สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์
Federation of Accounting Professions
Under the Royal Patronage of His Majesty the King

บทที่ 3

เรื่อง การควบคุมระบบงาน

(เอกสารประกอบการเตรียมตัวเป็นผู้สอบบัญชีรับอนุญาต)

โดย ศ.ดร.นิตยา วงศ์ภินันท์วัฒนา
คณะผู้ทรงคุณวุฒิเกี่ยวกับการทดสอบการปฏิบัติงานสอบบัญชี
ด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์
สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

บทที่ 3
เรื่อง การควบคุมระบบงาน

โดย ศ.ดร.นิตยา วงศ์ภินันท์วัฒนา
คณะผู้ทรงคุณวุฒิเกี่ยวกับการทดสอบการปฏิบัติงานสอบบัญชี
ด้านการสอบบัญชีเนื้อหาการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์
สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

สารบัญ

2. วัตถุประสงค์ในการศึกษา

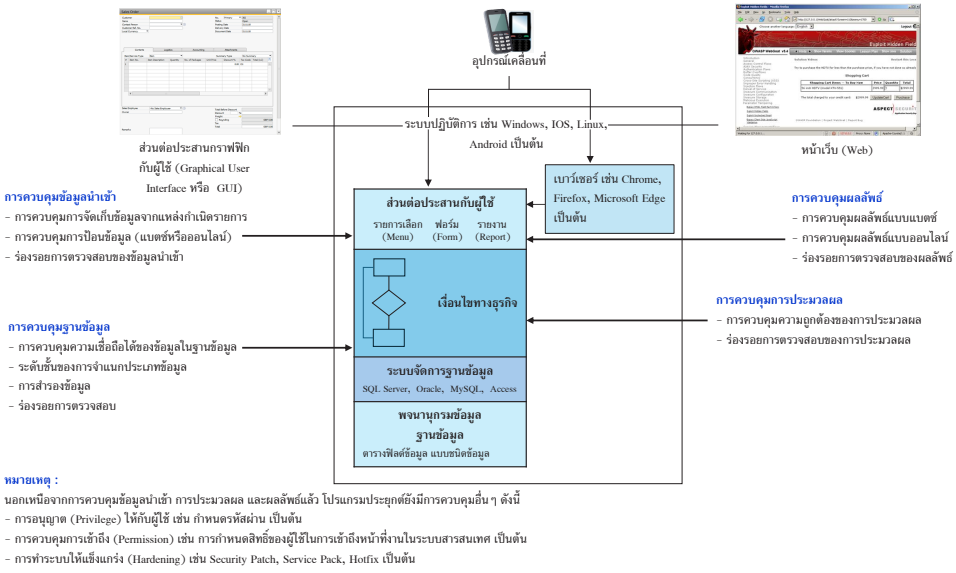
เมื่อได้ศึกษาเนื้อหาของบทนี้แล้ว ผู้ศึกษาจะได้รับความรู้เกี่ยวกับ

1. วัตถุประสงค์และประโยชน์ของการควบคุมระบบงาน
2. องค์ประกอบของระบบงานและความเสี่ยงในการนำระบบงานมาใช้งาน
3. การควบคุมระบบงานซึ่งประกอบด้วย ข้อมูลนำเข้า การประมวลผล และผลลัพธ์
4. ความเสี่ยงและการควบคุมระบบงานบนเว็บตามแนวทางของ The OWASP Foundation
5. ความเสี่ยงและการควบคุมอุปกรณ์เคลื่อนที่

3. คำนำ

ระบบงานเทคโนโลยีสารสนเทศ (ซึ่งต่อไปนี้จะเรียกว่า “ระบบงาน”) โดยทั่วไปจะมีองค์ประกอบหลัก 3 ส่วน ได้แก่ ส่วนต่อประสานกับผู้ใช้ซึ่งเป็นส่วนของข้อมูลนำเข้าและส่งผลลัพธ์ เงื่อนไขทางธุรกิจ และระบบจัดการฐานข้อมูลที่ทำหน้าที่จัดการฐานข้อมูล นอกจากนี้ยังสามารถแบ่งระบบงานออกเป็น ระบบงานที่ใช้งานบนระบบปฏิบัติการ (Application Running Under Operating System) และระบบงานที่ใช้งานบนเว็บ (Web Application หรือ Application Running Under Web Browser) ดังภาพที่ 1 ซึ่งระบบงานแต่ละประเภทจะมีความเสี่ยงและการควบคุมการปฏิบัติงานขั้นพื้นฐานเช่นเดียวกันเพื่อให้มั่นใจว่าข้อมูลได้รับการประมวลผลอย่างถูกต้องครบถ้วนในระยะเวลาที่เหมาะสมและมีสารสนเทศที่จำเป็นแก่ผู้บริหาร โดยความถูกต้องครบถ้วนของผลลัพธ์จะขึ้นอยู่กับองค์ประกอบของระบบงาน ซึ่งประกอบด้วย ส่วนต่อประสานกับผู้ใช้ (User Interface) การประมวลผล และฐานข้อมูล โดยส่วนต่อประสานกับผู้ใช้จะเป็นตัวเชื่อมโยงระหว่างผู้ใช้กับคอมพิวเตอร์เพื่อนำข้อมูลเข้าและส่งผลลัพธ์ ซึ่งอาจทำผ่านเมนูคำสั่ง (Menu) หน้าจอหรือฟอร์ม (Form) และรายงาน (Report) ในส่วนนี้ระบบงานจะมีการควบคุมข้อมูลนำเข้าและการควบคุมผลลัพธ์ เมื่อระบบงานได้รับข้อมูลนำเข้าผ่านทางส่วนต่อประสานกับผู้ใช้ก็จะนำข้อมูลไปประมวลผลตามเงื่อนไขทางธุรกิจที่กำหนดไว้ในระบบงานซึ่งผลลัพธ์และข้อมูลต่าง ๆ จะถูกนำไปจัดเก็บไว้ในฐานข้อมูล โดยจะมีการควบคุมการประมวลผลและการควบคุมฐานข้อมูลตามลำดับ

นอกจากการควบคุมข้อมูลนำเข้า การประมวลผล และผลลัพธ์ที่กล่าวมาข้างต้นแล้ว ระบบงานยังมีการควบคุมอื่น ๆ ได้แก่ (1) การอนุญาต (Privileges) ให้กับผู้ใช้ เช่น กำหนดรหัสผ่าน เป็นต้น (2) การควบคุมการเข้าถึง (Permission) เช่น การกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงหน้าที่งานในระบบสารสนเทศ เป็นต้น และ (3) การทำระบบให้แข็งแกร่ง (Hardening) เช่น Security Patch, Service Pack, Hotfix เป็นต้น กรณีที่ติดตั้งระบบงานในเครื่องคอมพิวเตอร์แบบ Stand Alone หรือ Client-Server ควรคำนึงถึงการควบคุมในเครื่องคอมพิวเตอร์ดังกล่าวที่อาจส่งผลกระทบต่อการควบคุมระบบงานด้วยเช่นกัน



ที่มา: ปรับจาก InnovizAxapta (2002)

ภาพที่ 1 องค์ประกอบหลักของระบบงาน

การควบคุมทั้งหมดข้างต้นนี้เรียกโดยรวมว่า “การควบคุมการประมวลผลสารสนเทศ” ซึ่งมีวัตถุประสงค์เพื่อลดความเสี่ยงที่มีผลต่อบูรณภาพของสารสนเทศ (นั่นคือ ความถูกต้อง ความครบถ้วน และความสมเหตุสมผลของรายการและสารสนเทศอื่นในระบบของกิจการ) โดยอาจเป็นการควบคุมแบบอัตโนมัติ (คือ ฝังอยู่ในระบบงาน) หรือแบบที่ปฏิบัติด้วยมือ (เช่น การควบคุมการนำเข้าและส่งออกของข้อมูล) และการควบคุมอื่น เช่น การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ เป็นต้น

บทนี้จะกล่าวถึงเฉพาะความเสี่ยงและการควบคุมขั้นพื้นฐานของระบบงานในแต่ละกิจกรรมทางธุรกิจ ทั้งที่เป็นการควบคุมแบบอัตโนมัติและแบบที่ปฏิบัติด้วยมือ ซึ่งประกอบด้วย การควบคุมข้อมูลนำเข้า การประมวลผล และผลลัพธ์ กล่าวคือ ไม่ว่าระบบงานนั้นจะเป็นระบบงานใด เช่น ระบบงานสำหรับจัดการรายได้ รายจ่าย และการผลิต เป็นต้น จะต้องมีการควบคุมขั้นพื้นฐานเหล่านี้เพื่อให้ผู้บริหารของกิจการ รวมถึงผู้สอบบัญชีมีความมั่นใจในบูรณภาพของสารสนเทศของกิจการ ส่วนความเสี่ยงและการควบคุมระบบงานที่ใช้งานบนเว็บซึ่งมีลักษณะเฉพาะที่แตกต่างจากระบบงานที่ใช้งานบนระบบปฏิบัติการ จะแยกกล่าวต่อไป

4. ความเสี่ยงในระบบงาน

ความเสี่ยงในระบบงานที่จะส่งผลต่อความถูกต้องครบถ้วนของสารสนเทศ ประกอบด้วย ความเสี่ยงที่จะถูกโจมตีจุดบกพร่องของรหัสคำสั่ง (Source Code) ที่ทำหน้าที่เกี่ยวกับข้อมูลนำเข้า การประมวลผล และผลลัพธ์ (Romney & Steinbart, 2018) ดังนี้

4.1 ความเสี่ยงที่จะถูกโจมตีจุดบกพร่องของรหัสคำสั่งที่ทำหน้าที่เกี่ยวกับข้อมูลนำเข้า

ข้อมูลนำเข้า คือ ข้อมูลที่จัดเก็บจากแหล่งกำเนิดรายการที่เป็นเอกสารหรืออาจจะเป็นการป้อนข้อมูลออนไลน์จากเอกสารก็ได้ เนื่องจากการจัดเก็บข้อมูลตามเอกสารต้องใช้คนในการจัดเก็บข้อมูล ทำให้โอกาสที่จะมีข้อผิดพลาดเป็นไปได้สูง เช่น จัดเก็บข้อมูลซ้ำ บันทึกข้อมูลไม่ถูกต้อง และไม่เหมาะสม กล่าวคือ เป็นรายการที่ไม่เป็นไปตามกฎเกณฑ์ที่องค์กรตั้งไว้ หรือไม่ได้รับอนุมัติ เป็นต้น

ความเสี่ยงที่มักเกิดกับการป้อนข้อมูลออนไลน์หรือการป้อนข้อมูลที่ระบบงานทันที ประกอบด้วย ไม่ป้อนข้อมูลบางรายการ รายการที่ป้อนไม่ถูกต้อง และไม่ตรงตามงวดเวลาทางการบัญชี นอกจากนี้อาจมีการป้อนข้อมูลซ้ำหรือมีรายการสูญหายและเป็นข้อมูลที่ไม่ได้รับอนุมัติก็ได้

4.2 ความเสี่ยงที่จะถูกโจมตีจุดบกพร่องของรหัสคำสั่งที่ทำหน้าที่เกี่ยวกับการประมวลผล

การประมวลผล คือ การปฏิบัติงานที่เกิดขึ้นภายในระบบงาน การปฏิบัติงานนี้เป็นการทำงานตามรหัสคำสั่งงานของระบบงานกับข้อมูล โดยทั่วไปการปฏิบัติงานของโปรแกรมประกอบด้วย การตรวจสอบความสมเหตุสมผลของข้อมูล การคำนวณ เปรียบเทียบ การปรับปรุงรายการในแฟ้มข้อมูล การจัดลำดับ และการแก้ไขข้อผิดพลาดในแฟ้มข้อมูล บางครั้งการทำงานของโปรแกรมดังกล่าวข้างต้นอาจไม่ถูกต้องทั้งหมด เนื่องจากมีข้อผิดพลาดที่เกิดจากการคำนวณผิด การเขียนรหัสคำสั่งงานของระบบงานผิด ใช้งานแฟ้มข้อมูลที่ไม่ถูกต้อง ใช้ตารางข้อมูลหรือข้อมูลอ้างอิงที่ไม่ถูกต้อง กำหนดค่าโดยปริยาย (Default Value) หรือค่าที่โปรแกรมกำหนดมาให้ไม่ถูกต้อง ใช้ระบบงานผิดรุ่น (Version) และข้อมูลที่นำมาประมวลผลเป็นข้อมูลที่ไม่ได้รับการอนุมัติ

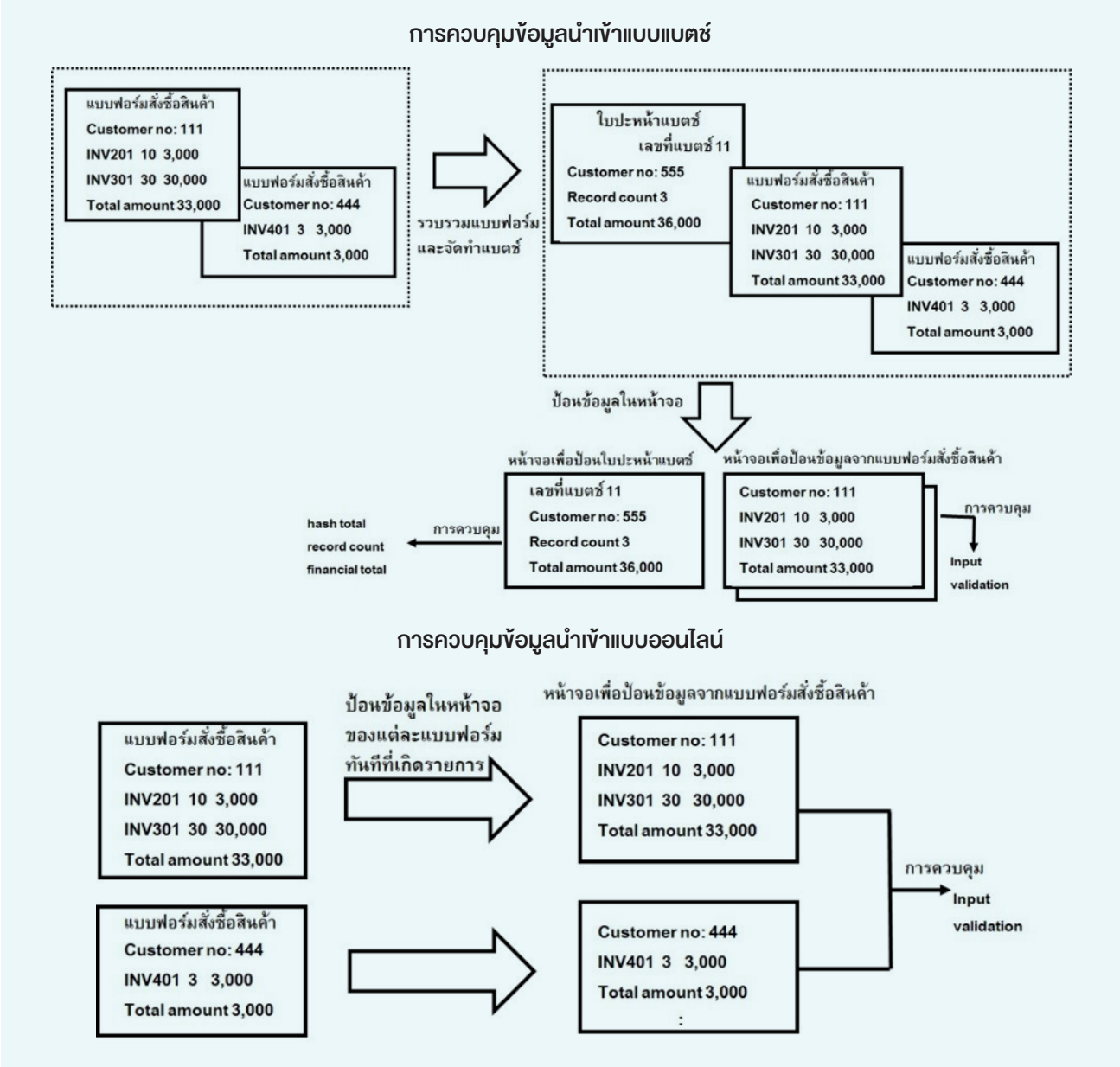
4.3 ความเสี่ยงที่จะถูกโจมตีจุดบกพร่องของรหัสคำสั่งที่ทำหน้าที่เกี่ยวกับผลลัพธ์

ผลลัพธ์หรือรายงานที่ได้จากการประมวลผลอาจอยู่ในรูปของการพิมพ์ลงบนกระดาษพิมพ์ (Hard Copy) หรือ แสดงออกมาทางหน้าจอ (Soft Copy) หรือจัดเก็บไว้ในสื่อบันทึก ความเสี่ยงที่อาจเกิดขึ้นกับผลลัพธ์ไม่ว่าจะอยู่ในรูปแบบใดก็ตามประกอบด้วย รายงานที่จัดส่งให้ผู้ใช้ไม่ถูกต้องครบถ้วน ส่งรายงานไม่ทันตามกำหนดเวลา การจัดเก็บและการทำลายไม่เหมาะสม หรือส่งรายงานให้ผู้ใช้ที่ไม่มีสิทธิได้รับรายงานนั้น ตัวอย่างของผลกระทบที่เกิดจากความเสี่ยงด้านผลลัพธ์ เช่น ถ้าใบเรียกเก็บเงินจากลูกค้าถูกทำลายจะส่งผลให้องค์กรขาดเงินสดหมุนเวียนเพื่อนำมาใช้ในการดำเนินงาน นอกจากนี้ถ้าผู้ที่ไม่เกี่ยวข้องได้รับรายงานจะส่งผลให้ข้อมูลที่มีความอ่อนไหวขององค์กร (Sensitive Data) ถูกเปิดเผยไปยังคู่แข่ง เป็นต้น

5. การควบคุมข้อมูลนำเข้า

การควบคุมข้อมูลนำเข้าขึ้นอยู่กับลักษณะของระบบงาน ซึ่งสามารถแบ่งการนำข้อมูลเข้าเป็น 2 รูปแบบคือ การนำข้อมูลเข้าแบบแบตช์หรือกลุ่ม (Batch Data Entry) และการนำข้อมูลเข้าแบบออนไลน์หรือเชื่อมตรง (Online Data Entry) ภาพที่ 2 แสดงการควบคุมข้อมูลนำเข้าแบบแบตช์และแบบออนไลน์ ซึ่งเป็นสิ่งที่มีความสำคัญอย่างมากต่อคุณภาพของข้อมูล กล่าวคือ ถ้าการป้อนข้อมูลไม่ถูกต้องครบถ้วน จะได้ผลลัพธ์ที่ไม่ถูกต้องครบถ้วนเช่นกัน

จากภาพแสดงให้เห็นว่าการควบคุมความถูกต้องและครบถ้วนของข้อมูลนำเข้าไม่ว่าจะเป็นการนำข้อมูลเข้าแบบแบตช์หรือแบบออนไลน์ จะต้องมีการควบคุมการออกแบบเอกสารต้นฉบับซึ่งเป็นแหล่งกำเนิดรายการ (Source Document) และการออกแบบรูปแบบหน้าจอหรือฟอร์ม (Screen Format or Form) ของระบบงานเพื่อใช้ในการป้อนข้อมูล นอกจากนี้ยังต้องมีการสอบทานความสมเหตุสมผลของข้อมูล (Input Validation) ผ่านหน้าจอ ซึ่งเป็นการจัดเก็บข้อมูลจากแหล่งกำเนิดรายการเพื่อให้มั่นใจว่าข้อมูลที่เกิดขึ้นทั้งหมดได้รับอนุมัติอย่างถูกต้องครบถ้วนและถูกนำเข้าสู่ระบบงานได้ทันเวลา



ภาพที่ 2 การควบคุมข้อมูลนำเข้าแบบแบตช์และแบบออนไลน์

ความแตกต่างของการนำข้อมูลเข้าแบบแบตช์และแบบออนไลน์จะอยู่ที่การควบคุมข้อมูลนำเข้าแบบแบตช์จะต้องมีการจัดทำใบปะหน้าแบตช์เพื่อใช้ในการควบคุมยอดรวมทางการเงิน (Financial Totals) ยอดรวมที่ไม่มีความหมายทางการเงิน (Hash Totals) และยอดรวมจำนวนรายการ (Record Counts) ของเอกสารที่ป้อนเข้าระบบงาน ในขณะที่การควบคุมข้อมูลนำเข้าแบบออนไลน์ไม่ต้องจัดทำใบปะหน้าแบตช์ เนื่องจากข้อมูลจะถูกป้อนเข้าไปในโปรแกรมทีละรายการเมื่อมีรายการเกิดขึ้น

ในการควบคุมความถูกต้องและครบถ้วนของข้อมูลนำเข้าโดยทั่วไปจะเริ่มที่การออกแบบเอกสารต้นฉบับ และการออกแบบรูปแบบหน้าจอให้เหมาะสม เนื่องจากเป็นต้นทางที่จะทำให้ข้อมูลที่จัดเก็บและป้อนเข้าสู่ระบบคอมพิวเตอร์ถูกต้องและครบถ้วนในเบื้องต้น แต่จะไม่กล่าวถึงรายละเอียดในที่นี้ ต่อไปจะกล่าวถึงการควบคุมความถูกต้องและครบถ้วนของข้อมูลนำเข้าโดยเริ่มที่การป้อนข้อมูลเข้าสู่ระบบคอมพิวเตอร์ ภาพที่ 3 แสดงสรุปภาพรวมของการควบคุมข้อมูลนำเข้า ส่วนรายละเอียดการควบคุมข้อมูลนำเข้า มีดังนี้

5. การควบคุมข้อมูลนำเข้า	5.1 การตรวจสอบความสมเหตุสมผลของข้อมูล (Validation)	5.1.1 การตรวจสอบเชิงตรรกะ	(1) การตรวจสอบระดับฟิลด์ ได้แก่ Blank Check, Field Check, Type Check, Limit Check, Range Check, Validity Check, Master File Check และ Size Check (2) การตรวจสอบระดับเรคคอร์ด ได้แก่ Reasonableness Test และ Completeness Check (3) การตรวจสอบระดับแบตช์ (4) การตรวจสอบระดับไฟล์ เช่น Internal Label, Version, Retention Period เป็นต้น
		5.1.2 เลขโดดตรวจสอบ (Check Digit)	
	5.2 การทวนสอบ หรือตรวจทาน (Verification)		
	5.3 การควบคุมการป้อนข้อมูลแบบแบตช์	5.3.1 การควบคุมการรวบรวมข้อมูล	(1) จำกัดจำนวนเอกสารในแบตช์ (2) กำหนดให้เอกสารในแบตช์เป็นเอกสารประเภทเดียวกัน (3) ใบปะหน้าแบตช์ประกอบด้วย Financial Totals, Hash Totals, Record Counts (4) ใบเส้นทางการจัดส่งแบตช์ (5) บันทึกการรับและส่งแบตช์หรือทะเบียนแบตช์
		5.3.2 จัดทำคู่มือการนำส่งข้อมูลเข้าสู่ระบบงาน	

ภาพที่ 3 สรุปภาพรวมของการควบคุมข้อมูลนำเข้า

5. การควบคุมข้อมูลนำเข้า (ต่อ)	5.3 การควบคุมการป้อนข้อมูลแบบแบตช์ (ต่อ)	5.3.3 ตรวจสอบการเรียงลำดับรายการ (เพื่อให้แน่ใจว่าข้อมูลที่ป้อนมีการเรียงลำดับตามที่กำหนด)	
		5.3.4 ไม่นำกลุ่มข้อมูลในแบตช์ไปประมวลผลจนกว่าจะแก้ไขข้อผิดพลาดในกลุ่มข้อมูลนั้นเรียบร้อยแล้ว (ตัวอย่างข้อมูลที่ควรทำทั้งหมดพร้อมกัน ได้แก่ ระบบงานเงินเดือน)	กรณีที่รายการที่มีข้อผิดพลาดถูกบันทึกในแฟ้มพักข้อมูล (Suspense File) ควรล้างรายการออกจากแฟ้มพักข้อมูล เมื่อรายการได้รับการแก้ไขแล้ว
		5.3.5 ทำการประมวลผลกลุ่มข้อมูลทั้งหมดแม้จะมีรายการผิดพลาด	รายการบางประเภท เช่น เปิดบัญชีใหม่ เป็นต้น แม้จะมีข้อผิดพลาดกับรายการนั้นก็ต้องประมวลผล ถ้าไม่ประมวลผลก็จะไม่สามารถประมวลผลรายการอื่น ๆ ได้
		5.3.6 ทำการประมวลผลเฉพาะข้อมูลในกลุ่มข้อมูลที่ไม่มีข้อผิดพลาดเท่านั้น	
		5.3.7 แก้ไขข้อผิดพลาดที่เกิดจากเอกสารแหล่งกำเนิดข้อมูล	
		5.3.8 แก้ไขข้อผิดพลาดที่เกิดจากพนักงานป้อนข้อมูลผิดพลาด	(1) จัดทำบันทึกการติดตามรายการที่มีข้อผิดพลาด (2) ทำการทวนสอบสำหรับรายการที่แก้ไขอีกครั้ง
	5.4 การควบคุมการป้อนข้อมูลออนไลน์	5.4.1 มีคู่มือการปฏิบัติงานสำหรับพนักงานที่ทำหน้าที่ในการป้อนข้อมูลออนไลน์	
		5.4.2 ควบคุมการเข้าถึงเครื่องคอมพิวเตอร์	เช่น จำกัดการเข้าถึงตัวเครื่องคอมพิวเตอร์ และกำหนดรหัสผ่าน เป็นต้น
		5.4.3 การตรวจสอบความสมเหตุสมผลของข้อมูล (Validation)	นอกจากการตรวจสอบความสมเหตุสมผลของข้อมูลที่กล่าวมาแล้ว ยังรวมถึงการกำหนดให้พนักงานป้อนข้อมูลตรวจทานความถูกต้องของข้อมูลที่ปรากฏบนหน้าจอ (Data Echo Check)

