

บทที่ 6
การควบคุมคุณภาพในสารสนเทศ

การจัดการคุณภาพสารสนเทศ
Information Quality Management
รหัส 4114311

ผู้ช่วยศาสตราจารย์จันทนา มีชัยชนะ
สาขาคอมพิวเตอร์
คณะวิทยาศาสตร์เทคโนโลยีและการเกษตร มหาวิทยาลัยราชภัฏยะลา

เนื้อหา

- บทนำ
- การควบคุมทั่วไปในระบบสารสนเทศ
- การกำหนดนโยบายการใช้สารสนเทศ
- การแบ่งแยกหน้าที่งานในระบบสารสนเทศ
- การควบคุมโครงการพัฒนาระบบสารสนเทศ
- การควบคุมการเปลี่ยนแปลงแก้ไขระบบ
- การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์
- การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์
- การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์
- การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ

เนื้อหา

- การควบคุมการเข้าถึงระบบงาน
- การควบคุมการจัดเก็บข้อมูล
- การควบคุมการสื่อสารข้อมูล
- การกำหนดมาตรฐานเอกสารระบบสารสนเทศ
- การลดความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์
- การวางแผนแก้ไขความเสียหายจากเหตุฉุกเฉิน
- การควบคุมระบบงานและการควบคุมการเข้าระบบหรือข้อมูล
- การควบคุมเกี่ยวกับการนำข้อมูลเข้า
- การควบคุมความถูกต้องของการปรับยอดบัญชีและการควบคุมความครบถ้วนของการปรับยอดบัญชี

บทนำ

การควบคุมทั่วไปในระบบสารสนเทศ ซึ่งเป็นกิจกรรมที่เกี่ยวข้องกับระบบสารสนเทศและทรัพยากรสารสนเทศในองค์กรที่ผู้บริหารควรให้ความสำคัญ ถึงแม้ว่าวัตถุประสงค์ของการควบคุมภายในจะไม่ขึ้นอยู่กับวิธีการประมวลผล แต่การกำหนดนโยบายและขั้นตอนการปฏิบัติงานที่แตกต่างออกไปสำหรับระบบสารสนเทศ อาจทำให้วิธีการควบคุมแตกต่างไปจากเดิม ตัวอย่างเช่น แม้ว่าการประมวลผลข้อมูลด้วยคอมพิวเตอร์ อาจช่วยลดข้อผิดพลาดในการทำงานของพนักงานได้ แต่ในขณะเดียวกันก็จะเพิ่มความเสี่ยงในการเข้าถึงข้อมูล หรือ การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาตในส่วนของ การแบ่งแยกหน้าที่งานระหว่างหน้าที่การบันทึกรายการ การเก็บรักษาทรัพย์สิน และการอนุมัติสำหรับระบบสารสนเทศจะแตกต่างไปจากเดิม เนื่องจากโปรแกรมคอมพิวเตอร์ที่ใช้อาจใช้ในการทำงานสำหรับแต่ละหน้าที่หรือทุกหน้าที่ ดังกล่าว อย่างไรก็ตาม การใช้คอมพิวเตอร์จะช่วยเพิ่มโอกาสในการควบคุมภายในที่ดีขึ้น

บทนำ(ต่อ)

การควบคุมระบบสารสนเทศอาจจัดเป็นประเภทต่าง ๆ ได้หลายวิธี วิธีที่เป็นที่นิยม เช่น การจำแนกประเภทการควบคุมตามลักษณะ (Classification by setting) และการจำแนกประเภทการควบคุมตามระดับความเสี่ยง (Classification by risk aversion) การจำแนกประเภทการควบคุมตามลักษณะของการควบคุม สามารถจำแนกเป็น 2 ประเภท ได้แก่

- 1) การควบคุมทั่วไป
- 2) การควบคุมระบบงาน

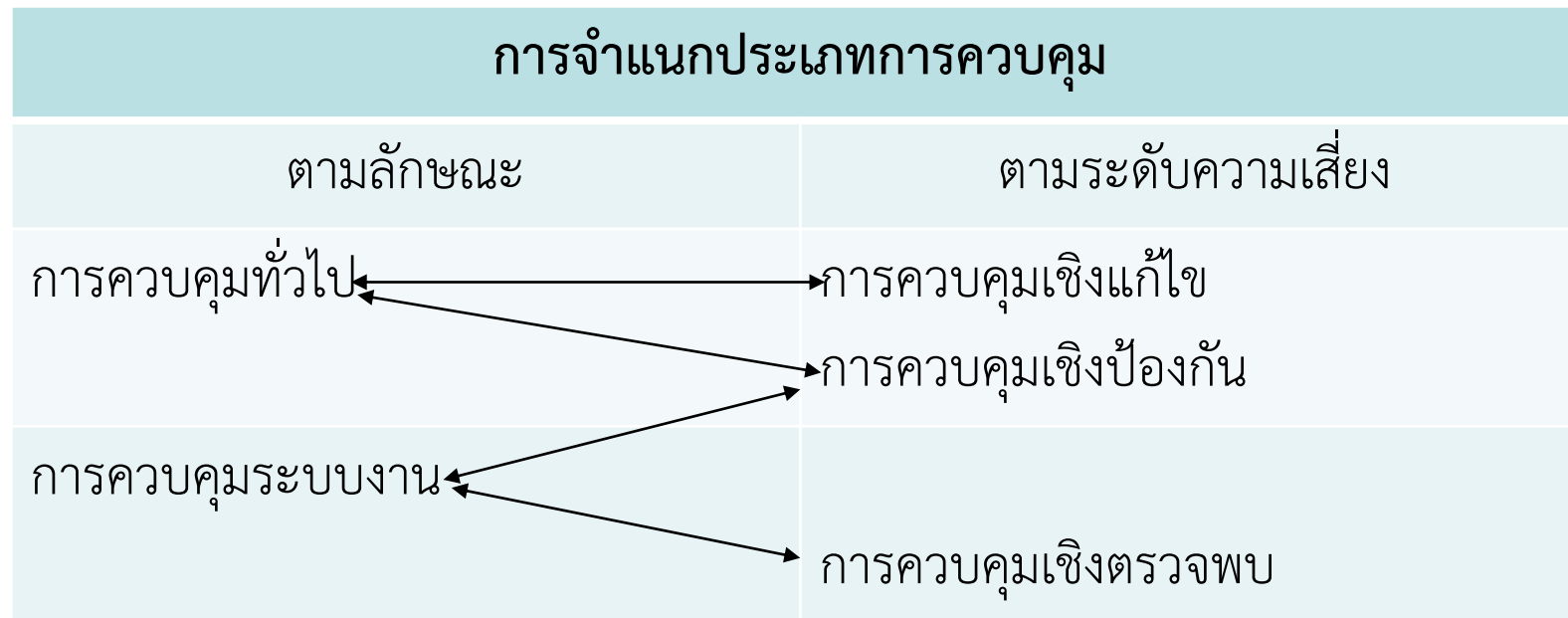
บทนำ(ต่อ)

การจำแนกประเภทการควบคุมตามระดับความเสี่ยงอาจแบ่งได้เป็น 3 ประเภท ได้แก่

- 1) **การควบคุมเชิงป้องกัน (Preventive control)** เป็นการดำเนินการล่วงหน้าเพื่อป้องกันไม่ให้เกิดข้อผิดพลาดหรือความเสียหายขึ้น ตัวอย่างเช่น การจัดให้มีคู่มือปฏิบัติงานเพื่อป้องกันความผิดพลาดที่เกิดขึ้นในการปฏิบัติงาน เป็นต้น
- 2) **การควบคุมเชิงตรวจพบ (Detective control)** เป็นการดำเนินการเพื่อให้สามารถตรวจพบภัยคุกคาม หรือข้อผิดพลาดที่เกิดขึ้น ตัวอย่างเช่น การสอบทานความถูกต้องของข้อมูลที่ได้มีการบันทึกในระบบคอมพิวเตอร์ ก่อนการประมวลผล เป็นต้น
- 3) **การควบคุมเชิงแก้ไข (Corrective control)** เป็นการดำเนินการเพื่อแก้ไขข้อผิดพลาดหรือความเสียหายที่ตรวจพบ เช่น การปรับปรุงรายการเพื่อแก้ไขข้อผิดพลาดทางการบัญชี เมื่อตรวจพบข้อผิดพลาดจากการตรวจสอบงบทดลอง เป็นต้น

บทนำ(ต่อ)

ความสัมพันธ์ของการจำแนกประเภทการควบคุมดังกล่าวข้างต้นสามารถแสดงได้ดังภาพ 6.1 ซึ่งจะเห็นว่าการควบคุมทั่วไปจะรวมถึงการควบคุมเชิงป้องกันและการควบคุมเชิงแก้ไข ส่วนการควบคุมระบบงานจะรวมถึงการควบคุมป้องกันและการควบคุมเชิงตรวจพบ



ภาพ 6.1 แสดงการจำแนกประเภทการควบคุม

การควบคุมทั่วไปในระบบสารสนเทศ

การควบคุมทั่วไปในระบบสารสนเทศ หมายถึงการควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุมภายใน (internal control environment) นโยบายและวิธีการในการควบคุมระบบสารสนเทศ การจัดแบ่งส่วนงานและหน้าที่ รวมทั้งวิธีการปฏิบัติงานของผู้ที่เกี่ยวข้องกับระบบสารสนเทศ การควบคุมความปลอดภัยระบบ การควบคุมการพัฒนาและปรับปรุงระบบ และการป้องกันความเสียหายหรือลดความเสียหายของระบบ การควบคุมทั่วไปเป็นการควบคุมภายในสำหรับระดับองค์กร หรือการควบคุมที่ควรมีในทุก ๆ ส่วนของระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อให้เกิดความมั่นใจว่าระบบคอมพิวเตอร์โดยรวมขององค์กรมีความเสถียร (stable) มีการจัดการที่ดี และเป็นส่วนหนึ่งที่จะก่อให้เกิดบูรณภาพ (integrity) ของระบบสารสนเทศของกิจการ ซึ่งแตกต่างจากการควบคุมภายในของระบบงาน ซึ่งใช้เฉพาะในระบบงานแต่ละระบบ เช่น ระบบลูกหนี้ หรือระบบเงินเดือนและค่าแรง เป็นต้น

การควบคุมทั่วไปในระบบสารสนเทศ(ต่อ)

การควบคุมทั่วไปในระบบสารสนเทศประกอบด้วยกิจกรรมต่าง ๆ ได้แก่

- การกำหนดนโยบายการใช้สารสนเทศ
- การแบ่งแยกหน้าที่งานในระบบสารสนเทศ
- การควบคุมโครงการพัฒนาระบบสารสนเทศ
- การควบคุมการเปลี่ยนแปลงแก้ไขระบบ
- การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์
- การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์

การควบคุมทั่วไปในระบบสารสนเทศ(ต่อ)

- การควบคุมการเข้าถึงระบบงาน
- การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ
- การควบคุมการจัดเก็บข้อมูล
- การควบคุมการ สื่อสารข้อมูล
- การกำหนดมาตรฐานของเอกสารระบบสารสนเทศ
- การลดความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์
- การวางแผนแก้ไขความเสียหายจากเหตุฉุกเฉิน

การกำหนดนโยบายการใช้สารสนเทศ

การรักษาความปลอดภัยของข้อมูลและสารสนเทศเป็นการควบคุมที่สำคัญอย่างหนึ่ง จึงต้องมีการกำหนดเป็นนโยบาย โดยมีการทบทวนเพื่อทำการปรับปรุงอย่างต่อเนื่องในการกำหนดนโยบายเกี่ยวกับความปลอดภัยของข้อมูลและการใช้งานนั้น เริ่มจากการพิจารณาว่า ใคร ต้อง เข้าถึงข้อมูลอะไร เมื่อไร และข้อมูลนั้นอยู่ใน ระบบงานใด ซึ่งการพิจารณาดังกล่าวจะเป็นปัจจัยในการระบุภัยคุกคาม (threat) ความเสี่ยง (risk) และผลของความเสียหาย (exposure) ที่จะมีต่อระบบสารสนเทศ เพื่อให้สามารถเลือกวิธีการรักษาความปลอดภัยที่เหมาะสมที่สุด และคุ้มค่ากับการลงทุน (cost-effective) โดยผู้บริหารระดับสูง ควรมีหน้าที่ในการกำหนดนโยบาย กำกับดูแล และควบคุมให้เป็นไปตามนโยบายที่กำหนดไว้ โดยมีการทบทวนและปรับปรุงอย่างต่อเนื่อง รวมทั้งชี้แจงให้ผู้ปฏิบัติงานที่เกี่ยวข้องทุกคนรับทราบ

