บทที่ 2

การตรวจสอบกรณีกิจการใช้คอมพิวเตอร์ ประมวลผลข้อมูลและการประเมินความเสี่ยง

การใช้คอมพิวเตอร์ ในการจัดทำและตรวจสอบบัญชี

โดย
ดร.เยาวลักษณ์ ชาติบัญชาชัย

สรุปเนื้อหาของบท

1. วัตถุประสงค์ของการศึกษา

เมื่อได้ศึกษาเนื้อหาของบทนี้แล้ว ผู้ศึกษาควรทราบและเข้าใจถึง

1. หลักการที่สำคัญสำหรับการตรวจสอบกรณีกิจการใช้คอมพิวเตอร์ประมวลผลข้อมูล
2. แนวทางการประเมินความเสี่ยงสำหรับระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผล
3. ขั้นตอนในการประเมินการควบคุมภายในสำหรับระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผล
4. เทคนิคและวิธีการตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผล

2. บทนำ

การตรวจสอบและการประเมินความเสี่ยงกรณีกิจการใช้คอมพิวเตอร์ประมวลผลข้อมูล มีหลักการพื้นฐานเดียวกับการตรวจสอบและการประเมินความเสี่ยงกรณีกิจการใช้ระบบประมวลข้อมูลแบบอื่นๆ แต่วิธีการและเทคนิคที่ใช้ในการตรวจสอบซึ่งรวมถึงการประเมินความเสี่ยงและการประเมินประสิทธิผลการควบคุมภายในจะมีความแตกต่างกันในรายละเอียด เนื่องจากระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการประมวลผลมีลักษณะสำคัญและความเสี่ยงสืบเนื่องที่แตกต่างไปจากระบบที่ประมวลผลด้วยมือ ดังนั้นผู้สอบบัญชีจึงจำเป็นต้องเข้าใจหลักการพื้นฐานที่เกี่ยวข้องกับการประเมินความเสี่ยงและการตรวจสอบ ตลอดถึงลักษณะสำคัญของระบบสารสนเทศที่ใช้ในการประมวลผลซึ่งมีผลกระทบต่อความเสี่ยงและการควบคุมภายในของระบบ ทั้งนี้เพื่อให้ผู้สอบบัญชีสามารถปฏิบัติงานการตรวจสอบตามมาตรฐานการสอบบัญชีได้อย่างมีประสิทธิผลและประสิทธิภาพ

บทนี้กล่าวถึงหลักการพื้นฐานเหล่านี้ โดยเริ่มจากการอธิบายแนวทางในการตรวจสอบระบบสารสนเทศและแนวคิดเกี่ยวกับการควบคุมภายในของระบบสารสนเทศ จากนั้นจึงอธิบายถึงหลักการและแนวทางในการประเมินความเสี่ยงและการควบคุมภายในของระบบสารสนเทศ ตลอดถึงเทคนิคและวิธีการตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการประมวลผล

3. หลักการตรวจสอบกรณีกิจการใช้คอมพิวเตอร์ประมวลผล

การใช้คอมพิวเตอร์ในการประมวลผลของระบบสารสนเทศไม่ทำให้วัตถุประสงค์และขอบเขตในการตรวจสอบเปลี่ยนแปลงไป แต่วิธีการที่ใช้ในการตรวจสอบซึ่งรวมถึงการประเมินความเสี่ยงและประสิทธิผลของการควบคุมภายในจะต้องเปลี่ยนแปลงไปให้เหมาะสมเนื่องจากระบบสารสนเทศซึ่งใช้คอมพิวเตอร์ในการประมวลผลมีลักษณะสำคัญและความเสี่ยงสืบเนื่องที่แตกต่างไปจากระบบที่ประมวลผลด้วยมือ ดังนั้นผู้สอบบัญชีจึงต้องมีความเข้าใจเกี่ยวกับแนวทางในการตรวจสอบ ลักษณะสำคัญของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการประมวลผลและหลักการควบคุมภายในเพื่อให้สามารถที่จะเลือกใช้วิธีการและเทคนิคที่เหมาะสมในการตรวจสอบ

3.1 แนวทางในการตรวจสอบระบบสารสนเทศ (Audit Approach)

การตรวจสอบระบบสารสนเทศของผู้สอบบัญชีมีวัตถุประสงค์เพื่อพิจารณาว่าระบบสารสนเทศที่ใช้ในการประมวลผลข้อมูลที่จำเป็นต่อการจัดทำงบการเงินและการตรวจสอบทำงานตามที่กำหนดไว้และรายการบัญชีที่บันทึกอยู่ในระบบและข้อมูลออกของระบบถูกต้อง ครบถ้วนและสะท้อนสถานะทางการเงินที่แท้จริงของกิจการ

กระบวนการในการตรวจสอบบัญชีกรณีกิจการใช้คอมพิวเตอร์ประมวลผลประกอบด้วย 5 ขั้นตอนหลักเช่นเดียวกับการตรวจสอบบัญชีของกิจการทั่วไปที่ไม่ได้ใช้คอมพิวเตอร์ประมวลผลดังนี้

1. การวางแผนการตรวจสอบขั้นต้นเพื่อกำหนดวัตถุประสงค์และขอบเขตของการตรวจสอบ
2. การสอบทานขั้นต้นเพื่อประเมินประสิทธิผลของโครงสร้างการควบคุมภายในและประเมินความเสี่ยงด้านการควบคุม
3. การสอบทานขั้นสุดท้ายเพื่อประเมินประสิทธิผลการควบคุมภายในและประเมินความเสี่ยงด้านการควบคุมโดยละเอียดและทดสอบการควบคุม
4. การทดสอบรายการ
5. การออกรายงานการตรวจสอบและรายงานถึงผู้บริหาร

ในเบื้องต้นผู้สอบบัญชีของกิจการที่ใช้คอมพิวเตอร์ประมวลผลจำเป็นต้องมีความเข้าใจเกี่ยวกับประเภทของการตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลซึ่งเป็นหลักการพื้นฐานที่ต้องใช้ในการพิจารณาวิธีการและเทคนิคที่เหมาะสมในการ

ตรวจสอบระบบสารสนเทศต่อไป โดยการจัดประเภทของการตรวจสอบระบบสารสนเทศอาจจัดตามวิธีการตรวจสอบและตามวัตถุประสงค์ของการตรวจสอบดังรายละเอียดต่อไปนี้

1) การจัดประเภทการตรวจสอบระบบสารสนเทศตามวิธีการตรวจสอบ

การจัดประเภทของการตรวจสอบระบบสารสนเทศอาจพิจารณาจากวิธีการหลักที่ใช้ในการตรวจสอบโดยจัดเป็นการตรวจสอบรอบระบบและการตรวจสอบผ่านระบบ

1.1 การตรวจสอบรอบระบบ (Auditing Around the Computer)

การตรวจสอบระบบโดยรอบหรือการตรวจสอบข้อมูลนำเข้าและผลลัพธ์ของระบบเป็นการตรวจสอบความถูกต้อง ครบถ้วนของข้อมูลเข้าและผลลัพธ์หรือข้อมูลออกของระบบโดยไม่มีการตรวจสอบการประมวลผลของระบบ การตรวจสอบวิธีนี้เหมาะสมสำหรับระบบที่มีการประมวลผลที่ไม่ซับซ้อนและไม่ได้เชื่อมต่อกับระบบงานอื่น วิธีการนี้อาจไม่สามารถทำได้ในกรณีที่ระบบที่ถูกตรวจสอบมีการประมวลผลที่ซับซ้อนและผลลัพธ์หรือข้อมูลออกของระบบงานหนึ่งมักจะเป็นข้อมูลเข้าของอีกระบบงานหนึ่ง ทำให้ไม่สามารถตรวจสอบระบบงานแต่ละระบบงานแยกจากกันอย่างเป็นอิสระได้

1.2 การตรวจสอบผ่านระบบ (Auditing Through the Computer)

การตรวจสอบผ่านระบบหรือการตรวจสอบการประมวลผลของระบบเป็นการตรวจสอบการประมวลผลของระบบเพื่อให้แน่ใจว่าผลลัพธ์หรือข้อมูลออกของระบบครบถ้วนและถูกต้อง ซึ่งในการตรวจสอบจำเป็นต้องใช้คอมพิวเตอร์เป็นเครื่องมือในการตรวจสอบ ทั้งนี้เนื่องจากระบบงานที่ใช้คอมพิวเตอร์ประมวลผลจะจัดเก็บข้อมูลและหลักฐานเพื่อการตรวจสอบในรูปอิเล็กทรอนิกส์ซึ่งไม่สามารถอ่านและตรวจสอบได้โดยตรงโดยผู้ตรวจสอบ การตรวจสอบวิธีนี้เหมาะสมสำหรับระบบที่มีการประมวลผลที่ซับซ้อนและผลลัพธ์หรือข้อมูลออกของระบบงานหนึ่งเป็นข้อมูลเข้าของอีกระบบงานหนึ่ง

2) การจัดประเภทของการตรวจสอบระบบสารสนเทศตามวัตถุประสงค์ของการตรวจสอบ

วิธีการในการตรวจสอบระบบสารสนเทศอาจจัดประเภทตามวัตถุประสงค์ของการตรวจสอบเป็นการทดสอบการควบคุมและการทดสอบเนื้อหาสาระ

2.1 การทดสอบการควบคุม (Test of Controls)

การทดสอบการควบคุมเป็นการตรวจสอบเพื่อพิจารณาว่าการควบคุมภายในที่วางไว้ทำงานอย่างเหมาะสมตามที่กำหนด ซึ่งรายละเอียดของเทคนิคและวิธีการที่ใช้ในการทดสอบการควบคุมจะอธิบายในหัวข้อเทคนิคและวิธีการตรวจสอบระบบสารสนเทศ

2.2 การทดสอบเนื้อหาสาระ (Substantive Test)

การทดสอบเนื้อหาสาระเป็นการตรวจสอบรายการและยอดคงเหลือตามบัญชีเพื่อพิจารณาว่ารายการและยอดคงเหลือเหล่านั้นแสดงค่าถูกต้องและเหมาะสม โดยทั่วไปความน่าจะเป็นที่ผู้สอบบัญชีจะไม่พบรายการผิดพลาดที่มีสาระสำคัญจะน้อยลงหากระบบที่ถูกตรวจสอบมีการควบคุมภายในที่ดี ดังนั้นผลจากการทดสอบการควบคุมจะมีผลโดยตรงต่อการออกแบบการทดสอบเนื้อหาสาระ กล่าวคือ หากผู้สอบบัญชีสรุปผลจากการทดสอบการควบคุมว่าการควบคุมภายในทำงานตามที่กำหนดไว้ ผู้สอบบัญชีสามารถที่จะลดงานการตรวจสอบความถูกต้องของรายการและยอดคงเหลือตามบัญชีลงได้ ในทางตรงกันข้าม หากผู้สอบบัญชีสรุปผลจากการทดสอบการควบคุมว่าการควบคุมภายในไม่ทำงานตามที่กำหนดไว้ ผู้สอบบัญชีจำเป็นต้องขยายขอบเขตการตรวจสอบความถูกต้องของรายการและยอดคงเหลือตามบัญชีขึ้นเพื่อลดความน่าจะเป็นที่จะไม่สามารถค้นพบรายการผิดพลาดที่มีสาระสำคัญ ซึ่งรายละเอียดของเทคนิคและวิธีการที่ใช้ในการทดสอบเนื้อหาสาระจะอธิบายในหัวข้อเทคนิคและวิธีการตรวจสอบระบบสารสนเทศ

3.2 แนวคิดเกี่ยวกับการควบคุมภายในของระบบสารสนเทศ

ตามหลักการตรวจสอบและการออกแบบการควบคุมภายในที่ยอมรับกันทั่วไปในปัจจุบันจัดว่าความเสี่ยงทางธุรกิจเป็นปัจจัยสำคัญในการกำหนดการควบคุมที่ระบบควรมีตลอดถึงการกำหนดลักษณะ ระยะเวลาและขอบเขตในการตรวจสอบที่เหมาะสม ดังนั้นในเบื้องต้นของการตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการประมวลผล ผู้สอบบัญชีจึงจำเป็นต้องพิจารณาถึงความเสี่ยงของระบบสารสนเทศที่กิจการใช้สนับสนุนกระบวนการหลักทางธุรกิจของกิจการ โดยการประเมินความเสี่ยงของระบบสารสนเทศนี้จะเกี่ยวข้องโดยตรงกับการประเมินโอกาสที่จะเกิดข้อผิดพลาดขึ้นในระบบสารสนเทศ หากระบบไม่มีระบบการควบคุมภายในเลยหรือที่เรียกความเสี่ยงประเภทนี้โดยทั่วไปว่าความเสี่ยงสืบเนื่อง (Inherent Risk) และการประเมินประสิทธิผลของระบบการควบคุม

ภายในที่เกี่ยวข้องกับระบบสารสนเทศของกิจการในการป้องกัน ค้นพบและแก้ไขข้อผิดพลาดหรือรายการผิดปกติที่เกิดขึ้นในเรื่องของความครบถ้วน มีอยู่จริง มูลค่าการแสดงรายการ และความทันต่อเวลาของรายการและข้อมูลในระบบ

ในการนี้ผู้สอบบัญชีจำเป็นต้องมีความรู้และความเข้าใจเกี่ยวกับลักษณะสำคัญในด้านข้อมูลเข้า ประมวลผล การจัดเก็บข้อมูล ข้อมูลออก การสื่อสาร และการใช้ไมโครคอมพิวเตอร์ของระบบสารสนเทศจึงสามารถประเมินความเสี่ยงและประสิทธิผลของการควบคุมภายในของระบบสารสนเทศได้อย่างมีประสิทธิผลและประสิทธิภาพ นอกจากนี้ผู้สอบบัญชีต้องมีความเข้าใจเกี่ยวกับองค์ประกอบ วัตถุประสงค์และประเภทของการควบคุมภายในของระบบสารสนเทศทางการบัญชีด้วย

3.2.1 ลักษณะสำคัญของระบบสารสนเทศที่มีผลต่อการควบคุมภายใน

เนื่องจากระบบสารสนเทศที่ใช้คอมพิวเตอร์ช่วยในการประมวลผลมีความเสี่ยงสืบเนื่องในบางประเด็นเพิ่มเติมจากระบบที่ใช้มือในการประมวลผล ซึ่งความเสี่ยงสืบเนื่องนี้เป็นปัจจัยสำคัญต่อการกำหนดการควบคุมภายในของระบบสารสนเทศของกิจการ ดังนั้นในขั้นตอนแรกของการประเมินประสิทธิผลหรือความเพียงพอของการควบคุมภายในของระบบจึงจำเป็นต้องพิจารณาถึงลักษณะสำคัญของระบบสารสนเทศด้านข้อมูลเข้า การประมวลผล การจัดเก็บข้อมูล ข้อมูลออก การสื่อสาร และการใช้ไมโครคอมพิวเตอร์ ที่ก่อให้เกิดความเสี่ยงแก่กิจการและมีผลในการกำหนดการควบคุมภายในของระบบ

3.2.1.1 ลักษณะสำคัญของระบบสารสนเทศด้านข้อมูลเข้า

ระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลมีลักษณะสำคัญและวิธีการในการนำเข้าข้อมูลที่มีผลต่อการควบคุมภายในของระบบดังนี้

1) การขาดเอกสารขั้นต้นที่ใช้ในการนำข้อมูลเข้า

การนำเข้าข้อมูลของระบบที่ประมวลผลด้วยคอมพิวเตอร์สามารถทำได้โดยที่ไม่จำเป็นต้องมีการจัดทำเอกสารขั้นต้นก่อน เช่น