ภาพที่ 3 สรุปภาพรวมของการควบคุมข้อมูลนำเข้า (ต่อ)

5. การควบคุมข้อมูลนำเข้า (ต่อ)	5.4 การควบคุมการป้อนข้อมูลออนไลน์ (ต่อ)	5.4.4 แก้ไขข้อผิดพลาด	ปกติมักทำการแก้ไขทันทีที่เกิดข้อผิดพลาด
		5.4.5 จัดการกับข้อผิดพลาด	เช่น ข้อผิดพลาดถูกบันทึกในแฟ้มข้อมูลรายการที่ผิดพลาดเพื่อป้องกันการลืมหรือส่งข้อมูลมาแก้ไขซ้ำ มีคำอธิบายสาเหตุของข้อผิดพลาด และลบข้อมูลที่มีข้อผิดพลาดออกจากแฟ้มข้อมูลรายการที่ผิดพลาดเมื่อมีการแก้ไขข้อมูลแล้ว เป็นต้น
	5.5 การควบคุมการป้อนข้อมูลแบบอัตโนมัติ (Robotic Process Automation หรือ RPA)		
	5.6 ร่องรอยการตรวจสอบของข้อมูลนำเข้า (ข้อมูลที่แสดงลำดับเหตุการณ์เรียงตามวันและเวลาของข้อมูลที่จัดเก็บและนำเข้าสู่ระบบงาน)	5.6.1 ร่องรอยการตรวจสอบการป้อนข้อมูลแบบแบตช์	- ข้อมูลการควบคุมด้านการบัญชี เช่น รหัสพนักงานที่จัดเก็บข้อมูล วันและเวลาที่จัดเก็บข้อมูล เป็นต้น - ข้อมูลการควบคุมด้านการปฏิบัติการ เช่น ระยะเวลาที่ใช้ในการป้อนข้อมูล จำนวนรายการที่ป้อนผิดพลาด เป็นต้น
		5.6.2 ร่องรอยการตรวจสอบการป้อนข้อมูลออนไลน์	- ข้อมูลการควบคุมด้านการบัญชี เช่น วันและเวลา รหัสประจำตัวผู้ป้อนข้อมูล เป็นต้น - ข้อมูลการควบคุมด้านการปฏิบัติการ เช่น จำนวนรายการที่ป้อนผิดพลาดแต่ผ่านการตรวจสอบความสมเหตุสมผลของข้อมูล เป็นต้น

ภาพที่ 3 สรุปภาพรวมของการควบคุมข้อมูลนำเข้า (ต่อ)

5.1 การตรวจสอบความสมเหตุสมผลของข้อมูล (Validation)

การตรวจสอบความสมเหตุสมผลของข้อมูลเป็นการค้นหาข้อผิดพลาด ซึ่งไม่ถูกต้องครบถ้วน ไม่เกี่ยวเนื่อง หรือไม่สอดคล้องกับกลุ่มข้อมูลในแบตช์ผ่านการคำนวณและเปรียบเทียบเชิงตรรกะ (Logical Tests) ปกติการตรวจสอบความสมเหตุสมผลของข้อมูลจะทำในขั้นตอนการป้อนข้อมูลและการประมวลผลมากกว่าในขั้นตอนการจัดเตรียมข้อมูล เนื่องจากคอมพิวเตอร์ที่ใช้ป้อนข้อมูลมีความสามารถที่จำกัดทางด้านการเปรียบเทียบเชิงตรรกะ ปัจจุบันคอมพิวเตอร์ที่ใช้ป้อนข้อมูลมีความสามารถในการเปรียบเทียบเชิงตรรกะเพิ่มมากขึ้น การตรวจสอบความสมเหตุสมผลของข้อมูลบางอย่างอาจจัดทำในขั้นตอนการป้อนข้อมูลได้ เช่น การตรวจสอบความถูกต้องของเลขโดดตรวจสอบ (Check Digit) และการตรวจสอบยอดรวมของกลุ่มข้อมูลในแบตช์ เป็นต้น รายละเอียดการตรวจสอบมีดังนี้

5.1.1 การตรวจสอบเชิงตรรกะ (Logical Tests) จะตรวจสอบมากหรือน้อยขึ้นอยู่กับความสามารถของคอมพิวเตอร์ที่ใช้ในการป้อนข้อมูล และความสำคัญของข้อมูลที่จะป้อนเข้าสู่ระบบงาน การตรวจสอบความถูกต้องของข้อมูลรูปแบบนี้สามารถทำได้ใน 4 ระดับดังนี้

(1) การตรวจสอบระดับฟิลด์ (Field) โดย ฟิลด์ คือ ส่วนย่อยของข้อมูลซึ่งอาจเป็นชื่อบุคคล ที่อยู่ และหมายเลขโทรศัพท์ การตรวจสอบฟิลด์เป็นการตรวจสอบเพื่อดูว่ามีข้อมูลขาดหายหรือเป็นค่าว่างเปล่า (Blank Check) มีข้อมูลตัวอักษรปรากฏในฟิลด์ที่เป็นตัวเลข (Field Check) ข้อมูลเป็นอักษร ตัวเลข และเครื่องหมายพิเศษผสมกันตามที่กำหนด (Type Check) ข้อมูลไม่เกินค่าที่กำหนด (Limit Check) เช่น คะแนนรวมต้องไม่เกิน 100 คะแนน เป็นต้น ข้อมูลอยู่ในช่วงค่าที่กำหนด (Range Check) เช่น มีค่าระหว่าง 0-100 เป็นต้น ข้อมูลเป็นสมาชิกของกลุ่มที่กำหนด (Validity Check) เช่น ข้อมูลต้องอยู่ในตารางอัตราดอกเบี้ย เป็นต้น (ภาพที่ 4) หรือข้อมูลปรากฏในแฟ้มข้อมูลหลัก (Master File Check) เช่น แฟ้มข้อมูลหลักยอดคงเหลือของลูกค้า เป็นต้น (ภาพที่ 5) และขนาดของฟิลด์ถูกต้องตามที่กำหนดหรือไม่ (Size Check) นอกจากนี้ยังรวมถึงการตรวจสอบความถูกต้องของเลขโดดตรวจสอบ ซึ่งจะกล่าวในรายละเอียดต่อไป

แฟ้มข้อมูลหลักเงินฝาก

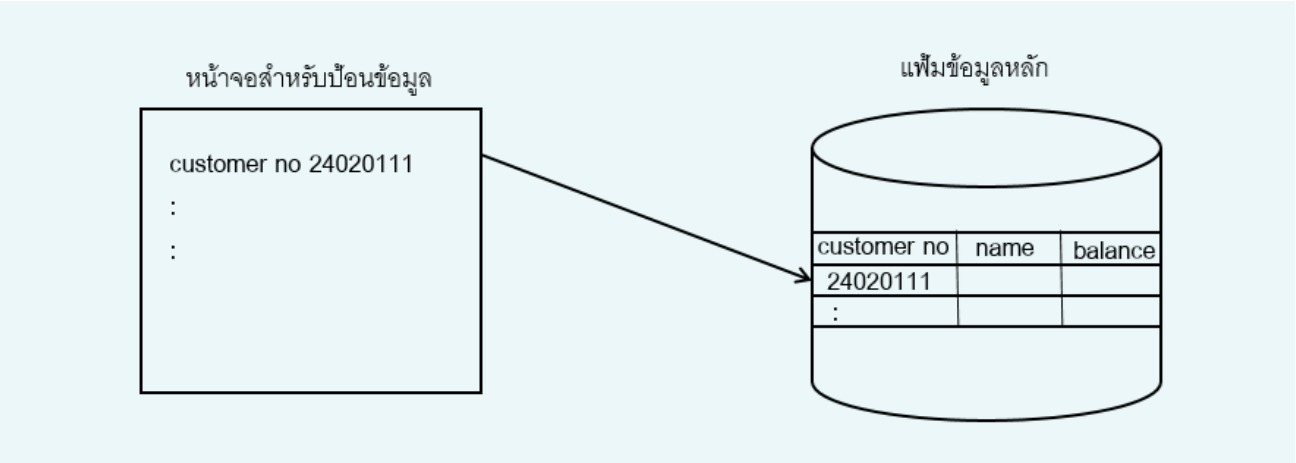
Account number	Name	Deposit type	Interest rate	Date for interest	Balance
1111	A	sav	0.25	12/02/58	10,000
2222	B	special sav	0.75	12/02/58	1,000,000
3333	C	sav	0.25	12/02/58	40,000
4444	D	sav	0.25	12/02/58	20,000
:	:	:	:	:	:

ตารางอัตราดอกเบี้ย

Date	Deposit type	Interest rate
15/02/XX	sav	0.20
15/02/XX	special sav	1.25

หมายเหตุ: กรณีที่แฟ้มข้อมูลหลักจัดเก็บข้อมูลอัตราดอกเบี้ย (Interest Rate) ของแต่ละเลขที่บัญชี (Account Number) โอกาสที่การป้อนข้อมูลหรือปรับเปลี่ยนอัตราดอกเบี้ยให้แต่ละเลขที่บัญชีอาจผิดพลาดได้ แต่ถ้าจัดเก็บประเภทเงินฝาก (Deposit Type) แทนอัตราดอกเบี้ย และค้นหาอัตราดอกเบี้ยจากตารางอัตราดอกเบี้ยแทนก็จะทำให้โอกาสที่จะเกิดข้อผิดพลาดในการป้อนอัตราดอกเบี้ยลดน้อยลง เนื่องจากแก้ไขอัตราดอกเบี้ยเพียงที่เดียวเท่านั้น

ภาพที่ 4 ตัวอย่างข้อมูลเป็นสมาชิกของกลุ่มที่กำหนด



ภาพที่ 5 ตัวอย่างข้อมูลปรากฏในแฟ้มข้อมูลหลัก

(2) การตรวจสอบระดับเรคคอร์ด (Record) โดยเรคคอร์ด คือ ฟิลด์ที่มีความสัมพันธ์กันและมาอยู่ร่วมกัน การตรวจสอบระดับเรคคอร์ดเป็นการตรวจสอบเพื่อดูว่า ข้อมูลของฟิลด์ต่าง ๆ มีความเหมาะสม (Reasonableness Test) เช่น เงินเดือนของพนักงานส่งหนังสือเท่ากับ 40,000 บาทต่อเดือนซึ่งเป็นไปไม่ได้ เป็นต้น นอกจากนี้ยังตรวจสอบว่าเครื่องหมายของฟิลด์ที่เป็นตัวเลขมีความเหมาะสม (Sign Check) เมื่อสัมพันธ์กับฟิลด์อื่น ๆ เช่น จำนวนเงินที่จ่ายออกไปควรมีเครื่องหมายเป็นลบ เป็นต้น และขนาดของเรคคอร์ดต้องเหมาะสมตามที่กำหนด การทดสอบความสมบูรณ์ของข้อมูล (Completeness Check) เช่น รายการขายจะไม่สามารถป้อนได้ถ้าไม่มีรายการข้อมูลลูกค้า หรือข้อมูลลูกค้าไม่สมบูรณ์ เป็นต้น รวมทั้งตรวจสอบลำดับที่ของเรคคอร์ด ซึ่งต้องเรียงลำดับกันในกรณีที่มีจำนวนเรคคอร์ดมากกว่าหนึ่งเรคคอร์ด

(3) การตรวจสอบระดับแบตช์ (Batch) เป็นการตรวจสอบเพื่อดูว่า การควบคุมจำนวนรวมของกลุ่มข้อมูลในแบตช์ถูกต้อง ประเภทของกลุ่มข้อมูลในแบตช์ตรงกับข้อมูลในใบปะหน้าแบตช์ และเลขที่แบตช์เรียงลำดับ

(4) การตรวจสอบระดับไฟล์ (File) เป็นการตรวจเพื่อดูว่า ฉลากหรือป้ายชื่อภายในแฟ้มข้อมูลถูกต้อง (Internal Label) รุ่นของแฟ้มข้อมูลถูกต้อง (Generation or Version) วันหมดอายุของแฟ้มข้อมูล (Retention Period) ยอดรวมในแฟ้มข้อมูลถูกต้องตรงกับการประมวลผลก่อนหน้า เช่น ยอดยกมาของแฟ้มข้อมูลครั้งนี้เท่ากับยอดยกไปของการประมวลผลในครั้งก่อน เป็นต้น

5.1.2 เลขโดดตรวจสอบ (Check Digit) เป็นตัวเลขที่เพิ่มเข้าไปในรหัสเพื่อใช้ตรวจสอบความถูกต้องของรหัส โดยตัวเลขดังกล่าวได้มาจากการคำนวณตามกฎเกณฑ์ที่กำหนดไว้ เมื่อป้อนรหัสเข้ามา ระบบงานจะคำนวณเลขโดดตรวจสอบ ต่อจากนั้นจะนำตัวเลขที่ได้จากการคำนวณไปเปรียบเทียบกับเลขโดดตรวจสอบในรหัสที่ป้อนเข้ามา กรณีที่ตัวเลขมีความแตกต่าง แสดงให้เห็นว่าข้อมูลที่ป้อนเข้ามีข้อผิดพลาด การตรวจสอบวิธีนี้สามารถตรวจสอบข้อผิดพลาดที่เกิดจากการสลับตำแหน่งของตัวเลขและการป้อนตัวเลขผิดได้เป็นอย่างดี ส่วนมากเลขโดดตรวจสอบมักนำมาใช้กับ รหัสสินค้า รหัสประจำตัวลูกค้า และเลขที่บัญชีเงินฝาก ความสามารถของการใช้เลขโดดตรวจสอบ เพื่อตรวจสอบข้อผิดพลาดขึ้นอยู่กับวิธีที่ใช้ในการคำนวณเลขโดดตรวจสอบซึ่งวิธีการดังกล่าวจะแตกต่างกันตาม Modulus และตัวเลขถ่วงน้ำหนัก (Digit Weights) ค่า Modulus คือ ฐานของตัวคูณซึ่งส่วนมากเป็นตัวเลขฐาน 10 หรือ 11 ตัวเลขถ่วงน้ำหนัก คือ ตัวคูณที่มีค่าเป็นบวกซึ่งจะนำไปคูณตัวเลขแต่ละตัวของรหัสที่ต้องการหาเลขโดดตรวจสอบ ค่าตัวเลขถ่วงน้ำหนักอาจมีค่า 2, 3, 4, 5, 6, 7 หรือ 1, 3, 5, 7, 9, 11 หรือค่าอื่น ๆ ขึ้นอยู่กับการกำหนดขององค์กร ตัวอย่างการคำนวณเลขโดดตรวจสอบดังตารางที่ 4.1 เมื่อใช้ Modulus 11 ตัวเลขถ่วงน้ำหนัก 1, 2, 3, 1, 2, 3

ตารางที่ 4.1 ตัวอย่างการคำนวณเลขโดดตรวจสอบ

ขั้นตอนการคำนวณ	วิธีการคำนวณ
1. อ่านรหัส	6 2 3 4 7 1
2. คูณตัวเลขแต่ละตัวในรหัสด้วยตัวเลขถ่วงน้ำหนัก	x1 x 2 x 3 x 1 x 2 x 3 6 4 9 4 14 3
3. บวกผลคูณในขั้นตอนที่ 2	40
4. คำนวณค่า Modulus ที่มีค่าต่อจากค่าในขั้นตอนที่ 3 โดยค่าดังกล่าวต้องเป็นค่าที่มากกว่าผลลัพธ์ในขั้นตอนที่ 3	4 x 11 = 44
5. หาผลต่างของขั้นตอนที่ 4 และขั้นตอนที่ 3 ค่าที่ได้ คือ เลขโดดตรวจสอบ	44 – 40 = 4
6. นำเลขโดดตรวจสอบไปใส่ในรหัส	6 2 3 4 7 1 4

ที่มา: ปรับจาก Weber (1999, p. 436-437)

เนื่องจากการควบคุมโดยใช้เลขโดดตรวจสอบต้องคำนวณตัวเลขเพิ่มเติมเข้าไปในรหัส ทำให้เสียเวลาและพื้นที่ในการจัดเก็บข้อมูล ถ้ามีการใช้เลขโดดตรวจสอบกับทุกข้อมูล ดังนั้นควรเลือกใช้เลขโดดตรวจสอบเฉพาะรหัสที่มีความสำคัญ เช่น เลขทะเบียนนักศึกษา และเลขที่บัญชีเงินฝาก เป็นต้น

5.2 การทวนสอบหรือตรวจทาน (Verification)

นอกจากการสอบทานความสมเหตุสมผลของข้อมูลดังกล่าวข้างต้น ยังสามารถนำวิธีการทวนสอบหรือตรวจทาน (Verification) เพื่อสอบทานความถูกต้องและครบถ้วนของข้อมูลนำเข้า โดยวิธีการทวนสอบ เป็นวิธีการสืบหาข้อผิดพลาดของการป้อนข้อมูลลงในสื่อบันทึก โดยการนำข้อมูลที่พนักงานป้อนครั้งที่สองจากเอกสารต้นฉบับไปเปรียบเทียบกับข้อมูลที่จัดเก็บไว้ในสื่อบันทึกครั้งแรกว่าตรงกันหรือไม่ กรณีที่ข้อมูลที่ป้อนครั้งแรกและครั้งที่สองไม่ตรงกัน พนักงานที่ป้อนข้อมูลในครั้งที่สองจะตรวจสอบว่าข้อมูลที่ป้อนครั้งใดผิดพลาด ต่อจากนั้นจะแก้ไขข้อมูลที่ป้อนให้ถูกต้องตรงกันโดยยึดถือข้อมูลในเอกสารต้นฉบับเป็นหลัก การตรวจสอบด้วยการทวนสอบเป็นวิธีที่เสียค่าใช้จ่ายสูง เนื่องจากต้องป้อนข้อมูลลงในสื่อบันทึกสองครั้ง วิธีที่จะช่วยลดค่าใช้จ่ายในการตรวจสอบด้วยวิธีนี้ทำโดยการทวนสอบเฉพาะส่วนที่สำคัญเท่านั้น เช่น จำนวนเงิน เป็นต้น ส่วนข้อมูลที่เกี่ยวกับชื่อ ที่อยู่ และคำอธิบายสินค้านั้นไม่จำเป็นต้องทวนสอบ อีกวิธีที่สามารถช่วยลดค่าใช้จ่ายในการทวนสอบ คือ ใช้เอกสารครบวงงานที่มีการพิมพ์ข้อมูลบางส่วนล่วงหน้า นอกจากนี้ไม่ควรให้พนักงานที่มีอัตราความผิดพลาดในการป้อนข้อมูลสูงกว่ามาตรฐานที่กำหนดมีหน้าที่ในการป้อนข้อมูล

5.3 การควบคุมการป้อนข้อมูลแบบแบตช์

เนื่องจากข้อมูลที่นำมาป้อนข้อมูลแบบแบตช์จะจัดเก็บในเอกสารต้นฉบับ ดังนั้นการออกแบบเอกสารต้นฉบับ การออกแบบรูปแบบหน้าจอ และการควบคุมรหัสข้อมูลที่กล่าวมาแล้วข้างต้นจึงมีความสำคัญต่อความถูกต้องครบถ้วนของข้อมูลที่จะป้อนในรูปแบบนี้เช่นกัน ในส่วนนี้จะกล่าวเฉพาะการควบคุมการป้อนข้อมูลแบบแบตช์ ซึ่งประกอบด้วย

5.3.1 ควบคุมการรวบรวมข้อมูล (Assembly) ในการรวบรวมเอกสารต้นฉบับเพื่อนำไปจัดกลุ่มเป็นแบตช์นั้น นอกจากจะต้องจัดกลุ่มให้มีจำนวนเอกสารที่เหมาะสมและมีการควบคุมด้านอื่น ๆ ดังกล่าวในขั้นต้นแล้ว ควรมีการจัดทำใบปะหน้าแบตช์ (Batch Header Record) ใบเส้นทางการจัดส่งแบตช์ (Batch Transmittal and Route Slips) และบันทึกการรับและจัดส่งแบตช์ ดังนี้

(1) จำกัดจำนวนเอกสารในแบตช์ กล่าวคือ จำนวนเอกสารในแบตช์ควรมีขนาดไม่มากเกินไปจนทำให้การกระทบยอดรายการระหว่างข้อมูลในแบตช์กับข้อมูลที่ป้อนเข้าสู่ระบบงานกระทำได้ยากเมื่อเกิดผลต่างขึ้น นอกจากนี้จำนวนเอกสารในแบตช์ไม่ควรมีน้อยเกินไปจนทำให้สิ้นเปลืองทรัพยากรในการจัดเตรียมแบตช์มากเกินไป

(2) กำหนดให้เอกสารในแบตช์เป็นเอกสารประเภทเดียวกัน เช่น แบตช์เงินฝาก หรือแบตช์เงินถอน เป็นต้น

(3) ใบปะหน้าแบตช์ประกอบด้วย เลขที่แบตช์ (Batch Number) วันที่ หรืองวดของแบตช์ ประเภทของเอกสารต้นฉบับในแบตช์ และยอดรวมของกลุ่มข้อมูลในแบตช์ที่มีความสำคัญและต้องการให้มีการควบคุมเป็นพิเศษ โดยเลขที่แบตช์เป็นเลขที่มีหมายเลขไม่ซ้ำกัน มีประโยชน์ในการอ้างอิง สามารถตรวจสอบและค้นหาเอกสารในภายหลังได้ การกำหนดเลขที่แบตช์ควรกำหนดให้มีความหมายและมีหมายเลขเรียงลำดับกันไป เช่น เลขที่สองหลักแรก หมายถึง หน่วยงานที่เป็นผู้จัดทำเอกสารนั้น และสองหลักต่อมาแทนลำดับที่ของแบตช์ของหน่วยงานนั้น ส่วนยอดรวมของกลุ่มข้อมูลดังกล่าวข้างต้นจะถูกนำไปใช้ในการสืบหาว่ามีเอกสารหรือข้อมูลส่วนใดผิดพลาดหรือขาดหายไปบ้าง การสืบหาข้อผิดพลาดดังกล่าวทำโดยเปรียบเทียบยอดรวมของกลุ่มข้อมูลที่จัดทำขึ้นกับยอดรวมของกลุ่มข้อมูลที่ระบบงานคำนวณขึ้นมาภายหลังการป้อนข้อมูล ถ้ายอดรวมของกลุ่มข้อมูลเท่ากันก็สามารถสรุปในขั้นต้นได้ว่าข้อมูลที่ป้อนถูกต้อง กรณีที่มีผลต่างก็แสดงว่ามีข้อผิดพลาดเกิดขึ้นในการป้อนข้อมูล ประเภทของยอดรวมของกลุ่มข้อมูลในแบตช์ (Control Totals) แบ่งออกเป็น 3 ประเภทดังนี้

- ยอดรวมทางการเงิน (Financial Totals) เป็นยอดรวมค่าทางการเงินของข้อมูลในแบตช์ เช่น ยอดรวมของจำนวนเงินในใบกำกับสินค้า เป็นต้น
- ยอดรวมที่ไม่มีความหมายทางการเงิน (Hash Totals) เป็นยอดรวมของค่าที่เป็นตัวเลขเพื่อใช้ในการควบคุมกลุ่มข้อมูลในแบตช์ เช่น ยอดรวมเลขที่บัญชีของลูกค้า เป็นต้น
- ยอดรวมจำนวนรายการ (Record Counts) เป็นยอดรวมจำนวนรายการทั้งหมดที่มีอยู่ในแบตช์ ยอดรวมจำนวนรายการดังกล่าวถูกนำมาใช้เพื่อให้เกิดความมั่นใจว่ารายการทั้งหมดในแบตช์ถูกนำมาป้อนเข้าสู่ระบบงานทั้งหมด ตัวอย่างใบปะหน้าแบตช์ ดังภาพที่ 6