การแบ่งแยกหน้าที่งานในระบบสารสนเทศ

วิธีการหนึ่งในการควบคุมระบบสารสนเทศขององค์กร คือการแบ่งแยกหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน ระบบงานคอมพิวเตอร์ให้ชัดเจน เพื่อลดโอกาสที่จะเกิดความผิดพลาดจากการปฏิบัติงานและโอกาสการทุจริตของผู้ปฏิบัติงานที่ไม่ถูกจำกัดสิทธิในการเข้าถึงระบบงาน โปรแกรม และข้อมูล โดยมีประเภทงานที่ควรมีการแบ่งแยกผู้ปฏิบัติงานดังนี้

- 1) งานวิเคราะห์ระบบ (system analysis) นักวิเคราะห์ระบบ (system analyst) เป็นผู้ที่ทำงานร่วมกับผู้ใช้ ในการพิจารณาถึงสารสนเทศที่ผู้ใช้ต้องการใช้งาน และออกแบบระบบงานให้ตรงกับความต้องการใช้งาน
- 2) งานเขียนโปรแกรม (programming) โปรแกรมเมอร์ (programmer) เป็นผู้นำระบบงานที่นักวิเคราะห์ระบบ ออกแบบไว้มาเขียนโปรแกรมสร้างระบบงาน

การแบ่งแยกหน้าที่งานในระบบสารสนเทศ(ต่อ)

4) งานของผู้ใช้ (user) หน่วยงานของผู้ใช้เป็นหน่วยงานที่สร้างข้อมูลรายการธุรกิจ กำกับ ดูแลข้อมูลที่ใช้ประมวลผล และใช้ผลลัพธ์จากการประมวลผลของระบบงาน

5) งานบรรณารักษ์ระบบ (system library) บรรณารักษ์ระบบ (system librarian) เป็นผู้เก็บรักษาและดูแล เพิ่มข้อมูลที่มีการจัดเก็บไว้ในเทปแม่เหล็กและจานแม่เหล็กในขณะที่ไม่ได้เชื่อมตรงกับระบบคอมพิวเตอร์ (offline)

6) งานควบคุมข้อมูล (data control) กลุ่มผู้ควบคุมข้อมูล (data control group) มีหน้าที่ในการรับรองความถูกต้อง สอบทานการทำงานผ่านเครื่องคอมพิวเตอร์ยืนยันข้อมูลเข้าและผลลัพธ์ที่ได้จากการประมวลผล แก้ไขรายการ นำเข้าที่ผิดพลาด และแจกจ่ายผลลัพธ์ที่ได้จากการประมวลผล

การแบ่งแยกหน้าที่งานในระบบสารสนเทศ(ต่อ)

ทั้งนี้ การอนุญาตให้ผู้ปฏิบัติงานทำงานได้หลายประเภทงาน จะเป็นการเปิดโอกาสให้ มีการทุจริตได้ง่าย ตัวอย่างเช่น นักเขียนโปรแกรมของหน่วยงานที่ได้รับสิทธิให้เข้าถึงและนำข้อมูลจริงมาใช้ในการทดสอบโปรแกรม อาจทำการลบหรือแก้ไขเปลี่ยนแปลงรายการเงินกู้ของตนเอง หรือนักปฏิบัติการ คอมพิวเตอร์ที่สามารถเข้าถึงโปรแกรมที่ติดตั้งในระดับตรรกะ (logic) อาจทำการแก้ไขเปลี่ยนแปลงโปรแกรมเพื่อให้ประมวลผลเพิ่มเงินค่าจ้างของตนเอง เป็นต้น

การควบคุมโครงการพัฒนาระบบสารสนเทศ

การพัฒนาระบบสารสนเทศที่ขาดการควบคุมการบริหารจัดการที่ดี ก่อให้เกิดความเสี่ยงในการที่ระบบไม่สามารถตอบสนองความต้องการทางธุรกิจ และระบบงานที่พัฒนาขึ้นอาจไม่มีการควบคุมภายในที่เพียงพอ ทำให้ทำงานผิดพลาด นอกจากนั้น ยังเป็นผลให้กิจการสูญเสียเงินลงทุนจำนวนมากในโครงการพัฒนาระบบสารสนเทศ การควบคุมโครงการพัฒนาระบบสารสนเทศ ประกอบด้วย

1) แผนแม่บทระยะยาว (long-range master plan) เป็นแผนงานที่แสดงให้เห็นทิศทางของเทคโนโลยีและโครงสร้างของโครงการต่าง ๆ ที่จะตอบสนองความต้องการเป้าหมายขององค์กรในระยะยาวซึ่งส่วนใหญ่จะเป็นแผนงานในระยะ 3-5 ปี

2) แผนงานพัฒนาระบบ (project development plan) เป็นแผนงานที่แสดงให้เห็นว่าจะดำเนินโครงการอย่างไร ประกอบด้วย รายละเอียดขั้นตอนของงาน ผู้ปฏิบัติงานในแต่ละขั้นตอนช่วงเวลาในการปฏิบัติงาน ค่าใช้จ่ายโครงการในแต่ละขั้นตอนและรายการอื่น ๆ โดยในแผนงานนั้นควรระบุการวัดความก้าวหน้าของโครงการ (project milestone) หรือจุดสำคัญที่จะใช้ในการสอบทานความก้าวหน้าของโครงการ และใช้ในการเปรียบเทียบระยะเวลาที่ใช้จริงกับประมาณการ

การควบคุมโครงการพัฒนาระบบสารสนเทศ(ต่อ)

3) กำหนดการประมวลผลข้อมูล (data processing schedule) เพื่อให้มีการใช้ทรัพยากรสารสนเทศในองค์กรให้เกิดประโยชน์สูงสุด ควรกำหนดให้งานประมวลผลข้อมูลทุกงานที่การดำเนินการตามตารางเวลาที่กำหนดไว้

4) การมอบหมายหน้าที่และความรับผิดชอบ (assignment of responsibility) โครงการพัฒนาระบบแต่ละโครงการจะต้องมีการกำหนดผู้จัดการโครงการและทีมงาน รวมถึงหน้าที่และความรับผิดชอบของแต่ละคน โดยผู้จัดการโครงการและทีมงานจะมีหน้าที่รับผิดชอบโดยตรงต่อความสำเร็จหรือความล้มเหลวของโครงการ

5) การประเมินผลงานระหว่างการดำเนินโครงการ (periodic performance evaluation) โดยควรมีการแบ่งแยกงานออกเป็นแต่ละส่วน (module หรือ task) ซึ่งจะแยกย่อยมาจาก ประเภทงานต่าง ๆ ตามแผนงาน เพื่อประเมินผลการดำเนินงานของบุคคลที่รับผิดชอบงานในแต่ละส่วน

การควบคุมโครงการพัฒนาระบบสารสนเทศ(ต่อ)

6) การสอบทานภายหลังการติดตั้งระบบและนำระบบมาใช้งาน (post-implementation review) หลังจากโครงการพัฒนาระบบได้เสร็จสิ้นลง ควรมีการสอบทานเพื่อพิจารณาว่าผลประโยชน์ที่ได้รับเป็นไปตามที่คาดหวังไว้หรือไม่ การสอบทานดังกล่าวจะช่วยในการควบคุมกิจกรรมการพัฒนาระบบ และส่งเสริมให้มีการประมาณการต้นทุนและผลประโยชน์อย่างถูกต้องแม่นยำ และมีหลักการตั้งแต่ในระยะเริ่มต้นโครงการ

7) การวัดผลการดำเนินงานของระบบ (system performance measurement) เพื่อให้มีการประเมินระบบงานที่พัฒนาขึ้นอย่างเหมาะสม การวัดผลโดยทั่วไปอาจรวมถึงการวัดปริมาณงาน (throughput) การวัดอัตราประโยชน์ (utilization) และการวัดระยะเวลาตอบสนอง(response time) เป็นต้น

การควบคุมการเปลี่ยนแปลงแก้ไขระบบ

การแก้ไขเปลี่ยนแปลงระบบโดยไม่ได้รับอนุญาต อาจมีผลให้เกิดความผิดพลาด ในโปรแกรม การทุจริต หรือมีข้อมูลที่ไม่ถูกต้องในงบการเงินและรายงานต่าง ๆ และอาจทำให้ระบบล้มเหลวหรือหยุดชะงักการทำงานได้ การเปลี่ยนแปลงแก้ไขระบบหรือโปรแกรมที่ใช้อยู่ จึงควรมีการกำหนดเป็นขั้นตอน โดยมีการอนุมัติและจัดทำเอกสารประกอบ โดยผู้สอบบัญชีควรมีการสอบถามความเพียงพอของการควบคุมภายในของระบบงาน หรือโปรแกรมที่มีการเปลี่ยนแปลงแก้ไขนั้นการควบคุมเปลี่ยนแปลงแก้ไขระบบประกอบด้วย

- 1) การกำหนดระเบียบวิธีการปฏิบัติในการเปลี่ยนแปลงแก้ไขระบบที่เป็นลายลักษณ์อักษร และมีการอนุมัติจากเจ้าของระบบงาน
- 2) มีการศึกษาผลกระทบต่าง ๆ ทั้งผลกระทบทางด้านเทคนิค ผลกระทบที่มีต่อระบบอื่น และความเสี่ยงจากการเปลี่ยนแปลง

การควบคุมการเปลี่ยนแปลงแก้ไขระบบ(ต่อ)

- 3) มีการทดสอบระบบที่แก้ไขแล้ว ก่อนนำมาใช้งาน
- 4) จัดทำเอกสารคู่มือประกอบการแก้ไขเปลี่ยนแปลงทั้งหมด และมีการแก้ไขเอกสารที่เกี่ยวข้องเช่น คู่มือการใช้งาน คู่มือระบบ ข้อมูลเกี่ยวกับการรักษาความปลอดภัยระบบ และตารางการทำงานของผู้ปฏิบัติงานคอมพิวเตอร์ เป็นต้น
- 5) มีการประเมินผลและสอบทานระบบงานหรือโปรแกรมภายหลังจากเริ่มใช้งานในระยะเวลาหนึ่ง

การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์

ศูนย์คอมพิวเตอร์เป็นหน่วยงานที่ให้บริการคอมพิวเตอร์แก่หน่วยงานอื่น การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์ประกอบด้วย การประมวลผลระบบงาน การสำรองข้อมูล และการจัดการปัญหาของระบบเพื่อส่งต่อให้ผู้ที่เกี่ยวข้องทำการแก้ไข

1) การประมวลผลระบบงาน การประมวลผลระบบงานควรมีการจัดทำตารางการประมวลผล โดยได้รับอนุมัติจากเจ้าของระบบงานนั้น ๆ และในแต่ละขั้นตอนของการประมวลผลต้องมีการบันทึกข้อมูลการทำงาน รวมทั้งปัญหาที่เกิดขึ้นและการดำเนินการแก้ไข เพื่อใช้ในการสอบทาน

2) การสำรองข้อมูล การสำรองข้อมูล (Data backup) เป็นวิธีการที่จะช่วยป้องกันข้อมูลจากการสูญหายเนื่องจากเหตุการณ์ต่าง ๆ ที่ทำให้ข้อมูลถูกทำลาย ลักษณะของการสำรองข้อมูลขึ้นอยู่กับวิธีการประมวลผลและเทคโนโลยีที่ใช้ในระบบสารสนเทศทางการบัญชี การควบคุมภายในเกี่ยวกับการสำรองข้อมูลมีดังต่อไปนี้

(1) ผู้บริหารควรกำหนดนโยบายเกี่ยวกับการสำรองข้อมูลและการกู้คืนข้อมูลในกรณีที่ข้อมูลถูกทำลาย

การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์(ต่อ)

(2) มีการสำรองข้อมูลเป็นประจำ โดยจัดทำตารางเวลาการทำงานเกี่ยวกับการสำรองข้อมูลของแต่ละระบบงานไว้เป็นส่วนหนึ่งของตารางการประมวลผล และจัดทำตารางเวลาสำหรับการสำรองโปรแกรมและข้อมูลอื่น ๆ แยกต่างหาก