- การถอนเงินจากเครื่องถอนเงินอัตโนมัติหรือเครื่องเอทีเอ็มจะไม่มีการจัดทำใบถอนเงินที่มีลายเซ็นของผู้ถอนเงินและผู้รับเงิน
- การสั่งซื้อสินค้าหรือบริการผ่านทางอินเทอร์เน็ตจะไม่มีใบสั่งซื้อที่เป็นสำเนากระดาษจากลูกค้าของกิจการ

- การชำระเงินผ่านทางอินเทอร์เน็ตจะไม่มีใบแจ้งการนำส่งเงินจากลูกค้าของกิจการ
- รายการบางรายการอาจทำอัตโนมัติโดยโปรแกรมคอมพิวเตอร์ทำให้ขาดเอกสารขั้นต้นที่ใช้ในการนำข้อมูลเข้า เช่น โปรแกรมระบบงานอาจกำหนดให้มีการจัดทำและส่งคำสั่งซื้อไปยังผู้ขายทันทีที่ระดับปริมาณสินค้าต่ำกว่าระดับที่กำหนดไว้ในเงื่อนไขที่ระบุไว้ในโปรแกรม ทำให้ไม่มีการจัดทำใบขอซื้อก่อนที่จะมีการจัดทำใบสั่งซื้อ หรือโปรแกรมระบบงานอาจกำหนดให้มีการคำนวณค่าเสื่อมราคาและดอกเบี้ยรับทุกสิ้นเดือนตามเงื่อนไขที่ระบุไว้ในโปรแกรมแล้วผ่านรายการโดยอัตโนมัติไปยังบัญชีแยกประเภทที่เกี่ยวข้องทำให้ไม่มีการจัดทำใบสำคัญทั่วไปก่อนที่จะมีการผ่านรายการ

การขาดเอกสารขั้นต้นที่ใช้ในการนำข้อมูลเข้ามีผลทำให้ไม่มีเอกสารที่จะใช้แสดงว่ารายการที่เกิดขึ้นเป็นรายการที่เกิดขึ้นจริงและได้รับการอนุมัติอย่างถูกต้องและไม่มีเอกสารที่สามารถใช้เป็นร่องรอยการตรวจสอบในภายหลัง ดังนั้นในการออกแบบและวิเคราะห์การควบคุมภายในของระบบสารสนเทศจึงต้องพิจารณาว่ารายการประเภทใดที่มีการนำข้อมูลเข้าโดยไม่ต้องมีการจัดทำเอกสารขั้นต้นและมีการควบคุมใดที่ใช้ในการป้องกันหรือค้นหาการนำเข้ารายการที่ไม่ได้เกิดขึ้นจริงหรือรายการที่ไม่ได้รับการอนุมัติอย่างถูกต้อง เช่น การกำหนดให้เฉพาะบุคคลที่มีหน้าที่ในการนำข้อมูลเข้าสามารถใช้โปรแกรมในการนำข้อมูลเข้าและสามารถเปลี่ยนแปลงแฟ้มข้อมูลที่จัดเก็บรายการที่เกี่ยวข้องกับข้อมูลที่นำเข้า การกำหนดให้มีการสอบทานรายการที่นำเข้าสู่ระบบแล้วโดยบุคคลที่ไม่มีหน้าที่ในการนำข้อมูลเข้า เป็นต้น

2) การนำเข้าข้อมูลสู่ระบบทำได้หลายทาง

การนำเข้าข้อมูลสู่ระบบคอมพิวเตอร์อาจสามารถทำได้โดยการใช้โปรแกรมระบบงานหรือการเพิ่มหรือเปลี่ยนแปลงรายการในแฟ้มข้อมูลโดยตรง ดังนั้นระบบที่ใช้คอมพิวเตอร์ประมวลผลจะถือว่าผู้ที่ได้รับอนุมัติให้นำเข้าข้อมูลได้ ได้แก่

- ผู้ที่สามารถเข้าถึงโปรแกรมที่ใช้ในการนำเข้าข้อมูลและมีสิทธิที่จะเปลี่ยนแปลงและปรับปรุงรายการในแฟ้มข้อมูล
- ผู้ที่มีสิทธิที่จะเปลี่ยนแปลงและปรับปรุงโดยตรงโดยไม่ต้องทำรายการผ่านโปรแกรมที่ใช้ในการนำเข้าข้อมูล ซึ่งบุคคลกลุ่มนี้จะต้อง

เป็นผู้ที่มีความรู้เกี่ยวกับระบบสารสนเทศเป็นอย่างดีโดยเฉพาะในส่วนที่เกี่ยวกับโครงสร้างของข้อมูลในระบบและระบบจัดการฐานข้อมูลที่ใช้

ระบบที่ใช้คอมพิวเตอร์ประมวลผลจะถือว่ารายการที่นำเข้าโดยบุคคลดังกล่าวข้างต้นและรายการที่อยู่ในระบบทั้งหมดเป็นรายการที่ได้รับอนุมัติแล้วแม้ว่าบุคคลดังกล่าวข้างต้นบางคนจะเป็นผู้ที่ไม่ได้รับอนุมัติให้มีหน้าที่ในการนำข้อมูลเข้าระบบก็ตาม ทั้งนี้บุคคลที่ไม่ได้รับอนุมัติให้นำข้อมูลเข้าระบบเหล่านี้อาจทำการนำเข้าข้อมูลที่ไม่ได้รับอนุมัติหรือเปลี่ยนแปลงแก้ไขข้อมูลในระบบโดยที่ไม่ได้รับอนุมัติ โดยระบบจะไม่สามารถแยกแยะได้ว่ารายการเหล่านั้นเป็นรายการที่ได้รับอนุมัติหรือไม่ได้รับอนุมัติ เนื่องจากระบบถือว่าบุคคลที่สามารถเข้าถึงแฟ้มข้อมูลหรือโปรแกรมระบบงานที่ใช้ในการนำเข้าข้อมูลเป็นบุคคลที่ได้รับอนุมัติให้นำเข้าข้อมูลได้ดังกล่าวข้างต้น ดังนั้นจึงจำเป็นอย่างยิ่งที่ระบบสารสนเทศจะต้องมีการควบคุมเพื่อป้องกันไม่ให้มีการนำเข้าข้อมูลที่ไม่ได้รับการอนุมัติโดยการจำกัดสิทธิการเข้าถึงแฟ้มข้อมูลหรือโปรแกรมระบบงานที่ใช้ในการนำเข้าข้อมูลกับบุคคลที่ไม่มีหน้าที่ในการนำข้อมูลเข้าและมีการควบคุมเพื่อค้นหาการนำเข้าข้อมูลที่ไม่ได้รับการอนุมัติ เช่น การกำหนดให้มีการสอบทานรายการที่นำเข้าสู่ระบบแล้วว่าเป็นไปตามเงื่อนไขการอนุมัติรายการโดยบุคคลที่ไม่มีหน้าที่ในการนำข้อมูลเข้า เป็นต้น

3) การนำเข้าข้อมูลสู่ระบบต้องใช้อุปกรณ์นำเข้าข้อมูล

เนื่องจากการนำเข้าข้อมูลของระบบสารสนเทศจำเป็นต้องมีการนำข้อมูลผ่านทางหน้าจอหรืออุปกรณ์นำเข้าข้อมูลอื่น เช่น สแกนเนอร์หรือเครื่องกราดตรวจ (Scanners) เครื่องอ่านอักขระด้วยแสง (Optical Character Readers) เครื่องอ่านอักขระหมึกแม่เหล็ก (Magnetic Ink Character Readers) เป็นต้น อุปกรณ์คอมพิวเตอร์ที่ใช้ในการนำข้อมูลเข้าเหล่านี้อาจเป็นแหล่งใหม่ที่ก่อให้เกิดการนำเข้าข้อมูลที่ผิดพลาดหรือไม่ถูกต้อง เช่น

- หน้าจอที่ใช้ในการนำเข้าข้อมูลอาจจะไม่ได้ออกแบบให้เข้าใจง่ายและง่ายต่อการใช้ ทำให้ผู้ปฏิบัติงานเข้าใจผิดและนำเข้าข้อมูลที่ไม่ถูกต้องหรือไม่สม่ำเสมอ เช่น ข้อมูลวันที่อาจถูกนำเข้าในรูปวันเดือนปี หรือปีเดือนวัน หรือเดือนวันปี เนื่องจากไม่ได้มีการกำหนดรูปแบบที่ต้องการให้เห็นเด่นชัดในหน้าจอที่ใช้ในการนำข้อมูลเข้า การนำเข้าข้อมูลปริมาณสินค้าที่ขายหรือรับที่ผิดพลาดเนื่องจากไม่ได้มีการกำหนดหน่วยวัดที่ชัดเจนในหน้าจอที่ใช้ในการนำข้อมูลเข้า เป็นต้น

- หน้าจอที่ใช้ในการนำเข้าข้อมูลอาจการกำหนดเนื้อที่ที่ไม่เพียงพอสำหรับข้อมูลที่ต้องนำเข้าทำให้ข้อมูลที่นำเข้าไม่ครบถ้วน
- หน้าจอที่ออกแบบไว้อาจไม่ได้รวมข้อมูลบางรายการที่ต้องนำเข้าทำให้ไม่มีการนำเข้าข้อมูลรายการเหล่านั้น
- โปรแกรมที่ใช้ในการรับข้อมูลเข้าอาจจะไม่ได้ออกแบบให้สามารถตรวจสอบหาข้อมูลนำเข้าที่มีข้อผิดพลาดหรือไม่ครบถ้วน เช่น การบันทึกรายการเกี่ยวกับลูกค้ารายใหม่ซึ่งอาจเป็นลูกค้าเดิมที่มีอยู่ในระบบแล้วแต่ระบบไม่ได้มีการตรวจสอบก่อนว่ามีลูกค้ารายนั้นอยู่ในระบบแล้ว การนำเข้าข้อมูลจำนวนเงินที่เป็นตัวอักษรแทนที่จะเป็นตัวเลข การบันทึกรายการสำหรับลูกหนี้ที่ไม่มีอยู่ในระบบเนื่องจากไม่มีการตรวจสอบรหัสลูกหนี้และชื่อของลูกหนี้ก่อนว่าเป็นลูกหนี้ที่มีอยู่ในระบบแล้วและเป็นลูกหนี้รายที่ต้องการบันทึกรายการ เป็นต้น
- โปรแกรมที่ใช้ในการรับข้อมูลเข้าอาจมีตรรกะที่ไม่ถูกต้องทำให้การรับและแปลงค่าของข้อมูลเข้าไม่ถูกต้อง เช่น ขนาดของตัวแปรที่ใช้ในการรับข้อมูลเข้าอาจกำหนดไว้น้อยไปทำให้มีการตัดส่วนข้อมูลบางส่วนไป เป็นต้น

ดังนั้นในการประเมินประสิทธิผลของการควบคุมภายในของระบบสารสนเทศจึงต้องพิจารณาถึงวิธีการที่ใช้ในการนำข้อมูลเข้าสู่ระบบ ความเสี่ยงหรือโอกาสที่จะเกิดการนำเข้าข้อมูลที่ผิดพลาดหรือไม่ถูกต้องและการควบคุมเพื่อป้องกัน ค้นหาและแก้ไขข้อมูลที่ผิดพลาดหรือไม่ถูกต้องอย่างทันเวลา เช่น การออกแบบหน้าจอที่ใช้ในการนำเข้าข้อมูลให้เข้าใจง่าย ง่ายต่อการใช้และมีเนื้อที่ที่เพียงพอสำหรับข้อมูลที่ต้องนำเข้า การออกแบบให้โปรแกรมที่ใช้ในการรับข้อมูลเข้าสามารถตรวจสอบหาข้อมูลนำเข้าที่มีข้อผิดพลาดหรือไม่ครบถ้วน เป็นต้น

3.2.1.2 ลักษณะสำคัญของระบบสารสนเทศด้านการประมวลผล

ระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลมีลักษณะสำคัญและวิธีการในการประมวลผลที่มีผลต่อการควบคุมภายในของระบบดังนี้

1) ระบบคอมพิวเตอร์ไม่มีวิจารณญาณ

ระบบคอมพิวเตอร์ในปัจจุบันยังไม่ได้รับการพัฒนาให้ถึงขั้นที่สามารถคิดและมีวิจารณญาณเองได้ การประมวลผลของระบบจึงเป็นไปตามคำสั่งที่กำหนด

ไว้ในโปรแกรม ดังนั้นระบบจึงไม่สามารถระบุรายการที่ผิดจากปกติได้หากโปรแกรมที่ใช้ในการประมวลผลไม่ได้ระบุเงื่อนไขในการค้นหารายการที่ผิดปกติต่างๆ ไว้ ซึ่งต่างจากระบบที่ประมวลผลด้วยมือที่ผู้ปฏิบัติงานมีโอกาสที่จะสังเกตเห็นและระบุข้อผิดพลาดหรือข้อมูลที่น่าสงสัยว่าจะไม่ครบถ้วนหรือผิดจากปกติได้ เช่น ผลลัพธ์ออกที่ระบุว่าดอกเบี้ยรับของงวดมียอดเงินจำนวนสูงมากเนื่องจากระบบอาจคำนวณจำนวนวันที่ใช้ในการคิดดอกเบี้ยไม่ถูกต้องซึ่งเป็นผลมาจากปัญหาปี ค.ศ. 2000 ระบบคอมพิวเตอร์จะไม่สามารถทราบได้ว่ามีความผิดพลาดเกิดขึ้นในการประมวลผลแล้ว หากการคำนวณดอกเบี้ยรับทำด้วยมือและยอดดอกเบี้ยรับที่คำนวณได้ไม่ถูกต้อง ผู้ปฏิบัติงานอาจจะสังเกตได้ทันทีว่าการคำนวณอาจไม่ถูกต้องเนื่องจากยอดเงินที่คำนวณได้ต่างจากงวดก่อนๆ มากหรือยอดดอกเบี้ยรับที่คำนวณได้ไม่สัมพันธ์กับยอดเงินต้น เป็นต้น ดังนั้นระบบสารสนเทศจึงจำเป็นต้องมีการกำหนดเงื่อนไขการตรวจสอบและค้นหารายการที่ผิดปกติต่างๆ ที่อาจเกิดขึ้นไว้ภายในโปรแกรมที่ใช้ในการประมวลผล ตลอดทั้งมีการกำหนดขั้นตอนและวิธีการในการสอบทานผลลัพธ์ออกที่ได้จากการประมวลผล

2) การรวมหน้าที่ต่างๆ เข้าด้วยกันเมื่อใช้ระบบคอมพิวเตอร์ในการประมวลผล

หลักการแบ่งแยกหน้าที่เป็นหลักการเบื้องต้นที่สำคัญของการควบคุมภายใน หน้าที่ที่ต้องแบ่งแยกกันในระบบที่ประมวลผลด้วยมืออาจทำโดยคอมพิวเตอร์ทั้งหมด เช่น การใช้คอมพิวเตอร์ในการประมวลผลระบบเจ้าหนี้และจ่ายเงิน คอมพิวเตอร์อาจจะทำหน้าที่ในการบันทึกรายการเจ้าหนี้ในบัญชีแยกประเภทย่อย ตรวจสอบใบแจ้งหนี้กับเอกสารการสั่งซื้อและการรับของเพื่อทำการจ่ายเงิน และจัดทำเช็คหรือโอนเงินให้แก่ผู้ขายโดยอัตโนมัติ ซึ่งจุดนี้อาจก่อให้เกิดความเสี่ยงในการควบคุมภายในได้หากมีผู้สามารถเข้ามาควบคุมการประมวลผลทั้งหมดของระบบได้ เช่น