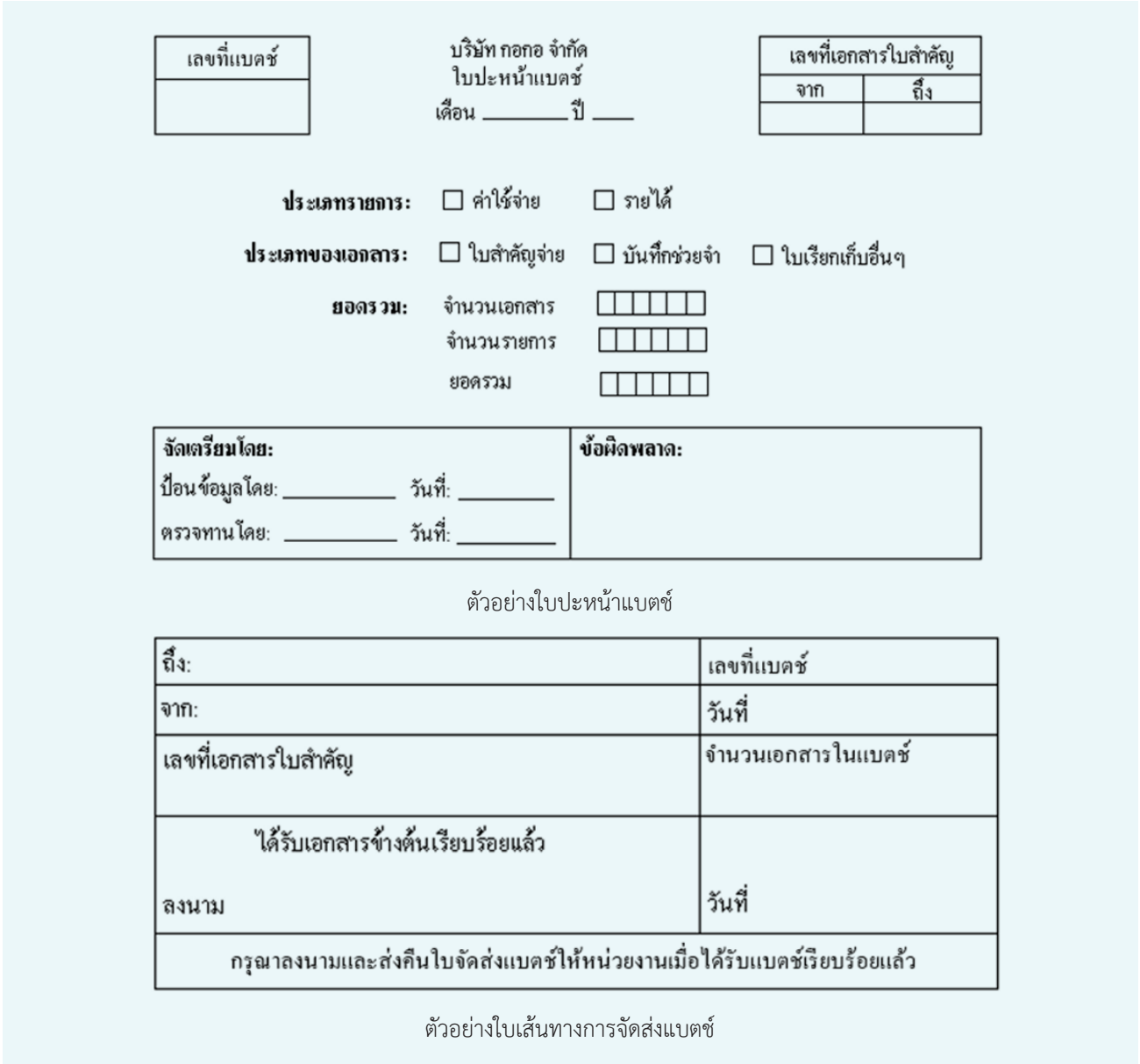
(4) ใบเส้นทางการจัดส่งแบตช์ เป็นเอกสารที่แสดงให้เห็นถึงสถานที่ที่ต้องจัดส่งแบตช์ รวมถึงคำอธิบายแบตช์และยอดรวมของกลุ่มข้อมูลในแบตช์ ตัวอย่างใบเส้นทางการจัดส่งแบตช์ ดังภาพที่ 6

(5) บันทึกการรับและส่งแบตช์หรือทะเบียนแบตช์ ควรประกอบด้วย เลขที่แบตช์ที่เรียงลำดับกัน (Batch Sequence Number) คำอธิบายลักษณะงาน (Job Description) วันและเวลาในการรับและจัดส่งแบตช์ และการลงนามของพนักงานที่ตรวจสอบกลุ่มข้อมูลและป้อนข้อมูลลงในสื่อบันทึก

5.3.2 จัดทำคู่มือการนำส่งข้อมูลเข้าสู่ระบบงาน เพื่อเป็นแนวทางในการปฏิบัติงานของพนักงานรับส่งข้อมูล (Control Clerk) และเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) แนวปฏิบัติในคู่มือดังกล่าวควรประกอบด้วย ตารางเวลาการรับข้อมูลและการจัดส่งรายงาน การควบคุมความถูกต้องของแบตช์ และการจัดการกับข้อผิดพลาดที่เกิดขึ้นกับการป้อนข้อมูล นอกจากนี้ระบบงานควรปฏิเสธข้อมูลที่มีวันที่ของรายการอยู่นอกเหนือจากระยะเวลาที่กำหนด

5.3.3 ตรวจสอบการเรียงลำดับรายการ นอกจากการตรวจสอบความสมเหตุสมผลของข้อมูลที่กล่าวมาแล้วข้างต้น เช่น การตรวจสอบระดับฟิลด์ เรคคอร์ด และไฟล์ และเลขโดดตรวจสอบ เป็นต้น การจัดเตรียมข้อมูลแบบแบตช์ยังควรมีการควบคุมเพิ่มเติม ได้แก่ การทดสอบการเรียงลำดับรายการ เพื่อให้แน่ใจว่าข้อมูลที่ป้อนเข้าสู่ระบบงาน มีการจัดเรียงลำดับรายการตามที่กำหนด โดยปริมาณการตรวจสอบข้อมูลในขั้นนี้จะมากหรือน้อยขึ้นอยู่กับปริมาณการตรวจสอบข้อมูลที่ได้จัดทำในขั้นตอนการจัดเตรียมข้อมูลเป็นสำคัญ

5.3.4 ไม่นำกลุ่มข้อมูลในแบตช์นั้นไปประมวลผลจนกว่าจะแก้ไขข้อผิดพลาดในกลุ่มข้อมูลนั้นเรียบร้อยแล้ว ตัวอย่างระบบงานที่ต้องประมวลผลข้อมูลทั้งหมดพร้อมกันในคราวเดียว ได้แก่ ระบบงานเงินเดือน นอกจากนี้รายการที่มีข้อผิดพลาดอาจถูกบันทึกในแฟ้มพักข้อมูล (Suspense File) เมื่อรายการดังกล่าวได้รับการแก้ไขแล้วจะล้างรายการออกจากแฟ้มพักข้อมูลพร้อมส่งรายการไปประมวลผลในขั้นตอนต่อไป



เลขที่แบตช์	บริษัท กอกอ จำกัด ใบปะหน้าแบตช์ เดือน _____ ปี ____	เลขที่เอกสารใบสำคัญ	
		จาก	ถึง

ประเภทรายการ: ☐ ค่าใช้จ่าย ☐ รายได้

ประเภทของเอกสาร: ☐ ใบสำคัญจ่าย ☐ บันทึกช่วยจำ ☐ ใบเรียกเก็บอื่นๆ

ยอดรวม: จำนวนเอกสาร ☐☐☐☐☐☐

จำนวนรายการ ☐☐☐☐☐☐

ยอดรวม ☐☐☐☐☐☐

จัดเตรียมโดย:	**ข้อผิดพลาด:**
ป้อนข้อมูลโดย: _____ วันที่: _____	
ตรวจทานโดย: _____ วันที่: _____	

ตัวอย่างใบปะหน้าแบตช์

ถึง:	เลขที่แบตช์
จาก:	วันที่
เลขที่เอกสารใบสำคัญ	จำนวนเอกสารในแบตช์
ได้รับเอกสารข้างต้นเรียบร้อยแล้ว ลงนาม	วันที่
กรุณาลงนามและส่งคืนใบจัดส่งแบตช์ให้หน่วยงานเมื่อได้รับแบตช์เรียบร้อยแล้ว	

ตัวอย่างใบเส้นทางการจัดส่งแบตช์

ที่มา: ปรับจาก Weber (1999, p. 440-441)

ภาพที่ 6 ตัวอย่างเอกสารที่เกี่ยวข้องกับการรวบรวมข้อมูลแบบแบตช์

5.3.5 ทำการประมวลผลกลุ่มข้อมูลทั้งหมดแม้จะมีรายการผิดพลาด รายการบางประเภท เช่น การเปิดบัญชีใหม่ เป็นต้น เป็นรายการที่ต้องประมวลผลแม้จะมีข้อผิดพลาดกับรายการนั้น เนื่องจากถ้าไม่ประมวลผลจะไม่สามารถประมวลผลข้อมูลด้านอื่น ๆ เช่น รายการซื้อขายสินค้าได้ ดังนั้นจึงต้องประมวลผลรายการที่มีข้อผิดพลาดก่อน ต่อจากนั้นจะบันทึกข้อผิดพลาดเพื่อเตือนให้ผู้ใช้แก้ไขข้อผิดพลาดต่อไป

5.3.6 ทำการประมวลผลเฉพาะข้อมูลในกลุ่มข้อมูลที่ไม่มีข้อผิดพลาดเท่านั้น การประมวลผลบางประเภทสามารถจัดทำกับรายการในกลุ่มข้อมูลที่ไม่ผิดพลาดเท่านั้น ส่วนรายการที่มีข้อผิดพลาดจะถูกจัดเก็บไว้เพื่อแก้ไขและส่งมาประมวลผลในครั้งต่อไป และเมื่อนำรายการที่มีข้อผิดพลาดออกจากกลุ่มข้อมูล ควรปรับปรุงยอดคุมแบตช์ด้วย เนื่องจากรายการที่ถูกแก้ไขแล้วนั้นอาจมีข้อผิดพลาดเกิดขึ้นได้เช่นกัน ดังนั้นจึงควรทดสอบความถูกต้องของรายการที่ได้รับการแก้ไขเหล่านั้นเช่นกัน

5.3.7 แก้ไขข้อผิดพลาดที่เกิดจากเอกสารต้นฉบับ เช่น ข้อความในเอกสารต้นฉบับมีรายการไม่ชัดเจน และข้อผิดพลาดที่เกิดจากขั้นตอนการจัดเก็บข้อมูลจากเอกสารต้นฉบับ เป็นต้น จึงควรนำเอกสารต้นฉบับคืนต้นสังกัดเพื่อแก้ไขข้อผิดพลาด นอกจากนี้ควรควบคุมเพื่อให้แน่ใจว่ามีการนำส่งเอกสารที่แก้ไขเรียบร้อยแล้วกลับคืนมาโดยจัดทำบันทึกการส่งและรับเอกสารกับต้นสังกัด และควรปรับปรุงยอดรวมของกลุ่มข้อมูลในแบตช์ที่ใบปะหน้าแบตช์โดยตัดยอดเอกสารที่ส่งคืนต้นสังกัดด้วย

5.3.8 แก้ไขข้อผิดพลาดที่เกิดจากพนักงานป้อนข้อมูลผิด การแก้ไขข้อผิดพลาดขึ้นอยู่กับเครื่องคอมพิวเตอร์ที่ใช้ในการป้อนข้อมูล กล่าวคือ ถ้าคอมพิวเตอร์ที่ใช้ป้อนข้อมูลแสดงข้อผิดพลาดทันทีที่พนักงานป้อนรายการผิด พนักงานสามารถแก้ไขข้อผิดพลาดได้ทันที แต่ถ้าเครื่องคอมพิวเตอร์ที่ใช้ป้อนข้อมูลแสดงข้อผิดพลาดหลังจากพนักงานป้อนข้อมูลเสร็จเรียบร้อยแล้ว การควบคุมการแก้ไขข้อผิดพลาดจะเป็นดังนี้

(1) จัดทำบันทึกการติดตามรายการที่มีข้อผิดพลาด เพื่อให้แน่ใจว่ารายการเหล่านั้นได้รับการแก้ไขและนำกลับเข้าสู่ระบบงาน
(2) ทำการทวนสอบสำหรับรายการที่แก้ไขอีกครั้ง เพื่อให้แน่ใจว่ารายการที่แก้ไขนั้นถูกต้องก่อนที่จะนำรายการเหล่านั้นไปรวมกับรายการอื่น ๆ ในแบตช์

นอกจากการจัดการกับข้อผิดพลาดดังกล่าวมาแล้ว ในการควบคุมการป้อนข้อมูลแบบแบตช์ ควรมีการจัดการกับข้อผิดพลาดโดยทั่วไป ดังนี้

(1) จัดพิมพ์รายงานของข้อมูลที่มีข้อผิดพลาด โดยทำเครื่องหมายภายใต้ข้อมูลที่ผิดพลาด
(2) กำหนดให้พนักงานที่แก้ไขข้อผิดพลาดลงนามในรายงานแสดงข้อมูลที่มีข้อผิดพลาด
(3) ใช้รายงานที่แสดงข้อมูลที่ผิดพลาดเป็นเอกสารประกอบการแก้ไขข้อมูลหรือเอกสารครบวงงาน
(4) จัดเก็บข้อมูลที่มีข้อผิดพลาดในแฟ้มข้อมูลรายการที่ผิดพลาด กรณีที่ไม่มีการแก้ไขข้อผิดพลาดของข้อมูลในแฟ้มข้อมูลนี้ระบบงานต้องมีการเตือนให้ผู้ใช้ทราบเพื่อแก้ไขข้อผิดพลาดต่อไป
(5) ลบข้อมูลที่มีข้อผิดพลาดออกจากแฟ้มข้อมูลรายการที่ผิดพลาดเมื่อมีการแก้ไขข้อมูลแล้ว เพื่อป้องกันการส่งข้อมูลมาแก้ไขซ้ำ นอกจากนี้อาจทำด้วยการขีดฆ่าข้อมูลในรายงานข้อมูลที่มีข้อผิดพลาดว่าได้มีการแก้ไขข้อมูลนั้นแล้ว

5.4 การควบคุมการป้อนข้อมูลออนไลน์

เนื่องจากการป้อนข้อมูลแบบออนไลน์จะทำผ่านหน้าจอคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ ดังนั้นการออกแบบรูปแบบหน้าจอและการควบคุมรหัสข้อมูลที่กล่าวมาแล้วข้างต้นจึงมีความสำคัญต่อความถูกต้องครบถ้วนของข้อมูลที่จะป้อนในรูปแบบนี้เช่นกัน จึงขอกล่าวเฉพาะการควบคุมการป้อนข้อมูลออนไลน์ ซึ่งมีดังนี้

5.4.1 มีคู่มือการปฏิบัติงานสำหรับพนักงานที่ทำหน้าที่ป้อนข้อมูลออนไลน์ คู่มือดังกล่าวควรประกอบด้วย การใช้งานเครื่องคอมพิวเตอร์สำหรับป้อนข้อมูล วิธีการเรียกใช้แฟ้มข้อมูลที่เกี่ยวข้อง และการแก้ไขข้อผิดพลาดที่เกิดจากการป้อนข้อมูล

5.4.2 ควบคุมการเข้าถึงเครื่องคอมพิวเตอร์เป็นสิ่งที่จำเป็นเพื่อให้แน่ใจว่ารายการที่มีตัวตนเท่านั้นที่ถูกป้อนเข้าคอมพิวเตอร์โดยบุคคลที่ได้รับอนุญาตเท่านั้นที่เป็นผู้ใช้งานและเข้าถึงระบบงานได้ ตัวอย่างการควบคุมมีดังนี้

(1) จำกัดการเข้าถึงตัวเครื่องคอมพิวเตอร์ทางกายภาพ เช่น ติดตั้งเครื่องคอมพิวเตอร์ในห้องที่ผู้ที่ไม่มีหน้าที่เกี่ยวข้องไม่สามารถเข้าได้ เพื่อให้แน่ใจว่าผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงเครื่องคอมพิวเตอร์ได้ เป็นต้น

(2) มีแบบแผนการอนุญาตอย่างเป็นทางการสำหรับเจ้าหน้าที่ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และมีรูปแบบการใช้งานที่เหมาะสม

(3) กำหนดรหัสผ่านเพื่อให้แน่ใจว่าผู้ใช้เป็นผู้ที่ได้รับอนุญาตเท่านั้น

(4) ป้องกันข้อมูลที่สำคัญโดยใช้วิธีการเข้ารหัสข้อมูล (Encryption) ให้อยู่ในรูปแบบที่บุคคลที่ไม่เกี่ยวข้องไม่สามารถแก้ไขเปลี่ยนแปลงหรืออ่านข้อมูลนั้นได้ในระหว่างการส่งผ่านข้อมูล

5.4.3 ตรวจสอบความสมเหตุสมผลของข้อมูล นอกจากการตรวจสอบความสมเหตุสมผลของข้อมูลที่กล่าวมาแล้วข้างต้น เช่น การตรวจสอบระดับฟิลด์ เรคคอร์ด และไฟล์ และเลขโดดตรวจสอบ เป็นต้น แล้วยังควรกำหนดให้พนักงานที่ป้อนข้อมูลตรวจทานความถูกต้องของข้อมูลที่ปรากฏบนหน้าจอว่าถูกต้องหรือไม่ (Data Echo Check) รวมถึงกำหนดให้ระบบงานใช้วิธีการอ้างอิงรายการที่ป้อนกับข้อมูลในแฟ้มข้อมูลหลัก เช่น เปรียบเทียบว่าเลขที่บัญชีลูกค้าที่ป้อนเข้าสู่ระบบงานตรงกับเลขที่บัญชีในแฟ้มข้อมูลหลัก เป็นต้น

5.4.4 แก้ไขข้อผิดพลาด ปกติการแก้ไขข้อผิดพลาดของรายการที่ป้อนผ่านเครื่องคอมพิวเตอร์มักทำทันทีที่เกิดข้อผิดพลาดและแก้ไขทีละรายการ การแก้ไขรายการที่ผิดมักทำเฉพาะส่วนที่ป้อนผิดเท่านั้น พนักงานที่ทำหน้าที่ป้อนข้อมูลไม่จำเป็นต้องป้อนรายการใหม่ทั้งหมด ในกรณีที่ข้อผิดพลาดมาจากเอกสารต้นฉบับ พนักงานที่ทำหน้าที่ป้อนข้อมูลจะยกเลิกรายการที่ป้อนทั้งรายการและส่งเอกสารคืนผู้ใช้เพื่อแก้ไขและส่งเอกสารที่แก้ไขแล้วกลับคืนมา

5.4.5 จัดการกับข้อผิดพลาด ในกรณีที่ข้อมูลที่นำเข้าในระบบงานมีข้อผิดพลาดจะต้องสอบทานความเหมาะสมของการจัดการกับข้อผิดพลาดเพื่อให้เกิดความมั่นใจว่า

(1) ข้อผิดพลาดได้รับการแก้ไข

(2) ข้อผิดพลาดถูกบันทึกในแฟ้มข้อมูลรายการที่ผิดพลาด (Error File) เพื่อป้องกันการลืมหรือส่งข้อมูลมาแก้ไขซ้ำ

(3) มีคำอธิบายสาเหตุของข้อผิดพลาด

(4) มีการแก้ไขข้อผิดพลาดภายในเวลาที่เหมาะสม

5.5 การควบคุมการป้อนข้อมูลแบบอัตโนมัติ

ปัจจุบันมีโปรแกรมวิทยาการหุ่นยนต์ หรือ Robotic Process Automation (RPA) ที่ช่วยให้ผู้ใช้งานสามารถจัดสร้างขั้นตอน (Flow) ให้โปรแกรมทำงานอัตโนมัติไม่ว่าจะเป็นการนำข้อมูลจากแฟ้มข้อมูลหนึ่ง เช่น แฟ้มข้อมูลที่เป็น Excel เป็นต้น เพื่อนำไปป้อนที่หน้าจอของระบบงานต่าง ๆ เมื่อสั่งให้โปรแกรม RPA ทำงาน ตัวอย่างของโปรแกรม RPA เช่น IBM RPA With Automation Anywhere, UiPath, BluePrism, NICE, RPA Argos, และ Microsoft Power Automate Desktop เป็นต้น การควบคุมความถูกต้องครบถ้วนของข้อมูลนำเข้าแบบอัตโนมัตินี้ นอกจากจะต้องกำหนดให้มีการสอบทานความสมเหตุสมผลของข้อมูลที่ป้อนเข้าในแฟ้มข้อมูลต้นฉบับแล้ว ควรตรวจสอบขั้นตอนอัตโนมัติที่กำหนดไว้ว่ามีการทำงานได้อย่างถูกต้องหรือไม่ด้วยการทดสอบการทำงานของขั้นตอนที่สร้างขึ้นก่อนนำไปใช้งานจริง โปรแกรม RPA นอกจากจะช่วยให้สามารถนำข้อมูลจากแฟ้มข้อมูลหนึ่งไปยังระบบงานหนึ่งแล้วยังสามารถนำข้อมูลออกจากระบบงานและจัดสร้างแฟ้มข้อมูลใหม่ด้วย โดยแฟ้มข้อมูลนั้นมีได้หลายประเภท กล่าวคือ อาจเป็น Excel, Text หรือ JSON File ขึ้นอยู่กับโปรแกรม RPA

นอกจากนี้ควรมีการควบคุม ดังนี้

(1) มีการกำหนดมาตรฐานในการออกแบบ การนำออกใช้งานและบำรุงรักษาขั้นตอนอัตโนมัติ

(2) จัดเก็บแฟ้มของขั้นตอนอัตโนมัติในแฟ้มข้อมูลที่ปลอดภัยรวมทั้งจัดเก็บเป็นเอกสาร ณ สถานที่อื่นภายนอกองค์กรด้วย

(3) ทดสอบการทำงานของขั้นตอนอัตโนมัติเมื่อมีการปรับปรุงเปลี่ยนแปลงขั้นตอนอัตโนมัติ

(4) ติดตามความถูกต้องครบถ้วนของขั้นตอนอัตโนมัติอย่างสม่ำเสมอ ในกรณีที่ขั้นตอนอัตโนมัติไม่สามารถทำงานได้ ควรกำหนดให้เจ้าหน้าที่ทำงานแทน ซึ่งองค์กรควรฝึกฝนเจ้าหน้าที่เพื่อให้สามารถทำงานแทนขั้นตอนอัตโนมัติด้วย เพราะเจ้าหน้าที่อาจขาดความรู้หรือประสบการณ์ที่จะทำงานนั้น ๆ ได้ รวมถึงการอนุญาตให้กับตัวแทน การควบคุมการเข้าถึง โดยมีการสอบทานรายชื่อผู้มีสิทธิ์แก้ไขขั้นตอนอัตโนมัติและสอบทานบัญชีผู้ใช้งาน (User) ที่ผูกอยู่กับขั้นตอนอัตโนมัติ (ถ้ามี) ว่ามีความเหมาะสมหรือไม่ และควรทำให้ระบบแข็งแกร่งด้วย

5.6 ร่องรอยการตรวจสอบของข้อมูลนำเข้า

ร่องรอยการตรวจสอบ (Audit Trail) เป็นสิ่งที่สำคัญที่แสดงให้เห็นถึงการควบคุมด้านการปฏิบัติการ การควบคุมด้านการบัญชี และการปฏิบัติตามกฎเกณฑ์ของหน่วยงานราชการ ผู้สอบบัญชีสามารถใช้ร่องรอยการตรวจสอบเพื่อวิเคราะห์สาเหตุและผลของข้อผิดพลาดของรายการต่าง ๆ ในระบบงาน รวมถึงใช้ในการทดสอบรายการและยอดคงเหลือทางการบัญชีได้ ร่องรอยการตรวจสอบของข้อมูลนำเข้า คือ ลำดับเหตุการณ์เรียงตามวันและเวลาของข้อมูลที่จัดเก็บและนำเข้าสู่ระบบงาน ซึ่งสามารถแยกออกเป็น 2 กลุ่มใหญ่ ๆ คือ ร่องรอยการตรวจสอบการป้อนข้อมูลแบบแบตช์และออนไลน์

