสังเกต
16. ผู้ตรวจสอบภายใน (1) ได้รับการบรรจุครบทุกตำแหน่ง (2) อัตราหมุนเวียนเข้า-ออกน้อยอยู่ในระดับปกติ (3) มีพนักงานชั้นบริหารเพียงพอที่จะทำงานทดแทนกันได้ 17. มีหลักเกณฑ์ที่ใช้ในการคัดเลือกงานตรวจสอบ หรือมีการวิเคราะห์ความเสี่ยงภัย เพื่อใช้พิจารณารอบระยะเวลาในการตรวจสอบคอมพิวเตอร์แต่ละด้าน 18. หลักเกณฑ์ที่ใช้ในการคัดเลือกงานตรวจสอบ ช่วยทำให้รอบระยะเวลาการตรวจสอบงานที่สำคัญมีความเหมาะสม 19. แผนการตรวจสอบประจำปีสอดคล้องกับหลักเกณฑ์ที่ใช้ในการคัดเลือกงานตรวจสอบ 20. คู่มือตรวจสอบ (1) มีรูปแบบของรายงานการตรวจสอบแสดงไว้เป็นตัวอย่าง (2) อธิบายขอบเขตการตรวจสอบ (3) มีข้อสังเกตและคำแนะนำของผู้ตรวจสอบภายในแสดงไว้เป็นแนวทาง (4) รวบรวมจุดอ่อน สาเหตุที่เกิดข้อผิดพลาด และวิธีแก้ไขข้อผิดพลาด แสดงไว้โดยละเอียด 21. ระเบียบการติดตามผลการตรวจสอบ (1) มีการกำหนดระยะเวลาให้หน่วยงานที่ถูกตรวจสอบตอบชี้แจง (2) มีหลักเกณฑ์ในการกำหนดระยะเวลาการตรวจสอบเพื่อติดตามผล 22. คู่มือจัดทำกระดาษทำการอธิบาย (1) วิธีจัดทำเอกสารหลักฐานและการจัดเก็บเอกสารเข้าแฟ้มเพื่อความสะดวกในการค้นหา (2) วัตถุประสงค์การตรวจสอบ (3) ขอบเขตการตรวจสอบ (4) รายละเอียดของงานที่จะตรวจสอบ รวมทั้งระเบียบการปฏิบัติงานและวิธีการควบคุมภายในที่ใช้ในงานที่จะตรวจสอบ (5) วิธีทบทวนกระดาษทำการเก่าที่เกี่ยวข้องกับคำแนะนำหรือข้อสังเกตในการตรวจสอบครั้งก่อน	

การตรวจสอบภายใน	*มีข้อสังเกต
(6) การปฏิบัติตามนโยบายและการปฏิบัติตามระเบียบของสถาบันการเงิน 23. คู่มือตรวจสอบอธิบาย (1) วิธีตรวจสอบการปฏิบัติงานคอมพิวเตอร์ (2) วิธีตรวจสอบระบบงานคอมพิวเตอร์ทุกงาน (3) วิธีพิจารณาระบบงานใหม่ก่อนอนุมัติให้นำออกใช้ประมวลผลข้อมูลจริง 24. มีระเบียบปฏิบัติในการประเมินผลระบบงานคอมพิวเตอร์ชุดใหม่หลังจากที่ได้นำออกใช้งานจริงแล้ว 25. ระเบียบการใช้โปรแกรมตรวจสอบ (1) กำหนดให้มีเอกสารประกอบการใช้โปรแกรมอย่างเพียงพอ (2) ให้ใช้โปรแกรมตรวจสอบงานที่มีความสำคัญทุกประเภท (3) กำหนดให้มีการสอบยันข้อมูล (4) กำหนดให้มีการรวมยอดรายการในแฟ้มข้อมูล (5) กำหนดให้มีการสอบทานการคำนวณและการบวกสะสมยอดข้อมูล 26. มีระเบียบการพัฒนาโปรแกรมตรวจสอบหรือจัดหาโปรแกรมตรวจสอบ 27. มีระเบียบการรักษาความปลอดภัย (1) กระดาษทำการ (2) รายงานการตรวจสอบ (3) หนังสือตอบชี้แจง (4) เอกสารระบบงานและโปรแกรม 28. มีการตรวจสอบเป็นครั้งคราวเกี่ยวกับ (1) การกระทบยอดข้อมูล (2) การเตรียมข้อมูล (3) การ Proof รายการเงินโอนและการเรียกเก็บเงินโอน (4) การปฏิบัติงานคอมพิวเตอร์ (5) ระบบงานและโปรแกรม (6) การประมวลผลที่อาศัยระบบสื่อสารในการรับส่งข้อมูลจากที่อื่นซึ่งอยู่ห่างไกลจากศูนย์คอมพิวเตอร์	

การตรวจสอบภายใน	*มีข้อสังเกต
(7) โปรแกรมที่ใช้กับงานที่มีความสำคัญ (8) เอกสารระบบงานและโปรแกรม (9) การควบคุมภายในหน่วยงานผู้ใช้ข้อมูล 29. วิธีการที่สถาบันการเงินใช้ตรวจสอบ ช่วยให้ทราบถึงความเหมาะสมในการแบ่งแยกหน้าที่การปฏิบัติงานเตรียมข้อมูล การปรับปรุงแก้ไขข้อมูลขั้นต้นที่ผิดพลาด และการตรวจสอบความถูกต้องของยอดรวมข้อมูลในรายงานคอมพิวเตอร์ 30. วิธีการตรวจสอบการเตรียมข้อมูล ครอบคลุมในเรื่อง (1) การคุมยอดข้อมูลทางการเงินและการคุมยอดข้อมูลที่ไม่ได้เป็นรายการทางการเงิน (2) การสอบทานความถูกต้องของข้อมูล (3) การปรับปรุงแก้ไขรายการที่มีข้อผิดพลาดให้เป็นไปตามขั้นตอนที่กำหนดไว้ (4) การจัดทำคู่มือปฏิบัติงานเตรียมข้อมูล และการปรับปรุงแก้ไขคู่มือดังกล่าวให้ทันต่อเวลาอยู่เสมอ 31. วิธีการตรวจสอบการจัดส่งรายงานคอมพิวเตอร์ให้ผู้ใช้ข้อมูลครอบคลุมในเรื่อง (1) การคุมยอดข้อมูลและการกระทบยอดข้อมูลเพื่อตรวจสอบความถูกต้องก่อนจัดส่งรายงานคอมพิวเตอร์ให้ผู้ใช้ข้อมูล (2) ระเบียบการจัดส่งรายงานคอมพิวเตอร์ให้ผู้ใช้ข้อมูล (3) การกำหนดมาตรการควบคุมข้อมูลที่มีความสำคัญให้มีความรัดกุมอย่างเพียงพอ 32. วิธีการตรวจสอบการปฏิบัติงานคอมพิวเตอร์ ครอบคลุมในเรื่อง (1) ระเบียบการปฏิบัติงานคอมพิวเตอร์และการปฏิบัติตามระเบียบดังกล่าว (2) รายงานต่าง ๆ ฝ่ายบริหารใช้เป็นเครื่องมือในการติดตามผลการปฏิบัติงานและการควบคุมดูแลการปฏิบัติงานคอมพิวเตอร์ รวมทั้งผลการใช้รายงานดังกล่าว (3) การบำรุงรักษาเครื่องคอมพิวเตอร์ สัญญาซ่อมบำรุงเครื่องคอมพิวเตอร์และทะเบียนบันทึกปัญหาการใช้เครื่องคอมพิวเตอร์ (4) การรักษาความปลอดภัยและการควบคุมการใช้เครื่องคอมพิวเตอร์ (5) การรักษาความปลอดภัยและการควบคุมการใช้แฟ้มข้อมูล รวมทั้งโปรแกรมที่ใช้ประมวลผลข้อมูล	

การตรวจสอบภายใน	*มีข้อสังเกต
(6) แผนฉุกเฉิน (7) วิธีการปรับปรุงแก้ไขระบบที่ได้รับความเสียหายให้กลับคืนสู่สภาพปกติ สามารถปฏิบัติงานได้ต่อไป และการจัดเตรียมเครื่องคอมพิวเตอร์ชุดสำรองไว้ใช้ทดแทนเมื่อเกิดเหตุฉุกเฉิน (8) การประกันภัยคอมพิวเตอร์ (9) การจัดองค์การและการแบ่งแยกหน้าที่การปฏิบัติงานคอมพิวเตอร์ (10) การปรับปรุงแก้ไขคู่มือปฏิบัติงานคอมพิวเตอร์ให้สมบูรณ์และทันต่อเวลาอยู่เสมอ 33. วิธีการตรวจสอบที่ใช้เฉพาะระบบงานคอมพิวเตอร์แต่ละระบบ ครอบคลุมในเรื่อง (1) ข้อมูลสำหรับใช้เป็นหลักฐานในการควบคุมและตรวจสอบ และเครื่องมือที่ใช้ในการควบคุมภายใน (2) เอกสารสนับสนุนการปฏิบัติงาน (3) การปฏิบัติตามระเบียบในการจัดทำโปรแกรมสำหรับกรณีที่เป็นระบบงานใหม่ วิธีการตรวจสอบดังกล่าวครอบคลุมในเรื่อง (4) การปฏิบัติตามวัตถุประสงค์ในการออกแบบระบบงาน (5) การรายงานสถานะความก้าวหน้าของโครงการต่อฝ่ายบริหารของธนาคาร เพื่อขอความเห็นชอบ เมื่อได้ดำเนินการพัฒนาระบบงานได้ตามเป้าหมายที่กำหนดไว้ในแต่ละขั้นตอน (6) แผนการทดสอบและการสรุปผลการทดสอบระบบงานใหม่ 34. วิธีการตรวจสอบระบบงานและโปรแกรม ครอบคลุมในเรื่อง (1) ระเบียบการจัดทำโปรแกรม และการปฏิบัติตามระเบียบของสถาบันการเงิน (2) การควบคุมการใช้ Utility program ที่ใช้ในการแก้ไขแฟ้มข้อมูลและ/หรือโปรแกรม (3) การรักษาความปลอดภัยและการควบคุมการใช้เอกสาร Operating system และเอกสารระบบงานคอมพิวเตอร์ (4) การควบคุมการปรับปรุงแก้ไข Operating system และโปรแกรมระบบงานคอมพิวเตอร์ (5) การจัดองค์การและการแบ่งแยกหน้าที่การปฏิบัติงานด้านระบบงานและโปรแกรม	

การตรวจสอบภายใน	*มีข้อสังเกต
35. วิธีการตรวจสอบการประมวลผลที่อาศัยระบบสื่อสารในการรับส่งข้อมูลจากที่อื่นซึ่งอยู่ห่างไกลจากศูนย์คอมพิวเตอร์ ครอบคลุมในเรื่อง (1) การจำกัดขอบเขตการใช้ระบบ เช่น จัดให้มีการใช้รหัสประจำตัว (Identification code) และ/หรือรหัสขอผ่านเข้าไปใช้ระบบ (Password) (2) การรักษาความปลอดภัยเกี่ยวกับรหัสดังกล่าว (3) การบันทึกข่าวสารมีการรับ-ส่งผ่านเครื่อง Terminal ทุกรายการลงในแฟ้มข้อมูลชุดที่เป็น Transaction file (4) การตรวจสอบและการติดตามพฤติการณ์ของผู้ที่พยายามเข้าไปใช้ระบบโดยไม่ชอบ (5) ความเพียงพอของรายละเอียดการปฏิบัติงานประมวลผลที่แสดงไว้ในคู่มือปฏิบัติงานสำหรับผู้ใช้ข้อมูล (6) การจัดเตรียมวิธีปฏิบัติงานประมวลผลข้อมูลแบบอื่นไว้ทดแทน 36. ผู้ตรวจสอบภายใน (1) ดำเนินการสอบทานการแก้ไขโปรแกรมที่มีความสำคัญก่อนนำไปใช้งาน (2) มีความเป็นอิสระในการตรวจสอบงานที่ใช้คอมพิวเตอร์ประมวลผลข้อมูลมีผลกระทบต่อบัญชีแยกประเภท ซึ่งเป็นบัญชีคุมอย่างน้อยปีละครั้ง (3) เป็นผู้เสนอแนะให้มีการเปลี่ยนแปลงวิธีการควบคุมที่มีความสำคัญต่องานที่ใช้คอมพิวเตอร์ 37. กรณีที่มีการให้บริการประมวลผลข้อมูลแก่ผู้อื่น มีการตรวจสอบ (1) สัญญาหรือข้อตกลงในการให้บริการแก่ลูกค้าหรือผู้ใช้ข้อมูล (2) การออกใบเสร็จรับเงินและการเรียกเก็บเงินค่าบริการจากลูกค้าหรือผู้ใช้ข้อมูล 38. กรณีใช้โปรแกรมตรวจสอบ (1) มีการสอบทานโปรแกรมตรวจสอบที่ผู้ตรวจสอบภายในไม่ได้พัฒนาด้วยตนเอง โดยผู้ตรวจสอบภายในที่มีความรู้ความชำนาญงานด้านนี้ (2) ผู้ขายโปรแกรมตรวจสอบให้ความสนับสนุนและให้ความช่วยเหลืออย่างเพียงพอ (3) มีการควบคุมการแก้ไขโปรแกรมตรวจสอบที่รัดกุมและเพียงพอ (4) โปรแกรมที่ใช้ตรวจสอบเหมาะสมกับขนาดความสลับซับซ้อนของงานและมีประสิทธิภาพในการให้ข้อมูลที่เป็นประโยชน์ต่อการตรวจสอบ	

การตรวจสอบภายใน	*มีข้อสังเกต
(5) มีเอกสารสนับสนุนการใช้โปรแกรมตรวจสอบอย่างเพียงพอ (6) ผู้ตรวจสอบภายในติดตามดูแลให้หน่วยงานที่มีหน้าที่พัฒนาระบบงานและโปรแกรม จัดทำเอกสารให้ครบถ้วนตามระเบียบของสถาบันการเงิน (7) มีการจัดเก็บโปรแกรมตรวจสอบและเอกสารประกอบชุดสำรองไว้ในที่ปลอดภัยภายนอกอาคารที่ตั้งหน่วยงานคอมพิวเตอร์ และมีการควบคุมที่รัดกุม 39. รายงานการตรวจสอบของผู้ตรวจสอบภายใน (1) มีรูปแบบตามมาตรฐานที่กำหนดไว้ในคู่มือตรวจสอบ (2) สมเหตุผลมีประสิทธิภาพ และทำความเข้าใจได้ (3) แสดงวัตถุประสงค์การตรวจสอบและขอบเขตการตรวจสอบโดยละเอียด (4) มีข้อสังเกตในการตรวจสอบและข้อแนะนำในการปรับปรุงแก้ไขข้อบกพร่อง (5) สามารถสื่อความหมายในเรื่องที่มีความสำคัญได้ 40. พนักงานชั้นบริหารของหน่วยงานที่ถูกตรวจสอบ (1) ตอบชี้แจงข้อสังเกตของผู้ตรวจสอบภายใน (2) ตอบชี้แจงภายในเวลาที่เหมาะสม (3) ตอบชี้แจงตรงประเด็นกับรายงานการตรวจสอบ 41. ผู้ตรวจสอบภายใน (1) ทบทวนหนังสือตอบชี้แจงของหน่วยงานที่ถูกตรวจสอบเพื่อยุติเรื่องอย่างเหมาะสม (2) ดำเนินการตรวจสอบเพื่อติดตามผลการปรับปรุงแก้ไขข้อบกพร่อง 42. ข้อบกพร่องที่สำคัญตามที่ปรากฏในรายงานการตรวจสอบได้รับการปรับปรุงแก้ไขจนเป็นพอใจของผู้ตรวจสอบภายใน 43. วัตถุประสงค์ของการตรวจสอบสมเหตุผลและเพียงพอ 44. กระดาษทำการที่ใช้ตรวจสอบการพัฒนาระบบงานและโปรแกรม และ/หรือ กระดาษทำการใช้ตรวจสอบเฉพาะระบบงาน มีรายละเอียดเกี่ยวกับ (1) การปฏิบัติงานตามโครงการได้สำเร็จตามเป้าหมายที่กำหนดไว้ (2) การจัดทำโปรแกรมที่ตรวจสอบให้สอดคล้องกับระเบียบของสถาบันการเงิน	

การตรวจสอบภายใน	*มีข้อสังเกต
(3) ข้อมูลสำหรับใช้เป็นหลักฐานในการควบคุมและตรวจสอบ และวิธีการควบคุมภายใน (4) แผนการทดสอบระบบงานและโปรแกรม (5) ผลการทดสอบระบบงานและโปรแกรม (6) ความเพียงพอของเอกสารสนับสนุนการปฏิบัติงาน (7) การสอบทานการแก้ไขโปรแกรม 45. รูปแบบของกระดาษทำการอำนวยความสะดวกในการค้นหาและใช้อ้างอิง 46. รายงานการตรวจสอบ กระดาษทำการ และรายงานการติดตามผลการตรวจสอบ (1) สอดคล้องกับระเบียบการตรวจสอบภายใน (2) มีการรักษาความปลอดภัยอย่างเพียงพอ 47. รายงานการตรวจสอบของผู้สอบบัญชี (1) แสดงขอบเขตการตรวจสอบและวัตถุประสงค์การตรวจสอบ (2) มีข้อสังเกตในการตรวจสอบ (3) มีข้อแนะนำในการปรับปรุงแก้ไขข้อบกพร่อง 48. ขอบเขตการตรวจสอบของผู้สอบบัญชีครอบคลุมในเรื่อง (1) การจัดองค์การและแผนงานคอมพิวเตอร์ (2) ระบบงานและโปรแกรม (3) การปฏิบัติงานคอมพิวเตอร์ (4) การรักษาความปลอดภัย (5) การควบคุมข้อมูลนำเข้า การควบคุมการประมวลผล และการควบคุมข้อมูลที่ได้จากการประมวลผล (6) การสื่อสารข้อมูล (7) การให้บริการประมวลผลข้อมูลแก่บุคคลอื่น (8) การปฏิบัติงานของผู้ตรวจสอบภายใน	

การจัดการ

การจัดการ	*มีข้อสังเกต
1. ผังการจัดองค์การของหน่วยงานคอมพิวเตอร์เหมาะสมกับโครงสร้างในการรายงานผลการปฏิบัติงาน 2. หัวหน้าหน่วยงานคอมพิวเตอร์รายงานผลการปฏิบัติงานโดยตรงต่อพนักงานชั้นบริหารระดับสูงของสถาบันการเงิน 3. ผังการจัดองค์การของหน่วยงานคอมพิวเตอร์ช่วยให้การแบ่งแยกหน้าที่การปฏิบัติงานมีความเหมาะสม 4. มีการกำหนดคุณสมบัติของพนักงานด้านคอมพิวเตอร์และพนักงานที่ดำรงตำแหน่งที่มีความสำคัญต่อการดำเนินงานประมวลผลข้อมูลมีคุณสมบัติครบถ้วนตามที่กำหนดไว้ 5. มีแผนให้การศึกษาต่อเนื่องแก่พนักงานของหน่วยงานคอมพิวเตอร์ทางด้าน (1) วิชาการคอมพิวเตอร์ (2) การบริหารงาน 6. มีพนักงานที่มีประสบการณ์และผ่านการฝึกอบรมในหลักสูตรต่าง ๆ เพียงพอที่จะบริหารงานคอมพิวเตอร์ทดแทนกันได้ 7. ผู้บริหารระดับสูงของธนาคารได้กำหนดบทบาทด้านคอมพิวเตอร์ไว้ในนโยบายการบริหารงานโดยทั่วไปของสถาบันการเงิน 8. ผู้บริหารระดับสูงของธนาคารหรือคณะกรรมการชุดต่าง ๆ ที่มีหน้าที่เกี่ยวข้องกับงานคอมพิวเตอร์ เป็นผู้พิจารณาและให้ความเห็นชอบในเรื่อง (1) นโยบายการใช้คอมพิวเตอร์ (2) การจัดสรรทรัพยากรให้แก่โครงการต่าง ๆ (3) มาตรการที่ใช้ในการรักษาความปลอดภัยและการควบคุมภายใน (4) การวิจัยและการศึกษาเพื่อพัฒนางานคอมพิวเตอร์ (5) งบประมาณคอมพิวเตอร์ (6) การจัดลำดับความสำคัญในการใช้คอมพิวเตอร์	

การจัดการ	*มีข้อสังเกต
(7) การเปลี่ยนแปลงระบบงาน การจัดองค์การ และเครื่องจักรหรืออุปกรณ์คอมพิวเตอร์ (8) สถานะของโครงการและผลการดำเนินงานตามเป้าหมายที่กำหนดไว้ (9) แผนงานคอมพิวเตอร์ในระยะยาว 9. ค่าใช้จ่ายด้านคอมพิวเตอร์ในงวดงบประมาณที่แล้วไม่เกินงบประมาณ 10. ผู้ตรวจสอบภายในได้ให้คำแนะนำเกี่ยวกับการควบคุมภายในและมีข้อสังเกตในการตรวจสอบ 11. หน่วยงานผู้ใช้ข้อมูลมีส่วนร่วมในการพิจารณาใช้คอมพิวเตอร์ 12. มีการจดบันทึกรายงานการประชุมของฝ่ายบริหาร หรือมีบันทึกช่วยจำเกี่ยวกับการพิจารณาตัดสินใจตามนโยบายที่กำหนดไว้โดยละเอียดและเพียงพอ 13. มีการกำหนดนโยบายบริหารบุคคลไว้เป็นลายลักษณ์อักษร 14. นโยบายดังกล่าวมีรายละเอียดเกี่ยวกับตำแหน่งงานและความรับผิดชอบของพนักงานในหน่วยงานคอมพิวเตอร์ 15. พนักงานของหน่วยงานคอมพิวเตอร์ปฏิบัติงานตรงตามหน้าที่ที่กำหนดไว้ในรายละเอียดลักษณะงาน 16. มีการตรวจสอบประวัติพนักงานใหม่อย่างเพียงพอก่อนอนุญาตให้เข้าเขตหวงห้ามหรือใช้ข้อมูลลับ หรือใช้ข้อมูลทางการเงิน 17. มีการแต่งตั้งพนักงานผู้รับมอบอำนาจในการปฏิบัติงานครบถ้วนทุกตำแหน่ง 18. อัตราหมุนเวียนเข้า-ออกของพนักงานในหน่วยงานคอมพิวเตอร์ระดับผู้ปฏิบัติงานและระดับบริหารมีน้อยอยู่ในเกณฑ์ปกติ 19. พนักงานของหน่วยงานคอมพิวเตอร์มีจำนวนเพียงพอต่อการปฏิบัติงานและมีคุณสมบัติเหมาะสม	

การจัดการ	*มีข้อสังเกต
20. มีระเบียบห้ามพนักงานของหน่วยงานคอมพิวเตอร์ดำรงตำแหน่ง หรือมีอำนาจหน้าที่หรือรับผิดชอบงานที่มีความสำคัญในหน่วยงานอื่น 21. กรณีพนักงานของหน่วยงานคอมพิวเตอร์ต้องทำหน้าที่ในหน่วยงานอื่นด้วย (1) ฝ่ายบริหารของธนาคารได้ตระหนักถึงอุปสรรค หรือความขัดแย้งในการควบคุมภายใน (2) มีการพิจารณาทบทวนอุปสรรคหรือความขัดแย้งในการควบคุมภายในดังกล่าวแล้ว 22. ในรายงานการประชุมคณะกรรมการสถาบันการเงิน หรือในเอกสารอื่นมีเรื่องที่กล่าวถึงการจัดทำแผนงานระยะสั้นและแผนงานระยะยาว 23. มีการปรับปรุงแผนงานระยะยาวเป็นครั้งคราว ให้สอดคล้องกับนโยบายของสถาบันการเงินในขณะนั้น 24. สถาบันการเงินได้ดำเนินการแก้ไขข้อบกพร่องตามข้อสังเกตในการตรวจสอบครั้งก่อนของผู้ตรวจการธนาคารพาณิชย์ 25. สถาบันการเงินพิจารณาแก้ไขข้อบกพร่องที่ผู้สอบบัญชีระบุไว้ในรายงานการตรวจสอบอย่างเพียงพอ 26. มีการวิเคราะห์ความเสี่ยงภัยและนำเทคนิคการบริหารงานอื่น ๆ มาใช้กำหนดประเภทการประกันภัย และวงเงินประกันภัยคอมพิวเตอร์ 27. พนักงานชั้นบริหารของหน่วยงานคอมพิวเตอร์พิจารณาทบทวนการประกันภัยคอมพิวเตอร์ เพื่อขอความเห็นชอบจากสถาบันการเงินอย่างน้อยปีละครั้ง 28. มีการจัดทำแผนการรักษาความปลอดภัยเพื่อให้คณะกรรมการสถาบันการเงินพิจารณา ทบทวน และให้ความเห็นชอบอย่างน้อยปีละครั้ง 29. มีพนักงานที่ได้รับมอบหมายให้รับผิดชอบในการรักษาปลอดภัยภายในหน่วยงานคอมพิวเตอร์	

การจัดการ	*มีข้อสังเกต
30. มีระบบการรายงานผลการปฏิบัติงานที่ดีและมีประสิทธิภาพ เพื่อให้พนักงานชั้นบริหารระดับสูงของสถาบันการเงินใช้ในการควบคุมดูแลและติดตามผลการปฏิบัติงานของหน่วยงานคอมพิวเตอร์	

ระบบงานและโปรแกรม

ระบบงานและโปรแกรม	*มีข้อสังเกต
1. มีระเบียบ (1) การออกแบบระบบงานและการพัฒนาระบบงาน (2) การคัดเลือกโปรแกรมสำเร็จรูป (3) การจัดทำโปรแกรม (4) การทดสอบระบบงานและโปรแกรม (5) การนำระบบงานและโปรแกรมใหม่ออกใช้งานจริง (6) การอนุมัติใช้โปรแกรม (7) การแก้ไขโปรแกรม (8) การปฏิบัติงานของ Operating systems programmers 2. มีการปรับปรุงแก้ไขระเบียบที่กล่าวในข้อแรกให้ทันต่อเวลาอยู่เสมอ 3. ระเบียบการออกแบบระบบงานและการพัฒนาระบบงาน กำหนดให้มี (1) การศึกษาความเหมาะสมของโครงการ (2) การวิเคราะห์ต้นทุนและผลตอบแทนที่ได้รับจากโครงการ (3) การรายงานผลความก้าวหน้าของการพัฒนาระบบงาน (4) การพิจารณาทบทวนและให้ความเห็นชอบในการออกแบบระบบงานทุกขั้นตอน (5) การขอความเห็นชอบในการออกแบบระบบงานจากผู้ใช้ข้อมูลก่อนจัดทำโปรแกรม (6) การทดสอบระบบงานโดยผู้ใช้ข้อมูลและผู้ปฏิบัติงานคอมพิวเตอร์ (7) การขอหนังสือรับรองระบบงานหรือหนังสือรับมอบระบบงานจากผู้ใช้ข้อมูล (8) การพิจารณาทบทวนผลการปฏิบัติงานภายหลังจากที่ได้นำระบบงานใหม่ออกใช้งานจริง 4. ระเบียบการคัดเลือกโปรแกรมสำเร็จรูป กำหนดให้มี (1) การวิเคราะห์โปรแกรมสำเร็จรูปของผู้ผลิตหรือผู้ขายแต่ละรายที่มีลักษณะการทำงานคล้ายกัน หรือใช้ทดแทนกันได้โดยละเอียด (2) การวิเคราะห์ต้นทุนและผลตอบแทนที่ได้รับจากการใช้โปรแกรมสำเร็จรูปของผู้ผลิตหรือผู้ขายแต่ละราย	

ระบบงานและโปรแกรม	*มีข้อสังเกต
5. ระเบียบการจัดทำโปรแกรม กำหนดให้มี (1) การคุมยอดข้อมูลทุกรายการ การคุมยอดข้อมูลแต่ละกลุ่ม และการนับจำนวนรายการให้มากที่สุดเท่าที่จะเป็นไปได้ (2) โปรแกรมตรวจสอบความถูกต้องของข้อมูลนำเข้าก่อนนำไปใช้ประมวลผลในขั้นตอนต่อไป (3) การใช้ File label เพื่อพิสูจน์ความถูกต้องในการใช้แฟ้มข้อมูล (4) จุดตรวจสอบความถูกต้องในการประมวลผลข้อมูลให้มากที่สุดเท่าที่จะเป็นไปได้ ซึ่งจุดตรวจสอบเหล่านี้สามารถใช้เป็นจุดตั้งต้นประมวลผลข้อมูลในขั้นตอนต่อไปได้โดยไม่จำเป็นต้องย้อนกลับไปประมวลผลใหม่ตั้งแต่เริ่มแรก (5) การบันทึกรายการไว้ในระบบสำหรับใช้เป็นหลักฐานในการควบคุมและตรวจสอบ (6) การใช้โปรแกรมย่อยมาตรฐาน (Standardized routine) ให้มากที่สุดเท่าที่จะเป็นไปได้ (7) การจัดทำรายงานแสดงสิ่งผิดปกติในการประมวลผลข้อมูล 6. ระเบียบการทดสอบระบบงานและโปรแกรม กำหนดให้มี (1) การทดลองปฏิบัติงานคู่ขนานกับระบบเดิม (2) การสอบทานและการทดสอบในแต่ละส่วนแยกกันโดยอิสระ (3) การห้ามใช้แฟ้มข้อมูลชุดจริงในการทดสอบ (4) การทดสอบเพื่อหาสาเหตุที่จะทำให้เกิดข้อผิดพลาดในทุกกรณี (5) การพิจารณาทบทวนผลการทดสอบครั้งสุดท้ายเพื่อขอความเห็นชอบจากผู้ที่เกี่ยวข้องทุกหน่วยงาน (6) การทดสอบโปรแกรมที่มีการปรับปรุงแก้ไขทุกครั้งก่อนนำออกใช้งานจริง 7. ระเบียบปฏิบัติก่อนนำระบบงานใหม่ออกใช้จริง กำหนดให้มี (1) การตรวจรับระบบงานอย่างเป็นทางการโดยผู้ใช้ข้อมูลและผู้ปฏิบัติงานคอมพิวเตอร์ (2) การจัดส่งคู่มือปฏิบัติงานชุดล่าสุดให้ผู้ใช้ข้อมูลและผู้ปฏิบัติงานคอมพิวเตอร์ (3) การฝึกอบรมผู้ใช้ข้อมูลให้เสร็จเรียบร้อย (4) การจัดทำเอกสารระบบงานและโปรแกรมให้เสร็จเรียบร้อย	

ระบบงานและโปรแกรม	*มีข้อสังเกต
8. ระเบียบที่กล่าวข้างต้นกระทำเป็นลายลักษณ์อักษร 9. มีเอกสารที่เกี่ยวกับการพัฒนาระบบงานสอดคล้องกับระเบียบที่กำหนดไว้ 10. กรณีมีการเสนอโครงการพัฒนาระบบงานหลายโครงการในงวดงบประมาณปัจจุบัน (1) มีการวิเคราะห์ต้นทุนและผลตอบแทนเพื่อคัดเลือกโครงการที่ดีที่สุด (2) มีการตั้งงบประมาณไว้เป็นเป้าหมายในการคัดเลือกโครงการรวมอยู่ในงบประมาณของสถาบันการเงิน (3) มีการกำหนดวันสิ้นสุดโครงการ 11. มีการใช้ระบบควบคุมโครงการอย่างเป็นทางการ 12. กรณีมีระบบควบคุมโครงการ (1) มีการกำหนดวันที่โครงการเสร็จสมบูรณ์ตามเป้าหมาย (2) มีการกำหนดวันที่เสร็จงานในแต่ละส่วนของโครงการ (3) มีรายงานแสดงสถานะของโครงการทุกระยะ เพื่อให้ทราบว่ามีงานใดบ้างที่เสร็จเรียบร้อยแล้ว และมีงานใดบ้างที่ยังไม่เสร็จสมบูรณ์ (4) มีการกำหนดให้มีการพิจารณาทบทวนวันสิ้นสุดโครงการไว้อย่างชัดเจน 13. มีการพิจารณาทบทวนผลการปฏิบัติงานภายหลังจากที่ได้นำระบบงานใหม่ออกใช้งานจริงแล้ว 14. การพิจารณาทบทวนภายหลังการนำระบบงานใหม่ออกใช้งานจริง ครอบคลุมในเรื่อง (1) การวิเคราะห์ค่าใช้จ่ายในการพัฒนาระบบงานที่กำหนดไว้ในแผนงานกับค่าใช้จ่ายจริง (2) การเปรียบเทียบระยะเวลาที่กำหนดไว้ตามแผนงานกับระยะเวลาที่ใช้ในการพัฒนาระบบงานจริง (3) การเปรียบเทียบค่าใช้จ่ายที่จะประหยัดได้ตามที่กำหนดไว้ในแผนงานกับค่าใช้จ่ายที่ประหยัดได้จริง (4) การเปรียบเทียบผลตอบแทนที่คาดว่าจะได้รับจากระบบงานใหม่กับผลตอบแทนที่ได้รับจริง (5) ปัญหาการปฏิบัติงานในระบบงานใหม่และการปรับปรุงแก้ไขให้ดีขึ้น	

ระบบงานและโปรแกรม	*มีข้อสังเกต
15. ข้อสนเทศแสดงความก้าวหน้าของโครงการถูกต้องตามความเป็นจริง ช่วยให้ทราบสถานะปัจจุบันของโครงการและแหล่งที่เป็นปัญหา 16. วัตถุประสงค์ ระยะเวลา และค่าใช้จ่ายตามโครงการต่าง ๆ ในงวดก่อนเป็นไปตามเป้าหมายที่กำหนดไว้ 17. มีเอกสารประกอบ Operating system จากผู้ผลิตหรือผู้ขายอย่างเพียงพอ 18. มีเอกสารอธิบายรายละเอียดการปรับคุณสมบัติของ Operating system ให้เหมาะสมกับงานของสถาบันการเงิน และมีเอกสารประกอบอื่น ๆ อย่างเพียงพอ 19. กรณีที่มีการประมวลผลข้อมูลในระบบ Multiprograming หรือ Timesharing (1) Operating system ที่ใช้อยู่ในปัจจุบันมี Storage protection หรือ Boundary protection เพื่อป้องกันการบันทึกหรืออ่านข้อมูลในหน่วยความจำบางส่วนโดยไม่ได้รับอนุญาต (2) Operating system ที่ใช้อยู่ในปัจจุบันมี Fetch protection เพื่อป้องกันโปรแกรมใด ๆ ก็ตามล่วงล้ำเข้าไปในหน่วยความจำที่มีโปรแกรมอื่นครอบครองพื้นที่อยู่ 20. มีการแบ่งแยกหน้าที่ระหว่างหน่วยงาน System programming และ Application programming 21. พนักงานผู้ชำนาญงานได้รับมอบหมายให้เป็นผู้บำรุงรักษาระบบงานที่มีความสำคัญ 22. มีพนักงานที่ผ่านการฝึกอบรมและมีประสบการณ์เพียงพอที่จะปฏิบัติงานทดแทนในด้านระบบงานและโปรแกรมที่มีความสำคัญได้ 23. กรณีที่มีการใช้ภาษาระดับใกล้เคียงกับภาษาเครื่องจักรในการเขียนโปรแกรมมีระเบียบห้ามผู้เขียนโปรแกรมใช้คำสั่งใน Operating system 24. มีระเบียบห้ามใช้คำสั่งคัดลอกข้อมูลจากหน่วยความจำ (Storage dump) เว้นแต่จะใช้ในการค้นหาข้อผิดพลาดเท่านั้น	

ระบบงานและโปรแกรม	*มีข้อสังเกต
25. มีระเบียบห้าม System programmer ใช้ Application program libraries และเอกสารที่เกี่ยวข้อง 26. มีระเบียบห้าม Programmer ทุกคนใช้แฟ้มข้อมูลชุดจริง 27. มีระเบียบห้าม Application programmer (1) ใช้เอกสาร Operating system (2) ใช้โปรแกรมที่ได้รับอนุมัติให้ใช้งานจริง 28. มีการรักษาความปลอดภัยหรือทำลาย Program listing ที่เลิกใช้ด้วยวิธีการที่เหมาะสม 29. มี Source listing ของโปรแกรมที่สถาบันการเงินจัดหาหรือจัดซื้อมาใช้เก็บไว้ที่หน่วยงานคอมพิวเตอร์ หรือที่อื่นที่สามารถนำออกมาใช้ได้ทันที 30. มีระเบียบการทำหนังสือขออนุมัติแก้ไขโปรแกรม 31. ระเบียบการแก้ไขโปรแกรม กำหนดให้มี (1) การให้หมายเลขหรือเลขลำดับลงในใบขออนุมัติแก้ไขโปรแกรมไว้ล่วงหน้า (2) การชี้แจงปัญหาหรือเหตุผลในการแก้ไขโปรแกรมไว้ในใบขออนุมัติโดยละเอียด (3) การขอความเห็นชอบจากผู้ที่ได้รับผลกระทบจากการแก้ไขโปรแกรมหรือที่เกี่ยวข้องทุกฝ่าย (4) การระบุชื่อผู้ขอแก้ไขโปรแกรมไว้ในใบขออนุมัติ (5) พนักงานชั้นบริหารควบคุมดูแลการแก้ไขโปรแกรม และลงนามให้ความเห็นชอบกำกับใบขออนุมัติ (6) การส่งสำเนาใบขออนุมัติแก้ไขโปรแกรมให้ผู้ตรวจสอบภายใน 32. มีระเบียบกำหนดให้หน่วยงานที่มีหน้าที่จัดทำโปรแกรมต้องพิจารณาทบทวนความเหมาะสมในการแก้ไขโปรแกรมก่อนรับไปดำเนินการ 33. ระเบียบการพิจารณาคำขอแก้ไขโปรแกรม มีข้อกำหนดเกี่ยวกับ (1) วิธีการที่จะเลือกใช้ในการแก้ไขโปรแกรม (2) ค่าใช้จ่ายในการแก้ไขโปรแกรม	

ระบบงานและโปรแกรม	*มีข้อสังเกต
(3) ระยะเวลาที่จำเป็นต้องใช้ในการแก้ไขโปรแกรม 34. มีระเบียบกำหนดให้มีการตรวจสอบ และมีการพิจารณาอนุมัติก่อนนำโปรแกรมที่มีการปรับปรุงหรือดัดแปลงให้ดีขึ้น (Modification) ไปใช้งานเช่นเดียวกับการแก้ไขโปรแกรม 35. มีระเบียบควบคุมการเปลี่ยนแปลงหรือปรับคุณสมบัติของ Operating system ให้เหมาะสมกับงานของธนาคาร เช่นเดียวกับการแก้ไข Application program 36. กรณีมีการใช้วิธี Petching หรือแก้ไขโปรแกรมอย่างฉุกเฉินเป็นการชั่วคราว มีการเก็บรายละเอียดเกี่ยวกับการอนุมัติ ประโยคคำสั่งที่แก้ไขชื่อผู้แก้ไข และเหตุผลในการแก้ไขไว้เป็นหลักฐานอย่างเพียงพอ 37. หลังจากที่ได้มีการแก้ไขโปรแกรมอย่างฉุกเฉินเป็นการชั่วคราวแล้ว มีการดำเนินการขออนุมัติเช่นเดียวกับกรณีปกติ และมีการแก้ไข Source program ให้สอดคล้องกันโดยไม่ชักช้า 38. มีการแก้ไขเอกสารระบบงานและโปรแกรมภายหลังการแก้ไขโปรแกรมโดยไม่ชักช้า 39. มีการเก็บรายละเอียดการแก้ไขโปรแกรมของแต่ละระบบงานไว้ทุกครั้งตามลำดับก่อนหลัง 40. ระเบียบการจัดทำเอกสารระบบงานและโปรแกรม กำหนดให้มี (1) คำอธิบายระบบงาน (2) ผังแสดงทางเดินของระบบงาน (3) คำอธิบายโปรแกรม (4) ผังแสดงรูปแบบการบันทึกข้อมูล (Record layout schematics) และผังแสดงรูปแบบข้อมูลที่ได้จากการประมวลผล (5) คำอธิบายวิธีการตรวจสอบความถูกต้องของข้อมูลนำเข้า และวิธีการควบคุมที่นำมาใช้ในแต่ละโปรแกรม (6) Source listing ชุดปัจจุบัน (7) คำสั่งที่ใช้ในการปฏิบัติงานสำหรับพนักงานในห้องคอมพิวเตอร์ (8) คู่มือปฏิบัติงานสำหรับผู้ใช้ข้อมูล	