- การที่บุคคลใดบุคคลหนึ่งซึ่งมีหน้าที่ในการบันทึกรายการบัญชีเจ้าหนี้สามารถเปลี่ยนแปลงและแก้ไขโปรแกรมที่ใช้ในการประมวลผลระบบเจ้าหนี้และจ่ายเงินทำให้ระบบงานไม่มีการตรวจสอบว่าปริมาณสินค้าที่ระบุในใบแจ้งหนี้ตรงกับปริมาณสินค้าที่กิจการได้รับแล้ว
- การที่บุคคลใดบุคคลหนึ่งซึ่งมีหน้าที่ในการบันทึกรายการบัญชีเจ้าหนี้สามารถเปลี่ยนแปลงและแก้ไขโปรแกรมที่ใช้ในการประมวลผลระบบเจ้าหนี้และจ่ายเงินทำให้ระบบงานไม่มีการตรวจสอบว่าราคาสินค้าที่ระบุในใบแจ้งหนี้ตรงกับราคาสินค้าที่ระบุในใบสั่งซื้อ

- การที่บุคคลใดบุคคลหนึ่งซึ่งมีหน้าที่ในการจัดทำเช็คสามารถเข้าถึงข้อมูลในระบบและทำการเปลี่ยนแปลงข้อมูลเกี่ยวกับชื่อและที่อยู่ของเจ้าหนี้ ทำให้มีการพิมพ์และจัดส่งเช็คไปให้ผู้อื่นที่ไม่ใช่เจ้าหนี้ที่แท้จริง
- การที่บุคคลใดบุคคลหนึ่งซึ่งมีหน้าที่ในการจัดซื้อสามารถเข้าถึงข้อมูลในระบบและทำการเปลี่ยนแปลงข้อมูลเกี่ยวกับการสั่งซื้อทำให้มีการสั่งซื้อที่ไม่ตรงกับความต้องการของกิจการ
- การที่บุคคลใดบุคคลหนึ่งซึ่งมีหน้าที่ในการจัดซื้อหรือตั้งหนี้สามารถเข้าถึงข้อมูลในระบบและทำการเปลี่ยนแปลงข้อมูลเกี่ยวกับการรับของทำให้ปริมาณสินค้าที่ปรากฏในระบบไม่ตรงกับปริมาณสินค้าที่กิจการได้รับจริง

ดังนั้นในระบบที่ใช้คอมพิวเตอร์ประมวลผลจึงยังจำเป็นต้องมีการแบ่งแยกหน้าที่ แต่เป็นการแบ่งแยกหน้าที่ในรูปแบบที่แตกต่างไปจากระบบที่ประมวลผลด้วยมือ เช่น ผู้พัฒนาระบบงานหรือโปรแกรมเมอร์ซึ่งเป็นผู้ที่มีความรู้เกี่ยวกับโปรแกรมระบบงานเป็นอย่างดี ไม่ควรมีหน้าที่ในการประมวลผลข้อมูลและการปฏิบัติการ เนื่องจากผู้ปฏิบัติหน้าที่ในการประมวลผลข้อมูลจำเป็นต้องสามารถใช้โปรแกรมและสามารถเปลี่ยนแปลงแก้ไขข้อมูลในระบบที่เกี่ยวข้องได้และผู้รับผิดชอบด้านการปฏิบัติการจำเป็นต้องสามารถเข้าถึงโปรแกรมในระบบที่ใช้งานจริงได้ หากให้โปรแกรมเมอร์รับผิดชอบในการประมวลผลและการปฏิบัติการ โปรแกรมเมอร์จะสามารถเปลี่ยนแปลงแก้ไขโปรแกรมและข้อมูลในระบบที่ใช้งานจริงได้ เป็นต้น

3) คอมพิวเตอร์สามารถประมวลผลได้อย่างรวดเร็ว

ระบบที่ใช้คอมพิวเตอร์ประมวลผลสามารถประมวลผลได้อย่างรวดเร็ว ทำให้สามารถประมวลผลข้อมูลได้จำนวนมากกว่าการประมวลผลที่ทำด้วยมือ ในกรณีที่ผู้ปฏิบัติงานคนใดคนหนึ่งตั้งใจที่จะทำรายการผิดปกติหรือผู้ปฏิบัติงานมีข้อบกพร่องในการปฏิบัติงาน เช่น ขาดความเข้าใจหรือเข้าใจผิดเกี่ยวกับขั้นตอนในการตรวจสอบก่อนที่จะประมวลผลต่อ ละเลยที่จะทำขั้นตอนใดขั้นตอนหนึ่งที่จำเป็นในระหว่างการประมวลผล เป็นต้น ข้อผิดพลาดหรือรายการผิดปกติที่เกิดขึ้นจึงมีแนวโน้มที่จะมีจำนวนมากกว่ากรณีที่การประมวลผลทำด้วยมือ ดังนั้นระบบสารสนเทศจึงจำเป็นต้องมีการควบคุมเพื่อลดความเสี่ยงจากการที่ผู้ปฏิบัติงานสามารถประมวลรายการจำนวนสูงขึ้น เช่น การเลือกสรรพนักงานที่มีคุณสมบัติตรงกับลักษณะของงานเข้าปฏิบัติงาน การจัดอบรมพนักงาน

เพื่อพัฒนาความรู้และทักษะในการปฏิบัติงาน การจัดทำเอกสารเพื่อให้พนักงานสามารถใช้อ้างอิงในการปฏิบัติงาน การติดตามและดูแลการปฏิบัติงานอย่างใกล้ชิดโดยผู้บังคับบัญชา เป็นต้น

4) องค์ประกอบของระบบนอกเหนือจากผู้ปฏิบัติงานอาจก่อให้เกิดข้อผิดพลาดได้

ในระบบที่ใช้คอมพิวเตอร์ประมวลผล ข้อผิดพลาดอาจจะเกิดจากปัจจัยอื่นนอกเหนือจากผู้ปฏิบัติงาน ได้แก่ ฮาร์ดแวร์ที่ใช้ ระบบปฏิบัติการ โปรแกรมระบบงานและส่วนประกอบอื่นของระบบ หากองค์ประกอบเหล่านี้มีปัญหาก็อาจมีผลทำให้การประมวลผลไม่ถูกต้องหรือไม่ครบถ้วนได้ เช่น

- ฮาร์ดแวร์อาจหยุดทำงานกลางคันทำให้ข้อมูลในระบบได้รับการปรับปรุงไม่ครบถ้วน
- ระบบปฏิบัติการอาจมีข้อบกพร่องทำให้การปรับปรุงแฟ้มข้อมูลของระบบไม่ครบถ้วน
- โปรแกรมระบบงานอาจมีตรรกะไม่ถูกต้องทำให้การประมวลผลไม่ถูกต้อง

ดังนั้นระบบสารสนเทศจึงจำเป็นต้องมีการควบคุมเพื่อลดความเสี่ยงจากการที่ส่วนประกอบระบบที่นอกเหนือจากผู้ปฏิบัติงานจะทำงานผิดพลาด เช่น การทดสอบการทำงานของส่วนประกอบระบบก่อนนำไปใช้งานจริง การกำหนดขั้นตอนการฟื้นฟูระบบ การจัดทำแผนสำรองเผื่อฉุกเฉินสำหรับกรณีที่เกิดเหตุการณ์ฉุกเฉินขึ้น เป็นต้น

5) การทดสอบระบบงานอาจไม่ครบถ้วนกรณีที่ระบบมีความซับซ้อนมาก

โปรแกรมระบบงานมีแนวโน้มที่จะซับซ้อนมากขึ้นตามลำดับ ซึ่งอาจมีผลทำให้ไม่สามารถที่จะทดสอบโปรแกรมระบบงานที่พัฒนาขึ้นได้ทุกเงื่อนไขก่อนนำไปใช้งานจริง ดังนั้นจึงมีความเป็นไปได้ที่โปรแกรมระบบงานที่ใช้จะประมวลผลผิดพลาดได้โดยผู้ใช้ไม่ทราบ ซึ่งข้อผิดพลาดที่อยู่ในโปรแกรมระบบงานจะมีผลกระทบต่อความถูกต้องในการประมวลผลสูงเนื่องจากรายการที่มีลักษณะเหมือนกันจะได้รับการประมวลผลด้วยขั้นตอนและคำสั่งแบบเดียวกัน ดังนั้นรายการทุกรายการที่ถูกประมวลผลด้วยโปรแกรมที่มีข้อผิดพลาดย่อมได้รับการประมวลผลที่ผิดพลาดทุกรายการ ดังนั้นระบบสารสนเทศจึงจำเป็นต้องมีการควบคุมเพื่อลดความเสี่ยงจากการที่โปรแกรมระบบงานจะทำงานผิดพลาดโดยผู้ใช้ไม่ทราบ เช่น การกำหนดให้มีการสอบทานความถูกต้องของผลลัพธ์

ออกอย่างสม่ำเสมอ การกำหนดให้ระบบจัดทำร่องรอยการตรวจสอบเพื่อให้สามารถติดตามการประมวลผลรายการของระบบได้ เป็นต้น

6) การรักษาความปลอดภัยของระบบปฏิบัติการ

มาตรการรักษาความปลอดภัยของระบบที่ใช้คอมพิวเตอร์ประมวลผลส่วนหนึ่งขึ้นอยู่กับการกำหนดการรักษาความปลอดภัยในระดับระบบปฏิบัติการด้วย ตัวอย่างของมาตรการรักษาความปลอดภัยที่สามารถกำหนดในระดับระบบปฏิบัติการ เช่น

- การกำหนดให้ต้องมีการใช้รหัสผู้ใช้และรหัสผ่านในการเข้าถึงระบบ
- การกำหนดเงื่อนไขในการตั้งรหัสผ่านที่ยากต่อการเดา เช่น ห้ามตรงกับรหัสผู้ใช้ ต้องมีอย่างน้อย 5-8 ตัวอักษร เป็นต้น
- การกำหนดเงื่อนไขให้ต้องมีการเปลี่ยนรหัสผ่านในเวลาที่เหมาะสม เช่น กำหนดให้ต้องเปลี่ยนรหัสผ่านทุก 60 วัน
- การกำหนดเงื่อนไขในกรณีที่ใส่รหัสผ่านผิดพลาด เช่น หากใส่รหัสผ่านผิดพลาดเกิน 3 ครั้งให้ยกเลิกผู้ใช้รายนั้น
- การกำหนดสิทธิในการเข้าถึงโปรแกรมและแฟ้มข้อมูลของระบบตามความจำเป็นของผู้ใช้ระบบแต่ละราย
- การกำหนดให้ระบบบันทึกหลักฐานในการติดตามเพื่อการตรวจสอบ (Audit Trail)

หากการรักษาความปลอดภัยที่ระดับระบบปฏิบัติการไม่มีประสิทธิผล เช่น ผู้ใช้ระบบสามารถเข้าถึงระบบได้โดยไม่ต้องใช้รหัสผ่าน ไม่มีการให้สิทธิในการใช้ทรัพยากรของระบบตามความจำเป็นในการปฏิบัติงานทำให้ผู้ใช้ได้รับสิทธิในการเข้าถึงโปรแกรมและข้อมูลเกินกว่าที่ควรจะได้รับ เป็นต้น ผู้ที่ไม่ได้รับอนุมัติอาจสามารถเข้าถึงโปรแกรมและข้อมูลในระบบทำให้ระบบประมวลผลผิดพลาดไปจากที่ควรจะเป็นได้ ดังนั้นระบบสารสนเทศจึงจำเป็นต้องมีการควบคุมให้ระบบปฏิบัติการมีความปลอดภัยเพื่อลดความเสี่ยงจากการที่บุคคลที่ไม่ได้รับอนุมัติจะสามารถเข้าถึงระบบและใช้ทรัพยากรของระบบโดยไม่ได้รับอนุมัติ เช่น การกำหนดนโยบายและมาตรฐานสำหรับรหัสผู้ใช้และรหัสผ่าน การกำหนดนโยบายในการให้สิทธิในการเข้าถึงทรัพยากรของระบบ การกำหนดให้ระบบจัดทำร่องรอยการตรวจสอบเพื่อให้สามารถติดตามการเข้าถึงและการใช้ทรัพยากรของระบบได้ เป็นต้น

3.2.1.3 ลักษณะสำคัญของระบบสารสนเทศด้านการจัดเก็บข้อมูล

ระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลมีลักษณะสำคัญและวิธีการในการจัดเก็บข้อมูลที่มีผลต่อการควบคุมภายในของระบบดังนี้

1) การขาดบันทึกและร่องรอยการตรวจสอบ

เมื่อมีการใช้คอมพิวเตอร์ในการประมวลผล บันทึกและร่องรอยการตรวจสอบซึ่งเป็นหลักฐานที่แสดงความเป็นมาของรายการและการประมวลผลของรายการมักอยู่ในรูปแบบที่อ่านได้ด้วยคอมพิวเตอร์เท่านั้น นอกจากนี้ระบบสารสนเทศบางระบบอาจไม่ได้รับการออกแบบให้จัดเก็บร่องรอยการตรวจสอบไว้หรือได้รับการออกแบบให้มีการจัดเก็บร่องรอยการตรวจสอบเพียงช่วงระยะเวลาหนึ่งเท่านั้นเนื่องจากการจัดเก็บร่องรอยการตรวจสอบมักจำเป็นต้องใช้เนื้อที่จัดเก็บภายในระบบเป็นจำนวนมาก ซึ่งมีผลทำให้การตรวจสอบความถูกต้องการอ้างอิงและการวิเคราะห์ข้อมูลที่แสดงในรายงานต่างๆทำได้ยาก ดังนั้นในตรวจสอบระบบสารสนเทศจึงจำเป็นต้องพิจารณาถึงบันทึกและร่องรอยการตรวจสอบที่ระบบควรมี และระยะเวลาที่บันทึกและร่องรอยการตรวจสอบควรได้รับการจัดเก็บไว้เพื่อให้สามารถติดตามการเข้าถึง การใช้ทรัพยากรของระบบและการประมวลผลรายการที่จำเป็นได้

2) ข้อมูลสามารถถูกเปลี่ยนแปลงโดยปราศจากร่องรอย

ในระบบที่ใช้คอมพิวเตอร์ประมวลผล ข้อมูลและโปรแกรมที่จัดเก็บอยู่ในระบบและสื่อสามารถถูกเปลี่ยนแปลงแก้ไขได้โดยระบบไม่บันทึกร่องรอยไว้ที่หน่วยความจำหรือที่สื่อที่ข้อมูลที่ถูกเปลี่ยนแปลงจัดเก็บอยู่ ซึ่งต่างจากการเปลี่ยนแปลงแก้ไขข้อมูลในระบบที่ใช้มือประมวลผลที่ร่องรอยการแก้ไขจะสามารถเห็นได้ชัดเจนกว่า เช่น รอยลบหรือสีหมึกที่ต่างไป เป็นต้น ดังนั้นในการตรวจสอบระบบสารสนเทศจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อค้นหาร่องรอยการแก้ไขที่เกิดขึ้นได้ เช่น การกำหนดให้ระบบมีการจัดทำร่องรอยการตรวจสอบเพื่อให้สามารถติดตามการเข้าถึง การใช้ทรัพยากรของระบบและการประมวลผลรายการที่จำเป็นได้ ตลอดถึงการกำหนดให้มีการสอบทานร่องรอยการตรวจสอบอย่างเหมาะสมและทันต่อเวลา เป็นต้น

3) การรวบรวมข้อมูลไว้ที่เดียวกันในระบบหรือบนสื่อ

ในระบบที่ใช้คอมพิวเตอร์ประมวลผล ข้อมูลมักถูกจัดเก็บรวมกันไว้ในระบบและไว้ในสื่อซึ่งในปัจจุบันมีขนาดเล็กลงและสามารถบรรจุข้อมูลได้เป็น