(3) จัดเก็บข้อมูลสำรองไว้นอกสถานที่แยกต่างหากจากข้อมูลจริง โดยมีการกำหนดระเบียบวิธีในการนำไปจัดเก็บ

(4) ทดสอบข้อมูลสำรองเป็นระยะ ๆ โดยการทดลองนำข้อมูลสำรองที่จัดทำไว้มาทำการกู้คืนข้อมูล และทดสอบแฟ้มข้อมูลที่กู้คืนอย่างสม่ำเสมอ

การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์(ต่อ)

(5) กำหนดเงื่อนไขในการนำเทปหรือดิสก์กลับมาใช้ใหม่ในการจัดเก็บข้อมูลสำรอง และเนื่องจากเทปหรือดิสก์มีอายุใช้งานจำกัด จึงควรมีการหมุนเวียนนำเทปหรือดิสก์ใหม่มาเปลี่ยนแทนอย่างสม่ำเสมอ นอกจากนี้เทปหรือดิสก์บางส่วนที่ใช้จัดเก็บข้อมูลสำรองอาจต้องมีการจัดเก็บอย่างถาวร เพื่อให้มีข้อมูลสำรองทั้งหมดสำหรับแต่ละเดือน

(6) จัดทำสารบบ (directory) สำหรับเทปหรือดิสก์ที่จัดเก็บไว้ทั้งหมด

(7) ในการกู้คืนข้อมูลและเริ่มต้นระบบงานใหม่ (recovery and restart) ควรมีการกำหนดขั้นตอนการทำงานที่เป็นลายลักษณ์อักษร และบันทึกการทำงานที่เกี่ยวข้องเพื่อใช้ในการสอบทาน

3) การจัดการปัญหาของระบบ ในกรณีที่ระบบคอมพิวเตอร์มีปัญหาหรือมีข้อผิดพลาดในการทำงาน เช่น ข้อผิดพลาดของโปรแกรม ปัญหาของระบบเครือข่าย ปัญหาเกี่ยวกับระบบปฏิบัติการ เป็นต้น ผู้ปฏิบัติงานคอมพิวเตอร์ควรมีการพิจารณาถึงสาเหตุของปัญหาหรือข้อผิดพลาดนั้น เพื่อส่งต่อให้ผู้ที่เกี่ยวข้องทำการแก้ไข

การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์

การเข้าถึงอุปกรณ์คอมพิวเตอร์ หมายถึงความสามารถในการเข้าถึงตัวเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ขององค์กร วิธีการควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์เพื่อรักษาความปลอดภัยของอุปกรณ์คอมพิวเตอร์ ได้แก่

- 1) สถานที่ติดตั้งอุปกรณ์คอมพิวเตอร์ควรอยู่ในห้องที่มีกุญแจปิด และจำกัดให้ใช้งานได้เฉพาะผู้ที่ได้รับอนุญาต
- 2) ห้องคอมพิวเตอร์ควรมีทางเข้าออกเพียง 1 หรือ 2 ทาง โดยกุญแจประตูต้องมีการปิดล็อกไว้และมีเจ้าหน้าที่รักษาความปลอดภัยคอยตรวจตราอย่างสม่ำเสมอ
- 3) ผู้ปฏิบัติงานต้องติดเครื่องหมายหรือบัตรประจำตัวผู้ผ่านเข้าออกในห้องคอมพิวเตอร์ หรือใช้อุปกรณ์ทางเทคนิคในการระบุตัวผู้ปฏิบัติงานก่อนผ่านเข้าทำงานในห้องคอมพิวเตอร์ เช่น การใช้กุญแจบัตรแถบแม่เหล็กบรรจุรหัสผ่านประจำตัวผู้ปฏิบัติงาน ซึ่งจะทำให้สามารถรวบรวมข้อมูลการเข้าทำงานในห้องคอมพิวเตอร์ของผู้ปฏิบัติงาน และมีการสอบทานการเข้าไปทำงานในห้องคอมพิวเตอร์เป็นระยะ เป็นต้น

การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์

- 4) กำหนดเป็นนโยบายการรักษาความปลอดภัย และชี้แจงให้บุคคลที่เข้ามาเยี่ยมชมทราบว่าต้องลงเวลาเข้าออก และติดเครื่องหมายหรือบัตรประจำตัวตลอดเวลาที่เข้ามาเยี่ยมชม
- 5) ติดตั้งระบบเตือนภัยกรณีมีผู้บุกรุก
- 6) จำกัดสิทธิการใช้โทรศัพท์ เครื่อง terminal และเครื่องคอมพิวเตอร์ส่วนบุคคลสำหรับงานส่วนตัว
- 7) ติดกุญแจล็อกเครื่องคอมพิวเตอร์และอุปกรณ์
- 8) การควบคุมสภาพแวดล้อมในการทำงานของเครื่องคอมพิวเตอร์ โดยมีการควบคุมอุณหภูมิความชื้น ฝุ่นละออง มีการติดตั้งระบบป้องกันเพลิงไหม้ เช่น เครื่องตรวจจับควัน (smoke detector) เป็นต้น

การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ

ในระบบแฟ้มข้อมูลเชิงระนาบ (flat file system) ผู้ใช้ข้อมูลต่างก็ดูแลรักษาแฟ้มข้อมูลที่เป็นของตนเอง ระบบดังกล่าวจึงมีสภาพแวดล้อมของการควบคุมที่เอื้ออำนวยต่อการควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ ในทางตรงกันข้าม ในระบบฐานข้อมูลซึ่งเน้นความสำคัญของบูรณภาพของข้อมูลและความจำเป็นในการใช้ข้อมูลร่วมกัน จะเพิ่มความเสี่ยงในการควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ ตัวอย่างเช่น ความเสี่ยงจากการทุจริต การขโมยข้อมูล การนำข้อมูลไปใช้ในทางที่ผิดการทำลายข้อมูล เป็นต้น ความเสี่ยงเหล่านี้ อาจเกิดขึ้นจากการที่มีผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล หรือการที่ผู้ใช้ที่ได้รับอนุญาตมีการเข้าถึงข้อมูลที่เกินกว่าขอบเขตที่ได้รับ การควบคุมการเข้าถึงข้อมูลในฐานข้อมูลมีหลายลักษณะ ดังต่อไปนี้

การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ

1) ทรทัศน์ของผู้ใช้ (user views) หรือเค้าร่างย่อย (sub - schema) เป็นส่วนย่อยของฐานข้อมูลทั้งหมดที่ระบุขอบเขตของข้อมูลของผู้ใช้ และกำหนดฐานข้อมูลที่ผู้ใช้เข้าถึง ในฐานข้อมูลแบบรวมศูนย์ (centralized database) ผู้บริหารฐานข้อมูล (database administrator หรือ DBA) มีหน้าที่รับผิดชอบโดยตรงต่อการออกแบบทรทัศน์ของผู้ใช้ โดยดำเนินการอย่างใกล้ชิดร่วมกับผู้ใช้และผู้ออกแบบระบบ ซึ่งการออกแบบทรทัศน์ของผู้ใช้ต้องสอดคล้องกับความต้องการของผู้ใช้ อย่างไรก็ตาม ถึงแม้ทรทัศน์ของผู้ใช้จะสามารถกำหนดขอบเขตข้อมูลที่ผู้ใช้เข้าถึง แต่ก็ไม่ได้ระบุหน้าที่งานที่ผู้ใช้สามารถทำได้ เช่น อ่าน ลบ แก้ไข เป็นต้น ในหลายกรณีผู้ใช้หลายคนอาจใช้ทรทัศน์ของผู้ใช้เดียวกัน แต่มีอำนาจในการเข้าถึงข้อมูลในระดับที่แตกต่างกัน โดยผู้ใช้ทุกคนที่เข้าถึงทรทัศน์ของผู้ใช้หนึ่ง อาจสามารถอ่านได้ แต่มีบางคนสามารถแก้ไขหรือลบข้อมูลนั้นได้ เป็นต้น การควบคุมการเข้าถึงข้อมูลจึงจำเป็นต้องมีการรักษาความปลอดภัยในลักษณะอื่น ๆ ประกอบด้วย

การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ

2) ตารางการอนุญาตให้เข้าถึงฐานข้อมูล (database authorization table) เป็นเทคนิคที่ใช้ในการกำหนดกฎเกณฑ์และการกระทำที่ผู้ใช้สามารถทำได้ ดังแสดงในตาราง 6.1 จากตารางดังกล่าว ผู้ใช้ทั้ง 5 คน สามารถเข้าถึงข้อมูลในระดับในทรยศณะของผู้ใช้เดียวกัน แต่ผู้ใช้แต่ละคนได้รับสิทธิในการเข้าถึงข้อมูลในระดับที่แตกต่างกัน

ตาราง 4.1 ตารางการอนุญาตให้เข้าถึงฐานข้อมูล

ทรยศณะของผู้ใช้ : ข้อมูลลูกค้า					
แผนก	บัญชีลูกหนี้			เรียกเก็บเงิน	
ผู้ใช้	สมศักดิ์	สมศรี	สมใจ	สมพล	สมปอง
รหัสผ่าน	DATA	JUNE	JAN	STAR	KEN
สิทธิการใช้งาน					
อ่าน	Y	Y	Y	Y	Y
เพิ่มข้อมูล	Y	Y	N	Y	N
แก้ไขข้อมูล	Y	N	N	Y	N
ลบข้อมูล	Y	N	N	N	N

การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ

3) การเข้ารหัสลับข้อมูล (data encryption) ระบบฐานข้อมูลอาจใช้การเข้ารหัสลับสำหรับป้องกันข้อมูลที่เป็นความลับ เช่น สูตรการผลิต อัตราเงินเดือนของพนักงาน แพ้มข้อมูล รหัสผ่าน และข้อมูลทางการเงินบางชนิด เป็นต้น การเข้ารหัสลับข้อมูล เป็นการใช้ขั้นตอนวิธีแปลงข้อมูลในรูปแบบที่คละกัน เพื่อให้ข้อมูลอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ นอกจากนี้การเข้ารหัสลับข้อมูลยังสามารถใช้ในการรักษาความปลอดภัยของข้อมูลที่มีการรับส่งผ่านระบบเครือข่ายได้อีกด้วย

การควบคุมการเข้าถึงระบบงาน

การเข้าถึงระบบงาน หมายถึง ความสามารถในการเข้าถึงโปรแกรมและข้อมูลในระบบงาน การควบคุมความสามารถดังกล่าวก็เพื่อรักษาความปลอดภัยของโปรแกรมและข้อมูลในระบบงาน ผู้ใช้ระบบจะได้รับอนุญาตให้เข้าถึงข้อมูลได้เพื่อทำการอ่าน ทำสำเนาเพิ่มและลบเฉพาะส่วนที่ตนเองมีสิทธิในการทำงานเท่านั้น และการป้องกันข้อมูลจากบุคคลภายนอกก็มีความสำคัญเช่นเดียวกัน การจำกัดการเข้าถึงระบบงานนั้น ตัวระบบงานเองจะต้องมีความสามารถแยกข้อแตกต่างระหว่างการใช้งานของผู้ได้รับอนุญาตกับผู้ไม่ได้รับอนุญาต ข้อมูลใดที่ผู้ใช้ระบบงานทราบหรือเป็นเจ้าของ สถานที่ที่ผู้ใช้ระบบงานเข้าใช้ระบบงาน หรือคุณลักษณะของแต่ละบุคคล วิธีการที่นิยมโดยทั่วไปสำหรับการควบคุมการเข้าถึงการใช้การตรวจสอบจากสิ่งที่ผู้ใช้ทราบ ตัวอย่างเช่น ให้เครื่องคอมพิวเตอร์แจ้งให้ผู้ใช้ป้อนรหัสประจำตัวบุคคล เป็นต้น