ระบบงานและโปรแกรม	*มีข้อสังเกต
(9) การบันทึกประวัติการแก้ไขโปรแกรม 41. เอกสารระบบงานและโปรแกรมมีครบถ้วนตามระเบียบที่กล่าวข้างต้น และเพียงพอต่อการปฏิบัติงาน 42. สถาบันการเงินจัดทำเอกสารระบบงานและโปรแกรมไว้เป็นระเบียบเรียบร้อย และมีการปรับปรุงแก้ไขให้ทันต่อเวลาอยู่เสมอ 43. มีพนักงานชั้นบริหารของหน่วยงานคอมพิวเตอร์หรือพนักงานอื่นที่ได้รับมอบหมายจากฝ่ายบริหาร ดำเนินการตรวจสอบเอกสารระบบงานและโปรแกรมเป็นครั้งคราว 44. ถ้าไม่มีการตรวจสอบเอกสารตามที่กล่าวข้างต้น มีวิธีการอื่นที่สถาบันการเงินใช้ทดแทนเพื่อช่วยให้ฝ่ายบริหารทราบว่า เอกสารดังกล่าวมีครบถ้วนสอดคล้องกับระเบียบ ของสถาบันการเงินอยู่เสมอ 45. Program source listings (1) มีวันที่ Compile ครั้งหลังสุด (2) มี Version number (3) มีรายละเอียดการแก้ไข Source code 46. วิธีการจัดส่งคู่มือปฏิบัติงานสำหรับผู้ใช้ข้อมูลมีความเหมาะสม 47. พนักงานที่ช่วยปฏิบัติงานเป็นบรรณารักษ์ควบคุมดูแลเอกสาร มีหน้าที่อื่นซึ่งไม่เป็นอุปสรรคต่อการควบคุมภายใน 48. บรรณารักษ์ควบคุมดูแลเอกสาร มีหน้าที่ (1) ตรวจทานการจัดทำเอกสารระบบงานและโปรแกรมให้เป็นไปตามระเบียบของสถาบันการเงิน หากมีการปฏิบัติที่ขัดต่อระเบียบจะต้องทำเรื่องขออนุมัติจากสถาบันการเงินก่อนดำเนินการตามความเหมาะสม (2) ควบคุมดูแลและป้องกันเอกสารไม่ให้ได้รับความเสียหาย (3) ดำเนินการทบทวนแก้ไขเอกสาร (4) แจ้งข่าวและจัดส่งเอกสารให้ผู้มีสิทธิใช้เอกสาร (5) บำรุงรักษาเอกสารและระเบียบปฏิบัติงานให้ทันต่อเวลาอยู่เสมอ	

ความน่าเชื่อถือของข้อมูล

ความน่าเชื่อถือของข้อมูล	* มีข้อสังเกต
1. หน่วยงานที่ทำหน้าที่รับและแจกจ่ายข้อมูลมีเอกสารหลักฐานในการรับและส่งมอบงาน รวมทั้งเอกสารที่ใช้ในการคุมยอดข้อมูล 2. มีทะเบียนรับงานแยกตามหน่วยงานผู้ใช้ข้อมูล และแยกตามงานที่ประมวลผล 3. การจัดเก็บแถบกระดาษบวกเลขรวมยอดข้อมูลที่แนบมาพร้อมกับข้อมูลนำเข้าเป็นไปตามลำดับความเหมาะสม ช่วยให้สามารถตรวจสอบยอดสิ้นวันได้สะดวก 4. มีการควบคุมความถูกต้องของรายการที่ไม่เป็นตัวเงินเช่นเดียวกับรายการที่เป็นตัวเงิน 5. การขอแก้ไขแฟ้มข้อมูล (1) มีทะเบียนจดบันทึกไว้เป็นหลักฐาน (2) มีการระบุตัวผู้แก้ไข (3) มีผู้บังคับบัญชาเป็นผู้อนุมัติการแก้ไข 6. มีระเบียบและมีการกำหนดเวลาเกี่ยวกับเช็คผ่านสำนักหักบัญชี 7. กรณีหน่วยงานผู้ใช้ข้อมูลอยู่ห่างไกลจากหน่วยงานเตรียมข้อมูล มีการถ่ายเอกสารหลักฐานที่เป็นแหล่งกำเนิดข้อมูลลง Microfilm หรือทำสำเนาเก็บไว้ก่อนส่งเอกสารให้หน่วยงานเตรียมข้อมูล 8. คู่มือปฏิบัติงานสำหรับพนักงาน Data entry แสดงรูปแบบของเอกสารที่เป็นแหล่งกำเนิดข้อมูลนำเข้าโดยละเอียด 9. มีการ Key สอบทานความถูกต้องของข้อมูลนำเข้าที่มีความสำคัญต่อการประมวลผล 10. กรณีสถาบันการเงินใช้ระบบ Key-to-disk หรือ Key-to-tape มีการคุมยอดจำนวนเงิน และมีการนับจำนวนรายการด้วยวิธีการที่เหมาะสม 11. เพื่อความสะดวกในการจัดทำข้อมูลนำเข้าใหม่อีกครั้ง มีการเก็บ Disk หรือ Tape	

ความน่าเชื่อถือของข้อมูล	* มีข้อสังเกต
ที่ได้จากการเตรียมข้อมูลไว้ระยะหนึ่งก่อนทำลายข้อมูล 12. การจัดเก็บเอกสารที่บันทึกข้อมูลด้วย MICR ในแต่ละกลุ่มเป็นไปตามลำดับสะดวกต่อการค้นหารายการที่คอมพิวเตอร์ไม่ยอมรับ 13. มีระเบียบห้ามพนักงาน Data entry จัดทำเอกสารขั้นต้นที่เป็นหลักฐานแสดงแหล่งกำเนิดข้อมูล 14. มีการสอบยันยอดคุมระหว่างรายงานที่สัมพันธ์กัน 15. มีการตรวจสอบคุณภาพรายงานก่อนจัดส่งให้ผู้ใช้ข้อมูล 16. มีการควบคุมการจัดทำรายงานและการจัดส่งรายงานให้ผู้ใช้ข้อมูลให้ตรงตามกำหนดเวลา 17. มีการจัดระบบในการจัดเก็บรวบรวมข้อมูล การประมวลผล และการจัดส่งรายงานให้ผู้ใช้ข้อมูล 18. การจัดส่งข้อมูลให้ถูกตัวผู้ใช้ข้อมูล กระทำด้วยวิธีการที่เหมาะสม 19. มีการควบคุมข้อมูลของลูกค้าที่ปรากฏอยู่ในรายงานคอมพิวเตอร์ด้วยวิธีการที่เหมาะสม 20. เอกสารสำคัญทางการเงินที่เกี่ยวข้องกับการประมวลผลข้อมูล เช่น สมุดเช็ค สมุดเงินฝาก ใบหุ้น บัตรประจำตัวลูกค้า และแผ่นถ่ายทอดลายเซ็น เป็นต้น (1) ถูกนำออกมาจากที่เก็บรักษาเฉพาะจำนวนที่ต้องการใช้เท่านั้น (2) ติดกุญแจเก็บไว้ในที่ปลอดภัย (3) มีทะเบียนควบคุม (4) มีการตรวจนับทุกงวดการบัญชี 21. มีการควบคุมการใช้ Microfilm ซึ่งเป็นรูปถ่ายข้อมูลที่ได้จากการประมวลผลเช่นเดียวกับการควบคุมรายงาน 22. Microfilm ที่เก็บรักษาไว้ในที่ปลอดภัย (1) มีการกำหนดตัวผู้มีอำนาจใช้	

ความน่าเชื่อถือของข้อมูล	* มีข้อสังเกต
(2) มีทะเบียนบันทึกการใช้ทุกครั้ง (3) มีทะเบียนแสดงรายละเอียดในการจัดเก็บ (4) มีการตรวจนับทุกงวดการบัญชี 23. มีการนำรายงานคอมพิวเตอร์ที่แสดงรายละเอียดของรายการที่นำเข้าประมวลผลไม่ได้ไปใช้ในการควบคุมการนำข้อมูลเหล่านี้มาประมวลผลใหม่อีกครั้ง 24. มีการกระทบยอดรายการที่คอมพิวเตอร์ไม่ยอมรับ กับรายงานแสดงรายละเอียดของข้อมูลทุกรายการที่ส่งเข้าประมวลผล 25. มีการสอบยันยอดที่ผู้ใช้ข้อมูลจัดทำด้วยมือกับยอดที่ได้จากการประมวลผล 26. มีการจัดส่งรายงานแสดงรายการที่คอมพิวเตอร์ไม่ยอมรับ และข้อมูลที่คอมพิวเตอร์บันทึกรายการไม่ได้กลับไปให้ผู้ใช้ข้อมูล 27. มีพนักงานชั้นบริหารอนุมัติการปรับปรุงแก้ไขข้อมูลนำเข้า ในกรณีที่มี (1) รายการที่หน่วยงานคอมพิวเตอร์รับมาจากผู้ใช้ข้อมูล แต่ไม่ได้นำเข้าประมวลผล (2) รายการที่หน่วยงานคอมพิวเตอร์จัดทำแทนผู้ใช้ข้อมูล หรือจัดทำเพิ่มเติมจากรายการที่ผู้ใช้ข้อมูลจัดส่งมาให้ 28. มีหัวหน้างาน Data base ซึ่งได้รับมอบหมายให้ทำหน้าที่ประสานงานและควบคุมการใช้ Data base 29. หัวหน้างาน Data base เป็นผู้กำหนดระเบียบการใช้ Data record และแฟ้มข้อมูล 30. มีการจำกัดอำนาจหัวหน้างาน Data base ในการใช้ข้อมูลจริง Source listing เอกสารระบบงานและโปรแกรม 31. มีคำอธิบายความหมายของ Data item ปรากฏอยู่ใน Data dictionary หรือ Central catalog 32. การแก้ไข Dictionary ต้องขออนุมัติจากหัวหน้างาน Data base	

ความน่าเชื่อถือของข้อมูล	* มีข้อสังเกต
33. มีวิธีปฏิบัติงานที่ช่วยให้แน่ใจว่า Data dictionary มีความถูกต้องและทันต่อเวลาอยู่เสมอ 34. มีสิ่งอำนวยความสะดวกในการปรับปรุงแก้ไข Data base ให้กลับคืนสู่สภาพปกติ หาก Hardware และ/หรือ Software ได้รับความเสียหาย 35. มี Transaction log เป็นหลักฐานในการควบคุมและตรวจสอบ ซึ่งจะช่วยให้สามารถติดตามรายการที่เกิดขึ้นได้ทุกประการ 36. มีทะเบียนบันทึกการปฏิบัติที่ขัดต่อระเบียบ หรือพยายามฝ่าฝืนการรักษาความปลอดภัยในระบบ Data base	

การปฏิบัติงานคอมพิวเตอร์

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
1. มีการแบ่งแยกหน้าที่ (1) การเตรียมข้อมูล (2) การใช้เครื่อง Data entry (3) การใช้เครื่องคอมพิวเตอร์ (4) การปรับปรุงแก้ไขรายการที่เครื่องคอมพิวเตอร์ไม่ยอมรับ หรืออ่านไม่ได้ เพื่อนำเข้าประมวลผลใหม่ (5) การกระทบยอดข้อมูลที่ได้จากการประมวลผล (6) การจัดส่งรายงานให้ผู้ใช้ข้อมูล	
2. มีระเบียบการจัดตารางปฏิบัติงานคอมพิวเตอร์	
3. การปฏิบัติงานคอมพิวเตอร์ในแต่ละผลัด จำเป็นต้องอาศัยตารางปฏิบัติงานคอม-พิวเตอร์เป็นแนวทาง	
4. ตารางปฏิบัติงานคอมพิวเตอร์เหมาะสมกับปริมาณงานในปัจจุบัน	
5. ความถี่ในการประมวลผลเหมาะสมและสอดคล้องกับความสำคัญของงาน	
6. มีการจัดลำดับความสำคัญในการปฏิบัติงานประมวลผลข้อมูล	
7. การประมวลผลงานจรที่ไม่ได้กำหนดไว้ในตารางปฏิบัติงานคอมพิวเตอร์ ต้องทำหนังสือขออนุมัติทุกครั้ง	
8. มีระเบียบห้ามพนักงานปฏิบัติงานผิดแผกหรือแตกต่างไปจากตารางปฏิบัติงานคอมพิวเตอร์ โดยไม่ได้รับความเห็นชอบจากผู้บังคับบัญชา	
9. มีการตรวจสอบการปฏิบัติงานที่ผิดแผกหรือแตกต่างไปจากตารางปฏิบัติงานคอมพิวเตอร์	
10. มีระเบียบปฏิบัติงานในกรณีที่ได้รับข้อมูลนำเข้าทั้งชุด หรือเพียงบางส่วนล่าช้ากว่าเวลาที่กำหนด	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
11. มีการบันทึกชื่อหรือรหัสของโปรแกรม เวลาเริ่มงาน และเวลาที่เสร็จงานการประมวลผลข้อมูลซ้ำ เวลาที่เครื่องจักรเสีย และชื่อหรือรหัสประจำตัวของผู้ปฏิบัติงาน ไว้ใน Machine log	
12. มีผู้รับผิดชอบลงนามกำกับไว้ใน Machine log หรือมีเอกสารหลักฐานอื่นให้ตรวจสอบในกรณีที่มีการประกอบกิจกรรมอื่นนอกจากการปฏิบัติงานตามปกติ	
13. มีรายงานแสดงรายละเอียดในการใช้เครื่องคอมพิวเตอร์ และการปฏิบัติงานประมวลผลข้อมูล เช่น System activity และ Job accounting เป็นต้น	
14. ระยะเวลาในการจัดทำรายงานในข้อ 13 เพื่อเสนอต่อพนักงานชั้นบริหารเหมาะสมและเป็นประโยชน์ต่อการควบคุมดูแลการปฏิบัติงาน	
15. มีการพิมพ์หมายเลขหน้ากระดาษที่ใช้กับ Console printer หรือมีวิธีการอื่นทดแทน	
16. มีการตรวจสอบ Console log สรุปผลการปฏิบัติงานที่ไม่ใช่กิจกรรมปกติโดยละเอียด	
17. มีการนับเวลาการใช้เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทุกประเภท	
18. มีการจำกัดอำนาจพนักงานในการใช้เครื่องจักรแต่ละประเภท	
19. มีระเบียบกำหนดให้มีพนักงานอย่างน้อย 2 คนอยู่ในห้องคอมพิวเตอร์ ตลอดเวลาที่ใช้เครื่องคอมพิวเตอร์ประมวลผลข้อมูล	
20. มีการฝึกอบรมพนักงานเพื่อให้สามารถปฏิบัติงานทดแทนกันได้ และลดความจำเป็นที่จะต้องพึ่งตัวบุคคลที่มีความสำคัญในการปฏิบัติงานประมวลผลให้น้อยลง	
21. มีการสับเปลี่ยนพนักงานเดินเครื่องคอมพิวเตอร์ให้ปฏิบัติงานหมุนเวียน ระหว่างผลัด หรืองานที่ประมวลผลเป็นครั้งคราว	
22. สถาบันการเงินมีวิธีการควบคุมอื่น ๆ ชดเชย กรณีไม่มีการสับเปลี่ยนพนักงานให้ปฏิบัติงานหมุนเวียนกันเป็นครั้งคราว	
23. มีสัญญาซ่อมบำรุงเครื่องจักรทุกประเภท	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
24. ในสัญญาซ่อมบำรุงเครื่องจักร (1) มีข้อตกลงในการใช้บริการซ่อมบำรุง (2) มีข้อตกลงในการซ่อมบำรุงเพื่อป้องกันการชำรุดเสียหาย (3) มีข้อตกลงเรื่องสถานที่และตารางกำหนดเวลาการซ่อมบำรุง (4) กรณีสถาบันการเงินใช้เครื่องจักรของผู้ผลิตหลายราย มีข้อตกลงเกี่ยวกับขอบเขตการซ่อมบำรุงของผู้ผลิตแต่ละราย	
25. มีทะเบียนจดบันทึกปัญหาของเครื่องจักรทุกเครื่อง	
26. ในระหว่างที่มีการซ่อมบำรุงมีการปลดแฟ้มข้อมูลออกจากระบบ และมีพนักงานของสถาบันการเงินคอยดูแลอยู่ในห้องคอมพิวเตอร์ หรือมีการควบคุมอื่น ๆ ทดแทน	
27. มีระเบียบห้ามพนักงานของหน่วยงานคอมพิวเตอร์ซ่อมเครื่องคอมพิวเตอร์ด้วยตนเอง	
28. การซ่อมบำรุงเพื่อป้องกันการชำรุดเสียหาย เป็นไปตามตารางที่กำหนดไว้ไม่ได้ใช้วิธีสุ่มตัวอย่างเพื่อซ่อมบำรุงเป็นครั้งคราว	
29. การซ่อมบำรุงเพื่อป้องกันการชำรุดเสียหาย มีการทำความสะอาด (1) เครื่องพิมพ์รายงาน (2) ตู้เทป (3) เครื่องอ่านและแยกประเภทข้อมูล (4) ช่องใต้พื้นห้องคอมพิวเตอร์	
30. ตารางซ่อมบำรุงเพื่อป้องกันการชำรุดเสียหาย เหมาะสมกับขนาดของเครื่องคอมพิวเตอร์และปริมาณงาน ซึ่งสอดคล้องกับคำแนะนำของผู้ผลิตคอมพิวเตอร์	
31. มีเอกสารการซ่อมบำรุงเพื่อป้องกันการชำรุดเสียหาย และมีการติดตามดูแลเพื่อให้มีการซ่อมบำรุงตามตารางที่กำหนดไว้	
32. มีระเบียบห้ามพนักงานเดินเครื่องคอมพิวเตอร์ใช้ Source program, Program listing และเอกสารอื่นที่ไม่จำเป็นต้องใช้ในการปฏิบัติงาน	

การปฏิบัติคอมพิวเตอร์	*มีข้อสังเกต
33. มีระเบียบให้พนักงานเดินเครื่องคอมพิวเตอร์ขออนุมัติก่อนทำสำเนา Source program หรือ Object program 34. มีการใช้รหัสลับขอผ่านเข้าระบบ หรือมีวิธีการอื่นในการป้องกันความเสียหายที่อาจเกิดขึ้นกับแฟ้มข้อมูล หรือโปรแกรม 35. มีการเปลี่ยนรหัสลับขอผ่านเข้าระบบเป็นครั้งคราว 36. แฟ้มข้อมูลและโปรแกรมมี Internal label ทุกแฟ้ม 37. มีระเบียบห้ามพนักงานเดินเครื่องคอมพิวเตอร์ปฏิบัติงานข้ามขั้นตอนการตรวจสอบความถูกต้องของ Internal label หรือระบบตรวจสอบอื่น ๆ โดยไม่ได้รับความเห็นชอบจากผู้บังคับบัญชา 38. มีการควบคุมการใช้โปรแกรมทุกชนิด รวมทั้งโปรแกรม Utility ที่สามารถแก้ไขเปลี่ยนแปลงข้อมูลด้วยวิธีการที่รัดกุมอย่างเพียงพอ 39. มีระเบียบห้ามพนักงานเดินเครื่องคอมพิวเตอร์ (1) สร้างรายการซึ่งเป็นแหล่งกำเนิดข้อมูล (2) แก้ไขข้อมูลที่มีข้อผิดพลาด รายการที่บันทึกไม่ได้ และรายการที่เครื่องคอมพิวเตอร์ไม่ยอมรับ (3) ทำรายการป้อนข้อมูลที่ประมวลผล (4) มีหน้าที่ในการทำยอดดุล ซึ่งไม่ได้ใช้ประโยชน์ในการคุมยอดข้อมูลที่มีการประมวลผลต่อเนื่องกัน (5) ทดสอบโปรแกรมกับแฟ้มข้อมูลจริง หรือแฟ้มข้อมูลชุดสำรอง (6) เรียกโปรแกรมที่อยู่ในระหว่างการทดสอบมาใช้ในระหว่างที่มีการประมวลผลข้อมูลจริง 40. มีระเบียบการรับมอบงานและระเบียบการโอนโปรแกรมที่ได้รับอนุมัติให้ใช้งานจริงออกจากงานที่อยู่ในระหว่างการทดสอบ 41. มีระเบียบห้ามพนักงานเดินเครื่องคอมพิวเตอร์ใช้ Object program ที่ยังไม่ได้รับการอนุมัติให้ใช้งานก่อนได้รับอนุญาต หรือได้รับความเห็นชอบจากผู้บังคับบัญชา	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
42. ระเบียบการขออนุมัติปรับปรุงแก้ไข หรือลบโปรแกรมใช้งานจริง กำหนดให้ผู้ขออนุมัติต้องอธิบายเหตุผลและความจำเป็นโดยละเอียด 43. พนักงานชั้นบริหารของหน่วยงานคอมพิวเตอร์และหน่วยงานอื่นที่มีส่วนเกี่ยวข้องร่วมกันพิจารณาและปรับปรุงวิธีการควบคุมภายใน รวมทั้งวิธีการรักษาความปลอดภัยแฟ้มข้อมูลและโปรแกรมเป็นครั้งคราว 44. มีระเบียบหรือคู่มือจัดเก็บแฟ้มข้อมูลและโปรแกรม 45. ระเบียบหรือคู่มือจัดเก็บแฟ้มข้อมูลและโปรแกรม (1) อธิบายวิธีปฏิบัติงานและวิธีการควบคุมภายใน (2) อธิบายวิธีจัดเก็บเทปบันทึกข้อมูลหรือโปรแกรม (3) มีตารางกำหนดอายุการจัดเก็บแฟ้มข้อมูล (4) อธิบายวิธีการจัดทำสลากหรือป้ายชื่อติดแฟ้มข้อมูลและโปรแกรม (5) อธิบายวิธีการจัดเก็บเทปหรือจานแม่เหล็กที่เช่าหรือซื้อมาใหม่ ๆ และใช้ปฏิบัติเมื่อเทปหรือจานแม่เหล็กหมดอายุการใช้งาน (6) มีระเบียบการตรวจนับเทปหรือจานแม่เหล็กที่เก็บไว้ภายในและภายนอกอาคารที่ตั้งหน่วยงานคอมพิวเตอร์เป็นครั้งคราว 46. ห้องเก็บเทปและจานแม่เหล็กเป็นห้องปิดมิดชิด ไม่มีฝุ่นละออง กันไฟไหม้ และมีการกำหนดตัวบุคคลที่มีสิทธิ์เข้าไปในห้องเก็บเทปหรือจานแม่เหล็ก 47. ในห้องเก็บเทปและจานแม่เหล็ก (1) มีหัวฉีดดับเพลิงหรือระบบดับเพลิงแบบอื่น ๆ ติดตั้งไว้อย่างเพียงพอ (2) มีระบบปรับอากาศที่เหมาะสม (3) มีระบบเตือนภัยที่เกิดจากอัคคีภัย 48. มีพนักงานปฏิบัติงานในห้องเก็บเทปและจานแม่เหล็กควบคู่กับการปฏิบัติงานในห้องคอมพิวเตอร์ทุกผลัด 49. พนักงานที่ได้รับมอบหมายให้ทำหน้าที่จัดเก็บเทปและจานแม่เหล็ก ไม่ได้ปฏิบัติงานในหน้าที่อื่นที่เป็นอุปสรรคต่อการควบคุมภายใน	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
50. มีการกำหนดหน้าที่และความรับผิดชอบในการบำรุงรักษาโปรแกรมที่ใช้งานจริง 51. มีการทำสำเนาโปรแกรม Supervisor และโปรแกรม Application สำรองเก็บไว้ใช้ทดแทนได้ทันที อย่างน้อย 1 ชุด 52. มีการจัดเก็บ Source program ในรูปภาษาเครื่องจักรครบถ้วนตามรายการที่ปรากฏอยู่ใน Object library ที่ใช้งานจริง 53. Object program ที่ใช้งานจริงสร้างมาจาก Source program ชุดที่มีอยู่ในปัจจุบัน 54. มีการลบโปรแกรมที่ใช้ไม่ได้หรือเลิกใช้ออกจาก Library ที่ใช้งานจริง 55. ป้ายชื่อที่ติดอยู่ภายนอกแฟ้มข้อมูลมีรายละเอียดเพียงพอ 56. มีทะเบียนบันทึกรายการเทปและจานแม่เหล็กที่มีไว้ใช้งานโดยละเอียด 57. ทะเบียนบันทึกรายการเทปและจานแม่เหล็ก (1) แสดงตำแหน่งหรือแหล่งที่จัดเก็บ (2) แสดงหมายเลขลำดับของม้วนเทปหรือแผ่นจานแม่เหล็ก (3) แสดงวันที่สร้างและวันที่หมดอายุการใช้งาน 58. มีการจัดเก็บเทปข้อมูลที่ใช้งานจริง แยกเทปที่ชำรุดเสียหาย และมีเครื่องหมายแสดงไว้ชัดเจน 59. มีการกำหนดตัวบุคคลที่มีอำนาจใช้แฟ้มข้อมูล 60. การนำแฟ้มข้อมูลออกจากห้องเก็บเทปและจานแม่เหล็ก ต้องสอดคล้องกับตารางปฏิบัติงานประมวลผลข้อมูลเท่านั้น สำหรับการนำแฟ้มข้อมูลออกจากห้องเก็บเทปและจานแม่เหล็กในกรณีอื่น ต้องมีการขออนุมัติตามความเหมาะสม 61. ระเบียบการปฏิบัติงานในห้องคอมพิวเตอร์เพียงพอต่อการปฏิบัติงาน และมีการปรับปรุงให้ทันต่อเวลาอยู่เสมอ	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
62. มีการทำสำเนาโปรแกรม Supervisor โปรแกรม Application และแฟ้มข้อมูลที่เก็บไว้เป็นชุดสำรองก่อนใช้ประมวลผลข้อมูล 63. มีการทดสอบใช้โปรแกรม Supervisor และโปรแกรม Application ชุดสำรองเป็นครั้งคราว 64. มีการปรับปรุงโปรแกรม Supervisor โปรแกรม Application และแฟ้มข้อมูลชุดสำรองที่เก็บไว้ในอาคารที่ตั้งหน่วยงานคอมพิวเตอร์ให้ทันต่อเวลาอยู่เสมอ 65. กรณีสถาบันการเงินใช้ระบบ Data base มีการถ่าย Record ที่สำคัญเก็บสำรองไว้ทุกระยะ 66. มีสำเนาแฟ้มข้อมูลชุดที่จัดส่งให้ผู้สอบบัญชีหรือบริษัทที่ปรึกษาของสถาบันการเงินหรือบุคคลภายนอกเก็บไว้ 67. มีการจัดหาหรือปรับปรุงวัสดุอุปกรณ์ชุดสำรองจัดเก็บไว้ ณ สถานที่อื่นภายนอกหน่วยงานคอมพิวเตอร์ เพื่อให้เพียงพอต่อการปฏิบัติงานและทันต่อเวลาอยู่เสมอ ซึ่งประกอบด้วย (1) Source program และ Object program (2) แฟ้มข้อมูล (3) เอกสารระบบงานและโปรแกรม (4) Operating system และโปรแกรม Utility 68. โปรแกรมและแฟ้มข้อมูลที่เก็บไว้ ณ สถานที่อื่นภายนอกหน่วยงานคอมพิวเตอร์อยู่ในรูปภาษาเครื่องจักร 69. มีการควบคุมการใช้วัสดุอุปกรณ์ชุดสำรองที่เก็บไว้ ณ สถานที่อื่นภายนอกหน่วยงานคอมพิวเตอร์ ด้วยวิธีการที่รัดกุมและเหมาะสม 70. มีทะเบียนบันทึกการจัดเก็บวัสดุอุปกรณ์ชุดสำรองที่เก็บไว้ ณ สถานที่อื่นภายนอกหน่วยงานคอมพิวเตอร์	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
71. ไม่มีเศษกระดาษหรือเศษวัสดุสะสมอยู่ภายในห้องคอมพิวเตอร์หรือบริเวณใกล้เคียงมากพอที่จะทำให้เกิดไฟไหม้ และมีการควบคุมข้อมูลที่มีความสำคัญไม่ให้ปะปนอยู่ในกองเศษกระดาษ ด้วยวิธีการที่รัดกุมและเหมาะสม	
72. มีระเบียบห้ามสูบบุหรี่ ดื่มเครื่องดื่ม และรับประทานอาหาร ในห้องคอมพิวเตอร์	
73. มีการจำกัดจำนวนกระดาษคอมพิวเตอร์ หมึกพิมพ์ และสารไวไฟอื่น ๆ ที่จะนำมาเก็บไว้ในห้องคอมพิวเตอร์ เฉพาะจำนวนที่จำเป็นต้องใช้ปฏิบัติงานประจำวันเท่านั้น	
74. กระดาษที่ไม่ได้ใช้เป็นประจำถูกเก็บไว้ห่างไกลจากห้องคอมพิวเตอร์ และมีเครื่องดับเพลิงติดตั้งอยู่ด้วย	
75. ของเหลวที่เป็นวัสดุไวไฟ น้ำยา และเครื่องมือทำความสะอาด ถูกเก็บไว้ห่างไกลจากห้องคอมพิวเตอร์และห้องเก็บกระดาษ	
76. ห้องคอมพิวเตอร์เป็นระเบียบเรียบร้อยดี	
77. มียามรักษาการณ์ควบคุมการเข้าออกหน่วยงานคอมพิวเตอร์	
78. มีระเบียบกำหนดให้มีการแสดงตัวต่อยามรักษาการณ์ก่อนเข้าไปในหน่วยงานคอมพิวเตอร์	
79. นักการ คนขนของ และช่างซ่อมบำรุง ต้องแสดงตัวต่อผู้มีหน้าที่รับผิดชอบเพื่อขออนุญาตก่อนเข้าห้องคอมพิวเตอร์	
80. มีระบบรักษาความปลอดภัยที่สามารถป้องกันบุคคลอื่นที่ไม่ได้รับอนุญาตเข้าห้องคอมพิวเตอร์หรือห้องเครื่องจักรที่มีความสำคัญต่อการประมวลผลได้โดยเด็ดขาด	
81. ทางเข้าออกที่ใช้ติดต่อกับผู้ใช้ข้อมูล ช่องลม ท่อระบายอากาศเสีย ประตูใหญ่ที่ติดต่อกับภายนอกและทางออกฉุกเฉิน มีความปลอดภัยเพียงพอที่จะป้องกันบุคคลอื่นใช้สถานที่ข้างเคียงหลบหลีกเข้ามาในหน่วยงานคอมพิวเตอร์	
82. มีเครื่องอำนวยความสะดวกในการรักษาความปลอดภัย	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
(1) เครื่องตรวจจับความร้อนและควันไฟ (2) ถังดับเพลิง (3) ระบบควบคุมเพลิงไม่ให้ลุกลามขยายวงกว้าง (4) เครื่องปรับอุณหภูมิและความชื้น (5) เครื่องตรวจจับผู้บุกรุก (6) แหล่งจ่ายกระแสไฟฟ้าทดแทน 83. เครื่องตรวจจับภัยต่างๆ (1) ถูกใช้งานตลอดเวลา 24 ชั่วโมง (2) ส่งสัญญาณกระตุ้นระบบเตือนภัยภายในอาคารที่ตั้งหน่วยงานคอมพิวเตอร์ให้ส่งเสียงดัง (3) ส่งสัญญาณเตือนภัยไฟยังสถานีตำรวจหรือสถานีดับเพลิง 84. มีแผนป้องกันน้ำท่วมเครื่องคอมพิวเตอร์ 85. สามารถหาตำแหน่งที่เปิดพื้นห้องและสามารถเปิดพื้นห้องคอมพิวเตอร์ได้โดยง่าย 86. มีการจดบันทึกรายละเอียดในการพิจารณาจัดหาเครื่องคอมพิวเตอร์ชุดสำรองไว้อย่างเพียงพอ 87. เครื่องคอมพิวเตอร์ชุดสำรองที่ติดตั้งอยู่ในอาคารที่ตั้งหน่วยงานคอมพิวเตอร์แยกเป็นสัดส่วนไม่ปะปนกับเครื่องคอมพิวเตอร์ชุดที่ใช้ปฏิบัติงานตามปกติ 88. เครื่องคอมพิวเตอร์ชุดสำรองตามข้อ 87 (1) ใช้น้ำและกระแสไฟฟ้าจากแหล่งอื่นไม่ปะปนกับเครื่องคอมพิวเตอร์ชุดที่ใช้งานตามปกติ (2) เครื่องจักรแต่ละชุดสามารถทำงานได้โดยอิสระ (3) สามารถทำงานทดแทนระบบที่ใช้งานตามปกติได้ทั้งหมด 89. กรณีสถาบันการเงินมีคอมพิวเตอร์หลายระบบในสถานที่แห่งเดียวกัน (1) มีแหล่งจ่ายน้ำและแหล่งจ่ายกระแสไฟฟ้าที่ใช้ทดแทนกันได้ (2) เครื่องจักรที่ใช้ร่วมกับเครื่องคอมพิวเตอร์ในแต่ละระบบสามารถสับสวิตช์เปลี่ยนไปทำงานร่วมกับระบบอื่นได้	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
90. สถาบันการเงินคาดว่าจะปรับปรุงแก้ไขความเสียหายที่อาจเกิดขึ้นให้คืนสู่สภาพปกติได้ที่หน่วยงานคอมพิวเตอร์ของตนเอง หรือสามารถใช้เครื่องคอมพิวเตอร์ที่อื่นภายนอกสถาบันการเงินได้	
91. มีสัญญาหรือข้อตกลงขอใช้คอมพิวเตอร์กับผู้อื่น เพื่อสำรองไว้ใช้ทดแทนเมื่อเกิดเหตุฉุกเฉิน	
92. มีการทดลองใช้คอมพิวเตอร์ชุดสำรองปฏิบัติงานประมวลผลข้อมูลเป็นครั้งคราว	
93. หน่วยงานคอมพิวเตอร์ได้รับแจ้งให้ทราบถึงการเปลี่ยนแปลง Hardware และ Software ชุดที่สถาบันการเงินสำรองไว้ใช้ทดแทนอยู่เสมอ	
94. สถาบันการเงินพอใจเครื่องคอมพิวเตอร์ชุดสำรอง และการจองเวลาใช้เครื่องสำรองไว้	
95. มีการวางแผนเกี่ยวกับ (1) การรักษาความปลอดภัยด้าน Physical security (2) วิธีปฏิบัติขณะเกิดเหตุฉุกเฉินในแต่ละกรณี (3) วิธีปฏิบัติงานชั่วคราวเพื่อปรับปรุงแก้ไขระบบที่ได้รับความเสียหายให้คืนสู่สภาพปกติ	
96. มีการซักซ้อมปฏิบัติตามแผนงานในข้อ 95 เป็นครั้งคราว	
97. การรักษาความปลอดภัยด้าน Physical security ประกอบด้วย (1) การป้องกันความเสียหายเกี่ยวกับบุคลากร เครื่องจักร และข้อมูล (2) การป้องกันการใช้ข้อมูล เครื่องคอมพิวเตอร์ และเอกสารต่าง ๆ (3) การจัดระบบป้องกันภัย หรือจัดให้มีเครื่องป้องกันภัยในแต่ละกรณี (4) การประกันภัย (5) ระเบียบการใช้เครื่องมือระงับเหตุฉุกเฉิน	
98. แผนปฏิบัติงานขณะเกิดเหตุฉุกเฉิน ประกอบด้วย (1) วิธีเผชิญเหตุการณ์ร้ายแรงเพื่อจำกัดขอบเขตความเสียหาย และเพื่อให้สามารถปฏิบัติงานต่อไปได้	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
(2) แผนอพยพพนักงานออกจากสถานที่เกิดเหตุ (3) ระเบียบปฏิบัติสำหรับพนักงานกรณีไฟไหม้ น้ำท่วม มีผู้บุกรุก ถูกวางระเบิด หรือมีเหตุการณ์ร้ายแรงอื่น ๆ (4) คุณสมบัติของตู้นิรภัยและวิธีใช้ตู้นิรภัยเก็บแฟ้มข้อมูลและเอกสารสำคัญ (5) ระเบียบการปิดเครื่องคอมพิวเตอร์ (6) ระเบียบการปรับปรุงแก้ไขระบบที่ได้รับความเสียหายให้คืนสู่สภาพปกติ กรณีเครื่องจักรขัดข้องหรือเสียหาย 99. แผนปฏิบัติงานชั่วคราวเพื่อปรับปรุงแก้ไขระบบที่ได้รับความเสียหายให้คืนสู่สภาพปกติ ประกอบด้วย (1) การมอบหมายหน้าที่ในการสร้างข้อมูลที่ได้รับความเสียหายขึ้นมาใหม่และหน้าที่ในการปฏิบัติงานประมวลผลข้อมูลนอกสถานที่ (2) กรณีที่จำเป็นต้องปฏิบัติงานประมวลผลข้อมูลนอกสถานที่ด้วยระบบคอมพิวเตอร์ชุดสำรอง (3) การพิจารณาตัดสินใจและความรับผิดชอบในการปฏิบัติงานประมวลผลข้อมูลนอกสถานที่ (4) ระเบียบการขออนุมัติปฏิบัติงานประมวลผลข้อมูลนอกสถานที่ (5) วิธีแจ้งขอใช้ระบบคอมพิวเตอร์ชุดสำรองตามข้อตกลง หรือสัญญาที่ได้กระทำไว้กับผู้อื่น (6) แฟ้มข้อมูล โปรแกรม และเอกสารที่จำเป็นต้องนำไปใช้ปฏิบัติงานประมวลผลข้อมูลนอกสถานที่ และวิธีขนย้ายวัสดุอุปกรณ์ดังกล่าว (7) ลำดับความสำคัญในการประมวลผลข้อมูล (8) วัสดุอุปกรณ์ต่าง ๆ ที่ต้องจัดหาหรือสำรองไว้ใช้ (9) สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล และข้อมูลที่มีความสำคัญ 100. มีการชี้แจงให้พนักงานรับทราบแผนปฏิบัติงานในข้อ 99 เฉพาะส่วนที่เกี่ยวข้องตามความเหมาะสม 101. การประกันภัย (1) มีการประกันความซื่อสัตย์ของพนักงาน (2) มีการประกันภัยเครื่องคอมพิวเตอร์และเครื่องจักรอื่นๆ	

การปฏิบัติงานคอมพิวเตอร์	*มีข้อสังเกต
(3) มีการประกันค่าใช้จ่ายในการสร้างข้อมูลหรือโปรแกรมที่บันทึกไว้ใน Media ที่ได้รับความเสียหายขึ้นมาใหม่ (4) มีการประกันภัยในการโอนเงินทางอิเล็กโทรนิกส์ (5) มีการประกันความเสียหายกรณีธุรกิจสถาบันการเงินต้องหยุดชะงัก เพราะมีอุปสรรคในการประมวลผลข้อมูล (6) มีการประกันความเสียหายอันเนื่องมาจากมีข้อผิดพลาดหรือหลงลืม (7) มีการประกันค่าใช้จ่ายพิเศษที่อาจเกิดขึ้น และค่าใช้จ่ายในการปฏิบัติงานประมวลผลข้อมูลนอกสถานที่ (8) มีการประกันภัยในการขนย้ายข้อมูล (9) มีการประกันภัยด้านอื่น ๆ นอกจากที่กล่าวข้างต้น 102. กรณีผู้ให้สถาบันการเงินเช่าเครื่องคอมพิวเตอร์เป็นผู้ประกันภัยเอง วงเงินที่ประกันภัยให้ความคุ้มครองอย่างเพียงพอ	

การประมวลผลโดยอาศัยระบบสื่อสาร

การประมวลผลโดยอาศัยระบบสื่อสาร	*มีข้อสังเกต
1. มีการจำกัดขอบเขตการใช้เครื่อง Terminal โดยจัดให้มี (1) การล็อคเครื่อง Terminal (2) การตรวจสอบรหัสประจำเครื่อง Terminal (3) การรักษาความปลอดภัยในบริเวณที่ตั้งเครื่อง Terminal (4) รหัสแสดงตัวผู้ใช้เครื่อง Terminal 2. การใช้เครื่อง Terminal มีการควบคุม (1) การใช้แฟ้มข้อมูล (2) การทำรายการผ่านเครื่อง Terminal 3. มีระบบที่ช่วยให้แน่ใจว่าข้อมูลที่ศูนย์คอมพิวเตอร์ได้รับทุกรายการ เป็นข้อมูลที่ส่งมาจากเครื่อง Terminal ของสถาบันการเงิน และผู้ใช้ข้อมูลที่ได้รับมอบหมายเท่านั้น 4. มีการรักษาความปลอดภัยบริเวณที่ติดตั้งอุปกรณ์สื่อสารอย่างเพียงพอ ผู้ที่เข้าไปในบริเวณนั้นได้ต้องเป็นบุคคลที่ได้รับมอบหมายเท่านั้น 5. สายรับส่งสัญญาณสื่อสารที่อยู่ในบริเวณที่ติดตั้งอุปกรณ์สื่อสาร ไม่ได้ทำเครื่องหมายไว้บนสายรับส่งสัญญาณ เพื่อความสะดวกในการค้นหา 6. มีการใช้รหัสเปลี่ยนข้อมูลที่รับส่งผ่านระบบสื่อสารให้ผิดไปจากข้อมูลจริงหรือใช้วิธีการอื่นทดแทนเพื่อความปลอดภัยในการรับส่งข้อมูล 7. กรณีที่มีการใช้รหัสเปลี่ยนข้อมูลให้ผิดไปจากข้อมูลจริง มีการควบคุมหลักเกณฑ์ที่ใช้ในการเข้ารหัสและถอดรหัสอย่างเพียงพอ 8. มีระเบียบหรือวิธีปฏิบัติในการค้นหาสิ่งที่เป็นปัญหาหรืออุปสรรคที่เกิดขึ้นในเครือข่ายการสื่อสารข้อมูล รวมทั้งวิธีการบำรุงรักษาและการกำหนดความรับผิดชอบในการปฏิบัติงาน	