5.6.1 ร่องรอยการตรวจสอบการป้อนข้อมูลแบบแบตช์ ร่องรอยการตรวจสอบประเภทนี้ ประกอบด้วย เอกสารต้นฉบับ รายการเปลี่ยนแปลง แฟ้มข้อมูลรายการเปลี่ยนแปลงที่ตรวจสอบความสมเหตุสมผลของข้อมูล บันทึกการรับและส่งแบตช์หรือทะเบียนแบตช์ บันทึกข้อผิดพลาดที่เกิดขึ้น แฟ้มพักข้อมูลที่มีข้อผิดพลาด และรายการข้อผิดพลาด โดยร่องรอยการตรวจสอบข้อมูลนำเข้าดังกล่าวควรประกอบด้วย ข้อมูลที่แสดงให้เห็นถึงการควบคุมด้านการบัญชีและการปฏิบัติงาน ดังนี้

ข้อมูลการควบคุมด้านการบัญชี ประกอบด้วย

- รหัสพนักงานที่จัดเก็บข้อมูลจากแหล่งกำเนิดข้อมูล
- รหัสพนักงานที่ป้อนข้อมูล
- วันและเวลาที่จัดเก็บข้อมูล ซึ่งช่วยให้ทราบถึงวันและเวลาในการตรวจสอบความสมเหตุสมผลของข้อมูลและการแก้ไขข้อผิดพลาด นอกจากนี้โปรแกรมสอบทานความสมเหตุสมผลของข้อมูลควรสร้างรหัสสำหรับแต่ละรายการที่มีข้อผิดพลาด เพื่อใช้อ้างอิงรายการจนกว่ารายการนั้นจะได้รับการแก้ไขจนถูกต้อง
- รหัสอุปกรณ์ที่ใช้ในการป้อนข้อมูล
- ข้อมูลหลักหรือบัญชีหลักที่ถูกปรับปรุงด้วยรายการหรือข้อมูลที่จัดเก็บ
- รายละเอียดของรายการหรือข้อมูลที่จัดเก็บ
- เลขที่แบตช์ของรายการหรือข้อมูลที่จัดเก็บ

ข้อมูลการควบคุมด้านการปฏิบัติการ ซึ่งเป็นร่องรอยการตรวจสอบที่สามารถนำมาใช้เพื่อปรับปรุงประสิทธิภาพและประสิทธิผลของระบบ ประกอบด้วย

- ระยะเวลาที่ใช้ในการป้อนข้อมูลจากเอกสารต้นฉบับ
- จำนวนรายการที่เครื่องอ่านข้อมูลผิดพลาด (กรณีที่ใช้เครื่องสแกนเนอร์อ่านข้อมูลจากเอกสารต้นฉบับที่เขียนด้วยลายมือ)
- จำนวนรายการที่ป้อนผิดพลาดและตรวจพบในขั้นตอนการทวนสอบ

5.6.2 ร่องรอยการตรวจสอบการป้อนข้อมูลออนไลน์ แม้ว่าการป้อนข้อมูลออนไลน์จะไม่มีเอกสารต้นฉบับ เนื่องจากรายการที่เกิดขึ้นมักถูกป้อนเข้าสู่ระบบงานโดยตรงเมื่อมีรายการเกิดขึ้น แต่สามารถหาร่องรอยการตรวจสอบได้โดยพิจารณาจากหลักฐานดังนี้

ข้อมูลการควบคุมด้านการบัญชี ประกอบด้วย

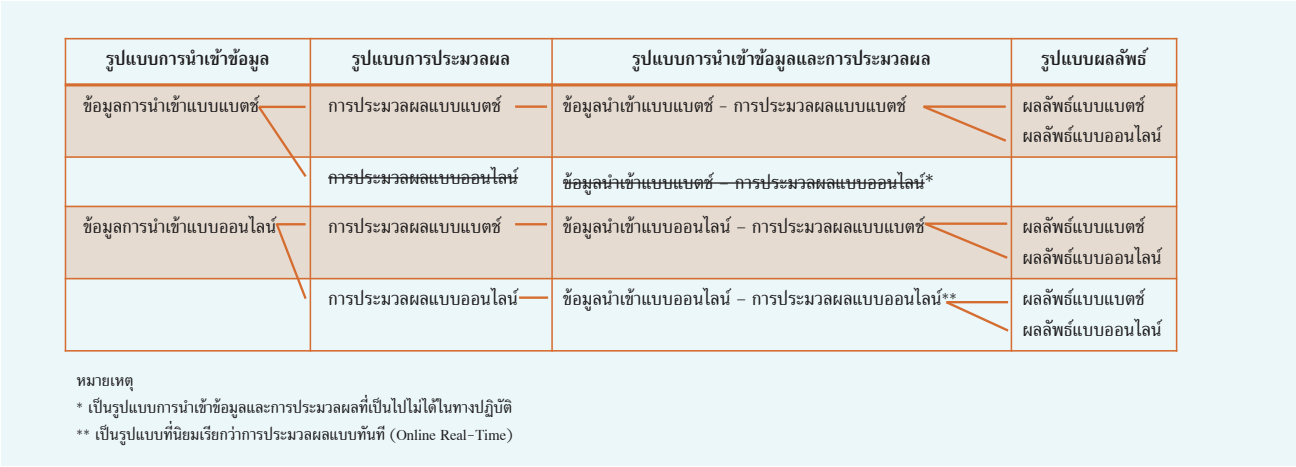
- รายการแต่ละรายการมักมีการระบุหมายเลขเฉพาะ (Transaction ID) ซึ่งสามารถใช้ติดตามรายการเหล่านั้นจากรายงานได้
- รายละเอียดของรายการที่จัดทำขึ้นเพื่อให้พนักงานใช้ป้อนข้อมูล โดยรายละเอียดของรายการเหมือนกับรายการเปลี่ยนแปลงในสมุดรายวัน
- ลงบันทึกรายการเปลี่ยนแปลงที่ทำผ่านเครื่องคอมพิวเตอร์ (Transaction Log) ซึ่งเป็นบันทึกการทำรายการทั้งหมดที่เครื่องคอมพิวเตอร์ โดยระบบงานจะบันทึกข้อมูล วัน เวลา รหัสประจำตัวผู้ใช้และรายการที่จัดทำ

ข้อมูลการควบคุมด้านการปฏิบัติการ ประกอบด้วย

- จำนวนรายการที่ป้อนผิดพลาดผ่านเครื่องคอมพิวเตอร์
- จำนวนรายการที่ป้อนผิดพลาดแต่ผ่านการตรวจสอบความสมเหตุสมผลของข้อมูล

6. การควบคุมการประมวลผล

การนำเข้าข้อมูลในแต่ละรูปแบบจะส่งผลต่อรูปแบบการประมวลผลดังภาพที่ 7 จากภาพจะเห็นได้ว่า ข้อมูลนำเข้าแบบออนไลน์สามารถนำไปประมวลผลทันทีที่เรียกว่า การประมวลผลทันที (Online Real-Time) หรืออาจจัดเก็บไว้ระยะเวลาหนึ่งแล้วจึงนำไปประมวลผลที่เรียกว่า การประมวลผลแบบแบตช์ (Batch Processing) ในขณะที่ข้อมูลนำเข้าแบบแบตช์ ไม่สามารถที่จะนำไปประมวลผลทันทีได้ เนื่องจากการควบคุมการประมวลผลแบบแบตช์และแบบออนไลน์จะเป็นไปในทำนองเดียวกัน จึงขอกล่าวถึงการควบคุมการประมวลผลในภาพรวมเดียว



ภาพที่ 7 ภาพรวมรูปแบบการนำเข้าข้อมูล การประมวลผล และผลลัพธ์

การควบคุมความถูกต้องและร่องรอยการตรวจสอบของการประมวลผล ดังภาพที่ 8 โดยรายละเอียดการควบคุมการประมวลผลมีดังนี้

6. การควบคุมการประมวลผล	6.1 การควบคุมความถูกต้องของการประมวลผล	6.1.1 การจับคู่รายการที่จะประมวลผลกับรายการที่สัมพันธ์กัน เช่น การจ่ายเงินให้ผู้ค้าต้องมีรายการคำสั่งซื้อและรับสินค้าก่อน เป็นต้น	

ภาพที่ 8 สรุปผลรวมของการควบคุมการประมวลผล

6. การควบคุมการประมวลผล (ต่อ)	6.1 การควบคุมความถูกต้องของการประมวลผล (ต่อ)	6.1.2 การควบคุมข้อผิดพลาดจากการประมวลผล	(1) การสอบทานรายงานการประมวลผล เช่น เป็นรายงานที่แสดงชื่อโปรแกรม วันที่ที่โปรแกรมถูกนำมาใช้งาน ข้อมูลที่ใช้ประมวลผล และข้อมูลที่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ทำผ่านทางเครื่องคอนโซล และค่าโดยปริยาย เป็นต้น (2) การสอบทานเพื่อสืบหาข้อผิดพลาดจากข้อมูลนำเข้า เช่น - การตรวจสอบ File Label (Header and Trailer Record) - การตรวจสอบ Record Identification (สำหรับการประมวลผลแบบเรียงลำดับ เช่น ประมวลผลการถอนเงินก่อนรายการฝากเงินด้วยเช็คที่ยังไม่ทราบผลการเรียกเก็บ เป็นต้น) - การตรวจสอบ Transaction Code - การตรวจสอบ Sequence Test (ใช้สำหรับการประมวลผลแบบแบตช์ โดยเรียงลำดับข้อมูลรายการเปลี่ยนแปลงตามแฟ้มข้อมูลหลัก) (3) การสอบทานเพื่อสืบหาข้อผิดพลาดจากการประมวลผล - การตรวจสอบความถูกต้องของการคำนวณ (Arithmetic Accuracy Test, Double Arithmetic, Reverse Multiplication, Overflow) - การตรวจสอบว่าผลลัพธ์ที่ได้มีค่าอยู่ในช่วงที่คาดหมาย - การตรวจสอบว่าผลลัพธ์มีค่าไม่เกินกว่าที่กำหนดไว้

ภาพที่ 8 สรุปผลรวมของการควบคุมการประมวลผล (ต่อ)

6. การควบคุมการประมวลผล (ต่อ)	6.1 การควบคุมความถูกต้องของการประมวลผล (ต่อ)	6.1.2 การควบคุมข้อผิดพลาดจากการประมวลผล (ต่อ)	- การสอบยันตัวเลขระหว่างกัน (Cross-Footing Tests เช่น นำยอดรวมเงินเดือนสุทธิบวกภาษีหัก ณ ที่จ่ายควรเท่ากับยอดรวมเงินเดือน เป็นต้น) - การทดสอบยอดดุลให้เป็นศูนย์ (Zero-Balance Test) - การคุมยอดของระบบ (System Balancing Controls) ประกอบด้วย 1) Inter-Subsystem Totals เช่น เปรียบเทียบยอดรวมที่ได้จากโปรแกรมลูกหนี้รายตัวกับยอดรวมในบัญชีแยกประเภทลูกหนี้ 2) Run-To-Run Totals เช่น นำยอดคงเหลือยกมาในบัญชีลูกหนี้บวกหรือลบกับรายการในช่วงเวลาที่กำหนดจะต้องเท่ากับยอดคงเหลือยกไป (4) การจัดการกับการปัดเศษเลขทศนิยมอย่างถูกต้อง (Rounding) (5) ลดการเข้าแทรกแซงการทำงานของระบบงานของเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์
		6.1.3 การป้องกันการบันทึกข้อมูลทับข้อมูลเดิม	
		6.1.4 การควบคุมการใช้งานข้อมูลในฐานข้อมูลของระบบงาน	
		6.1.5 การควบคุมการจัดการการประมวลผลใหม่	(1) ข้อผิดพลาดที่ตรวจพบก่อนที่จะประมวลผล ทำโดยนำข้อมูลที่มีข้อผิดพลาดไปบันทึกใน Suspense File (2) ข้อผิดพลาดที่ตรวจพบภายหลังการประมวลผลทำโดยล้างรายการที่ผิดพลาดออก

ภาพที่ 8 สรุปผลรวมของการควบคุมการประมวลผล (ต่อ)

6. การควบคุมการประมวลผล (ต่อ)	6.2 ร่องรอยการตรวจสอบของการประมวลผล (ข้อมูลที่แสดงลำดับเหตุการณ์เรียงตามวันและเวลานับตั้งแต่ข้อมูลส่งผ่านไปยังระบบงานเพื่อประมวลผล)	6.2.1 รายงานกิจกรรมการประมวลผล	(1) ข้อมูลการควบคุมด้านการบัญชี ได้แก่ ข้อมูลที่ระบบงานบันทึกระหว่างการประมวลผล ซึ่งช่วยในการตรวจสอบความถูกต้องครบถ้วนของการประมวลผล เช่น ผลลัพธ์ระหว่างทาง ค่าข้อมูลหลักและค่าของข้อมูลนำเข้าและผลลัพธ์ เป็นต้น (2) ข้อมูลการควบคุมด้านการปฏิบัติการ - หลักฐานที่แสดงถึงการใช้ทรัพยากรทางคอมพิวเตอร์ในการประมวลผล เช่น CPU Time เป็นต้น - หลักฐานที่แสดงการเปลี่ยนแปลงรหัสผ่านหรือสิทธิเข้าถึง หรือพยายามใช้ทรัพยากรทางคอมพิวเตอร์ - หลักฐานที่แสดงให้เห็นถึงความล้มเหลวของการทำงานของคอมพิวเตอร์
		6.2.2 รายงานกิจกรรมในแฟ้มข้อมูล	(1) Trailer Record ซึ่งเป็นระเบียนสุดท้ายของเทปที่บอกจุดสิ้นสุดของการบันทึกม้วนเทปนั้น (2) การบันทึกเลขที่อ้างอิงของรายการสุดท้ายที่ผ่าน รายการไปยังแฟ้มข้อมูลหลัก (3) การจัดเก็บยอดของบัญชีก่อนการประมวลผลรายการที่ประมวลผลและยอดของบัญชีหลังการประมวลผล

ภาพที่ 8 สรุปภาพรวมของการควบคุมการประมวลผล (ต่อ)

6.1 การควบคุมความถูกต้องของการประมวลผล

การควบคุมการประมวลผลเพื่อให้เกิดความมั่นใจว่า รหัสคำสั่งงานของระบบงานทำงานถูกต้องและครบถ้วน นอกจากนี้ยังก่อให้เกิดความมั่นใจว่าระบบงานที่นำมาใช้ประมวลผลเป็นรุ่นที่ถูกต้องและมีการใช้แฟ้มข้อมูลที่ถูกต้องมาประมวลผลเช่นกัน นอกจากนี้เพื่อให้แน่ใจว่าสามารถตรวจพบการประมวลผลที่ไม่ได้รับอนุมัติ ไม่น่าเชื่อถือ และไม่เหมาะสมได้ Weber (1999) กล่าวว่าการควบคุมความถูกต้องของการประมวลผลมีดังนี้

6.1.1 การจับคู่รายการที่จะประมวลผลกับรายการที่สัมพันธ์กัน ก่อนการประมวลผลควรสอบทานว่ามีรายการที่สัมพันธ์กับข้อมูลที่จะนำไปประมวลผล เช่น การจ่ายเงินให้ผู้ค้าต้องมีรายการคำสั่งซื้อและการรับสินค้าก่อนการจ่ายเงิน เป็นต้น

6.1.2 การควบคุมข้อผิดพลาดจากการประมวลผล ประกอบด้วย

(1) การสอบทานรายงานการประมวลผล รายงานการประมวลผลเป็นรายงานที่แสดงให้เห็นถึงรหัสและชื่อของระบบงาน วันที่ที่ระบบงานถูกนำมาใช้งาน และรายการที่ระบบงานจัดสร้างให้โดยอัตโนมัติ เช่น รายการจ่ายชำระหนี้ที่ถึงกำหนดชำระเพื่อนำไปจัดพิมพ์เช็คสั่งจ่ายอัตโนมัติ เป็นต้น นอกจากนี้รายงานยังแสดงให้เห็นถึงข้อมูลที่นำมาประมวลผลดังนี้

1) ข้อมูลทั้งหมดที่นำมาประมวลผล ซึ่งอาจจัดเรียงตามประเภทของข้อมูล เลขที่บัญชี และความสัมพันธ์อื่น ๆ เป็นต้น

2) ตารางข้อมูลที่ใช้อ้างอิงในการประมวลผล เช่น ตารางดอกเบี้ย เป็นต้น

3) ข้อมูลที่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ป้อนผ่านทางเครื่องคอนโซล (Console) พร้อมทั้งวันและเวลา

4) ค่าโดยปริยาย (Default) เป็นค่าที่กำหนดไว้เป็นอัตโนมัติโดยไม่ต้องป้อนข้อมูลนำเข้า เพื่อให้ผู้ใช้งานนำไปตรวจสอบความถูกต้องได้ เช่น ถ้าไม่มีการป้อนข้อมูลจำนวนชั่วโมงทำงานของพนักงาน ระบบงานจะถือว่าพนักงานทำงาน 40 ชั่วโมงต่อสัปดาห์ เป็นต้น

(2) การสอบทานเพื่อสืบหาข้อผิดพลาดจากข้อมูลนำเข้า เป็นการสอบทานเพื่อให้มั่นใจว่าระบบงานประมวลผลกับแฟ้มข้อมูลและเรคคอร์ดที่ถูกต้อง การควบคุมทำโดย

1) การตรวจสอบฉลากหรือป้ายแฟ้มข้อมูล (File Label) ของระบบงานโดยตรวจสอบชื่อ วันที่ครบกำหนดอายุการใช้งานและเลขที่ซึ่งกำกับอยู่ภายในแฟ้มข้อมูล ซึ่งส่วนมากจะจัดเก็บไว้ในเรคคอร์ดหัวเรื่อง (Header Record) ของแฟ้มข้อมูลเพื่อให้มั่นใจว่าระบบงานใช้แฟ้มข้อมูลที่ถูกต้องและตรงตามรุ่นที่กำหนดไว้ นอกจากนี้ ยังสามารถตรวจสอบยอดรวมแบตช์ที่คำนวณระหว่างการป้อนข้อมูลซึ่งมักจะอยู่ที่เรคคอร์ดท้าย (Trailer Record) ของแฟ้มข้อมูลเช่นกัน

2) การตรวจสอบลักษณะรายการ (Record Identification) ในการประมวลผลในลักษณะเรียงลำดับ ควรให้โปรแกรมตรวจสอบการเรียงลำดับของข้อมูลก่อนการประมวลผล เพื่อให้มั่นใจว่ารายการที่นำมาประมวลผลต่อไปเป็นรายการที่เรียงลำดับต่อมาจริง เช่น ควรประมวลผลรายการถอนเงินก่อนรายการฝากเงินด้วยเช็คที่ยังไม่ทราบผลการเรียกเก็บ เป็นต้น

3) การตรวจสอบรหัสรายการเปลี่ยนแปลง (Transaction Code) เนื่องจากข้อมูลที่นำมาประมวลผลจะประกอบด้วยรายการที่หลากหลายกันไป เช่น รายการรับหรือเบิกจ่ายสินค้าประจำวัน เป็นต้น ดังนั้นระบบงานควรตรวจสอบรหัสรายการของข้อมูลก่อนจัดส่งข้อมูลเหล่านั้นไปประมวลผลกับโปรแกรมย่อย เพื่อให้มั่นใจว่าโปรแกรมจัดส่งรายการไปยังโปรแกรมย่อยถูกต้อง

4) การตรวจสอบลำดับรายการ (Sequence Test) รายการในแฟ้มข้อมูลและรายการเปลี่ยนแปลงที่นำมาประมวลผลกับแฟ้มข้อมูลหลักแบบแบตช์นั้นควรมีการเรียงลำดับให้เป็นไปในทำนองเดียวกับการเรียงลำดับของข้อมูลในแฟ้มข้อมูลหลัก ถ้ารายการในแฟ้มข้อมูลรายการเปลี่ยนแปลงเรียงลำดับแตกต่างจากแฟ้มข้อมูลหลักจะส่งผลให้การประมวลผลผิดพลาดได้ ดังนั้นระบบงานควรตรวจสอบลำดับของรายการก่อนประมวลผลด้วย

(3) การสอบทานเพื่อสืบหาข้อผิดพลาดจากการประมวลผล ข้อผิดพลาดของการประมวลผลนอกจากจะมาจากข้อมูลผิดพลาดแล้ว ยังอาจมาจากข้อผิดพลาดของระบบงาน หรือซอฟต์แวร์ระบบ หรือฮาร์ดแวร์ก็ได้ การสอบทานเพื่อสืบหาข้อผิดพลาดนี้ประกอบด้วย

1) การตรวจสอบความถูกต้องของการคำนวณ (Arithmetic Accuracy Test) ทำโดย

- คำนวณซ้ำ (Double Arithmetic) เป็นการกำหนดให้โปรแกรมคำนวณค่าซ้ำกันสองครั้งแล้วนำค่าที่คำนวณได้มาเปรียบเทียบว่าตรงกันหรือไม่
- การคำนวณย้อนกลับ (Reverse Multiplication) เป็นการนำผลลัพธ์ที่ได้จากการคำนวณของโปรแกรมมาคำนวณย้อนกลับทางเดิม ต่อจากนั้นนำผลที่ได้ไปเปรียบเทียบกับตัวเลขก่อนการคำนวณ
- การตรวจสอบการล้นของข้อมูล (Overflow) ซึ่งจะเกิดขึ้นในกรณีที่ผลลัพธ์ที่ได้จากการคำนวณของโปรแกรมมีจำนวนตัวเลขมากกว่าขนาดของพื้นที่ที่ใช้ในการจัดเก็บตัวเลข กรณีนี้ควรนำตัวเลขดังกล่าวไปจัดเก็บในพื้นที่แยกต่างหากพร้อมทั้งแสดงข้อผิดพลาด

2) การตรวจสอบว่าผลลัพธ์ที่ได้มีค่าอยู่ในช่วงที่คาดหมาย (Data Reasonableness Test) เป็นการตรวจสอบว่าผลลัพธ์ที่ได้จากการประมวลผลมีค่าอยู่ในช่วงที่คาดหมายไว้หรือไม่ กรณีที่ผลลัพธ์มีค่าแตกต่างจากค่าที่กำหนด โปรแกรมจะพิมพ์รายงานที่แสดงข้อผิดพลาดเพื่อให้ผู้ใช้ติดตามและแก้ไขรายการดังกล่าว

3) การตรวจสอบการจำกัดค่าของข้อมูล (Data Limit Test) เป็นการตรวจสอบว่าผลลัพธ์ที่ได้จากการประมวลผลมีค่าไม่เกินกว่าที่กำหนดไว้ โดยโปรแกรมจะเปรียบเทียบผลลัพธ์กับการจำกัดค่าที่กำหนดไว้

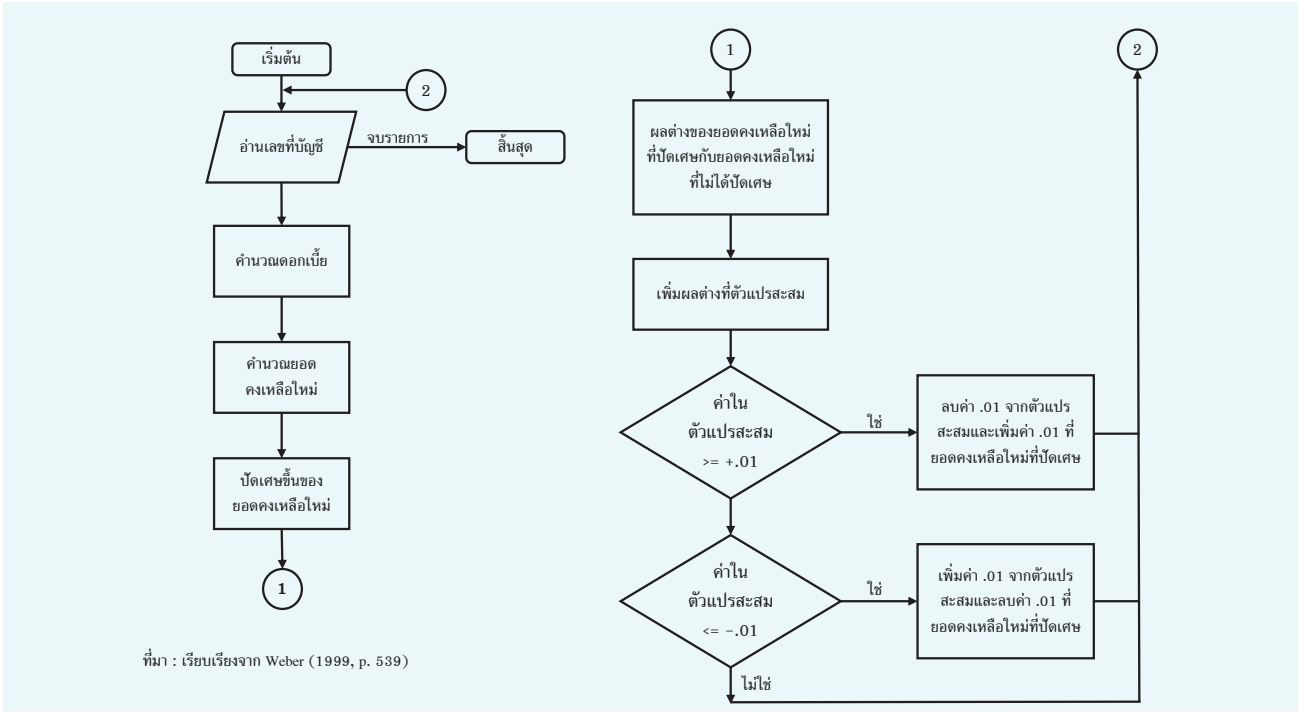
4) การสอบยันตัวเลขระหว่างกัน (Cross-Footing Test) เป็นการนำผลลัพธ์ที่ได้จากการประมวลผลในแต่ละวิธีมาเปรียบเทียบกัน ซึ่งแต่ละวิธีควรให้ผลลัพธ์เหมือนกัน เช่น ยอดรวมเงินเดือนสุทธิบวกภาษีหัก ณ ที่จ่ายควรเท่ากับยอดรวมเงินเดือน เป็นต้น