การควบคุมการเข้าถึงระบบงาน

การควบคุมการเข้าถึงระบบงาน ประกอบด้วย

1) การพิสูจน์ตัวตนจริง (authentication) สามารถทำได้หลายวิธี เช่น

(1) รหัสผ่าน (password) เป็นวิธีการที่นิยมใช้ในการระบุตัวตนของผู้ใช้ระบบงานเพื่อแสดงสิทธิเข้าใช้ระบบงาน การป้อนรหัสผ่านเพื่อเข้าสู่ระบบงาน ผู้ใช้อาจจะป้อนหมายเลขพนักงาน ชื่อ หรือชื่อตามบัญชีผู้ใช้ระบบ ซึ่งหลังจากมีการป้อนรหัสผ่านแล้ว ชุดของตัวอักษร ที่ไม่ซ้ำกันนั้นจะเป็นสิ่งที่ระบุว่าเป็นผู้ใช้ระบบ ซึ่งจะเป็นที่ทราบกันเฉพาะระหว่างผู้ใช้ระบบงานกับตัวระบบงานเองเท่านั้น ถ้าผู้ใช้ระบบงานป้อนชื่อผู้ใช้ระบบและรหัสผ่านที่ตรงกันกับที่มีอยู่ในระบบงานแล้ว จะถือว่าการแสดงสิทธิของผู้ใช้ระบบงาน ในทางปฏิบัติความสำคัญของรหัสผ่านได้ลดลงเนื่องจากสามารถคาดเดาได้ง่าย สูญหาย ถูกจดไว้ หรือถูกเปิดเผย ซึ่งเป็นการเพิ่มโอกาสให้ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงระบบงานได้

การควบคุมการเข้าถึงระบบงาน

(2) การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ (physical possession identification) เช่น บัตรประจำตัว (ID card) ที่มีการบันทึกข้อมูลบุคคลและสามารถอ่านได้ด้วยเครื่องคอมพิวเตอร์ เป็นต้น การระบุตัวตนด้วยสิ่งที่มีทางกายภาพอาจใช้อุปกรณ์รักษาความปลอดภัย เช่น กุญแจประตู เป็นต้น ระดับการรักษาความปลอดภัยอาจเพิ่มขึ้นโดยการใช้ทั้งบัตรประจำตัว และ รหัสผ่านร่วมกันก่อนที่จะผ่านเข้าสู่ระบบงาน อย่างไรก็ตาม ระบบนี้สามารถใช้ในการควบคุมได้เฉพาะบางส่วน เนื่องจากบัตรประจำตัวอาจจะหายหรือถูกขโมย รหัสผ่านอาจถูกขโมยหรือถูกเปิดเผย เป็นต้น

(3) การระบุตัวตนด้วยค่าทางชีวภาพ (biometric identification) อุปกรณ์อ่านค่าทางชีววิทยา เพื่อระบุตัวตนแยกลักษณะบุคคลตามคุณสมบัติของร่างกาย เช่น ลายมือ เสียง เรตินา โครงสร้างและลักษณะใบหน้า ลายเซ็นและลักษณะการใช้แป้นพิมพ์จากรูปแบบการใช้ตัวอักษรต่าง ๆ เมื่อผู้ใช้ระบบต้องการเข้าระบบงาน ข้อมูลของร่างกายผู้ใช้หรือคุณสมบัติทางชีวภาพระบุตัวตนต้องตรงกับข้อมูลที่จัดเก็บในระบบงาน อย่างไรก็ตาม ในการใช้งานจริงยังมีปัญหาอยู่บ้าง เช่น ในการใช้เสียงเป็นสิ่งระบุตัวตน กรณีที่ผู้ใช้เป็นหวัดเครื่องอ่านค่าจะจำเสียงเจ้าตัวไม่ได้และปฏิเสธไม่ให้เข้าระบบงาน หรือในการใช้เรตินาเป็นสิ่งระบุตัวตน กรณีผู้ใช้เป็นตาแดงเครื่องอ่านค่าจะอ่านไม่ได้และปฏิเสธไม่ให้เข้าระบบงาน เป็นต้น

การควบคุมการเข้าถึงระบบงาน

ตาราง 6.2 ตารางการควบคุมการเข้าถึงระบบงาน

ผู้ใช้งานระบบงาน		แฟ้มข้อมูล			โปรแกรม			
เลขประจำตัว	รหัสผ่าน	A	B	C	1	2	3	4
11111	Aaa1	0	0	1	0	0	0	0
11112	Bbb2	0	2	0	0	0	0	0
11113	Ccc3	1	1	1	0	0	0	0
11114	Ddd4	3	0	0	0	0	0	0
11115	Eee5	0	1	0	0	3	0	0
11116	Fff6	1	1	1	1	1	1	1

การควบคุมการเข้าถึงระบบงาน

รหัสประเภทของการเข้าถึง

0 = ไม่อนุญาตให้เข้าถึง

1 = อ่านและแสดงผลทางหน้าจอเท่านั้น

2 = อ่าน แสดงผลทางหน้าจอ และปรับปรุง

3 = อ่าน แสดงผลทางหน้าจอ ปรับปรุง สร้าง และลบ

3) การบันทึกกิจกรรมต่าง ๆ ในระบบเพื่อการตรวจสอบ (audit logging) เป็นการบันทึกกิจกรรมต่าง ๆ ที่ผู้ใช้ได้ดำเนินการในระบบเพื่อให้สามารถตรวจสอบได้ และช่วยให้เกิดหลักฐานการตรวจสอบสำหรับรายการต่าง ๆ ที่เกิดขึ้นในระบบสารสนเทศ

การควบคุมการจัดเก็บข้อมูล

สารสนเทศเป็นสิ่งที่สร้างทั้งความได้เปรียบคู่แข่งชั้นและมูลค่าแก่องค์กร เนื่องจากเป็นทรัพยากรที่ทรงคุณค่า จึงต้องมีการป้องกันผู้ไม่ได้รับอนุญาตมาเปิดเผยหรือทำลาย ซึ่งองค์กรจะต้องกำหนดประเภทของข้อมูลที่จะต้องบำรุงรักษาและระดับการป้องกันที่จำเป็นสำหรับข้อมูลแต่ละประเภท โดยขั้นตอนต่าง ๆ ในการป้องกันต้องจัดทำเป็นเอกสาร มีการรวบรวมข้อมูล เหตุการณ์ต่าง ๆ ในการรักษาความปลอดภัย มีการดูแลเอกสาร ข้อมูลประเภทรายการ และเพิ่มข้อมูลลับ และมีการเก็บข้อมูล การเข้าไปใช้ข้อมูลลับเหล่านั้น เพื่อให้สามารถตรวจสอบได้ พนักงานจะต้องทำสัญญาว่าจะไม่เปิดเผยข้อมูลที่เป็นความลับของ บริษัทการกำกับดูแลด้วยคลังเพิ่มข้อมูล (File library) ที่เหมาะสม เป็นส่วนที่สำคัญในการป้องกันข้อมูลสูญหาย หน่วยงานที่มีหน้าที่จัดเก็บเพิ่มข้อมูล (File storage) จะต้องเก็บรักษาเพิ่มข้อมูลให้พ้นจากเพลิงไหม้ ฝุ่นผง ความร้อน ความชื้น หรือสถานการณ์ที่สร้างความเสียหายให้ข้อมูลที่จัดเก็บไว้

การควบคุมการจัดเก็บข้อมูล

การติดป้ายชื่อแฟ้มข้อมูล (File label) จะช่วยป้องกันการนำไปใช้ผิดประเภทโดยไม่ได้ตั้งใจ ป้ายชื่อภายนอก (external label) เป็นป้ายกระดาษที่ติดไว้กับอุปกรณ์ที่เป็นหน่วยเก็บ (storage device) ซึ่งจะต้องมีชื่อ เนื้อหา และวันที่ ประมวลผล ส่วนป้ายชื่อภายใน (internal label) เป็นป้ายชื่อที่เครื่องคอมพิวเตอร์อ่านได้จากแบบฟอร์มในสื่อบันทึกข้อมูล ซึ่งจะมีอยู่ 3 ประเภท คือ

- 1) ป้ายหมวด (volume label) เป็นคำอธิบายเนื้อหาทั้งหมดของข้อมูลที่บันทึกในสื่อบันทึกข้อมูลเช่น ฮาร์ดดิสก์ แผ่นดิสเก็ตต์ หรือเทปแม่เหล็ก เป็นต้น
- 2) ป้ายหัวเรื่อง (header label) จะเป็นป้ายบอกจุดเริ่มต้นของแต่ละแฟ้มข้อมูลประกอบด้วยชื่อแฟ้มข้อมูล วันหมดอายุ และข้อมูลอื่น ๆ
- 3) ป้ายชื่อท้ายแฟ้ม (trailer data) เป็นป้ายบอกจุดสิ้นสุดของแฟ้มข้อมูล ซึ่งจะมีผลรวมคุมยอดของแฟ้ม (file control total) เพื่อเป็นข้อมูลสอบทานสำหรับเครื่องคอมพิวเตอร์ระหว่างการประมวลผล

การควบคุมการจัดเก็บข้อมูล

กลไกการป้องกันการเขียนทับ (write protection mechanism) จะช่วยป้องกันผู้ใช้ระบบงานเขียนข้อมูลทับหรือลบข้อมูลโดยไม่ตั้งใจ เช่น ในแผ่นดิสเก็ตต์จะมีสวิตช์ เปิดปิดให้เลือกป้องกันการเขียนทับได้แต่เป็นที่น่าเสียดายที่กลไกนี้ยกเลิกได้ง่ายมาก

ในระบบฐานข้อมูลจะใช้ผู้บริหารฐานข้อมูล พจนานุกรมข้อมูล (data dictionary) และการควบคุม การปรับปรุงข้อมูล เพื่อป้องกันข้อมูล โดยผู้บริหารฐานข้อมูลจะเป็นผู้สร้างและควบคุมให้การเข้าถึงและการปรับปรุงฐานข้อมูลเป็นไปตามวิธีการที่กำหนด พจนานุกรมข้อมูลจะสร้างความมั่นใจว่ารายการข้อมูลมีการกำหนดและใช้อย่างถูกต้อง ส่วนการควบคุมการปรับปรุงข้อมูล จะช่วยป้องกันรายการข้อมูลจากข้อผิดพลาดที่เกิดจากผู้ใช้หลายคนปรับปรุงข้อมูลรายการเดียวกันพร้อม ๆ กัน ซึ่งการควบคุมนี้จะช่วยล็อกข้อมูลรายการนั้นให้ปรับปรุงได้ที่ละคน โดยจะปลดล็อกภายหลังจากปรับปรุงเรียบร้อยแล้ว ผู้ใช้รายอื่นจึงจะสามารถเข้ามาทำการปรับปรุงต่อไป

การควบคุมการสื่อสารข้อมูล

การลดความเสี่ยงจากความล้มเหลวในการสื่อสารข้อมูล องค์กรจะต้องตรวจตราระบบเครือข่าย เพื่อหาจุดอ่อน รวมทั้งการบำรุงรักษาส่วนประกอบที่ใช้ในการสำรอง และออกแบบเครือข่ายให้มีขีดความสามารถเพียงพอที่จะรองรับความต้องการในช่วงเวลาที่มีการใช้งานเต็มที่ และจะต้องสร้างเส้นทางการสื่อสารภายในเครือข่ายไว้หลาย ๆ เส้นทาง เพื่อให้ระบบสามารถทำงานต่อเนื่องได้แม้ว่าจะมีบางเส้นทางที่ล้มเหลว และนอกจากการบำรุงรักษาอุปกรณ์ในการสื่อสารแล้ว ควรจะมีการปรับปรุงระบบ เช่น เปลี่ยนสายโทรศัพท์ไปใช้ชนิดที่เร็วกว่าหรือมีประสิทธิภาพมากกว่า เป็นต้น

การเติบโตของอินเทอร์เน็ตและพาณิชย์อิเล็กทรอนิกส์ ทำให้การเข้ารหัสลับข้อมูลเป็นการควบคุมที่สำคัญมาก วิทยาการเข้ารหัสลับเป็นวิทยาการเกี่ยวกับรหัสลับที่มีการนำมาใช้ในการสื่อสารข้อมูลและการพาณิชย์อิเล็กทรอนิกส์ เพื่อให้มั่นใจว่ามีการรักษาความปลอดภัยที่สำคัญ 3 ประการ คือ

การควบคุมการสื่อสารข้อมูล

1) ความลับ (confidentiality) หมายถึงการจำกัดสิทธิหรือการกำหนดให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการเข้าถึงข้อมูล