การประมวลผลโดยอาศัยระบบสื่อสาร	*มีข้อสังเกต
9. รหัสแสดงตัวผู้ใช้ข้อมูลแต่ละรายไม่ซ้ำกัน 10. วิธีการกำหนดหรือวิธีการเปลี่ยนแปลงรหัสแสดงตัวผู้ใช้ข้อมูล รหัสลับขอผ่านเข้าไปใช้ระบบ และรหัสอื่น ๆ ที่ใช้ในการรักษาความปลอดภัย มีความเหมาะสมและรัดกุมเป็นประโยชน์ต่อการรักษาความปลอดภัย 11. ไม่มีการเปิดเผยรหัสลับขอผ่านเข้าไปใช้ระบบ หรือรหัสแสดงตัวผู้ใช้ข้อมูลให้ผู้อื่นทราบ โดยการพิมพ์หรือแสดงทางจอภาพ หรือมีเสียงออกมาให้ได้ยิน 12. มีการเปลี่ยนแปลงรหัสแสดงตัวผู้ใช้ข้อมูล รหัสอื่น ๆ ที่ใช้ในการรักษาความปลอดภัยและหมายเลขโทรศัพท์ที่ใช้ในการสื่อสารข้อมูลแบบ Dial-up เป็นครั้งคราว 13. มีการใช้รหัสเปลี่ยนหมายเลขที่ใช้เป็นหลักในการคำนวณรหัสลับ รหัสลับขอผ่านเข้าใช้ระบบ และ Authorization table ที่เก็บอยู่ใน Memory และ/หรืออุปกรณ์บันทึกข้อมูล เช่น เทปและจานแม่เหล็ก เป็นต้น เพื่อให้รหัสดังกล่าวผิดไปจากรหัสที่แท้จริง หรือใช้วิธีการอื่นทดแทน 14. มีการใช้วิธี Call back ควบคุมการรับส่งข้อมูลแบบ Dial-up lines 15. มีการจำกัดอำนาจผู้ใช้ข้อมูลเกี่ยวกับ (1) การใช้แฟ้มข้อมูล (2) รายการที่อนุญาตให้ทำผ่านเครื่อง Terminal 16. มีการพิจารณาทบทวนการมอบอำนาจการใช้เครื่อง Terminal ให้ผู้ใช้ข้อมูลและอำนาจในการอนุมัติรายการของพนักงานทุกระดับชั้นเป็นครั้งคราว 17. มีการจำกัดอำนาจพนักงานให้ใช้เครื่อง Terminal ได้เฉพาะเครื่องที่มีไว้ ใช้งานภายในฝ่ายที่สังกัดเท่านั้น 18. มีการควบคุมไม่ให้ใช้เครื่อง Terminal นอกเวลาที่กำหนด 19. มีการควบคุมเวลาการใช้เครื่อง Terminal ในแต่ละวัน	

การประมวลผลโดยอาศัยระบบสื่อสาร	*มีข้อสังเกต
20. ต้องมีผู้บังคับบัญชาให้ความเห็นชอบกรณีมีการใช้เครื่อง Terminal นอกเวลาที่ได้รับมอบหมาย 21. มีวัสดุอุปกรณ์ฝึกอบรมพนักงาน คู่มือปฏิบัติงานและคู่มือฝึกใช้เครื่อง Terminal สำหรับผู้ใช้ข้อมูลอย่างเพียงพอ 22. การฝึกอบรมพนักงานใช้เครื่อง Terminal ไม่เป็นอันตรายต่อแฟ้มข้อมูลที่ใช้งานจริง 23. มีการตรวจสอบความถูกต้องของข้อมูลที่ป้อนผ่านเครื่อง Terminal เพื่อลดข้อผิดพลาดโดยอัตโนมัติ 24. มีระบบตรวจสอบความสมบูรณ์ของรายการ หรือความถูกต้องในการใช้รหัสรายการเพื่อให้ข้อมูลแต่ละรายการถูกต้องตามหลักเกณฑ์ที่กำหนดไว้ 25. มีการบวกสะสมยอดจำนวนรายการและจำนวนเงินที่ผ่านเครื่อง Terminal แสดงไว้ที่เครื่อง Terminal และที่ศูนย์คอมพิวเตอร์ 26. มีการทำยอดดุลประจำวันของข้อมูลนำเข้าแยกตามเครื่อง Terminal แต่ละเครื่องหรือผู้ใช้ข้อมูลแต่ละราย 27. มีการบันทึกและรายงานการปรับปรุงแก้ไขรายการที่มีข้อผิดพลาดทุกรายการ 28. การปรับปรุงแก้ไขข้อผิดพลาดหรือข้ามขั้นตอนการปฏิบัติงานตามระเบียบของสถาบันการเงิน ต้องได้รับความเห็นชอบจากผู้บังคับบัญชา 29. มีรายงานพิเศษสำหรับใช้ควบคุมและตรวจสอบ (1) งานจรและกิจกรรมที่เกี่ยวข้อง (2) พฤติการณ์ที่น่าสงสัย พยายามเข้าไปใช้ระบบโดยไม่ได้รับอนุญาต (3) ปัญหาและอุปสรรครวมทั้งสถิติต่าง ๆ ภายในเครือข่ายประมวลผลข้อมูลของสถาบันการเงิน 30. รายงานพิเศษสำหรับใช้ควบคุมและตรวจสอบที่มีอยู่ในปัจจุบัน ตรงกับความต้องการของฝ่ายบริหาร ผู้ใช้ข้อมูล และผู้ตรวจสอบภายใน	

การประมวลผลโดยอาศัยระบบสื่อสาร	*มีข้อสังเกต
31. มีพนักงานชั้นบริหารรับผิดชอบในการสอบทานรายการที่ปรากฏอยู่ในรายงานพิเศษสำหรับใช้ควบคุมและตรวจสอบเป็นประจำ 32. มีระเบียบให้ผู้ใช้ข้อมูลจัดเก็บเอกสารชั้นต้น ซึ่งเป็นหลักฐานในการทำรายการผ่านเครื่อง Terminal ไว้อย่างเพียงพอ 33. ข้อความที่ได้รับจากเครื่อง Terminal ทุกเครื่อง ถูกบันทึกเก็บรวบรวมไว้ในแฟ้มข้อมูลชุดที่ใช้บันทึกรายการ 34. แฟ้มข้อมูลชุดที่ใช้บันทึกรายการ มีการบันทึก (1) รายละเอียดในการแสดงตัวผู้ใช้ข้อมูล (2) เครื่อง Terminal ที่ใช้ (3) รหัสรายการ (4) รายละเอียดประกอบรายการตามหลักเกณฑ์ที่กำหนดไว้ (5) วันที่และเวลาที่ทำรายการ 35. มีการตรวจสอบเครือข่ายในระหว่างเวลาที่มีการประมวลผลตามปกติเป็นครั้งคราวเพื่อสอบทานการปฏิบัติงานและตรวจจับข้อผิดพลาดที่อาจเกิดขึ้นในสายการสื่อสาร 36. การจัดทำโปรแกรมแบบ On-line interaction programming ในกรณีที่ใช้ภาษาใกล้เคียงกับภาษาเครื่องจักร ต้องได้รับความเห็นชอบจากผู้บังคับบัญชา 37. มีการควบคุมการใช้เครื่อง Terminal จัดทำโปรแกรมด้วยวิธีการที่เหมาะสมสามารถป้องกันผู้เขียนโปรแกรมใช้แฟ้มข้อมูลจริงทดสอบงาน 38. มีการควบคุมการใช้เครื่อง Terminal ปรับปรุงแก้ไขโปรแกรมที่ใช้งานจริงด้วยวิธีการที่รัดกุม 39. มีระบบอัตโนมัติพิมพ์รายงานแสดงรายละเอียดในการจัดทำโปรแกรม และการปรับปรุงแก้ไขโปรแกรมไว้เป็นเอกสารหลักฐานอย่างเพียงพอ 40. การจัดเตรียมเครื่องจักรและวัสดุอุปกรณ์ชุดสำรอง ประกอบด้วย	

การประมวลผลโดยอาศัยระบบสื่อสาร	*มีข้อสังเกต
(1) คู่สายโทรศัพท์ที่ใช้ในการสื่อสารข้อมูล (2) สวิตช์อัตโนมัติ (3) เครื่อง Terminal สำหรับใช้ปฏิบัติงานทดแทนในจุดที่มีความสำคัญ (4) ระบบควบคุมการสื่อสารข้อมูล (5) เครื่องคอมพิวเตอร์ (6) แฟ้มข้อมูลที่มีข้อมูลหรือรายการซ้ำซ้อนกัน 41. เครื่องจักรและวัสดุอุปกรณ์ชุดสำรองที่มีอยู่ตามข้อ 40 สามารถนำมาใช้ประมวลผลในระบบ Batch ทดแทนได้ หรือสามารถป้องกันวิกฤตการณ์ใน การปฏิบัติประจำวันได้ 42. กรณีประมวลผลด้วยระบบ Batch ทดแทนระบบ On-line (1) มีเอกสารสนับสนุนการปฏิบัติงานอย่างเพียงพอ เช่น เอกสารแสดงขั้นตอนปฏิบัติงาน แบบฟอร์มสำหรับข้อมูลนำเข้า แบบฟอร์มสำหรับตรวจสอบความถูกต้องของข้อมูล เป็นต้น (2) ปริมาณงานไม่มากเกินระดับความสามารถในการประมวลผลข้อมูลของระบบที่ใช้ทดแทน 43. กรณีคอมพิวเตอร์เครื่องใหญ่ของเครือข่ายทำงานขัดข้องหรือเสียหายสามารถใช้เครื่อง Terminal ปฏิบัติงานแบบ Off-line หรือ Off-host ได้ 44. ระบบ On-line ที่สถาบันการเงินใช้สามารถลดระดับการทำงานของเครื่อง Terminal เพื่อให้ปฏิบัติงานบางประเภทได้ หากการทำงานของระบบขัดข้องหรือเสียหาย 45. มีวิธีป้องกันการบันทึกรายการซ้ำซ้อนและวิธีป้องกันข้อมูลสูญหายในกรณีที่มีการปรับปรุงแก้ไขข้อมูลที่ได้รับความเสียหาย เนื่องจากระบบคอมพิวเตอร์ทำงานขัดข้อง ให้คืนสู่สภาพปกติ 46. มีการทดสอบระบบสำรองที่จัดเตรียมไว้เป็นครั้งคราว	

ระบบเงินโอน

ระบบเงินโอน	*มีข้อสังเกต
การประกันภัย 1. มีการประกันภัยการโอนเงินด้วยระบบอัตโนมัติ ซึ่งให้ความคุ้มครองแก่ลูกค้าผู้ใช้บริการด้วย 2. การประกันภัยดังกล่าวได้รับความเห็นชอบจากคณะกรรมการสถาบันการเงิน 3. กรณีสัญญาประกันภัยประเภทที่ให้ความคุ้มครองภัยทุกด้านที่สถาบันการเงินทำไว้ไม่ครอบคลุมถึงบริการโอนเงินด้วยระบบอัตโนมัติ ฝ่ายบริหารของสถาบันการเงินพิจารณาจัดให้มีการประกันภัยด้านนี้เป็นพิเศษ 4. มีการประกันภัยบริการเครื่องฝากถอนเงินอัตโนมัติ และ/หรือบริการสำนักหักบัญชีอัตโนมัติต่อท้ายสัญญาประกันภัยประเภทที่ให้ความคุ้มครองภัยทุกด้าน 5. คณะกรรมการสถาบันการเงินเป็นผู้พิจารณาตัดสินใจขั้นสุดท้าย หากฝ่ายบริหารของสถาบันการเงินมีมติไม่ประกันภัยบริการโอนเงินด้วยระบบอัตโนมัติและยอมเสี่ยงภัยเอง 6. กรณีสถาบันการเงินใช้ระบบเงินโอนร่วมกับผู้อื่น มีการประกันความซื่อสัตย์ของกิจการ และพนักงานที่มีส่วนเกี่ยวข้องในการใช้ระบบร่วมกัน 7. สถาบันการเงินมีสิ่งชดเชยกรณีไม่มีการประกันภัยตามข้อ 6 ระบบเงินโอนประเภทที่ต้องทำรายการผ่านพนักงานธนาคาร **การมอบอำนาจและการขอใช้บริการ** 8. สถาบันการเงินคัดเลือกพนักงานที่ทำหน้าที่ที่มีความสำคัญในการโอนเงินด้วยวิธีการที่เหมาะสม 9. มีระเบียบห้ามพนักงานใหม่ทำงานในบริเวณที่มีความสำคัญในการโอนเงิน 10. การออกหนังสือแต่งตั้งและถอดถอนพนักงานที่มีอำนาจในการทำรายการโอนเงินให้ลูกค้าทันต่อเวลาอยู่เสมอ	

ระบบเงินโอน	*มีข้อสังเกต
11. มีการใช้วิธีการคุมซ้อนในการจัดเก็บบัตรตัวอย่างลายมือชื่อพนักงานที่ได้รับมอบอำนาจปฏิบัติงาน 12. บัตรตัวอย่างลายมือชื่อลูกค้าที่ใช้บริการโอนเงินทันต่อเวลาอยู่เสมอ 13. มีการใช้วิธีการคุมซ้อนในการจัดเก็บบัตรตัวอย่างลายมือชื่อลูกค้า **วิธีการอื่นทดแทน** 14. มีการระบุวงเงินโอนไว้ในบัตรตัวอย่างลายมือชื่อลูกค้า 15. มีการตรวจสอบลายมือชื่อลูกค้าที่ลงนามไว้ในเอกสารขั้นต้น ซึ่งเป็นหลักฐานในการขอโอนเงิน เปรียบเทียบกับตัวอย่างลายมือชื่อ 16. กรณีลูกค้าขอใช้บริการโอนเงินทางโทรศัพท์ สถาบันการเงินมีระเบียบให้ลูกค้าแจ้งข้อมูลให้ครบถ้วนตามที่กำหนด 17. สถาบันการเงิน (1) กำหนดตัวพนักงานที่มอบหมายให้ทำรายการโอนเงินทางโทรศัพท์ และติดต่อรับคำสั่งโอนเงินจากลูกค้า (2) ทำใบแจ้งให้ลูกค้าทราบการโอนเงินทางโทรศัพท์ที่สถาบันการเงินได้ดำเนินการให้ตามคำขอ (3) มีการใช้วิธีการโทรฯ เรียกกลับไปหาลูกค้า และมีการทดสอบรหัสลับขอผ่านเข้าไปใช้ระบบของลูกค้า และ/หรือรหัสอื่น ๆ เพื่อสอบทานความถูกต้องในการขอโอนเงิน (4) มีการกำหนดวงเงินโอนที่จำเป็นต้องใช้วิธีการโทรฯ เรียกกลับไปหาลูกค้า 18. แบบฟอร์มขอโอนเงินของลูกค้าทุกใบมีเลขลำดับพิมพ์ไว้ล่วงหน้า 19. มีการบันทึกเวลาที่ได้รับคำสั่งโอนเงินจากลูกค้า 20. ข้อมูลที่บันทึกไว้เป็นหลักฐานการโอนเงิน ประกอบด้วย (1) เลขลำดับรายการ (2) จำนวนเงินที่ลูกค้าขอโอน (3) ชื่อลูกค้าที่ขอโอนเงิน	

ระบบเงินโอน	*มีข้อสังเกต
(4) วันที่โอน (5) การทดสอบความถูกต้องของรหัสลับที่ใช้โอนเงิน (6) คำสั่งจ่าย (7) ลายมือชื่อพนักงานผู้มีอำนาจโอนเงินแต่ละประเภท และจำนวนเงินที่โอนให้ลูกค้า 21. มีผู้รับผิดชอบตรวจสอบคำขอโอนเงินทุกรายการ เพื่อพิจารณาความเหมาะสมในการรับคำขอจากลูกค้า และการประมวลผลตามคำขอโอนเงิน **การกระทบยอดเงินโอน** 22. มีการกระทบยอดเงินโอนและจำนวนรายการที่โอนประจำวัน 23. มีพนักงานชั้นบริหารรับผิดชอบตรวจสอบการกระทบยอดเงินโอนประจำวัน 24. มีการแบ่งแยกหน้าที่การทำยอดดุลเงินโอนสิ้นวันออกจากหน้าที่ในการรับคำสั่งโอนเงิน หน้าที่ในการประมวลผลข้อมูล และหน้าที่ในการส่งคำสั่งโอนเงินเข้าสู่ระบบ 25. หน่วยงานที่ทำหน้าที่โอนเงินดำเนินการสอบทานความถูกต้องของงานที่ทำกับยอดรวมของข้อมูลก่อนจัดส่งให้หน่วยงานอื่นที่เกี่ยวข้อง 26. มีการตรวจสอบความสอดคล้องเกี่ยวกับการขอเปิดรายการโอนเงินของลูกค้ากับรายการโอนเงินที่เกิดขึ้นจริงที่ปรากฏอยู่ใน Statement ของเครือข่ายการโอนเงินเป็นประจำทุกวัน 27. การปรับปรุงแก้ไขรายการโอนเงินต้องมีผู้รับมอบอำนาจ 2 คน ร่วมกันดำเนินการ 28. มีระเบียบห้ามโอนเงินจากบัญชีที่ไม่ได้ทำข้อตกลงไว้ล่วงหน้า หรือโอนเงินจากบัญชีที่อาจเรียกเก็บเงินไม่ได้ 29. ระเบียบการรับคำสั่งโอนเงินภายหลังกำหนดเวลาตัดยอดรายการประจำวัน มีความรัดกุมและมั่นใจว่า คำสั่งโอนเงินดังกล่าวจะถูกส่งเข้าประมวลผล ในวันเปิดทำงานวันถัดไปอย่างแน่นอน	

ระบบเงินโอน	*มีข้อสังเกต
การควบคุมการปฏิบัติงาน 30. มีการแบ่งแยกหน้าที่พนักงานรับคำสั่งโอนเงินออกจากพนักงานตรวจสอบ ความถูกต้องในการโอนเงิน และพนักงานรับส่งข้อมูล 31. คำสั่งโอนเงินที่รับเข้ามาหรือส่งออกไปมีหมายเลขกำกับทุกรายการ 32. คำสั่งโอนเงินที่รับเข้ามาหรือส่งออกไปมีรหัสข้อความ (Test word) ที่ช่วยให้ทราบว่าเป็นคำสั่งที่แท้จริง 33. รายงานที่บันทึกข่าวสารการโอนเงินมีข้อความครบถ้วนตลอดวันทำงานและไม่ถูกฉีกขาดหายไปบางส่วน 34. มีพนักงานอื่นที่ไม่มีหน้าที่เกี่ยวข้องกับการโอนเงินเป็นผู้ตรวจสอบและควบคุมดูแลรายงานที่กล่าวในข้อ 35. 35. มี Test key ช่วยให้ทราบว่าข้อมูลที่ได้รับหรือส่งออกไปเป็นข้อมูลการโอนเงินที่แท้จริง 36. พนักงานที่รับผิดชอบในการกำหนด และ/หรือยกเลิก Test key ไม่ได้เป็นพนักงานที่ทำหน้าที่ตรวจสอบรหัสคำสั่งโอนเงิน 37. มีการใช้วิธีคุมซ้อนหรือมีวิธีการอื่นทดแทนเพื่อความปลอดภัยในการเก็บรักษาสูตร Test key 38. มีการติดกุญแจป้องกันการใช้เครื่องมือและวัสดุอุปกรณ์ในการโอนเงินโดยไม่ได้รับอนุญาต 39. มีระเบียบที่สามารถป้องกันพนักงานของหน่วยงานคอมพิวเตอร์ใช้เครื่องมือ และวัสดุอุปกรณ์ในการโอนเงิน รวมทั้งมีส่วนรู้เห็นรายละเอียด Test key โดยไม่ได้รับความเห็นชอบจากผู้บังคับบัญชา 40. มีการเปลี่ยนรหัสขอผ่านเข้าไปใช้ระบบเป็นครั้งคราว 41. มีระเบียบและกำหนดเวลาจัดเก็บข้อมูลทางบัญชีเกี่ยวกับการโอนเงิน	

ระบบเงินโอน	*มีข้อสังเกต
รหัสลับประจำตัวลูกค้า 42. รหัสลับประจำตัวลูกค้าแต่ละรายที่ใช้บริการโอนเงินแต่ละประเภทไม่ซ้ำกัน 43. กรณีลูกค้าสามารถเลือกรหัสลับประจำตัวได้ มีการแนะนำลูกค้าให้หลีกเลี่ยง ใช้เลขรหัสเรียงลำดับ หรือใช้รหัสที่เดาได้ง่าย 44. กรณีลูกค้าลืมรหัสลับประจำตัว (1) มีระเบียบการค้นหารหัส หรือการยกเลิกรหัส และการออกรหัสใหม่ให้ลูกค้าด้วยวิธีการที่รัดกุม (2) มีการบันทึกประวัติลูกค้าที่ลืมรหัสทุกครั้งและทุกราย 45. มีระเบียบห้ามแจ้งข้อมูลเกี่ยวกับรหัสลับแก่ลูกค้าทางโทรศัพท์ 46. หากรูปแบบของรหัสลับประจำตัวลูกค้าและเลขที่บัญชีลูกค้าสอดคล้องกันสามารถจับคู่ได้โดยง่าย สถาบันการเงินมีการควบคุมหรือมีการป้องกันในกรณีนี้ด้วยวิธีการที่รัดกุม 47. มีการเปลี่ยนรูปแบบหรือซ่อนรูปแบบที่แท้จริงของรหัสลับประจำตัวลูกค้าในกรณี (1) มีการแจ้งรหัสลับประจำตัวลูกค้าทางโทรศัพท์ (2) มีการบันทึกรหัสลับประจำตัวลูกค้าลงในแฟ้มข้อมูล 48. มีการรักษาความปลอดภัยเอกสารที่เกี่ยวกับการเปลี่ยนรูปแบบหรือซ่อนรูปแบบที่แท้จริงของรหัสลับประจำตัวลูกค้า และเอกสารที่เกี่ยวกับการสร้างรหัสลับประจำตัวลูกค้า 49. มีวิธีการควบคุมที่รัดกุมและเพียงพอในกรณีฝ่ายบริหารจำเป็นต้องใช้รหัสลับประจำตัวลูกค้า และเลขที่บัญชีลูกค้า **บัตรประจำตัวลูกค้า** 50. มีการใช้วิธีคุมซ้อนในการจัดเก็บบัตรเปล่าที่ยังไม่ได้ใช้ และมีทะเบียนคุมยอดบัตรที่นำไปบันทึกข้อมูลลงในแถบแม่เหล็กด้านหลังบัตร และพิมพ์ชื่อลูกค้าเป็นตัวนูนลงในบัตร รวมทั้งนำบัตรใส่ซองและจัดส่งให้ลูกค้า 51. มีการรักษาความปลอดภัยในการจัดเก็บวัสดุอุปกรณ์ที่ใช้ทำบัตรประจำตัวลูกค้า	

ระบบเงินโอน	*มีข้อสังเกต
52. มีการกำหนดตัวพนักงานที่ได้รับอนุญาตให้ปฏิบัติงานในบริเวณที่ทำงานบันทึกข้อมูลลงในบัตรประจำตัวลูกค้า ซึ่งเป็นเขตหวงห้าม	
53. การควบคุมการใช้อุปกรณ์หรือเครื่องบันทึกข้อมูลลงในบัตรประจำตัวลูกค้ามีความรัดกุม	
54. มีการใช้วิธีคุมซ้อนในการทำลายบัตรเสีย และมีเอกสารหลักฐานการทำลายบัตรอย่างเพียงพอ	
55. การควบคุมบัตรที่ใช้ทดสอบระบบ หรือบัตรที่ใช้สาธิตให้ลูกค้าชมมีความรัดกุม	
56. การควบคุมการจัดเก็บบัตรประจำตัวลูกค้าชุดสำเนาหรือชุดสำรองที่ไม่ได้จัดส่งให้ลูกค้ามีความรัดกุม	
57. กรณีสถาบันการเงินมีสถานที่ออกบัตรให้ลูกค้าหลายแห่ง สถาบันการเงินมีระเบียบควบคุมการจัดเก็บบัตรที่รัดกุมทุกแห่ง	
58. กรณีสถาบันการเงินจ้างผู้อื่นทำบัตรประจำตัวลูกค้า ฝ่ายกฎหมายของสถาบันการเงินเป็นผู้พิจารณาสัญญาจ้างทำบัตร	
59. การขนบัตรจากบริษัทผู้ผลิตหรือผู้ขายมายังสถาบันการเงินมีความปลอดภัย	
60. ไม่มีชื่อประเภทธุรกิจแสดงไว้ในที่อยู่ของสถาบันการเงินที่ปรากฏบนซองจดหมายที่ใส่บัตรส่งให้ลูกค้า เพื่อความสะดวกในการส่งจดหมายคืนหากไม่ถึงมือผู้รับ	
61. พนักงานควบคุมและจัดทำทะเบียนบัตรที่เรียกคืนจากลูกค้า ไม่ได้ทำหน้าที่ออกบัตรให้ลูกค้า หรือไม่ได้มีหน้าที่รับผิดชอบเกี่ยวกับระบบงานหรือปฏิบัติงานโอนเงินให้ลูกค้า	
62. สถาบันการเงินไม่มีนโยบายส่งบัตรให้ลูกค้าที่ไม่ได้ขอใช้บริการโอนเงิน	
63. มีการควบคุมบัตรที่เครื่องบริการโอนเงินยึดคืนมาจากลูกค้าด้วยวิธีการที่รัดกุม	
64. สถาบันการเงินจัดส่งบัตรและรหัสลับประจำตัวลูกค้าแยกจากกันคนละครั้ง โดยทิ้งระยะเวลาจัดส่งให้ห่างกันพอสมควร	

ระบบเงินโอน	*มีข้อสังเกต
65. มีการติดตามผลการจัดส่งบัตรและรหัสลับประจำตัวลูกค้า เพื่อให้แน่ใจว่าสถาบันการเงินได้จัดส่งบัตรและรหัสลับดังกล่าวถูกตัวบุคคลแล้ว	
66. มีระเบียบเกี่ยวกับการกำหนดอายุการใช้บัตรประจำตัวลูกค้า บัตรที่สูญหายบัตรที่ถูกโจรกรรม และการใช้บัตรผิดวัตถุประสงค์	
ระบบเงินโอนประเภทที่ลูกค้าทำรายการด้วยตนเอง หรือทำรายการผ่านผู้อื่น	
การใช้เครื่อง Terminal **ร่วมกับผู้อื่น**	
67. มีสัญญาหรือข้อตกลงเป็นลายลักษณ์อักษรระหว่างผู้ใช้เครื่อง Terminal ร่วมกันเกี่ยวกับเรื่องสิทธิความรับผิดชอบ การติดตั้งเครื่อง การให้บริการ และการฝึกอบรมไว้ชัดเจน	
68. ผู้ใช้เครื่อง Terminal ร่วมกับสถาบันการเงินทุกราย ทราบถึงความรับผิดชอบกรณีเครื่องเสียโดยละเอียด	
69. กรณีส่วนหนึ่งส่วนใดของ Switch equipment ไม่ทำงาน สถาบันการเงินได้จัดเตรียมการปฏิบัติงานแบบ Store and forward เพื่อ up date ระบบในภายหลังไว้อย่างเพียงพอ	
70. มีการกำหนดความรับผิดชอบของผู้ผลิตหรือผู้ขายเครื่อง Terminal Switch equipment และอุปกรณ์อื่น ๆ ที่ใช้ในการโอนเงินไว้ในสัญญาซ่อมบำรุง	
71. การควบคุมการใช้เครื่อง Terminal มีความรัดกุม	
72. สถาบันการเงินสามารถระบุตำแหน่งที่ตั้งเครื่อง Terminal หรือเครื่องมือสื่อสารทุกเครื่องที่มีอยู่ในเครือข่ายได้	
73. มีการกำหนดวิธีปฏิบัติในการทำยอดดุลสุทธิประจำวันระหว่างผู้ใช้บริการร่วมกัน	

ระบบเงินโอน	*มีข้อสังเกต
การมอบอำนาจโอนเงิน 74. รหัสประจำเครื่อง รหัสประจำตัวผู้ปฏิบัติงาน และรหัสประจำตัวผู้ที่ได้รับมอบอำนาจที่สถาบันการเงินใช้ มีผลกระทบต่อรายการโอนเงินทุกประเภท 75. การโอนเงินทางโทรศัพท์ที่ลูกค้าต้องทำความตกลงกับสถาบันการเงินไว้ล่วงหน้า ได้แก่ (1) การโอนเงินชำระหนี้แก่เจ้าหนี้เฉพาะราย (2) การโอนเงินระหว่างบัญชีลูกค้า 76. เมื่อได้รับคำสั่งโอนเงินทางโทรศัพท์จากลูกค้า สถาบันการเงินจัดส่งใบยืนยันคำสั่งโอนเงินให้ลูกค้าและผู้รับประโยชน์โดยทันที **การควบคุมการปฏิบัติงาน** 77. สถาบันการเงิน (1) มีสัญญาหรือข้อตกลงเป็นลายลักษณ์อักษรกำหนดความรับผิดชอบระหว่างสถาบันการเงิน ลูกค้า ร้านค้า กิจการที่ให้บริการโอนเงิน และผู้อื่นที่เกี่ยวข้อง (2) มีระเบียบปฏิบัติงานด้านเงินโอน เช่น การอนุมัติสินเชื่อและการอนุมัติเช็ค รวมทั้งเรื่องที่เกี่ยวกับวงเงินโอนขั้นต่ำ และการข้ามขั้นตอนการปฏิบัติงาน เป็นต้น (3) มีสัญญาหรือข้อตกลงในการซ่อมบำรุงเครื่องจักรและอุปกรณ์ที่ใช้ในการโอนเงิน ซึ่งได้แก่ เครื่อง Terminal และเครื่องมือสื่อสาร 78. มีการกระทบยอดเงินโอนทั้งระบบเป็นประจำทุกวัน 79. เงินโอนทุกรายการถูกบันทึกเข้าบัญชีลูกค้าโดยทันที 80. มีการจัดทำรายชื่อบัตรประจำตัวลูกค้าที่สถาบันการเงินยกเลิกการใช้ เนื่องจากสูญหาย หรือสงสัยว่าอาจมีผู้อื่นนำบัตรมาใช้โดยไม่ชอบ เพื่อจัดส่งให้สำนักงานสาขาและผู้ที่เกี่ยวข้องเป็นประจำ 81. สถาบันการเงินมีมาตรการ (1) ป้องกันลูกค้าโอนเงินออกจากบัญชีเกินกว่ายอดเงินที่ลูกค้ามีสิทธิถอนและ/หรือเกินกว่าวงเงินเบิกเกินบัญชี	

ระบบเงินโอน	*มีข้อสังเกต
(2) ป้องกันลูกค้าโอนเงินที่ฝากเข้าบัญชีด้วยเช็คก่อนทราบผลการเรียกเก็บเช็ค 82. มีการควบคุมการใช้เครื่อง Terminal ในการเปลี่ยนแปลงวงเงินสินเชื่อ และข้อมูลทางบัญชีด้วยวิธีการที่รัดกุม 83. มีระเบียบห้ามพนักงานร้านค้าที่ลูกค้าไปใช้บริการเงินโอนขอดูบัญชีลูกค้า หรือข้อมูลทางบัญชีที่สถาบันการเงินเก็บรักษาไว้ 84. เครื่องมือหรืออุปกรณ์ที่ใช้ในการโอนเงินซึ่งเป็นแป้นกดข้อมูล และ/หรือจอภาพมีที่กำบังป้องกันผู้อื่นเห็นรหัสประจำตัวลูกค้า 85. มีใบตอบรับการใช้บริการเงินโอนให้ลูกค้า แสดงวันที่ เวลา และสถานที่ลูกค้าไปใช้บริการทุกรายการ 86. มีหมายเลขลำดับรายการเงินโอนทุกรายการ เพื่อประโยชน์ในการควบคุม และตรวจสอบ 87. มีการสอบทานความถูกต้องของข้อมูลในเทปเงินโอนทุกประเภทก่อนนำไปประมวลผล 88. มีรายงาน (1) แสดงการใช้บริการของลูกค้าที่เพิ่มขึ้นหรือลดลง (2) แสดงรายการที่ลูกค้าใช้บริการได้สำเร็จ และรายการที่ลูกค้าพยายามใช้บริการแต่ไม่ได้ผล (3) แสดงรายการเงินโอนที่มีจำนวนสูง 89. รายงานที่ใช้ควบคุมและตรวจสอบ (1) ตรงกับความต้องการของผู้บริหารหน่วยงานผู้ใช้ข้อมูล (2) ผู้บริหารหน่วยงานผู้ใช้ข้อมูลสอบทานการปฏิบัติงานตามที่ปรากฏอยู่ในรายงานเป็นประจำทุกวัน 90. การควบคุมการปฏิบัติงานเกี่ยวกับชื่อและที่อยู่ของลูกค้า มีความรัดกุมสามารถป้องกันการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต 91. คู่มือปฏิบัติงานสำหรับพนักงานชั้นต้นมีครบถ้วนและสมบูรณ์เพียงพอ	

ระบบเงินโอน	*มีข้อสังเกต
92. หน่วยงานคอมพิวเตอร์ที่ทำหน้าที่ควบคุมระบบเงินโอนดำเนินการทดสอบระบบบันทึกผลการทดสอบ และสอบทานผลการทดสอบทุกขั้นตอน 93. มีเครื่องมือและวิธีการรักษาความปลอดภัยที่ใช้กับระบบเงินโอนอย่างเพียงพอ 94. มีการควบคุมดูแลช่างซ่อมเครื่องจักรและอุปกรณ์ที่ใช้ในการโอนเงินโดยใกล้ชิด **การเตรียมระบบสำรอง** 95. สถาบันการเงินเตรียมวิธีปฏิบัติงานแบบอื่นหรือวิธีการโอนเงินแบบอื่นสำรองไว้ทดแทนระบบเงินโอนอัตโนมัติอย่างเพียงพอ 96. มีการทดสอบปฏิบัติงานโอนเงินตามแผนฉุกเฉินเป็นครั้งคราว **การตรวจสอบภายใน** 97. ขอบเขตการตรวจสอบระบบเงินโอนของผู้ตรวจสอบภายในมีความเหมาะสมและเพียงพอ 98. ผู้ตรวจสอบภายในมีส่วนร่วมแสดงความเห็นเกี่ยวกับการจัดหา หรือเปลี่ยน Hardware และ/หรือ Software รวมทั้งการเปลี่ยนแปลงวิธีการปฏิบัติงานด้านระบบเงินโอนทุกครั้ง	

การใช้บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน

การใช้บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน	*มีข้อสังเกต
1. สัญญาการใช้บริการคอมพิวเตอร์ที่สถาบันการเงินทำกับผู้ให้บริการคอมพิวเตอร์มีเงื่อนไขเหมือนกับผู้ใช้บริการรายอื่น 2. ในสัญญาการใช้บริการคอมพิวเตอร์มีข้อตกลงในเรื่องต่อไปนี้ (1) งานที่ประมวลผล ความถี่ของการประมวลผล และรายละเอียดของรายงานคอมพิวเตอร์ (2) หลักเกณฑ์การคำนวณค่าใช้จ่ายในการพัฒนาระบบงานและโปรแกรมการแปลงรูปข้อมูลจากเอกสารขั้นต้น การประมวลผลและค่าใช้จ่ายกรณีที่เป็นงานจรตามคำขอของสถาบันการเงิน (3) การจัดตารางเวลารับมอบงานและส่งมอบงาน (4) ความรับผิดชอบในการตรวจสอบ รวมทั้งสิทธิในการเข้าตรวจสอบของผู้ตรวจสอบภายในจากสถาบันการเงินผู้ใช้บริการ และผู้ตรวจการธนาคารพาณิชย์จากธนาคารแห่งประเทศไทย (5) การจัดเตรียมระบบสำรองและการป้องกันข้อมูลเสียหาย เพื่อให้สามารถประมวลผลข้อมูลได้ตามกำหนดเวลา แม้จะมีเหตุฉุกเฉินเกิดขึ้น (6) ความรับผิดชอบในการขนส่งเอกสารชั้นต้น ซึ่งเป็นแหล่งกำเนิดข้อมูลระหว่างสถาบันการเงินกับศูนย์คอมพิวเตอร์ (ควรมีการประกันภัยที่ให้ความคุ้มครองอย่างเพียงพอ โดยเฉพาะกรณีผู้ให้บริการเป็นผู้รับผิดชอบการขนส่งเอกสาร) (7) การประกันภัยเกี่ยวกับการบำรุงรักษาข้อมูลที่อาจสูญหาย เนื่องจากมีข้อผิดพลาด หรือหลงลืมปฏิบัติงาน (8) การรักษาความลับของข้อมูล (9) สิทธิความเป็นเจ้าของโปรแกรมและเอกสารที่เกี่ยวข้อง (10) สิทธิความเป็นเจ้าของแฟ้มข้อมูลทุกประเภท และการรับมอบหรือการส่งมอบข้อมูลที่อยู่ในรูปภาษาเครื่องจักรเมื่อสิ้นสุดสัญญาหรือข้อตกลง (11) การเปลี่ยนแปลงราคาและค่าใช้จ่ายการใช้บริการคอมพิวเตอร์ และการบอกเลิกสัญญาจากฝ่ายหนึ่งฝ่ายใด รวมทั้งระยะเวลาสำหรับการเตรียมตัวก่อนเลิกสัญญา	

การใช้บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน	*มีข้อสังเกต
(12) การจัดลำดับความสำคัญของการประมวลผลข้อมูล (13) การกำหนดให้ศูนย์คอมพิวเตอร์แจ้งเรื่องการเปลี่ยนแปลงที่มีผลกระทบต่อวิธีปฏิบัติงาน รายงาน และเรื่องอื่น ๆ ที่เกี่ยวข้อง (14) การจัดส่งข้อมูลเกี่ยวกับฐานะทางการเงินของผู้ให้บริการคอมพิวเตอร์ให้สถาบันการเงินผู้ใช้บริการทราบเป็นครั้งคราว (โดยปกติปีละครั้ง) 3. ในสัญญาการใช้บริการคอมพิวเตอร์มีข้อความเกี่ยวกับการป้องกันความเสียหายและความรับผิดชอบในหนี้สินที่อาจเกิดขึ้นระหว่างศูนย์คอมพิวเตอร์ผู้ให้บริการกับสถาบันการเงินผู้ใช้บริการอย่างเพียงพอ 4. ผู้ให้บริการคอมพิวเตอร์ปฏิบัติตามสัญญาทุกประการ 5. มีแฟ้มรวบรวมเรื่องราวที่สถาบันการเงินร้องเรียนต่อผู้ให้บริการคอมพิวเตอร์ 6. ผู้ให้บริการคอมพิวเตอร์ดำเนินการสอบสวนและพยายามแก้ไขปัญหาที่สถาบันการเงินร้องเรียนทุกครั้ง 7. ผู้ให้บริการคอมพิวเตอร์แจ้งหลักเกณฑ์การคำนวณค่าใช้จ่ายและค่าธรรมเนียมที่เรียกเก็บให้สถาบันการเงินทราบโดยละเอียด 8. ค่าธรรมเนียมที่ผู้ให้บริการคอมพิวเตอร์เรียกเก็บจากสถาบันการเงินอยู่ในเกณฑ์ที่เหมาะสม 9. มีการควบคุมการจ่ายเงินตามใบเสร็จ และ/หรือใบรับค่าธรรมเนียมที่ผู้ให้บริการคอมพิวเตอร์เรียกเก็บด้วยวิธีการที่รัดกุม 10. คู่มือปฏิบัติงานสำหรับผู้ใช้ข้อมูลที่ผู้ให้บริการคอมพิวเตอร์จัดทำให้สถาบันการเงินมีครบถ้วน และทันต่อเวลาอยู่เสมอ 11. คู่มือปฏิบัติงานสำหรับผู้ใช้ข้อมูลครอบคลุมเรื่อง (1) การจัดทำเอกสารขั้นต้นซึ่งเป็นแหล่งกำเนิดข้อมูลและการควบคุมเอกสารดังกล่าว (2) การควบคุมข้อมูล รูปแบบของข้อมูล และวิธีใช้ข้อมูลที่ได้จากการประมวลผล (3) วิธีตัดยอดข้อมูล และวิธีกระทบยอดข้อมูล	

การใช้บริการคอมพิวเตอร์ภายนอกสถาบันการเงิน	*มีข้อสังเกต
12. รายงานคอมพิวเตอร์ที่ใช้ควบคุมและตรวจสอบเป็นไปตามความต้องการของพนักงานชั้นบริหารในหน่วยงานผู้ใช้ข้อมูลของสถาบันการเงิน 13. มีการฝึกอบรม พนักงานสถาบันการเงินให้เข้าใจวิธีการใช้ข้อมูลให้เป็นประโยชน์ต่อการปฏิบัติงาน 14. สถาบันการเงินมีระเบียบการขนย้ายหรือการรับส่งรายงานคอมพิวเตอร์ และเอกสารขั้นต้น 15. ผู้ให้บริการคอมพิวเตอร์จะต้องจัดทำรายงานคอมพิวเตอร์ส่งให้สถาบันการเงินครบถ้วนทุกรายการ แม้จะมีข้อมูลน้อย หรือในกรณีที่ไม่มีข้อมูลเลยจะ ต้องมีรายงานคอมพิวเตอร์แจ้งให้ทราบว่ารายงานชุดนั้นไม่มีข้อมูล 16. ฐานะทางการเงินของผู้ให้บริการคอมพิวเตอร์อยู่ในระดับเพียงพอที่จะดำเนินงานต่อไปได้	

29

แนวทางการตรวจสอบคอมพิวเตอร์ขนาดเล็ก

แนวทางการตรวจสอบคอมพิวเตอร์ขนาดเล็ก (Small Systems)

ในปัจจุบันธุรกิจต่าง ๆ ได้นำเครื่องคอมพิวเตอร์ขนาดเล็กมาใช้งานกันมากขึ้น อันเนื่องมาจากความเจริญก้าวหน้าทางเทคโนโลยี ที่ทำให้เครื่องคอมพิวเตอร์มีขนาดเล็กและราคาถูกลง แต่ยังทำงานได้อย่างมีประสิทธิภาพเหมือนเดิม ดังนั้นผู้ตรวจสอบจึงมีหน้าที่ตรวจสอบความถูกต้องของข้อมูลของธุรกิจที่ใช้เครื่องคอมพิวเตอร์ประมวลผลดังกล่าว โดยพิจารณาว่าธุรกิจมีความน่าเชื่อถือได้ และมีการควบคุมภายในเพียงพอหรือไม่