5) การทดสอบยอดดุลให้เป็นศูนย์ (Zero-Balance Test) ใช้หลักการเช่นเดียวกับการสอบยันตัวเลขระหว่างกัน กล่าวคือยอดในบัญชีเงินเดือนต้องมียอดเป็นศูนย์ภายหลังการจัดสรรเงินเดือนไปยังบัญชีต้นทุนของแผนกต่าง ๆ ในกรณีที่ยอดของบัญชีเงินเดือนมียอดคงเหลือแสดงว่ามีข้อผิดพลาดเกิดขึ้น

6) การคุมยอดของระบบ (System Balancing Controls) เป็นการเปรียบเทียบยอดรวมของข้อมูลที่ส่งเข้ามาประมวลผลกับยอดรวมที่จัดเก็บในเรคคอร์ดท้ายของแฟ้มข้อมูลนำเข้าและแฟ้มข้อมูลหลัก การคุมยอดของระบบประกอบด้วย

- ยอดรวมระหว่างระบบย่อย (Inter-Subsystem Totals) เป็นการเปรียบเทียบยอดรวมที่ได้จากการประมวลผลของโปรแกรมหนึ่งกับอีกโปรแกรมหนึ่งที่ทำหน้าที่คล้ายคลึงกัน เช่น การเปรียบเทียบยอดรวมที่ได้จากโปรแกรมลูกหนี้รายตัวกับยอดรวมในบัญชีแยกประเภทลูกหนี้ เป็นต้น
- ยอดรวมของระบบหนึ่งกับอีกระบบหนึ่ง (Run-To-Run Totals) การสอบทานการคุมยอดนี้เกิดจากการนำผลลัพธ์ที่ได้จากการประมวลผลของโปรแกรมแรกไปประมวลผลต่อกับข้อมูลนำเข้าของอีกโปรแกรมหนึ่งแล้วจึงนำผลลัพธ์ที่ได้มาตรวจสอบว่าโปรแกรมทำงานถูกต้องหรือไม่ โดยเปรียบเทียบกับผลลัพธ์ของอีกโปรแกรม ตัวอย่างเช่น การนำยอดคงเหลือยกมาในบัญชีลูกหนี้ บวกหรือลบกับรายการในช่วงเวลาที่กำหนด จะต้องเท่ากับยอดคงเหลือยกไป เป็นต้น

(4) การจัดการกับการปัดเศษเลขทศนิยมอย่างถูกต้อง (Rounding) การปัดเศษเลขทศนิยมเกิดจากผลลัพธ์ที่ได้จากการคำนวณมีจำนวนเลขทศนิยมมากกว่าที่ต้องการจัดเก็บ เช่น เลขทศนิยมที่ได้จากการคำนวณดอกเบี้ยเป็น 5 เลขทศนิยม ในขณะที่ต้องการจัดเก็บเพียง 2 เลขทศนิยม ถ้ามีการตัดเลขทศนิยม 3 ตัวหลังจะส่งผลให้ยอดรวมของดอกเบี้ยที่จัดเก็บในบัญชีเงินฝากมีจำนวนน้อยกว่ายอดรวมดอกเบี้ยทั้งหมดที่ได้จากการคำนวณ เป็นต้น การจัดการกับปัญหาดังกล่าวทำโดยกำหนดขั้นตอนการคำนวณเพื่อปัดเศษบางบัญชีขึ้นและปัดเศษบางบัญชีลง (ดังภาพที่ 9) ซึ่งวิธีการนี้จะทำให้ยอดรวมของดอกเบี้ยที่จัดเก็บในบัญชีเงินฝากเท่ากับยอดรวมดอกเบี้ยทั้งหมดที่ได้จากการคำนวณ ในการจัดการกับการปัดเศษดังกล่าวอาจก่อให้เกิดการทุจริตได้ กล่าวคือ โปรแกรมเมอร์จะโอนผลต่างของเลขทศนิยมเข้าบัญชีของตนเอง แม้ว่าค่าของเลขทศนิยมจะน้อยแต่ถ้ามีบัญชีเงินฝากจำนวนมากอาจจะส่งผลให้ยอดรวมของเลขทศนิยมที่เป็นผลต่างนี้มีจำนวนมากเช่นกัน



ที่มา: เรียบเรียงจาก Weber (1999, p. 539)

ภาพที่ 9 การจัดการกับการปัดเศษ

(5) ลดการเข้าแทรกแซงการทำงานของระบบงานของเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ ตามปกติโปรแกรมมักต้องการให้คนกำหนดพารามิเตอร์หรือค่าตัวแปร (Parameter) เพื่อกำหนดขั้นตอนการประมวลผล เช่น เป็นรายเดือนหรือรายสามเดือน เป็นต้น และเนื่องจากการกำหนดค่าพารามิเตอร์มีโอกาสผิดพลาดได้ง่าย ดังนั้น ระบบงานที่ดีควรลดการแทรกแซงการทำงานของโปรแกรมให้มากที่สุดเท่าที่จะมากได้ ในกรณีที่ไม่สามารถหลีกเลี่ยงการแทรกแซงการทำงานของระบบงานโดยคน ก็ควรกำหนดขั้นตอนการทำงานให้ชัดเจน

6.1.3 การป้องกันการบันทึกข้อมูลทับข้อมูลเดิม เป็นการป้องกันการลบข้อมูลเดิมและแทนที่ด้วยข้อมูลใหม่ในแฟ้มข้อมูลที่จัดเก็บไว้ในสื่อบันทึก เพื่อให้มั่นใจว่าไม่มีผู้ใดสามารถลบหรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตได้

6.1.4 การควบคุมการใช้งานข้อมูลในฐานข้อมูลของระบบงาน ประกอบด้วย การปรับปรุงข้อมูลในฐานข้อมูล และการออกรายงาน

6.1.5 การควบคุมการจัดการการประมวลผลใหม่ในกรณีที่พบความผิดพลาดและต้องประมวลผลใหม่ สามารถแบ่งการควบคุมได้ดังนี้

(1) ข้อผิดพลาดที่ตรวจพบก่อนที่จะประมวลผล ข้อผิดพลาดประเภทนี้มักตรวจพบในขั้นตอนการตรวจสอบความสมเหตุสมผลของข้อมูล ซึ่งการจัดการกับข้อผิดพลาดสามารถทำโดย นำข้อมูลที่มีข้อผิดพลาดไปบันทึกในแฟ้มพักข้อมูล (Suspense File) เมื่อแก้ไขข้อผิดพลาดเรียบร้อยแล้วจะนำข้อมูลดังกล่าวไปประมวลผลต่อไป ปกติรายการที่บันทึกในแฟ้มพักข้อมูลมักกำกับหมายเลขที่เรียงลำดับไว้ด้วย ทำให้สามารถอ้างอิงเลขที่ดังกล่าวเมื่อแก้ไขข้อมูล โดยปกติมักจะจัดทำรายงานที่เกี่ยวกับรายการที่ผิดพลาดให้กับผู้ใช้ และผู้ใช้จะแก้ไขข้อผิดพลาดลงในรายงานแล้วจึงนำส่งรายงานกลับมายังศูนย์คอมพิวเตอร์เพื่อประมวลผลต่อไป

(2) ข้อผิดพลาดที่ตรวจพบภายหลังการประมวลผล ข้อผิดพลาดประเภทนี้มักตรวจพบจากการตรวจทานรายงานประมวลผลหรือกระทบยอดคุม เนื่องจากข้อผิดพลาดลักษณะนี้มักพบภายหลังที่มีการปรับปรุงข้อมูลในแฟ้มข้อมูลหลักแล้ว ดังนั้นการแก้ไขข้อผิดพลาดจะทำโดยล้างรายการที่ผิดพลาดออกและป้อนรายการที่ถูกต้องกลับเข้าไปใหม่ ในการตรวจหาข้อผิดพลาดนอกจากจะตรวจทานจากรายงานประมวลผลแล้วยังตรวจทานจากบันทึกข้อผิดพลาดได้เช่นกัน

นอกจากนี้ยังครอบคลุมถึงแผนฟื้นฟูระบบจากภัยพิบัติ (Disaster Recovery Plan) เพื่อให้ระบบงานอยู่ในสภาพพร้อมใช้งาน (Availability) ด้วย (รายละเอียดสามารถศึกษาได้จากบทที่เกี่ยวข้อง)

6.2 ร่องรอยการตรวจสอบของการประมวลผล

ร่องรอยการตรวจสอบของการประมวลผล คือ ข้อมูลที่แสดงลำดับเหตุการณ์เรียงตามวันและเวลานับตั้งแต่ข้อมูลถูกส่งผ่านไปยังระบบงานเพื่อประมวลผล จนกระทั่งผลลัพธ์ที่ได้จากการประมวลผลถูกจัดส่งไปยังฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ หรือเครื่องพิมพ์ปกติระบบงานโดยทั่วไปจะมีรายงานที่เกี่ยวกับรายงานกิจกรรมการประมวลผล (Processing Activity Output) และ รายงานกิจกรรมในแฟ้มข้อมูล (File Activity Data) ดังมีรายละเอียดดังนี้

6.2.1 รายงานกิจกรรมการประมวลผล เป็นเอกสารที่แสดงให้เห็นถึงขั้นตอนการทำงานของระบบงานที่ทำให้สามารถปฏิบัติตามขั้นตอนการประมวลผลของโปรแกรม เพื่อทำความเข้าใจการทำงานของระบบงานได้ ระบบงานที่ซับซ้อนบางโปรแกรมอาจบันทึกผลลัพธ์ซึ่งประกอบด้วยข้อมูลที่แสดงให้เห็นถึงการควบคุมด้านการบัญชีและด้านการปฏิบัติการดังนี้

(1) ข้อมูลการควบคุมด้านการบัญชี เป็นข้อมูลที่ระบบงานบันทึกระหว่างการประมวลผลซึ่งช่วยในการตรวจสอบความถูกต้องครบถ้วนของการประมวลผลได้ ประกอบด้วย (1) ผลลัพธ์ระหว่างทาง (2) ค่าข้อมูลหลัก และ (3) ค่าของข้อมูลนำเข้าและผลลัพธ์

(2) ข้อมูลการควบคุมด้านการปฏิบัติการ ประกอบด้วย

1) หลักฐานที่แสดงให้เห็นถึงการใช้ทรัพยากรทางคอมพิวเตอร์ในการประมวลผล เช่น ระยะเวลาที่โปรแกรมใช้งานหน่วยประมวลผลกลาง (Central Processing Unit) จำนวนพื้นที่ในหน่วยความจำที่ใช้ในการประมวลผล อุปกรณ์สื่อสารที่ใช้ในการประมวลผล ซอฟต์แวร์ระบบที่ใช้ การเข้าถึงแฟ้มข้อมูล ความถี่ในการเข้าถึงข้อมูล จำนวนข้อมูลสำรองที่จัดทำ และจำนวนครั้งที่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์เข้าไปแทรกแซงการทำงานของระบบงาน เช่น นำเทปหรือดิสก์ไปบรรจุในเครื่องอ่านเทปหรือดิสก์เพื่อให้ระบบงานประมวลผลต่อไป เป็นต้น ซึ่งสามารถใช้หลักฐานดังกล่าวเพื่อประเมินการทำงานของโปรแกรมว่ามีประสิทธิภาพหรือไม่ ถ้าระบบงานใช้เวลาในการประมวลผลนานกว่าปกติอาจมีสาเหตุมาจากคำสั่งงานของโปรแกรมบางส่วนมีปัญหาต้องปรับปรุงแก้ไข เป็นต้น นอกจากนี้การตรวจสอบการใช้ทรัพยากรทางคอมพิวเตอร์ในการประมวลผลอาจแสดงให้เห็นถึงสิ่งผิดปกติในการประมวลผลได้ เช่น จำนวนครั้งในการสั่งให้ระบบงานประมวลผลรายการเช็คสั่งจ่ายมากผิดปกติ และพนักงานที่ไม่มีหน้าที่ที่เกี่ยวข้องสั่งประมวลผลโปรแกรมพิมพ์เช็คสั่งจ่าย เป็นต้น

2) หลักฐานที่แสดงให้เห็นถึงการเปลี่ยนแปลงรหัสผ่านหรือสิทธิ์เข้าถึงแฟ้มข้อมูลหรือความพยายามใช้ทรัพยากรทางคอมพิวเตอร์ที่ล้มเหลว หลักฐานดังกล่าวสามารถดึงข้อมูลมาจากแฟ้มลงบันทึก (Log) ที่คอมพิวเตอร์บันทึกไว้เมื่อมีผู้เข้ามาใช้งานระบบงาน

3) หลักฐานที่แสดงให้เห็นถึงความล้มเหลวของการทำงานของคอมพิวเตอร์ เช่น หน่วยประมวลผลและหน่วยความจำทำงานผิดพลาด เป็นต้น โดยข้อมูลนี้สามารถดึงมาจากแฟ้มลงบันทึกเช่นเดียวกับหลักฐานอื่น ๆ ที่กล่าวมาในข้างต้น ข้อผิดพลาดที่เกิดขึ้นนี้อาจแสดงให้เห็นว่าถึงเวลาต้องเปลี่ยนเครื่องคอมพิวเตอร์แล้วก็ได้

6.2.2 รายงานกิจกรรมในแฟ้มข้อมูล เป็นรายงานที่แสดงรายละเอียดรายการเปลี่ยนแปลงที่ประมวลผล (Transaction Listings) เนื่องจากรายงานกิจกรรมในแฟ้มข้อมูลอาจไม่เพียงพอที่จะใช้ติดตามการประมวลผลของระบบงานที่มีความซับซ้อน จึงจำเป็นต้องมีข้อมูลเสริม (Supplementary) ในแฟ้มข้อมูลหลักเพื่อใช้ในการติดตามการประมวลผลโดยเฉพาะ ข้อมูลเสริมที่แสดงให้เห็นถึงการควบคุมด้านการบัญชีมีดังนี้

(1) เรคคอร์ดท้าย (Trailer Record) เป็นการบันทึกไว้ตอนท้ายของแฟ้มข้อมูลหลักของแต่ละรายการเปลี่ยนแปลงที่ผ่านไปยังบัญชีแยกประเภทแล้ว โดยเรคคอร์ดท้ายนี้มีข้อมูลที่เกี่ยวกับยอดเงินด้านเดบิตหรือเครดิต วันที่ เลขที่ของเอกสารต้นฉบับ การรวมรายการดังกล่าวไว้ในที่เดียวกันทำให้ง่ายต่อการติดตามการประมวลผลรายการ แต่ถ้าจำนวนรายการมีจำนวนมาก วิธีการนี้จะส่งผลให้มีเรคคอร์ดท้ายเป็นจำนวนมากตามไปด้วย ซึ่งจะต้องใช้พื้นที่ในการจัดเก็บข้อมูลและเสียเวลาในการบันทึกรายการเช่นกัน

(2) การบันทึกเลขที่อ้างอิงของรายการสุดท้ายที่ผ่านรายการไปยังแฟ้มข้อมูลหลัก ทำให้สามารถใช้เลขที่อ้างอิงดังกล่าวในการติดตามรายการด้วยมือต่อไป แต่หากมีรายการเปลี่ยนแปลงที่ประมวลผลเป็นจำนวนมากจะทำให้เสียเวลาอย่างมากด้วยเช่นกัน

(3) การป้อนข้อมูลก่อนและหลังการประมวลผลในบัญชีแยกประเภทของแฟ้มข้อมูลหลัก กล่าวคือ มีการจัดเก็บยอดของบัญชีก่อนการประมวลผล รายการที่ประมวลผล และยอดของบัญชีหลังการประมวลผล เช่น รายการเงินเดือนของพนักงานจะปรากฏยอดยกมาตามด้วยรายละเอียดของรายการที่ประมวลผลและยอดยกไป เป็นต้น

นอกจากหลักฐานข้างต้นแล้ว บางระบบงานอาจกำหนดให้มีการป้อนข้อมูลคุม (Control Data) ที่เกี่ยวกับยอดรวมข้อมูลทางการเงินในแฟ้มข้อมูลหลัก ยอดรวมของจำนวนรายการที่ประมวลผล จำนวนรายการที่ประมวลผล และคำสั่งสุดท้ายที่ประมวลผลเป็นระยะ ๆ ในกรณีที่มีปัญหาในการประมวลผล จะทำให้สามารถนำข้อมูลคุมมาตรวจสอบเพื่อค้นหาว่า ณ จุดใดที่การประมวลผลมีข้อผิดพลาดขึ้นและไม่ต้องประมวลผลรายการใหม่ทั้งหมด

7. การควบคุมผลลัพธ์

การที่ข้อมูลนำเข้าและประมวลผลสามารถอยู่ในรูปแบบแบตช์และออนไลน์ ดังนั้นผลลัพธ์จากการประมวลผลจึงสามารถเป็นได้ทั้งแบบแบตช์และออนไลน์เช่นกัน โดยผลลัพธ์แบบแบตช์ คือ ผลลัพธ์ที่จัดทำขึ้นในช่วงเวลาที่กำหนดไว้ และกระจายไปยังผู้ใช้ต่อไป ผลลัพธ์แบบแบตช์มักอยู่ในรูปของรายงานที่จัดพิมพ์บนกระดาษ หรือรายงานที่จัดเก็บในสื่อบันทึกต่าง ๆ ที่จัดส่งไปยังผู้ใช้งาน ส่วนผลลัพธ์แบบออนไลน์ส่วนใหญ่จะเป็นผลลัพธ์ที่กระจายไปยังผู้ใช้ผ่านทางระบบเครือข่ายคอมพิวเตอร์ โดยการแสดงที่หน้าจอคอมพิวเตอร์ของผู้ใช้ จากรูปแบบของผลลัพธ์ดังกล่าว ทำให้การควบคุมผลลัพธ์ทั้งแบบแบตช์และแบบออนไลน์มีการควบคุมที่เหมือนและแตกต่างกันบางประการ ซึ่งจะได้กล่าวต่อไป

วัตถุประสงค์หลักของการควบคุมผลลัพธ์เพื่อให้แน่ใจว่าผลลัพธ์จากการประมวลผลได้จัดส่งหรือแสดงให้ผู้ที่ได้รับอนุมัติเท่านั้น ถ้าผลลัพธ์ถูกจัดส่งหรือแสดงให้ผู้ที่ไม่เกี่ยวข้องทราบจะส่งผลให้การแบ่งแยกหน้าที่งานไม่มีประสิทธิผลทางด้านการควบคุม ภาพที่ 10 แสดงสรุปภาพรวมของการควบคุมผลลัพธ์ ดังนี้

7. การควบคุมผลลัพธ์	7.1 การควบคุมความถูกต้องครบถ้วนของผลลัพธ์ทั่วไป	7.1.1 การกำหนดขั้นตอนในการกระจายผลลัพธ์ เช่น ชื่อผู้รับ ตารางเวลาส่งมอบ และใบเซ็นรับรายงาน เป็นต้น
		7.1.2 การควบคุมการแสดงผลลัพธ์ทางหน้าจอ เช่น การควบคุมการเข้าถึงคอมพิวเตอร์ทางกายภาพ และการเข้าถึงผลลัพธ์ด้วยรหัสผ่าน เป็นต้น
		7.1.3 การควบคุมผลลัพธ์ที่ไม่ถูกต้องครบถ้วน - กำหนดการปฏิบัติงานของพนักงานรับส่งข้อมูล - กำหนดการปฏิบัติงานของผู้ใช้
		7.1.4 การควบคุมการแก้ไขข้อผิดพลาดกับผลลัพธ์ เช่น ปฏิบัติตามกฎเกณฑ์ที่เขียนในคู่มือการปฏิบัติงาน เป็นต้น

ภาพที่ 10 สรุปภาพรวมของการควบคุมผลลัพธ์

7. การควบคุมผลลัพธ์ (ต่อ)	7.2 การควบคุมผลลัพธ์แบบแบตช์	7.2.1 การควบคุมการจัดเก็บแบบฟอร์มเปล่า เช่น เก็บรักษาตรายางลายเซ็น และแบบฟอร์มเปล่าแยกต่างหากจากกัน เป็นต้น
		7.2.2 การควบคุมการใช้โปรแกรมคำสั่งเพื่อพิมพ์รายงาน เช่น กำหนดให้เฉพาะผู้มีอำนาจสามารถใช้โปรแกรมเพื่อพิมพ์รายงานและ Checkpoint/Restart เป็นต้น
		7.2.3 การควบคุมลำดับการจัดพิมพ์รายงาน เช่น ไม่สามารถแก้ไขหรือทำสำเนารายงานที่รอพิมพ์ที่เครื่องพิมพ์ (Spool File) เป็นต้น
		7.2.4 การควบคุมการพิมพ์ เช่น ลืมเปลี่ยนเครื่องพิมพ์, Impact Printer, ตรวจนับจำนวนแบบฟอร์มที่นำมาใช้ในการจัดพิมพ์ เป็นต้น
		7.2.5 การควบคุมการรวบรวมรายงาน เช่น บันทึกวันและเวลาที่รวบรวมรายงานแต่ละรายงาน และชื่อผู้ที่มารับรายงาน เป็นต้น
		7.2.6 การตรวจทานความถูกต้องของรายงานเบื้องต้น
		7.2.7 การควบคุมการกระจายรายงาน เช่น บันทึกวันและเวลาในการกระจายรายงาน เป็นต้น
		7.2.8 การควบคุมรายงานของผู้ใช้
		7.2.9 การควบคุมการจัดเก็บรายงาน
		7.2.10 การกำหนดระยะเวลาในการจัดเก็บรายงาน
		7.2.11 การทำลายรายงาน

ภาพที่ 10 สรุปภาพรวมของการควบคุมผลลัพธ์ (ต่อ)

7. การควบคุมผลลัพธ์ (ต่อ)	7.3 การควบคุมผลลัพธ์แบบออนไลน์	7.3.1 การควบคุมแหล่งกำเนิดของรายงาน เช่น กรณีที่เข้าถึงรายงานผ่านเว็บบราวเซอร์ ต้องแน่ใจว่ารายงานนั้นเป็นรายงานที่ได้รับอนุมัติ เป็นต้น
		7.3.2 การควบคุมการกระจายรายงาน เช่น กระจายรายงานไปยังผู้รับในเวลาที่เหมาะสมและครบถ้วน เป็นต้น
		7.3.3 การควบคุมการสื่อสาร เช่น เข้ารหัสข้อมูลที่ส่งผ่านระบบเครือข่าย เป็นต้น
		7.3.4 การควบคุมการรับรายงาน เช่น กำหนดให้ตรวจสอบว่ารายงานที่ส่งมาเป็น file ไม่มีไวรัส เป็นต้น
		7.3.5 การควบคุมการตรวจทาน เช่น กำหนดให้มีระบบตอบกลับอัตโนมัติเพื่อแจ้งให้ผู้ส่งรายงานทราบว่ารายงานที่จัดส่งนั้นยังไม่ได้เปิด เป็นต้น
		7.3.6 การควบคุมการจัดการ เช่น การกำหนดว่าพนักงานที่ได้รับรายงานจะต้องส่งต่อรายงานหรือจัดทำสำเนาให้กับส่วนงานใดบ้าง เป็นต้น
		7.3.7 การควบคุมการเก็บรักษา
		7.3.8 การควบคุมการลบทิ้ง
	7.4 ร่องรอยการตรวจสอบของผลลัพธ์ (ข้อมูลที่แสดงลำดับเหตุการณ์เรียงตามวันและเวลานับตั้งแต่ได้ผลลัพธ์จนกระทั่งผู้ใช้ทำลายผลลัพธ์)	- ร่องรอยการควบคุมด้านการบัญชี เช่น วันเวลาที่ได้รับรายงาน และระยะเวลาในการจัดเก็บ เป็นต้น - ร่องรอยการควบคุมด้านการปฏิบัติการ เช่น จำนวนรายงานที่พิมพ์ และเวลาที่ใช้ในการพิมพ์ เป็นต้น