2) บุรณภาพของข้อมูล หมายถึงการป้องกันไม่ให้ผู้ที่ได้รับอนุญาตมายุ่งเกี่ยวกับข้อมูล

3) ความเป็นตัวตนที่แท้จริง หมายถึงความสามารถในการพิสูจน์ให้ทราบได้ว่าใครเป็นผู้ที่ส่งข้อความที่แท้จริง

ในการเข้ารหัสลับข้อมูล ผู้ส่งจะใช้กุญแจรหัสและขั้นตอนวิธี (algorithm) แปลงข้อมูลในรูปแบบที่คละกัันก่อน หลังจากนั้นจึงส่งข้อมูลที่เข้ารหัสแล้วไปตามเครือข่ายจนถึงผู้รับ ซึ่งมีกุญแจรหัสและขั้นตอนวิธีจะถอดรหัสเพื่อคืนกลับเป็นข้อมูลที่ใช้งานได้ตามเดิม ทั้งนี้ ผู้ที่จะอ่านข้อมูลที่เข้ารหัสได้ จะต้องมิกุญแจถอดรหัสที่เหมาะสม

การควบคุมการสื่อสารข้อมูล

ระบบการเข้ารหัสข้อมูลโดยทั่วไปมี 2 ระบบ คือ กุญแจรหัสลับ (private key) และกุญแจรหัสสาธารณะ (public key) ดังต่อไปนี้

1) ระบบกุญแจรหัสลับ บางครั้งเรียกว่ากุญแจรหัสสมมาตร (symmetric key) ทั้งผู้ส่งและผู้รับจะใช้กุญแจรหัสเดียวกัน ทั้งในการเข้าและถอดรหัสลับ ข้อด้อยของระบบนี้ ได้แก่ ในกรณีที่กุญแจ รหัสลับไม่ปลอดภัยเต็มที่ การป้องกันจะไม่เกิดผล จึงเหมาะสำหรับการใช้งานภายในองค์กรหรือเฉพาะระหว่างกลุ่มองค์กรที่เป็นระบบปิดเท่านั้น แต่ไม่เหมาะสำหรับการพาณิชย์ อิเล็กทรอนิกส์

การควบคุมการสื่อสารข้อมูล

2) ระบบกุญแจรหัสสาธารณะ จะแยกกุญแจรหัสเป็น 2 กุญแจ คือ กุญแจรหัสสาธารณะ ที่ทุกคนสามารถใช้ได้ กับ กุญแจรหัสลับที่จะทราบเฉพาะผู้ใช้เท่านั้น ในการเข้ารหัสและถอดรหัสจำเป็นต้องใช้กุญแจรหัสทั้งคู่ โดยข้อมูลที่ส่งออกไปจะถูกเข้ารหัสด้วยกุญแจรหัสสาธารณะของผู้รับและกุญแจรหัสลับของผู้ส่ง เมื่อข้อมูลที่เข้ารหัสส่งไปถึงผู้รับ ผู้รับจะถอดรหัสด้วยกุญแจรหัสสาธารณะของผู้ส่งและกุญแจรหัสลับของผู้รับ ซึ่งในอุตสาหกรรมคอมพิวเตอร์มีการป้องกันการปลอมแปลงกุญแจรหัสสาธารณะด้วยเอกสารอิเล็กทรอนิกส์ที่เรียกว่าใบรับรองดิจิทัล (digital certificate) ที่ออกให้โดยองค์การอิสระที่มีอำนาจออกใบรับรอง (certificate authority) ซึ่งใบรับรองนี้จะมีข้อมูลแยกเป็น 3 ส่วน ได้แก่

- หัวเรื่อง (header) ประกอบด้วยชื่อบริษัท เลขประจำตัว วันหมดอายุ ฯลฯ
- กุญแจรหัสสาธารณะของบริษัท
- ลายเซ็นของผู้มีอำนาจออกใบรับรองซึ่งจะส่งไปให้ผู้รับพร้อมกับข้อมูลโดยผู้รับจะใช้ในการตรวจสอบความถูกต้อง หลังจากนั้น จึงจะสามารถถอดรหัสออกได้

การควบคุมการสื่อสารข้อมูล

กระบวนการในการตรวจสอบเส้นทาง (Routing verification procedure) เป็นวิธีการทำงานที่จะช่วยสร้างความมั่นใจว่าข้อมูลส่งไปถูกที่ โดยในการส่งข้อมูลจะมีการแนบข้อมูลที่อยู่ของปลายทางไว้ด้วยการตรวจสอบความถูกต้องของข้อมูลที่รับส่ง โดยทั่วไปจะใช้ภาวะคู่หรือคี่ (parity) คอมพิวเตอร์ใช้การผสมผสานกลุ่มของบิตจำนวนหนึ่งแทนตัวอักขระหนึ่งตัว เช่น เลข 5 อาจประกอบด้วยกลุ่มของบิต (bit) คือ 0101 เป็นต้น เมื่อข้อมูลถูกส่งไปอาจจะสูญหายหรือการรับข้อมูลผิดพลาด เพื่อให้สามารถตรวจพบข้อผิดพลาดนี้ได้ จึงมีการเพิ่มจำนวนบิตต่อ 1 อักขระสำหรับการส่ง ซึ่ง 1 บิตที่เพิ่มขึ้นนี้เรียกว่าบิตภาวะคู่ หรือคี่ (parity bit) ซึ่งค่าของบิตที่เพิ่มเข้าไปคำนวณมาจากค่าของบิตที่มีอยู่เดิม เมื่อมีการรับข้อมูลจะมีการทดสอบการคำนวณในรูปแบบเดียวกันเพื่อหาค่าบิตที่เพิ่มมา แล้วนำมาเปรียบเทียบกับข้อมูลที่ส่งมาจะทำให้พบข้อผิดพลาดที่เกิดขึ้นจากการรับส่งข้อมูลได้ส่วนหนึ่ง

การกำหนดมาตรฐานเอกสารระบบสารสนเทศ

การควบคุมทั่วไปที่สำคัญประการหนึ่ง คือ วิธีการและมาตรฐานในการจัดทำเอกสารระบบสารสนเทศเพื่อให้มั่นใจว่ามีความชัดเจนและรัดกุม การจัดทำเอกสารที่มีคุณภาพทำให้การติดต่อสื่อสารและการติดตามความก้าวหน้าในการพัฒนาระบบงานสะดวกขึ้น และใช้เป็นเอกสารอ้างอิงและเป็น เครื่องมือฝึกอบรมพนักงาน รวมทั้งช่วยให้การบำรุงรักษาและแก้ไขปรับปรุงโปรแกรมประยุกต์สามารถทำได้ง่ายขึ้น การจัดทำเอกสารระบบงานดังกล่าวแยกเป็น 3 ประเภท ดังนี้

1) การจัดทำเอกสารทางการบริหาร (administrative documentation) อธิบายมาตรฐานและวิธีการปฏิบัติงานต่าง ๆ ในการประมวลผลข้อมูล รวมทั้งเหตุผลและการให้อำนาจต่าง ๆ ของระบบงานใหม่และระบบงานที่มีการเปลี่ยนแปลง มาตรฐานในการวิเคราะห์ ออกแบบ และเขียนโปรแกรมระบบงานและวิธีการปฏิบัติงานเกี่ยวกับแฟ้มข้อมูล และหน่วยเก็บ

การกำหนดมาตรฐานเอกสารระบบสารสนเทศ

2) การจัดทำเอกสารระบบงาน (system documentation) อธิบายระบบงานแต่ละระบบ รวมทั้งปัจจัยต่าง ๆ ผังการทำงาน รายการโปรแกรม ซึ่งจะแสดงการนำเข้าสู่ขั้นตอนการประมวลผลผลลัพธ์จากระบบ และวิธีการควบคุมข้อผิดพลาด

3) การจัดทำเอกสารประกอบการปฏิบัติการ (operating documentation) อธิบายสิ่งที่จำเป็นในการเดินเครื่องระบบงาน รวมถึงการกำหนดค่าให้อุปกรณ์ต่าง ๆ โปรแกรมและแฟ้มข้อมูลวิธีการติดตั้งและวิธีการทำงาน สถานการณ์ที่อาจขัดขวางการทำงานของโปรแกรมและวิธีการแก้ไข

การลดความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์

ฮาร์ดแวร์ (hardware) หรือซอฟต์แวร์ (software) ที่ทำงานล้มเหลวอาจสร้างความสูญเสียทางการเงินที่สำคัญได้ วิธีการต่าง ๆ ที่จะลดความเสียหาย ได้แก่

1) การบำรุงรักษาเชิงป้องกัน (preventive maintenance) จะเป็นการตรวจสอบส่วนประกอบของระบบตามระยะเวลา การบำรุงรักษา และเปลี่ยนเมื่อมีสภาพไม่ดี

2) อุปกรณ์ไฟฟ้าสำรอง (uninterrupted power system หรือ UPS) เป็นอุปกรณ์ไฟฟ้าที่จะช่วยให้การจ่ายกระแสไฟฟ้าให้เครื่องคอมพิวเตอร์เป็นไปอย่างราบรื่น ซึ่งจะป้องกันไฟกระชาก ไฟตก หรือไฟเกินที่อาจจะทำให้ข้อมูลสูญหาย และจ่ายกระแสไฟฟ้าสำรองแทนได้ในกรณีไฟดับ

3) ระบบที่ทนต่อความผิดพลาด (fault tolerant) เป็นความสามารถที่ทำให้ระบบทำงานต่อไปได้ แม้ว่าจะมีส่วนประกอบบางส่วนเสียหายหรือไม่ทำงาน โดยอาจมีส่วนประกอบที่ติดตั้งไว้มากเกินความจำเป็นในเวลาปกติแต่จะใช้ทดแทนได้เมื่อส่วนอื่นเสียหาย

การวางแผนแก้ไขความเสียหายจากเหตุฉุกเฉิน

การควบคุมทั่วไปในระบบสารสนเทศ หมายถึงการควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุม ภายใน นโยบายและวิธีการในการควบคุมระบบสารสนเทศ การจัดแบ่งส่วนงานและหน้าที่รวมทั้งวิธีการปฏิบัติงานของผู้ที่เกี่ยวข้องกับระบบสารสนเทศ การควบคุมความปลอดภัยระบบ การควบคุมการพัฒนาและปรับปรุงระบบ และการป้องกันความเสียหายหรือลดความเสียหายของระบบ การควบคุมทั่วไปเป็นการควบคุมภายในสำหรับระดับองค์กร หรือการควบคุมที่ควรมีในทุก ๆ ส่วนของระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อให้เกิดความมั่นใจว่าระบบคอมพิวเตอร์โดยรวมขององค์กรมีความเสถียร มีการจัดการที่ดีและเป็นส่วนหนึ่งที่จะก่อให้เกิดบูรณภาพ

การวางแผนแก้ไขความเสียหายจากเหตุฉุกเฉิน

การควบคุมทั่วไปในระบบสารสนเทศ ประกอบด้วยกิจกรรมต่าง ๆ ได้แก่ การวางแผนรักษาความปลอดภัย การแบ่งแยกหน้าที่งานในระบบสารสนเทศ การควบคุมการพัฒนาระบบสารสนเทศ การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ การควบคุมการเข้าถึงระบบงาน การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ การควบคุมการจัดเก็บข้อมูล การควบคุมการสื่อสารข้อมูล การกำหนดมาตรฐานของเอกสารระบบสารสนเทศ การลดความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และการวางแผนแก้ไขความเสียหายจากเหตุฉุกเฉิน

การควบคุมทั่วไปที่ไม่เหมาะสมก่อให้เกิดความเสี่ยงในด้านต่าง ๆ เช่น การควบคุมภายในของระบบสารสนเทศ อาจเกิดความเสียหาย เกิดข้อผิดพลาด หรือถูกแก้ไขเปลี่ยนแปลงให้ผิดไปจากข้อเท็จจริงข้อมูลหรือโปรแกรมของระบบสารสนเทศอาจถูกนำไปใช้โดยไม่ได้รับอนุญาต และระบบงานอาจหยุดชะงักหรือไม่สามารถดำเนินต่อไปได้ เป็นต้น