หัวข้อที่จะกล่าวต่อไปนี้ เป็นเรื่องการควบคุมการดำเนินงานด้านคอมพิวเตอร์ของธุรกิจที่มีระบบงานขนาดเล็ก เรียกว่า ระบบ Turnkey โดยอาศัยผู้ผลิตหรือผู้ขายช่วยออกแบบระบบงาน จัดหาเครื่องจักรและวัสดุอุปกรณ์ รวมทั้งจัดทำ Software และเอกสารประกอบ ธุรกิจดังกล่าวจะไม่มีหน่วยงานตรวจสอบภายใน ไม่มีผู้เขียนโปรแกรม และไม่มีการว่าจ้างบุคคลภายนอกประมวลผลงาน แต่มีเจ้าหน้าที่ปฏิบัติงานจำนวนหนึ่งซึ่งมีความรู้ทางด้านเทคนิคไม่มากนัก

1. การนำคอมพิวเตอร์มาใช้งาน

การนำคอมพิวเตอร์มาใช้งานนั้น ธุรกิจจะต้องศึกษาความเป็นไปได้ (Feasibility Study) เสียก่อน โดยพิจารณาว่าระบบงานในปัจจุบันมีปัญหาอะไรบ้าง การใช้คอมพิวเตอร์จะช่วยแก้ไขปัญหาได้อย่างไร ราคาซื้อหรือค่าเช่าเครื่องเป็นจำนวนเท่าใด

นอกจากนี้ในรายงานดังกล่าวอาจครอบคลุมเรื่อง ต่อไปนี้

- การพนักงานและการอบรม
- การควบคุมภายใน
- การจัดเตรียมสถานที่สำหรับติดตั้งเครื่องและการรักษาความปลอดภัย
- การจัดให้มีผู้ตรวจสอบภายใน
- แผนฉุกเฉินและวัสดุอุปกรณ์สำรอง
- เงื่อนไขในสัญญาซื้อขายหรือเช่า
- การวิเคราะห์ฐานะทางการเงินของผู้ขายเครื่อง
- เปรียบเทียบค่าใช้จ่ายกับธุรกิจอื่นที่ใช้เครื่องชนิดเดียวกัน

ส่วนการตัดสินใจที่จะเลือกเครื่องคอมพิวเตอร์ของผู้ผลิตรายใด ควรกำหนดหลักเกณฑ์การพิจารณาไว้ล่วงหน้า โดยเน้นเรื่องประสิทธิภาพในการทำงานของเครื่องให้มีความสามารถทำงานได้ทั้งในปัจจุบันและอนาคต

2. การเลือก Application software

เนื่องจากธุรกิจที่ใช้คอมพิวเตอร์ขนาดเล็กมักจะไม่มีผู้เขียนโปรแกรม จึงจำเป็นต้องซื้อหรือเช่าโปรแกรมสำเร็จรูปจากบุคคลภายนอก แล้วนำมาดัดแปลงแก้ไขให้ใช้งานได้ตามวัตถุประสงค์ แต่ก่อนที่จะตัดสินใจซื้อหรือเช่าโปรแกรม ควรพิจารณาคำถามต่อไปนี้

1) โปรแกรมนั้นสามารถสนองความต้องการของธุรกิจทั้งในปัจจุบันและอนาคตได้ หรือไม่ มีรายงาน System log หรือ Online log หรือไม่ มีโปรแกรมเช็คสอบความถูกต้องของข้อมูลเพียงพอหรือไม่
2) ธุรกิจที่ใช้โปรแกรมประเภทเดียวกันมีปัญหาหรือไม่
3) โปรแกรมมีราคาเท่าใด และผู้ขายมีฐานะการเงินพอที่จะสนับสนุนธุรกิจในระยะยาวเพียงใด
4) ผู้ขายมีเอกสารประกอบโปรแกรมครบถ้วนหรือไม่ ธุรกิจมีสิทธิได้รับเอกสารเหล่านั้นหรือไม่ และมีสิทธิที่จะปรับปรุงแก้ไขโปรแกรมโดยลำพังได้หรือไม่
5) ในสัญญาซื้อขายมีข้อห้ามนำโปรแกรมไปใช้กับคอมพิวเตอร์ของผู้ผลิตรายอื่นหรือในธุรกิจอื่นหรือไม่
6) วิธีการใช้โปรแกรมสะดวกหรือไม่ คู่มือการใช้เครื่องเขียนชัดเจนและอ่านเข้าใจง่ายหรือไม่ มีการให้การอบรมพนักงานของธุรกิจเพียงพอหรือไม่

ภายหลังจากตกลงซื้อหรือเช่าโปรแกรมจากผู้ขายแล้ว ควรจัดทำสัญญาบำรุงรักษาโปรแกรมด้วย อนึ่ง โดยปกติผู้ขายจะมอบโปรแกรมให้ในรูปของ Object Code ส่วน Source Program ผู้ขายจะเก็บรักษาไว้ ดังนั้น ในสัญญาซื้อขายหรือเช่าโปรแกรมควรระบุให้ธุรกิจมีสิทธิได้รับ Source Program และเอกสารอื่น ๆ ในกรณีที่ผู้ขายไม่เต็มใจหรือไม่สามารถบำรุงรักษาโปรแกรมให้ได้

3. การสนับสนุนจากผู้ขาย

เมื่อธุรกิจตกลงใจที่จะนำคอมพิวเตอร์มาใช้งานแล้ว ก็ควรปรึกษากับผู้ขายเพื่อกำหนดขั้นตอนในการเปลี่ยนแปลงการทำงานจากระบบเดิมไปสู่ระบบใหม่ โดยพิจารณาถึงประเภทและปริมาณรายการของงานที่จะใช้คอมพิวเตอร์ โดยเฉพาะงานที่มีปริมาณรายการเป็นจำนวนมากควรได้รับการพิจารณาก่อน และเพื่อมั่นใจว่าผู้ขายจะให้ความช่วยเหลือในเรื่องนี้ จึงควรจะกำหนดหน้าที่และความรับผิดชอบของแต่ละฝ่าย ดังนี้

- ฝ่ายใดมีหน้าที่รับผิดชอบในการจัดเตรียมแฟ้มข้อมูล
- ให้ผู้ขายมีหน้าที่ในการจัดทำโปรแกรมคำสั่งงาน และอบรมการใช้เครื่องแก่พนักงานของผู้ซื้อ
- กำหนดหลักเกณฑ์การยอมรับระบบงานใหม่

หน่วยงานผู้ใช้จะต้องรับรองความถูกต้องของข้อมูลทั้งก่อนและหลังการเปลี่ยนแปลงระบบงาน ผู้ตรวจสอบควรเข้ามามีบทบาทในการกำหนดจุดควบคุมภายในก่อนจะนำระบบงานใหม่ออกใช้ อย่างไรก็ดีการทดสอบด้วยการปฏิบัติงานคู่ขนานระหว่างระบบงานใหม่กับระบบงานเดิมเป็นระยะเวลาหนึ่งอาจเป็นสิ่งที่จำเป็น เพื่อพิสูจน์ว่าข้อมูลที่ได้รับจากระบบงานใหม่นั้นถูกต้องเชื่อถือได้

4. การจัดทำสัญญาซ่อมแซมบำรุงรักษา

ภายหลังจากตกลงซื้อขายหรือเช่าเครื่องคอมพิวเตอร์ พร้อมทั้งอุปกรณ์ประกอบแล้ว ควรจัดทำสัญญาซ่อมแซมบำรุงรักษาควบคู่กันไปด้วย ในสัญญาดังกล่าวจะกำหนดเวลาในการซ่อมแซมบำรุงรักษาเครื่องไว้ และเมื่อมีการซ่อมแซมบำรุงรักษาตามสัญญาแล้วควรจดบันทึกไว้เป็นหลักฐานด้วย

5. การรักษาความปลอดภัยด้านสถานที่

ในสถานที่สำหรับติดตั้งเครื่องคอมพิวเตอร์ ควรมีการรักษาความปลอดภัย ดังนี้

1) ป้องกันบุคคลผู้ไม่ได้รับอนุญาตเข้าไป
2) อยู่ห่างจากบริเวณที่พนักงานลูกจ้างสัญจรไปมา
3) อยู่ในระดับที่น้ำท่วมไม่ถึง
4) มีเครื่องปรับอากาศและเครื่องควบคุมความชื้น
5) มีเครื่องตรวจจับความร้อนและควัน ซึ่งทำงานตลอด 24 ชั่วโมง
6) มีอุปกรณ์ดับเพลิง

6. System Software

ผู้ผลิตคอมพิวเตอร์จะเป็นผู้จัดทำ System Software เพื่อให้คอมพิวเตอร์ทำงานมีประสิทธิภาพมากยิ่งขึ้น System Software ประกอบด้วย Operating System, System Utilities, Compiler หรือ Interpreter การบำรุงรักษา (Maintain) System Software นี้เป็นหน้าที่ของผู้ผลิต โดยเรียกเก็บค่าบริการจากลูกค้าเป็นรายเดือนหรือรายปี

โดยทั่วไปธุรกิจไม่จำเป็นต้องมีความรู้เกี่ยวกับ System Software มากนัก แต่ควรจะมีความรู้ความเข้าใจเกี่ยวกับเครื่องมือที่นำมาใช้ในการควบคุม และตรวจสอบการปฏิบัติงานคอมพิวเตอร์ เช่น การใช้ Pass - words, Security Codes, Terminal Logs และ Console หรือ System Activity Logs เครื่องมือเหล่านี้ควรมีเอกสารอธิบายประกอบด้วย

ในระบบคอมพิวเตอร์ที่ดีจะมี System Logs หรือ Activity Logs เพื่อบันทึกรายละเอียดเกี่ยวกับการใช้โปรแกรมกำลังงาน Utilities Program, แฟ้มข้อมูล เวลา และอื่น ๆ เครื่องจะบันทึกข้อมูลดังกล่าวโดยอัตโนมัติ ซึ่งไม่มีผู้ใดสามารถเปลี่ยนแปลงแก้ไขได้ ดังนั้นการแก้ไขโปรแกรมโดยมิได้รับอนุญาต หรือการนำ Utilities Programs มาใช้ในการแก้ไขโปรแกรมหรือข้อมูลจะถูกบันทึกไว้เช่นเดียวกัน เจ้าหน้าที่ผู้ควบคุมหรือผู้ตรวจสอบควรตรวจสอบดังกล่าว หากมีสิ่งใดผิดปกติจะได้รีบค้นหาสาเหตุโดยเร็ว

หากในระบบคอมพิวเตอร์ไม่มี System Logs ตามที่กล่าวแล้ว ให้ผู้ปฏิบัติงานบันทึกการใช้โปรแกรมด้วยมือ (Manual Logs) และควรมีการตรวจสอบวันที่ Compile ใน Manual Logs กับ Program Listings ชุดหลังสุดว่าตรงกันหรือไม่เป็นครั้งคราว หากไม่ตรงกันแสดงว่าได้มีการเปลี่ยนแปลงแก้ไขโปรแกรมเกิดขึ้นแล้ว ซึ่งจะต้องมีการสอบสวนเพื่อหาสาเหตุต่อไป

อย่างไรก็ตามบางเครื่องมีเนื้อที่ file สำหรับบรรจุ System หรือ Activity Logs เพียงจำกัด ดังนั้น เมื่อเนื้อที่ file เต็มเครื่องจะบันทึกรายการใหม่ทับรายการเดิม ทำให้รายการเดิมถูกทำลายไป วิธีป้องกันอาจทำได้โดยการพิมพ์ Logs ดังกล่าวออกมาให้หมดเสียก่อน

7. การจ้างบุคคลภายนอกเขียนโปรแกรม

ปัจจุบันการจ้างบุคคลภายนอกเพื่อเขียนโปรแกรมคำสั่งงานนั้น นับวันมีความสำคัญน้อยลง เนื่องจากมีโปรแกรมสำเร็จรูปในท้องตลาดให้เลือกมากมาย อย่างไรก็ดีธุรกิจบางแห่งก็ยังใช้วิธีการจ้างบุคคลภายนอกเขียนโปรแกรมให้ ซึ่งอาจก่อให้เกิดปัญหาหรือความเสี่ยงภัยได้ เช่น

- บุคคลภายนอกผู้เขียนโปรแกรมเข้าใจผิดในวัตถุประสงค์ของงานที่ทำ
- ฐานะทางการเงินของบุคคลภายนอกมีปัญหา
- การพึ่งพาอาศัยบุคคลภายนอกแต่เพียงผู้เดียวในการพัฒนาโปรแกรม

ดังนั้นหากมีความจำเป็นที่จะต้องจ้างบุคคลภายนอกเพื่อเขียนโปรแกรมดังกล่าว ธุรกิจจำเป็นต้องควบคุมดังนี้

- พิจารณาว่าผู้เขียนโปรแกรมมีคุณสมบัติเหมาะสมที่จะทำงานได้หรือไม่
- กำหนดงบประมาณของโครงการ แล้วให้จ่ายเงินเป็นงวด ๆ ตามผลงานที่แล้วเสร็จ
- กำหนดเวลาสิ้นสุดของโครงการ

เมื่อเขียนโปรแกรมเสร็จแล้วจะต้องทดสอบเสียก่อน เพื่อให้แน่ใจว่าโปรแกรมดังกล่าวทำงานได้ตามวัตถุประสงค์ที่กำหนดไว้ นอกจากนี้ผู้เขียนโปรแกรมจะต้องจัดทำเอกสารประกอบโปรแกรม เช่น Source Listing คู่มือสำหรับผู้ใช้งาน เป็นต้น เสร็จเรียบร้อยแล้ว

8. การควบคุมทางด้านเอกสาร

- ควรเก็บรักษาเอกสารประกอบระบบงานและโปรแกรมไว้ภายนอกห้องคอมพิวเตอร์
- หากมีการแก้ไขโปรแกรม จะต้องจัดทำบันทึกการแก้ไขทุกครั้ง โดยได้รับอนุมัติจากผู้มีอำนาจเสียก่อน
- ควรแก้ไขปรับปรุงคู่มือสำหรับผู้ใช้งานให้ทันสมัยอยู่เสมอ

9. การแก้ไขโปรแกรมโดยอาศัยระบบสื่อสาร

ผู้ขายโปรแกรมสามารถแก้ไขโปรแกรมของลูกค้าได้ โดยวิธีเชื่อมต่อสายโทรศัพท์มายังคอมพิวเตอร์ของลูกค้า เรียกว่า "Remote Access Programming" ซึ่งเป็นที่นิยมและเสียค่าใช้จ่ายน้อย อย่างไรก็ตามวิธีนี้ยังไม่ปลอดภัยสำหรับลูกค้า เพราะผู้ขายสามารถแก้ไขโปรแกรมและ/หรือข้อมูลโดยปราศจากการรับรู้ของลูกค้าได้ ดังนั้นการควบคุมที่อาจทำได้โดยให้ Modem มีสภาวะ "ปิด" แทนที่จะ "เปิด" ตลอดเวลา จนกว่าลูกค้าจะอนุญาตให้ผู้ขายแก้ไขโปรแกรมได้ ระหว่างที่มีการแก้ไขโปรแกรมจะต้องนำแฟ้มข้อมูลชุดปัจจุบันออกจากระบบด้วย นอกจากนี้จะต้องส่งเอกสารเกี่ยวกับการแก้ไขโปรแกรมไปให้ลูกค้าเก็บรักษาไว้ชุดหนึ่ง

10. การปฏิบัติการทางด้านคอมพิวเตอร์

ปัจจัยสำคัญที่ส่งเสริมให้สภาพการทำงานมีการควบคุมภายในที่ดีก็คือ การแบ่งแยกหน้าที่ กล่าวคือ หน่วยงานผู้ใช้จะเป็นผู้จัดทำข้อมูล แล้วให้เจ้าหน้าที่ผู้รับมอบอำนาจตรวจสอบความถูกต้องของรายการ จากนั้นจึงจะบันทึกรายการเข้าคอมพิวเตอร์โดยตรงโดยผ่านเครื่อง Terminal หรือบันทึกข้อมูลเข้าไปเก็บไว้ใน Cassette tape หรือ diskette แล้วจึงนำ Cassette tape หรือ diskette ไปประมวลผลอีกครั้งหนึ่งก็ได้ รายการที่เกิดขึ้นประจำวันจะถูกนำไปปรับปรุงแก้ไข (Update) กับ master file และพิมพ์รายงานออกมาให้ผู้ใช้ (Users) รวบรวมยอดและตรวจสอบความถูกต้องขั้นสุดท้าย

ในธุรกิจขนาดเล็ก การแบ่งแยกหน้าที่อาจจะไม่เด่นชัดนัก เนื่องจากมีพนักงานจำนวนน้อย อย่างไรก็ดีก็ควรหามาตรการอื่นมาควบคุมเพื่อชดเชย เช่น ให้มีการหมุนเวียนงาน หรือให้เจ้าหน้าที่แผนกอื่น ๆ ทบทวนงานของแผนกคอมพิวเตอร์ เป็นต้น

ในหน่วยงานผู้ใช้ เจ้าหน้าที่ผู้จัดทำข้อมูลไม่ควรมาทำหน้าที่ตรวจสอบรายงาน รายงานทุกประเภทควรมี Audit Trail สำหรับการตรวจสอบและติดตามรายการได้ โดยเฉพาะอย่างยิ่งควรจะพิมพ์รายงานที่แสดงรายการที่เกิดขึ้นประจำวันเพื่อประโยชน์ในการตรวจสอบ

การรักษาความปลอดภัยของแฟ้มข้อมูลก็เป็นสิ่งสำคัญ แม้ว่าธุรกิจขนาดเล็กอาจจะไม่มีห้อง library สำหรับเก็บรักษาแฟ้มข้อมูล เนื่องจากมีแฟ้มข้อมูลจำนวนน้อย ไม่คุ้มกับค่าใช้จ่ายที่เกิดขึ้น อย่างไรก็ตามแฟ้มข้อมูลที่ยังไม่ได้ใช้งานประจำวันก็ควรเก็บรักษาไว้ในตู้นิรภัย ซึ่งอยู่ห่างจากห้องคอมพิวเตอร์ และไม่ควรนำแฟ้มข้อมูลชุดสำรอง (Backup File) ออกมาใช้หลาย ๆ ชุด ทั้ง ๆ ที่มีความจำเป็นต้องการใช้เพียงชุดเดียวเท่านั้น

11. การตรวจสอบ

ธุรกิจขนาดเล็กอาจมอบหมายให้เจ้าหน้าที่คนใดคนหนึ่งรับผิดชอบงานตรวจสอบ โดยให้จัดทำเอกสารที่เกี่ยวข้องกับการตรวจสอบ เพื่อเสนอให้ฝ่ายบริหารอนุมัติก่อนจะนำไปปฏิบัติ นอกจากนี้ควรพัฒนาการจัดทำกระดาษทำการให้เกิดประโยชน์ต่องานตรวจสอบ ตลอดจนอนุญาตให้ผู้สอบบัญชีภายนอกและเจ้าหน้าที่ระดับบริหารทบทวนถึงขอบเขตและความเพียงพอของงานตรวจสอบของผู้ตรวจสอบภายในได้

12. การ Backup

ธุรกิจจำเป็นต้องจัดเตรียมเครื่องคอมพิวเตอร์และอุปกรณ์สำรอง โปรแกรมสำรอง และแฟ้มข้อมูลสำรอง เพื่อนำมาใช้ในกรณีที่ธุรกิจประสบกับปัญหาต่าง ๆ โดยมิได้คาดหมายไว้ ช่วยทำให้ธุรกิจสามารถดำเนินงานต่อไปได้โดยไม่หยุดชะงัก

1) Hardware Backup

กรณีที่เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ ธุรกิจอาจจำเป็นต้องขอใช้บริการประมวลผลข้อมูลจากศูนย์คอมพิวเตอร์ของบุคคลภายนอก ทั้งนี้โดยจัดทำข้อตกลงล่วงหน้ากับผู้จัดการศูนย์คอมพิวเตอร์แห่งนั้น เพื่อกำหนดเงื่อนไขและเวลาในการขอใช้บริการ รวมทั้งอนุญาตให้ธุรกิจเข้าไปสำรวจเป็นครั้งคราว เพื่อให้มั่นใจว่าศูนย์คอมพิวเตอร์แห่งนั้นสามารถประมวลผลงานได้โดยไม่มีปัญหา

2) Software Backup

ควรจัดเก็บรักษาโปรแกรมชุดสำรองและเอกสารประกอบระบบงาน และโปรแกรมชุดสำรอง ณ สถานที่แห่งอื่น ซึ่งอยู่ภายนอกอาคารของธุรกิจ เมื่อเกิดกรณีฉุกเฉินก็สามารถนำมาใช้ได้ทันที

3) Data File Backup

ในระบบคอมพิวเตอร์ขนาดเล็ก แฟ้มข้อมูลชุดปัจจุบันจะอยู่ใน Fixed Disk ตลอดเวลา เมื่อเสร็จสิ้นงานประจำวัน ทั้ง Master File และ Transaction File จะถูกสำเนา (Copy) ลงในแผ่น Diskette หรือ Disk Pack หรือ Tape เพื่อเก็บเป็นชุดสำรอง (Backup) ปกติจะเก็บรักษาไว้เป็นระยะเวลา 3-5 วัน โดยที่แฟ้มข้อมูลชุดสำรองดังกล่าวเก็บไว้ในสถานที่เดียวกับแฟ้มข้อมูลชุดปัจจุบัน จึงนับว่าเป็นอันตรายอย่างมากหากเกิดอัคคีภัยขึ้น ดังนั้นจึงควรแยกแฟ้มข้อมูลสำรองออกมาเก็บรักษาไว้ ณ สถานที่แห่งอื่นที่มีความปลอดภัยเพียงพออีกชุดหนึ่งต่างหาก

13. แผนปฏิบัติงานชั่วคราวกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Contingency Plan)

แผนปฏิบัติงานชั่วคราวกรณีเกิดเหตุฉุกเฉิน มีเรื่องสำคัญดังนี้

- เงื่อนไขการขอใช้บริการจากศูนย์คอมพิวเตอร์ของบุคคลภายนอก (Backup Site)
- การเดินทางไปยัง Back Site
- เวลาที่จะใช้ในการประมวลผล
- พลังงานต่าง ๆ ที่จำเป็นต้องใช้
- การจัดลำดับความสำคัญของงาน

เมื่อได้จัดทำแผนการดังกล่าวเสร็จเรียบร้อยแล้ว ควรซักซ้อมความเข้าใจกับเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อที่จะปฏิบัติได้ถูกต้องและรวดเร็วในระหว่างที่เกิดเหตุ

14. การประกันภัย

ธุรกิจส่วนใหญ่จะทำประกันภัยประเภท Blanket Bond หรือประกันความซื่อสัตย์ของพนักงานลูกจ้าง หรือประกันอัคคีภัย ซึ่งการทำประกันภัยดังกล่าวจะให้ความคุ้มครอง รวมถึงกรณีการจัดทำข้อมูลใหม่ ค่าใช้จ่ายที่เกิดขึ้นผิดปกติ และทรัพย์สินที่เอาประกัน โดยเฉพาะการประกันภัยทรัพย์สินนั้น ธุรกิจอาจไม่จำเป็นต้องทำประกันถ้าหากว่าธุรกิจเป็นผู้เช่าทรัพย์สินนั้นมา

สำหรับการจัดทำข้อมูลใหม่ หมายถึง การเตรียมข้อมูลที่อยู่ในรูปของ tape, disk หรือ diskette ส่วนค่าใช้จ่ายที่เกิดขึ้นผิดปกติ หมายถึง รายได้ที่ขาดหายไปอันเนื่องมาจากการหยุดปฏิบัติงาน เพราะอุปกรณ์หรือสื่อข้อมูลสูญหาย ธุรกิจจะทำประกันภัยประเภทใดนั้นควรคำนึงถึงค่าใช้จ่ายในการทำประกันภัย กับความเสี่ยงที่จะเกิดขึ้นกับธุรกิจ และควรมีการทบทวนการทำประกันภัยเป็นประจำทุกปี

ผู้รับประกันภัยบางแห่งอาจมีข้อเสนอให้การคุ้มครองแก่กิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานด้านคอมพิวเตอร์ โดยสลักหลังใบกรมธรรม์ว่า “Blanket Bond” ซึ่งให้การคุ้มครองเกี่ยวกับ

- การรับส่งข้อมูลผ่านระบบโอนเงินทางอิเล็กโทรนิกส์
- ความไม่ซื่อสัตย์ของพนักงานลูกจ้างของผู้ขาย Software
- การรับส่งข้อมูลโดยผ่านเครื่อง Terminal ของลูกค้า
- การประกอบอาชญากรรมคอมพิวเตอร์ อันมีผลกระทบต่อเครื่องจักรและอุปกรณ์สื่อสาร ข้อมูล และการทำงานของโปรแกรม

15. บทสรุป

เรื่องที่กล่าวไปทั้งหมดข้างต้นนี้ เป็นเรื่องการควบคุมการดำเนินงานด้านคอมพิวเตอร์ของธุรกิจที่ใช้คอมพิวเตอร์ขนาดเล็ก โดยเน้นว่าการจัดหาเครื่องคอมพิวเตอร์มาใช้งานนั้น จะต้องมีการวางแผนอย่างรอบคอบ และผู้บริหารควรให้ความสนใจอย่างมาก การขาดความเข้าใจของผู้บริหารในเรื่องการประมวลผลงานด้วยคอมพิวเตอร์อาจทำให้ธุรกิจได้รับความเสียหายได้ นอกจากนั้นการดำเนินการควบคุมการปฏิบัติงานทุกขั้นตอน จะช่วยทำให้มั่นใจว่าระบบงานและข้อมูลมีความถูกต้องเชื่อถือได้

ภาคผนวก

ภาคผนวก ก.

Information Which May Be Recorded on Journals (Logs) for Purposes of System Protection and Auditing

KEY: ✓ = Yes
P = Possibly
I = At specified intervals

Functions:	To provide an audit trail for an auditor to follow the history of a transaction	To permit recovery when it is found that a user has incorrectly updated or deleted a record	To investigate the causes when a record is found to be faulty	To assist recovery from massive file destruction	To assist in correcting the file when a program has been damaging data	To correct false information which has been sent to system users	To monitor procedural violations to highlight possible breaches of security	To assist in correct recovery from a system failure	To monitor the way the system is being used (as an aid to design)	To recover from the loss of a file-action journal
Transaction journal										
Incoming inquiry transaction	✓	✓	✓			✓		✓	✓	✓
Incoming update transaction	✓	✓	✓			✓		✓	✓	✓
Transaction type	✓	P	P			✓		✓	P	✓
Transaction number	✓	✓	✓			✓	✓	✓	✓	✓
Originating terminal	✓	✓	✓			✓	✓	✓	✓	✓
Originating operator	✓	✓	✓			✓	✓	✓	✓	✓
Time and date	I	I	I			I	✓	I	I	I
Response to inquiry transaction	✓	✓	✓			✓	✓	✓	✓	✓
Response to update transaction	✓	✓	✓			✓	✓	✓	✓	✓
Indication that response was received correctly	✓	✓	✓			✓	✓	✓	✓	✓
Procedural violations on input							✓			
Record of start and end of file reconstruction										
Note of completion of update									✓	
File-action journal										
Transaction number	✓	✓	✓		✓					
Time and date		I	I	✓	I					
Addresses of items updated	✓	✓	✓	✓	✓					
Contents of items before they are updated										
Contents of items after they are updated	✓	✓	✓		✓					
Note of completion of update	✓	✓	✓	✓	✓					
List of programs used for update			✓		✓					
Full contents of any records created			✓		✓					
Full contents of any records deleted			✓		✓					
Details of any indices opened or closed			✓	✓	✓			✓		
Procedural violations deleted during update or processing							✓			
Contents of items corrected before correction	✓		✓	✓				✓		
Contents of items corrected after correction	✓		✓	✓				✓		
Indication of start and end of a correction run	✓		✓	✓				✓		

The above information may be all on the same journal.

ภาคผนวก ข.
ตัวอย่างเปรียบเทียบการตรวจสอบสินค้าคงคลัง ในระบบ Manual และในระบบ Computer

1.ข้อเท็จจริง

ผู้สอบบัญชีจะทำการตรวจสอบงบการเงินของผู้ขายส่งเครื่องสำอางที่มีสินค้าคงคลังแต่ละรายการจำนวนมาก ๆ (หลายพันรายการ) ซึ่งผู้ขายส่งได้จัดเก็บสินค้าคงคลังไว้ที่ศูนย์ขายส่งของตนและที่คลังสินค้าสาธารณะอีก 2 แห่ง แฟ้มข้อมูลสินค้าคงคลัง (Inventory Computer File) บันทึกอยู่ในจานแม่เหล็ก (disk) ทั้งนี้ในสิ้นวันทำการของแต่ละวันแฟ้มข้อมูลสินค้าคงคลังนี้จะถูกบันทึกข้อมูลให้เป็นปัจจุบัน รายละเอียดของแต่ละ Record ในแฟ้มข้อมูลสินค้าคงคลังประกอบด้วยข้อมูลดังต่อไปนี้

1. เลขหมายรายการสินค้า
2. สถานที่เก็บสินค้า
3. ลักษณะสินค้า
4. จำนวนสินค้าคงคลังที่อยู่ในมือ
5. ต้นทุนต่อหน่วย
6. วันที่ซื้อครั้งสุดท้าย
7. วันที่ขายครั้งสุดท้าย
8. จำนวนขายระหว่างปี

ผู้สอบบัญชีได้วางแผนที่จะเข้าสังเกตการณ์ตรวจนับสินค้าคงคลังของผู้ขายส่งตามวันที่ที่ได้กำหนดไว้ ทั้งนี้ผู้สอบบัญชีจะมีรายละเอียดข้อมูลสินค้าคงคลัง ณ วันที่สังเกตการณ์ในรูปของ Computer tape และมีคอมพิวเตอร์พร้อมอุปกรณ์ที่จะนำมาช่วยในการปฏิบัติงาน (General purpose computer software package)

2. สิ่งที่ต้องการให้พิจารณา/ศึกษา

ผู้สอบบัญชีได้วางแผนที่จะใช้วิธีการตรวจสอบขั้นพื้นฐานในการตรวจสอบสินค้าคงคลังจงระบุวิธีการตรวจสอบขั้นพื้นฐานในการตรวจสอบสินค้าคงคลัง พร้อมทั้งอธิบายด้วยว่าจะใช้ประโยชน์จากการนำคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (General purpose software package) และรายละเอียดข้อมูลสินค้าคงคลังซึ่งบันทึกไว้ในรูปเทปข้อมูล (tape of the inventory tape) มาช่วยในการปฏิบัติงานตรวจสอบสินค้าคงคลังดังกล่าวได้อย่างไร

3. แนวคำตอบ

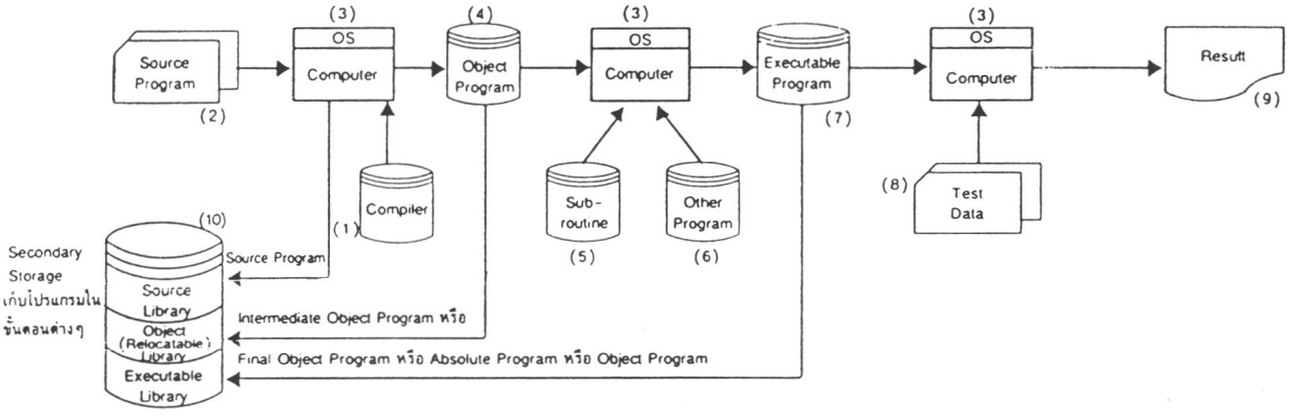
วิธีการตรวจสอบขั้นพื้นฐาน (manual) ในการตรวจสอบสินค้าคงคลังและข้อสังเกต	กรณีนำคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์และเทปข้อมูลสินค้าคงคลังมาช่วยในการตรวจสอบ
1. สังเกตการณ์การตรวจนับ ทดสอบการตรวจนับและบันทึกผลการตรวจนับที่ทดสอบนั้น (เป็นการทดสอบปริมาณสินค้าคงเหลือ ซึ่งมีจำนวนมากมายว่าถูกต้องหรือไม่)	1. กำหนดรายการที่จะทดสอบการตรวจนับ โดยเลือกตัวอย่างแบบสุ่ม (random sample) เพื่อเป็นตัวแทนของสินค้าจาก inventory file ณ วันที่มีการตรวจนับ
2. ทดสอบความถูกต้องของตัวเลขรายละเอียดและยอดรวมของสินค้าคงคลัง (ต้องทำการบวกรายการมากมายมหาศาลเพื่อพิสูจน์ความถูกต้อง)	2. คำนวณมูลค่าจำนวนเงินของสินค้าคงคลังแต่ละรายการที่ตรวจนับโดยนำปริมาณสินค้าคงคลังที่อยู่ในมือคูณกับต้นทุนต่อหน่วย และสอบทานจำนวนเงินที่เกิดจากผลคูณนี้
3. เปรียบเทียบผลการตรวจนับที่ผู้ตรวจสอบได้ทดสอบนั้นกับ inventory records (เปรียบเทียบผลการทดสอบกับรายละเอียดสินค้าคงเหลือซึ่งใช้เวลามากและลำบากในการค้นหาข้อมูลในแต่ละ records)	3. จัดเก็บข้อมูลผลการตรวจนับที่ทดสอบนั้นใน tape ซึ่งมี format ในลักษณะเดียวกับ inventory file และ matching tape ทั้งสองนั้น
4. เปรียบเทียบข้อมูลที่ได้จากการตรวจนับกับ inventory records (เนื่องจากมีจำนวนมากมายทำให้เสียเวลาและยุ่งยากในการค้นหา)	4. เปรียบเทียบยอดรวมของมูลค่าจำนวนเงินของสินค้าคงคลังทุกรายการที่ตรวจนับได้ และมูลค่าจำนวนเงินของแต่ละรายการสินค้าคงคลังที่ตรวจนับกับ inventory rocords
5. ทดสอบการตีราคา (pricing) ของสินค้าคงคลังโดยขอ list ต้นทุนต่อหน่วยจากผู้ซื้อ ผู้ขาย หรือจากแหล่งอื่น ๆ (เป็นงานซ้ำ ๆ และมีปริมาณมาก)	5. เตรียม tape ใน format เดียวกับเทปข้อมูลสินค้าคงคลัง และ matching tape นั้น

วิธีการตรวจสอบขั้นพื้นฐาน (manual) ในการตรวจสอบสินค้าคงคลังและข้อสังเกต	กรณีนำคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์และเทปข้อมูลสินค้าคงคลังมาช่วยในการตรวจสอบ
6. ตรวจสอบการตัดยอดซื้อและขาย (cut - off) (ตัดยอดการรับ-จ่ายสินค้าคงคลังจนถึงวันตรวจนับจะทราบยอดสินค้าคงคลัง)	6. list ตัวอย่างรายการสินค้าจาก inventory file โดยมีวันที่ซื้อครั้งสุดท้ายและวันที่ขายครั้งสุดท้าย ณ หรือใกล้กับวันก่อนวันที่เข้าตรวจนับ
7. ต้องแน่ใจว่าสินค้าคงคลังที่จัดเก็บอยู่ในคลังสินค้าสาธารณะเป็นสินทรัพย์ของกิจการ	7. list รายการสินค้าคงคลังที่จัดเก็บไว้ที่คลังสินค้าสาธารณะ
8. วิเคราะห์สินค้าคงคลังว่าอาจจะล้าสมัย (ดูสภาพและคุณภาพ เช่น ทดสอบรายที่ไม่ค่อยมีการเคลื่อนไหว หรือค้างนาน ๆ)	8. list รายการสินค้าจาก inventory file ซึ่งวันที่ขายครั้งสุดท้าย แสดงว่าไม่มีรายการซื้อขายมานานแล้ว
9. วิเคราะห์สินค้าคงคลังว่าอาจจะเป็นการถือไว้เกินจำเป็น (overstocking) หรือรายการที่เคลื่อนไหวช้า (เช่นทดสอบรายที่ค้างนาน 4-6 เดือนขึ้นไป)	9. list รายการสินค้าจาก inventory file ที่มีจำนวนคงคลังที่อยู่ในมือเกินไปเมื่อเปรียบเทียบกับจำนวนที่ขายได้ระหว่างปี
10. ทดสอบความถูกต้องของ inventory master file ทั้งหมด (overall)	10. list รายการสินค้า (ถ้ามี) ที่มีจำนวนสินค้าคงคลังติดลบหรือต้นทุนติดลบเพื่อดูความผิดปกติ

ภาคผนวก ค.
ผังแสดงขั้นตอนการแปลงโปรแกรมที่เขียนขึ้นด้วยภาษาเขียนให้เป็นโปรแกรมที่พร้อมจะทำงานได้ ขั้นตอนทดสอบการทำงานของโปรแกรมและการ Catalog โปรแกรม

(ก) ขั้นตอนการแปลงโปรแกรมที่เขียนขึ้นให้เป็นโปรแกรมพร้อมจะทำงานได้ (Translation Stage)

(ข) ขั้นตอนทดสอบการทำงานของโปรแกรม (Execution Stage)



ก. ขั้นตอนการแปลงโปรแกรมที่เขียนขึ้นให้เป็นโปรแกรมพร้อมจะทำงานได้ (Translation Stage)

เป็นขั้นตอนที่เครื่องคอมพิวเตอร์ทำการประมวลผล Source Program โดยใช้ Compiler ทำการตรวจทานประโยคคำสั่ง (Command) ต่าง ๆ และแปลงให้อยู่ในรูปของภาษาเครื่อง (Machine language) ให้พร้อมที่จะใช้งานกับเครื่องคอมพิวเตอร์ ซึ่งมีขั้นการทำงานของ Compiler อยู่ 2 ขั้นตอน ดังนี้

ขั้นตอนแรก Compiler จะแปลง Source Program ให้เป็น Object Program ชุดแรก หรือเรียกว่า Intermediate Object Program โดย Compiler จะทำการ

- ดึงประโยคต่าง ๆ ของ Source Program ซึ่งเข้ามาในรูปของ Input แล้วจัดแยกตามประเภทของประโยคเหล่านั้นออกมาและตรวจหาข้อผิดพลาดใน Source Program ตามหลักเกณฑ์ของแต่ละภาษา ถ้าพบข้อผิดพลาดเกิดขึ้นจะมีการพิมพ์เครื่องหมายในจุดที่ผิดออกมาให้เห็นเพื่อใช้หาสาเหตุและทำการแก้ไขต่อไป

- หาข้อมูลที่มีการกำหนดค่าแล้วกำหนดตำแหน่งที่อยู่ใน Memory ให้ทุกตัว
- กำหนดตำแหน่งใน Memory ให้ข้อความในประโยคต่าง ๆ ใน Source Program ทุก ๆ ตัว
- แปลงข้อความในประโยคต่าง ๆ ของ Source Program ให้อยู่ในรูปของ Object Program
- สร้างตารางสัญญลักษณ์ที่จำเป็นต้องใช้

ขั้นตอนที่สอง Compiler จะแปลง Intermediate Object Program ซึ่งเป็นผลที่ได้จากขั้นตอนแรกให้เป็น Final Object Program (หรือเรียกว่า Object Program, Absolute Program, Executable Program ก็ได้) ในขั้นตอนนี้ Compiler จะทำการ

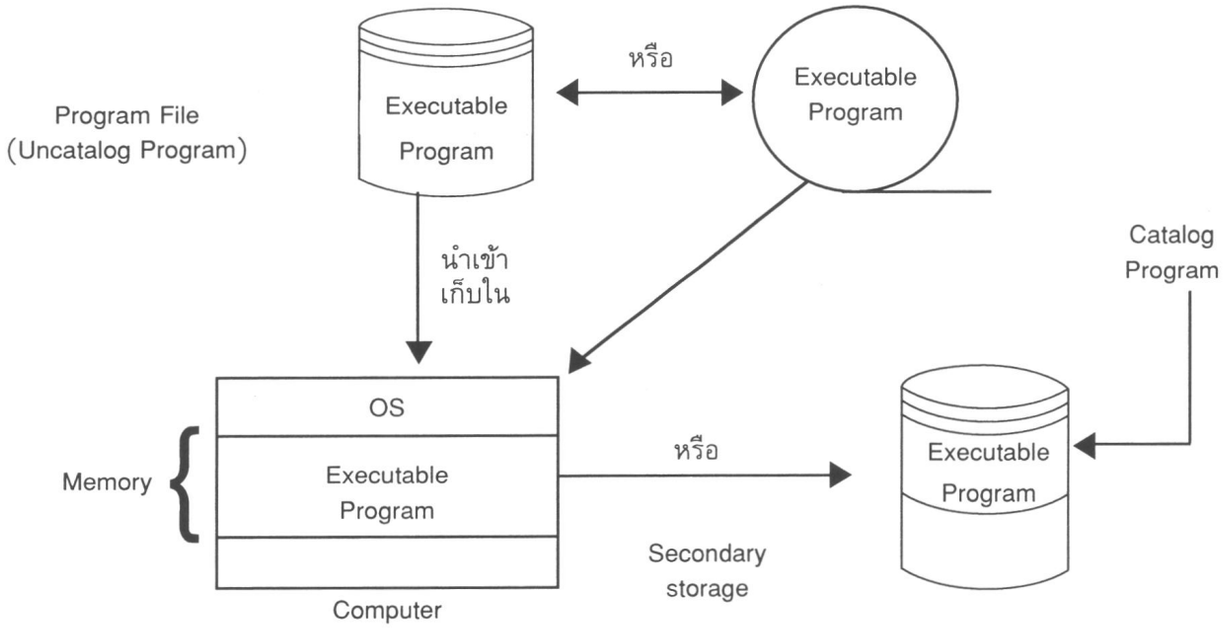
- สร้างรหัส Object
- เรียกโปรแกรมย่อย (Subroutine) ที่จำเป็นต้องใช้ทำงาน
- เรียกโปรแกรมอื่น ๆ เช่น โปรแกรมที่ใช้ในการแสดงผลของการประมวลผล Output Object Program