จำนวนมากขึ้นเรื่อยๆ นอกจากนี้ข้อมูลอาจถูกจัดเก็บรวมกันในระบบที่สามารถเข้าถึงระบบแบบระยะไกล (Remote Access) ด้วย การจัดเก็บข้อมูลในลักษณะข้างต้นนี้ทำให้ข้อมูลง่ายต่อการถูกขโมยมากกว่ากรณีที่ข้อมูลถูกจัดเก็บในสื่อที่เป็นกระดาษ ดังนั้นในการตรวจสอบระบบสารสนเทศจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงจากการที่ข้อมูลของระบบจะถูกขโมย เช่น การกำหนดให้ต้องมีการใช้รหัสผ่านในการเข้าถึงระบบ การจำกัดสิทธิในการเข้าถึงข้อมูลของระบบตามหน้าที่ของผู้ปฏิบัติงาน การจัดเก็บสื่อที่ใช้ในการจัดเก็บข้อมูลและการติดตั้งระบบคอมพิวเตอร์ในที่ปลอดภัยและยากต่อการเข้าถึงโดยผู้ที่ไม่ได้รับอนุมัติ การกำหนดให้ระบบมีการจัดทำร่องรอยการตรวจสอบเพื่อให้สามารถติดตามการเข้าถึงและการใช้ทรัพยากรของระบบได้ตลอดถึงการกำหนดให้มีการสอบทานร่องรอยการตรวจสอบอย่างเหมาะสมและทันต่อเวลา เป็นต้น

4) การจัดเก็บข้อมูลในรูปของอิเล็กทรอนิกส์

การที่ข้อมูลของระบบที่ใช้คอมพิวเตอร์ประมวลผลจำเป็นต้องเก็บอยู่ในรูปของอิเล็กทรอนิกส์ทำให้ง่ายต่อการสูญหายเนื่องจากการทำรายการหรือการทำงานของระบบที่ผิดพลาดเพียงเล็กน้อยอาจทำให้ข้อมูลทั้งหมดถูกลบทิ้งจากระบบได้ นอกจากนี้ข้อมูลที่อยู่ในรูปของอิเล็กทรอนิกส์ยังอาจถูกลบหรือทำลายโดยตั้งใจหรือไม่ตั้งใจหากสื่อที่เก็บข้อมูลถูกคลื่นแม่เหล็ก ดังนั้นในการออกแบบและวิเคราะห์ระบบสารสนเทศจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงจากการที่ข้อมูลของระบบจะถูกทำลายหรือสูญหายทั้งที่เกิดโดยตั้งใจและไม่ตั้งใจ เช่น การจัดเก็บสื่อที่ใช้ในการจัดเก็บข้อมูลในที่ปลอดภัยจากความร้อน ความชื้น และคลื่นแม่เหล็ก การจัดให้มีการสำรองข้อมูลอย่างสม่ำเสมอ การกำหนดให้มีการทดสอบการฟื้นฟูข้อมูลที่สำรองไว้ การกำหนดให้มีการใช้วิธีการป้องกันการลบข้อมูลจากแฟ้มข้อมูลโดยไม่ตั้งใจ โดยให้ระบบส่งข้อความยืนยันกับผู้ใช้ก่อนที่จะทำการลบข้อมูล การกำหนดสิทธิในการเข้าถึงข้อมูลอย่างเหมาะสม เป็นต้น

3.2.1.4 ลักษณะสำคัญของระบบสารสนเทศด้านข้อมูลออก

ระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลมีลักษณะสำคัญและวิธีการในด้านข้อมูลออกที่มีผลต่อการควบคุมภายในของระบบดังนี้

1) การให้ความเชื่อถือข้อมูลออกของระบบคอมพิวเตอร์

ผู้ใช้โดยมากเชื่อว่าข้อมูลออกของระบบคอมพิวเตอร์ถูกต้องจึงมักไม่ได้ทำการตรวจสอบหรือสอบทาน ดังนั้นจึงไม่พบข้อมูลออกที่ไม่ถูกต้องในกรณีที่การทำงานของระบบคอมพิวเตอร์มีปัญหาหรือมีการเปลี่ยนแปลงแก้ไขข้อมูลหรือโปรแกรมงานที่ไม่ได้รับการอนุมัติ ดังนั้นในการตรวจสอบระบบสารสนเทศจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงที่ผู้ใช้ให้ความเชื่อถือข้อมูลออกของระบบคอมพิวเตอร์โดยไม่ได้ทำการตรวจสอบหรือสอบทานที่จำเป็น เช่น การกำหนดขั้นตอนและผู้รับผิดชอบในการสอบทานข้อมูลออก การออกแบบให้ระบบจัดทำรายงานสรุปข้อผิดพลาดหรือข้อยกเว้น ตลอดถึงการกำหนดให้มีการสอบทานรายงานสรุปข้อผิดพลาดหรือข้อยกเว้นอย่างเหมาะสมและทันต่อเวลา เป็นต้น

2) การขาดผลที่สามารถมองเห็นได้จากการประมวลผลของคอมพิวเตอร์

ในการประมวลผลแต่ละขั้นตอน ผลหรือข้อมูลออกที่ได้อาจเก็บอยู่ภายในระบบที่ไม่สามารถเห็นได้ ซึ่งข้อมูลดังกล่าวอาจจะไม่ตรงกับความเป็นจริง เช่น ระบบอาจสามารถแสดงเฉพาะยอดรวมสุดท้ายที่ได้จากการประมวลผลโดยไม่มีการแสดงรายละเอียดประกอบยอดดังกล่าว การตรวจสอบความถูกต้องจึงไม่สามารถทำได้โดยง่าย ดังนั้นในการตรวจสอบระบบสารสนเทศจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงจากการที่ผลหรือข้อมูลออกที่ได้อาจเก็บอยู่ภายในระบบที่ไม่สามารถเห็นได้ เช่น การกำหนดให้ระบบมีการจัดทำและจัดเก็บร่องรอยการตรวจสอบเพื่อให้สามารถติดตามการประมวลผลรายการได้ซึ่งรวมถึงการจัดทำรายงานประกอบยอดต่างๆ ด้วย เป็นต้น

3.2.1.5 ลักษณะสำคัญของระบบสารสนเทศด้านการสื่อสาร

ระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลมีลักษณะสำคัญและวิธีการในด้านการสื่อสารข้อมูลที่มีผลต่อการควบคุมภายในของระบบดังนี้

1) ความเชื่อถือได้ของระบบโทรคมนาคม

ระบบคอมพิวเตอร์ในปัจจุบันมีการเชื่อมต่อระหว่างระบบกันมากขึ้นและระบบโดยมากเปิดโอกาสให้ผู้ใช้สามารถเข้าถึงระบบแบบระยะไกลได้ ซึ่งมีผลทำให้ต้องอิงระบบโทรคมนาคมมากขึ้น เช่น การเชื่อมต่อระบบหรือการเข้าถึงระบบผ่านระบบโทรศัพท์หรือดาวเทียม ดังนั้นความเชื่อถือได้ของระบบโทร

คมนาคมจึงมีผลโดยตรงต่อความสามารถในการทำงานอย่างสม่ำเสมอและถูกต้องของระบบคอมพิวเตอร์ ในการตรวจสอบระบบสารสนเทศจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงจากการที่ระบบโทรคมนาคมไม่สามารถทำงานอย่างน่าเชื่อถือได้ เช่น การทดสอบการทำงานของระบบก่อนใช้งานจริง การติดตั้งอุปกรณ์เพิ่มเติมและการจัดทำรายงานหรือร่องรอยการตรวจสอบเพื่อติดตามการทำงานของระบบเชื่อมต่อและเพื่อให้สามารถระบุจุดที่มีปัญหา การจัดทำแผนสำรองเผื่อฉุกเฉินสำหรับกรณีที่ระบบโทรคมนาคมหลักไม่สามารถใช้งานได้ เป็นต้น

2) การเข้าถึงระบบผ่านระบบโทรคมนาคม

การที่ระบบคอมพิวเตอร์สามารถเข้าถึงได้ผ่านทางระบบโทรคมนาคมเพิ่มโอกาสที่บุคคลภายนอกที่ไม่ได้รับอนุมัติจะสามารถเข้าถึงระบบได้ง่ายขึ้น เนื่องจากระบบโทรคมนาคมเป็นระบบสาธารณูปโภคพื้นฐานที่เป็นสาธารณะ เช่น ระบบของกิจการอาจสามารถเข้าถึงได้โดยการเรียกเลขหมาย (Dial-up) และใช้โมเด็ม ดังนั้นผู้ที่ทราบเลขหมายโทรศัพท์ที่ต่อกับระบบคอมพิวเตอร์ของกิจการจะสามารถเรียกเลขหมายดังกล่าวเพื่อเชื่อมต่อเข้าระบบ หากบุคคลดังกล่าวสามารถใส่รหัสผู้ใช้และรหัสผ่านที่ถูกต้อง บุคคลนั้นจะสามารถเข้าถึงทรัพยากรที่อยู่ในระบบได้ทันที ดังนั้นการกำหนดให้ต้องมีการใช้รหัสผ่านและการตั้งรหัสผ่านที่ยากต่อการเดาจึงจำเป็นอย่างยิ่งในการป้องกันผู้ที่ไม่ได้รับอนุมัติไม่ให้เข้าถึงระบบได้ นอกจากนี้ระบบสารสนเทศควรได้รับการออกแบบให้ผู้ที่ไม่ได้รับอนุมัติไม่สามารถเข้าถึงข้อมูลที่เป็นความลับได้โดยง่ายแม้ว่าบุคคลนั้นจะสามารถเข้าถึงระบบของกิจการที่เชื่อมต่อกับระบบภายนอกแล้วก็ตาม เช่น การจัดเก็บข้อมูลที่เป็นความลับไว้ในเครื่องคอมพิวเตอร์ที่แยกต่างหากจากระบบของกิจการที่เชื่อมต่อกับระบบภายนอก เป็นต้น

3) การส่งข้อมูลผ่านระบบโทรคมนาคม

ข้อมูลที่ส่งเข้าสู่ระบบผ่านทางระบบโทรคมนาคมอาจถูกเปลี่ยนแปลงหรือส่งผ่านไม่ครบถ้วนในระหว่างการสื่อสาร ซึ่งอาจเป็นผลจากข้อผิดพลาดของอุปกรณ์หรือโปรแกรมที่ใช้ในการสื่อสารหรือ ความไม่สม่ำเสมอของกระแสไฟฟ้าที่ใช้ ดังนั้นระบบจึงจำเป็นต้องมีการตรวจสอบความถูกต้องและครบถ้วนของข้อมูลที่ได้รับผ่านทางระบบโทรคมนาคมก่อนที่จะนำข้อมูลดังกล่าวไปประมวลผล นอกจากนี้ข้อมูลที่ถูกส่งผ่านระบบโทรคมนาคมอาจถูกลักลอบเข้าถึงโดยผู้ที่ไม่ได้

รับอนุมัติได้ ดังนั้นระบบจึงควรมีการควบคุมที่ดี เช่น การเข้ารหัสข้อมูลเพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุมัติสามารถนำข้อมูลของกิจการไปใช้ได้

4) การกระจายของข้อมูลอยู่ตามสถานที่ต่างๆ

การจัดเก็บข้อมูลในระบบคอมพิวเตอร์ที่กระจายอยู่ตามสถานที่ต่างๆ เพื่อให้ผู้ใช้สามารถเข้าถึงระบบได้พร้อมกันอย่างสะดวกและรวดเร็ว อาจก่อให้เกิดปัญหาในการปรับปรุงข้อมูลในกรณีที่ข้อมูลชุดเดียวกันมีหลายสำเนาหรือในกรณีที่มีผู้ใช้มากกว่าหนึ่งคนต้องการปรับปรุงข้อมูลเดียวกันพร้อมกันได้ กล่าวคือ

- ในการปรับปรุงข้อมูลในกรณีที่ข้อมูลชุดเดียวกันมีหลายสำเนาหรือมีอยู่ในหลายฐานข้อมูล อาจมีข้อมูลบางชุดเท่านั้นที่ได้รับการปรับปรุง ทำให้ข้อมูลในระบบขาดความสม่ำเสมอหากระบบไม่มีการควบคุมเพื่อให้มั่นใจว่าการปรับปรุงข้อมูลแต่ละรายการในฐานข้อมูลหนึ่งจะมีการปรับปรุงแบบประสานจังหวะไปยังข้อมูลเดียวกันทุกชุดในระบบ
- ในกรณีที่มีผู้ใช้มากกว่าหนึ่งคนต้องการปรับปรุงข้อมูลเดียวกันพร้อมกัน อาจทำให้มีข้อมูลที่นำเข้าระบบบางส่วนหายไปหากระบบไม่มีการควบคุมเพื่อป้องกันไม่ให้มีผู้ใช้ที่ได้รับอนุมัติมากกว่าหนึ่งคนสามารถปรับปรุงข้อมูลเดียวกันได้พร้อมกัน

5) การเข้าถึงระบบผ่านเครื่องปลายทางที่เพิ่มจำนวนขึ้น

การเพิ่มจำนวนเครื่องปลายทางที่สามารถเข้าถึงระบบคอมพิวเตอร์ทำให้การควบคุมภายในยากขึ้น เนื่องจากเครื่องปลายทางแต่ละเครื่องที่ต่อเข้ากับระบบคอมพิวเตอร์เปิดโอกาสให้ผู้ที่เข้าถึงเครื่องปลายทางดังกล่าวสามารถเข้าถึงระบบคอมพิวเตอร์ได้ ดังนั้นในตรวจสอบระบบสารสนเทศจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงจากการเพิ่มจำนวนเครื่องปลายทางที่สามารถเข้าถึงระบบคอมพิวเตอร์ เช่น การติดตั้งเครื่องปลายทางในที่ปลอดภัยและยากต่อการเข้าถึงโดยผู้ที่ไม่ได้รับอนุมัติ การกำหนดให้ระบบมีการจัดทำร่องรอยการตรวจสอบเพื่อให้สามารถติดตามการเข้าถึงและการใช้ทรัพยากรของระบบได้ ตลอดถึงการกำหนดให้มีการสอบทานร่องรอยการตรวจสอบอย่างเหมาะสมและทันต่อเวลา เป็นต้น

3.2.1.6 ลักษณะสำคัญของระบบสารสนเทศที่เกี่ยวกับการใช้ไมโครคอมพิวเตอร์

ระบบสารสนเทศการจัดทำรายงานหรือร่องรอยการตรวจสอบมีลักษณะสำคัญที่เกี่ยวกับการใช้ไมโครคอมพิวเตอร์ซึ่งมีผลต่อการควบคุมภายในของระบบดังนี้

1) ผู้ใช้เป็นผู้รับผิดชอบต่อระบบไมโครคอมพิวเตอร์ที่ใช้

โดยทั่วไปผู้ที่รับผิดชอบต่อไมโครคอมพิวเตอร์คือผู้ใช้ กล่าวคือผู้ใช้จะต้องรับผิดชอบต่อความปลอดภัยทางกายภาพของเครื่อง ความปลอดภัยของข้อมูลต่างๆ ที่อยู่ในเครื่องตลอดถึงการเตรียมการต่างๆ เพื่อให้สามารถประมวลผลได้อย่างต่อเนื่อง หากผู้ใช้ละเลยที่จะดูแลรักษาความปลอดภัยและสภาพของเครื่องคอมพิวเตอร์ อาจมีผลทำให้ผู้ที่ไม่ได้รับอนุมัติสามารถเข้าถึงข้อมูลได้ ตลอดทั้งระบบคอมพิวเตอร์อาจทำงานผิดพลาดทำให้ข้อมูลที่อยู่ในระบบสูญหายหรือผิดพลาดได้ ดังนั้นในการตรวจสอบระบบสารสนเทศที่มีการใช้ไมโครคอมพิวเตอร์ในการประมวลผลจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงและผลเสียหายที่อาจเกิดขึ้นต่อทรัพยากรของกิจการ เช่น การติดตั้งเครื่องไมโครคอมพิวเตอร์ในที่ปลอดภัยและยากต่อการเข้าถึงโดยผู้ที่ไม่ได้รับอนุมัติ การกำหนดให้มีการใส่รหัสผ่านก่อนทำการประมวลผลได้ การกำหนดมาตรการและขั้นตอนและความรับผิดชอบในการดูแลรักษาเครื่องไมโครคอมพิวเตอร์ การกำหนดมาตรการไม่ให้มีการติดตั้งและใช้ซอฟต์แวร์ที่ผิดกฎหมายหรือที่ไม่ได้รับอนุมัติ การตรวจสอบและป้องกันไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ เป็นต้น