การควบคุมระบบงาน

การควบคุมอาจแบ่งออกได้เป็น 4 ประเภทหลัก ๆ ได้แก่

- 1) การควบคุมการเข้าถึงระบบข้อมูล
- 2) การควบคุมเกี่ยวกับการนำข้อมูลเข้า
- 3) การควบคุมเกี่ยวกับการประมวลผล
- 4) การควบคุมเกี่ยวกับการเสนอข้อมูลออก

การควบคุมการเข้าระบบหรือข้อมูล

กิจการมักใช้รหัสผ่านในการควบคุมการเข้าถึงระบบหรือข้อมูล รหัสที่ให้แกผู้ใช้ทุกคนหรือกลุ่มคนกลุ่มเดียวกันใช้รหัสเดียวกันเป็นการละเลยการควบคุมที่ดี แต่การให้รหัสเฉพาะบุคคลเพื่อทำงานแต่ละอย่างอาจทำให้เกิดความสับสนแก่ผู้ใช้นั้น เนื่องจากบุคคลนั้นจะต้องจดจำรหัสหลายรหัสเพื่องานต่าง ๆ คำถามปลีกย่อยต่าง ๆ ที่ติดตามมา ได้แก่

- รหัสผ่านออกให้แกผู้ใช้แต่ละรายหรือตามบทบาท
- รหัสผ่านมีการกำหนดจำนวนน้อยที่สุด มากที่สุดหรือไม่ ใช้สัญลักษณ์อะไรบนแป้นพิมพ์ได้บ้าง
- มีทะเบียนบันทึก (log) ว่าใครใช้โปรแกรมหรือแฟ้มข้อมูลใด เมื่อไร หรือไม่

การควบคุมการเข้าระบบหรือข้อมูล

- โปรแกรมถูกแปลง (compile) หรือไม่ หมายถึงถูกเขียนขึ้นโดยใช้ภาษาทางคอมพิวเตอร์หรือไม่ โปรแกรมที่ถูกเขียนขึ้นโดยใช้ภาษาทางคอมพิวเตอร์เท่านั้นที่จะสามารถป้องกันการเปลี่ยนแปลงตัวโปรแกรมโดยไม่ได้รับอนุญาตได้

“Program control deters users from making unauthorized changes to the software. This is possible only if the software is written in computer-based language.” (ที่มา : AIS โดย Romney, 2003)

- แฟ้มข้อมูลถูกเก็บอยู่บนโครงสร้างแอสกี (ASCII) หรือไม่ถ้าแฟ้มข้อมูลถูกเก็บบนแอสกีก็จะสามารถแยกดูข้อมูลเหล่านั้นได้อย่างสะดวก
- ข้อมูลที่อยู่ในแฟ้มข้อมูลถูกตั้งรหัสลับไว้หรือไม่ การตั้งรหัสลับสำหรับข้อมูลช่วยเพิ่มความปลอดภัยให้แก่ข้อมูลเหล่านั้น แต่ในขณะเดียวกันระบบจะต้องใช้เนื้อที่ในการจัดเก็บข้อมูลเพิ่มขึ้น การประมวลผลที่ตามมาก็จะใช้เวลามากขึ้นด้วย

การควบคุมการเข้าระบบหรือข้อมูล

- โปรแกรมถูกแปลง (compile) หรือไม่ หมายถึงถูกเขียนขึ้นโดยใช้ภาษาทางคอมพิวเตอร์หรือไม่ โปรแกรมที่ถูกเขียนขึ้นโดยใช้ภาษาทางคอมพิวเตอร์เท่านั้นที่จะสามารถป้องกันการเปลี่ยนแปลงตัวโปรแกรมโดยไม่ได้รับอนุญาตได้

“Program control deters users from making unauthorized changes to the software. This is possible only if the software is written in computer-based language.” (ที่มา : AIS โดย Romney, 2003)

- เพิ่มข้อมูลถูกเก็บอยู่บนโครงสร้างแอสกี (ASCII) หรือไม่ ถ้าเพิ่มข้อมูลถูกเก็บบนแอสกีก็จะสามารถแยกดูข้อมูลเหล่านั้นได้อย่างสะดวก

การควบคุมเกี่ยวกับการนำข้อมูลเข้า

การควบคุมเกี่ยวกับการนำข้อมูลเข้าเป็นสิ่งสำคัญสำหรับระบบบัญชี โดยคอมพิวเตอร์เป็นตัวควบคุมที่ทำให้เราแน่ใจได้ว่าข้อมูลที่ป้อนเข้าเครื่องเป็นไปอย่างถูกต้องและสมบูรณ์ ข้อมูลเข้าเป็นต้นกำเนิดของการประมวลผล ผลลัพธ์ที่ได้จะเที่ยงตรง แม่นยำเที่ยงตรงมากแค่ไหน ขึ้นอยู่กับความถูกต้องของข้อมูลเข้า สมมติว่ารายการค้า คือ เดบิตบัญชีเลขที่ 10100 ซึ่งเป็นบัญชีเงินสด และเครดิตบัญชีเลขที่ 61934 ซึ่งเป็นบัญชีทุน ด้วยจำนวนเงิน 500,000 บาท ข้อมูลเข้าคือ เลขที่บัญชีเครดิต 61934 เลขที่บัญชีเดบิต 10100 และจำนวนเงิน 500,000 บาท จะเห็นได้ว่า ถ้ามีรายการค้าสัก 100 รายการต้องวาดบัญชีโอกาสที่จะคีย์ข้อมูลผิดพลาดมีมากเหลือเกิน ตัวควบคุมการนำข้อมูลเข้าจึงเป็นสิ่งจำเป็น ซึ่งมีให้เลือกใช้หลายตัวตามความเหมาะสม และสามารถจำแนกได้เป็น 2 ประเภทใหญ่ ๆ ได้แก่

การควบคุมเกี่ยวกับการนำข้อมูลเข้า

1) การตรวจทานข้อมูลเข้า เช่น

- การใช้เครื่องทวนสอบ (key verification) คือการป้อนข้อมูลลงสื่อ (media) ไม่ว่าจะ เป็นเทปหรือดิสก์ 2 ครั้ง ครั้งที่สองเป็นการป้อนเพื่อสอบทานว่าตรงกับการป้อนครั้งแรกหรือไม่
- เลขโดดตรวจสอบ (check digit) เป็นการใส่ตัวเลขข้างท้ายข้อมูลที่เป็นตัวเลขล้วน ๆ เช่น 61934 เข้าไปอีกตัวหนึ่ง เพื่อเป็นการตรวจสอบความถูกต้องของข้อมูลข้างหน้า เช่น เติมเลข 5 เข้าไป 61934 ฉะนั้นรหัสบัญชีทุนคือ 619345 เลข 5 ได้มาจาก 61934 หารด้วย 7 (หารด้วยตัวเลขใดก็ได้) ได้ 8847 เหลือเศษ 5 วิธีการกำหนดตัวเลขสุดท้ายเพื่อตรวจสอบความถูกต้องของตัวเลขข้างหน้ามีอยู่หลายวิธี วิธีข้างต้นเป็นตัวอย่างของวิธีหนึ่งเท่านั้น

การควบคุมเกี่ยวกับการนำข้อมูลเข้า

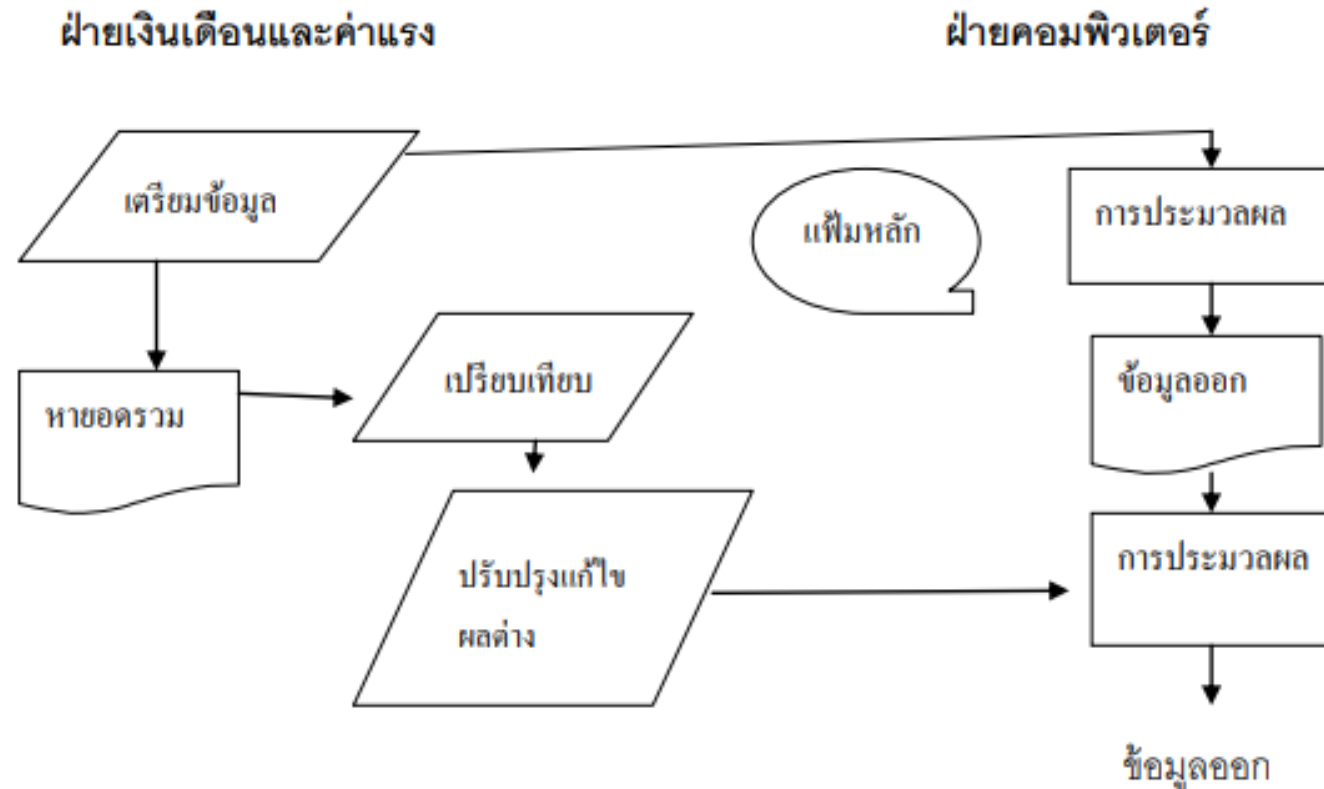
- การตรวจสอบความสมเหตุสมผล (validity check) เป็นการตรวจสอบว่าข้อมูลเข้ามีลักษณะตรงตามที่กำหนดไว้หรือไม่ เช่น รหัสบัญชีถูกกำหนดให้เป็นตัวเลข 6 ตำแหน่ง แต่ปรากฏว่าป้อนข้อมูลเข้าผิดเป็น b1934 ซึ่งเป็นตัวอักษรเลข (alphanumeric) ข้อมูลที่ป้อนเข้านั้นจึงใช้ไม่ได้ เครื่องจะไม่ยอมรับข้อมูลนั้น
- การตรวจทานข้อมูลเข้าตัวอื่น ๆ เช่น ข้อจำกัด (limit) หรือตรวจสอบความมีเหตุผล (reasonableness check) การทดสอบเชิงตรรกะ (logic test) การตรวจสอบเขตข้อมูล (field check) การตรวจสอบจำนวนบวกหรือจำนวนลบ (sign check)
- การนำเอกสารต้นฉบับอัตโนมัติ (automated source document) มาใช้ เช่น UPC/POS terminal, MICR, OSR