ข. ขั้นตอนทดสอบการทำงานของโปรแกรม (Execution Stage)

เป็นขั้นตอนของการทดสอบการทำงานของโปรแกรมที่ทำเสร็จเรียบร้อยแล้วใน Translation Stage ว่าได้ผลตรงตามเป้าหมายที่วางไว้หรือไม่

ค. การ Catalog Program

การ Catalog Program คือ การนำ Executable Program (หรือ Object Program เข้าไปเก็บไว้ในที่เก็บโปรแกรมหรือข้อมูล (System Library) ซึ่งอยู่ภายใต้การควบคุมของ Operation System ที่สามารถเรียกเข้ามาใช้งานได้ทันทีเพียงแต่เรียกชื่อโปรแกรมเท่านั้นไม่ต้องนำโปรแกรมเข้าเครื่องใหม่อีก



Catalog Program คือ Executable Program ที่ถูกนำเข้าเก็บไว้ใน System Library แล้ว ถ้าจะใช้งานก็เพียงเรียกชื่อโปรแกรมเท่านั้น ไม่ต้องนำโปรแกรมเข้าเครื่องใหม่อีก

Uncatalog Program คือ Executable Program ที่ยังไม่ถูกนำเข้าเก็บไว้ใน System Library ถ้าจะใช้โปรแกรมนี้ทำการประมวลผลทุกครั้งจะต้องนำโปรแกรมนี้เข้าเครื่องทุกครั้ง

คำอธิบาย

1. **Compiler** เป็นโปรแกรมที่บริษัทผู้ผลิตเครื่องคอมพิวเตอร์หรือกลุ่มผู้ใช้เครื่องคอมพิวเตอร์สร้างขึ้น เพื่อใช้แปลงโปรแกรมที่เขียนด้วยภาษาที่ใช้ในการเขียนโปรแกรมให้เป็นภาษาเครื่อง ซึ่งเครื่องคอมพิวเตอร์เข้าใจและสามารถทำงานได้
2. **Source Program** เป็นโปรแกรมที่ผู้เขียนโปรแกรมเขียนขึ้นด้วยภาษาเขียนและได้จัดเตรียมให้อยู่ในรูปแบบที่นำเข้าเครื่องคอมพิวเตอร์โดยอุปกรณ์นำข้อมูลเข้าได้
3. **Computer** เป็นอุปกรณ์ที่ทำหน้าที่ประมวลผลตามโปรแกรมที่ผู้เขียนโปรแกรมเขียนขึ้น ภายใต้การควบคุมของโปรแกรมควบคุมการทำงานของเครื่องคอมพิวเตอร์ (Operating System ตัวย่อ OS ซึ่งได้นำเข้าตอนการเตรียมเครื่องให้พร้อมที่จะใช้งานแล้ว)
4. **Object Program** เป็นโปรแกรมที่เครื่องคอมพิวเตอร์แปลงจาก Source Program ให้เป็นภาษาเครื่องโดยอาศัย Compiler
5. **Subroutine** เป็นโปรแกรมย่อยที่ทำงานเฉพาะอย่างได้และสามารถนำมารวมอยู่ในโปรแกรมอื่นที่ผู้เขียนโปรแกรมเขียนขึ้นใหม่ได้ เพื่อใช้ในการสั่งเครื่องคอมพิวเตอร์ให้ทำงานตามที่ต้องการ
6. **Other Program** เป็นโปรแกรมที่นอกเหนือจาก Subroutine ซึ่งอาจเป็น Operating System หรือโปรแกรมอื่นที่ไม่ได้อยู่ประจำในเครื่องคอมพิวเตอร์ แต่เกี่ยวข้องกับการทำงานของเครื่องคอมพิวเตอร์
7. **Executable Program** เป็นโปรแกรมที่ได้มาจากการแปลง Intermediate Object Program อีกครั้งหนึ่งเพื่อให้พร้อมที่จะทำงานได้ทันที ซึ่งอาจเรียกว่า Object Program ขั้นสุดท้ายก็ได้
8. **Test Data** เป็นข้อมูลที่จัดทำขึ้น ซึ่งรู้ผลลัพธ์แล้วใช้ในการทดสอบโปรแกรมแต่ละโปรแกรม (Program test) หรือใช้ทดสอบโปรแกรมทั้งหมดในระบบงานหนึ่ง ๆ (System test)
9. **Result** ผลที่ได้รับจากการทดสอบโปรแกรมหรือระบบงาน ซึ่งอาจอยู่ในรายงานตัวพิมพ์หรือทางจอแสดงผลก็ได้
10. **Secondary Storage** จะทำหน้าที่เก็บโปรแกรมในขั้นตอนต่าง ๆ แยกต่างหากออกจากกันตามคำสั่งของเครื่องคอมพิวเตอร์ ดังนี้
    - Source Library จะเป็นที่เก็บ Source program ไว้
    - Object Library หรือ Relocatable Library จะเป็นที่เก็บ Object program
    - Executable Library จะเป็นที่เก็บ Executable program

องค์ประกอบพื้นฐานทางเทคนิคของการสื่อสารข้อมูล

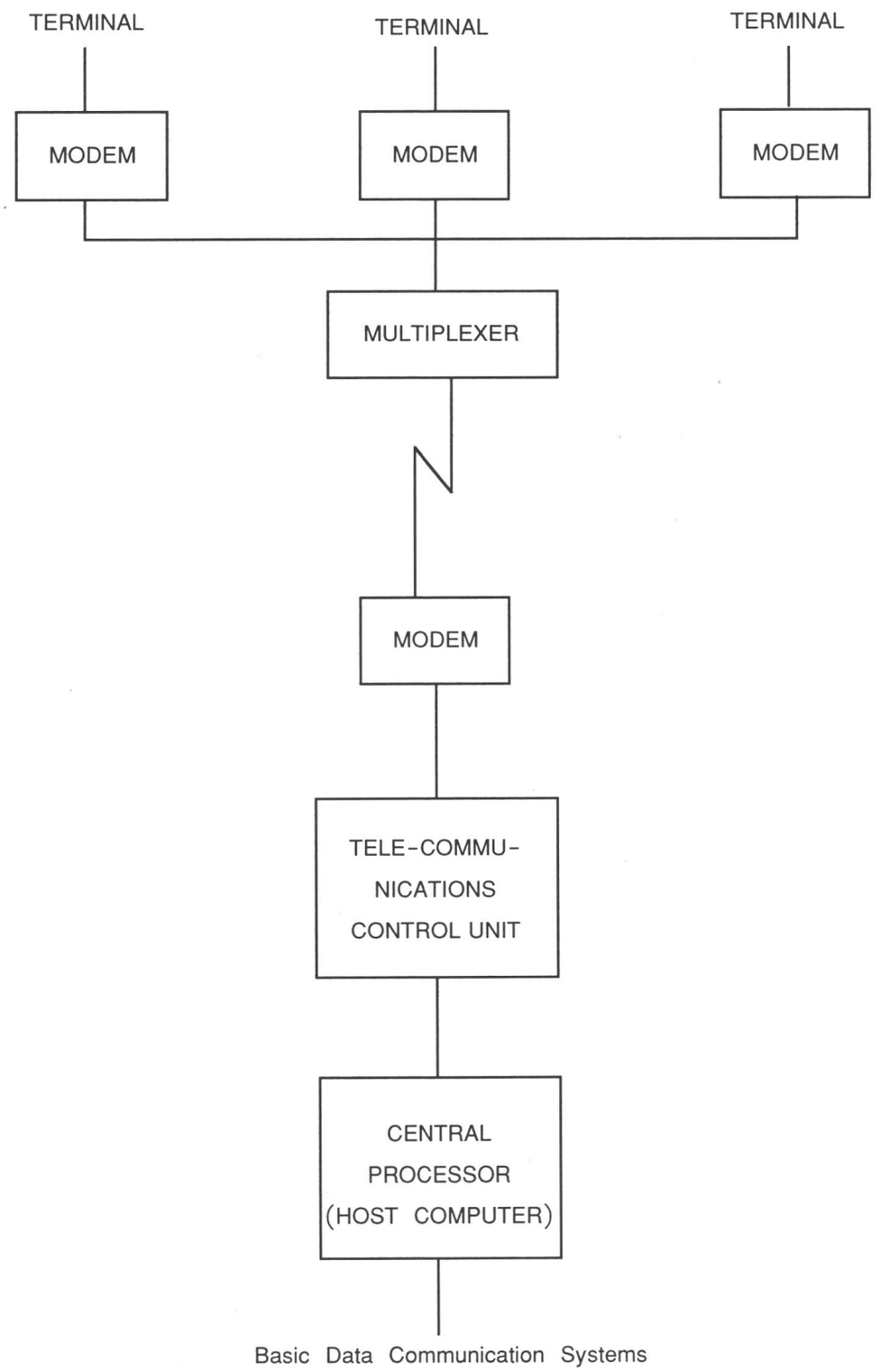
การสื่อสารข้อมูล หมายถึง การป้อนข้อมูลหรือความต้องการเข้าสู่เทอร์มินัลหรือ Personal computer ผ่านเครื่องมือสื่อสารไปยังระบบคอมพิวเตอร์ ข้อมูลที่ได้จากเทอร์มินัลจะเป็นสัญญาณไฟฟ้า (digital signals) ดังนั้นจึงต้องใช้ modem แปลงให้เป็นสัญญาณคลื่นเสียง (analog signals) เพื่อให้สามารถผ่านไปตามสายโทรศัพท์ได้ ที่ปลายทางก่อนข้อมูลเข้าไปถึงระบบคอมพิวเตอร์จะมี Modem อีกชุดหนึ่งทำหน้าที่แปลงสัญญาณคลื่นเสียงเป็นสัญญาณไฟฟ้า เพื่อให้ระบบคอมพิวเตอร์นำไปประมวลผลต่อไป เครื่องมือสื่อสารข้อมูลในระบบคอมพิวเตอร์ ได้แก่

1. Modem (Modulator-demodulator) คือ เครื่องมือสำหรับแปลงข้อมูลจากสัญญาณ Digital เป็นสัญญาณ Analog หรือกลับกัน Modem อาจรวมอยู่ในเครื่องเดียวกับเทอร์มินัลหรือเป็นอุปกรณ์ชิ้นหนึ่งในระบบสื่อสารก็ได้

2. Multiplexer คือ เครื่องมือที่ช่วยให้สามารถส่งสัญญาณข้อมูลหลายชุดไปในทิศทางเดียว แต่ใช้สายโทรศัพท์เพียงคู่สายเดียว โดยวิธีการแบ่งแถบคลื่นความถี่และแบ่งเวลาเป็นส่วนย่อย ๆ แล้วส่งข้อมูลไปพร้อม ๆ กัน

3. Telecommunications control unit หรือเรียกอีกอย่างหนึ่งว่า controller คือ เครื่องมือสื่อสารหน่วยสุดท้ายก่อนสัญญาณข้อมูลจะไปยังระบบคอมพิวเตอร์ มีลักษณะเป็นเครื่องคอมพิวเตอร์ขนาดเล็ก (minicomputer) ทำหน้าที่ควบคุมข้อมูลนำเข้าและข้อมูลผลลัพธ์ (input & output) ที่ส่งไปมาระหว่างอุปกรณ์ต่าง ๆ ในข่ายการสื่อสาร นอกจากนั้นยังทำหน้าที่หลายอย่างแทนหน่วยประมวลผลกลาง เช่น บันทึกข้อมูลเก็บไว้ในหน่วยความจำเพื่อรอส่งให้เทอร์มินัลหรือคอมพิวเตอร์ ตรวจสอบความถูกต้องของข้อมูล (parity checking และ format checking) ตามลำดับและมีวันที่กำกับข้อมูลทุกรายเพื่อป้องกันการสูญหาย และทำหน้าที่ควบคุมและตรวจสอบการทำงานของเครื่องเทอร์มินัลทุกเครื่องในเครือข่ายตามที่โปรแกรมคอมพิวเตอร์กำหนด




TERMINAL
TERMINAL
TERMINAL
MODEM
MODEM
MODEM
MULTIPLEXER
MODEM
TELE-COMMU-
NICATIONS
CONTROL UNIT
CENTRAL
PROCESSOR
(HOST COMPUTER)
Basic Data Communication Systems

ภาคผนวก ง.
แนวการตรวจสอบระบบการควบคุม
(Functional Tests : Specimen Tests)

ลักษณะของการควบคุม	แนวการตรวจสอบ
การควบคุมทางด้านผู้ใช้ (User Controls) 1. ความครบถ้วนและถูกต้องของข้อมูลนำเข้า (Input) - การตรวจสอบรายงานที่ได้จากคอม-พิวเตอร์	ก. ตรวจสอบรายงานคอมพิวเตอร์เพื่อดูหลักฐานว่า: (1) รายการหรือ Batches ที่คงค้างหรือที่คอมพิวเตอร์สอบยันยอดไม่ตรงกัน หรือที่รายการบางส่วนขาดหายไป ได้รับการเช็คสอบและแก้ไขโดยบุคคลอื่นที่มีหน้าที่รับผิดชอบโดยเอกเทศไม่เกี่ยวข้องกับการดำเนินงานดังกล่าว (2) เจ้าหน้าที่ระดับบริหารที่รับผิดชอบเป็นผู้ตรวจสอบ และรับรองความถูกต้องของผลในข้อ (1) ข. ทดสอบความถูกต้องและครบถ้วนของรายการหรือ Batches โดยการเลือกรายการหรือ Batches ที่ถูกต้องเรียบร้อยแล้วบางรายการมาเช็คสอบกับเอกสารหลักฐานที่เกี่ยวข้องว่าถูกต้องจริง
2. ความครบถ้วนและถูกต้องของการนำเข้าข้อมูล การปรับปรุง (Update) และการรักษาสภาพของข้อมูลในแฟ้มข้อมูล (Maintenance) - การเช็คสอบผลรวมข้อมูลที่คำนวณไว้แล้วด้วยมือกับผลรวมที่ได้จากรายงานคอมพิวเตอร์	ก. (1) ตรวจสอบทะเบียนหรือบัญชีคุม (Register/Control Account) เพื่อดูว่าได้มีการเช็คสอบยอดผลรวมหรือยอดคงเหลือของข้อมูลในทะเบียนหรือบัญชีคุมกับยอดรายงานการ Edit, Update และ Maintenance ที่คอมพิวเตอร์พิมพ์ออกมา โดยบุคคลอื่นที่มีหน้าที่รับผิดชอบโดยเอกเทศ (2) ตรวจสอบหลักฐานว่าผลต่างที่เกิดขึ้นได้รับการค้นหาสาเหตุและแก้ไขโดยบุคคลอื่นที่มีหน้าที่รับผิดชอบโดยเอกเทศ

ลักษณะของการควบคุม	แนวการตรวจสอบ
	(3) ตรวจสอบหลักฐานว่าผลของการปฏิบัติงานข้อ (1) และ (2) ได้รับการตรวจสอบและรับรองจากเจ้าหน้าที่ระดับบริหารที่รับผิดชอบ ข. ทดสอบความถูกต้องของยอดรวมโดยวิธีปฏิบัติงานซ้ำ (Reperform) ดังนี้ (1) ทดสอบว่ายอดรวมในทะเบียนหรือบัญชีคุมตรงกับยอดรวมที่ปรากฏในรายงานการ Edit Update หรือ Maintenance ที่คอมพิวเตอร์พิมพ์ให้ (2) ทดสอบการบวกเลขจำนวนรายการใน Batches กับจำนวนรายการข้อมูลในทะเบียนหรือบัญชีคุม ค. ทดสอบเพื่อให้แน่ใจว่ารายงานดังกล่าวไม่มีรายการข้อมูลที่ผิดพลาด โดยเลือกข้อมูลบางรายที่ประมวลผลถูกต้อง แล้วมาตรวจสอบกับเอกสารหลักฐาน เพื่อยืนยันว่าข้อมูลนั้นถูกต้องจริง
3. ความครบถ้วนและถูกต้องของการ Update รายการ - การตรวจสอบความถูกต้องของยอดรวมในรายงานคอมพิวเตอร์ด้วยมือ	ก. (1) ตรวจสอบรายงานคอมพิวเตอร์หรือทะเบียน เพื่อดูหลักฐานว่าการเช็คสอบผลรวมรายการข้อมูลนำเข้ากับผลรวมในรายงานการupdate กระทำโดยบุคคลที่มีอำนาจหน้าที่โดยเอกเทศ (2) ตรวจสอบหลักฐานว่าการค้นหาสาเหตุของผลต่าง และการแก้ไขกระทำโดยบุคคลที่มีอำนาจหน้าที่โดยเอกเทศ (3) ตรวจสอบหลักฐานว่าผลของการปฏิบัติในข้อ (1) และ (2) ได้รับการตรวจสอบและรับรองจากเจ้าหน้าที่ระดับบริหารที่รับผิดชอบ ข. ทดสอบความถูกต้องของผลรวมในข้อ (1) ข้างต้น ค. ทดสอบเพื่อให้แน่ใจว่าไม่มีข้อมูลที่ผิดพลาดหลงเหลือ โดยการเลือกรายการข้อมูลบาง

ลักษณะของการควบคุม	แนวการตรวจสอบ
	รายที่ถูกต้องแล้วจากรายงานคอมพิวเตอร์มาเช็คสอบกับเอกสารหลักฐาน เพื่อยันว่าข้อมูลทั้งหมดในรายงานนั้นถูกต้องและครบถ้วนจริง
4. ความครบถ้วนและถูกต้องของการ Update รายการ - การสอบทานการเช็คสอบความถูกต้องของผลรวมข้อมูลโดยโปรแกรมคอมพิวเตอร์ (Programmed Reconciliations) ด้วยมือ	ก. ตรวจสอบรายงานคอมพิวเตอร์เพื่อดูหลักฐานว่า (1) การตรวจสอบรายงานการเช็คสอบความถูกต้องของผลรวมข้อมูล (คอมพิวเตอร์เช็คสอบและออกรายงาน) กระทำโดยบุคคลที่มีอำนาจหน้าที่โดยเอกเทศ และการค้นหาสาเหตุและแก้ไขเป็นไปอย่างเหมาะสม (2) มีหลักฐานแสดงว่าเจ้าหน้าที่ระดับบริหารที่รับผิดชอบเป็นผู้ตรวจสอบ และรับรองผลของการตรวจสอบตามข้อ (1) ข. ทดสอบเพื่อให้แน่ใจว่าไม่มีข้อมูลที่ผิดพลาดหลงเหลืออีก โดยเลือกรายการข้อมูลบางรายที่ถูกต้องแล้วจากรายงานมาเช็คสอบกับเอกสารหลักฐานเพื่อยันว่าข้อมูลทั้งหมดถูกต้องและครบถ้วนจริง
5. ความครบถ้วนและถูกต้องของการนำเข้าข้อมูลและการปรับปรุง (Update) รายการ - การเช็คสอบรายงาน (Print-Outs) ที่คอมพิวเตอร์พิมพ์ออกมา	ก. ทดสอบวิธีการปฏิบัติที่วางไว้ เพื่อให้แน่ใจว่าเอกสารเบื้องต้นประกอบรายการข้อมูล (Source Documents) ทั้งหมดได้รับการถ่ายทอดหรือแปลงสภาพเป็นข้อมูลนำเข้า (Input) ครบถ้วน ข. ตรวจสอบบันทึก (Records) หรือแฟ้ม (File) ของ เอกสารเบื้องต้น หรือเอกสารข้อมูลนำเข้าชุดสำเนา (Input Documents) ว่ามีรายการที่ครบกำหนดแล้ว แต่ยังไม่ได้รับการนำเข้าไปประมวลหรือรายการที่ไม่สมควรอยู่หรือไม่ ค. (1) ตรวจสอบรายงานการ Update ข้อมูลเพื่อดูว่ามีการเช็คสอบด้วยวิธีใดวิธีหนึ่งหรือไม่

ลักษณะของการควบคุม	แนวการตรวจสอบ
	(2) ทดสอบความถูกต้องของการเช็คสอบรายงานตามข้อ (1) โดยเลือกรายการข้อมูลบางรายจากรายงานมาเช็คสอบกับเอกสารหลักฐาน (Original Documents) (3) ตรวจสอบรายงานการ Update หรือเอกสารหลักฐานอื่นเพื่อดูว่าผลต่างที่เกิดขึ้นได้รับการค้นหาสาเหตุและแก้ไขโดยบุคคลที่มีอำนาจหน้าที่เอกเทศ (4) ทดสอบเพื่อให้แน่ใจว่าไม่มีข้อผิดพลาดหลงเหลืออยู่ โดยเลือกรายการข้อมูลบางรายที่ถูกต้องแล้วมาเช็คสอบกับ หลักฐานว่าถูกต้องจริง
6. ความถูกต้องของข้อมูลนำเข้า - การเช็คสอบความถูกต้องของการเจาะหรือ Key รายการ (Verification of Conversion)	ก. ตรวจสอบหลักฐานดูว่าวิธีการเช็คสอบ (Verification) ที่ใช้เหมาะสม ข. เข้าไปสังเกตการณ์ในแผนกเจาะหรือ Key ข้อมูล เพื่อดูว่ามีการเช็คสอบความถูกต้องของข้อมูลในช่วง (Field) ที่จำเป็นต้องมีการควบคุม หรือไม่
7. ข้อมูลที่คอมพิวเตอร์สร้างขึ้นเองโดยอัตโนมัติตามเวลาที่กำหนด (Computer Generated Data) - การเช็คสอบความถูกต้องด้วยมือ	ก. ตรวจสอบรายงานคอมพิวเตอร์เพื่อดูว่า (1) การเช็คสอบความถูกต้องของข้อมูลกระทำโดยบุคคลที่มีอำนาจหน้าที่โดยเอกเทศ และการแก้ไขปรับปรุงรายการใด ๆ ก็ตาม กระทำโดยความเหมาะสม (2) ผลของการปฏิบัติตามข้อ (1) ได้รับการเช็คสอบ และรับรองโดยเจ้าหน้าที่บริหารที่รับผิดชอบ ข. สอบทานการเช็คสอบความถูกต้องของธนาคาร โดยทดลองเช็คสอบด้วยมือตนเอง ด้วยการเลือกรายการข้อมูลบางรายมาเช็คสอบกับเอกสาร

ลักษณะของการควบคุม	แนวการตรวจสอบ
	หลักฐานอ้างอิงว่ารายการดังกล่าวผ่านการเช็คสอบความถูกต้องหรือการปรับปรุงอย่างเหมาะสม
8. การควบคุมให้ข้อมูลในแฟ้มข้อมูลอยู่ในสภาพที่ถูกต้องและครบถ้วนอยู่ตลอดเวลา (Maintenance Control) - การจัดทำบัญชีคุมยอดคงเหลือด้วยมือ (Manual Control Account)	ก. (1) ตรวจสอบบัญชีคุมยอดคงเหลือว่ามีหลักฐานการเช็คสอบยอดคงเหลือตามบัญชีคุมกับยอดคงเหลือในแฟ้มข้อมูล (File) เป็นประจำ โดยบุคคลที่มีอำนาจหน้าที่โดยเอกเทศ และการแก้ไขและปรับปรุงผลต่างกระทำด้วยความเหมาะสมหรือไม่ (2) ตรวจสอบหลักฐานว่าผลของการปฏิบัติตามข้อ (1) ข้างบน ได้รับการเช็คสอบและรับรองโดยเจ้าหน้าที่บริหารที่รับผิดชอบ ข. ทดสอบบัญชีคุมยอดคงเหลือโดย (1) ทดสอบการจัดทำบัญชีคุมยอดคงเหลือ (2) ทดสอบว่ายอดคงเหลือในบัญชีคุมตรงกับยอดคงเหลือใน File ค. ทดสอบการปรับปรุงแก้ไขผลต่างที่เกิดขึ้นโดยเลือกรายการที่ได้รับการแก้ไขเรียบร้อยแล้วมาตรวจสอบว่ากระทำด้วยความเหมาะสม หรือไม่
9. Maintenance Control - การควบคุมความปลอดภัยของข้อมูลใน File (Computer Control Record)	ก. ตรวจสอบรายงานการพิสูจน์ยอดคงเหลือของคอมพิวเตอร์ (Computer Reconciliations) เพื่อดูว่า (1) บุคคลที่มีอำนาจหน้าที่โดยเอกเทศเป็นผู้ตรวจสอบความถูกต้องและการแก้ไขปรับปรุงผลต่างกระทำด้วยความเหมาะสม (2) ยอดคงเหลือยกมา (Brought Forward) ที่ปรากฏในรายงานการ Update แฟ้มข้อมูลหลัก (Master File) ตรงกับยอดคงเหลือยกไป (Carried Forward) ในรายงานครั้งก่อน

ลักษณะของการควบคุม	แนวการตรวจสอบ
	(3) ผลของการปฏิบัติงานตามข้อ (1) และ (2) ข้างต้นได้รับการเช็คสอบและรับรองโดยเจ้าหน้าที่ระดับบริหารที่รับผิดชอบ ข. ทดสอบการควบคุมตามวิธีในข้อ ก(2) ข้างต้น เพื่อพิสูจน์ว่ายอดคงเหลือยกมาตรงกับยอดคงเหลือครั้งก่อนยกไป ค. ทดสอบการปรับปรุงแก้ไขผลต่างที่เกิดขึ้นโดยเลือกรายการที่แก้ไขเรียบร้อยแล้วมาตรวจสอบว่ากระทำด้วยความเหมาะสมหรือไม่ ง. ในกรณีไม่มีการจัดทำรายงานการพิสูจน์ยอดให้เช็คสอบผลของการทดสอบ Integrity Control ว่าการควบคุมความปลอดภัยของ Data File ดีพอหรือไม่
10. Maintenance Control - การเช็คสอบความถูกต้องของข้อมูลชนิดถาวร (Standing Data) ที่เก็บไว้ใน File เป็นระยะ ๆ	ก. (1) ตรวจสอบรายงานคอมพิวเตอร์หรือข้อมูลเบื้องต้น (Source Data) เพื่อดูว่าการเช็คสอบอย่างละเอียดภายในขอบเขตและความถี่ที่ต้องการกระทำโดยบุคคลที่มีอำนาจหน้าที่โดยเอกเทศ และผลต่างที่เกิดขึ้นได้รับการปรับปรุงแก้ไขอย่างเหมาะสม (2) ตรวจสอบหลักฐานว่าผลของการปฏิบัติตามข้อ (1) ข้างต้น ได้รับการเช็คสอบและรับรองโดยเจ้าหน้าที่บริหาร ที่รับผิดชอบ ข. ทดสอบการควบคุมโดยเลือกรายการใน Print-out ที่มีเครื่องหมายแสดงว่าได้เช็คสอบแล้วมาตรวจสอบกับ Source Data ค. ทดสอบการปรับปรุงแก้ไขผลต่างที่เกิดขึ้นโดยเลือกรายการที่แก้ไขเรียบร้อยแล้วมาเช็คสอบว่ากระทำอย่างเหมาะสมหรือไม่

ลักษณะของการควบคุม	แนวการตรวจสอบ
11. Timing of Authorization - การเช็คสอบรายการข้อมูลที่ผ่านขั้นตอนการควบคุมข้อมูลนำเข้าแล้วอีกครั้งหนึ่ง เพื่อให้แน่ใจว่าเป็นรายการข้อมูลที่ถูกต้องจริง (Authorized Data) ทั้งหมด .	ก. ตรวจสอบหลักฐานว่าเจ้าหน้าที่ระดับบริหารที่รับผิดชอบได้เช็คสอบรายการข้อมูลที่ผ่านการทำ Batch Totals และเรียงลำดับหมายเลขแล้วอีกครั้งหนึ่ง เพื่อให้แน่ใจว่ารายการข้อมูลที่ส่งเข้าไปประมวลเป็นข้อมูลที่ถูกต้องจริงทั้งหมด ข. ทดลองเช็คสอบอีกครั้งโดยเลือกชุดข้อมูล (Current Batches) บางชุดมาตรวจสอบกับเอกสารหลักฐานที่เกี่ยวข้อง
การควบคุมโดยขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) 12. การเปรียบเทียบข้อมูลนำเข้ากับข้อมูลที่อยู่ในแฟ้มข้อมูล (Computer Matching)	ทดสอบวิธีการเปรียบเทียบโดยเลือกรายการข้อมูลบางรายเข้ากับข้อมูลที่อยู่ในแฟ้ม จากจำนวนข้อมูลทั้งหมดที่ส่งเข้าไปในคอมพิวเตอร์ และ ก. ถือไว้จนกว่าคอมพิวเตอร์จะออกรายการแจ้งข้อมูลขาดหายไปบางส่วน ข. แก้ไขข้อความบางตัว (Fields) บนเอกสารและให้ติดตามดูว่าคอมพิวเตอร์รายงานข้อมูลไม่ถูกต้องตรงกัน (Mismatched) หรือไม่
13. การเช็คสอบลำดับเลขที่ข้อมูลนำเข้า (Computer Sequence Check)	ทดสอบการเช็คสอบลำดับเลขที่ข้อมูล โดยเลือกเอกสารจากชุดข้อมูลที่กำลังส่งเข้าไปในคอมพิวเตอร์ และ ก. ยึดเอาไว้จนกว่าคอมพิวเตอร์จะออกรายงานแจ้งข้อมูลขาดหายไปบางส่วน ข. นำเอกสารนั้น key ซ้ำเข้าไปเป็นครั้งที่สอง แล้วดูว่าคอมพิวเตอร์ไม่ยอมรับรายการนั้นหรือไม่

ลักษณะของการควบคุม	แนวการตรวจสอบ
14. การเช็คสอบความถูกต้องและครบถ้วนของข้อมูลในชุด (Computer Batch Totals)	ทดสอบวิธีการเช็คสอบของคอมพิวเตอร์ โดยเลือกชุด เอกสารข้อมูลที่กำลังใช้อยู่ (Current Batches of Documents) ก. เช็คสอบการบวกเลขเอกสารข้อมูลในชุดว่าตรงกับใบปะหน้า (Batch Header) หรือไม่ ข. เปลี่ยนแปลงใบปะหน้าแล้วดูว่าคอมพิวเตอร์ออกรายงาน Rejected ข้อมูลชุดนั้นหรือไม่
15. การวางโปรแกรมให้คอมพิวเตอร์พิมพ์รายงานออกมาเมื่อมีรายการข้อมูลผิดพลาดหรือผิดปกติในการควบคุม ดังนี้ 15.1 การควบคุมความถูกต้องของการนำเข้าข้อมูลและการ Update ข้อมูล เช่น การตรวจสอบ Check Digit, Dependency Tests 15.2 การควบคุมความถูกต้องในการคำนวณ 15.3 การควบคุมสภาพของข้อมูลใน File (Maintenance of Data Stored) เช่น Dependency Tests คอมพิวเตอร์จะพิมพ์รายงานข้อมูลที่ผิดปกติเมื่อพบว่ามีรายการที่ค้างนานหรือไม่เคลื่อนไหวมาหลายงวดแล้ว	ทดสอบการรายงานของคอมพิวเตอร์ ก. เช็คสอบรายงานกับหลักฐานอ้างอิง เพื่อพิสูจน์ว่ารายการข้อมูลทั้งหมดในรายงานนั้นผ่านการ Accepted และ Rejected จากคอมพิวเตอร์อย่างถูกต้อง หรือ ข. เลือกเอกสารที่จะ Key เข้าไปในคอมพิวเตอร์บางใบออกมาแล้วแก้ไขรายละเอียดของข้อความในเอกสารนั้น แล้วให้ติดตามดูว่าคอมพิวเตอร์จะออกรายงานเป็นข้อมูลที่ไม่ถูกต้อง (Invalid or Rejected Items) หรือไม่
16. ข้อมูลที่คอมพิวเตอร์สร้างขึ้นเองโดยอัตโนมัติ (Computer Generated Data)	ทดสอบการสร้างข้อมูลดังกล่าวโดย ก. เช็คสอบกับข้อมูลเบื้องต้นเพื่อพิสูจน์ว่ารายการที่สร้างขึ้นนั้นตรงตามเวลาที่กำหนด ข. ขอรายงานพิเศษเกี่ยวกับข้อมูลที่คอมพิวเตอร์สร้างขึ้น (1) สอบยันกับข้อมูลเบื้องต้นว่า ข้อมูลทั้งหมดนั้นถูกสร้างขึ้นมาอย่างเหมาะสม (2) ดูว่ามีการรายงานข้อมูลที่ผิดปกติใน Exception Report หรือไม่

ลักษณะของการควบคุม	แนวการตรวจสอบ
17. การคำนวณของคอมพิวเตอร์ (Computer Calculating)	ทดสอบความถูกต้องในการคำนวณ โดยเลือกรายการบางรายจากรายงานคอมพิวเตอร์ (Computer Output) มาเช็คสอบผลการคำนวณ
18. การสรุปจำนวนและผลรวมของข้อมูล (Computer Summarization)	ทดสอบดูว่าผลรวมที่คอมพิวเตอร์สรุปออกมาได้รวมรายการข้อมูลทั้งหมดที่ผ่านเข้าไปและเก็บอยู่ในคอมพิวเตอร์แล้ว โดยเลือกทดสอบตามวิธีใดวิธีหนึ่งดังต่อไปนี้ ก. ถ้าในรายงานแสดงรายละเอียดข้อมูลทั้งหมดให้ตรวจสอบว่ารายงานนั้นประกอบด้วยข้อมูลที่เข้ามาในคอมพิวเตอร์ครบทุกรายการหรือไม่ และให้เช็คสอบการบวกเลขด้วย ข. กรณีในรายงานมิได้แสดงรายละเอียดข้อมูลไว้ ให้ใช้วิธี (1) ขอรายงานพิเศษเกี่ยวกับรายการข้อมูล (Printout of Transaction) แล้วดำเนินการทดสอบตามแบบ ในข้อ ก. **หรือ** (2) ทดลองส่งงานเข้าไปทำ (Run) เพื่อดูว่าผลลัพธ์ตรงกับที่ได้คำนวณไว้แล้วหรือไม่ ตัวอย่าง เช่น แยกจำนวน ข้อมูลในชุดหนึ่งออกเป็น 2 ชุดย่อย โดยให้ชุดหนึ่งใหญ่กว่าอีกชุดหนึ่ง คำนวณผลรวมของข้อมูลชุดเล็กไว้แล้วดูว่าตรงกับในรายงานการ Update หรือไม่
19. การแยกประเภทรายการและบันทึกบัญชี (Computer Categorization and Updating)	ทดสอบความถูกต้องในการผ่านบัญชี โดยเลือกข้อมูลเบื้องต้น (Source Data) บางรายมาเช็คสอบการผ่านบัญชี

ลักษณะของการควบคุม	แนวการตรวจสอบ
การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) 20. การตรวจสอบการจัดทำเอกสาร (Examination of Documentation) - System Specifications - Job Set-up and Instructions - Operating Instructions	ก. ตรวจสอบการจัดทำคู่มือประกอบ เพื่อดูว่า (1) จัดทำในรูปแบบที่เหมาะสมสำหรับใช้ในการควบคุม เช่น การอนุมัติให้ใช้โปรแกรมที่พัฒนาขึ้นใหม่ การทำ Job Set-Up (2) ถูกต้องและทันสมัย (Up to Date) ข. เลือกตัวอย่างจากเอกสารบางเล่ม และสอบถามดูว่าผู้ใช้เอกสารเหล่านั้น (User) เข้าใจความหมายและตรงตามที่ต้องการหรือไม่ ค. เลือกตัวอย่างการแก้ไขในเอกสารเหล่านั้นมาเช็คสอบกับหลักฐานว่ามีบุคคลที่มีอำนาจหน้าที่เป็นผู้เช็คสอบรายการแก้ไขนั้น
21. การทดสอบรายงานใหม่และโปรแกรมที่ได้รับการแก้ไข	ก. ตรวจสอบผลของการทดสอบและดูว่าขอบเขตและวิธีการทดสอบมีประสิทธิภาพมากเพียงพอที่จะใช้ทดสอบการทำงานตามโปรแกรม ข. เลือกขั้นตอนการทำงานตามโปรแกรมบางด้านมาทดลองทำการทดสอบเอง (1) ตรวจสอบความถูกต้องของผลลัพธ์ที่คาดการณ์ไว้ (Predicted Results) จากนั้นให้เช็คสอบผลที่ได้จากการทดสอบกับผลลัพธ์ที่คาดการณ์ไว้ (2) ขอ Program Source Listings และเช็คสอบดูว่าชุดคำสั่งงานเหมาะสมหรือไม่ (3) เลือกเวลาช่วงใดช่วงหนึ่งของการทำงานคู่ขนาน (Parallel Runnings) เพื่อเช็คสอบผลลัพธ์ที่ได้จากระบบงานใหม่กับผลลัพธ์จากระบบงานเดิม (4) เลือกการ Run งานครั้งแรก (Pilot Run) บางส่วน มาเช็คสอบผลลัพธ์ของงานนั้นกับลักษณะของผลลัพธ์ตามคำอธิบายในเอกสารประกอบระบบงาน

ลักษณะของการควบคุม	แนวการตรวจสอบ
22. การควบคุมความสมบูรณ์ (Completeness Control) - การเรียงลำดับหมายเลขเอกสารไว้ล่วงหน้า	ก. ตรวจสอบบันทึก (Records) รายการ (Lists) หรือหลักฐานอื่นเพื่อดูว่ามีการเช็คสอบแบบฟอร์มเอกสารประเภทที่มีหมายเลขเรียงลำดับไว้ เช่น แบบฟอร์มการแก้ไขโปรแกรม System Log Reports เป็นประจำหรือไม่ มอบหมายให้บุคคลที่มีอำนาจหน้าที่เป็นผู้ค้นหาสาเหตุของหมายเลขที่ขาดหายไป ข. ตรวจสอบหลักฐานว่าการเช็คสอบตามข้อ ก. ข้างต้น ได้รับการสอบทานและรับรองโดยเจ้าหน้าที่ระดับบริหารที่รับผิดชอบ ค. ทดสอบการควบคุมโดยเลือกเอกสารบางปึกมาตรวจสอบ (1) การเรียงลำดับหมายเลข (2) คำอธิบายอย่างเพียงพอสำหรับหมายเลขที่ขาด หายไป (3) เอกสารที่ถูกยกเลิกหรือเสีย ให้ติดตามดูว่าการปฏิบัติเป็นไปตามขั้นตอนที่วางไว้หรือไม่
23. การควบคุมความสมบูรณ์รายการที่บันทึกอยู่ในทะเบียน ต่าง ๆ (Entry In Register)	ก. ตรวจสอบรายละเอียดในทะเบียนว่าบันทึกรายละเอียดทันเวลาและไม่มีรายการค้างนาน ข. ตรวจสอบหลักฐานว่ามีเจ้าหน้าที่ระดับบริหารเช็คสอบ และรับรองความถูกต้องหรือไม่ ค. ทดสอบการควบคุมโดยเลือกทดสอบรายการในทะเบียนกับเอกสารหลักฐานว่ารายการที่เรียบร้อยไปแล้ว หรือคงค้างนั้นเป็นรายการที่ถูกต้องจริง ง. เช็คสอบเพื่อยืนยันว่าเอกสารที่ถูกยกเลิกหรือทำลายนั้นมีการปฏิบัติเป็นไปตามขั้นตอนที่วางไว้หรือไม่