2) ผู้ใช้เป็นผู้รับผิดชอบในการพัฒนาและจัดหาระบบงานที่ประมวลผลด้วยเครื่องไมโครคอมพิวเตอร์

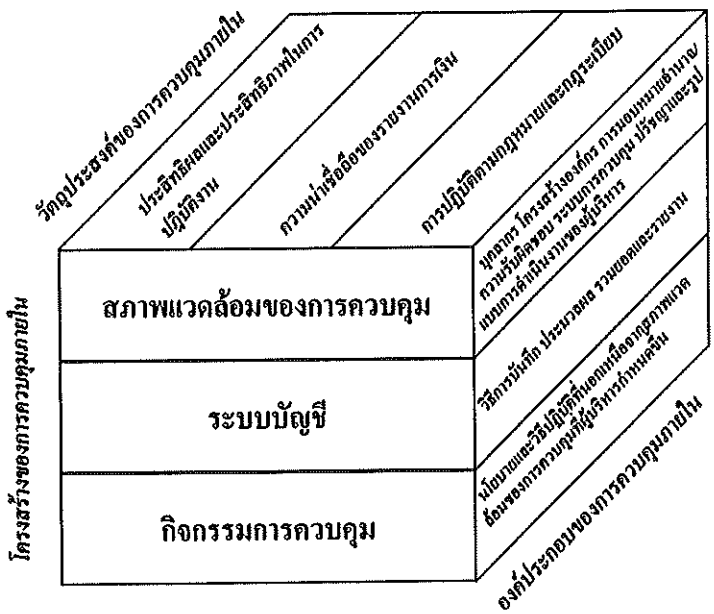
การที่ผู้ใช้เป็นผู้รับผิดชอบในการพัฒนาและจัดหาระบบอาจทำให้ไม่มีการทดสอบระบบและการจัดทำเอกสารประกอบระบบอย่างเพียงพอ ซึ่งอาจก่อให้เกิดปัญหาเมื่อนำระบบไปใช้งานจริง ดังนั้นในการตรวจสอบระบบสารสนเทศที่มีการใช้ไมโครคอมพิวเตอร์ในการประมวลผลจึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงและผลเสียหายที่อาจเกิดขึ้นต่อทรัพยากรของกิจการ เช่น การกำหนดขั้นตอนในการพัฒนาและจัดหา การกำหนดนโยบายไม่ให้ใช้ซอฟต์แวร์ที่ผิดกฎหมาย การทดสอบและอนุมัติโปรแกรมระบบงานก่อนที่จะนำไปใช้งานจริงได้ การกำหนดมาตรฐานในการจัดทำเอกสารประกอบระบบซึ่งรวมถึงคู่มือสำหรับผู้ใช้ด้วย เป็นต้น

3) ผู้ใช้เป็นผู้รับผิดชอบในการควบคุมด้านการสื่อสาร

ในกรณีที่ผู้ใช้ใช้เครื่องไมโครคอมพิวเตอร์ในการสื่อสารกับเครื่องคอมพิวเตอร์อื่น ผู้ใช้จะต้องรับผิดชอบในการป้องกันภัยที่อาจเกิดขึ้นกับเครื่องไมโครคอมพิวเตอร์ที่ใช้และข้อมูลต่างๆ ที่อยู่ภายใน เช่น ภัยจากคอมพิวเตอร์ไวรัส ภัยจากการที่บุคคลภายนอกจะเข้าถึงข้อมูลที่สำคัญในเครื่อง หากผู้ใช้ขาดความระมัดระวัง ระบบที่เชื่อมต่อกับเครื่องไมโครคอมพิวเตอร์ดังกล่าวอาจได้รับภัยจากคอมพิวเตอร์ไวรัสหรือจากการเข้าถึงของบุคคลภายนอกได้ ดังนั้นในการตรวจสอบระบบสารสนเทศที่มีการใช้ไมโครคอมพิวเตอร์ในการประมวลผลหรือมีเครื่องไมโครคอมพิวเตอร์เชื่อมต่ออยู่จึงจำเป็นต้องพิจารณาถึงการควบคุมที่สามารถใช้เพื่อลดความเสี่ยงและผลเสียหายที่อาจเกิดขึ้นต่อทรัพยากรของกิจการ เช่น การกำหนดมาตรการและขั้นตอนในการใช้เครื่องไมโครคอมพิวเตอร์ในการสื่อสารกับเครื่องคอมพิวเตอร์อื่น การกำหนดมาตรการเกี่ยวกับข้อมูลที่สามารถรับและส่งระหว่างเครื่องไมโครคอมพิวเตอร์กับเครื่องคอมพิวเตอร์อื่น การกำหนดให้มีการติดตั้งและใช้ซอฟต์แวร์เพื่อป้องกันคอมพิวเตอร์ไวรัส เป็นต้น

3.2.2 องค์ประกอบของการควบคุมภายในสำหรับระบบสารสนเทศ

ในการประเมินประสิทธิผลของระบบการควบคุมภายใน ผู้สอบบัญชีจำเป็นต้องมีความเข้าใจเกี่ยวกับวัตถุประสงค์และองค์ประกอบของการควบคุมภายในของระบบสารสนเทศ ดังแสดงสรุปในภาพ 2-1



ภาพ 2-1 วัตถุประสงค์และองค์ประกอบของระบบการควบคุมภายในของระบบสารสนเทศ

3.2.2.1 วัตถุประสงค์ของการควบคุมภายในสำหรับระบบสารสนเทศ

การควบคุมภายในของระบบสารสนเทศมีวัตถุประสงค์ที่ไม่แตกต่างจากวัตถุประสงค์ของการควบคุมภายในสำหรับระบบที่ประมวลผลด้วยมือ กล่าวคือ การควบคุมภายในของระบบสารสนเทศเป็นกระบวนการที่ออกแบบขึ้นโดยมีวัตถุประสงค์เพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผล (Reasonable Assurance) ว่ากิจการจะสามารถบรรลุวัตถุประสงค์ในเรื่องต่อไปนี้

- ประสิทธิผลและประสิทธิภาพในการปฏิบัติงาน
- ความน่าเชื่อถือของรายงานทางการเงิน
- การปฏิบัติตามกฎหมายและกฎระเบียบที่มีผลบังคับใช้

วัตถุประสงค์ข้อที่สองเป็นวัตถุประสงค์ที่เกี่ยวข้องโดยตรงกับการควบคุมด้านการเงินในขณะที่วัตถุประสงค์ข้อที่หนึ่งและสามเกี่ยวข้องกับการควบคุมทางการบริหารหรือการควบคุมด้านที่มิใช่ด้านการเงิน โดยรายละเอียดของการควบคุมภายในแต่ละประเภทเหล่านี้ได้อธิบายไว้ในหัวข้อ 3.2.3 ประเภทของการควบคุมภายใน ทั้งนี้ วัตถุประสงค์ของการควบคุมภายในที่ผู้สอบบัญชีเน้นในการตรวจสอบงบการเงินของกิจการได้แก่ วัตถุประสงค์ข้อที่สองและวัตถุประสงค์ข้อที่สามเฉพาะส่วนที่มีผลกระทบต่อความถูกต้องและการเปิดเผยข้อมูลของงบการเงิน

3.2.2.2 องค์ประกอบของการควบคุมภายในสำหรับระบบสารสนเทศ

โครงสร้างของการควบคุมภายใน (Internal Control Structure) ของระบบสารสนเทศประกอบด้วยนโยบายและขั้นตอนต่างๆ ที่กำหนดขึ้นเพื่อให้สามารถมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ในเรื่องของการดำเนินงานอย่างมีประสิทธิผลและประสิทธิภาพ การจัดทำรายงานการเงินที่น่าเชื่อถือและการปฏิบัติตามกฎหมายและระเบียบข้อบังคับอย่างถูกต้อง ซึ่งมาตรฐานการสอบบัญชีระหว่างประเทศฉบับที่ 400 ซึ่งเป็นต้นแบบของร่างมาตรฐานการสอบบัญชี รหัส 400 เรื่องการประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายในได้แบ่งนโยบายและขั้นตอนเหล่านี้เป็น 3 ส่วนคือ ส่วนที่เกี่ยวกับสภาพแวดล้อมของการควบคุม (Control Environment) ส่วนที่เกี่ยวข้องกับระบบบัญชี (Accounting System) และส่วนที่เกี่ยวกับกิจกรรมการควบคุมหรือวิธีการควบคุม (Control Activities or Control Procedures)

1) สภาพแวดล้อมของการควบคุม

สภาพแวดล้อมของการควบคุมเป็นองค์ประกอบสำคัญที่มีผลต่อประสิทธิผลของการควบคุมภายในเนื่องจากสภาพแวดล้อมของการควบคุมเป็นตัวกำหนดบรรยากาศของกิจการที่มีต่อการควบคุมภายในซึ่งเป็นพื้นฐานสำหรับองค์ประกอบอื่นของโครงสร้างการควบคุมภายใน ปัจจัยสำคัญของสภาพแวดล้อมของการควบคุม ได้แก่

1.1 นโยบายและวิธีปฏิบัติเกี่ยวกับบุคลากร

ความสามารถและความซื่อสัตย์ของพนักงานมีความสำคัญต่อการควบคุมภายในสำหรับระบบสารสนเทศทางการบัญชีมากกว่าระบบบัญชีที่ประมวลผลด้วยมือ ซึ่งมีผลมาจากลักษณะและวิธีการของระบบสารสนเทศทางการบัญชีในด้านต่างๆ เช่น การนำเข้าข้อมูลและการประมวลผล ที่แตกต่างไปจากระบบที่ประมวลผลด้วยมือ ดังนั้นเพื่อให้มั่นใจว่าพนักงานของกิจการเป็นบุคคลที่มีความซื่อสัตย์และมีความสามารถในการปฏิบัติงานที่ได้รับมอบหมายให้ลุล่วงด้วยดี กิจการจึงจำเป็นอย่างยิ่งที่จะต้องมีการดำเนินการในเรื่องต่อไปนี้

- การกำหนดนโยบายหรือระเบียบปฏิบัติเพื่อส่งเสริมให้บุคลากรที่มีส่วนเกี่ยวข้องกับระบบตระหนักถึงความรับผิดชอบที่ต้องมีต่อการควบคุมภายในและความปลอดภัยของระบบ เช่น การกำหนดให้พนักงานทุกคนต้องเซ็นรับทราบเกี่ยวกับการรักษาความลับของข้อมูลของบริษัทและรหัสผ่านที่ใช้ในการเข้าถึงระบบ การกำหนดความรับผิดชอบของพนักงานที่ต้องมีต่อการควบคุมภายในและความปลอดภัยของระบบในคู่มือพนักงาน
- การกำหนดนโยบายหรือระเบียบปฏิบัติในการเลือกสรรพนักงานและการจัดอบรมบุคลากรที่มีส่วนเกี่ยวข้องกับระบบให้มีความรู้ ความชำนาญที่จำเป็นต่อการที่จะปฏิบัติงานเพื่อให้มั่นใจว่าบุคลากรของกิจการมีความรู้ ความสามารถและศักยภาพที่เพียงพอต่อการปฏิบัติงาน เช่น กำหนดให้ในการคัดเลือกพนักงานใหม่ต้องมีการทดสอบโดยการสัมภาษณ์และการทดสอบภาคปฏิบัติเกี่ยวกับงานในตำแหน่ง
- การกำหนดนโยบายหรือระเบียบปฏิบัติในการจำกัดการเข้าถึงระบบสำหรับพนักงานที่ลาออกและพนักงานที่ถูกพักงานหรือไล่ออกเพื่อป้องกันการเข้าถึงข้อมูลและโปรแกรมเพื่อเปลี่ยนแปลงแก้ไขหรือทำลายโดยไม่ได้รับอนุมัติ

- การกำหนดนโยบายหรือระเบียบปฏิบัติที่ช่วยลดช่องว่างของการควบคุมภายในเพื่อป้องกันและค้นหาข้อผิดพลาดหรือรายการผิดปกติที่อาจเกิดขึ้น เช่น การกำหนดนโยบายให้มีการผลัดเปลี่ยนงาน การลาพักร้อน การทำงานล่วงเวลาและการมอบหมายงานให้พนักงานมากกว่าหนึ่งคนรับผิดชอบงานร่วมกัน

1.2 โครงสร้างองค์กรและวิธีการมอบหมายอำนาจหน้าที่และความรับผิดชอบ

การจัดโครงสร้างองค์กรที่ดีช่วยให้เกิดความชัดเจนในการกำหนดและมอบหมายอำนาจและความรับผิดชอบและช่วยลดความเสี่ยงที่จะเกิดการผิดพลาดในการปฏิบัติงานด้วย ตัวอย่างของการควบคุมเกี่ยวกับการจัดโครงสร้างองค์กร ได้แก่

- การจัดทำและปรับปรุงผังองค์กรให้ทันสมัยอยู่เสมอ โดยผังองค์กรที่จัดทำขึ้นนี้ควรได้รับการอนุมัติหรือเห็นชอบจากผู้บริหาร ผังองค์กรที่ดีจะช่วยให้พนักงานมีความเข้าใจที่ถูกต้องเกี่ยวกับความสัมพันธ์ระหว่างหน่วยงานต่างๆ ภายในองค์กรและสายการบังคับบัญชาและการรายงาน ซึ่งมีผลให้การปฏิบัติงานและการติดต่อสื่อสารภายในองค์กรเป็นไปอย่างราบรื่นและมีข้อผิดพลาดน้อยลง
- การจัดทำและปรับปรุงคำบรรยายลักษณะงาน โดยคำบรรยายลักษณะงานที่จัดทำขึ้นนี้ควรได้มีการส่งสำเนาให้กับพนักงานด้วย คำบรรยายลักษณะงานจะช่วยให้พนักงานมีความเข้าใจที่ถูกต้องเกี่ยวกับหน้าที่และความรับผิดชอบของตน ซึ่งมีผลให้พนักงานปฏิบัติหน้าที่ที่ได้รับมอบหมายอย่างครบถ้วนและไม่ไปก้าวก่ายหน้าที่ของบุคคลอื่นอันอาจก่อให้เกิดปัญหาเกี่ยวกับการแบ่งแยกหน้าที่ที่จะได้กล่าวในรายละเอียดต่อไป นอกจากนี้กิจการยังสามารถใช้คำบรรยายลักษณะงานเป็นเกณฑ์ในการคัดเลือกพนักงานใหม่ด้วย

1.3 ปรัชญาและรูปแบบการดำเนินงานของผู้บริหาร

ปรัชญาและรูปแบบการดำเนินงานของผู้บริหารมีผลกระทบต่อประสิทธิผลของการควบคุมภายในสำหรับระบบสารสนเทศทางการบัญชีด้วย ผู้บริหารที่มีทัศนคติที่ดีต่อการควบคุมภายในย่อมเกื้อกูลให้ระบบมีสภาพแวดล้อมในการควบคุมภายในที่ดีและพนักงานตระหนักถึงความสำคัญของการควบคุมภายในซึ่งมีผลให้มีการปฏิบัติตามระบบการควบคุมภายในอย่างเคร่งครัด

1.4 การปฏิบัติหน้าที่ของคณะกรรมการบริษัทและคณะกรรมการต่างๆ ตลอดถึงระบบการควบคุมของผู้บริหารและการตรวจสอบภายใน