ภาพที่ 10 สรุปภาพรวมของการควบคุมผลลัพธ์ (ต่อ)

7.1 การควบคุมความถูกต้องครบถ้วนของผลลัพธ์ทั่วไป

การควบคุมนี้เป็นการควบคุมซึ่งต้องกำหนดไว้ไม่ว่าผลลัพธ์จะแสดงในรูปแบบใดก็ตามการควบคุม ประกอบด้วย

7.1.1 การกำหนดขั้นตอนในการกระจายผลลัพธ์ ปกติขั้นตอนในการกระจายผลลัพธ์มักกำหนดไว้ในคู่มือการปฏิบัติงานของแต่ละระบบงาน เพื่อให้แน่ใจว่าผลลัพธ์จากการประมวลผลถูกจัดส่งไปยังผู้มีหน้าที่เกี่ยวข้องเท่านั้น โดยมีพนักงานรับส่งข้อมูลของศูนย์คอมพิวเตอร์เป็นผู้ทำหน้าที่กระจายผลลัพธ์ สำหรับการควบคุมการกระจายผลลัพธ์ ประกอบด้วย

- กำหนดรายชื่อผู้รับ (Distribution Checklist) โดยมีข้อมูลเกี่ยวกับ ชื่อรายงาน และชื่อผู้มีสิทธิ์ได้รับรายงาน เพื่อให้รายงานส่งถึงมือบุคคลที่เกี่ยวข้องเท่านั้น
- กำหนดตารางเวลาส่งมอบ (Distribution Schedule) ซึ่งประกอบด้วย ความถี่ของการจัดเตรียมรายงานและการแจกจ่ายรายงาน เพื่อให้มั่นใจว่ามีการจัดส่งรายงานไปถึงผู้รับทันเวลา
- ใบนำส่งผลลัพธ์ (Transmittal Sheets) เป็นใบที่แนบติดกับสำเนารายงาน โดยใบนำส่งดังกล่าวแสดงให้เห็นถึงชื่อรายงาน ชื่อผู้รับรายงานและหน่วยงานพร้อมทั้งที่อยู่

- รายงานการกระจายผลลัพธ์ (Distribution Log) เป็นรายงานที่จัดทำขึ้นเพื่อแสดงว่ามีการจัดส่งรายงานอะไรไปให้ใครที่ส่วนงานไหน และจัดส่งรายงานแต่ละรายงานเมื่อไร
- ใบเซ็นรับรายงาน (Report Release Forms) เป็นเอกสารที่ผู้รับรายงานลงนามเพื่อแสดงให้เห็นถึงการรับรายงาน นอกจากนี้ยังเป็นการเตือนให้ผู้รับรายงานทราบว่า รายงานดังกล่าวอยู่ในความรับผิดชอบของผู้รับซึ่งต้องจัดเก็บรายงานไว้ในที่ปลอดภัย

7.1.2 การควบคุมการแสดงผลลัพธ์ทางหน้าจอ เป็นการควบคุมเพื่อให้ผู้ที่ไม่เกี่ยวข้องไม่สามารถอ่านข้อมูลจากหน้าจอคอมพิวเตอร์ได้ การควบคุมทำโดยควบคุมการเข้าถึงคอมพิวเตอร์ทั้งทางด้านกายภาพ และการควบคุมการเข้าถึงผลลัพธ์ที่เป็นรายงานโดยการใช้รหัสผ่าน

7.1.3 การควบคุมการค้นพบผลลัพธ์ที่ไม่ถูกต้องครบถ้วน การค้นหาข้อผิดพลาดของผลลัพธ์เป็นหน้าที่ร่วมกันของทั้งพนักงานรับส่งข้อมูลและผู้ใช้ การควบคุมมีดังนี้

(1) กำหนดการปฏิบัติงานของพนักงานรับส่งข้อมูล ดังนี้

- ตรวจสอบรายงานกิจกรรมการประมวลผล (Processing Activity Output) และยอดรวม (Control Totals) เพื่อดูว่ารายงานถูกต้องครบถ้วน
- ตรวจสอบรายการในลงบันทึกรายการเปลี่ยนแปลงที่ได้รับการประมวลผล (Processing Transaction Log) กับบันทึกรายการข้อมูลนำเข้า เพื่อให้แน่ใจว่าข้อมูลนำเข้าทั้งหมดได้รับการประมวลผล
- กระทบยอดรวมของรายการที่ประมวลผลกับยอดรวมของรายการที่ส่งเข้าประมวลผลก่อนจัดส่งรายการไปยังผู้ใช้ เพื่อให้แน่ใจว่ารายการที่ผู้ใช้ส่งเข้าประมวลผลได้รับการประมวลผลครบถ้วน
- สอบยันรายงานการกระจายผลลัพธ์ (Distribution Log) กับรายชื่อการกระจายผลลัพธ์ (Distribution Checklist) เพื่อให้แน่ใจว่ารายงานได้กระจายไปยังผู้ที่ได้รับอนุมัติเท่านั้น

(2) กำหนดการปฏิบัติงานของผู้ใช้ ดังนี้

- สอบทานรายละเอียดในใบนำส่งผลลัพธ์กับรายงานที่ได้รับว่าถูกต้องตรงกันหรือไม่
- สอบทานว่าได้รับรายงานทั้งหมดตามกำหนดในตารางเวลาการกระจายผลลัพธ์
- สอบทานรายการที่ได้รับการประมวลผลกับเอกสารต้นฉบับ เพื่อให้แน่ใจว่าข้อมูลในเอกสารต้นฉบับทุกรายการได้รับการประมวลผล
- สอบทานรายการที่เครื่องคอมพิวเตอร์สร้างขึ้นจากการประมวลผล เพื่อให้แน่ใจว่ารายการนั้นอยู่ในรูปแบบและได้รับอนุมัติตามที่องค์กรกำหนด
- สอบทานตารางการเปลี่ยนแปลงแฟ้มข้อมูลหลัก รวมถึงการปรับปรุงเปลี่ยนแปลงแฟ้มข้อมูล เพื่อให้แน่ใจว่าการเปลี่ยนแปลงมีเหตุผลและเหมาะสม นอกจากนี้ผู้ใช้ควรกระทบยอดรายงาน ดังนี้
  1) กระทบยอดรวมแบตช์ที่คอมพิวเตอร์คำนวณกับยอดรวมแบตช์ที่คำนวณด้วยมือก่อนการจัดส่งรายการในเอกสารต้นฉบับไปประมวลผล
  2) กระทบยอดรวมของยอดคงเหลือจากแฟ้มข้อมูลรายละเอียดกับยอดคงเหลือในแฟ้มข้อมูลหลัก เช่น ยอดรวมของบัญชีย่อยกับยอดในบัญชีแยกประเภท เป็นต้น
  3) กระทบยอดรวมที่คอมพิวเตอร์คำนวณกับยอดที่ได้จากการตรวจนับทางกายภาพ เช่น ยอดการตรวจนับเงินสดและสินค้าคงเหลือ เป็นต้น
  4) ในกรณีที่ไม่มีการตรวจนับทางกายภาพ สามารถนำยอดจากแหล่งข้อมูลอื่นมากระทบยอดกับยอดรวมที่คอมพิวเตอร์คำนวณให้ เช่น คำนวณหาต้นทุนสินค้าจากกำไรขั้นต้นขององค์กร ถ้ายอดที่คอมพิวเตอร์คำนวณอยู่ในช่วงที่ประมาณการไว้ก็ถือว่า ค่าดังกล่าวยอมรับได้ เป็นต้น

5) สุ่มตรวจทานว่ารายการที่ประมวลผลเป็นรายการที่ได้รับอนุมัติและมีเหตุผลเป็นระยะ ๆ โดยสุ่มรายการที่ได้รับการประมวลผลกับเอกสารต้นฉบับ

นอกจากนี้ผู้ใช้ควรเก็บรักษารายงานไว้ในที่ปลอดภัยและทำลายรายงานเมื่อถึงเวลาที่กำหนดไว้

7.1.4 การควบคุมการแก้ไขข้อผิดพลาดกับผลลัพธ์ การควบคุมทำโดยกำหนดขั้นตอนการแก้ไขข้อผิดพลาดและการนำส่งข้อมูลเพื่อประมวลผล ดังนี้

- กรณีที่ข้อผิดพลาดเกิดจากการประมวลผล ข้อผิดพลาดที่เกิดขึ้นจะถูกจัดส่งไปยังพนักงานรับส่งข้อมูล แต่ถ้าข้อผิดพลาดเกิดจากเอกสารต้นฉบับ ข้อผิดพลาดดังกล่าวจะถูกจัดส่งไปยังหน่วยงานของผู้ใช้เพื่อแก้ไขต่อไป ทั้งนี้ควรจัดทำรายงานอธิบายสาเหตุของข้อผิดพลาดพร้อมทั้งขั้นตอนในการแก้ไขด้วย
- การแก้ไขข้อผิดพลาดและการนำส่งข้อมูลเข้าประมวลผลควรปฏิบัติตามกฎเกณฑ์ที่เขียนในคู่มือการปฏิบัติงาน
- บันทึกข้อผิดพลาดที่เกิดขึ้นควรได้รับการสอบทานจากพนักงานรับส่งข้อมูลและหน่วยงานผู้ใช้ นอกจากนี้ควรตรวจทานบันทึกดังกล่าวเป็นระยะ ๆ เพื่อให้แน่ใจว่าข้อผิดพลาดที่เกิดขึ้นได้รับการแก้ไขภายในระยะเวลาที่เหมาะสม กรณีที่รายการใดได้รับการแก้ไขแล้วควรขีดฆ่ารายการนั้นออก
- กรณีของรายการที่ยังไม่ได้รับการแก้ไข ควรจัดเรียงอายุของรายงาน (Aging Report) เพื่อติดตามรายการที่ยังไม่ได้รับการแก้ไข รายการที่แก้ไขจะต้องผ่านขั้นตอนการควบคุมข้อมูลนำเข้า การควบคุมการประมวลผล จนถึงการควบคุมผลลัพธ์เช่นเดียวกับการควบคุมการจัดส่งเอกสารต้นฉบับครั้งแรก

7.2 การควบคุมผลลัพธ์แบบแบตช์

ผลลัพธ์แบบแบตช์ เป็นรายงานที่จัดทำขึ้นและมีการกระจายไปยังผู้ใช้ รายงานนี้อาจอยู่ในลักษณะของรายงานที่เป็นกระดาษ ซีดีรอม และเทป วัตถุประสงค์ของการควบคุมการผลิตและการกระจายผลลัพธ์แบบแบตช์เพื่อให้แน่ใจว่ารายงานถูกต้อง ครบถ้วนและได้จัดส่งไปยังผู้รับที่มีสิทธิ์ได้รับรายงานนั้นตามเวลาที่กำหนด การควบคุมผลลัพธ์แบบแบตช์ขึ้นอยู่กับขั้นตอนในการจัดทำรายงาน กล่าวคือ รายงานที่ถูกพิมพ์ที่เครื่องพิมพ์โดยตรงนั้นไม่จำเป็นต้องมีการควบคุมลำดับการจัดพิมพ์ (Queued or Spooled) การควบคุมในแต่ละขั้นตอนควรคำนึงถึงค่าใช้จ่ายและผลประโยชน์ด้วย การควบคุมในแต่ละขั้นตอนประกอบด้วย

7.2.1 การควบคุมการจัดเก็บแบบฟอร์มเปล่า ในการจัดทำรายงานในรูปของกระดาษพิมพ์และเอกสารสัญญานั้นจำเป็นต้องพิมพ์ข้อมูลลงในแบบฟอร์มเปล่า ซึ่งมักจะมีสัญลักษณ์ ที่อยู่ และหมายเลขโทรศัพท์ของกิจการ ตัวอย่างของแบบฟอร์มเปล่าที่มักมีการจัดพิมพ์เป็นการล่วงหน้า คือ เช็ค เมื่อมีการนำแบบฟอร์มเปล่ามาใช้ในการจัดพิมพ์รายงาน กิจการต้องควบคุมแบบฟอร์มเปล่าให้เหมาะสม ดังนี้

- กำหนดให้บริษัทที่จัดพิมพ์แบบฟอร์มเปล่า จัดพิมพ์แบบฟอร์มให้กับกิจการเมื่อได้รับคำสั่งจากผู้มีอำนาจเท่านั้น นอกจากนี้แบบฟอร์มเปล่าจะต้องจัดส่งไปยังผู้ที่รับมอบอำนาจเท่านั้นเช่นกัน
- มีระบบจัดการกับแบบฟอร์มเปล่าเช่นเดียวกับการจัดการสินค้าคงเหลือ
- จัดเก็บแบบฟอร์มเปล่าในที่ที่ปลอดภัย
- กำหนดหมายเลขเรียงลำดับให้กับแบบฟอร์มเปล่า
- เก็บรักษาตรายางลายเซ็นและแบบฟอร์มเปล่าแยกต่างหากจากกัน

7.2.2 การควบคุมการใช้โปรแกรมคำสั่งเพื่อพิมพ์รายงาน การควบคุมการใช้โปรแกรมดังกล่าว มีดังนี้

- กำหนดให้เฉพาะผู้มีอำนาจสามารถใช้โปรแกรมคำสั่งเพื่อพิมพ์รายงาน โดยเฉพาะรายงานที่มีความสำคัญ เช่น การพิมพ์เช็คหรือรหัสประจำตัว (Personal Identification Number หรือ PIN) เป็นต้น
- กำหนดสิทธิ์ให้กับผู้มีอำนาจในการจัดพิมพ์รายงานให้เหมาะสม เช่น กำหนดจำนวนสำเนาที่ผู้มีอำนาจสามารถจัดพิมพ์ได้ในแต่ละวันหรือแต่ละเดือน เป็นต้น
- ควบคุมการใช้งานจุดตรวจสอบหรือจุดเริ่มทำต่อ (Checkpoint/Restart) ปกติโปรแกรมที่จัดพิมพ์รายงานจำนวนมาก

มักมีการกำหนดจุดตรวจสอบหรือจุดเริ่มทำต่อ เพื่อลดเวลาที่ต้องจัดพิมพ์รายงานใหม่ทั้งหมดเมื่อเกิดปัญหากับระบบงาน ดังนั้น กิจการต้องมีการควบคุมการใช้งานจุดเริ่มทำต่อดังกล่าวให้เหมาะสม เพื่อให้แน่ใจว่าไม่มีการสั่งพิมพ์รายงานที่มีความสำคัญอีกชุดจากจุดเริ่มทำต่อโดยไม่ได้รับอนุมัติ การตรวจสอบทำโดยตรวจทานลงบันทึกระบบปฏิบัติการ (Operating System Log) เพื่อดูว่ามีการใช้งานจุดเริ่มทำต่อโดยไม่ได้รับการอนุมัติหรือไม่

7.2.3 การควบคุมลำดับการจัดพิมพ์รายงาน ในกรณีที่รายงานไม่สามารถพิมพ์ออกมาที่เครื่องพิมพ์โดยตรง รายงานจะถูกบันทึกลงในจานบันทึกหรือดิสก์เพื่อรอให้เครื่องพิมพ์ว่างจึงจะจัดพิมพ์ข้อมูลออกมา การที่ระบบงานนำรายงานที่จะจัดพิมพ์ไปรอคิวดังกล่าวอาจก่อให้เกิดปัญหาด้านการควบคุม กล่าวคือ เป็นการเปิดโอกาสให้บุคคลที่ไม่ได้รับอนุมัติปรับปรุงเปลี่ยนแปลงข้อมูลในรายงานหรือจัดทำสำเนารายงานก่อนที่รายงานจะถูกจัดพิมพ์ที่เครื่องพิมพ์ หรือกรณีที่เกิดปัญหากับเครื่องพิมพ์นั้น บุคคลที่ไม่ได้รับอนุมัติสามารถจัดพิมพ์รายงานในจานบันทึก (Disk) ซ้ำได้ การควบคุมทำโดย

- กำหนดให้ไม่สามารถแก้ไขข้อมูลของรายงานที่บันทึกในจานบันทึกเพื่อรอพิมพ์ที่เครื่องพิมพ์ได้
- กำหนดให้ไม่สามารถจัดทำสำเนารายงานที่ถูกบันทึกลงจานบันทึกเพื่อรอพิมพ์
- กำหนดให้สามารถพิมพ์รายงานที่ถูกบันทึกในจานบันทึกได้เพียงครั้งเดียว
- ควรควบคุมการใช้งานรายงานที่ถูกบันทึกลงในจานบันทึก กล่าวคือ ไม่ให้ผู้ที่ไม่ได้รับอนุมัติจัดทำสำเนารายงานในจานบันทึกที่กิจการจัดเก็บเป็นรายงานสำรอง (Backup)

7.2.4 การควบคุมการพิมพ์ วัตถุประสงค์ของการควบคุมการพิมพ์เพื่อให้มั่นใจว่ารายงานถูกจัดพิมพ์ที่เครื่องพิมพ์ที่ถูกต้อง ผู้ที่ไม่ได้รับอนุมัติไม่สามารถดูข้อมูลที่สำคัญในรายงานที่จัดพิมพ์ได้ และการจัดพิมพ์เอกสารสัญญาได้รับการควบคุมการจัดพิมพ์ที่เหมาะสมการควบคุมทำโดย

- กรณีที่มีเครื่องพิมพ์หลายเครื่องที่สามารถใช้ในการจัดพิมพ์ เจ้าหน้าที่จัดพิมพ์รายงานอาจเลือกเครื่องพิมพ์ผิดเครื่องเพื่อออกรายงาน เนื่องจากลืมเปลี่ยนเครื่องพิมพ์ให้เป็นเครื่องพิมพ์ที่ตั้งอยู่ในห้องปิดมิดชิด นอกจากนี้ความผิดพลาดอาจเกิดจากระบบเครือข่ายคอมพิวเตอร์ทำงานผิดพลาดโดยจัดส่งรายงานไปผิดเครื่องพิมพ์ กรณีเช่นนี้การควบคุมทำโดยกำหนดให้สามารถพิมพ์รายงานที่มีความสำคัญจากเครื่องพิมพ์ที่กำหนดเท่านั้น ฝึกอบรมพนักงานให้เลือกเครื่องพิมพ์ที่เหมาะสมทุกครั้งที่ออกรายงาน และจัดทำโปรแกรมตรวจสอบว่ามีรายงานสำคัญที่ส่งไปพิมพ์ยังเครื่องพิมพ์ที่ไม่ปลอดภัยหรือไม่
- แม้ว่ารายงานอาจถูกจัดพิมพ์ที่เครื่องพิมพ์ที่เหมาะสมแล้วก็ตาม องค์กรควรควบคุมการเปิดเผยข้อมูลที่มีความสำคัญในกระดาษพิมพ์ เช่น รหัสประจำตัว เป็นต้น โดยใช้แบบฟอร์มพิเศษที่เจ้าหน้าที่จัดพิมพ์รายงานไม่สามารถอ่านข้อมูลที่พิมพ์ได้
- เนื่องจากเครื่องพิมพ์แบบกระทบ (Impact Printer) จะทำให้ตัวอักษรหรือตัวเลขที่พิมพ์ปรากฏในผ้าพิมพ์ (Ribbon) โดยเฉพาะผ้าพิมพ์ที่เพิ่งเปลี่ยนใหม่ ดังนั้นควรกำหนดให้ใช้ผ้าพิมพ์ที่ใช้มาเป็นระยะเวลาหนึ่งแล้วในการจัดพิมพ์รายงาน กรณีที่ใช้ผ้าพิมพ์ใหม่ควรกำหนดไม่ให้นำผ้าพิมพ์ออกจากเครื่องพิมพ์ภายหลังเสร็จสิ้นการพิมพ์รายงาน
- ตรวจนับจำนวนเอกสารสัญญาหรือแบบฟอร์มเปล่าสำคัญที่นำมาใช้ในการจัดพิมพ์ว่าต้องเท่ากับผลรวมของจำนวนเอกสารหรือแบบฟอร์มที่ใช้พิมพ์และจำนวนเอกสารหรือแบบฟอร์มที่เหลือ นอกจากนี้การกำหนดหมายเลขเอกสารเรียงลำดับเป็นการล่วงหน้าจะมีส่วนช่วยให้การกระทบยอดทำได้โดยสะดวกมากขึ้น
- เนื่องจากกระดาษคาร์บอนที่ใช้ในการจัดทำสำเนารายงานจะมีตัวอักษรหรือตัวเลขที่พิมพ์ปรากฏบนกระดาษคาร์บอน ดังนั้นควรมีการควบคุมการทำลายกระดาษคาร์บอนที่แยกจากสำเนารายงานด้วย

7.2.5 การควบคุมการรวบรวมรายงาน พนักงานรับส่งข้อมูลของศูนย์คอมพิวเตอร์ มีหน้าที่รวบรวมรายงานที่จัดพิมพ์เรียบร้อยแล้วเพื่อนำไปกระจายให้ผู้ใช้ต่อไป กรณีที่ผู้ใช้เป็นผู้สั่งพิมพ์รายงานเอง ผู้ใช้มีหน้าที่รวบรวมและเก็บรักษารายงานด้วยตนเอง ในการรวบรวมรายงานพนักงานรับส่งข้อมูลควรบันทึกวันและเวลาที่รวบรวมรายงานแต่ละรายงาน พร้อมทั้งชื่อของเจ้าหน้าที่ที่มารับรายงาน นอกจากนี้องค์กรควรกำหนดแนวปฏิบัติ ในกรณีที่ไม่มีใครมารับรายงานที่จัดพิมพ์เรียบร้อยแล้ว ซึ่งอาจกำหนดให้มีพนักงานที่รับผิดชอบในการรวบรวมและเก็บรักษารายงานนั้นจนกว่าผู้ที่เกี่ยวข้องจะมารับรายงาน

7.2.6 การตรวจทานความถูกต้องของรายงานเบื้องต้น พนักงานรับส่งข้อมูลของศูนย์คอมพิวเตอร์มีหน้าที่ตรวจทานความถูกต้องของรายงานในเบื้องต้นก่อนจัดส่งรายงานไปยังผู้ใช้ การตรวจทานประกอบด้วย ตรวจทานความชัดเจนของข้อมูลในหน้ารายงาน และตรวจทานความครบถ้วนของหน้ารายงาน

7.2.7 การควบคุมการกระจายรายงาน นอกจากหน้าที่ในการรวบรวมรายงานแล้ว พนักงานรับส่งข้อมูลของศูนย์คอมพิวเตอร์ยังมีหน้าที่ในการกระจายรายงานไปยังผู้ใช้อย่างปลอดภัยและภายในระยะเวลาที่เหมาะสม การกระจายรายงานไปให้ผู้ใช้อาจทำโดย นำรายงานไปใส่ในตู้เก็บของที่ใส่กุญแจ ซึ่งผู้ใช้จะนำรายงานออกจากตู้ดังกล่าวเอง หรือจัดส่งรายงานไปยังผู้ใช้โดยตรง หรือจัดส่งไปยังผู้ใช้ทางไปรษณีย์ การควบคุมการกระจายรายงาน มีดังนี้

- จดบันทึกวันและเวลาในการกระจายรายงาน นอกจากนี้ควรลงนามผู้ที่มารับรายงานด้วย ในกรณีที่จัดส่งรายงานทางไปรษณีย์ควรบันทึกจำนวนรายงานที่จัดส่งพร้อมทั้งติดตามว่ามีการจัดส่งรายงานไปถึงปลายทางเรียบร้อยภายในเวลาที่เหมาะสม
- จัดทำชื่อและที่อยู่ของส่วนงานที่จะจัดส่งรายงานให้เด่นชัด นอกจากนี้ควรจัดเก็บแฟ้มข้อมูลที่บันทึกชื่อและที่อยู่ของส่วนงานที่ได้รับรายงานให้ปลอดภัยจากการเพิ่มเติมหรือเปลี่ยนแปลงรายชื่อผู้มีสิทธิ์ได้รับรายงานโดยไม่ได้รับอนุมัติด้วย
- กรณีที่ผู้มารับรายงานเป็นบุคคลที่สาม เช่น ผู้รับจ้างรับและส่งเอกสาร เป็นต้น ควรตรวจสอบเอกสารการอนุมัติให้บุคคลนั้นมารับรายงานแทนด้วย