ลักษณะของการควบคุม	แนวการตรวจสอบ
24. การควบคุมรายการคงค้าง (Outstanding Items)	ก. ตรวจสอบบันทึกเกี่ยวกับรายการค้างนาน รายการ (Lists) บันทึกความจำ (Memoranda) หรือหลักฐานอื่น เพื่อดูว่ามีการเช็คสอบเป็นประจำหรือไม่ สำหรับรายการที่ค้างนานมีบุคคลที่มีอำนาจหน้าที่เช็คสอบและหาสาเหตุของการค้างนาน และให้เจ้าหน้าที่ระดับบริหารที่รับผิดชอบสอบทานและรับรองหรือไม่ ข. ทดสอบการควบคุมโดยเช็คสอบบันทึกและขอคำอธิบายสำหรับรายการค้างนานจนเป็นที่พอใจ
25. การอนุมัติให้ใช้ระบบงานที่พัฒนาขึ้นใหม่หรือโปรแกรมที่ได้รับการแก้ไข	ก. ตรวจสอบหลักฐานดูว่าเจ้าหน้าที่ระดับบริหารที่รับผิดชอบเป็นผู้อนุมัติก่อนที่นำโปรแกรมเข้าไปบรรจุไว้ใน Library ของคอมพิวเตอร์ เพื่อนำไปใช้งานต่อไป (Cataloguing) ข. ตรวจสอบหลักฐานการไม่ยอมรับ (Rejections) หรือข้อสงสัย (Query) ของเจ้าหน้าที่ระดับบริหาร และการทดสอบระบบหรือโปรแกรมก่อนที่อนุมัติให้ใช้งานได้ ค. ทดสอบการควบคุม โดยเลือกตัวอย่างเอกสารหลักฐานตามข้อ ก. ข้างบน (1) ดูว่าการจัดทำเอกสารสนับสนุนที่สำคัญครบถ้วน เช่น ผลของการทดสอบ คำสั่งในการปฏิบัติงาน คู่มือการปฏิบัติงานของ User (2) ทดลองการทำงานขั้นตอนอื่น ๆ ที่คิดว่าเจ้าหน้าที่ระดับบริหารที่รับผิดชอบควรเอาใจใส่
26. เช็คสอบรายงานที่ได้จากคอมพิวเตอร์ - Listings From Librarian Package - System Activity Reports	ก. ตรวจสอบรายงานคอมพิวเตอร์ เพื่อดูว่า (1) มีหลักฐานแสดงว่าบุคคลที่มีอำนาจหน้าที่เป็นผู้เช็คสอบข้อความในรายงาน (Reported

ลักษณะของการควบคุม	แนวการตรวจสอบ
- Console Logs - Operating System Output	Items) เช่น รายงาน Jobs Processed Operation Action (2) ผลของการเช็คสอบตามข้อ (1) ได้รับการเช็คสอบ และรับรองจากเจ้าหน้าที่ระดับบริหารที่รับผิดชอบ ข. ทดสอบเพื่อให้แน่ใจว่ารายงานดังกล่าวไม่มีรายการผิดพลาดหลงเหลืออยู่ โดยเลือกรายการบางรายมาเช็คสอบว่ากระทำอย่างเหมาะสมหรือไม่
27. ความถูกต้องในการแก้ไข โปรแกรม (Validity of Program Changes)	ก. ตรวจสอบใบขอแก้ไข (Requests) จำนวนหนึ่งกับโปรแกรมปฏิบัติงาน และดูว่ามีการอนุมัติโดยเจ้าหน้าที่ระดับบริหารที่เหมาะสม เช่น ผู้จัดการแผนกจัดทำโปรแกรมหรือไม่ ข. เลือกใบขอแก้ไข (Requests) จำนวนหนึ่งตามข้อ ก. ข้างบน และเช็คสอบบันทึกเรื่องราวดูว่ามีเหตุผลสมควรในการแก้ไขหรือไม่
28. การควบคุมความปลอดภัยของแฟ้มข้อมูลและโปรแกรม	ก. เข้าไปในห้องคอมพิวเตอร์แล้วเช็คสอบดูว่าแฟ้มข้อมูลและโปรแกรมที่ยังมิได้นำไปใช้งาน (1) เก็บไว้อย่างปลอดภัยภายใน Library (2) การนำออกไปนอก Library ยอมให้เฉพาะบุคคล ที่ได้รับอนุญาตเท่านั้น ทั้งนี้โดยมอบหมายให้บุคคลที่มีอำนาจหน้าที่เป็นผู้ควบคุม ข. ตรวจสอบทะเบียนการนำแฟ้มข้อมูล/โปรแกรมออกไปจาก Library เพื่อดูว่ารายการที่เกินกำหนดส่งคืนแล้วได้รับการค้นหาสาเหตุโดยบุคคลที่มีอำนาจหน้าที่หรือไม่ ค. ทดสอบการควบคุม โดยเช็คสอบแฟ้มข้อมูล/โปรแกรมที่อยู่นอกห้องคอมพิวเตอร์กับทะเบียนยืมหรือใบอนุมัติ เพื่อให้แน่ใจว่า

ลักษณะของการควบคุม	แนวการตรวจสอบ
	(1) การนำออกไปได้รับการอนุมัติและบันทึกทะเบียนยืมถูกต้องเรียบร้อยแล้ว (2) ไม่เกินกำหนดส่งคืน
System Software 29. การบรรจุโปรแกรมเข้าไปเก็บไว้ใน Library (Cataloguing)	ทดสอบการ Cataloguing ระบบงานใหม่และโปรแกรมที่ได้รับการแก้ไขแล้ว โดย (ตามความเหมาะสม) ก. ขอรายชื่อโปรแกรมที่เก็บอยู่ใน Library และเช็คสอบดูว่ามีโปรแกรมใหม่ ๆ อยู่ในนั้นหรือไม่ ข. ขอ Program Source Listings แล้วเช็คสอบว่ามีคำสั่งงานที่เหมาะสม (Appropriate Instructions) หรือไม่ ค. เช็คสอบการ Cataloguing โปรแกรมสำหรับงานที่ใช้ เพื่อการตรวจสอบโดยเฉพาะ (Job Run for Audit Purposes) ง. เปรียบเทียบ Source Program ที่ใช้อยู่ในปัจจุบันกับ โปรแกรมรุ่นก่อน แล้วบันทึกข้อแตกต่างไว้ จ. ใช้ Test Data ทดสอบการทำงานของโปรแกรมใหม่ หรือที่เปลี่ยนแปลง และเช็คสอบผลลัพธ์ที่ได้รับกับผลลัพธ์ที่เตรียมไว้แล้ว
30. การจัดทำรายงานจำนวนงานทั้งหมดที่ส่งเข้าไปปฏิบัติ (Job Processed)	ทดสอบการจัดทำรายงานจำนวนงานที่ปฏิบัติ โดย ก. เปรียบเทียบรายงานกับตารางจัดงาน (Authorised Job Schedule) แล้วให้บันทึกรายละเอียดของผลต่าง ข. เช็คสอบความถูกต้องของรายงาน จำนวนงานที่ส่งเข้าไปปฏิบัติ เพื่องานการตรวจสอบโดยเฉพาะ ค. บันทึกรายละเอียดของงานทั้งหมดก่อนที่

ลักษณะของการควบคุม	แนวการตรวจสอบ
	จะส่งเข้าไปปฏิบัติ แล้วเช็คสอบว่าถูกต้องตรงกับรายงานหรือไม่
31. การเปรียบเทียบโปรแกรม (Program Comparision)	ทดสอบการเปรียบเทียบ Production Program โดยทำการเปรียบเทียบ Source Programs ที่ใช้งานอยู่กับชุดสำเนาที่เก็บไว้ต่างหากว่ามีผลต่างหรือไม่
32. การสั่งการและเช็คสอบการทำงานของโปรแกรมงาน (Supervision of Application Programs)	ในกรณีที่การตรวจสอบอย่างอื่น ด้าน Programmed Procedures ยังไม่เพียงพอ ให้ทดสอบโปรแกรมที่ทำหน้าที่สั่งการ (Supervisor Program) โดยเลือกข้อมูลบางรายการมาทดสอบว่าได้รับการปฏิบัติ (Processed) จากโปรแกรมที่เหมาะสมหรือไม่
33. การจัดทำรายงานการปฏิบัติของคอม-พิวเตอร์ (Reporting of Computer Operations)	ทดสอบการจัดทำรายงานการปฏิบัติงานโดย ก. เปรียบเทียบรายละเอียดในรายงานกับ System Log ข. เช็คสอบความถูกต้องของรายงานการใช้เครื่อง เพื่อวัตถุประสงค์ของการตรวจสอบ
34. การสร้างแฟ้มข้อมูล (File-Set-Up)	ทดสอบ Label Checking โดย ก. บันทึกรายละเอียดของรายการที่จะมีใน Files ก่อนที่จะสร้างขึ้นมาและเช็คสอบความเหมาะสม ข. เลือกแฟ้มข้อมูลที่ไม่ถูกต้องออกมาและเช็คสอบดูว่าปรากฏอยู่ในรายงานการ Rejected หรือไม่ ค. เช็คสอบความถูกต้องของรายงานการใช้ Files ของผู้ตรวจสอบ

ลักษณะของการควบคุม	แนวการตรวจสอบ
35. การใช้ Password ป้องกันการใช้คอม-พิวเตอร์โดยมิได้รับอนุญาต	ทดสอบการป้องกันโดยใส่ Password ปลอมเข้าไป แล้วดูว่าจะถูก Rejected หรือไม่
36. ทะเบียนบันทึกการใช้ Library	ทดสอบการบันทึกการใช้ Library โดย ก. เปรียบเทียบกับตารางกำหนดงาน (Authorized Job Schedule) และบันทึกผลต่างไว้ ข. เช็คสอบความถูกต้องของการจัดทำรายงานการใช้ โปรแกรมและแฟ้มข้อมูลสำหรับงานการตรวจสอบ ค. บันทึกรายละเอียดของโปรแกรมและแฟ้มข้อมูลก่อนส่งเข้าไปประมวลในคอมพิวเตอร์ แล้วเช็คสอบว่ามีรายการปรากฏอยู่ในทะเบียนการใช้ Library หรือไม่

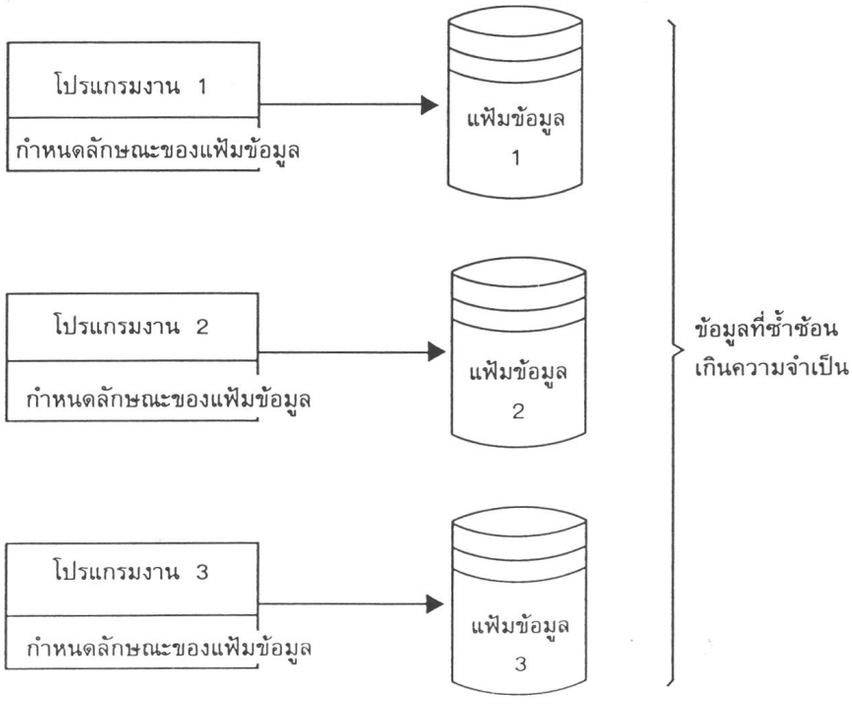
ภาคผนวก จ.
การตรวจสอบระบบฐานข้อมูล

1. คำนำ

ด้วยเหตุที่ระบบฐานข้อมูล (Database System) ได้ถูกนำเข้ามาใช้ในทางธุรกิจมากยิ่งขึ้นและด้วยเหตุที่ผู้ตรวจสอบจำเป็นต้องตรวจสอบระบบการประมวลผลข้อมูลของธุรกิจ ดังนั้น ผู้ตรวจสอบจึงจำต้องเข้าไปตรวจสอบระบบฐานข้อมูลเพื่อพิสูจน์ความถูกต้องของการประมวลผลที่ใช้ข้อมูลจากระบบฐานข้อมูลนั้น ในที่นี้จะได้ชี้ให้เห็นความแตกต่างระหว่างระบบแฟ้มข้อมูล (File System) กับระบบฐานข้อมูลซึ่งจะมีผลกระทบต่อการปฏิบัติงานของผู้ตรวจสอบ

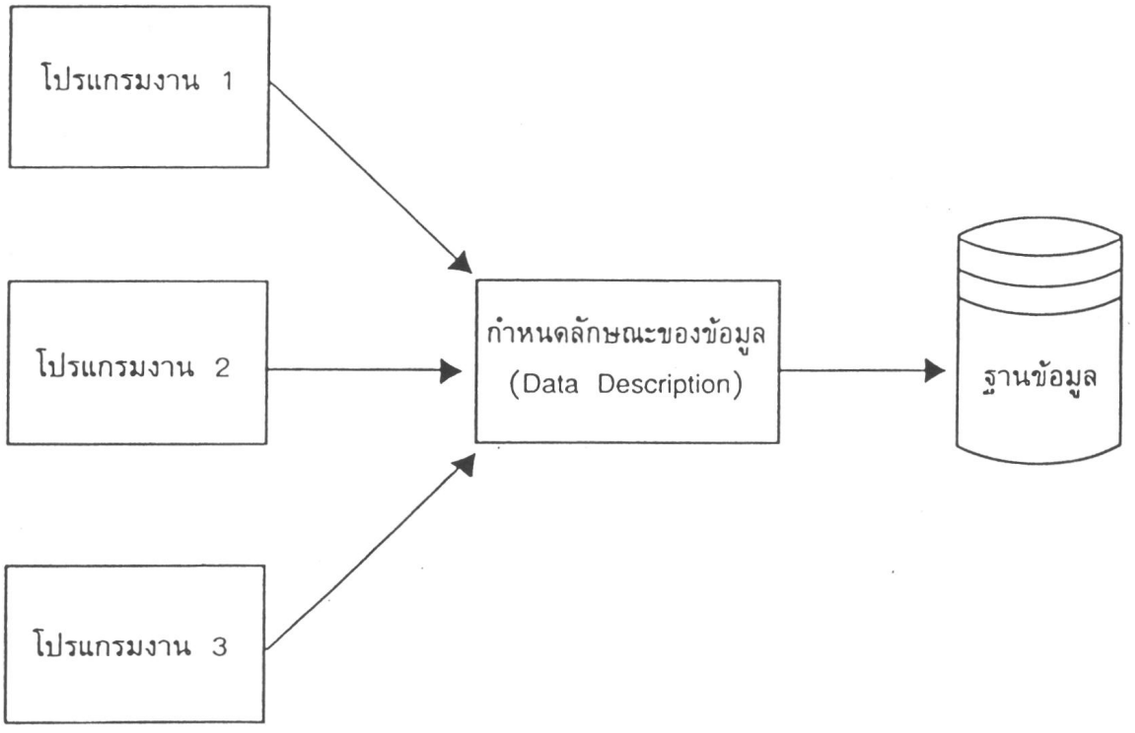
2. ความแตกต่างระหว่างระบบแฟ้มข้อมูลกับระบบฐานข้อมูล

การจัดเก็บข้อมูลในระบบแฟ้มข้อมูลจะถูกออกแบบสำหรับใช้เฉพาะงาน เช่น งานจ่ายเงินเดือน งานบัญชี งานสินเชื่อ เป็นต้น โดยจัดเก็บข้อมูลที่จำเป็นต่อการประมวลผลลงในแฟ้มข้อมูลแยกเป็นงาน ๆ ไปเช่นแฟ้มข้อมูลของระบบงานจ่ายเงินเดือนจะประกอบด้วยข้อมูลที่ใช้ในการคำนวณเงินได้สุทธิของพนักงาน และยอดเงินสะสมฯ ซึ่งไม่สามารถนำไปใช้ประมวลผลกับระบบงานอื่น เช่น งานสินเชื่อหรืองานเงินฝากได้โดยตรง เนื่องจากการจัดองค์ประกอบภายในแฟ้มข้อมูล และการใช้อุปกรณ์ที่จัดเก็บข้อมูลจะถูกกำหนดไว้สำหรับโปรแกรมงานที่ใช้แฟ้มข้อมูลนั้น โดยเฉพาะหากจะนำแฟ้มข้อมูลไปใช้กับระบบงานอื่นอาจจำเป็นต้องทำการประมวลผลเพื่อปรับปรุงแฟ้มข้อมูลหรือจัดรูปแบบของแฟ้มข้อมูลใหม่ นอกจากนี้ประสิทธิภาพในการประมวลผลอาจลดลงด้วย



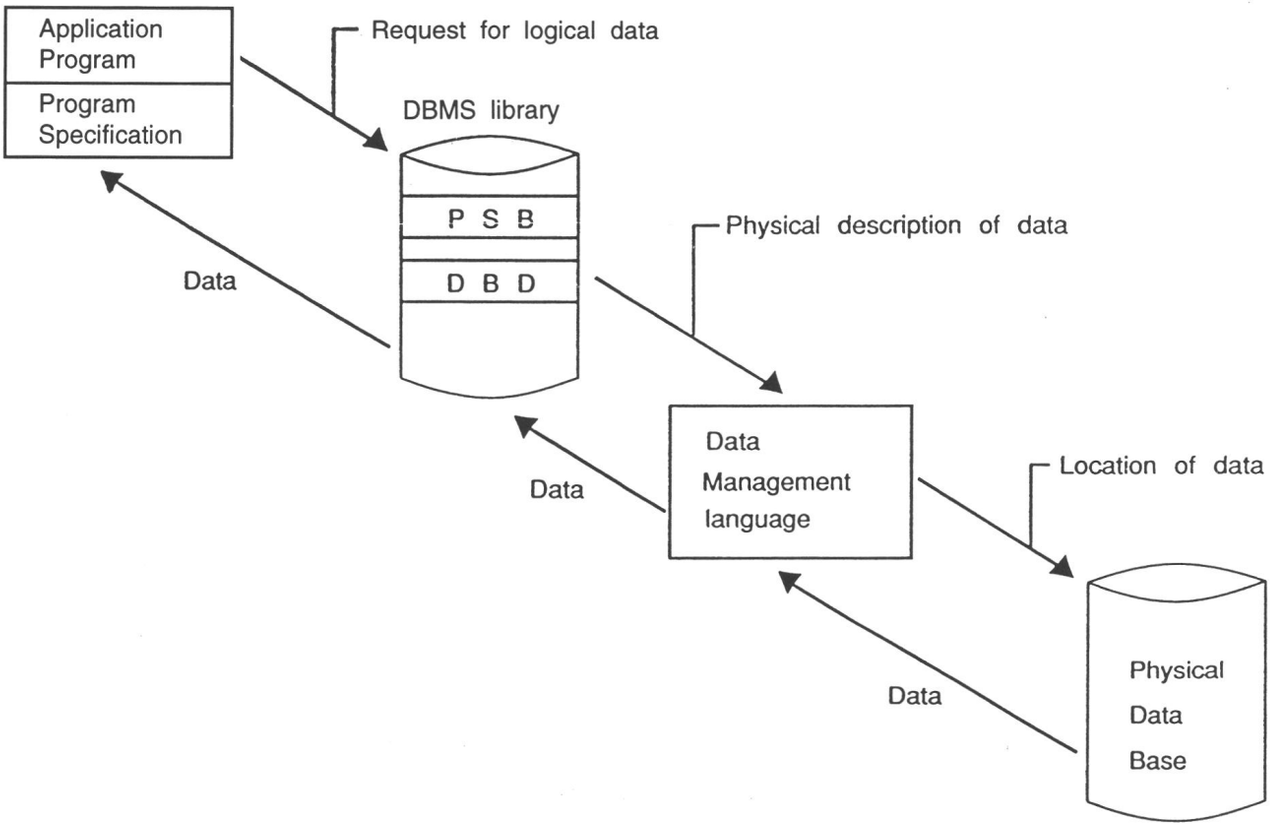
รูปแบบของลักษณะโดยทั่วไปของระบบแฟ้มข้อมูล ซึ่งแต่ละงานจะมีแฟ้มข้อมูลไว้ใช้โดยเฉพาะ และการจัดเก็บข้อมูลของแต่ละแฟ้มจะไม่สัมพันธ์กัน หรืออาจจะสัมพันธ์กันโดยบังเอิญแต่ไม่มีหลักเกณฑ์ที่แน่นอน

ระบบฐานข้อมูลจะช่วยให้การประมวลผลในระบบงานต่าง ๆ มีประสิทธิภาพเพราะใช้ฐานข้อมูลเดียวกัน ข้อมูลที่เคยกระจัดกระจายอยู่ในแฟ้มข้อมูลต่าง ๆ จะถูกรวบรวมเก็บไว้ในแฟ้มข้อมูลเพียงชุดเดียวอย่างมีหลักเกณฑ์ ลดความซ้ำซ้อนในการจัดเก็บข้อมูล สำหรับโปรแกรมที่ใช้กับระบบฐานข้อมูลจะมีลักษณะแตกต่างไปจากโปรแกรมที่ใช้กับระบบแฟ้มข้อมูลเพียงเล็กน้อย คือแทนที่จะมีการกำหนดลักษณะของแฟ้มข้อมูล (File Description) ไว้ในโปรแกรมเพื่อใช้อ้างอิงเหมือนในระบบแฟ้มข้อมูล กลับใช้วิธีกำหนดลักษณะของข้อมูลหรือบรรยายลักษณะของข้อมูล (Data Description) เพื่อประโยชน์ในการอ้างอิงไว้ในระบบฐานข้อมูลสำหรับเชื่อมโยงติดต่อระหว่างโปรแกรมที่ใช้ประมวลผลกับข้อมูลแต่ละรายการและสามารถใช้ Data Description นี้จำกัดขอบเขตการใช้ข้อมูลของแต่ละโปรแกรมด้วย



แผนภาพแสดงลักษณะโดยทั่วไปของระบบฐานข้อมูล

สำหรับโปรแกรมงานที่จะเข้าไปใช้ฐานข้อมูล จะต้องแสดงข้อมูลที่จำเป็นต้องใช้ไว้ในส่วนที่บรรยายลักษณะเฉพาะของโปรแกรม ซึ่งบริษัท IBM เรียกว่า Program Specification Block (PSB) เพื่อให้ระบบควบคุมฐานข้อมูล (Data Base Management System = DBMS) ใช้ค้นหาชื่อโปรแกรมและข้อมูลที่โปรแกรมนั้นมีสิทธิใช้ซึ่งเก็บไว้ในอุปกรณ์จัดเก็บข้อมูล (Library) เกี่ยวกับโปรแกรมที่ได้รับการอนุมัติให้ใช้ฐานข้อมูลเมื่อพบว่าโปรแกรมนั้นสามารถใช้ฐานข้อมูลได้ระบบควบคุมฐานข้อมูลจะค้นหาตำแหน่งของข้อมูลที่โปรแกรมต้องการใช้จาก DataBase Description (DBD) และอาศัย Data Management Language Processor (DL/I) ให้ช่วยดำเนินการเกี่ยวกับการนำข้อมูลในระบบมาใช้ประมวลผล



แผนภาพแสดงการทำงานของระบบฐานข้อมูล

ส่วนที่ต้องควบคุมอย่างเข้มงวดคือ DBMS Library เพราะเป็นที่เก็บรายละเอียดของโปรแกรมและฐานข้อมูล นอกจากนี้ระบบฐานข้อมูลจะจัดข้อมูลในระบบให้โปรแกรมที่รับการอนุมัติให้ใช้ระบบทันทีที่โปรแกรมเหล่านั้นเรียกใช้โดยอัตโนมัติ จึงควรจัดระบบรักษาความปลอดภัยเพื่อควบคุมการใช้ข้อมูลในระบบให้รัดกุมที่สุด

3. การตรวจสอบ

ในการสอบทานระบบประมวลผล ผู้ตรวจสอบควรประเมินการควบคุมทั่วไป (General Controls) และการควบคุมเฉพาะงาน (Application Controls) ในระบบฐานข้อมูลของธนาคารมีความเหมาะสมและเชื่อถือได้เพียงใด

การควบคุมทั่วไปเกี่ยวกับการพัฒนาและการบำรุงรักษาโปรแกรมในระบบฐานข้อมูลจะแตกต่างไปจากระบบแฟ้มข้อมูล แต่อาจนำวิธีการควบคุมพื้นฐาน เช่น การอนุมัติคำขอแก้ไขโปรแกรม การปรับปรุงเอกสาร การทดสอบโปรแกรม การจัดระบบสำรอง และการเตรียมรับเหตุฉุกเฉิน ที่เคยใช้ในระบบแฟ้มข้อมูลมาปรับปรุงใช้กับระบบฐานข้อมูลและเพิ่มเติมวิธีการควบคุมบางอย่างได้ตามความเหมาะสม การแก้ไขโครงสร้างของโปรแกรมและการแก้ไขคำสั่งบางคำสั่งเพื่อเพิ่มประสิทธิภาพในการประมวลผล หรือแก้ไขข้อผิดพลาดที่พบในประโยคคำสั่งของโปรแกรมในระบบแฟ้มข้อมูลอาจไม่มีผลกระทบต่อแฟ้มข้อมูล แต่การแก้ไข Program Specification ของโปรแกรมสำหรับติดต่อกับระบบฐานข้อมูลเพื่อให้ DBMS จัดข้อมูลที่ใช้ในการประมวลให้จะมีผลกระทบต่อการใช้ข้อมูลในระบบด้วย ดังนั้น จึงจำเป็นต้องมีการควบคุมการอนุมัติและตรวจสอบการแก้ไขโปรแกรมที่รัดกุมและเหมาะสมมากขึ้น

เนื่องจากโปรแกรมงานในระบบฐานข้อมูลสามารถใช้ข้อมูลได้หลายรายการ และการใช้ข้อมูลของโปรแกรมต่าง ๆ มักจะมีผลกระทบตามมาอยู่เสมอ เช่น การเปลี่ยนแปลงข้อมูลพนักงานที่ปลดเกษียณ โดยวิธีลบหมายเลขประจำตัวพนักงานที่เกษียณอายุออกจากระบบฐานข้อมูลเพื่อควบคุมจำนวนพนักงานที่ธนาคารโอนเงินเดือนเข้าบัญชีเงินฝากของพนักงาน อาจมีผลกระทบต่อข้อมูลที่เกี่ยวกับเงินสะสมของพนักงานด้วยจึงจำเป็นต้องมีพนักงานบริหารงานฐานข้อมูล (Data Base Administrator = DBA) ควบคุมการปรับปรุงและการพัฒนาโปรแกรมซึ่งเป็นการควบคุมทั่วไปโดยใกล้ชิด

การควบคุมการใช้ข้อมูลในระบบฐานข้อมูลจะแตกต่างกับระบบแฟ้มข้อมูลมากในระบบแฟ้มข้อมูลจะมีแฟ้มข้อมูลสำหรับใช้กับโปรแกรมงานแต่ละงานโดยตรง จึงอาจใช้วิธีการควบคุมแบบ Physical Control ที่สามารถสัมผัสได้เพราะการจัดองค์ประกอบของข้อมูลไม่สลับซับซ้อนและไม่สัมพันธ์กับงานอื่น โดยปกติจะมอบให้พนักงานจัดเก็บข้อมูล (Librarian) เป็นผู้ควบคุมการจัดส่งแฟ้มข้อมูลไปประมวลผลและควบคุมการปฏิบัติงานของผู้ใช้เครื่องคอมพิวเตอร์ (Operator) ในการใช้แฟ้มข้อมูลตามตารางการประมวลผลรวมทั้งควบคุมการใช้เอกสารสนับสนุนการปฏิบัติงานอย่างใกล้ชิดส่วนในระบบฐานข้อมูลการควบคุมการใช้ข้อมูลจะยุ่งยากกว่าระบบแฟ้มข้อมูลมากและไม่สามารถใช้ Physical Control ได้มากนักเพราะโปรแกรมงานต่าง ๆ สามารถใช้ข้อมูลในระบบได้คล้าย ๆ กัน และข้อมูลเหล่านี้จะถูกเก็บไว้กับเครื่องอยู่ตลอดเวลา จึงจำเป็นต้องมอบหมายหน้าที่ในการควบคุมดูแลฐานข้อมูลให้

แก่โปรแกรมสำเร็จรูป DBMS ซึ่งจำเป็นต้องมีการบำรุงรักษาเช่นเดียวกับโปรแกรมสำเร็จรูปอื่น ๆ โดยอาจกำหนดเป็นตารางไว้หรือไม่ก็ได้แล้วแต่ความเหมาะสม ในกรณีที่ DBMS เสียหายหรือไม่สามารถนำมาใช้ควบคุมการใช้ฐานข้อมูลได้ และจำเป็นต้องใช้ฐานข้อมูลในการประมวลผล ควรทำสำเนาข้อมูลที่จะถูกลบทิ้งหรือนำไปใช้ประมวลผลเก็บไว้ตรวจสอบการใช้ข้อมูลและควรหาวิธีป้องกันการใช้ฐานข้อมูลเกินอำนาจที่ได้รับมอบหมายด้วย

การควบคุมทั่วไปเกี่ยวกับการจัดองค์กรและการดำเนินงานเป็นการควบคุมเพื่อให้แน่ใจว่าการประมวลผลของโปรแกรมเป็นไปตามวิธีการที่ได้รับอนุมัติ เช่น การควบคุมการปฏิบัติงานด้วยมือหรือโดยบุคคล การควบคุมการปฏิบัติงานของพนักงานในห้องคอมพิวเตอร์ในแต่ละงาน การควบคุมการบำรุงรักษาระบบงาน การตรวจสอบรายงานการใช้ระบบคอมพิวเตอร์ที่คอมพิวเตอร์พิมพ์ให้โดยอัตโนมัติ เป็นต้น การควบคุมดังกล่าวมีความสำคัญต่อการประมวลผลทั้งในระบบแฟ้มข้อมูลและระบบฐานข้อมูล แต่ในระบบฐานข้อมูลจำเป็นต้องมีพนักงานบริหารงานฐานข้อมูลรับผิดชอบการปรับปรุงแก้ไขข้อมูลในระบบ และจัดหาหรือจัดซื้อโปรแกรมสำเร็จรูปเพื่อทำการวิเคราะห์โครงสร้าง Logical PSD และข้อกำหนดต่าง ๆ ในระบบฐานข้อมูลโดยละเอียดนอกจากนี้ผู้บริหารงานฐานข้อมูลควรตรวจสอบรายงานการใช้ฐานข้อมูลที่คอมพิวเตอร์พิมพ์ให้โดยอัตโนมัติอยู่เสมอรายงานดังกล่าวควรมีรายละเอียดเกี่ยวกับการแก้ไขข้อมูลในระบบ โปรแกรมที่ใช้ข้อมูลและขอบเขตการใช้ฐานข้อมูล เพื่อให้แน่ใจว่าโปรแกรมดังกล่าวไม่ได้ใช้ข้อมูลในระบบเกินอำนาจที่ได้รับมอบหมาย และการแก้ไขข้อมูลในระบบได้ผ่านการอนุมัติแล้ว

4. การควบคุมระบบฐานข้อมูล

การควบคุมระบบฐานข้อมูลแบ่งได้ 4 หัวข้อ คือ

- การแบ่งแยกความรับผิดชอบ
- การใช้ข้อมูล
- การปฏิบัติงานประมวลผล
- โปรแกรมใช้งาน

4.1 การแบ่งแยกความรับผิดชอบ

การแบ่งแยกความรับผิดชอบในที่นี้หมายถึง การจัดให้มีการแบ่งแยกหน้าที่ของผู้วิเคราะห์ระบบงาน ผู้เขียนโปรแกรมใช้งาน และผู้ปฏิบัติงานประมวลผล เช่น เดียวกับในระบบแฟ้มข้อมูลรวมทั้งการจัดองค์กรควบคุมตามความจำเป็นโดยมีผู้บริหารงานฐานข้อมูล (DBA) รับผิดชอบเกี่ยวกับ

- การกำหนดลักษณะเฉพาะ (Definition)
- การจัดองค์กร
- การป้องกันภัย

- การใช้ฐานข้อมูลให้มีประสิทธิภาพ
- การควบคุม
- ให้คำแนะนำในการเลือกใช้อุปกรณ์เครื่องมือและโปรแกรม
- การจัดทำแผนและโครงสร้างของฐานข้อมูล
- การจัดทำเอกสาร
- เป็นที่ปรึกษาของผู้ใช้ฐานข้อมูล
- การกำหนดวิธีการรักษาความปลอดภัย
- การเตรียมรับเหตุฉุกเฉินในกรณีที่ฐานข้อมูลถูกทำลาย
- การติดตามและตรวจสอบการใช้ฐานข้อมูล

สำหรับการควบคุมโดยองค์กร (Organizational Controls) ที่ควรใช้มี ดังนี้

(1) ห้าม DBA เข้าห้องคอมพิวเตอร์และใช้เครื่องมือหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยมิได้รับอนุญาต ทั้งนี้เพราะ DBA เป็นบุคคลเพียงคนเดียวที่มีความรอบรู้เกี่ยวกับข้อมูลที่เก็บไว้ในระบบ (DBMS Library) และโปรแกรมที่ใช้ปฏิบัติงานทุกโปรแกรม ซึ่งอาจนำไปใช้ให้เป็นประโยชน์แก่ตนเองได้โดยง่าย

(2) กำหนดให้ DBA เป็นผู้มีอำนาจอนุมัติในการแก้ไข DBMS Library และควรห้ามผู้เขียนโปรแกรมใช้งานแก้ไข DBMS Library ด้วย

(3) หากมีการสร้างรายการใหม่ DBA ต้องขอความเห็นชอบจากผู้ใช้ข้อมูลทุกครั้ง

(4) ในระบบแฟ้มข้อมูลมีการควบคุมมิให้ผู้เขียนโปรแกรมรู้เห็นรายละเอียดอื่น ๆ ในระบบงานนอกเหนือไปจากรายละเอียดที่จำเป็นต้องใช้ในการเขียนโปรแกรมของตน แต่ในระบบฐานข้อมูลจะต้องมีการควบคุมที่เข้มงวดกว่าในระบบแฟ้มข้อมูล เพราะไม่สามารถควบคุมหรือจัดเก็บตัวอุปกรณ์ที่เป็นแฟ้มข้อมูลได้เหมือนระบบเก่า

4.2 การควบคุมการใช้ข้อมูล

การนำเอาวิธีการควบคุมตัวอุปกรณ์ที่บันทึกข้อมูลและการควบคุมโดยองค์กรที่เคยใช้ในระบบแฟ้มข้อมูลมาใช้กับระบบฐานข้อมูลอาจไม่ได้ผลเต็มที่จึงจำเป็นต้องใช้วิธีการควบคุมอื่น ๆ มาช่วย ดังนี้

(1) ควรมอบหมายให้ DBA เป็นผู้ควบคุมดูแลการใช้โปรแกรมเอนกประสงค์ที่ใช้ช่วยในการประมวลผล (Utility Program) เช่นพิมพ์รายละเอียดเกี่ยวกับลักษณะของข้อมูล (Database Descriptions) หรือการทดสอบภาษาที่ใช้ควบคุมการถ่ายเทข้อมูล (Data Manipulation Language) ซึ่งอาจช่วยให้สามารถใช้ฐานข้อมูลในส่วนที่ไม่มีสิทธิใช้ได้

(2) ในกรณีที่ไม่สามารถใช้โปรแกรม DBMS ควบคุมการใช้ฐานข้อมูลที่ติดตั้งค้างไว้กับเครื่องคอมพิวเตอร์ได้ควรหาวิธีการควบคุมอื่น ๆ ที่เหมาะสมมาใช้ทดแทน

(3) DBA ควรตรวจสอบรายงานการปฏิบัติงานประมวลผล (Operating System Log) และรายงานการใช้ฐานข้อมูล (DBMS Log) อยู่เสมอโดยตรวจสอบการใช้โปรแกรมที่ได้รับอนุมัติให้ใช้ประมวลผลกับตารางการประมวลผล ซึ่งอาจทำได้โดยง่ายหากมีโปรแกรมช่วยสรุปผลให้

(4) DBA ควรควบคุมและอนุมัติการใช้ Utility Program ในการบำรุงรักษาฐานข้อมูลหรือทำงานอื่นที่มีลักษณะใกล้เคียงกันเช่นการบรรจุ (Loading) ฐานข้อมูลเข้าสู่ระบบคอมพิวเตอร์ และการลบข้อมูลที่ไม่ต้องการออกจากระบบ เพราะการปฏิบัติงานดังกล่าวจะทำให้ผู้ปฏิบัติทราบโครงสร้างของระบบฐานข้อมูลโดยละเอียด

(5) ควรแยกฐานข้อมูลชุดจริงกับชุดที่ใช้ทดสอบโปรแกรมออกจากกันเพื่อให้แน่ใจว่าข้อมูลที่ใช้งานจริงไม่ถูกเปลี่ยนแปลงด้วยโปรแกรมทดสอบ

4.3 การควบคุมการปฏิบัติงานประมวลผล

ในระบบแฟ้มข้อมูลและในระบบฐานข้อมูล มีการควบคุมการปฏิบัติงานประมวลผลที่คล้าย ๆ กัน เช่น มีการควบคุมวิธีการทำงานทั้งในส่วนที่ทำด้วยมือหรือใช้บุคคลปฏิบัติ (Manual) และส่วนที่ต้องปฏิบัติตามข้อกำหนด (Operating Instruction) ของแต่ละโปรแกรมการควบคุมการปฏิบัติงานตามตารางที่กำหนดและการควบคุมเมื่อเกิดเหตุฉุกเฉิน เป็นต้น แต่อย่างไรก็ดีเพื่อความรัดกุมควรนำวิธีการควบคุมต่อไปนี้มาใช้ในระบบฐานข้อมูลด้วย

(1) เพื่อให้แน่ใจว่าโปรแกรมใช้งานเข้าไปใช้ข้อมูลในระบบเฉพาะรายการที่ได้รับอนุมัติ ควรให้ DBA เป็นผู้อนุมัติและบันทึกการแก้ไขข้อมูลไว้ทุกครั้ง

(2) เพื่อให้แน่ใจว่าข้อมูลในระบบไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต DBA ควรตรวจสอบDBMS Library เป็นครั้งคราว

(3) DBA ควรตรวจสอบรายงานการใช้โปรแกรมในการประมวลผล และการใช้ Program Specification ของโปรแกรมต่าง ๆ เป็นครั้งคราว เพื่อให้แน่ใจว่าการใช้ข้อมูลในระบบเป็นไปตามข้อกำหนดที่ได้รับอนุมัติในแต่ละโปรแกรม นอกจากนี้ยังช่วยให้ทราบการเปลี่ยนแปลงชั่วคราวใน DBMS Library เช่น รายละเอียดเกี่ยวกับการใช้ Program Specification ที่ยังไม่ได้รับอนุมัติให้ใช้ประมวลผลและการเคลื่อนย้ายรายการเป็นการชั่วคราวเป็นต้น

(4) ควรกำหนดให้มีการขอความเห็นชอบจาก DBA ทุกครั้งที่มีการปรับปรุงแก้ไขโปรแกรม DBMS ที่สำคัญ ทั้งนี้ เพราะ DBA เป็นผู้ที่รอบรู้ระบบ DBMS เป็นอย่างดี สามารถควบคุมการใช้ข้อมูลและทราบผลกระทบที่มีต่อความถูกต้องของข้อมูล หากมีการปรับปรุงแก้ไขโปรแกรม DBMS ในส่วนใดก็ตามแต่ในกรณีที่บริษัทผู้ขายโปรแกรมสำเร็จรูปปรับปรุงแก้ไขคำสั่งที่ผิดพลาดเพียงเล็กน้อยอาจไม่จำเป็นต้องดำเนินการควบคุมตามที่กล่าวข้างต้นก็ได้

4.4 การควบคุมโปรแกรมที่ใช้ประมวลผล

การควบคุมโปรแกรมที่ใช้ประมวลผลในระบบฐานข้อมูลมีลักษณะเหมือนกับระบบแฟ้มข้อมูล คือมีการควบคุมเอกสารเกี่ยวกับโปรแกรมการทดสอบโปรแกรมการจัดระบบสำรองเตรียมรับเหตุฉุกเฉิน และวิธีแก้ปัญหาเมื่อเกิดความเสียหาย อย่างไรก็ดี ควรจัดให้มีการควบคุมเพิ่มเติมในระบบฐานข้อมูลดังนี้

(1) ควรมีมาตรฐานการเขียนโปรแกรมเป็นลายลักษณ์อักษรกำหนดชนิดของคำสั่งที่สามารถเรียกใช้ข้อมูลในระบบ (Type of Data Manipulation Language = DML) เพื่อทราบลักษณะการทำงานของคำสั่งโปรแกรมที่ถูกควบคุมโดย DBMS Return Codeและควรจำกัดการใช้ Call ของ DML เช่น คำสั่งที่เกี่ยวกับการสอดแทรกข้อมูล (Insert) การสับเปลี่ยนหรือแทนที่ข้อมูล (Replace) และการลบข้อมูล (Delete) ด้วยโดยปกติ DBMS Return Code จะแสดงเงื่อนไขที่ผิดพลาดในระบบฐานข้อมูลให้ทราบ จึงควรจัดทำโปรแกรมที่เหมาะสำหรับนำไปใช้กับ DBMS Return Code เพื่อให้แน่ใจว่าจะสามารถตรวจจับข้อผิดพลาดในการประมวลผลได้

(2) DBA ควรตรวจทานการจัดทำเอกสารประกอบโปรแกรมใช้งานให้ครบถ้วนตามมาตรฐานที่กำหนดไว้ให้เสร็จเรียบร้อยก่อนที่นำโปรแกรมออกใช้งาน ความสมบูรณ์ของเอกสารที่ใช้ในระบบฐานข้อมูลเป็นเรื่องที่สำคัญยิ่งเพราะข้อมูลที่ใช้งานทั่ว ๆ ไปในระบบจะถูกโปรแกรมต่าง ๆ หลายโปรแกรมนำไปใช้ประมวลผล และ DBA สามารถพิจารณาได้ว่าโปรแกรมใหม่ที่จะนำมาใช้ประมวลผลหรือโปรแกรมที่มีการเปลี่ยนแปลงแก้ไขจะมีผลกระทบต่อโปรแกรมอื่นที่ใช้ฐานข้อมูลร่วมกันเพียงใด