การควบคุมเกี่ยวกับการนำข้อมูลเข้า

2) การตรวจสอบจากยอดรวม

- การนับจำนวนระเบียน (record count) คือการตรวจนับข้อมูลเข้าว่ามีทั้งสิ้นกี่รายการ เช่น รายการค้า ในระหว่างงวดบัญชีนี้มีทั้งสิ้น 100 รายการเครื่องจะรับรายการค้าทุกครั้งที่ถูกป้อนเข้าจนครบ 100 รายการ ถ้าขาดไปเครื่องจะเตือน ถ้าเกินเครื่องจะไม่ยอมรับ
- การรวมยอดแบบกลุ่ม (batch total) คือการรวมยอดข้อมูลเข้าเขตข้อมูล (field) ใดเขตข้อมูล หนึ่งที่เป็นจำนวนเงินว่าจำนวนเงินของทุก ๆ ระเบียน (record) รวมกันได้เท่าไร เครื่องจะบอกจำนวนเงินนั้น ทุกๆ ครั้งที่คีย์ข้อมูลเข้า ผลลัพธ์ที่เก็บไว้จะต้องเท่ากับผลลัพธ์ที่ได้จากตัวเครื่อง
- การรวมยอดแบบแฮช (hash total) เป็นวิธีการควบคุมเกี่ยวกับการรวมยอดแบบกลุ่มต่างกันตรง การรวมยอดแบบแฮชไม่ใช่ช่องจำนวนเงินแต่ใช้เขตข้อมูลที่ผลลัพธ์ของการบวกเลขนั้นไม่มีความหมาย ใด ๆ เช่น เลขรหัสบัญชี เป็นต้น

การควบคุมเกี่ยวกับการนำข้อมูลเข้า



ภาพ 6.2 การใช้ Control total

การควบคุมเกี่ยวกับการประมวลผล

เมื่อข้อมูลถูกนำเข้าสู่เครื่องเรียบร้อยแล้ว ก็จะต้องมีตัวควบคุมที่จะทำให้การประมวลผลเป็นไปอย่างถูกต้อง เช่นเดียวกัน

- การตรวจสอบภาวะคู่หรือคี่ (parity check) จัดเป็นการควบคุมฮาร์ดแวร์ (hard-ware control) ซึ่งผู้ผลิตเครื่องคอมพิวเตอร์มักใส่มาในตัวเครื่อง การตรวจสอบภาวะคู่หรือคี่มี 2 อย่าง คือ ภาวะคี่ (odd) กับภาวะคู่ (even) หลักการคือการเติมตัวเลข 0 หรือ 1 ข้างท้ายไบต์ ถ้าเป็น ไบต์การตรวจสอบภาวะคี่ (odd parity check) ผลรวมของตัวเลขในหนึ่งไบต์จะมีเลข 0 เตรียมข้อมูล เข้าเพิ่มหลัก การประมวลผลข้อมูลออก การประมวลผล เปรียบเทียบ ปรับปรุงแก้ไขผลต่างหายโดยรวม เป็นตัวสุดท้าย ถ้าเป็นการตรวจสอบภาวะคู่ (even parity check) จะมีเลข 1 เป็นตัวสุดท้ายของไบต์

การควบคุมเกี่ยวกับการประมวลผล

- Duplicate circuitry คือการกำหนดให้ CPU ทำการประมวลผลที่เป็นการคำนวณ 2 ครั้ง เพื่อตรวจสอบความถูกต้องของกันและกัน
- การตรวจสอบการสะท้อน (echo check) คือการกำหนดให้เครื่องสะท้อนข้อความกลับมาให้ผู้ใช้รู้ว่าข้อมูลที่ป้อนเข้าไปนั้นถูกต้องหรือไม่ เช่น ผู้ใช้อาจคีย์เลขรหัสบัญชี 61934 เข้าเครื่องเครื่องจะสะท้อนข้อความกลับให้ผู้ใช้ทราบว่าบัญชี 61934 คือบัญชีทุน เป็นต้น
- หน่วยความจำอ่านอย่างเดียว (read-only memory-ROM) คือการกำหนดให้ส่วนหนึ่งของ CPU เป็นที่เก็บคำสั่งโดยเฉพาะ ข้อมูลในส่วนนี้อาจถูกอ่านได้แต่ไม่สามารถถูกลบออก
- การเสื่อมที่ละน้อย (graceful degradation) เมื่อส่วนใดส่วนหนึ่งของเครื่องคอมพิวเตอร์เกิดทำงานไม่ได้ ส่วนอื่นจะทำงานแทนด้วยประสิทธิภาพที่ด้อยกว่า
- อุปกรณ์ไฟฟ้าสำรอง (UPS) เมื่อเกิดไฟฟ้าดับ UPS จะเข้าทำงานแทนได้ช่วงเวลาหนึ่ง

การควบคุมเกี่ยวกับการประมวลผล

- การทดสอบสว่นย่อยของโปรแกรม (test deck) คือการกำหนดข้อมูลป้อนขึ้นมาชุดหนึ่งโดยรวมเหตุการณ์ปกติ ผิดปกติต่าง ๆ เพื่อทดสอบการทำงานของชุดคำสั่งที่เขียนขึ้นมา โดยมุ่งไปที่ตัวควบคุมแต่ละตัวที่ใส่ไว้เพื่อจับข้อผิดพลาดว่าทำงานตามความมุ่งหมายหรือไม่
- การทดสอบระบบ (system testing) คือการทดสอบการเชื่อมโยงหรือการประมวลผลอย่างต่อเนื่องของชุดคำสั่งหลายๆ ชุดในระบบเดียวกันที่ทำงานตามที่ได้กำหนดไว้หรือไม่
- ข้อความระบุความผิดพลาด (error messages หรือ error logs) ในการประมวลแต่ละครั้งข้อมูลออกหรือผลลัพธ์ตัวหนึ่งมักได้แก่ error log ซึ่งเป็นรายการข้อผิดพลาดที่ปรากฏในการดำเนินงานนั้นเมื่อเครื่องคอมพิวเตอร์สามารถจับข้อผิดพลาดได้ การที่จะให้เครื่องหยุดการประมวลผลลงทันทีอาจทำให้เสียค่าใช้จ่ายมาก ฉะนั้นผู้ใช้อาจกำหนดให้เครื่องทำการประมวลผลต่อไป แต่เสนอราคาที่ต้องจ่ายก็จะได้รับการประมวลผลไปตามปกติ
- การควบคุมเกี่ยวกับการประมวลผลตัวอื่น ๆ เช่น การปกป้องหน่วยความจำ (memory protection) และการตรวจสอบการทวนสอบวงวนปิด (closed-loop verification check) เป็นต้น

การควบคุมเกี่ยวกับการประมวลผล

- Duplicate circuitry คือการกำหนดให้ CPU ทำการประมวลผลที่เป็นการคำนวณ 2 ครั้ง เพื่อตรวจสอบความถูกต้องของกันและกัน
- การตรวจสอบการสะท้อน (echo check) คือการกำหนดให้เครื่องสะท้อนข้อความกลับมาให้ผู้ใช้รู้ว่าข้อมูลที่ป้อนเข้าป้อนนั้นถูกต้องหรือไม่ เช่น ผู้ใช้อาจคีย์เลขรหัสบัญชี 61934 เข้าเครื่องเครื่องจะสะท้อนข้อความกลับมาให้ผู้ใช้ทราบว่าบัญชี 61934 คือบัญชีทุน เป็นต้น
- หน่วยความจำอ่านอย่างเดียว (read-only memory-ROM) คือการกำหนดให้ส่วนหนึ่งของ CPU เป็นที่เก็บคำสั่งโดยเฉพาะ ข้อมูลในส่วนนี้อาจถูกอ่านได้แต่ไม่สามารถถูกลบออก
- การเสื่อมที่ละน้อย (graceful degradation) เมื่อส่วนใดส่วนหนึ่งของเครื่องคอมพิวเตอร์เกิดทำงานไม่ได้ ส่วนอื่นจะทำงานแทนด้วยประสิทธิภาพที่ด้อยกว่า
- อุปกรณ์ไฟฟ้าสำรอง (UPS) เมื่อเกิดไฟฟ้าดับ UPS จะเข้าทำงานแทนได้ช่วงเวลาหนึ่ง

การควบคุมเกี่ยวกับการประมวลผล

- การทดสอบส่วนย่อยของโปรแกรม (test deck) คือการกำหนดข้อมูลป้อนขึ้นมาชุดหนึ่งโดยรวมเหตุการณ์ปกติและผิดปกติต่าง ๆ เพื่อทดสอบการทำงานของชุดคำสั่งที่เขียนขึ้นมา โดยมุ่งไปที่ตัวควบคุมแต่ละตัวที่ใส่ไว้เพื่อจับข้อผิดพลาดว่าทำงานตามความมุ่งหมายหรือไม่
- การทดสอบระบบ (system testing) คือการทดสอบการเชื่อมโยงหรือการประมวลผลอย่าง ต่อเนื่องของชุดคำสั่งหลายๆ ชุดในระบบเดียวกันที่ทำงานตามที่ได้กำหนดไว้หรือไม่
- ข้อความระบุความผิดพลาด (error messages หรือ error logs) ในการประมวลแต่ละครั้งข้อมูลออกหรือผลลัพธ์ตัวหนึ่งมักได้แก่ error log ซึ่งเป็นรายการข้อผิดพลาดที่ปรากฏในการดำเนินงานนั้นเมื่อเครื่องคอมพิวเตอร์สามารถจับข้อผิดพลาดได้ การที่จะให้เครื่องหยุดการประมวลผลลงทันทีอาจทำให้เสียค่าใช้จ่ายมาก ฉะนั้นผู้ใช้อาจจะกำหนดให้ เครื่องทำการประมวลผลต่อไป แต่เสนอราคาที่ถูกต้องก็จะได้รับการประมวลผลไปตามปกติ

การควบคุมเกี่ยวกับการประมวลผล

การควบคุมเกี่ยวกับการประมวลผลตัวอื่น ๆ เช่น การปกป้องหน่วยความจำ (memory protection) และการตรวจสอบการทวนสอบวงวนปิด (closed-loop verification check) เป็นต้น การควบคุมความถูกต้องในการป้อนข้อมูลลงสู่เอกสารเบื้องต้นและการควบคุมความครบถ้วนของข้อมูลเข้า

ในการควบคุมความถูกต้องครบถ้วนของข้อมูลเข้า กิจการอาจใช้วิธีการต่าง ๆ ได้หลายวิธี ได้แก่

1) การใช้เอกสารเบื้องต้นที่จัดพิมพ์ไว้ล่วงหน้า เรียงเลขที่การออกแบบเอกสารเบื้องต้นที่มีรูปแบบที่ชัดเจน เข้าใจง่าย เอกสารเหล่านี้อาจถูกจัดทำขึ้นหลายใบจากหน่วยงานหนึ่งไปยังหน่วยงานต่าง ๆ

2) การใช้หน้าจอคอมพิวเตอร์ในการป้อนข้อมูลเข้า เอกสารเบื้องต้นอาจไม่ได้อยู่ในรูปของกระดาษเสมอไป แต่เป็นเอกสารเบื้องต้นที่ปรากฏอยู่บนหน้าจอคอมพิวเตอร์นี้ โครงสร้างของเอกสารเบื้องต้นจะถูกเก็บในรูปแบบที่ออกแบบไว้ล่วงหน้า พนักงานคีย์ข้อมูลเข้าโดยใช้แป้นพิมพ์เติมข้อมูลลงสู่เอกสารเบื้องต้น ลงสู่สื่ออิเล็กทรอนิกส์โดยที่พนักงานฝ่ายประมวลผลไม่ต้องคีย์ข้อมูลเข้าซ้ำอีกครั้งหนึ่ง

การควบคุมเกี่ยวกับการประมวลผล

3) ในกรณีที่การบันทึกรายการค้ากระทำบนเอกสารเบื้องต้นที่อยู่ในรูปของกระดาษการส่งเอกสารเบื้องต้นหลายใบจากหน่วยงานหนึ่ง (หน่วยงานที่เกิดรายการค้านั้น ๆ) ไปยังหน่วยงานบัญชีหรือหน่วยงานประมวลผล เอกสารอาจสูญหายหรือถูกทำลายได้ จึงควรมีการควบคุมการเคลื่อนย้ายเอกสารเหล่านี้ เทคนิคที่เป็นที่นิยมใช้ ได้แก่การรวมยอดสดมภ์จำนวนเงินหรือวิธีการรวมยอดแบบกลุ่ม (batch total) และการรวมยอดสดมภ์ตัวเลขหรือวิธีการรวม ยอดแบบแฮช (hash total)