2) ระบบบัญชี

ระบบบัญชีประกอบด้วยวิธีการและบันทึกที่จัดทำขึ้นเพื่อบันทึก ประมวลผล รวมยอดและรายงานเกี่ยวกับรายการค้า สินทรัพย์ หนี้สินและทุนของกิจการ ดังนั้น ระบบบัญชีจึงประกอบด้วย 2 องค์ประกอบหลักดังนี้

2.1 วิธีการของระบบบัญชี

วิธีการของระบบบัญชีในการบันทึก ประมวลผล รวมยอดและรายงานที่เหมาะสมช่วยให้การบันทึกสินทรัพย์ หนี้สิน ทุน รายได้และค่าใช้จ่ายของกิจการและการจัดทำรายงานเป็นไปอย่างถูกต้อง ครบถ้วนและทันเวลาและช่วยลดความเสี่ยงที่จะเกิดการผิดพลาดในการปฏิบัติงานด้วย ตัวอย่างของนโยบายและขั้นตอนที่เกี่ยวข้องได้แก่ นโยบายบัญชีของกิจการ ผังบัญชี คู่มือการลงบัญชี เอกสารและแบบฟอร์มที่ต้องใช้ในการบันทึกรายการบัญชี เป็นต้น

2.2 เอกสารและบันทึก

เนื่องจากข้อมูลในระบบที่ประมวลผลด้วยคอมพิวเตอร์จะถูกจัดเก็บในรูปอิเล็กทรอนิกส์ซึ่งง่ายต่อการสูญหาย ดังนั้นจึงมีความจำเป็นที่ระบบจะต้องจัดเก็บข้อมูลที่จำเป็นและมีหลักฐานเพื่อการตรวจสอบอย่างครบถ้วน โดยทั่วไปเอกสารของระบบที่ใช้คอมพิวเตอร์สามารถแบ่งเป็น 3 ประเภทคือ

- เอกสารประกอบระบบ (System Documentation) ซึ่งเป็นเอกสารแสดงภาพรวมของระบบและให้ข้อมูลรายละเอียดเกี่ยวกับการทำงานและการควบคุมภายในของระบบ
- เอกสารประกอบโปรแกรม (Program Documentation) ซึ่งเป็นเอกสารที่ให้ข้อมูลที่จำเป็นต่อการทำความเข้าใจและเปลี่ยนแปลงแก้ไขโปรแกรมแต่ละโปรแกรม
- เอกสารประกอบการปฏิบัติงาน (Operations Documentation) ซึ่งเป็นเอกสารที่ให้ข้อมูลที่จำเป็นต่อการใช้ระบบ

นอกจากนี้เอกสารที่ระบบควรมีเพิ่มเติมได้แก่ เอกสารเกี่ยวกับมาตรฐานและระเบียบปฏิบัติในเรื่องต่อไปนี้

- มาตรฐานในการจัดทำเอกสารที่จำเป็น
- มาตรการในการรักษาความปลอดภัยของแฟ้มข้อมูล โปรแกรม และห้องคอมพิวเตอร์
- มาตรการในการขออนุมัติประมวลข้อมูล
- มาตรการในการปฏิบัติงานของคอมพิวเตอร์และการดูแลรักษาแฟ้มข้อมูล

3) กิจกรรมการควบคุม

กิจกรรมการควบคุมเป็นนโยบายและขั้นตอนที่กำหนดขึ้นเพื่อช่วยให้แน่ใจว่ากิจกรรมต่างๆ ที่จำเป็นต่อการลดความเสี่ยงเพื่อให้กิจการสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ได้มีการปฏิบัติตาม กิจกรรมการควบคุมของกิจการอาจมีวัตถุประสงค์หลายหลากและหลายรูปแบบ โดยปกติกิจกรรมการควบคุมที่เกี่ยวข้องโดยตรงกับการตรวจสอบสามารถแยกเป็นนโยบายและขั้นตอนที่เกี่ยวข้องกับการแบ่งแยกหน้าที่ การประมวลรายการ การควบคุมทางกายภาพและการตรวจสอบผลการปฏิบัติงานอย่างอิสระ

3.1 การแบ่งแยกหน้าที่

การแบ่งแยกหน้าที่ที่ดีจะช่วยลดความเสี่ยงที่จะเกิดการทุจริต โดยหลักการในการแบ่งแยกหน้าที่สำหรับระบบที่ใช้คอมพิวเตอร์ประมวลผลคือ จะต้องมีการแบ่งแยกระหว่างบุคคลที่มีความรู้เกี่ยวกับการทำงานของระบบกับบุคคลที่สามารถเข้าถึงระบบและจะต้องมีการแบ่งแยกหน้าที่งานที่หากรับผิดชอบโดยบุคคลเดียวกันแล้วบุคคลนั้นสามารถทำการทุจริตได้ ดังนั้นผู้ที่มีความรู้เกี่ยวกับการทำงานของระบบ เช่น ผู้จัดการฝ่ายระบบสารสนเทศ ผู้วิเคราะห์ระบบ และโปรแกรมเมอร์จึงไม่ควรที่จะได้รับมอบหมายให้เป็นผู้ที่สามารถเข้าถึงระบบ เอกสารและข้อมูลของระบบ เช่น ผู้ปฏิบัติการระบบ พนักงานนำข้อมูลเข้า และพนักงานควบคุมข้อมูลเป็นต้น

3.2 การควบคุมด้านกายภาพ

การควบคุมด้านกายภาพมีความสำคัญมากต่อระบบที่ประมวลผลด้วยคอมพิวเตอร์เนื่องจากการเปลี่ยนแปลงแก้ไขอาจจะไม่สามารถสังเกตเห็นได้ การควบคุมด้านกายภาพมีองค์ประกอบดังนี้

- การควบคุมการเข้าถึงด้านกายภาพ ประกอบด้วยการควบคุมการเข้าถึงข้อมูลในระบบ โปรแกรมในระบบ เอกสารระบบต่างๆ สื่อที่จัดเก็บข้อมูล ห้องคอมพิวเตอร์ ข้อมูลเข้าและข้อมูลออก
- การป้องกันทางด้านกายภาพ ประกอบด้วยดำเนินมาตรการในการป้องกันการสูญเสียที่จะเกิดขึ้นรวมถึงการทำประกันภัยสำหรับภัยพิบัติต่างๆ เช่น ไฟไฟม้ น้ำท่วม ตัวอย่างเช่น การเก็บรักษาสื่อที่เก็บข้อมูลที่สำคัญไว้ในตู้นิรภัยที่ผู้ที่ได้รับอนุมัติสามารถเปิดได้ การเก็บสื่อที่เก็บข้อมูลที่สำคัญอีกชุดหนึ่งไว้นอกสถานที่ การจัดเตรียมแผนสำรองเผื่อฉุกเฉิน
- การดูแลด้านกายภาพ ประกอบด้วยการดูแลรักษาระบบเพื่อลดความเสี่ยงที่ระบบคอมพิวเตอร์จะไม่ทำงานตามปกติ เช่น การดูแลรักษาสภาพแวดล้อมทางด้านกายภาพของระบบเกี่ยวกับอุณหภูมิและความชื้นของห้องคอมพิวเตอร์ การกำหนดให้มีการบำรุงรักษาระบบเชิงป้องกันอย่างสม่ำเสมอ

3.3 การประมวลรายการ

การประมวลรายการของระบบที่ใช้คอมพิวเตอร์มีความแตกต่างจากระบบที่ประมวลผลด้วยมือเนื่องจากคอมพิวเตอร์ถูกใช้ในหลายขั้นตอนของการประมวลรายการ เช่น การอนุมัติรายการ การรับข้อมูล การจัดเก็บข้อมูล การป้องกันการสูญหายของข้อมูล การประมวลผล เป็นต้น ดังนั้นระบบจึงจำเป็นต้องมีการควบคุมภายในในเรื่องต่อไปนี้

- การกำหนดนโยบายหรือระเบียบปฏิบัติเพื่อให้แน่ใจว่าเฉพาะบุคคลที่ได้รับอนุมัติสามารถเข้าถึงระบบหรือเครื่องปลายทางที่เชื่อมกับระบบได้
- การกำหนดและออกแบบหน้าจอที่รับข้อมูลเข้าให้ง่ายต่อการนำข้อมูลเข้าและทำความเข้าใจ รวมทั้งป้องกันไม่ให้ข้อมูลที่ไม่ถูกต้องถูกนำเข้าสู่ระบบ
- การกำหนดนโยบายในการจัดการสื่อที่ใช้จัดเก็บข้อมูล เช่น วิธีการในการจัดทำฉลากภายนอกและฉลากภายในสำหรับเทปที่ใช้ในการจัดเก็บข้อมูลเพื่อป้องกันการนำเอาเทปม้วนที่ไม่ถูกต้องไปใช้ในการประมวลผล

- การกำหนดนโยบายในการป้องกันการสูญหายของข้อมูล เช่น ขั้นตอนและวิธีการในการจัดทำข้อมูลสำรอง
- การกำหนดนโยบายและวิธีการในการเปลี่ยนแปลงหรือจัดหาโปรแกรมหรือระบบงานใหม่
- การกำหนดนโยบายเกี่ยวกับการฟื้นฟูระบบในกรณีที่เกิดเหตุฉุกเฉิน เช่น การกำหนดให้มีระบบสำรอง การกำหนดวิธีการในการฟื้นฟูระบบและทดสอบความถูกต้องของระบบที่ฟื้นฟูขึ้น การใช้ซอฟต์แวร์ให้แจ้งข้อความให้ผู้ใช้ทราบในกรณีที่การทำงานของระบบมีปัญหาและบันทึกข้อความของการทำงานของระบบไว้สำหรับใช้ในการฟื้นฟูระบบ

3.4 การตรวจสอบผลการปฏิบัติงานอย่างอิสระ

การตรวจสอบผลการปฏิบัติงานอย่างอิสระมีวัตถุประสงค์เพื่อให้แน่ใจว่าการทำงานของระบบเป็นไปอย่างถูกต้องและเหมาะสมตามที่กำหนดไว้ ซึ่งการตรวจสอบจะประกอบด้วย

- การตรวจสอบว่าการดำเนินการในเรื่องต่างๆ เป็นไปตามมาตรฐานและขั้นตอนการปฏิบัติงานที่กำหนดไว้
- การตรวจสอบบันทึกการทำงานของระบบ (System Logs) เพื่อตรวจหารายการผิดพลาดหรือรายการที่ผิดปกติ
- การตรวจสอบโดยผู้ที่เป็นอิสระจากการปฏิบัติงาน เช่น การตรวจสอบการปฏิบัติงานโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระจากภายนอก
- การสอบทานนโยบาย ระเบียบปฏิบัติ ระบบการควบคุมภายในและการตรวจสอบภายในโดยคณะกรรมการตรวจสอบ (Audit Committee) ซึ่งกรรมการของคณะกรรมการตรวจสอบประกอบด้วยกรรมการอิสระของบริษัทที่มีคุณสมบัติที่เหมาะสม เช่น มีความรู้เกี่ยวกับธุรกิจของกิจการ มีความเข้าใจเกี่ยวกับบัญชีและการควบคุมภายใน เป็นต้น

3.2.3 ประเภทของการควบคุม

วิธีการจัดประเภทของการควบคุมของระบบสารสนเทศสามารถจัดได้หลายลักษณะ เช่น ตามลักษณะของการควบคุม ตามวัตถุประสงค์ของการควบคุม ตามลักษณะของวิธีการควบคุมและตามประเภทของการควบคุม เป็นต้น ดังรายละเอียดต่อไปนี้

3.2.3.1 การจัดประเภทตามลักษณะของการควบคุม

การจัดประเภทของการควบคุมของระบบสารสนเทศตามลักษณะของการควบคุมแบ่งออกเป็นการควบคุมทางด้านการเงินและการควบคุมทางด้านที่มิใช่ด้านการเงิน

1) การควบคุมทางด้านการเงิน

การควบคุมทางด้านการเงิน (Financial Controls) เป็นการควบคุมเพื่อให้แน่ใจว่างบการเงินและรายงานทางการเงินที่จัดทำขึ้นถูกต้อง ครบถ้วนและน่าเชื่อถือ การควบคุมทางด้านการเงินถือเป็นการควบคุมภายในที่สำคัญของระบบสารสนเทศ โดยการควบคุมทางด้านการเงินมีวัตถุประสงค์ย่อยซึ่งถือเป็นวัตถุประสงค์หลักของการควบคุมภายในของระบบสารสนเทศดังต่อไปนี้

- เพื่อให้แน่ใจว่ารายการทุกรายการที่นำเข้าระบบและประมวลผลเป็นรายการที่เกิดขึ้นจริงและได้รับอนุมัติ
- เพื่อให้แน่ใจว่ารายการที่เกิดขึ้นจริงและได้รับอนุมัติทุกรายการได้ถูกนำเข้าระบบและประมวลผลอย่างถูกต้อง ครบถ้วนและทันต่อเวลา
- เพื่อให้แน่ใจว่ามีการบันทึกรายการบัญชีที่เกี่ยวข้องอย่างถูกต้องและทันต่อเวลา
- เพื่อให้แน่ใจว่าข้อมูลออกและรายงานต่างๆที่จำเป็นได้รับการจัดทำอย่างถูกต้อง เหมาะสมและทันเวลา
- เพื่อให้แน่ใจว่าสินทรัพย์ ข้อมูลและเอกสารที่สำคัญได้รับการป้องกันจากการสูญหาย ถูกฉ้อฉลหรือถูกนำไปใช้ในทางมิชอบ

การควบคุมทางด้านการเงินเพื่อให้บรรลุวัตถุประสงค์ข้างต้นมีมากมายหลายวิธี ตัวอย่างของการควบคุมทางด้านการเงินที่ใช้กันโดยทั่วไป ได้แก่

- การออกแบบและใช้เอกสารที่มีการพิมพ์เลขที่เอกสารไว้ล่วงหน้าเพื่อให้แน่ใจว่ารายการทุกรายการจะได้รับการบันทึกอย่างครบถ้วน
- การจัดให้มีการแบ่งแยกหน้าที่อย่างเหมาะสมเพื่อให้แน่ใจว่ารายการทุกรายการที่นำเข้าระบบและประมวลผลเป็นรายการที่เกิดขึ้นจริงและได้รับอนุมัติ

- การกำหนดให้ต้องมีการอนุมัติรายการที่เหมาะสม เช่น การกำหนดนโยบายในการจัดซื้อว่ารายการซื้อแต่ละรายการจะต้องได้รับการอนุมัติจากผู้ที่มีอำนาจอนุมัติก่อนจึงจะสามารถทำการสั่งซื้อได้
- การกำหนดมาตรการในการดูแลความปลอดภัยสินทรัพย์ของกิจการเพื่อให้มั่นใจว่าสินทรัพย์ ข้อมูลและเอกสารที่สำคัญได้รับการป้องกันจากการสูญหาย ถูกฉ้อฉลหรือถูกนำไปใช้ในทางมิชอบ เช่น การกำหนดให้มีพนักงานรักษาความปลอดภัยคอยตรวจตราบริเวณโรงงาน การกำหนดให้บุคคลภายนอกต้องลงชื่อ เหตุผลในการเข้าอาคาร และเวลาเข้า-ออกในทะเบียน เป็นต้น
- การกำหนดให้มีการตรวจสอบการปฏิบัติงานโดยผู้ที่ไม่ได้เกี่ยวข้องกับการปฏิบัติงาน เช่น การให้ผู้ตรวจสอบภายในทำการตรวจนับเงินสดที่ถือโดยผู้รักษาเงินสดเพื่อให้มั่นใจว่าเงินสดมิได้สูญหาย ถูกฉ้อฉลหรือถูกนำไปใช้ในทางมิชอบ
- การกำหนดให้มีการประเมินมูลค่าของสินทรัพย์ที่บันทึกอยู่ในบัญชีเพื่อให้แน่ใจว่ามูลค่าของสินทรัพย์ที่บันทึกอยู่ในบัญชีถูกต้องตามความเป็นจริง เช่น การตรวจนับสินค้าคงเหลือตอนสิ้นปีเพื่อปรับมูลค่าของสินค้าคงเหลือที่ปรากฏตามบัญชีให้สอดคล้องกับปริมาณและสภาพของสินค้าที่ตรวจนับ

