2

มาตรฐานขั้นต่ำสำหรับการควบคุมภายใน และการรักษาความปลอดภัย เกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ ของสถาบันการเงินและองค์กรทั่วไป

มาตรฐานขั้นต่ำสำหรับการควบคุมภายในและการรักษาความปลอดภัยเกี่ยวกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ของสถาบันการเงินและองค์กรทั่วไป

1. บทนำ

การนำระบบคอมพิวเตอร์มาใช้ในการประกอบธุรกิจ และการประมวลผลข้อมูลของสถาบันการเงินรวมทั้งองค์กรอื่น 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 แผนงานและระเบียบปฏิบัติตามที่ฝ่ายบริหารกำหนด การกำหนดขอบเขตและลักษณะการควบคุมภายในที่ดีควรคำนึงถึงขนาดธุรกิจ ปริมาณธุรกิจ และลักษณะการนำคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูล

ดังนั้น เพื่อให้สถาบันการเงินที่ใช้ระบบคอมพิวเตอร์ในการให้บริการทางธุรกิจ และการประมวลผลข้อมูลมีแนวทางในการกำหนดการควบคุมภายในที่สามารถป้องกันหรือลดความเสี่ยงต่อความเสียหายที่กล่าวข้างต้นได้ 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 แต่ในโปรแกรมควรมีคำสั่งงานที่เกี่ยวกับการเช็คสอบความควบถ้วนของจำนวนข้อมูล (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 ทุกครั้งที่จะปรับปรุงแก้ไขโปรแกรมระบบงานควรกำหนดให้หน่วยงานผู้ใช้โปรแกรมระบบงานจัดทำหลักฐานใบคำขอระบุเหตุผลและความต้องการแก้ไข 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 และเป็นงานด้านที่ไม่สร้างสรร จึงมักถูกปล่อยปละละเลยอยู่เสมอ 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) รายการโปรแกรมชุดปัจจุบัน (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 ในระบบปฏิบัติการเครื่องคอมพิวเตอร์ขนาดใหญ่โดยทั่วไป 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 ซึ่งหากมีการขโมยไปถึงมือบุคคลภายนอกแล้วไม่สามารถนำไปใช้ประโยชน์ได้

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 การตรวจเช็คหัวรายการ 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 จึงต้องมีการควบคุมดูแลอุปกรณ์ที่ว่างในขณะที่ยังไม่ได้นำไปใช้งานประมวลผลอย่างรัดกุม เพื่อป้องกันมิให้เกิดความเสียหาย ดังนี้

3.1) ควรเก็บรักษาอุปกรณ์บันทึกข้อมูลขณะที่ไม่ได้นำไปใช้งานประมวลผลไว้ในสถานที่ปลอดภัย มีการควบคุมอุณหภูมิ ความชื้น ฝุ่นละออง การป้องกันเพลิงไหม้ อุปกรณ์ดับเพลิง และจัดให้มีเจ้าหน้าที่เฉพาะควบคุมดูแลการนำออกไปใช้งาน และมีการตรวจนับจำนวนคงเหลือเป็นครั้งคราว

3.2) ควรจัดทำป้ายชื่อติดกำกับภายนอกอุปกรณ์บันทึกข้อมูล ภายในบริเวณหัวและท้ายแฟ้มข้อมูลควรบันทึกข้อมูลเกี่ยวกับชื่อแฟ้มข้อมูลวันที่และจำนวนรายการข้อมูลทั้งหมดที่บรรจุอยู่ในแฟ้มข้อมูลนั้น

3.3) ควรมีอุปกรณ์บันทึกข้อมูลชุดสำเนา (Back-up file) แยกเก็บไว้ในที่ที่ปลอดภัยห่างจากอาคารที่ทำการประมวลผลข้อมูล

3.1.3 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 สถาบันการเงินควรฝึกฝนพนักงานให้สามารถปฏิบัติงานตามแบบเต็มได้ 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 เนื่องจากกระดาษทำการเป็นหลักฐานสำคัญที่แสดงถึงขอบเขต 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 แบบตั้งลำพังในตัวเอง (Stand alone) หรือเป็นเทอร์มินัลของเครื่องคอมพิวเตอร์ใหญ่ (Computer Terminal) หรือเป็นเครือข่ายภายในสำนักงาน (Local area network) การใช้งานไมโครคอมพิวเตอร์เป็นไปด้วยความสะดวก ผู้ที่ไม่มีความรู้ทางคอมพิวเตอร์เทคนิคก็สามารถเรียนรู้และใช้งานไมโครคอมพิวเตอร์ได้ไม่ยาก เป็นระบบประมวลผลข้อมูลแบบเบ็ดเสร็จด้วยบุคคลเพียงคนเดียว ไม่มีการแบ่งแยกหน้าที่ปฏิบัติงาน ซึ่งแตกต่างไปจากระบบการประมวลผลด้วยเครื่องคอมพิวเตอร์ขนาดใหญ่ ดังนั้นหากไม่มีการควบคุมที่เหมาะสมก็อาจก่อให้เกิดความเสียหายได้ง่ายต่อเครื่องไมโครคอมพิวเตอร์ แฟ้มข้อมูล และโปรแกรม สถาบันการเงินที่มี เครื่องไมโครคอมพิวเตอร์ไว้ใช้งาน 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 เพื่อป้องกันมิให้ผู้ไม่มีสิทธิใช้เครื่องและข้อมูลในเครื่อง กรณีเป็นไมโครคอมพิวเตอร์ที่ใช้ร่วมกันหลายงานและหลายคน ควรกำหนดรหัสประจำตัวผู้มีสิทธิเข้าถึงแฟ้มข้อมูลและโปรแกรม (Identification code) และรหัสการใช้งาน (password) ซึ่งระบุขอบเขตของการใช้งานแฟ้มข้อมูลและโปรแกรมดังกล่าว

3) ควรจัดทำสำเนาแฟ้มข้อมูลและโปรแกรมที่สำคัญ ๆ ไว้ใช้ทดแทนในกรณีที่แฟ้มข้อมูลและโปรแกรมที่ใช้อยู่ปัจจุบันสูญหาย หรือเสียหายจนใช้การไม่ได้ เพื่อป้องกันมิให้การประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์หยุดชะงัก

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

3.2.3 การตรวจสอบการประมวลผลข้อมูลด้วยไมโครคอมพิวเตอร์

ควรมอบหมายให้ผู้ตรวจสอบภายในหรือหน่วยงานที่ไม่เกี่ยวข้องกับการประมวลผลข้อมูลตรวจสอบการรักษาความปลอดภัยไมโครคอมพิวเตอร์ แฟ้มข้อมูล และโปรแกรม การจัดทำสำเนาแฟ้มข้อมูลและโปรแกรม และตรวจสอบความถูกต้องของข้อมูลและรายงานที่ได้จากการประมวลผล