(3) ควรมีมาตรฐานการทดสอบโปรแกรมเกี่ยวกับการสร้างข้อมูลสำหรับการทดสอบ การตรวจสอบผลการทดสอบ การจัดเก็บข้อมูลที่ใช้ทดสอบ และผลการทดสอบไว้เป็นหลักฐาน

(4) ควรตรวจสอบการจัดระบบสำรองเตรียมรับเหตุฉุกเฉินและวิธีแก้ไขความเสียหายที่เกิดขึ้นก่อนที่จะนำระบบงานออกใช้ เช่นเดียวกับระบบแฟ้มข้อมูลโดยทดสอบการทำงานเพื่อให้แน่ใจว่าระบบสำรองและวิธีการดังกล่าวที่เตรียมไว้สามารถทำงานได้ตามที่กำหนดไว้ ซึ่งมีความสำคัญต่อระบบฐานข้อมูลเป็นอย่างมาก เพราะหากมีโปรแกรมหนึ่งโปรแกรมใดในระบบไม่สามารถทำงานได้ตามปกติจะมีผลกระทบต่อโปรแกรมอื่น ๆ ในระบบที่ใช้ข้อมูลชุดเดียวกับโปรแกรมนั้นด้วย

5. สรุป

การเปลี่ยนแปลงเทคนิคในการจัดเก็บข้อมูลจากระบบแฟ้มข้อมูลซึ่งเหมาะสำหรับประมวลผลในแต่ละงานไปเป็นการจัดเก็บข้อมูลในระบบฐานข้อมูลซึ่งโปรแกรมต่าง ๆ หลาย ๆ งานสามารถใช้ข้อมูลในระบบร่วมกันได้ ทำให้ลักษณะการประมวลผลเปลี่ยนแปลงไปด้วยการควบคุมและตรวจสอบในระบบฐานข้อมูลจะต้องรัดกุมและเข้มงวดกว่าระบบแฟ้มข้อมูล เพราะการใช้ข้อมูลในระบบในแต่ละครั้งจะมีผลกระทบต่อการประมวลผลในงานอื่น ๆ ด้วย

ภาคผนวก ฉ.
การใช้ตัวอย่างข้อมูลทดสอบการประมวลผล

1. วัตถุประสงค์และขอบเขตของการใช้ Audit Test Data

วัตถุประสงค์สำคัญของการใช้ Audit Test Data คือ เพื่อทดสอบขั้นตอนการทำงานต่าง ๆ ของโปรแกรม และเพื่อทดสอบประสิทธิภาพของระบบงานที่แท้จริง นอกจากนั้นยังสามารถใช้ Audit Test Data ทดสอบขั้นตอนการทำงานของโปรแกรมที่เกี่ยวเนื่องกัน และช่วยให้งานที่ทำอยู่นั้นถูกต้องยิ่งขึ้นด้วย

Audit Test Data คือ ข้อมูลที่ไม่ได้ใช้งานจริงซึ่งผู้ตรวจสอบได้จัดเตรียมไว้เพื่อประโยชน์ในการตรวจสอบ โดยป้อนข้อมูลเหล่านี้เข้าไปในเครื่องคอมพิวเตอร์เพื่อดำเนินการประมวลผลโดยใช้โปรแกรมปฏิบัติงานจริงของธนาคาร แล้วนำผลลัพธ์ที่ได้ (Output) มาเปรียบเทียบกับผลลัพธ์ที่ผู้ตรวจสอบคำนวณไว้ล่วงหน้าก่อนแล้ว

Audit Test Data มีลักษณะแตกต่างกับ Test Data ของธนาคารที่จัดทำไว้เพื่อทดสอบการทำงานของโปรแกรมปฏิบัติงานที่เขียนขึ้นใหม่ ซึ่งเป็นข้อมูลที่ใช้ทดสอบรายละเอียดต่าง ๆ ของโปรแกรมโดยทั่วไป ข้อมูลทดสอบประเภทนี้จึงไม่ได้เป็นตัวแทนข้อมูลที่จะแสดงให้เห็นว่าคอมพิวเตอร์ทำงานได้อย่างถูกต้องและเชื่อถือได้

สำหรับ Audit Test Data เป็นข้อมูลที่ใช้ทดสอบเฉพาะบางขั้นตอนของโปรแกรมที่ผู้ตรวจสอบต้องการความแน่ใจเท่านั้น ในการออกแบบข้อมูลประเภทนี้ควรกำหนดให้มีลักษณะใกล้เคียงกับข้อมูลที่ใช้ประมวลผลจริง ๆ ของธนาคาร และเป็นตัวแทนของข้อมูลที่มีผลกระทบต่องบการเงินของธนาคารอย่างแท้จริง

สิ่งสำคัญในการใช้ Audit Test Data ก็คือ ต้องทำการทดสอบกับโปรแกรมที่ใช้ปฏิบัติงานจริงในขณะนั้น สำหรับขั้นตอนการทดสอบกับโปรแกรมที่แท้จริงนั้นจะกล่าวในเรื่อง การสอบยันเพื่อให้แน่ใจว่าได้มีการใช้โปรแกรมที่ใช้งานจริงในการทดสอบในหัวข้อที่ 3

เมื่อได้ตัดสินใจใช้ Audit Test Data ทดสอบเฉพาะขั้นตอนใดขั้นตอนหนึ่งของโปรแกรมเป็นพิเศษแล้ว ควรรวมการทดสอบขั้นตอนอื่น ๆ ที่ทำการทดสอบได้ด้วยมือ ซึ่งเป็นวิธีปฏิบัติที่มีประสิทธิภาพ และควรระมัดระวังไม่ให้ข้อมูลที่ใช้ในการทดสอบมีรายละเอียดที่ยุ่งยากและสลับซับซ้อนมากเกินไป

2. ปริมาณของรายการ Volume of Transaction

จำนวนรายการที่ประมวลผลอย่างน้อยควรมีเพียงพอที่จะทดสอบการปฏิบัติงานครบทุกขั้นตอน ดังนั้นข้อมูลตัวอย่างที่คัดเลือกมาใช้ทดสอบควรเป็นตัวแทนของประเภทรายการที่สำคัญ ๆ

ในการพิจารณาประเภทของรายการที่ใช้ทดสอบ จำเป็นต้องคำนึงถึงขนาด (Size) ของรายการแต่ละรายการที่นำไปประมวลผลด้วย เพื่อให้แน่ใจว่ารายการที่ใช้ทดสอบโปรแกรมรายการเดียวกันนั้นให้ผลลัพธ์ได้แตกต่างกันหลาย ๆ แบบ ในกรณีดังกล่าวปริมาณของรายการที่ใช้ทดสอบต้องมีมากพอที่จะครอบคลุมการแสดงผลลัพธ์ได้หลาย ๆ อย่างด้วย

การทดสอบข้อมูลจะทำได้ง่ายและประหยัดมากขึ้น เมื่อทำการทดสอบเพียง 2-3 รายการ โดยการใช้รายการที่สามารถทดสอบเงื่อนไข (Condition) ต่าง ๆ ได้มากกว่าหนึ่งเงื่อนไข ซึ่งจะช่วยให้จำนวนรายการที่ทำการทดสอบลดน้อยลง

วิธีการที่สะดวกคือ การใช้ตาราง Matrix เพื่อแสดง Records ที่บันทึกไว้ใน Master Files และรายการ (Transactions) ที่จะใช้ในการทดสอบขั้นตอนต่าง ๆ ของโปรแกรม ในบางกรณีที่มีความจำเป็นต้องใช้ปริมาณรายการทดสอบจำนวนมาก หรือเมื่อปรากฏว่าโปรแกรมที่ทดสอบไปแล้วนั้นผู้ตรวจสอบยังมีความสนใจอยู่อีก เพื่อประหยัดค่าใช้จ่ายควรใช้ Test Data Generator สร้างรายการที่ทดสอบให้

Test Data Generator เป็นโปรแกรมสำเร็จรูปที่ใช้สร้างข้อมูลเพื่อทำการทดสอบโปรแกรมที่ใช้ปฏิบัติงานหรือสร้าง Master File จำลองแบบของจริง โดยผู้ใช้ข้อมูลเป็นผู้กำหนดลักษณะข้อมูลที่ต้องการก่อน แล้วจึงให้โปรแกรมดังกล่าวสร้าง File ข้อมูลที่ใช้ในการทดสอบ พร้อมทั้งพิมพ์รายละเอียดของข้อมูลที่ถูกสร้างขึ้นให้แก่ผู้ใช้ข้อมูลที่ถูกสร้างขึ้นมาด้วย

3. วิธีการประมวลผลด้วย Audit Test Data (Methods of Running Audit Test Data)

วิธีการใช้ Audit Test Data ตรวจสอบมีอยู่ 2 วิธี คือ วิธี “Dead” และ “Live”

3.1 การตรวจสอบวิธี Dead คือ การใช้ข้อมูลที่ใช้ในการทดสอบประมวลผลร่วมกับ Master File ชุดที่สำเนามาจาก Master File ที่ใช้งานจริง หรือ Dummy File ที่จัดทำขึ้นเพื่อใช้ทดสอบโดยใช้โปรแกรมปฏิบัติงานจริงของธนาคารเป็นการประมวลผลแยกต่างหากจากการประมวลผลจริง

3.2 การตรวจสอบวิธี Live คือ การใช้ข้อมูลที่ใช้ในการทดสอบประมวลผลในเวลาเดียวกันกับการจัดทำข้อมูลใช้งานจริงของธนาคาร โดยใช้ Master File ตัวจริงร่วมประมวลผลด้วย ซึ่งโดยปกติมักจะกันหรือสร้างข้อมูล (Records) ใน Master File ไว้ชุดหนึ่งโดยเฉพาะเพื่อใช้ในการทดสอบ การตรวจสอบในลักษณะวิธี Live นี้เรียกได้อีกอย่างหนึ่งคือ Integrated Test Facility (ITF)

การใช้ Audit Test Data ทั้งวิธี “Dead” และ “Live” จะมีทั้งข้อดีและข้อเสีย ข้อเสียของวิธีหนึ่งจะเป็นข้อดีของอีกวิธีหนึ่ง ในทางปฏิบัติข้อดีของการใช้วิธี “Live” จะมีข้อดีกว่า “Dead”

องค์ประกอบที่ใช้ในการตัดสินใจเลือกใช้วิธี "Dead" หรือ "Live" มีดังนี้คือ

- อุปสรรคในการประมวลผล
- ความสะดวกในการที่จะบรรลุวัตถุประสงค์ของการตรวจสอบ
- ความสลับซับซ้อนในการจัดทำ Audit Test Data
- การสอบยันเพื่อให้แน่ใจว่าได้มีการใช้โปรแกรมที่ใช้งานจริงในการทดสอบ
- เวลาในการใช้เครื่องคอมพิวเตอร์

(1) อุปสรรคในการประมวลผล

การทดสอบด้วยวิธี "Live" ในเวลาเดียวกับการปฏิบัติงานจริงนั้น จะทำให้การประมวลผลยุ่งยากมาก

ส่วนอุปสรรคในการทดสอบด้วยวิธี "Dead" นั้นเกิดจากความพยายามที่จะใช้ข้อมูลเพียงเล็กน้อยสร้างรายการที่ผิดปกติลงใน Master File และต้องควบคุมให้ข้อมูลเหล่านี้ถูกประมวลผลในช่วงกลางของการประมวลผลด้วย นอกจากนี้ความยุ่งยากในการทดสอบจะมากขึ้นหากต้องขยายระยะเวลาในการประมวลผลเพื่อทดสอบอีก 2-3 ครั้ง

สำหรับการใช้ Test Data ตรวจสอบการประมวลผลในระบบ On-line หรือ Real-time จำเป็นต้องใช้วิธี "Live" ในการตรวจสอบ เนื่องจากไม่สามารถดำเนินการทำสำเนาข้อมูลในระบบดังกล่าวทั้งระบบเพื่อนำมาใช้ทดสอบการประมวลผลตามวิธี "Dead" ได้

(2) ความสะดวกในการที่จะบรรลุวัตถุประสงค์ของการตรวจสอบ

ปัญหาที่จะกล่าวต่อไปนี้เป็นปัญหาที่เกิดขึ้นในกรณีที่ตรวจสอบด้วยวิธี "Live" และจะไม่พบปัญหาเหล่านี้เมื่อตรวจสอบด้วยวิธี "Dead" มีดังนี้

- ปัญหาในการคาดคะเนผลลัพธ์ และปัญหาในการหลีกเลี่ยงผลกระทบด้านอื่น
- ปัญหาในการทดสอบยอดรวม (Total) และหรือการวิเคราะห์ตัวเลข คือ ในขณะที่ Test Data ถูกนำไปรวมกับข้อมูลใช้งานจริง (Actual Data) จะไม่สามารถคำนวณยอดรวม (Total) ที่ได้จากการประมวลผลไว้ล่วงหน้าได้ แต่อาจแก้ปัญหาได้ด้วยการสร้างข้อมูลสำหรับทดสอบสาขาที่เป็น Dummy
- ปัญหาในการบันทึกข้อมูลที่ใช้ในการทดสอบ ซึ่งมิใช่ข้อมูลจริงปะปนกับรายการบัญชี (Accounting Records) ของธนาคารตอนสิ้นปี ถ้าเป็นรายการที่ไม่ค่อยมีความสำคัญมากนักก็น่าจะทำได้ แต่ผู้ตรวจสอบน่าจะเลือกใช้วิธีแทรกข้อมูลที่ใช้ในการทดสอบและล้างรายการเหล่านี้ให้หมดก่อนการปิดบัญชี

- ปัญหาในการทิ้ง Audit Test Data ค้างไว้ในระบบงานเป็นระยะเวลานานเพื่อทดสอบการประมวลผลให้ครบทุกขั้นตอน ในกรณีนี้จำเป็นต้องทำแผนด้วยความระมัดระวัง

(3) ความสลับซับซ้อนในการทำ Audit Test Data

การจัดทำข้อมูลเพื่อใช้ทดสอบโดยวิธี "Live" จะง่ายกว่าวิธีอื่น เพราะเป็นระบบที่ทำได้ง่าย โดยเพียงแต่จัดเตรียมข้อมูลจำลองขึ้นเท่านั้นก็ใช้ได้ ส่วนวิธี "Dead" จำเป็นต้องสร้าง Master Files จำลอง เพื่อใช้ทดสอบร่วมกับ Test Data ด้วย

(4) การสอบยันเพื่อให้แน่ใจว่าได้มีการใช้โปรแกรมที่ใช้งานจริงในการทดสอบ

องค์ประกอบในหัวข้อนี้ไม่ต้องพิจารณาเมื่อทดสอบด้วยวิธี "Live" เนื่องจากโปรแกรมที่ใช้ทดสอบอยู่เป็นโปรแกรมที่ใช้งานจริงของธนาคารอยู่แล้ว แต่ถ้าทดสอบด้วยวิธี "Dead" จำเป็นต้องยืนยันให้ได้ว่าโปรแกรมที่ใช้ทดสอบนั้นเป็นโปรแกรมใช้งานจริง โดยการเปรียบเทียบชื่อและลำดับเลขที่ของโปรแกรมที่คอมพิวเตอร์บันทึกไว้ในระบบ (System log) หากการควบคุมเกี่ยวกับการใช้โปรแกรมในการประมวลผลไม่น่าเชื่อถือหรือมีจุดอ่อน หรือผิดสังเกต ต้องให้เครื่องคอมพิวเตอร์พิมพ์หรือแสดงชื่อและเลขที่โปรแกรมในขณะทำการทดสอบด้วย

(5) เวลาในการใช้เครื่องคอมพิวเตอร์

องค์ประกอบในหัวข้อนี้ไม่ต้องพิจารณาเมื่อทดสอบด้วยวิธี "Live" แต่ถ้าทดสอบด้วยวิธี "Dead" องค์ประกอบการพิจารณานี้จะมีความสำคัญมาก เมื่อต้องขอเวลาใช้เครื่องคอมพิวเตอร์มักมีอุปสรรคเกิดขึ้นเสมอ โดยเฉพาะอย่างยิ่งในระบบ On-line และ Real-time

4. กระบวนการใช้ Test Data

สิ่งที่ควรพิจารณาในการใช้ Audit Test Data มีดังนี้คือ

(ก) ความสลับซับซ้อนทางด้านเทคนิค

(ข) ความเอาใจใส่และความร่วมมือของธนาคารที่มีต่อผู้ตรวจสอบ

(ค) ผลกระทบด้านอื่นที่อาจมีผลต่อธนาคาร

(ง) วิธีปฏิบัติที่แตกต่างกัน

(จ) ความจำเป็นในการจัดให้มีศูนย์รวบรวมประสบการณ์ในการใช้ Audit Test Data เพื่อช่วยให้การใช้ข้อมูล การกำหนดวัตถุประสงค์ในการทดสอบ การจัดทำข้อมูล และการจัดทำงบประมาณค่าใช้จ่าย เป็นไปด้วยความเหมาะสม

การจัดทำกระบวนการใช้ Audit Test Data ควรทำเป็นมาตรฐานเดียวกัน โดยพิจารณาการใช้ Audit Test Data แยกเป็นการใช้ในปีแรก ปีที่สอง และปีต่อ ๆ ไป ดังนี้

4.1 การใช้ Audit Test Data ในปีแรก

ผู้ตรวจสอบควรพิจารณาจากลักษณะการทำงานของโปรแกรมที่ต้องการตรวจสอบว่า การใช้ Audit Test Data เป็นวิธีที่ให้ผลดีที่สุดที่ควรจะใช้ทดสอบหรือไม่ โดยมองดูขั้นตอนต่าง ๆ ของโปรแกรมในระบบนั้นอย่างกว้าง ๆ แล้วจึงตัดสินใจเลือกเทคนิคและจำนวนขั้นตอนที่จะทดสอบด้วยการใช้ Audit Test Data ต่อไป

การจัดทำรายงานเสนอใช้ (Proposal) Audit Test Data และขอความเห็นชอบจากผู้ร่วมรับผิดชอบงานตรวจสอบ ควรมีรายงานดังนี้

(ก) รายละเอียดขั้นตอนที่ทดสอบและเหตุผลที่ต้องใช้ Audit Test Data

(ข) กำหนดว่าจะใช้ Audit Test Data ตรวจสอบด้วยวิธี "Live" หรือ "Dead" (ถ้ากำหนดว่าจะตรวจสอบด้วยวิธี "Live" ควรแสดงวิธีการแก้ไขผลกระทบที่อาจเกิดขึ้นด้วย และถ้ากำหนดว่าจะตรวจสอบด้วยวิธี "Dead" ก็ควรแสดงรายละเอียดประมาณการระยะเวลาที่จำเป็นต้องใช้เครื่องคอมพิวเตอร์ไว้ด้วยเช่นกัน

(ค) รายละเอียดของ record ใน Master File ที่สร้างขึ้นใช้ทดสอบ พร้อมทั้งปริมาณและชนิดของข้อมูลที่ทดสอบ (ตามตาราง Matrix จะแสดงรายการที่ทดสอบขั้นตอนต่าง ๆ ของโปรแกรมแต่ละรายการว่าทดสอบอะไรบ้าง)

(ง) รายละเอียดงบประมาณรายจ่ายของการใช้ Audit Test Data ในปีแรกและปีต่อ ๆ ไป

(จ) รายการแสดงผลการทดสอบโดยใช้ Audit Test Data

(ฉ) อุปสรรคต่าง ๆ ในการปฏิบัติงานที่คาดว่าจะมี

หลักการใช้ Audit Test Data ในการตรวจสอบ ควรสอดคล้องกับระเบียบปฏิบัติของธนาคาร ธนาคารจำเป็นอย่างยิ่งที่ต้องระมัดระวังแผนงานของผู้ตรวจสอบ เพื่อให้แน่ใจว่าจะไม่เกิดผลกระทบด้านอื่น ๆ ต่อธนาคาร โดยเฉพาะอย่างยิ่งการทดสอบด้วยวิธี "Live" ดังนั้นเพื่อความเหมาะสมจึงควรทราบระเบียบปฏิบัติ วัตถุประสงค์ที่กำหนดไว้ การจัดเวลา วิธีปฏิบัติเกี่ยวกับการใช้ Test Data และสิ่งอำนวยความสะดวกต่าง ๆ ที่จะใช้ได้ เช่น เครื่องเจาะบัตร หรือเวลาใช้เครื่องคอมพิวเตอร์

ผู้ตรวจสอบควรจัดเตรียมกระดาษทำการให้พร้อม รวมทั้งจัดทำผลลัพธ์ที่ควรจะได้จากการประมวลผลไว้ล่วงหน้า และตารางการประมวลผลข้อมูล ให้เสร็จเรียบร้อยก่อนที่จะดำเนินการตรวจสอบและใช้เครื่องคอมพิวเตอร์ทำงาน Test Data เพื่อความสะดวกในการใช้ Test Data ควรปรับปรุงแผนงานและรายการทดสอบการทำงาน (Functional Tests) ด้วย ถ้าจำเป็นต้องเปลี่ยนแปลง Test Data ควรกระทำด้วยความรอบคอบและควรตรวจเช็คอุปกรณ์ที่ใช้ในการป้อนข้อมูลด้วย เพื่อหลีกเลี่ยงข้อผิดพลาดที่อาจเกิดขึ้น

เมื่อประเมินผลการตรวจสอบได้แล้ว หากมีเวลาว่างควรเตรียมจัดทำรายงานการตรวจสอบ ซึ่งประกอบด้วยเรื่องเหล่านี้ คือ

(ก) ข้อเสนอที่ให้เลือกใช้ในการตรวจสอบ

(ข) ข้อบกพร่องที่พบในการทดสอบการทำงานของโปรแกรม

(ค) อุปสรรคที่เกิดขึ้นและข้อเสนอแนะในการแก้ไขอุปสรรคเหล่านั้น

(ง) ข้อเสนอแนะเพื่อให้มีการทดสอบขั้นตอนการทำงานของโปรแกรมที่จำเป็นต้องทดสอบในครั้งต่อไปให้มากขึ้น

(จ) ข้อมูลที่แสดงว่าเอกสารประกอบ Audit Test Data ที่ใช้อยู่นี้สมบูรณ์และทันเวลา

(ฉ) ค่าใช้จ่ายการจัดเตรียมและทดสอบ Audit Test Data ที่เกิดขึ้นจริง และคำชี้แจงเหตุผลที่ค่าใช้จ่ายที่เกิดขึ้นจริงแตกต่างจากงบประมาณที่ตั้งไว้

4.2 การใช้ Audit Test Data ในปีที่สองและปีต่อ ๆ ไป

กระบวนการใช้ Audit Test Data ในปีที่สองและปีต่อ ๆ ไป ส่วนใหญ่จะมีลักษณะคล้ายคลึงกัน คือ แทนที่จะทำ Audit Test Data ขึ้นใหม่ ผู้ตรวจสอบเพียงแต่แก้ไขข้อมูลบางอย่างที่จำเป็นเพื่อให้แน่ใจได้ว่าข้อมูลนั้นจะไม่ถูกส่งคืนกลับมาเพราะไม่ถูกต้อง ตัวอย่างเช่น การแก้ไขวันที่ของเอกสารประกอบ ข้อควรระวังคือต้องแน่ใจว่าระบบงาน (system) ไม่มีการเปลี่ยนแปลงไปจากเดิม หรือถ้ามีการเปลี่ยนแปลงก็ควรแก้ไข Audit Test Data ให้เหมาะสม ข้อเสนอและรายงานควรจัดเตรียมเฉพาะส่วนที่เปลี่ยนแปลงจากปีก่อนเท่านั้น อย่างไรก็ดีควรปรับปรุงแผนการใช้ Audit Test Data กับธนาคารอีกครั้ง



ภาคผนวก ช.
ตัวอย่างการใช้ตัวอย่างข้อมูลทดสอบการประมวลผล

ระบบงานเงินเดือน

1. ระบบงาน

ธนาคารมีพนักงานทั้งหมด 5,000 คน และจัดทำใบจ่ายเงินเดือนด้วยเครื่องคอมพิวเตอร์ รายละเอียดพนักงานเข้าใหม่ พนักงานที่ลาหยุดงาน และการแก้ไขเปลี่ยนแปลงข้อมูลหลักจะถูกนำเข้าประมวลผลและตรวจสอบด้วยมือในแต่ละสัปดาห์ ชั่วโมงการทำงานจะบันทึกเก็บไว้ในบัตรลงเวลาทำงาน (clock cards) และส่งเป็นข้อมูลเข้าประมวลผลทุกสัปดาห์

นอกเหนือจากการคำนวณเงินที่จ่าย ทำใบจ่ายเงินเดือน และบันทึกรายการเงินได้พนักงานแล้ว คอมพิวเตอร์ยังจัดทำรายงานต่อไปนี้ให้อีกด้วย คือ

(ก) รายงานการแก้ไขข้อมูลหลัก
(ข) รายงานรายชื่อพนักงานที่ไม่มีบัตรลงเวลาทำงาน
(ค) รายงานรายชื่อพนักงานที่มีบัตรลงเวลาทำงานมากกว่า 1 บัตร (เมื่อเกิดกรณีดังกล่าวนี้บัตรลงเวลาทั้งหมดของพนักงานเหล่านี้จะถูกส่งคืน)
(ง) รายงานบัตรลงเวลาทำงานที่เลขประจำตัวพนักงานไม่ถูกต้อง
(จ) รายงานพนักงานที่มีชั่วโมงการทำงานรวมเกินกว่า 60 ชั่วโมง
(ฉ) รายงานพนักงานที่มีเงินได้เบื้องต้นเกินกว่า 1,500 บาทต่อสัปดาห์
(ช) รายงานพนักงานที่มีเงินได้เบื้องต้นรวมค่าล่วงเวลาในสัปดาห์เกินกว่า 2,500 บาท
(ซ) ตารางการผ่านบัญชีแยกประเภททั่วไป

2. การตรวจสอบด้วย Test Data

วัตถุประสงค์ของการตรวจสอบและรายละเอียดของ Test Data จะอยู่ในตาราง Matrix ซึ่งประกอบด้วย 2 ส่วน คือ

(1) ตารางสรุปข้อมูลที่ต้องการทดสอบ (Summary of Data Requirements)

วัตถุประสงค์ของตารางสรุปนี้ก็เพื่อแสดงจำนวนรายการที่ต้องการตรวจสอบด้วย Audit Test Data ตามตารางแสดงรายละเอียด บรรทัดบนแสดงรายละเอียดของรายการข้อมูลพนักงานใน Master File ที่ต้องใช้ทดสอบ สำหรับหัวข้อในแนวยืนเป็นรายละเอียดของรายการทั้งข้อมูลหลักและข้อมูลที่เปลี่ยนแปลง (standing and

transaction data) ที่ใช้ประมวลผลการทดสอบ รายการดังกล่าวจะแทรกเพิ่มเข้าไปเพื่อแสดงผลกระทบและการเปลี่ยนแปลงรายการข้อมูลใน Master File ที่จะเกิดขึ้น คอลัมภ์ขวาสุดแสดงยอดรวมข้อมูลที่ต้องการทดสอบ สำหรับตารางประกอบนี้ต้องการตัวอย่างข้อมูลทดสอบเพื่อสร้าง Master File จำนวน 10 รายการ รายการแก้ไขข้อมูลหลัก 10 รายการและบัตรลงเวลาทำงาน 10 บัตร

(2) ตารางประมวลผลข้อมูลและขั้นตอนการทดสอบ (Data Processed and Procedures Tested)

วัตถุประสงค์ของตารางนี้ก็เพื่อแสดงว่าขั้นตอนในการทดสอบการประมวลผลรายการต่าง ๆ อย่างไรบ้าง จึงจะทำให้วัตถุประสงค์ของการตรวจสอบด้วยตัวอย่างข้อมูลทดสอบสำเร็จลงได้ รายการข้อมูลใน Master File ที่คงเหลืออยู่หลังผ่านขั้นตอนการทดสอบแล้วจะมีจำนวนรายการที่จะประมวลผลทดสอบต่อไปลดลงด้วย เช่น พนักงานที่ลาหยุดงานจะถูกตัดออกจาก Master File ในการนำไปประมวลผลทดสอบขั้นต่อไป ทำข้อรายการในแนวยืนนี้จะถูกเปลี่ยนเป็นหัวข้อย่อย ๆ (จากตารางสรุปแรก) เพื่อเป็นหัวข้อรายการทดสอบตามขั้นตอนที่กำหนดเพื่อช่วยให้ตาราง Matrix ง่ายต่อการเข้าใจ จึงได้แสดงรายการข้อมูลใน Master ที่ยังคงใช้ทดสอบต่อไปอีก หลังจากทดสอบแต่ละกลุ่มเรียบร้อยแล้ว ตามตัวอย่างนี้คือ หลังจากขั้นตอนทดสอบการแก้ไขข้อมูลหลักขั้นตอนหนึ่งแล้ว และหลังจากขั้นตอนทดสอบความสมบูรณ์และถูกต้องของข้อมูลจากบัตรลงเวลาทำงานอีกขั้นตอนหนึ่ง มีข้อสังเกตว่าเมื่อแสดงรายการข้อมูลใน Master File อีกครั้งหลังจากขั้นตอนทดสอบความสมบูรณ์และถูกต้องของข้อมูลจากบัตรลงเวลาทำงานแล้ว จะไม่แสดงรายการเหล่านั้นอีกเมื่อข้อมูลนั้นไม่ใช้อีกต่อไป

ระดับของการแสดงการทดสอบนี้มีวัตถุประสงค์เพื่อเป็นการอธิบายประกอบอย่างเดียวเท่านั้น

ตารางสรุปข้อมูลที่ต้องการทดสอบ

	พนักงานที่ทดสอบ												รวม
	1	2	3	4	5	6	7	8	9	10	11	12	
คัดเลือกข้อมูลใน Master file ที่ใช้ทดสอบ													
Master file ค่าจ้าง	–	–	*	*	*	*	*	*	*	*	*	*	10
รายการแก้ไขข้อมูลหลัก													
พนักงานเข้าใหม่	*	*											2
พนักงานที่ลาหยุดงาน			*	*									2
เงินจ่ายเพิ่ม					*								1
การเปลี่ยนรหัสภาษี						*							1
รายการหักเพิ่มเติม							*						1
ลบล้างรายการหักครั้งก่อนออก								*					1
ข้อมูลที่มีการเปลี่ยนแปลง													
บัตรลงเวลาทำงาน	*	–	*	–	–	*	*	*	*	{* *	*	*	10

ตารางประมวลผลข้อมูลและขั้นตอนการทดสอบที่ 1

รายละเอียดข้อมูลทดสอบ												รวม
1	2	3	4	5	6	7	8	9	10	11	12	
ข้อมูล Master file ที่คัดเลือกไว้และใช้ทดสอบ												
ข้อมูลหลักเกี่ยวกับเงินเดือน												
ความสมบูรณ์ในการบันทึกการแก้ไขข้อมูลหลักใน Master file												
เป็นการทดสอบเพื่อดูความถูกต้องว่ารายการที่ผ่านเข้าไปแก้ไข Master file												
ถูกพิมพ์รายการไว้ในรายงานการแก้ไข เพื่อนำไปตรวจสอบกับสำเนาใบอนุมัติ												
การแก้ไขรายการ												
พนักงานเข้าใหม่	*											2
พนักงานลาหยุดงาน			*	*								2
เงินจ่ายเพิ่ม					*							1
การเปลี่ยนรหัสภาษี						*						1
รายการหักเพิ่มเติม							*					1
ลบล้างรายการหักครั้งก่อนออก								*				1
ความถูกต้องในการบันทึกการแก้ไขข้อมูลหลักใน Master file												
เป็นการทดสอบเพื่อดูความถูกต้องว่ารายการแก้ไขทั้งหมดที่พิมพ์ไว้ใน												
รายงานการแก้ไขนั้น ไปบันทึกแก้ไขข้อมูลของพนักงานที่ตรงกับความ												
ต้องการ รวมทั้งความถูกต้องของรายละเอียดของ Master file												
ที่พิมพ์ออกมาด้วย	*	*	*	*	*	*	*	*				8
ข้อมูล Master file นำไปทดสอบรายการต่อไป ในขั้นตอนที่ 2	*	*	-	-	*	*	*	*	*	*	*	10

ตารางประมวลผลข้อมูลและขั้นตอนการทดสอบที่ 2

	รายละเอียดข้อมูลทดสอบ												รวม
	1	2	3	4	5	6	7	8	9	10	11	12	
ข้อมูล Master file ที่ใช้ทดสอบ (ยกมาจากขั้นตอนที่ 1)	*	*	–	–	*	*	*	*	*	*	*	*	10
การจัดทำใบจ่ายเงินเดือน													
ความสมบูรณ์ของข้อมูลที่ป้อนเข้า													
เป็นการทดสอบเพื่อดูความถูกต้องว่ารายการต่างๆต่อไปนี้ต้องถูกพิมพ์ไว้ใน													
รายงานข้อสังเกตพิเศษ คือ													
(ก) พนักงานที่ไม่มีบัตรลงเวลาทำงาน		*			*								2
(ข) บัตรลงเวลาทำงานที่มีเลขประจำตัวพนักงานไม่ถูกต้อง			*						*				2
(ค) บัตรลงเวลาทำงานที่ส่งคืนเนื่องจากเลขประจำตัวพนักงานซ้ำกัน										* *			2
ความถูกต้องของข้อมูลที่ป้อนเข้า													
เป็นการทดสอบเพื่อดูความถูกต้องว่าบัตรลงเวลาทำงานที่มีชั่วโมงการ													
ทำงานเกินกว่า 60 ชั่วโมง ต้องถูกพิมพ์ไว้ในรายงานข้อสังเกตพิเศษ						*							1
ข้อมูล Master file และรายการที่ใช้ทดสอบต่อไปในขั้นตอนที่ 3	*	–	–	–	–	*	*	*	–	–	*	*	6

ตารางประมวลผลข้อมูลและขั้นตอนการทดสอบที่ 3

ข้อมูล Master file และรายการที่ใช้ทดสอบ (ยกมาจากขั้นตอนที่ 2)	รายละเอียดข้อมูลทดสอบ						รวม
	1	6	7	8	11	12	
ความถูกต้องของการจัดทำใบจ่ายเงินเดือน	*	*	*	*	*	*	6
เป็นการทดสอบเพื่อดูความถูกต้องว่ารายการต่าง ๆดังต่อไปนี้ต้องถูกพิมพ์ไว้ในรายงานข้อสังเกตพิเศษ คือ							
(ก) พนักงานที่ได้รับอัตราค่าจ้างเกินกว่า 1,500 บาท ต่อสัปดาห์			*				1
(ข) พนักงานที่มีเงินได้รวมก่อนหักภาษีเกินกว่า 2,500 บาท ต่อสัปดาห์		*	*	*			3
เพื่อให้แน่ใจว่าการคำนวณเงินได้เบื้องต้น รายการหักและเงินได้สุทธิถูกต้อง	*	*	*	*	*	*	6
เพื่อดูความถูกต้องในการรวบรวมเงินได้เบื้องต้น รายการหักและเงินได้สุทธิ	*	*	*	*	*	*	6
เป็นการทดสอบเพื่อดูความถูกต้องว่าได้สรุปรายจ่ายค่าจ้างถูกต้องตรงกับบัญชีแยกประเภท	*	*	*	*	*	*	6
เพื่อให้แน่ใจว่ารายจ่ายค่าจ้างและรายการหักถูกบันทึกบัญชีเงินได้พนักงานถูกต้อง	*	*	*	*	*	*	6
ข้อมูล Master file และรายการที่แสดงในตอนเสร็จสิ้นการประมวลผลข้อมูลทดสอบ	*	*	*	*	*	*	6

ภาคผนวก ซ.
การวิเคราะห์รหัสคำสั่งโปรแกรม

1. วัตถุประสงค์และขอบเขตของการวิเคราะห์รหัสคำสั่งโปรแกรม (The Purpose and Scope of Program Code Analysis)

วัตถุประสงค์ที่สำคัญของการวิเคราะห์รหัสคำสั่งโปรแกรม เพื่อเป็นการยืนยันความเชื่อถือได้ว่าขั้นตอนการทำงานของโปรแกรม (programmed procedures) ที่กำหนดไว้นั้นมีอยู่จริง ๆ ในตัวโปรแกรมหรือชุดของโปรแกรมที่ใช้งาน ดังนั้นการวิเคราะห์รหัสโปรแกรมของผู้ตรวจสอบก็คือการทดสอบขั้นตอนการทำงานของโปรแกรมนั่นเอง โดยผู้ตรวจสอบอาจใช้เทคนิคต่าง ๆ เข้าช่วย เพื่อทำความเข้าใจหรือสอบยันความเข้าใจที่มีอยู่เดิมในโปรแกรมงาน หรือส่วนของโปรแกรมงานภายในระบบ แต่อย่างไรก็ดีผู้ตรวจสอบอาจไม่ต้องใช้ขั้นตอนการวิเคราะห์ทุกขั้นตอนที่กล่าวไว้ในภาคผนวกนี้ก็ได้

เพื่อให้การใช้เทคนิคการตรวจสอบมีประสิทธิภาพ ผู้ตรวจสอบอาจใช้วิธีการใดวิธีการหนึ่งดังนี้คือ ใช้วิธีการตรวจสอบรหัสคำสั่งในรูปของภาษาเครื่อง (Object Form) ซึ่งวิธีนี้ไม่นิยมใช้ปฏิบัติ หรืออาจใช้วิธีการตรวจ-สอบรหัสคำสั่งในรูปของภาษาเขียน (Source Statement Form) ผู้ตรวจสอบต้องมั่นใจว่ารหัสคำสั่งที่ตรวจสอบนั้นเป็นรหัสคำสั่งของโปรแกรมที่ใช้ปฏิบัติงานประมวลผลข้อมูลทางบัญชีจริง โดยการตรวจสอบการควบคุมรักษาความปลอดภัยโปรแกรม (Program Security Controls) และการควบคุมการปฏิบัติงาน (Computer Operation Controls) ของธนาคาร

2. วิธีวิเคราะห์รหัสคำสั่งโปรแกรม (Method of Work)

วิธีวิเคราะห์รหัสคำสั่งโปรแกรมมี 4 ขั้นตอน ดังต่อไปนี้คือ

2.1 การกำหนดตัวโปรแกรมที่จะตรวจสอบ

2.2 การคัดชนิดของรูปแบบรหัสคำสั่งที่จะตรวจสอบ

2.3 การวิเคราะห์รหัสคำสั่งของโปรแกรมที่คัดเลือกไว้

2.4 การสอบยันเพื่อให้แน่ใจว่ารหัสคำสั่งที่ตรวจสอบนั้นเป็นรหัสคำสั่งที่ใช้ประมวลผลข้อมูลด้านการบัญชีจริง

2.1 การกำหนดตัวโปรแกรมที่จะตรวจสอบ

สิ่งที่ควรดำเนินการเป็นอันดับแรกในการวิเคราะห์รหัสคำสั่งโปรแกรม คือการกำหนดตัวโปรแกรมหรือชุดโปรแกรมที่จะนำมาวิเคราะห์เพื่อสอบยันว่า ขั้นตอนการทำงานของโปรแกรมที่วางหรือกำหนดไว้นั้นมีอยู่จริง ๆ ในตัวโปรแกรมหรือไม่ โดยอาศัยเอกสารประกอบระบบงานของธนาคารเป็นหลัก ซึ่งส่วนใหญ่จะมีลักษณะเป็นรูปแผนภูมิ (Block Diagram) ที่แสดงลำดับการทำงานก่อนหลังของโปรแกรมที่ใช้ในระบบงานนั้นอย่างสมเหตุผล จากนั้นจึงตรวจสอบข้อกำหนดของแต่ละโปรแกรมโดยละเอียดเพื่อให้ทราบขั้นตอนการทำงานของโปรแกรม

2.2 การคัดเลือกชนิดของรูปแบบรหัสคำสั่งที่จะตรวจสอบ

โดยทั่วไปผู้ตรวจสอบมักตัดสินใจเลือกตรวจสอบรหัสคำสั่งโปรแกรมในรูปภาษาเขียน (Source Statement Program) ซึ่งผู้ตรวจสอบจำเป็นต้องมีความรู้ความเข้าใจเกี่ยวกับภาษาที่ใช้เขียนโปรแกรมนั้น และต้องระมัดระวังในการแปลความหมายของประโยคคำสั่งในโปรแกรมที่ใช้ตรวจสอบนั้นด้วย ผู้ตรวจสอบอาจขอรายละเอียดโปรแกรมได้จากเอกสารประกอบโปรแกรม หรือจากสำเนารายละเอียดโปรแกรมชุดที่ธนาคารเก็บสำรองไว้เพื่อประโยชน์ในการรักษาความปลอดภัย แต่ผู้ตรวจสอบต้องแน่ใจว่าเป็นรายละเอียดโปรแกรมที่มีการปรับปรุงแก้ไขให้ตรงกับโปรแกรมชุดที่ใช้งานในปัจจุบันอยู่เสมอ (Up to Date) ดังนั้นวิธีที่ดีควรขอให้เครื่องพิมพ์รายละเอียดของโปรแกรมที่ใช้ทำงานอยู่นั้นออกมาจากเครื่องคอมพิวเตอร์โดยตรง ซึ่งเป็นวิธีที่สะดวกต่อการปฏิบัติ โดยเพียงแต่ให้เครื่องแปลโปรแกรมที่ใช้งานอยู่นั้นแล้วพิมพ์เป็นรายละเอียดโปรแกรมออกมาให้ ผู้ตรวจสอบอาจขอให้เครื่องเลือกแปลโปรแกรมในส่วนที่เป็นประโยชน์ต่อการวิเคราะห์ของผู้ตรวจสอบเองก็ได้ เช่น ให้พิมพ์รายละเอียดของชื่อข้อมูลและคำกริยาที่ใช้ในโปรแกรมเพื่อใช้เป็นเอกสารอ้างอิง เป็นต้น