7.2.8 การควบคุมรายงานของผู้ใช้ ผู้ใช้ควรตรวจทานความถูกต้องของรายงานเช่นเดียวกับพนักงานรับส่งข้อมูล ซึ่งการตรวจทานรายงานของผู้ใช้จะทำในรายละเอียดมากกว่า เนื่องจากเป็นผู้คุ้นเคยกับการปฏิบัติงานนั้น ๆ การตรวจทานประกอบด้วย การคำนวณความถูกต้องของยอดรวมในรายงาน หรืออาจตรวจนับจำนวนสินค้าเปรียบเทียบกับตัวเลขที่ปรากฏในรายงาน เป็นต้น นอกจากนี้ผู้ใช้ควรตรวจทานความถูกต้องของรายงานภายในระยะเวลาที่เหมาะสมด้วย เนื่องจากถ้ามีข้อผิดพลาดที่เกิดจากการประมวลผลองค์กรสามารถปรับปรุงความถูกต้องของรายการได้ทันเวลา

7.2.9 การควบคุมการจัดเก็บรายงาน การควบคุมที่สำคัญ ประกอบด้วย

- จัดเก็บรายงานในสภาพแวดล้อมที่เหมาะสมกับลักษณะของรายงาน กล่าวคือ รายงานที่บันทึกในซีดีรอมหรือแถบบันทึก ควรจัดเก็บในสถานที่ไม่มีฝุ่นและความชื้น ส่วนรายงานที่พิมพ์ด้วยเครื่องพิมพ์เลเซอร์นั้นไม่ควรจัดเก็บในสถานที่ร้อนและชื้น เนื่องจากคุณภาพของตัวอักษรหรือตัวเลขที่พิมพ์จะเสื่อมสภาพได้ง่าย ในกรณีของไมโครฟิล์มนั้นควรจัดเก็บในห้องเย็น แห้งและปราศจากฝุ่น
- จัดเก็บรายงานในสถานที่ที่ปลอดภัย
- จัดทำทะเบียนจำนวนรายงานที่จัดเก็บ ชื่อรายงานที่จัดเก็บ สถานที่จัดเก็บรายงาน ผู้นำรายงานไปใช้และการส่งคืน
- ควรตรวจสอบความถูกต้องของรายงานที่จัดเก็บกับบันทึกการจัดเก็บรายงาน

7.2.10 การกำหนดระยะเวลาในการจัดเก็บรายงาน ระยะเวลาในการจัดเก็บรายงานนั้นมีความสำคัญต่อการเลือกสื่อบันทึกที่ใช้ในการจัดเก็บรายงาน เช่น รายงานที่พิมพ์ด้วยเครื่องพิมพ์เลเซอร์จะมีอายุการใช้งานน้อยกว่ารายงานที่พิมพ์ด้วยเครื่องพิมพ์แบบกระทบ นอกจากนี้ข้อมูลที่จัดเก็บในซีดีรอมเสื่อมสภาพเร็วกว่าการจัดเก็บข้อมูลในไมโครฟิล์ม และสภาพแวดล้อมของสถานที่จัดเก็บจะส่งผลต่อระยะเวลาในการจัดเก็บรายงานเช่นเดียวกัน ดังนั้นองค์กรควรกำหนดระยะเวลาในการจัดเก็บรายงานให้เหมาะสมกับอายุการใช้งานด้วย

7.2.11 การทำลายรายงาน รายงานที่ไม่ต้องการใช้แล้วควรทำลายทิ้ง โดยรายงานที่จัดพิมพ์บนกระดาษอาจใช้เครื่องทำลายกระดาษ กรณีของรายงานที่จัดเก็บในแถบบันทึกหรือซีดีรอมอ่าน/บันทึก (CD-Rewritable) ควรลบทิ้งเมื่อถึงเวลาที่กำหนด ส่วนซีดีรอมอ่านอย่างเดียว (CD-Recordable) นั้นสามารถทำลายโดยใช้เครื่องทำลายโดยเฉพาะซึ่งมีลักษณะเช่นเดียวกับเครื่องทำลายกระดาษ

7.3 การควบคุมผลลัพธ์แบบออนไลน์

วัตถุประสงค์ของการควบคุมผลลัพธ์แบบออนไลน์ เพื่อให้แน่ใจว่า

- ผู้ที่ได้รับรายงานเป็นผู้ที่ได้รับอนุมัติเท่านั้น
- รายงานที่จัดส่งทางออนไลน์มีความเชื่อถือได้ กล่าวคือ ข้อมูลในรายงานไม่ผิดพลาดหรือไม่มีการแก้ไขระหว่างทาง
- ผู้ที่ไม่เกี่ยวข้องไม่สามารถดูข้อมูลในรายงานได้ เมื่อมีการแสดงรายงานบนหน้าจอ

- ไม่มีการจัดทำสำเนารายงานที่ส่งไปยังเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุมัติ

ปัจจุบันการจัดส่งรายงานทางออนไลน์มีจำนวนมากขึ้น กล่าวคือ ส่วนงานหลาย ๆ ส่วนงานมีการแลกเปลี่ยนข้อมูลผ่านทางระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะเป็นแบบการสับเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (Electronic Data Interchange หรือ EDI) หรือการแสดงผลลัพธ์บนเว็บเพจ การจัดส่งข้อมูลดังกล่าวก่อให้เกิดโอกาสของข้อผิดพลาดมากขึ้น ดังนั้นองค์กรควรควบคุมผลลัพธ์ออนไลน์ ดังนี้

7.3.1 การควบคุมแหล่งกำเนิดของรายงาน เพื่อให้แน่ใจว่ารายงานที่สร้างขึ้นมาหรือสามารถเข้าถึงได้เป็นรายงานที่ได้รับการอนุมัติถูกต้องครบถ้วนและจัดสร้างขึ้นในระยะเวลาที่เหมาะสม ลักษณะของการควบคุมแหล่งกำเนิดรายงานขึ้นอยู่กับวิธีการที่ผู้ใช้เข้าถึงรายงาน โดยแหล่งกำเนิดรายงานและการควบคุม มีดังนี้

(1) การแลกเปลี่ยนข้อมูลระหว่างองค์กร เช่น การจัดส่งข้อมูลการซื้อขายสินค้าทางระบบสับเปลี่ยนข้อมูลอิเล็กทรอนิกส์ซึ่งระบบงานมักจะสร้างรายการเพื่อจัดส่งไปยังองค์กรอื่นโดยอัตโนมัติ เช่น รายการซื้อสินค้าและการโอนเงินค่าสินค้า เป็นต้น การควบคุมการแลกเปลี่ยนข้อมูลในลักษณะนี้เพื่อให้แน่ใจว่ารายการที่ส่งไปยังอีกองค์กรนั้นเป็นรายการที่ได้รับการอนุมัติถูกต้องครบถ้วนและจัดทำขึ้นในระยะเวลาที่เหมาะสม โดยมีการสร้างรายการที่จะจัดส่งเพียงครั้งเดียว นอกจากนี้ควรมีการควบคุมการจัดทำรายการในกรณีที่พนักงานขององค์กรเป็นผู้จัดทำรายการและจัดส่งไปยังองค์กรอื่น แต่ถ้าระบบงานจัดสร้างรายการโดยอัตโนมัติ องค์กรจำเป็นต้องมีการควบคุมความถูกต้องของการประมวลผลของระบบงานเช่นกัน การควบคุมดังกล่าวจะทำให้กิจการที่ได้รับข้อมูลมีความมั่นใจในความถูกต้องครบถ้วนของข้อมูลที่ได้รับ

(2) การควบคุมกรณีที่ผู้ใช้เข้าถึงข้อมูลในฐานข้อมูลเพื่อจัดทำรายงานโดยใช้ภาษาสอบถาม เช่น Structured Query Language (SQL) หรือ Not Only SQL (NOSQL) เป็นต้น ประกอบด้วย

1) ข้อมูลในฐานข้อมูลที่จะนำมาจัดสร้างรายงานต้องเป็นข้อมูลที่ได้รับการอนุมัติ ถูกต้อง ครบถ้วน และทันเวลา

2) ภาษาสอบถามที่ใช้ในการเข้าถึงข้อมูลในฐานข้อมูลทำงานอย่างถูกต้องครบถ้วน และผู้ใช้โปรแกรมภาษาสอบถามต้องเป็นผู้ที่ได้รับอนุมัติ

3) ฝึกอบรมผู้ใช้ให้สามารถเรียกใช้ภาษาสอบถามเชิงจัดทำรายงานและกำหนดคำสั่งในการออกรายงานได้อย่างถูกต้อง

(3) ผู้ใช้เข้าถึงรายงานผ่านเว็บบราวเซอร์ (Browser) กรณีนี้องค์กรต้องแน่ใจว่ารายงานทางออนไลน์นั้นเป็น

1) รายงานที่ได้รับอนุมัติ ถูกต้องครบถ้วนและทันเวลา นอกจากนี้รายงานต้องให้ข้อมูลที่ทันสมัยและเหมาะสมกับเป้าหมายและวัตถุประสงค์ขององค์กร

2) รายงานที่จัดสร้างมาจากองค์กรจริง การยืนยันว่ารายงานถูกจัดสร้างขึ้นโดยองค์กรจริงมักใช้การแปลงรหัสรายการในรายงานเพื่อไม่ให้ผู้ที่ไม่เกี่ยวข้องสามารถอ่านข้อมูลในรายงานได้ และยังสามารถใช้ลายมือชื่อดิจิทัลประกอบได้ด้วย

(4) ผู้ใช้จัดส่งรายงานทางอีเมล เนื่องจากการจัดส่งรายงานทางอีเมลถือเป็นการจัดส่งรายงานไปยังผู้ที่เกี่ยวข้องในนามขององค์กร ซึ่งผู้ที่ได้รับรายงานจากอีเมลอาจนำมาฟ้องร้ององค์กรได้เมื่อเกิดปัญหาขึ้น ดังนั้นองค์กรควรกำหนดแนวทางในการจัดส่งและรับอีเมล กล่าวคือ ควรกำหนดองค์ประกอบของข้อมูลที่สามารถจัดส่งทางอีเมล และการจัดการกับรายงานที่ได้รับ ทั้งนี้รายงานที่ได้รับผ่านทางอีเมลนั้นอาจเป็นรายงานที่ปลอมแปลงมา ดังนั้นควรกำหนดวิธีการจัดส่งรายงานระหว่างองค์กรซึ่งอาจใช้ลายเซ็นอิเล็กทรอนิกส์ได้เช่นกัน

7.3.2 การควบคุมการกระจายรายงาน เพื่อให้มั่นใจว่าพนักงานที่ได้รับอนุมัติเท่านั้นได้รับรายงาน การควบคุมทำโดย

(1) จัดเก็บที่อยู่ทางอิเล็กทรอนิกส์ของผู้รับรายงานให้เป็นปัจจุบันอยู่เสมอ นอกจากนี้ควรตรวจสอบเป็นระยะ ๆ ว่าไม่มีการเพิ่มเติมที่อยู่ที่ไม่ได้รับอนุมัติ และข้อมูลที่จัดเก็บเป็นข้อมูลที่ถูกต้องเท่านั้น

(2) ตรวจสอบว่ามีการกระจายรายงานไปยังผู้รับในเวลาที่เหมาะสมและครบถ้วน

7.3.3 การควบคุมการสื่อสาร วัตถุประสงค์หลักของการควบคุมการสื่อสารเพื่อให้แน่ใจว่ารายงานที่จัดส่งผ่านระบบเครือข่ายคอมพิวเตอร์ไม่ถูกดัดแปลง เพิ่มเติม ลบทิ้ง หรือถูกลักลอบดูองค์ประกอบของรายงานโดยบุคคลที่ไม่เกี่ยวข้อง การควบคุมหลักที่ใช้ในการจัดส่งรายงานผ่านระบบเครือข่ายคอมพิวเตอร์ทำโดยการเข้าและถอดรหัสข้อมูลเพื่อให้อยู่ในรูปแบบที่ผู้ที่ไม่เกี่ยวข้องไม่สามารถอ่านข้อมูลได้

7.3.4 การควบคุมการรับรายงาน เมื่อได้รับรายงานผู้ที่รับรายงานควรพิจารณาว่าจะรับรายงานนั้นหรือไม่ เช่น รายงานที่ส่งมากับอีเมลเป็นต้น องค์กรควรกำหนดว่าก่อนการเปิดอ่านรายงานที่ได้รับทางออนไลน์ทุกครั้งต้องตรวจสอบว่ารายงานที่จัดส่งมาไม่มีไวรัส หรือไม่เป็นแฟ้มข้อมูลที่ไปจองพื้นที่ในสื่อบันทึกทั้งหมดจนทำให้คอมพิวเตอร์ขององค์กรมีปัญหาได้

7.3.5 การควบคุมการตรวจทาน รายงานที่จัดส่งไปยังผู้รับอาจไม่ได้เปิดอ่านทันที เนื่องจากผู้รับรายงานไม่อยู่หรือกำลังปฏิบัติงานอื่น ในกรณีนี้คอมพิวเตอร์ขององค์กรควรมีระบบตอบกลับอัตโนมัติเพื่อแจ้งให้ผู้ส่งรายงานทราบว่ารายการที่จัดส่งมานั้นยังไม่ได้รับการประมวลผล แต่จะประมวลผลทันทีในเวลาที่กำหนด เนื่องจากปัจจุบันรายการที่ส่งผ่านทางอิเล็กทรอนิกส์มีจำนวนมากขึ้นเป็นลำดับ ดังนั้นอาจส่งผลให้ผู้ปฏิบัติงานไม่สามารถปฏิบัติงานกับรายการทั้งหมดที่ได้รับให้ทันกำหนดเวลาได้ จึงมีการนำโปรแกรมที่เรียกว่า Intelligent Agent เพื่อเลือกรายการที่มีความสำคัญมากมาประมวลผลหรือดำเนินการก่อน แต่โปรแกรมการเลือกรายการดังกล่าวอาจมีข้อบกพร่อง เนื่องจากเกณฑ์ในการกำหนดทางเลือกไม่ชัดเจน ดังนั้นองค์กรควรกำหนดนโยบายในการจัดการกับรายการที่จัดส่งมาให้พนักงานว่าควรดำเนินการกับรายการใดก่อนและหลัง เช่น จะดำเนินรายการให้กับสมาชิกก่อน เป็นต้น นอกจากนี้ผู้ที่ไม่เกี่ยวข้องที่เดินผ่านเครื่องคอมพิวเตอร์อาจอ่านข้อมูลจากหน้าจอที่เปิดทิ้งไว้ได้ ดังนั้นควรจัดวางเครื่องคอมพิวเตอร์ให้อยู่ในตำแหน่งที่เหมาะสมและผู้ที่เดินผ่านไปมาไม่สามารถอ่านข้อมูลที่หน้าจอได้ หรืออาจตั้งฉากบังหน้าจอก็ได้ กรณีของรายงานที่มีความสำคัญมาก ๆ อาจแสดงที่หน้าจอโดยใช้แสงอ่อน ๆ เพื่อให้ผู้ที่อยู่ใกล้หน้าจออ่านได้เท่านั้น ทั้งนี้ บางองค์กรอาจให้พนักงานหลายคนใช้เครื่องคอมพิวเตอร์ร่วมกัน ส่งผลให้พนักงานที่ไม่มีหน้าที่ที่เกี่ยวข้องสามารถจัดส่งรายงานไปยังบุคคลอื่นผ่านทางเครื่องคอมพิวเตอร์ได้ ดังนั้นควรกำหนดให้การเข้าถึงรายงานที่สำคัญต้องมีรหัสผ่าน โดยรหัสดังกล่าวจะทราบเฉพาะผู้ที่เกี่ยวข้องเท่านั้น

7.3.6 การควบคุมการจัดการ องค์กรควรกำหนดนโยบายเพื่อเป็นแนวทางสำหรับพนักงานในการจัดการกับรายงานที่ได้รับทางออนไลน์ โดยนโยบายดังกล่าวควรกำหนดว่าพนักงานที่ได้รับรายงานแล้วจะต้องส่งต่อรายงานหรือจัดทำสำเนาให้กับส่วนงานใดบ้าง และควรตระหนักว่ารายงานที่ตนได้รับนั้น แม้ว่าจะไม่มีความสำคัญกับตนเองก็ตาม แต่รายงานดังกล่าวอาจมีคุณค่าต่อบุคคลอื่น ๆ ในองค์กรได้ รายงานที่ได้รับจากคอมพิวเตอร์มักเป็นแฟ้มข้อมูลที่อาจถูกส่งต่อไปให้บุคคลอื่นได้ การควบคุมจึงทำได้ยาก กล่าวคือ ผู้ใช้อาจทำสำเนารายงานเพื่อนำไปใช้ที่อื่นทำให้ยากต่อการควบคุมรายงานดังกล่าว ดังนั้นนโยบายที่องค์กรกำหนดควรมีความชัดเจนเพื่อให้แน่ใจว่า พนักงานทุกคนเข้าใจถึงการปฏิบัติงานที่เกี่ยวข้องกับรายงานทางออนไลน์ นอกจากนี้ควรจัดทำลงบันทึกกิจกรรมที่เกิดขึ้นของพนักงานกับรายงานที่มีความอ่อนไหวและมีการตรวจหารายการผิดปกติในบันทึกกิจกรรมเป็นระยะ ๆ โดยผู้บริหารด้วย

7.3.7 การควบคุมการเก็บรักษา การที่จำนวนรายงานทางออนไลน์ที่จัดส่งไปยังผู้ใช้มีจำนวนมาก อาจทำให้ผู้ใช้ต้องลบรายงานทิ้งจากคอมพิวเตอร์ให้เร็วที่สุดเท่าที่จะเป็นไปได้ แต่รายงานบางประเภท เช่น รายงานจากระบบสับเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ เป็นต้น เป็นรายงานที่มีความสำคัญซึ่งองค์กรควรกำหนดระยะเวลาในการจัดเก็บเพื่อเป็นหลักฐานทางภาษีอากร หรือเป็นสัญญาข้อตกลงระหว่างองค์กร ดังนั้นองค์กรควรกำหนดแนวทางเพื่อช่วยให้พนักงานตัดสินใจได้ว่ารายงานใดเป็นรายงานที่มีความสำคัญต่อองค์กรและต้องจัดเก็บไว้หรือรายงานใดไม่สำคัญและสามารถลบได้ นอกจากนี้ควรกำหนดให้เฉพาะผู้บริหารขององค์กรสามารถเข้าถึงรายงานที่จัดเก็บได้เท่านั้น รวมทั้งควรมีการสำรองข้อมูลและมีระบบกู้รายงานคืนด้วย

7.3.8 การควบคุมการลบทิ้ง เมื่อรายงานออนไลน์หมดอายุแล้วควรลบรายงานทิ้ง โดยใช้โปรแกรมลบแฟ้มข้อมูลรายงาน นอกจากนี้องค์กรควรตรวจว่ามีรายงานใดที่ครบอายุและต้องลบออกเป็นระยะ ๆ การลบรายงานออกจากแฟ้มข้อมูลส่งผลให้ไม่สามารถเรียกใช้รายงานที่ลบออกได้เท่านั้น แต่รายงานยังไม่ได้ถูกลบหรือทำลายจากที่จัดเก็บโดยสมบูรณ์ กล่าวคือ สามารถใช้โปรแกรมพิเศษในการเรียกรายงานที่ลบทิ้งไปแล้วกลับคืนมาได้ ดังนั้นองค์กรควรแน่ใจว่าหลังจากลบรายงานทิ้งแล้วควรบันทึกรายงานอื่นซ้ำลงไปในเนื้อที่ของรายงานที่ลบทิ้งเพื่อให้แน่ใจว่ารายงานถูกลบทิ้งโดยสมบูรณ์แล้ว

7.4 ร่องรอยการตรวจสอบของผลลัพธ์

ร่องรอยการตรวจสอบของผลลัพธ์ คือ ลำดับเหตุการณ์เรียงตามวันและเวลานับตั้งแต่ได้ผลลัพธ์จนกระทั่งผู้ใช้ทำลายผลลัพธ์ ร่องรอยการตรวจสอบของผลลัพธ์สามารถแบ่งเป็นร่องรอยการควบคุมด้านการบัญชีและการปฏิบัติงาน ดังนี้

ร่องรอยการควบคุมด้านการบัญชี แสดงให้เห็นว่าส่วนงานใดได้รับรายงานอะไรบ้าง วันเวลาที่ได้รับรายงาน และการจัดการกับรายงานที่ได้รับ เช่น วิธีการจัดเก็บ การควบคุมการใช้งาน และระยะเวลาในการจัดเก็บรายงาน เป็นต้น ข้อมูลดังกล่าวช่วยให้ทราบว่าส่วนงานใดมีหน้าที่รับผิดชอบกับรายงานใดบ้าง นอกจากนี้ถ้ารายงานที่แจกจ่ายมีข้อผิดพลาดจะทำให้ทราบว่าหน่วยงานใดอาจได้รับผลกระทบจากรายงานดังกล่าวและสามารถติดตามพร้อมทั้งแจ้งให้ส่วนงานที่ได้รับรายงานทราบและระมัดระวังการใช้ข้อมูลในรายงานเพื่อการตัดสินใจ กรณีที่รายงานถูกแจกจ่ายให้กับสาธารณชนนั้น องค์กรมักแจ้งให้ผู้ใช้ข้อมูลในรายงานทราบว่าองค์กรไม่รับผิดชอบต่อความเสี่ยงที่อาจเกิดขึ้นจากการใช้รายงานนั้น ๆ นอกจากนี้ร่องรอยการตรวจสอบของผลลัพธ์ยังสามารถใช้พิจารณาว่ามีบุคคลที่ไม่ได้รับอนุมัติเข้าถึงรายงานหรือไม่ โดยผู้บริหารสามารถตรวจสอบบันทึกการเข้าใช้รายงานเพื่อให้ทราบว่ามีการเข้าถึงข้อมูลในรายงานโดยไม่ได้รับอนุญาตหรือไม่

ส่วนร่องรอยการควบคุมด้านการปฏิบัติการ จะให้ข้อมูลเกี่ยวกับการใช้ทรัพยากรเพื่อจัดพิมพ์รายงานประเภทต่าง ๆ เช่น จำนวนรายงานที่พิมพ์ และเวลาที่ใช้ในการพิมพ์ เป็นต้น ร่องรอยดังกล่าวสามารถนำมาใช้พิจารณาถึงความทันต่อเวลาของรายงานที่จัดส่งไปยังผู้ใช้ได้

8. ความเสี่ยงและการควบคุมระบบงานบนเว็บ

The OWASP Foundation (2023) ได้จัดทำ The Open Web Application Security Project (OWASP) เพื่อจัดอันดับความเสี่ยงที่อาจเกิดขึ้นกับระบบงานบนเว็บ 10 อันดับรวมทั้งแนวทางในการป้องกันล่าสุด เมื่อปี ค.ศ. 2021 ดังนี้