2) การควบคุมทางด้านที่มิใช่ด้านการเงิน

การควบคุมทางด้านที่มิใช่ด้านการเงิน (Nonfinancial Controls) เป็นการควบคุมที่เกี่ยวข้องกับการปฏิบัติตามระบบ (Compliance Controls) และการควบคุมที่เกี่ยวข้องกับการปฏิบัติงาน (Operations Controls) เพื่อให้แน่ใจว่าการปฏิบัติงานเป็นไปอย่างมีประสิทธิผลและประสิทธิภาพตามที่กิจการได้ตั้งเป้าหมายไว้และการดำเนินธุรกิจและการปฏิบัติงานเป็นไปตามกฎหมายและกฎระเบียบที่มีผลบังคับใช้ ตัวอย่างของการควบคุมทางด้านที่มิใช่ด้านการเงินที่ใช้กันโดยทั่วไป ได้แก่

- การกำหนดให้มีการจัดทำงบประมาณและเปรียบเทียบผลการปฏิบัติงานจริงกับงบประมาณที่ตั้งไว้เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปอย่างมีประสิทธิผลและประสิทธิภาพตามที่กิจการได้ตั้งเป้าหมายไว้

- การสอบทานรายงานต่างๆ เพื่อติดตามการปฏิบัติงาน เช่น การสอบทานยอดลูกหนี้คงค้างและอายุลูกหนี้เพื่อให้แน่ใจว่าการเก็บหนี้เป็นไปอย่างมีประสิทธิผล การสอบทานแนวโน้มของยอดขายเพื่อให้มั่นใจว่าการขายยังเป็นไปตามเป้าหมายที่ตั้งไว้ การสอบทานอัตราของเสียจากการผลิตเพื่อให้แน่ใจว่าอัตราของเสียไม่สูงกว่าเป้าหมายที่ตั้งไว้
- การกำหนดให้มีการตรวจสอบประสิทธิภาพในการปฏิบัติงานและการปฏิบัติตามกฎหมายและกฎระเบียบที่มีผลบังคับใช้โดยผู้ที่ไม่ได้เกี่ยวข้องกับการปฏิบัติงาน เช่น การให้ผู้ตรวจสอบภายในตรวจสอบว่าการอนุมัติรายการเป็นไปตามระเบียบที่กำหนดไว้

การควบคุมบางวิธีการอาจสามารถใช้เพื่อการควบคุมทางด้านการเงินและการควบคุมทางด้านที่มิใช่ด้านการเงิน เช่น การสอบทานรายงานอายุลูกหนี้สามารถใช้เป็นการควบคุมทางด้านการเงินเพื่อให้แน่ใจว่ามูลค่าของลูกหนี้ที่บันทึกอยู่ในบัญชีสะท้อนมูลค่าที่แท้จริงและเป็นการการควบคุมทางด้านที่มิใช่ด้านการเงินเพื่อให้แน่ใจว่าการเก็บหนี้เป็นไปอย่างมีประสิทธิผล เป็นต้น

3.2.3.2 การจัดประเภทตามวัตถุประสงค์ของการควบคุม

การจัดประเภทของการควบคุมของระบบสารสนเทศอาจจัดตามวัตถุประสงค์ของการควบคุมเพื่อจัดการกับความเสี่ยงต่อทรัพยากรและข้อมูลของระบบ ซึ่งสามารถแบ่งได้เป็น การควบคุมเชิงป้องกัน การควบคุมเชิงตรวจพบ และการควบคุมเชิงแก้ไข

1) การควบคุมเชิงป้องกัน

การควบคุมเชิงป้องกัน (Preventive Controls) เป็นการควบคุมที่จัดให้มีขึ้นเพื่อป้องกันไม่ให้เกิดข้อผิดพลาด การทุจริตหรือผลเสียหายขึ้น โดยทั่วไปการควบคุมเพื่อป้องกันมักกำหนดไว้เป็นส่วนหนึ่งของขั้นตอนการปฏิบัติงาน หากมีการละเว้นไม่ปฏิบัติตามขั้นตอนที่กำหนดไว้ก็อาจจะเกิดข้อผิดพลาดขึ้น เช่น

- การกำหนดวิธีการขั้นตอนในการเบิกจ่ายเงินให้บุคคลภายนอกเพื่อป้องกันการจ่ายเงินให้กับรายการที่กิจการไม่ได้รับสินค้าหรือบริการ หากผู้ปฏิบัติงานไม่ได้ทำการเบิกจ่ายตามขั้นตอนที่กำหนดไว้ว่าต้องมีการตรวจสอบใบแจ้งหนี้ของผู้ขายกับใบสั่งซื้อและใบรับของก่อน อาจมีผลทำให้เกิดข้อผิดพลาดในการจ่ายเงินได้

- การกำหนดขั้นตอนในการเข้าถึงระบบสารสนเทศทางการบัญชีว่าต้องใส่รหัสผู้ใช้และรหัสผ่านก่อน หากผู้บริหารระบบละเลยที่จะกำหนดให้ระบบตรวจสอบรหัสผู้ใช้และรหัสผ่านก่อนอนุญาตให้ผู้ใช้เข้าถึงระบบได้ บุคคลที่ไม่ได้รับอนุมัติอาจสามารถเข้าถึงระบบและใช้ทรัพยากรของระบบโดยไม่ได้รับอนุมัติได้

2) การควบคุมเชิงตรวจพบ

การควบคุมเชิงตรวจพบ (Detective Controls) เป็นการควบคุมที่ใช้ในการค้นหาข้อผิดพลาด การทุจริตหรือเหตุการณ์ที่มีผลด้านลบที่เกิดขึ้นเพื่อแจ้งให้ผู้ปฏิบัติงานหรือผู้ที่เกี่ยวข้องทราบว่ามีข้อผิดพลาดหรือรายการผิดปกติเกิดขึ้นแล้ว ตัวอย่างของการควบคุมประเภทนี้ ได้แก่

- การกำหนดให้ระบบสารสนเทศทางการบัญชีแสดงรายการสินค้าคงเหลือและรายการลูกหนี้ที่มียอดคงเหลือติดลบ
- การกำหนดให้ระบบปฏิบัติการจัดทำรายงานแสดงรายชื่อผู้ใช้ที่ใส่รหัสผ่านผิดติดต่อกันเกินจำนวนครั้งที่กำหนดไว้ เช่น 3 ครั้ง
- การกำหนดให้ระบบปฏิบัติการจัดทำรายงานแสดงรายชื่อผู้ใช้ที่พยายามเข้าถึงระบบช่วงนอกเวลาทำงาน
- การกำหนดให้มีการตรวจสอบข้อมูลที่นำเข้าและการประมวลผลด้วยโปรแกรม

3) การควบคุมเชิงแก้ไข

การควบคุมเชิงแก้ไข (Correction Controls) เป็นการควบคุมที่นำไปสู่การแก้ไขผลจากข้อผิดพลาด การทุจริตหรือเหตุการณ์ที่มีผลด้านลบที่เกิดขึ้น ตัวอย่างของการควบคุมเพื่อแก้ไข ได้แก่

- การจัดทำประกันอัคคีภัยสำหรับสินทรัพย์ของกิจการเพื่อให้กิจการสามารถดำเนินงานต่อไปได้ในกรณีที่เกิดอัคคีภัยขึ้น
- การจัดทำแผนสำรองเผื่อฉุกเฉินในกรณีที่ระบบสารสนเทศทางการบัญชีไม่สามารถทำงานตามปกติได้ เช่น ให้เปลี่ยนไปปฏิบัติงานด้วยมือแทน เป็นต้น

- การจัดทำขั้นตอนสำหรับกรณีที่ระบบงานพบว่าสินค้าคงเหลือมีระดับต่ำกว่าที่กำหนดไว้ เช่น ให้ทำการสั่งซื้อด้วยปริมาณที่กำหนดไว้ในระบบได้ทันทีโดยไม่ต้องได้รับการอนุมัติ
- การกำหนดให้มีการจัดทำร่องรอยการตรวจสอบที่สมบูรณ์เพื่อใช้เป็นข้อมูลในการแก้ไขข้อผิดพลาดหรือรายการผิดปกติที่เกิดขึ้น

3.2.3.3 การจัดประเภทตามลักษณะของวิธีการควบคุม

การจัดประเภทของการควบคุมของระบบสารสนเทศตามลักษณะของวิธีการควบคุมประกอบด้วยการควบคุมโดยโปรแกรมและการควบคุมโดยผู้ปฏิบัติงาน

1) การควบคุมโดยโปรแกรม (Programmed Controls)

การควบคุมโดยโปรแกรมเป็นการควบคุมโดยใช้ระบบคอมพิวเตอร์ เช่น

- การจัดทำยอดรวมกลุ่มของรายการที่นำเข้าสู่ระบบ (Batch Control Totals) เพื่อช่วยในการป้องกันการนำเข้าข้อมูลที่ไม่ครบถ้วนหรือไม่ถูกต้องเป็นลักษณะเด่นของการควบคุมสำหรับระบบประมวลผลแบบรวมกลุ่ม
- การตรวจสอบข้อมูลที่นำเข้าระบบโดยโปรแกรม (Programmed Edit Checks) เช่น การตรวจสอบข้อมูลที่ส่งผ่านเข้าระบบโดยการสะท้อนกลับ เป็นลักษณะเด่นของการควบคุมสำหรับระบบประมวลผลแบบเชื่อมตรง

รายละเอียดเกี่ยวกับการควบคุมโดยโปรแกรมได้อธิบายเพิ่มเติมในบทที่ 4 การควบคุมระบบงานและการประเมินความเสี่ยง

2) การควบคุมโดยผู้ปฏิบัติงาน (User Controls)

ในบางกรณีการควบคุมโดยผู้ปฏิบัติงานอาจเป็นวิธีที่มีประสิทธิภาพมากกว่าในการลดความเสี่ยงที่จะเกิดข้อผิดพลาดและรายการผิดปกติ ตัวอย่างของการควบคุมโดยผู้ปฏิบัติงาน เช่น

- การแบ่งแยกหน้าที่ระหว่างผู้ดูแลรักษาสินทรัพย์ ผู้บันทึกรายการ ผู้ปฏิบัติงานและผู้อนุมัติเพื่อป้องกันมิให้บุคคลหนึ่งบุคคลใดสามารถปกปิดข้อผิดพลาดหรือรายการผิดปกติได้

- การอนุมัติรายการต่างๆโดยผู้มีอำนาจก่อนที่จะดำเนินการได้
- การกระทบยอดบัญชีคุมยอดและบัญชีแยกประเภทย่อย
- การจัดเจ้าหน้าที่เพื่อดูแลสถานที่จัดเก็บสินค้าให้ปลอดภัยจากการถูกขโมยและจากภัยพิบัติ
- การกระทบยอดเงินฝากธนาคาร
- การตรวจนับสินค้าคงเหลือโดยสม่ำเสมอ

รายละเอียดเกี่ยวกับการควบคุมโดยผู้ปฏิบัติงานได้อธิบายเพิ่มเติมในบทที่ 4 การควบคุมระบบงานและการประเมินความเสี่ยง

3.2.3.4 การจัดประเภทตามประเภทของการควบคุม

การจัดประเภทของการควบคุมของระบบสารสนเทศตามประเภทของการควบคุมเป็นวิธีการจัดประเภทของการควบคุมที่นิยมมากวิธีหนึ่งสำหรับการศึกษาการควบคุมของระบบสารสนเทศ โดยจัดประเภทของการควบคุมเป็นการควบคุมทั่วไปและการควบคุมระบบงาน

1) การควบคุมทั่วไป

การควบคุมทั่วไป (General Controls) เป็นการควบคุมที่เกี่ยวข้องกับกิจกรรมทั้งหมดของระบบสารสนเทศทางการบัญชีและทรัพยากรต่างๆ ของระบบ ซึ่งรายละเอียดของการควบคุมทั่วไปได้อธิบายไว้ในบทที่ 3 การควบคุมทั่วไปและการประเมินความเสี่ยง

2) การควบคุมระบบงาน

การควบคุมระบบงาน (Application Controls) เป็นการควบคุมที่เกี่ยวข้องกับระบบงานแต่ละระบบงาน ซึ่งจะประกอบด้วยการควบคุมที่เกี่ยวของกับกิจกรรมแต่ละกิจกรรมหรือรายการบัญชีเฉพาะรายการ ดังนั้นในบางครั้งการควบคุมประเภทนี้จึงเรียกว่า การควบคุมเฉพาะหรือการควบคุมรายการ (Transaction Controls) ซึ่งรายละเอียดของการควบคุมระบบงานได้อธิบายไว้ในบทที่ 4 การควบคุมระบบงานและการประเมินความเสี่ยง

4. การประเมินความเสี่ยง

โดยทั่วไปขั้นตอนขั้นต้นของการตรวจสอบกรณีกิจการใช้คอมพิวเตอร์ในการประมวลผลข้อมูลคือการทำความเข้าใจเกี่ยวกับธุรกิจที่ตรวจสอบและการประเมินความเสี่ยงของระบบ ซึ่งในการประเมินความเสี่ยงของระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลใช้หลักการพื้นฐานเดียวกันกับการประเมินความเสี่ยงของระบบประมวลข้อมูลแบบอื่นๆ ดังนั้นผู้สอบบัญชีจึงจำเป็นต้องเข้าใจหลักการพื้นฐานที่เกี่ยวข้องได้แก่ ความหมายและประเภทของความเสี่ยง วัตถุประสงค์ของการประเมินความเสี่ยง ปัจจัยที่มีผลกระทบต่อระดับความเสี่ยง ตลอดถึงขั้นตอนและวิธีการประเมินความเสี่ยงและการจัดการและควบคุมความเสี่ยง

4.1 ความหมายและประเภทของความเสี่ยง

ความเสี่ยงในระบบสารสนเทศหมายถึงผลเสียหายที่อาจเกิดขึ้นเนื่องจากภัยที่มีต่อระบบและจุดอ่อนของระบบ ความเสี่ยงในการสอบบัญชี (Audit Risk) หรือโอกาสที่ผู้สอบบัญชีจะแสดงความเห็นต่องบการเงินผิดพลาดอย่างมีสาระสำคัญประกอบด้วยความเสี่ยง 3 ประเภท คือ

1. ความเสี่ยงสืบเนื่อง (Inherent Risk) คือ โอกาสที่จะเกิดข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทหนึ่งๆ ซึ่งเมื่อพิจารณาหรือรวมพิจารณากับข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทอื่นแล้ว มีสาระสำคัญต่อความถูกต้องของงบการเงิน โดยไม่พิจารณาถึงการควบคุมภายในของระบบเลย
2. ความเสี่ยงจากการควบคุม (Control Risk) คือ โอกาสที่จะเกิดข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทหนึ่งๆ ซึ่งเมื่อพิจารณาหรือรวมพิจารณากับข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทอื่นแล้ว มีสาระสำคัญต่อความถูกต้องของงบการเงิน แม้ว่าระบบจะมีการควบคุมภายในก็ตาม กล่าวคือ ระบบบัญชีและระบบการควบคุมภายในที่มีไม่สามารถป้องกัน ตรวจพบและแก้ไขข้อผิดพลาดที่เกิดขึ้นได้ทำให้งบการเงินไม่ถูกต้องและครบถ้วนอย่างมีสาระสำคัญ
3. ความเสี่ยงจากการตรวจสอบ (Detection Risk) คือ โอกาสที่ผู้สอบบัญชีจะสรุปผลจากวิธีการที่ใช้ในการตรวจสอบว่า ข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทหนึ่งๆ เมื่อพิจารณาหรือรวมพิจารณากับข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทอื่นแล้ว ไม่มีสาระสำคัญต่อความถูกต้องของงบการเงิน ทั้งที่ตามความเป็นจริงแล้วมีข้อผิดพลาดที่เป็นสาระสำคัญเกิดขึ้น