Batch total: สมมติว่าเมื่อเกิดการขายขึ้นที่หน่วยขายหลายจุด พนักงานขายบันทึกการขายในใบเสร็จรับเงิน ชุดหนึ่งมอบให้ลูกค้า อีกชุดหนึ่งรวบรวมไว้จนถึงสิ้นวันจึงจัดส่งไปที่สำนักงานใหญ่ พนักงานอาจรวบรวมใบเสร็จรับเงินใส่ซองให้เจ้าหน้าที่นำส่ง การที่ใบเสร็จรับเงินถูกพิมพ์ไว้ล่วงหน้า เรียงเลขที่ ก็เป็นการควบคุมความครบถ้วนขั้นหนึ่งแล้ว แต่ถ้าพนักงานรวมยอดจำนวนเงินทั้งหมดสมมติว่าเท่ากับ 250 บาท ส่งยอดจำนวนเงินรวมนี้ไปที่ผู้อำนวยการฝ่ายบัญชี เมื่อใบเสร็จรับเงินถูกส่งถึงฝ่ายบัญชีหรือประมวลผล ข้อมูลในใบเสร็จรับเงินจะถูกป้อนลงสื่อคอมพิวเตอร์ ในการนี้ กิจการอาจตั้งโปรแกรมให้ระบบคิดคำนวณหาตัวเลขจำนวนเงินรวมด้วย ยอดนี้จะต้องได้เท่ากับ 250 บาท

การควบคุมเกี่ยวกับการประมวลผล

Hash total: คือวิธีการลักษณะเดียวกับ batch total หากแต่ตัวเลขจำนวนรวมไม่ได้ใช้ช่องสตมภ์ที่เป็นจำนวนเงิน แต่ใช้สตมภ์อื่นที่เป็นตัวเลข เช่น เลขที่ใบเสร็จรับเงิน เป็นต้น

4) การกำหนดให้ชุดคำสั่งตรวจสอบความถูกต้องของข้อมูลเข้าก่อนที่จะนำข้อมูลลงสู่ระบบ(programmed edit check) เช่น ทุกครั้งที่มีการสั่งซื้อสินค้าจากลูกค้ากิจการอาจกำหนดให้ระบบงานเข้าไปค้นหาจากแฟ้มรายชื่อลูกค้าที่สามารถซื้อเชื่อกับกิจการได้ หากไม่มีชื่อลูกค้ารายนั้นปรากฏในแฟ้มลูกค้า ระบบจะทำการปฏิเสธการสั่งซื้อนั้นโดยอัตโนมัติในการใช้ชุดคำสั่ง ตรวจสอบความถูกต้องของข้อมูลเข้า กิจการอาจใช้วิธีตรวจสอบได้หลายวิธี เช่น

- การตรวจสอบความสมเหตุสมผลของข้อมูล เช่น การขึ้นเงินเดือนพนักงานแต่ละครั้งจะต้องไม่เกิน 10% ของฐานเงินเดือน เป็นต้น

การควบคุมเกี่ยวกับการประมวลผล

- การใช้เลขโดดตรวจสอบ เช่น ในการกำหนดรหัสลูกค้าแต่แรก สมมุติลูกค้ารายหนึ่งมีรหัสลูกค้า 1234 กิจการจะเพิ่มตัวที่ 5 เพื่อใช้เป็นเลขโดดตรวจสอบ ในการหาตัวเลขลำดับที่ 5 กิจการอาจใช้วิธีคิด เช่น $1+2+3+4=10$ เมื่อนำตัวเลข 4 ตัวข้างหน้ามาบวกกันได้ 10 แล้ว ให้หารด้วยจำนวนเต็มอะไรก็ได้ เช่น 7 จะได้ $10/7 = 1.4285...$ กิจการจะใช้ตัวเลขที่เป็นเศษตัวแรก ได้แก่ 4 เป็นตัวเลขตำแหน่งที่ 5 ดังนั้นลูกค้ารายนี้จะได้แก่ 12344 ทุกครั้งที่มีการใส่รหัสลูกค้าระบบจะนำตัวเลข 4 ลำดับแรกมาบวกกันหารด้วย 7 จะต้องได้เศษตัวแรกเป็น 4 เสมอถ้าไม่ใช่แสดงว่าพนักงานป้อนข้อมูลรหัสลูกค้าตัวใดตัวหนึ่งผิด

5) การกำหนดให้ระบบสามารถเตือนผู้ใส่ข้อมูลได้ทันที (online prompting) เช่น เมื่อพนักงานใส่ชั่วโมงทำงานล่วงหน้าของพนักงานคนหนึ่งลงคอมพิวเตอร์ ระบบจะทำการตรวจสอบว่าชั่วโมงทำงานล่วงเวลาสูงสุดของพนักงานคนหนึ่งจะเกิน 4 ชั่วโมงต่อวันไม่ได้ หากข้อมูลเข้าเกี่ยวกับชั่วโมงทำงานล่วงเวลานี้ถูกป้อนเข้าเป็น 8 ชั่วโมง ระบบจะเตือนกลับว่าชั่วโมงทำงานล่วงเวลาจะเกิน 4 ชั่วโมงต่อวันไม่ได้หรือในกรณีที่พนักงานป้อนข้อมูลเข้าลิ้มใส่เบอร์โทรศัพท์ของลูกค้าบนหน้าจอคอมพิวเตอร์ เมื่อพยายามสั่งให้ระบบรับข้อมูล ระบบจะเตือนว่าช่องหมายเลขโทรศัพท์เป็นข้อมูลที่บังคับให้ใส่ (Forcefield)

การควบคุมเกี่ยวกับการประมวลผล

6) การกำหนดให้ระบบแจ้งกลับให้ผู้คีย์ข้อมูลเข้าทราบว่าระบบตอบสนองต่อข้อมูลเข้าอย่างไร (interactive feedback check) เช่น เมื่อพนักงานคีย์ข้อมูลบนใบเสร็จรับเงินที่อยู่บนหน้าจอคอมพิวเตอร์เรียบร้อยแล้ว กด Enter เพื่อส่งข้อมูลเข้าสู่ระบบระบบจะตอบกลับทันทีว่ารายการค้าได้ถูกนำเข้าสู่ระบบแล้ว (accepted) หรือข้อมูลเข้าไม่ผ่านการตรวจสอบ (rejected)

7) การคีย์ข้อมูลเข้า 2 ครั้ง โดยต่างบุคคล คนแรกคีย์ข้อมูลลงสู่สื่ออิเล็กทรอนิกส์ คนที่สองตรวจทานการคีย์ข้อมูลซ้ำของคนแรก ข้อมูลเข้าที่คีย์โดยบุคคลทั้งสองต้องตรงกัน

8) ในการประมวลผล ทุกขั้นตอนที่มีรายการปฏิเสธข้อมูลเข้า กิจการจะต้องมีคู่มือที่ระบุขั้นตอนงานอย่างชัดเจนว่า ข้อมูลเข้าที่ถูกปฏิเสธจะต้องมีการจัดการอย่างไร เช่น จัดทำเป็นรายงานรายการที่ถูกปฏิเสธเสนอผู้บริหารรับทราบต่อไป

การควบคุมเกี่ยวกับการประมวลผล

9) เอกสารเบื้องต้นที่ใช้ในการบันทึกการเกิดของรายการค้าทุกรายการ จะต้องมีการจัดเก็บเข้าแฟ้ม เพื่อใช้เป็นเอกสารอ้างอิงต่อไป เช่น แฟ้มใบเสนอซื้อ แฟ้มใบสั่งซื้อ แฟ้มใบรับสินค้า แฟ้มเงินสดรับ เป็นต้น เอกสารเหล่านี้อาจถูกเก็บในรูปแบบของเอกสารอิเล็กทรอนิกส์ โดยการใช้สแกนเนอร์รับรูปแบบของข้อมูลเป็น 0 หรือ 1 (ปิดหรือเปิด) เมื่อรวมจุดภาพ (pixel) ที่มีค่าเป็น 0 หรือ 1 นี้มาประกอบขึ้นเป็นรูปภาพ (image) ก็จะได้รูปแบบของเอกสารแต่ละใบ 10) การดึงข้อมูลเข้ามาจากแฟ้มหลัก เช่น เมื่อพนักงานป้อนรหัสลูกค้าบนหน้าจอเพื่อรอรับข้อมูลในการจัดทำใบสั่งขาย ระบบจะไปดึงข้อมูลต่าง ๆ เกี่ยวกับลูกค้ารายนั้นออกมาจากแฟ้มหลักลูกค้า เช่น ชื่อ สกุล อยู่ เงื่อนไขการชำระหนี้ วงเงินซื้อเชื่อคงเหลือ ยอดการค้าชำระ เป็นต้น

การควบคุมเกี่ยวกับการประมวลผล

11) การป้อนข้อมูลเข้า ณ จุดกำเนิดข้อมูลนั้น เช่น การกำหนดให้พนักงานขายเป็นคนป้อนข้อมูลเข้าบนหน้าจอคอมพิวเตอร์ เพื่อรับข้อมูล เข้า ณ จุดที่เกิดการขายแทนการให้พนักงานขายกรอกข้อมูลลงบนเอกสารเบื้องต้นแบบกระดาษ แล้วส่งเอกสารเบื้องต้นนั้นไปให้ฝ่ายประมวลผล เพื่อเป็นผู้ป้อนข้อมูลลงสู่ระบบคอมพิวเตอร์

12) การใช้เอกสารกลับ (turnaround document) ตัวอย่างเช่น ใบหีบสินค้า เป็นเอกสารซึ่งเป็นข้อมูลออกของระบบการส่งขาย หากใบหีบสินค้าเป็นข้อมูลออกที่ถูกจัดทำโดยคอมพิวเตอร์เมื่อพนักงานคลังสินค้าหีบสินค้าแล้ว ก็จะสแกนรหัสแท่งสินค้าที่ปรากฏบนสินค้าลงสู่ใบหีบสินค้า ใบหีบสินค้าที่มีรหัสแท่งสินค้านี้อาจถูกใช้เป็นเอกสารกลับนำเข้าสู่ระบบการจัดส่งสินค้าต่อไป

การควบคุมความถูกต้องของการปรับยอดบัญชีและการควบคุมความครบถ้วนของการปรับยอดบัญชี

1) การใช้การควบคุมแบบกลุ่ม (batch control) คือการใช้ผลรวมของเขตข้อมูลที่มีค่าเป็นจำนวน

เงินเป็นตัวควบคุม และการควบคุมแบบแฮช (hash control)

2) การใช้การตอบกลับอย่างรวดเร็วไปยังหน่วยงานที่เริ่มรายการค้า เช่น ตอบกลับฝ่ายเสนอซื้อว่าได้ทำการจัดซื้อสินค้าแล้ว โดยการส่งสำเนาใบสั่งซื้อกลับให้ฝ่ายเสนอซื้อและตอบกลับลูกค้าว่ากิจการตอบรับการสั่งซื้อจากลูกค้า โดยการส่งสำเนาใบสั่งซื้อขายให้ลูกค้า

3) การติดตามรายการค้าที่เป็นรายการต่อเนื่องจนจบกระบวนการ เช่น ใบสั่งซื้อจะต้องมีการบันทึกการรับสินค้า ในใบรับสินค้าจะต้องมีใบเรียกเก็บเงินจากผู้ขาย รายการสั่งซื้อจะสิ้นสุดกระบวนการก็ต่อเมื่อมีการชำระค่าสินค้า เมื่อมีใบสั่งซื้อและใบรับสินค้า กิจการจะต้องเพิ่มบัญชีเจ้าหนี้ และเมื่อมีการจ่ายชำระหนี้ กิจการจะต้องหักบัญชีเจ้าหนี้ รายงานที่แสดงให้เห็น

สถานะของรายการค้าต่อเนื่องจะทำให้กิจการสามารถติดตาม บันทึก และประมวลผลรายการค้าได้อย่างถูกต้อง ครบถ้วนในกระบวนการขาย ใบสั่งซื้อขายจะต้องมีใบตราส่งสินค้า ใบแจ้งหนี้และเรียกเก็บเงิน จึงจะสามารถปรับยอดบัญชีลูกหนี้ได้และเมื่อรับชำระหนี้จากลูกหนี้แล้ว มีใบสำคัญเงินสดรับแนบชุดเอกสาร จึงจะถือได้ว่าจบกระบวนการขายเชื่อได้

อ้างอิง

พลพธู ปิยวรรณ และกัญนิภักดิ์ นิธิโรจน์ธนนท์. (2557). ระบบสารสนเทศทางการบัญชี.พิมพ์ครั้งที่ 3. หน้า 138 – 172 .กรุงเทพฯ :
วิทย์พัฒน์.

จบบทที่ 6