ความเสี่ยง	การควบคุม
อันดับที่หนึ่ง : Broken Access Control ความเสี่ยงที่จะถูกโจมตีช่องโหว่จากการที่ระบบงานบนเว็บรับข้อมูลจากผู้ใช้ผ่าน URL ทำให้ผู้ใช้สามารถเข้าถึงข้อมูลหรือไฟล์ต่าง ๆ ที่ไม่มีสิทธิ์ในการเข้าถึงได้โดยตรง ก่อให้เกิดปัญหาข้อมูลไม่ถูกต้องครบถ้วน หรือข้อมูลไม่เป็นความลับ นอกจากนี้ยังรวมถึงช่องโหว่ที่เกิดจากความผิดพลาดในการตรวจสอบสิทธิ์ กล่าวคือ มีการพิสูจน์ตัวจริงเมื่อผู้ใช้ลงบันทึกเข้าแต่ไม่ได้ตรวจสอบว่ามีสิทธิ์เข้าใช้งานหรือไม่	- หลีกเลี่ยงการให้ข้อมูลการอ้างอิง Object ให้กับผู้ใช้ เช่น รหัสผู้ใช้ เป็นต้น - ใช้ค่าของดรรชนี (Index Value) ในการอ้างอิงเพื่อป้องกันการโจมตีด้วยการปรับเปลี่ยนค่าพารามิเตอร์ (Manipulation) เช่น http://www. example.com/application?file=1 เป็นต้น และควรกำหนดให้มีการสอบทานอำนาจในการอนุมัติ สำหรับการอ้างอิง object - ตรวจสอบการควบคุมการเข้าถึง (Access Control) ที่เซิร์ฟเวอร์
อันดับที่สอง : Cryptographic Failures ความเสี่ยงของการเปิดเผยข้อมูลที่มีความอ่อนไหว เนื่องจากไม่มีการป้องกันด้วยเทคนิคต่าง ๆ อย่างถูกวิธี	- เข้ารหัสข้อมูล
อันดับที่สาม : Injection ความเสี่ยงที่จะถูกโจมตีด้วยการฉีดคำสั่งค้นหาข้อมูล หรือการที่ผู้ไม่หวังดีจัดส่งรหัสต้นฉบับ (Source Code) ไปให้ระบบงานบนเว็บประมวลผลหรือจัดเก็บ เพื่อหวังผลในการโจรกรรม ลบ แก้ไข หรือหยุดการทำงานของระบบงานบนเว็บ โดยการฉีดคำสั่งซึ่งอาจอยู่ในรูปแบบต่าง ๆ เช่น XSS (Cross Site Scripting), SQL Injection, NoSQL Injection เป็นต้น	- สอบทานความสมเหตุสมผลของข้อมูลนำเข้า (Input Validation) - กำหนดสิทธิ์ในการเข้าถึงฐานข้อมูลอย่างรัดกุม - หลีกเลี่ยงการให้ข้อมูลในการระบุความผิดพลาดของระบบงานบนเว็บมากเกินไปจนผู้โจมตีสามารถนำไปใช้ประโยชน์ในการทำอันตรายกับระบบงานบนเว็บได้
อันดับที่สี่ : Insecure Design ความเสี่ยงที่จะถูกโจมตีที่การออกแบบระบบงานบนเว็บที่ผิดพลาดเนื่องจากไม่มีการวิเคราะห์ความเสี่ยงของกิจกรรมทางธุรกิจอย่างเพียงพอ ทำให้มีหรือไม่มีการติดตั้งการควบคุมที่เหมาะสมสำหรับระบบงานบนเว็บที่พัฒนามาใช้งาน เช่น การพิสูจน์ตัวจริง การรักษาความลับ ความถูกต้องครบถ้วน การมีให้ใช้ได้ และการควบคุมการเข้าถึง เป็นต้น โดยข้อผิดพลาดของการออกแบบระบบงานบนเว็บนี้ไม่ใช่ข้อผิดพลาดจากการ Implement	- ใช้กระบวนการพัฒนาระบบที่มีการประเมินและออกแบบระบบงานบนเว็บที่มีการรักษาความมั่นคงปลอดภัย - ทดสอบระบบงานบนเว็บที่พัฒนามาใช้งานว่ามีการป้องกันความเสี่ยงหลัก ๆ ได้อย่างเหมาะสม

ความเสี่ยง	การควบคุม
อันดับที่ห้า : Security Misconfiguration ความเสี่ยงที่จะถูกโจมตีช่องโหว่ของการตั้งค่าการทำงานที่ผิดพลาดของระบบงานบนเว็บ เช่น ติดตั้งหน้าที่งานที่ไม่จำเป็นต้องใช้โปรแกรมที่ใช้งานไม่เป็นปัจจุบันหรือมีช่องโหว่ และไม่เปลี่ยนค่ารหัสผ่านที่โปรแกรมกำหนดค่าให้โดยปริยายภายหลังการติดตั้งระบบ เป็นต้น	- สแกนระบบอย่างสม่ำเสมอเพื่อช่วยค้นหาการกำหนดค่าการทำงานของตัวแปรที่ไม่เหมาะสม - ปรับ Security Patch, Service Pack หรือ Hotfix ให้เป็นปัจจุบันอย่างสม่ำเสมอ
อันดับที่หก : Vulnerable and Outdated Components ความเสี่ยงที่จะถูกโจมตีช่องโหว่ของการใช้ส่วนประกอบของระบบงานบนเว็บที่มีความบกพร่องและไม่เป็นปัจจุบัน	- ผู้พัฒนาโปรแกรมควรใช้ส่วนประกอบของระบบงานทุกส่วนที่เป็นรุ่นล่าสุด และควรกำหนดให้ไม่สามารถประมวลผลมอดูลของระบบงานบนเว็บแบบ Full Privileges และควรปรับ Security Patch, Service Pack หรือ Hotfix ของทุกส่วนให้ทันสมัย
อันดับที่เจ็ด : Identification and Authentication Failures ความเสี่ยงที่จะถูกโจมตีช่องโหว่ของการพิสูจน์ตัวจริงเนื่องจากระบบงานบนเว็บมีจุดอ่อนในการพิสูจน์ตัวจริง (Authentication) และการจัดการกับสถานะของผู้ใช้ (Session Management)	- ตรวจสอบช่วงเวลาของผู้ใช้ก่อนที่จะอนุญาตให้เข้าใช้งานได้ - ตรวจสอบสิทธิ์ทุกหน้าเว็บที่ต้องการเข้าไปใช้งาน - เมื่อผู้ใช้ออกจากระบบงานบนเว็บแล้วควรมีคำสั่งลบช่วงเวลาที่ให้ใช้งานทั้งหมดด้วยเพื่อไม่ให้สามารถกลับไปหน้าเว็บอื่นได้อีก
อันดับที่แปด : Software and Data Integrity Failures ความเสี่ยงที่จะถูกโจมตีช่องโหว่ของการใช้ส่วนประกอบของระบบงานบนเว็บโดยไม่มีการทดสอบความถูกต้องครบถ้วน (Integrity) หรือการทำงานร่วมกันได้ของส่วนประกอบของโปรแกรมนี้กับระบบงานบนเว็บ เช่น ไม่มีการทดสอบว่าส่วนประกอบของระบบงานนั้นเข้ากันได้กับระบบงานหรือไม่ หรือส่วนประกอบของระบบงานมาจากแหล่งที่ถูกต้องหรือไม่ เป็นต้น นอกจากนี้ยังรวมถึงการโจมตีช่องโหว่ของกระบวนการ Serialization และ Deserialization กล่าวคือ ถ้าระบบงานบนเว็บแปลงสายข้อมูล Object ให้เป็นรูปแบบบิต (Serialization) ที่เป็น Text-based เช่น HTTP หรือ XML เป็นต้น จะทำให้ผู้ไม่หวังดีสามารถอ่านข้อมูลได้ทันทีหรือปรับเปลี่ยนข้อมูลในสายข้อมูลได้ เมื่อปลายทางได้รับสายข้อมูลในรูปแบบบิตและแปลงสายข้อมูลนั้นกลับมาเป็น Object (Deserialization) เพื่อประมวลผลโดยไม่ตรวจสอบว่าสายข้อมูลในรูปแบบบิตดังกล่าวมีการเปลี่ยนแปลงระหว่างทางหรือไม่ ซึ่งจะเป็นภัยคุกคามต่อระบบได้ เช่น ผู้โจมตีปรับเปลี่ยนสายข้อมูลเพื่อให้สิทธิ์ผู้ดูแลระบบหรือบัญชีผู้ใช้ที่ชื่อว่า Administrator กับตนเอง ดังตัวอย่าง a:4:{i:0;1;s:5:”Alice”;i:2;s:5:”admin”;i:3;s:32:”b6a8b3bea87fe0e05022f8f3c88bc960”;} เป็นต้น หรือทราบข้อมูลที่อยู่ในสายข้อมูล เช่น รหัสผู้ใช้ รหัสผ่าน และข้อมูลสำคัญอื่น ๆ เป็นต้น	- สอบทานแหล่งของส่วนประกอบของระบบงานบนเว็บว่ามาจากแหล่งที่ถูกต้องและไม่ถูกเปลี่ยนแปลง - สอบทานกระบวนการเปลี่ยนแปลงระบบงานบนเว็บและการปรับค่าการทำงานเพื่อลดโอกาสที่จะเกิดข้อผิดพลาดจากการเปลี่ยนแปลงข้างต้นกับระบบงานอื่น ๆ ในระบบคอมพิวเตอร์ - เข้ารหัสสายข้อมูลในรูปแบบบิต - ลงบันทึกและติดตามการแปลงสายข้อมูลในรูปแบบบิตให้กลับมาเป็น Object ที่ผิดปกติ หรือน่าสงสัย

ความเสี่ยง	การควบคุม
อันดับที่เก้า : Security Logging and Monitoring Failures ความเสี่ยงที่จะถูกโจมตีช่องโหว่ของระบบงานบนเว็บที่ไม่มีการจัดเก็บและสอบทานรายการในลงบันทึกอย่างเหมาะสมทำให้ผู้ไม่หวังดีสามารถโจมตีระบบงานบนเว็บได้เนื่องจากไม่ดำเนินการกับภัยนั้นอย่างทันท่วงที	- กำหนดให้มีการลงบันทึกรายการที่สำคัญ ๆ อย่างครบถ้วน เช่น การพยายามเข้าถึงระบบงานบนเว็บด้วยรหัสผ่านที่ไม่ถูกต้องหลายครั้ง เป็นต้น - กำหนดให้มีการสอบทานรายการที่ผิดปกติ ลงในบันทึกและมีการจัดการกับสิ่งผิดปกติโดยทันที
อันดับที่สิบ : Server-Side Request Forgery (SSRF) ความเสี่ยงที่จะถูกโจมตีช่องโหว่ที่เกิดจากผู้ไม่หวังดี สามารถส่งคำร้องขอใช้บริการปลอมผ่าน http หรือผ่านระบบงานบนเว็บเพื่อดึงข้อมูล (Fetch Data) ที่อยู่บนเซิร์ฟเวอร์หรือคอมพิวเตอร์อื่น ๆ ในระบบเครือข่ายที่ไม่อนุญาตให้ดึงข้อมูลได้ โดยคำร้องขอใช้บริการปลอมนี้จะดึงข้อมูลที่ไม่อนุญาตให้เข้าถึงได้ แม้ว่าจะมีการกำหนดค่าไฟร์วอลล์ (Firewall), VPN, หรือกำหนดรายชื่อผู้มีสิทธิ์ที่สามารถเข้าถึงระบบเครือข่ายก็ตาม การโจมตีดังกล่าวจะเกิดจากการอนุญาตให้ดึงข้อมูลกับฐานข้อมูลบนเซิร์ฟเวอร์ในรูปแบบของคำสั่งเรียกใช้ Application Programming Interface (API) นอกจากนี้การโจมตีดังกล่าวจะมีมากขึ้นเมื่อมีการใช้บริการ Cloud Computing และความซับซ้อนของสถาปัตยกรรมคอมพิวเตอร์ที่เพิ่มขึ้น	- แยกเซิร์ฟเวอร์ที่อนุญาตให้ดึงข้อมูลจากระยะไกลออกมาจากเครือข่ายอื่น ๆ - กำหนดกฎหรือเงื่อนไขในไฟร์วอลล์ (Firewall) หรือควบคุมการเข้าถึงเครือข่ายให้ปฏิเสธการจราจรทั้งหมดยกเว้นการจราจรที่สำคัญใน Intranet - สอบทานความสมเหตุสมผลของข้อมูลนำเข้า (Input Validation) จากไคลเอนต์ - กำหนด URL เฉพาะที่ไม่สามารถปรับเปลี่ยนช่องทางเข้าออก (Port) หรือการเชื่อมต่อปลายทาง (Destination) และกำหนดรายการที่สามารถให้เข้าถึงได้ (Allow List) เท่านั้น - ไม่จัดส่งข้อความตอบกลับที่มีค่าและมีส่วนหัวของข้อความตอบกลับที่เป็นทางเลือก (Raw Response) กลับไปที่ไคลเอนต์

9. ความเสี่ยงและการควบคุมอุปกรณ์เคลื่อนที่

จากภาพที่ 1 จะเห็นได้ว่าอุปกรณ์เคลื่อนที่เป็นหนึ่งในองค์ประกอบหลักของระบบงาน โดยอุปกรณ์เคลื่อนที่อาจเป็น Smartphones, Tablets, Laptops, Notebooks หรือสื่อบันทึกข้อมูลพกพาที่ต่อพ่วงกับคอมพิวเตอร์ (Portable Universal Serial Bus Devices For Storage) เช่น Thumb Drives เป็นต้น หรืออุปกรณ์เชื่อมต่อ เช่น อุปกรณ์โมเด็มที่เชื่อมต่อผ่านสัญญาณไวไฟหรือ Bluetooth เป็นต้น ที่ผู้ใช้สามารถใช้อุปกรณ์เหล่านี้ประมวลผลระบบงานตามสถานที่ต่าง ๆ เช่น ที่บ้าน สำนักงาน และอื่น ๆ เป็นต้น การอนุญาตให้ใช้อุปกรณ์เคลื่อนที่ดังกล่าวในการประมวลผลระบบงานของกิจการผ่านทางระบบเครือข่ายก่อให้เกิดความเสี่ยงซึ่งต้องมีการควบคุมดังนี้ (ISACA, 2010)

ความเสี่ยง	การควบคุม
1. อุปกรณ์เคลื่อนที่อาจมีโปรแกรมมุ่งร้าย (Malware) ทำให้สามารถนำโปรแกรมมุ่งร้ายเข้าสู่ระบบเครือข่ายของกิจการได้ ส่งผลให้ข้อมูลของกิจการรั่วไหลถูกเปลี่ยนแปลง สูญหาย หรือถูกทำลาย	- กำหนดนโยบายเกี่ยวกับการนำอุปกรณ์เคลื่อนที่ โดยนโยบายระบุถึงความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่ทั้งทางกายภาพและตรรกะ ประเภทของอุปกรณ์และข้อมูลที่สามารถประมวลผลระบบงานและเข้าถึงข้อมูลของกิจการได้ - กำหนดให้มีการติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุง Virus Definition ให้เป็นปัจจุบันเสมอ - เข้ารหัสข้อมูลที่มีความอ่อนไหวซึ่งส่งผ่านระบบเครือข่าย - กำหนดให้ผู้ใช้ที่ต้องการเข้าถึงระบบคอมพิวเตอร์ของกิจการผ่านทางระบบเครือข่ายให้ทำผ่าน VPN (Virtual Private Network), IP Security (Ipse) หรือ Secure Sockets Layer (SSL) กล่าวอีกนัยหนึ่งคือการเข้าถึงระบบคอมพิวเตอร์ของกิจการต้องเข้าทางช่องทางพิเศษที่มีการพิสูจน์ตัวจริงและมีการเข้ารหัสข้อมูลที่ส่งผ่านระหว่างกัน - กำหนดให้มีการบริหารจัดการอุปกรณ์เคลื่อนที่ เช่น มีระบบติดตามอุปกรณ์เคลื่อนที่ที่ถูกขโมยหรือสูญหาย เป็นต้น รวมถึงการบริหารจัดการอุปกรณ์เคลื่อนที่ของเจ้าหน้าที่ที่ลาออก สิ้นสุดสัญญาหรือไล่ออก - กำหนดประเภทและระดับการเข้าถึงข้อมูลที่อุปกรณ์เคลื่อนที่สามารถเข้าถึงได้ - สร้างความตระหนักในการรักษาความมั่นคงปลอดภัยให้กับผู้ใช้งานที่นำอุปกรณ์เคลื่อนที่มาประมวลผลระบบงานของกิจการ
2. ผู้มุ่งร้ายดักจับข้อมูลที่ส่งไปและกลับจากอุปกรณ์เคลื่อนที่ระหว่างการสื่อสารกับระบบเครือข่ายของกิจการหรือขโมยอุปกรณ์เคลื่อนที่ เนื่องจากผู้ใช้อุปกรณ์ไม่ติดตั้งระบบรักษาความปลอดภัยในอุปกรณ์เคลื่อนที่อย่างเหมาะสม ส่งผลให้ข้อมูลที่มีความอ่อนไหวของกิจการถูกเปิดเผยได้	
3. อุปกรณ์เคลื่อนที่สูญหายหรือถูกขโมย ส่งผลให้ผู้ใช้ไม่สามารถใช้งานระบบงาน นอกจากนี้ ผู้ที่ไม่เกี่ยวข้องที่สามารถเข้าถึงอุปกรณ์เคลื่อนที่จะสามารถเข้าถึงข้อมูลของกิจการที่จัดเก็บในอุปกรณ์นั้นได้	
4. อุปกรณ์เคลื่อนที่ไม่มีการเข้ารหัสข้อมูลของกิจการที่จัดเก็บในอุปกรณ์ ส่งผลให้ข้อมูลที่มีความอ่อนไหวของกิจการถูกเปิดเผยได้	
5. อุปกรณ์เคลื่อนที่อนุญาตให้ติดตั้งโปรแกรมของบุคคลที่สามที่ไม่มีการยืนยันความปลอดภัย Unsigned Third-Party Applications ได้ส่งผลให้ข้อมูลของกิจการรั่วไหล ถูกเปลี่ยนแปลง สูญหายหรือถูกทำลาย	

10. การตรวจสอบ

ในการดำเนินการตรวจสอบ ผู้สอบบัญชีจะจัดเก็บข้อมูลจากผู้รับตรวจ ดังนี้

- สำรวจหรือสังเกต (Observations) ว่าเจ้าหน้าที่มีการปฏิบัติตามระเบียบที่เกี่ยวกับการควบคุมหรือไม่
- สอบถาม (Interview) หรือทบทวนเอกสารหรือคู่มือของผู้รับตรวจ (Documented Information) เพื่อให้ได้ข้อมูลว่ามีการปฏิบัติเกี่ยวกับการควบคุมอย่างไร สำหรับการถามคำถามนั้น ผู้สอบบัญชียังต้องกำหนดว่าจะสอบถามผู้รับตรวจตำแหน่งอะไรเพื่อให้ได้คำตอบประกอบการตรวจสอบอย่างเหมาะสมที่สุด
- ทดสอบ (Test) เพื่อให้ได้ข้อมูลว่าระบบการควบคุมสามารถควบคุมความเสี่ยงได้หรือไม่ ปกติเป้าหมายหลักของการตรวจสอบระบบงานเพื่อให้มั่นใจว่า ระบบงานได้บันทึกข้อมูลอย่างถูกต้องและครบถ้วน โดยทั่วไปการตรวจสอบจะมีองค์ประกอบหลักของโปรแกรมประยุกต์ ตามภาพที่ 1 ตั้งแต่การอนุญาตให้เข้าถึงระบบงาน การกำหนดสิทธิ์ของผู้ใช้ การทำให้ระบบงาน แข็งแกร่ง รวมถึงการทดสอบระบบงานโดยใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป (Generalized Audit Software หรือ GAS) หรือวิทยาการวิเคราะห์ข้อมูล (Data Analytics) ผลจากการวิเคราะห์ข้อมูลจะทำให้ผู้สอบบัญชีทราบว่าระบบงานที่ตรวจสอบมีการควบคุมข้อมูลนำเข้า การประมวลผล และผลลัพธ์อย่างเหมาะสมหรือไม่

  ในการตรวจสอบระบบงาน โดยทั่วไปผู้สอบบัญชีจะแบ่งการตรวจสอบระบบงานเป็นระบบงานหลักๆ เช่น ระบบงานด้านรายได้ รายจ่าย การผลิต เป็นต้น

11. บทสรุป

การควบคุมระบบงานในบทนี้จะเน้นที่การควบคุมข้อมูลนำเข้า การประมวลผล และผลลัพธ์ โดยวัตถุประสงค์ของการควบคุมเพื่อให้มั่นใจว่าระบบงานให้ผลลัพธ์ที่ถูกต้อง ครบถ้วน และผลลัพธ์ได้แจกจ่ายไปยังผู้ที่เกี่ยวข้องที่ได้รับอนุมัติเท่านั้น การควบคุมข้อมูลเข้า ประกอบด้วย การควบคุมการจัดเก็บข้อมูลจากแหล่งกำเนิดรายการ การควบคุมการป้อนข้อมูลและร่องรอยการตรวจสอบของข้อมูลนำเข้า ส่วนการควบคุมการประมวลผล ประกอบด้วย การควบคุมความถูกต้องของการประมวลผล และร่องรอยการตรวจสอบของการประมวลผล สำหรับการควบคุมผลลัพธ์ ประกอบด้วย การควบคุมความถูกต้องครบถ้วนของผลลัพธ์ทั่วไป การควบคุมผลลัพธ์แบบแบตช์ การควบคุมผลลัพธ์แบบออนไลน์ และร่องรอยการตรวจสอบของผลลัพธ์ ส่วนการควบคุมระบบงานที่ใช้งานบนเว็บ ประกอบด้วย (1) สอบทานความสมเหตุสมผลของข้อมูลนำเข้า (2) กำหนดสิทธิ์ในการเข้าถึงฐานข้อมูลอย่างรัดกุม (3) ตรวจสอบช่วงเวลาของผู้ใช้ก่อนที่จะอนุญาตให้เข้าใช้งานได้ (4) ตรวจสอบสิทธิ์ทุกหน้าเว็บที่ต้องการเข้าไปใช้งาน (5) เข้ารหัสข้อมูล (6) ใช้ Whitelist สำหรับตรวจสอบข้อมูลที่เข้ามาว่ามีข้อความที่เป็นการโจมตีในลักษณะ XXE หรือไม่ (7) หลีกเลี่ยงการให้ข้อมูลการอ้างอิง Object ให้กับผู้ใช้ (8) ใช้ค่าของดรรชนีในการอ้างอิง (9) ตรวจสอบการควบคุมการเข้าถึงที่เซิร์ฟเวอร์ (10) สแกนระบบอย่างสม่ำเสมอ (11) ปรับ Security Patch, Service Pack หรือ Hotfix ให้เป็นปัจจุบันอย่างสม่ำเสมอ และ (12) กำหนดให้มีการสอบทานรายการที่ผิดปกติในลงบันทึก ท้ายที่สุดการควบคุมอุปกรณ์เคลื่อนที่ ประกอบด้วย (1) กำหนดนโยบายเกี่ยวกับการนำอุปกรณ์เคลื่อนที่ (2) กำหนดให้มีการติดตั้งโปรแกรมป้องกันไวรัส (3) เข้ารหัสข้อมูลที่มีความอ่อนไหว (4) กำหนดให้การเข้าถึงระบบคอมพิวเตอร์ของกิจการผ่านระบบเครือข่ายต้องทำผ่าน VPN (5) กำหนดให้มีการบริหารจัดการอุปกรณ์เคลื่อนที่เกี่ยวกับการที่อุปกรณ์สูญหายหรือสิ้นสุดสัญญาของเจ้าหน้าที่ (6) กำหนดระดับการเข้าถึงข้อมูล และ (7) สร้างความตระหนักในการรักษาความมั่นคงปลอดภัย

12. บรรณานุกรม

นิตยา วงศ์ภินันท์วัฒนา. (2563). *ความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศ.* (พิมพ์ครั้งที่ 2). สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

InnovizAxapta. (2002). *เอกสารประกอบการบรรยายการติดตั้งระบบ Microsoft Dynamics AX.* มหาวิทยาลัยธรรมศาสตร์, คณะพาณิชยศาสตร์และการบัญชี.

ISACA. (2010). *Securing Mobile Devices*. An ISACA Emerging Technology White Paper, 4-10.

Porter, W. T., & Perry, W. E. (1987). *EDP: Controls and Auditing* (5th Edition). Kent Publisher.

Romney, S. and Steinbart, P. J. (2009). *Accounting information Systems (11th Edition)*. New Jersy: Peason Education, Inc., Upper Saddle River.

Vasarhelyi, M. A., and Lin, T. W. (1988). *Advanced Auditing Fundamentals of EDP and Statistical Audit Technology.* USA:Addison-Wesley Publishing Company, Inc.

Watne, D. A., & Turney, P. B. B. (1990). *Auditing EDP System* (2nd Edition). Prentice Hall.

Weber, R. (1999). *Information Systems Control and Audit.* Prentice Hall.

คณะผู้ทรงคุณวุฒิจัดทำคู่มือด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์

ศ.ดร.ศิริลักษณ์	โรจนกิจอำนวย	ประธานคณะทำงาน
ศ.ดร.นิตยา	วงศ์ภินันท์วัฒนา	คณะทำงาน
ดร.เยาวลักษณ์	ชาติบัญชาชัย	คณะทำงาน
นางปิยะพัชร์	อัศวจินดากรณ์	คณะทำงาน
นางสาวผุสดี	จันทะสุวันนะ	คณะทำงาน
นายพิรุฬน์	กิตติเดชปรีชา	คณะทำงาน
นางสาวรินรัตน์	ภาสเวคิน	คณะทำงาน
นางวราลี	วัฒนวิบูลย์	คณะทำงาน
นายวันชัย	พิทักษ์กรณ์	คณะทำงาน
นางเสาวนีย์	เสตเสถียร	คณะทำงาน
นายอธิษฐ์	ตระกูลเดช	คณะทำงาน

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

เลขที่ 133 ถนนสุขุมวิท 21 (อโศก) แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

0 2685 2500 โทรสาร 0 2685 2501

tfac@tfac.or.th www.tfac.or.th