2.3 การวิเคราะห์รหัสคำสั่งของโปรแกรมที่คัดเลือกไว้

ผู้ตรวจสอบจำเป็นต้องมีความรู้ความเข้าใจภาษาของโปรแกรมที่เขียนอธิบายวิธีการทำงานนั้นเป็นอย่างดี จึงจะสามารถใช้วิธีการวิเคราะห์รหัสคำสั่งในตัวโปรแกรมภาษาเขียนนั้นได้ ผู้เขียนโปรแกรมส่วนมากตระหนักดีว่าการทำความเข้าใจกับเหตุผลการทำงานของโปรแกรม (program logic) ที่บุคคลอื่นเป็นผู้เขียนขึ้นนั้นทำได้ยากลำบากมากแต่ถ้าธนาคารมีการกำหนดมาตรฐานการจัดทำโปรแกรมและเอกสารประกอบโปรแกรมไว้เป็นอย่างดีแล้ว ก็จะช่วยให้ผู้ตรวจสอบทำงานได้ง่ายยิ่งขึ้น และมีความสำคัญต่อการวางแผนการตรวจสอบรหัสโปรแกรมเป็นอย่างมาก การตรวจสอบรหัสคำสั่งไม่ควรทำโดยการดูตั้งแต่ประโยคคำสั่งแรกไล่ไปจนถึงประโยคสุดท้าย เพราะเป็นการเสียเวลามาก และไม่ใช่วิธีการที่มีประสิทธิภาพ

วิธีดำเนินการตรวจสอบรายละเอียดรหัสคำสั่งโปรแกรม สรุปขั้นตอนการทำงานได้เป็น 3 ขั้นตอนดังต่อไปนี้ คือ

- การทำความเข้าใจข้อมูลที่ประมวลผล ซึ่งได้แก่ การทำความเข้าใจแฟ้มข้อมูล (Files) และตัวข้อมูล (Data) ภายในแฟ้มข้อมูลที่โปรแกรมนั้นใช้ประมวลผล

- การวิเคราะห์ Logic
- การตรวจสอบเพื่อให้แน่ใจว่าได้วิเคราะห์รหัสคำสั่งอย่างครบถ้วน

ขั้นตอนที่กล่าวข้างต้น เป็นกรณีที่ใช้ภาษา COBOL ซึ่งเป็นภาษาที่นิยมใช้กันมาก

ถึงแม้ว่าการวิเคราะห์รหัสคำสั่งที่คัดเลือกมานั้น จำเป็นต้องใช้ผู้ตรวจสอบที่มีความรู้ความชำนาญเป็นอย่างมากก็ตาม แต่การตรวจสอบอาจง่ายขึ้นถ้าธนาคารได้จัดให้มีการใช้เทคนิคในการวางโครงสร้างโปรแกรมที่ดี ช่วยให้สามารถติดตาม logic ของโปรแกรมได้ง่ายยิ่งขึ้น เพราะว่า

(ก) โปรแกรมที่พัฒนาตามแนวทางนี้จะมีโครงสร้างที่ดีกว่า

(ข) มีการใช้ประโยคคำสั่ง GO TO น้อย และใช้ประโยคคำสั่ง PERFORM มาก ในภาษา COBOL

(ค) ประโยคคำสั่ง IF จะถูกรวบรวมเอาไว้ในส่วนที่เกี่ยวกับการ "เลือกตัดสินใจ (decision)" ในตัวโปรแกรมเพียงที่เดียว และไม่กระจัดกระจาย

2.3.1 การทำความเข้าใจข้อมูลที่ประมวลผล

เมื่อได้รับรายละเอียดของโปรแกรมภาษาเขียนที่ผู้ตรวจสอบต้องการวิเคราะห์เรียบร้อยแล้ว งานเบื้องต้นของผู้ตรวจสอบคือทำความเข้าใจเกี่ยวกับแฟ้มข้อมูล (File) ข้อมูลที่บันทึกแต่ละรายการ (Records) และองค์ประกอบส่วนย่อยของข้อมูลแต่ละรายการ (Data Fields) ที่ต้องใช้ รวมทั้งลักษณะการใช้ด้วย

หลังจากผู้ตรวจสอบมีความเข้าใจในข้อเบื้องต้นดังกล่าวแล้ว ก็จะดำเนินการศึกษารายละเอียดโปรแกรม (Source Listing) ร่วมกับเอกสารประกอบโปรแกรม (Program Documentation) เพื่อทำให้ทราบข้อกำหนดต่าง ๆ คือ

(1) การใช้แฟ้มข้อมูล

โดยปกติผู้ตรวจสอบจะเริ่มต้นตรวจสอบคำสั่งเกี่ยวกับการ SELECT ซึ่งเป็นประโยคย่อยหรืออนุประโยค (clauses) ก่อน เพราะเป็นตัวที่บอกแฟ้มข้อมูลทั้งหมดที่ต้องใช้ในโปรแกรม แล้วจึงตรวจสอบประโยค (statements) เกี่ยวกับการ OPEN และ CLOSE ในส่วนของ Procedure Division เพื่อจะได้รู้ว่าแฟ้มข้อมูลถูกนำไปใช้ได้อย่างไรบ้างในโปรแกรมนั้น ขั้นตอนต่าง ๆ ที่กล่าวมานี้ช่วยให้ผู้ตรวจสอบรู้ถึงหน้าที่การทำงานของแต่ละแฟ้มข้อมูล ตัวอย่างเช่น เป็นแฟ้มป้อนข้อมูลเข้า (Input File) แฟ้มข้อมูลผลลัพธ์ (Output File) หรือเป็นทั้งแฟ้มข้อมูลป้อนเข้าและข้อมูลผลลัพธ์ (Input and Output File)

(2) ลักษณะการบันทึกข้อมูลแต่ละรายการ (Data Record) ลงในแฟ้มข้อมูล

ผู้ตรวจสอบจะตรวจสอบคำบรรยายลักษณะรายการข้อมูล File Description (FD) ของแต่ละแฟ้มข้อมูล ในกรณีที่ลักษณะการบันทึกข้อมูลแต่ละรายการ (Data Record) ในแฟ้มข้อมูลเดียวกันมีหลายแบบ ผู้ตรวจสอบต้องมีความเข้าใจในการใช้ข้อมูลแต่ละแบบ และดูผลกระทบที่อาจมีต่อขั้นตอนในโปรแกรมที่ตรวจสอบนั้น โดยทั่วไปข้อมูลที่มีความแตกต่างกันจะมีเหตุผลในการทำงาน (logical paths) ในแต่ละส่วนของโปรแกรมแตกต่างกันด้วย

(3) องค์ประกอบส่วนย่อย (Data Field) ของข้อมูลที่สำคัญในแต่ละรายการ

องค์ประกอบส่วนย่อยของข้อมูลที่สำคัญในแต่ละรายการที่บรรยายรายละเอียด ไว้ในส่วนที่เรียกว่า File Descriptions หรือ Working Storage Fields ของโปรแกรม จะช่วยให้เข้าใจความหมายของแต่ละ Field ได้เป็นอย่างดี และผู้ตรวจสอบจำเป็นต้องทำความเข้าใจเกี่ยวกับองค์ประกอบที่สลับซับซ้อน ซึ่งเป็นลักษณะเฉพาะของข้อมูลในแต่ละ Field ด้วย ตัวอย่างเช่น ในภาษา COBOL จะยอมให้โปรแกรมต่าง ๆ เรียกใช้เนื้อหาข้อมูลชุดเดียวกันในลักษณะแตกต่างกัน โดยอาศัยคำสั่งอนุประโยค (clause) RE-DEFINES หรือ RENAMES

ถ้าธนาคารมีการจัดทำพจนานุกรมของข้อมูล (data dictionary) ก็อาจขอรายละเอียดพจนานุกรมมาช่วยในการทำความเข้าใจเนื้อหาของข้อมูลได้เช่นกัน

ผู้ตรวจสอบควรตรวจสอบด้วยว่าโปรแกรมคำสั่งนั้นมีการใช้สัญญาณคุม (Switches) (อาจสร้างไว้ในโปรแกรมหรือรวมไว้ในคำสั่งควบคุมการทำงาน (Job Control Statement) หรือ Console ก็ได้) เพื่อควบคุมการทำงานของโปรแกรมให้เป็นไปตามความต้องการในขณะปฏิบัติงานหรือไม่ เช่น อาจมีการใช้ Switches หยุดการประมวลผลในบางส่วนของโปรแกรมหรือโปรแกรมย่อย (Routines) ในช่วงระยะเวลาที่ต้องการ ผู้ตรวจ-สอบควรเข้าใจ Switches ต่าง ๆ ที่ใช้อยู่ทั้งหมด เพราะจะมีความสำคัญต่อการตรวจสอบกับคำสั่งโปรแกรมในรายละเอียด

2.3.2 การวิเคราะห์ Logic

สิ่งแรกที่ผู้ตรวจสอบจะทำคือ จะต้องทราบว่าคำสั่งที่เกี่ยวกับ Logic ซึ่งเป็นชุดคำสั่งที่ต้องอาศัยความสมเหตุผล หรือความสอดคล้องกันเป็นหลักนั้นอยู่ในส่วนใด หรือย่อหน้า (paragraphs) ใดของ Programed Procedures ซึ่งอาจดูได้จากเอกสารประกอบโปรแกรม ถ้าธนาคารมีเอกสารประกอบน้อยหรือมีรายละเอียดไม่เพียงพอ อาจต้องใช้เวลาในการค้นหามาก เนื่องจากต้องใช้วิธีศึกษาจาก Source Listing โดยละเอียด

เมื่อผู้ตรวจสอบทราบว่ารหัสคำสั่งที่เกี่ยวกับ Logic อยู่ใน Paragraph ใดของโปรแกรมแล้ว ก็จะดำเนินการวิเคราะห์ Logic โดยละเอียด ซึ่งสามารถแบ่งลักษณะการทำงานของรหัสคำสั่งประเภทนี้ได้เป็น 3 แบบ คือ

- COMPARISON เป็นประโยคคำสั่งให้ทำการเปรียบเทียบ Data Field หนึ่งกับ Data Field อื่น หรือค่าคงที่ (Constants) ที่ตั้งไว้
- CALCULATION เป็นประโยคคำสั่งให้ดำเนินการคำนวณตามกฎทางคณิต-ศาสตร์
- WRITING เป็นประโยคคำสั่งให้พิมพ์ข้อมูลหรือบันทึกข้อมูลออกลงในอุปกรณ์จัดเก็บข้อมูล (Magnetic Storage Devices)

รหัสคำสั่งแต่ละประเภทนี้จะประกอบด้วยประโยคคำสั่ง (Statement) เป็นจำนวนมาก

ลักษณะขั้นตอนต่าง ๆ ของโปรแกรมจะแตกต่างกันออกไป และขั้นตอนการทำงานของโปรแกรมจะประกอบด้วยประโยคคำสั่งตามลักษณะที่กล่าวข้างต้นมากกว่าหนึ่งลักษณะ ตัวอย่างเช่น โปรแกรมที่เขียนขึ้นเพื่อควบคุมพัสดุของธนาคาร มีการเก็บข้อมูลการใช้พัสดุแต่ละชนิดตลอดระยะเวลา 12 เดือนที่ผ่านมา ขั้นตอนการทำงานของโปรแกรมที่วางไว้จะมีโครงสร้างดังต่อไปนี้

(ก) รวมยอดข้อมูลการใช้พัสดุตลอดระยะเวลาที่ผ่านมา 12 เดือน (CALCULATION)

(ข) เปรียบเทียบยอดรวมของข้อ (ก) กับยอดพัสดุคงเหลือปัจจุบัน (COMPARISON)

(ค) คำนวณมูลค่าของพัสดุคงเหลือโดยใช้ราคาที่ซื้อมา (CALCULATION)

(ง) รวมยอดมูลค่าพัสดุคงเหลือ (CALCULATION)

(จ) เปรียบเทียบยอดพัสดุคงเหลือแต่ละรายการกับค่าคงที่ที่ตั้งไว้ (constant) เพื่อหาผลต่าง (COMPARISON)

(ฉ) พิมพ์รายละเอียดพัสดุคงเหลือ (WRITING)

ผู้ตรวจสอบต้องพิจารณารายละเอียดโดยการวิเคราะห์ Logic แต่ละประเภทดังต่อไปนี้

(1) **การเปรียบเทียบ** (Comparison)

ในภาษา COBOL นั้นการเปรียบเทียบสามารถทำได้โดยใช้ประโยค IF clause เพื่อเลือกตัดสินใจประมวลผลข้อมูลตามแนวทางการทำงานที่สมเหตุผลที่กำหนดไว้ในโปรแกรม

ผู้ตรวจสอบควรตรวจสอบ IF clause ใน Paragraph ของรหัสคำสั่งนั้น เพื่อให้แน่ใจได้ว่า

(ก) การเปรียบเทียบที่ทำขึ้น ณ จุดที่ทดสอบนั้นถูกต้องสมเหตุผลตามหลักการทำงาน ตัวอย่างเช่น การทดสอบเพื่อตัดข้อมูลรายการ (Record) ที่ไม่ต้องการออกเพื่อไม่ให้ประมวลผลในขั้นตอนต่อไป ดังนั้น Logic ที่ใช้คือ การตัดรายการที่ไม่ต้องการออกไปเท่านั้น

(ข) ใช้ Data Field ที่ถูกต้องในการเปรียบเทียบ

(ค) คำจำกัดความของ Data Field ที่ใช้ในการเปรียบเทียบตามที่กำหนดไว้ใน File Description หรือ Working Storage ของโปรแกรมจะต้องให้ผลลัพธ์จากการทดสอบตรงกับผลที่คาดคะเนไว้ เพื่อตรวจสอบลักษณะของ Data Field ว่าเป็นไปตามข้อกำหนดหรือไม่ พิจารณาผลลัพธ์ที่ได้จากการเปรียบเทียบนั้นเป็นไปตามกฎข้อบังคับของภาษาโปรแกรมที่ใช้อยู่นั้นเพียงใด

(ง) การทำงานของคำสั่งที่ใช้ในการกำหนดเส้นทางเดินของข้อมูล โดยยินยอมให้ข้อมูลรายการที่ถูกต้องตามข้อกำหนดผ่านไปประมวลผลในขั้นต่อไปได้ ส่วนข้อมูลที่ไม่ถูกต้องจะไม่สามารถผ่านไปประมวลผลได้ เป็นการตรวจสอบจุดที่ข้อมูลจะเดินทางไปถึงเมื่อมีการใช้คำสั่ง GO TO หรือ PERFORM

(2) **การคำนวณ** (Calculation)

คำสั่งที่เกี่ยวกับการคำนวณ ได้แก่ ประโยคคำสั่ง ADD, MULTIPLY, SUBTRACT, DIVIDE และ COMPUTE ผู้ตรวจสอบควรตรวจสอบความถูกต้องของการคำนวณทุกขั้นตอนจนเป็นที่พอใจได้ว่า

(ก) การคำนวณถูกต้องตามคำสั่งที่กำหนดไว้อย่างสมเหตุผล

(ข) ใช้ Data Field ที่ถูกต้องในการคำนวณ

(ค) Data Field ที่ใช้ในการคำนวณตามที่กำหนดลักษณะไว้ใน Field Description หรือ Working Storage จะต้องได้ผลลัพธ์ที่มีขนาดเท่ากับที่กำหนดไว้ก่อนแล้ว ผู้ตรวจสอบควรให้ความสนใจเกี่ยวกับขนาด (Field Sizes) และคำจำกัดความ (Definition) ของข้อมูล เพื่อให้แน่ใจได้ว่าขนาดความยาวของข้อมูลที่คำนวณจะต้องไม่เกินไปกว่าเนื้อที่ที่กันไว้ เพื่อให้สามารถบรรจุข้อมูลที่เป็นทั้งบวกและลบได้อย่างเพียงพอ และต้องคำนึงถึงจุดทศนิยมหรือเศษสตางค์ที่ถูกต้องด้วย

(3) **การบันทึกหรือการพิมพ์** (Writing)

Writing คือ การบันทึกผลลัพธ์ที่ได้ลงใน Tape หรือ Disc หรือให้พิมพ์รายการข้อมูลออกมาทางเครื่องพิมพ์ (Printer) ในการวิเคราะห์รหัสคำสั่งประเภทนี้ ผู้ตรวจสอบจะต้องแน่ใจว่า

(ก) ข้อมูลที่ถูก MOVE ไปเพื่อทำการ Write นั้นเป็นข้อมูลที่ถูกต้อง (correct Data Fields)

(ข) ขนาดของเนื้อที่ที่เก็บข้อมูลที่จะ Write จะต้องสอดคล้องกันกับข้อมูลที่จะ MOVE เข้าไป

(ค) ต้องไม่มีคำสั่งในโปรแกรมที่จะทำให้ Writing รายการผิด

(4) **ความสัมพันธ์ของรหัสคำสั่งแต่ละประเภท**

ผู้ตรวจสอบต้องตรวจสอบการประมวลผลทั้ง 3 ลักษณะ คือ Comparison, Calculation และ Writing ว่ามีความถูกต้องตาม Logic จริงเพียงใด ในกรณีที่ Logic ทั้ง 3 ลักษณะตามที่กล่าวข้างต้นถูกแยกเขียนคนละโปรแกรม ควรนำโปรแกรมเหล่านี้มาตรวจสอบ Logic ให้สอดคล้องกันด้วย

2.3.3 การตรวจสอบเพื่อให้แน่ใจว่าได้วิเคราะห์รหัสคำสั่งอย่างครบถ้วน (Ensuring that analysed coding is not bypassed)

แม้ผู้ตรวจสอบจะได้ทำการตรวจสอบตามขั้นตอนต่าง ๆที่กำหนดไว้ในหัวข้อที่กล่าวข้างต้นแล้วก็ตาม แต่อาจละเลยการตรวจสอบรหัสคำสั่งได้ 2 ทางด้วยกัน คือ

(1) ละเลยไม่ตรวจสอบในบางส่วนของโปรแกรมเดียวกัน

(2) ละเลยไม่ตรวจสอบโปรแกรมอื่น ๆ ในระบบงานเดียวกัน

(1) **ละเลยไม่ตรวจสอบในบางส่วนของโปรแกรมเดียวกัน**

ผู้ตรวจสอบจำเป็นต้องใส่ Logic ของโปรแกรมทั้งย้อนหลัง และไปข้างหน้าจาก Paragraph ที่กำลังวิเคราะห์ความละเอียด เพื่อให้แน่ใจได้ว่า Logic ของโปรแกรมที่ได้จัดทำไว้ยินยอมให้ข้อมูลที่ถูกต้องเท่านั้นผ่านเข้าไปใน Paragraph ที่เกี่ยวข้องกันได้ และ Logic ของ Paragraph ที่อยู่ในลำดับต่อไปนั้นไม่ทำให้ขั้นตอนการทำงานของโปรแกรมก่อนหน้านั้นผิดความจริงไปด้วย และผู้ตรวจสอบต้องแน่ใจว่าความสัมพันธ์ของ Logic ในระหว่าง Paragraph ที่วิเคราะห์อยู่นั้นถูกต้อง

ผู้ตรวจสอบอาจใช้โปรแกรมสำเร็จรูป (Software Package) เข้าช่วยในการวิเคราะห์โปรแกรม และสร้างผังแสดงลักษณะการทำงาน (Flowchart) ของ Logic ซึ่งโดยปกติ Flowchart จะเป็นตัวแสดงรายละเอียดของคำสั่งใน Paragraph ที่ใช้ในโปรแกรม การเชื่อมต่อ (Connecting Paths) ระหว่างโปรแกรมและแสดงการทดสอบเปรียบเทียบที่มีอยู่ในโปรแกรมนั้น ผู้ตรวจสอบสามารถใช้ Flowchart นี้เพื่อตรวจสอบ Logic ก่อนและหลัง Paragraph ที่กำลังวิเคราะห์อยู่นั้น นอกจากนี้ยังสามารถตรวจสอบประโยค IF, GO TO และ PERFORM ในโปรแกรมซึ่งเป็นประโยคหลักสำหรับควบคุม Logic ของโปรแกรม ในกรณีที่ไม่มี Flowchart สำเร็จรูปผู้ตรวจสอบต้องเตรียม Flowchart ด้วยตนเอง

เมื่อผู้ตรวจสอบได้ตรวจสอบผังทางเดินของข้อมูลตาม Logic ในโปรแกรมว่ามีความถูกต้องแล้ว ขั้นต่อไปก็คือ ต้องให้ความเชื่อถือได้ว่ารหัสคำสั่งของบรรทัดอื่น ๆ ภายในโปรแกรมนั้นไม่ได้ทำให้ Data Fields ที่ใช้ประมวลผลผิดไปจากที่ได้วิเคราะห์ไว้แล้ว ดังนั้นจึงมีความจำเป็นที่ต้องตรวจสอบรหัสคำสั่งทุกบรรทัดในโปรแกรมที่มีการใช้ Data Field ที่ผิดสังเกตโดยตรวจ Cross-Reference Listing ของโปรแกรมที่อาจได้จาก Flowcharting Package หรือจากการแปลโปรแกรมภาษาเขียนเป็นภาษาเครื่องจักร (Compilation) ซึ่งจะแสดงชื่อของข้อมูลและคำกริยาที่ใช้ในโปรแกรม พร้อมด้วยจำนวนบรรทัดของรหัสคำสั่งที่ใช้ด้วย หลังจากผู้ตรวจสอบได้ดูความถูกต้องของชื่อข้อมูลแล้ว ก็ควรตรวจสอบความถูกต้องของรหัสคำสั่งแต่ละบรรทัดที่ปรากฏอยู่ด้วย ผู้ตรวจสอบอาจจำเป็นต้องตรวจสอบการประมวลผลเกี่ยวกับชื่อข้อมูลอีกครั้งหนึ่ง เมื่อปรากฏว่ามีการกำหนดชื่อ Field ขึ้นใหม่อีกชุดหนึ่งซ้ำกับ Field เดิม ซึ่งผู้ตรวจสอบควรให้ความสนใจข้อมูลที่จับกลุ่มกันขึ้นเป็น Field

ในขั้นสุดท้าย ผู้ตรวจสอบจะใช้ Cross-Reference Listing ตรวจสอบความถูกต้องในการใช้คำกริยาที่จะมีผลทำให้ข้อมูลหรือ Logic ของโปรแกรมเปลี่ยนแปลงไปในขณะเดินเครื่อง ตัวอย่างเช่น คำกริยา ALTER ถ้ามีอยู่ในบรรทัดรหัสคำสั่งใดควรตรวจสอบอย่างระมัดระวัง ศูนย์คอมพิวเตอร์หลายแห่งห้ามใช้คำกริยาดังกล่าวนี้ โดยระบุไว้เป็นข้อห้ามในมาตรฐานการเขียนโปรแกรม

(2) **ละเลยไม่ตรวจสอบโปรแกรมอื่น ๆ ในระบบงานเดียวกัน**

ความเหมาะสมในการขยายขอบเขตการตรวจสอบโปรแกรมอื่นนั้น ขึ้นอยู่กับสภาพการณ์ของแต่ละกรณี ผู้ตรวจสอบควรยึดถือความสมบูรณ์และความถูกต้องของข้อมูลที่จะต้องไม่ถูกบิดเบือนข้อเท็จจริงไปโดยโปรแกรมอื่นที่ประมวลผลก่อนหน้าและหลังจากนั้นเป็นหลักในการพิจารณา ถ้าผู้ตรวจสอบประเมินผลการควบคุมของผู้ใช้ข้อมูลแล้วเห็นว่าวิธีการควบคุมที่ใช้อยู่นั้นไม่สามารถตรวจพบความผิดพลาดข้อมูลได้แล้ว ก็ควรจะเพิ่มขั้นตอนการตรวจสอบต่อไปนี้เข้าไปด้วย คือ

ก) จุดที่ความสมบูรณ์ (Completeness) ของข้อมูลอาจถูกบิดเบือนได้โดยตรวจสอบทางเดินของข้อมูล (Logical Flow of Data) ตลอดทั้งโปรแกรมก่อนหน้าและหลังจากงานนั้น ผู้ตรวจสอบควรมุ่งความสนใจไปที่ประโยคคำสั่ง IF, GO TO, PERFORM และ ALTER

ข) จุดที่ความถูกต้อง (Accuracy) ของข้อมูลอาจถูกบิดเบือนได้ โดยตรวจสอบการจัดทำ Data Field ที่เกี่ยวข้องกันในโปรแกรมก่อนหน้าและหลังจากงานนั้น ผู้ตรวจสอบควรมุ่งความสนใจไปที่ประโยคคำสั่ง ADD, SUBTRACT, MULTIPLY, DIVIDE, COMPUTE และ MOVE สำหรับระบบงานที่มีการใช้พจนานุกรมข้อมูล (Data Dictionary) รายละเอียดที่ปรากฏอยู่ในพจนานุกรมจะช่วยให้ทราบว่ามีโปรแกรมใดบ้างที่เรียกใช้ข้อมูลที่เก็บไว้

2.3.4 การวิเคราะห์ในปีที่สองและปีต่อ ๆ ไป (Second and subsequent years)

เมื่อผู้ตรวจสอบได้เคยวิเคราะห์รายละเอียดมาก่อนครั้งหนึ่งแล้ว ในปีต่อ ๆ ไปก็จะตรวจสอบเฉพาะส่วนที่มีการเปลี่ยนแปลงไป และวิเคราะห์ถึงผลกระทบของการเปลี่ยนแปลงนั้น การวิเคราะห์อย่างละเอียดจะมีก็ต่อเมื่อมีการเขียนโปรแกรมขึ้นใหม่ทั้งหมด

ผู้ตรวจสอบจะทราบการเปลี่ยนแปลงรหัสคำสั่งในโปรแกรมในแต่ละปีได้ง่ายยิ่งขึ้น ถ้าสามารถใช้โปรแกรมสำเร็จรูปเข้าไปเปรียบเทียบประโยคคำสั่งของโปรแกรมเก่ากับใหม่ และแสดงผลแตกต่างให้เห็นด้วย โดยผู้ตรวจสอบดำเนินการดังนี้คือ

(1) ในปีแรกที่ผู้ตรวจสอบวิเคราะห์รหัสคำสั่ง ผู้ตรวจสอบควรขอสำเนาของโปรแกรมภาษาเขียนไว้เป็นของผู้ตรวจสอบเอง

(2) ในปีต่อไปผู้ตรวจสอบก็จะใช้สำเนาของโปรแกรมภาษาเขียนของผู้ตรวจสอบเองเปรียบเทียบเพื่อดูการเปลี่ยนแปลงระหว่างสำเนาตามข้อ (1) และโปรแกรมที่ใช้ปฏิบัติงานในขณะนั้น

(3) การเปรียบเทียบประโยคคำสั่งควรเน้นให้เห็นถึงคำสั่งที่เพิ่มขึ้น คำสั่งเก่าที่เลิกใช้และคำสั่งที่มีการเปลี่ยนแปลง ผู้ตรวจสอบควรตรวจเฉพาะส่วนที่มีการเปลี่ยน-แปลงเท่านั้นก็พอ

(4) ผู้ตรวจสอบจะต้องไตร่ตรองถึงผลกระทบของการเปลี่ยนแปลงที่มีต่อส่วนอื่น ๆ ของโปรแกรมที่ไม่มีการเปลี่ยนแปลงด้วย

2.4 การสอบยันเพื่อให้แน่ใจว่ารหัสคำสั่งที่ตรวจสอบนั้นเป็นรหัสคำสั่งที่ใช้ในการประมวลผลข้อมูลด้านการบัญชีจริง

หลังจากผู้ตรวจสอบได้ตรวจสอบรหัสคำสั่งที่เกี่ยวข้องกันในโปรแกรมนั้นแล้ว ขั้นต่อไปคือ ต้องสอบยันเพื่อให้แน่ใจว่าโปรแกรมที่ตรวจสอบอยู่นั้นเป็นโปรแกรมที่ใช้ประมวลผลข้อมูลจริง ๆ

การสอบยันดังกล่าวนี้ทำได้โดยการทดสอบการควบคุมการรักษาความปลอดภัยของโปรแกรม สำหรับศูนย์คอมพิวเตอร์ที่ใช้ System Software ควบคุมการใช้โปรแกรม ผู้ตรวจสอบส่วนมากจะใช้วิธีวิเคราะห์รหัสคำสั่งของ System Software ที่ใช้ควบคุมการใช้โปรแกรมทั้งชนิดที่เป็นภาษาเขียนและชนิดที่ใช้ประมวลผลได้ และทำการทดสอบขั้นตอนต่าง ๆ ในการควบคุมนั้นผู้ตรวจสอบเพียงแต่ให้ความระมัดระวังเกี่ยวกับการใช้โปรแกรมประเภท Utilities แก้ไขโปรแกรมที่ใช้ปฏิบัติงาน (Executable Program) โดยตรงเท่านั้น

ผู้ตรวจสอบอาจเลือกใช้โปรแกรมคำสั่ง (Software) ให้เปรียบเทียบโปรแกรมภาษาเขียนที่ต้องการตรวจสอบกับโปรแกรมปฏิบัติงาน (executable program) ก็ได้

3. ขั้นตอนการดำเนินงาน (Administrative Procedures)

ผู้ตรวจสอบควรใช้ขั้นตอนการดำเนินงานตามที่กล่าวไว้ในเรื่องการใช้ Audit Test Data กับการวิเคราะห์ในบทนี้เพื่อควบคุมการวิเคราะห์รหัสคำสั่งโปรแกรม



ภาคผนวก ฌ.
รายงานหลักที่ได้จากการประมวลผลด้วยคอมพิวเตอร์

เนื่องจากรายงานที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ของแต่ละธนาคารมีชื่อแตกต่างกัน และข้อมูลที่ปรากฏในรายงานก็มีลักษณะที่แตกต่างกันด้วย ดังนั้น จึงขอสรุปลักษณะของรายงานหลักโดยทั่วไป ดังนี้

1. รายงานที่เกี่ยวกับบัญชีกระแสรายวัน (Demand Deposit Accounting Reports)

(1) รายงานแสดงยอดเงินคงเหลือตามบัญชีเมื่อสิ้นวัน (Daily Trial Balance) รายละเอียดประกอบด้วยยอดคงเหลือประจำวันของลูกค้าแต่ละบัญชี ทั้งด้านเครดิตและเดบิตที่ยกมาจากวันก่อนและยอดสิ้นวัน วันที่เกิดรายการครั้งหลังสุดของแต่ละบัญชีแทนบัญชีแยกประเภทไปในตัว และมีการสรุปยอดให้ด้วย

(2) รายละเอียดสำหรับพิสูจน์ความถูกต้องในการบันทึกบัญชี (Batch Proof Listing) เป็นข้อมูลขั้นต้นที่ฝ่ายบัญชีบันทึกไว้ สามารถตรวจสอบจำนวนเงินได้ทุกรายการ เพื่อใช้ตรวจสอบยอดคุมในแต่ละ batch

(3) รายงานเงินเบิกเกินบัญชี (Overdraft Report) เป็นรายงานแสดงยอดเงินเบิกเกินบัญชีของลูกหนี้แต่ละบัญชี จำนวนวันที่เบิกเกินบัญชี วันที่นำเงินเข้าบัญชีครั้งหลังสุด และจำนวนครั้งที่เบิกเงินเกินบัญชี

(4) รายงานระงับการสั่งจ่ายเงินตามเช็ค (Stop-Hold Report) คือ รายงานเช็คฉบับที่ถูกระงับการสั่งจ่ายเงิน (stop orders) หรือลูกค้าขอให้ยับยั้งการจ่ายเงินไว้ชั่วคราว (hold orders) ตามปกติจะใช้รายงานฉบับนี้ประกอบกับ Float Suspect Report

(5) รายการที่น่าสงสัย (Float Suspect Report) ข้อมูลที่ปรากฏในรายงานจะเป็นรายละเอียดเกี่ยวกับการหมุนเงิน (kiting) เช่น ยอดคงเหลือตามบัญชี จำนวนเงินที่เดบิตและเครดิตแต่ละครั้งในวันก่อน ๆ เป็นต้น

(6) รายงานแสดงรายชื่อลูกค้ารายที่ยอดคงเหลือตามบัญชีมีการเปลี่ยนแปลงสูง (Significant Balance Report)

(7) รายงานแสดงข้อมูลที่ควรเอาใจใส่เป็นพิเศษ (Exceptions Report) เป็นรายงานประจำวันสรุปรายการที่ประมวลผลด้วยคอมพิวเตอร์เพื่อประโยชน์ในการปฏิบัติงานบันทึกบัญชี

(8) รายงานบัญชีที่ไม่เคลื่อนไหว (Dormant Accounts Report) เป็นรายชื่อบัญชีลูกค้ารายที่บัญชีไม่เคลื่อนไหวเป็นเวลานาน (ตั้งแต่ 1 ปีขึ้นไป)

(9) รายงานบัญชีที่ไม่มียอดเงินคงค้างตามบัญชี (Zero Balance Report) เป็นรายชื่อบัญชีลูกค้ารายที่มียอดเงินคงเหลือตามบัญชีเป็นศูนย์ แต่ยังไม่ปิดบัญชี

(10)*รายงานบัญชีที่มีการเรียกเก็บค่าบริการ (Service Charge Report) เป็นรายชื่อบัญชีที่มีการเก็บเงินค่าบริการบางชนิด

(11) รายงานยอดเงินคงค้างตามบัญชีโดยเฉลี่ย (Average Balance Report) ปกติจะออกเป็นรายเดือน แสดงยอดเงินคงค้างตามบัญชีของลูกค้าโดยเฉลี่ยในรอบเดือนก่อน หรือในรอบ 6 เดือน หรือในรอบ 1 ปี และมักจะใช้ประกอบกับ Service Charge Report

(12) รายงานประจำเดือนแสดงความเคลื่อนไหวของบัญชีลูกค้า (Monthly Statement) เป็น statement แสดงการเดบิทและเครดิตในบัญชีลูกค้าทุกรายการ หรืออาจสรุปเฉพาะยอดรวมด้านเดบิทและเครดิตในรอบเดือนที่ผ่านมา เพื่อส่งให้ลูกค้าตามรอบระยะเวลาที่กำหนด

2. รายงานที่เกี่ยวกับเงินฝากที่ต้องจ่ายคืนเมื่อสิ้นระยะเวลา (Time Deposit Reports)

(1) รายงานแสดงยอดเงินฝากคงเหลือตามบัญชี (Trial Balance) มีรายละเอียดเกี่ยวกับยอดเงินฝากคงเหลือของลูกค้าทุกบัญชี และรายการที่เปลี่ยนแปลงจากวันก่อนหรือสัปดาห์ก่อน

(2) รายงานแสดงรายการที่เกิดขึ้นในแต่ละวัน (Transaction Journal)

(3) รายงานดอกเบี้ยเงินฝาก (Interest Report) แสดงดอกเบี้ยค้างจ่ายที่คิดให้แก่ลูกค้าแต่ละบัญชีนับแต่วันฝากจนถึงวันที่ออกรายงาน

(4)* รายงานแสดงจำนวนดอกเบี้ยทั้งปีที่ธนาคารจ่ายให้ลูกค้าแต่ละราย (W - 2 Forms) เพื่อส่งให้ลูกค้าไปเสียภาษีเงินได้

3. รายงานเงินให้กู้ยืมชนิดผ่อนชำระเป็นงวด (Installment Loan Reports)

(1) รายงานแสดงยอดหนี้คงค้าง (Trial Balance) รายละเอียดประกอบด้วยยอดหนี้คงค้างทั้งสิ้น จำนวนเงินที่จะต้องผ่อนชำระในงวดที่จะถึงกำหนดชำระ วันที่ถึงกำหนดชำระ จำนวนดอกเบี้ยที่คิดจากลูกค้ามากเกินไป ซึ่งจะต้องปรับปรุงคืนให้ลูกค้าในงวดสุดท้าย

(2) รายงานลูกหนี้รายใหม่ (New Loan Journal) ประกอบด้วยรายละเอียดเกี่ยวกับลูกหนี้รายใหม่แต่ละราย

(3) สมุดคูปองสำหรับการชำระหนี้ในแต่ละงวด (Coupon Books) เป็นเอกสารแสดงการชำระหนี้ในแต่ละงวด ซึ่งธนาคารจะมอบให้ลูกหนี้รายใหม่ไว้ทุกราย เพื่อให้ลูกหนี้ฉีกส่งให้ธนาคารเป็นหลักฐานในการชำระหนี้แต่ละงวด

(4) ใบทวงหนี้ที่เกินกำหนดชำระ (Past-Due Notices) เป็นใบทวงหนี้ที่ส่งไปยังลูกหนี้ที่มิได้ชำระหนี้ตามกำหนด

---

* รายงานประเภทนี้ธนาคารพาณิชย์ในประเทศไทยยังไม่ได้ใช้

(5) รายงานหนี้ที่เกินกำหนดชำระ (Delinquency Report) เป็นรายละเอียดเกี่ยวกับลูกหนี้รายที่ไม่ชำระหนี้ตามกำหนด จำนวนครั้งและจำนวนเงินที่ขาดการผ่อนชำระ วันที่ไม่ชำระตามกำหนด

(6) รายงานการชำระหนี้ที่เกินกำหนดชำระ (Report of Transactions of Delinquents)

(7) รายงานหนี้ที่เกินกำหนดชำระเป็นระยะเวลานาน (Age Delinquency Report) เป็นรายงานแสดงลูกหนี้ที่ไม่ชำระหนี้ตามกำหนดเป็นระยะเวลานาน ส่วนจะนานแค่ไหนนั้นสุดแล้วแต่ธนาคารจะกำหนด

(8) รายงานหนี้ที่ได้รับการอนุมัติให้ยืดระยะเวลาการชำระหนี้ (Extension Report) เป็นรายละเอียดเกี่ยวกับลูกหนี้รายที่ธนาคารอนุมัติให้ยืดเวลาการชำระหนี้ออกไปอีก

(9) รายงานการชำระหนี้ครบจำนวน (Closed Loan Journal) มีรายละเอียดเกี่ยวกับลูกหนี้รายที่ชำระหนี้หมดสิ้นตามสัญญา

(10) รายงานสรุปเงินให้กู้ยืมประจำเดือน (Monthly Summary of Loans) เป็นรายงานแสดงเงินให้กู้ยืมคงค้างประจำเดือน วันที่ให้กู้ยืม จำนวนครั้งและจำนวนเงินที่ลูกหนี้ได้ชำระหนี้ ดอกเบี้ยที่เรียกเก็บจากลูกหนี้ และวันครบกำหนดสัญญา

4. รายงานทั่ว ๆ ไป

(1) รายงานสรุปผลการปฏิบัติงานประจำวัน (Summary Report) แสดงจำนวนรายการที่ผ่านเครื่องคอมพิวเตอร์ตลอดวัน ยอดรวมด้านเดบิทและเครดิต ยอดดุลในวันก่อน และยอดดุลเมื่อสิ้นวัน นอกจากนี้ยังอาจแสดงจำนวนบัญชีที่ปิดและเปิดใหม่ เงินเบิกเกินบัญชี ฯลฯ

(2) รายงานชื่อและที่อยู่ของลูกค้า (Name and Address Report) แสดงรายชื่อและที่อยู่ของลูกค้าเรียงตามเลขที่บัญชีหรือตัวอักษร

(3) รายงานการเปลี่ยนชื่อและที่อยู่ของลูกค้า (Name and Address Change Report)

(4) รายชื่อบัญชีที่เปิดใหม่ (New Account Report) ปกติจะออกเป็นรายวันแยกตามประเภทบัญชี

(5) รายงานการปิดบัญชีลูกค้า (Closed Account Report) แสดงรายชื่อบัญชีที่ยอดคงเหลือตามบัญชีเป็นศูนย์ และ/หรือบัญชีที่ลูกค้าปิดบัญชีโดยแยกตามประเภทบัญชี

(6) รายงานแสดงรายการที่ประมวลผลไม่ได้ (Rejected Item Report) แสดงรายละเอียดเกี่ยวกับรายการที่ประมวลผลไม่ได้ และรหัสแสดงสาเหตุที่คอมพิวเตอร์ไม่สามารถประมวลผล



บรรณานุกรม*

1. EDP Examination Handbook by Federal Financial Institution Examination Council (FFIEC - USA.).
2. An Audit Approach to Computer by Bakin Jenkins & Anthony Pinkney.
3. System Auditability and Control by Standford Research Institute.
4. Auditing Bank EDP Systems by Bank Administration Institute.
5. Auditing Computer (Applications) by Keagle W. Davis and William E. Perry.
6. Statement on Internal Control in a Computer Based Accounting System ของ Institute of Chartered Accountant and Wales.
7. Audit and Accounting Guide : The Auditor's Study and Evaluation of Internal Control in EDP Systems - AICPA.
8. Auditing Guidelines : Internal Controls in Computer Based Accounting Systems.
9. The Institute of Chartered Accountant in England and Wales.
10. Specimen Questions for Evaluating the System of Internal Control in a Computer-Based Accounting System : Institute of Chartered Accountants in England and Wales.
11. Auditing EDP Systems by Donald A Watne and Peter B.B. Turney.

**หมายเหตุ : ผิด ตก ยกเว้น*

บันทึก

บันทึก

บันทึก

พิมพ์ที่ : ห้างหุ้นส่วนจำกัด โรงพิมพ์คลังนานาวิทยา
33/17-18 ถ.หน้าเมือง อ.เมือง จ.ขอนแก่น 40000 โทร. (043) 236344, 332152-3