ความเสี่ยงทั้งสามประเภทมีความสัมพันธ์กับความเสี่ยงในการสอบบัญชี ดังนี้

ความเสี่ยงในการสอบบัญชี = ความเสี่ยงสืบเนื่อง x ความเสี่ยงจากการควบคุม x ความเสี่ยงจากการตรวจสอบ

จากคำจำกัดความข้างต้นจะเห็นว่าผู้สอบบัญชีไม่สามารถควบคุมระดับของความเสี่ยงสืบเนื่องและความเสี่ยงจากการควบคุมได้ แต่ผู้สอบบัญชีสามารถควบคุมระดับของความเสี่ยงจากการตรวจสอบได้ เนื่องจากระดับของความเสี่ยงจากการตรวจสอบมีความสัมพันธ์โดยตรงกับลักษณะ ระยะเวลาและขอบเขตของวิธีการที่ใช้ในการตรวจสอบ ดังนั้นผู้สอบบัญชีจะต้องพยายามที่จะลดความเสี่ยงในการที่จะแสดงความเห็นต่องบการเงินผิดพลาดอย่างมีสาระสำคัญให้อยู่ในระดับต่ำที่ยอมรับได้ โดยการประเมินระดับของความเสี่ยงสืบเนื่องและความเสี่ยงจากการควบคุม ประกอบกับการวางแผนการสอบบัญชีให้เหมาะสมเพื่อลดความเสี่ยงจากการตรวจสอบ

ในการประเมินความเสี่ยงของระบบสารสนเทศ ผู้สอบบัญชีจำเป็นต้องสามารถระบุความเสี่ยงที่สำคัญของระบบได้ ซึ่งความเสี่ยงในระบบสารสนเทศสามารถแบ่งได้เป็น 6 ประเภท คือ ความเสี่ยงจากข้อผิดพลาดที่ไม่ตั้งใจ ความเสี่ยงจากข้อผิดพลาดที่ตั้งใจ ความเสี่ยงจากการสูญเสียสินทรัพย์ที่ไม่ตั้งใจ ความเสี่ยงจากการขโมยสินทรัพย์ ความเสี่ยงจากการฝ่าฝืนระบบรักษาความปลอดภัยและความเสี่ยงจากภัยธรรมชาติหรือเหตุการณ์ที่รุนแรง ทั้งนี้จะเห็นว่าโอกาสที่จะเกิดความเสียหายอันเนื่องจากความเสี่ยงแต่ละประเภทนั้นขึ้นอยู่กับความเสี่ยงสืบเนื่องของระบบสารสนเทศและประสิทธิผลของระบบการควบคุมภายในที่เกี่ยวข้องกับระบบสารสนเทศของกิจการในการป้องกัน ค้นพบและแก้ไขข้อผิดพลาดหรือรายการผิดปกติที่เกิดขึ้นในเรื่องของความครบถ้วน มีอยู่จริง มูลค่า การแสดงรายการ และความทันต่อเวลาของรายการและข้อมูลในระบบ

1. ความเสี่ยงจากข้อผิดพลาดที่ไม่ตั้งใจ (Unintentional Errors)

ข้อผิดพลาดอาจเกิดจากการที่พนักงานขาดความรู้ เหนื่อยล้า เลินเล่อหรือขาดการควบคุมดูแลจากผู้บังคับบัญชาทำให้นำข้อมูลเข้าที่ไม่ถูกต้องเข้าสู่ระบบ ซึ่งข้อผิดพลาดเช่นนี้ มักจะเกิดขึ้นในลักษณะสุ่ม (Random) ซึ่งเป็นการเกิดขึ้นโดยไม่ตั้งใจและเกิดขึ้นเป็นครั้งคราว เช่น การนำข้อมูลเข้าที่ผิดพลาดเนื่องจากการเลือกหรือพิมพ์รหัสรายการผิดพลาดโดยไม่ตั้งใจของพนักงานขาย เป็นต้น นอกจากนี้ข้อผิดพลาดอาจเกิดขึ้นในช่วงของการประมวลผลของระบบเนื่องจากโปรแกรมที่ใช้ในการประมวลผลมีเงื่อนไขในการ

ประมวลผลที่ไม่ถูกต้องอันอาจเป็นผลจากการที่ผู้พัฒนาโปรแกรมขาดความรู้และความเข้าใจเกี่ยวกับความต้องการของผู้ใช้อย่างเพียงพอตลอดถึงไม่ได้มีการตรวจสอบโปรแกรมอย่างละเอียดก่อนใช้งานจริง ทำให้ผลลัพธ์ (Outputs) ที่ได้จากการประมวลผลไม่ถูกต้องทุกครั้งที่ระบบใช้โปรแกรมนี้ในการประมวลผล

2. ความเสี่ยงจากข้อผิดพลาดที่ตั้งใจ (Deliberate Errors)

ความเสี่ยงจากข้อผิดพลาดที่ตั้งใจเกิดจากความตั้งใจของพนักงานของกิจการที่จะทำการทุจริตหรือบุคคลภายนอกที่จะทำการฉ้อฉลเพื่อผลประโยชน์ส่วนตัวที่ขัดกับกฎหมายหรือระเบียบข้อบังคับของกิจการ เช่น พนักงานรับเงินอาจไม่บันทึกรายการรับเงินเข้าระบบแล้วนำเงินที่ได้รับไปใช้สอยส่วนตัว หรือผู้บริหารอาจสั่งการให้มีการจัดประเภทรายการที่ไม่ถูกต้องเพื่อให้งบการเงินแสดงยอดกำไรที่สูงไป เป็นต้น

3. ความเสี่ยงจากการสูญเสียสินทรัพย์ที่ไม่ตั้งใจ (Unintentional Losses of Assets)

สินทรัพย์อาจจะสูญหายหรือถูกจัดเก็บผิดที่โดยไม่ตั้งใจ เช่น สินค้าที่ได้รับจากผู้ขายอาจถูกจัดเก็บไว้ผิดที่ทำให้หาไม่พบเมื่อต้องการใช้ หรือข้อมูลที่จัดเก็บในสื่ออาจถูกลบทิ้งไปโดยไม่ตั้งใจในระหว่างที่พนักงานปฏิบัติการใช้เทปแม่เหล็กที่มีข้อมูลอยู่แล้วในการทำข้อมูลสำรองชุดใหม่ เป็นต้น

4. ความเสี่ยงจากการขโมยสินทรัพย์ (Thefts of Assets)

สินทรัพย์ของกิจการอาจถูกขโมยโดยบุคคลภายนอกหรือพนักงานของกิจการ เช่น บุคคลภายนอกอาจงัดประตูคลังสินค้าแล้วขโมยสินค้าที่จัดเก็บไป พนักงานอาจนำอุปกรณ์หรือโปรแกรมใช้งานของกิจการไปใช้ที่บ้านเพื่อประโยชน์ส่วนตัว พนักงานอาจทำสำเนาข้อมูลทางการค้าที่สำคัญโดยไม่ได้รับอนุมัติแล้วนำสำเนาดังกล่าวไปให้กับคู่แข่งขันของกิจการ การขโมยสินทรัพย์โดยพนักงานในบางกรณีจะเกิดควบคู่กับการทำข้อผิดพลาดโดยตั้งใจ เช่น การยักยอกเงินโดยพนักงานรับเงินจะเกิดควบคู่กับการไม่บันทึกรายการรับเงินเข้าระบบ

5. ความเสี่ยงจากการฝ่าฝืนระบบรักษาความปลอดภัย (Security Breaches)

บุคคลที่ไม่ได้รับอนุมัติอาจสามารถเข้าถึงข้อมูลหรือรายงานที่สำคัญของกิจการโดยการฝ่าฝืนระบบรักษาความปลอดภัยที่มีอยู่ เช่น พนักงานที่ไม่ได้รับอนุมัติอาจเข้าถึงข้อมูลเงินเดือนของผู้อื่นโดยใช้รหัสผู้ใช้และรหัสผ่านของพนักงานเงินเดือน บุคคลภายนอกหรือแฮ็คเกอร์อาจเข้าถึงระบบผ่านทางอินเทอร์เน็ตแล้วขโมยข้อมูลที่เป็นความลับของกิจการไป

6. ความเสี่ยงจากภัยธรรมชาติหรือเหตุการณ์ที่รุนแรง (Natural Disasters and Violent Acts)

เหตุการณ์ที่รุนแรงที่ทำให้สูญเสียสินทรัพย์อาจทำโดยบุคคลภายนอกหรือภายใน แต่โดยทั่วไปมักเกิดจากพนักงานหรืออดีตพนักงานที่มีปัญหากับกิจการ เช่น การใส่โปรแกรมเข้าไปในระบบเพื่อลบข้อมูลทั้งหมดเมื่อเงื่อนไขที่กำหนดไว้ในโปรแกรมเป็นจริง แต่ถ้าเงื่อนไขที่กำหนดไว้ในโปรแกรมยังไม่เป็นจริงโปรแกรมดังกล่าวก็จะยังไม่ทำงาน นอกจากนี้เหตุการณ์ที่รุนแรงที่ทำให้สูญเสียสินทรัพย์อาจเกิดจากสาเหตุที่ไม่เกี่ยวข้องกับคนหรือเป็นภัยธรรมชาติ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหวหรือพายุ

4.2 วัตถุประสงค์ของการประเมินความเสี่ยงในระบบสารสนเทศ

ผู้สอบบัญชีประเมินความเสี่ยงของระบบที่ใช้คอมพิวเตอร์ในการประมวลข้อมูล เพื่อที่จะระบุถึงโอกาสที่จะเกิดผลเสียหายแก่สินทรัพย์และทรัพยากรด้านสารสนเทศของกิจการอันมีผลกระทบต่อความถูกต้องและน่าเชื่อถือของงบการเงินอย่างมีสาระสำคัญ

กิจกรรมที่ผู้สอบบัญชีทำเพื่อให้เกิดความเข้าใจในความเสี่ยงสืบเนื่องของระบบสารสนเทศและโครงสร้างการควบคุมภายในจะเป็นพื้นฐานแก่ผู้สอบบัญชีในการประเมินระดับความเสี่ยงจากการควบคุม โดยผู้สอบบัญชีจะใช้ข้อมูลดังกล่าวในการประเมินประสิทธิผลหรือความเพียงพอของนโยบายการควบคุมภายในที่เกี่ยวข้องกับระบบสารสนเทศของกิจการ (Internal Control Structure Policies) ในการป้องกัน ค้นพบและแก้ไขข้อผิดพลาดที่มีสาระสำคัญที่ทำให้เกิดผลเสียหายแก่สินทรัพย์และทรัพยากรด้านสารสนเทศของกิจการอันมีผลกระทบต่อความถูกต้องและน่าเชื่อถือของงบการเงินอย่างมีสาระสำคัญ โดยเฉพาะในเรื่องของความครบถ้วน มีอยู่จริง สิทธิและภาระผูกพัน มูลค่า การแสดงรายการและการเปิดเผยข้อมูล ซึ่งผู้สอบบัญชีจะใช้ผลจากการประเมินความเพียงพอของการประเมินประสิทธิผลของการควบคุมภายในหรือความเสี่ยงจากการควบคุมนี้ในการกำหนดกลยุทธ์และแผนการตรวจสอบว่าผู้สอบบัญชีควรจัดสรรเวลาและทรัพยากรอย่างไรระหว่างการประเมินประสิทธิผลการควบคุมภายในเพิ่มเติม (Additional Control Evaluation Procedures) กับการทดสอบเนื้อหาสาระ (Substantive Tests) ตลอดจนถึงการกำหนดลักษณะและขอบเขตการตรวจสอบและการทดสอบรายการที่เหมาะสมเพียงพอในการแสดงความเห็นต่องบการเงิน

4.3 ปัจจัยที่มีผลกระทบต่อระดับความเสี่ยงในระบบสารสนเทศ

ผู้สอบบัญชีต้องพิจารณาปัจจัยที่มีผลกระทบต่อระดับความเสี่ยงของระบบประมวลข้อมูลในการประเมินความเสี่ยงของระบบประมวลข้อมูลของกิจการ ตัวอย่างของปัจจัยเหล่านี้ได้แก่

1. การเปลี่ยนแปลงบุคลากรและคุณภาพของบุคลากร เช่น ระดับการศึกษา ทักษะ ความสามารถ ทัศนคติในการทำงาน และความซื่อสัตย์
2. ลักษณะกิจกรรมขององค์กร ได้แก่ ประเภทธุรกิจของกิจการ ลักษณะและปริมาณของกิจกรรมที่ต้องปฏิบัติ วิธีการปฏิบัติภายในองค์กร วัฒนธรรมและลักษณะขององค์กร ความซับซ้อนของวิธีการบัญชีที่ถือปฏิบัติ ลักษณะของระบบข้อมูลและระบบบัญชี
3. สภาพแวดล้อมของการควบคุมภายในขององค์กร ได้แก่ บรรยากาศในการควบคุมภายในของกิจการ ซึ่งเป็นผลมาจากทัศนคติของผู้บริหารและพนักงานที่มีต่อการควบคุมภายใน มาตรการการควบคุมภายในที่มี และมาตรการที่ใช้เมื่อไม่มีการปฏิบัติตามมาตรการการควบคุมภายในที่กำหนดไว้
4. การเปลี่ยนแปลงข้อบังคับหรือสภาพแวดล้อมในการปฏิบัติงานขององค์กร
5. การเปลี่ยนแปลงระบบสารสนเทศที่ใช้
6. การเจริญเติบโตอย่างรวดเร็วของกิจการ

นอกจากนี้การกำหนดมาตรการที่เหมาะสมเพื่อลดความเสี่ยงของระบบจำเป็นที่จะต้องพิจารณาถึงปัจจัยที่มีผลกระทบต่อระดับของความเสี่ยง ได้แก่ ความถี่ของการเกิดรายการ ขนาดของรายการ และลักษณะของสินทรัพย์ที่ง่ายต่อการถูกขโมยหรือสูญหาย

1. ความถี่ของการเกิดรายการ (Frequency)

รายการหรือเหตุการณ์ที่เกิดขึ้นบ่อยย่อมมีความเสี่ยงที่จะเกิดข้อผิดพลาดหรือรายการผิดปกติสูงกว่ารายการหรือเหตุการณ์ที่เกิดขึ้นไม่บ่อย เช่น กิจการซื้อมาขายไปที่มีรายการขายจำนวนมากย่อมมีความเสี่ยงที่ข้อมูลรายการขายจะมีข้อผิดพลาดสูงกว่ากิจการที่มีรายการขายจำนวนน้อย

2. ขนาดของรายการ (Size)

ระดับความเสี่ยงจะยิ่งสูงหากการสูญเสียที่อาจเกิดขึ้นเกี่ยวข้องกับรายการที่มีมูลค่าเป็นจำนวนเงินมาก เช่น แฟ้มข้อมูลรายการลูกหนี้ของกิจการที่ให้บริการบัตรเครดิตย่อมมีระดับความเสี่ยงสูง เนื่องจากแฟ้มข้อมูลดังกล่าวเก็บข้อมูลที่สำคัญในการเรียกเก็บเงินจากลูกหนี้และรายการแต่ละรายการมักมีจำนวนเงินสูงกว่ารายการซื้อขายที่จ่ายชำระเป็นเงินสด

3. ลักษณะของสินทรัพย์ที่ง่ายต่อการถูกขโมยหรือสูญหาย (Vulnerability)

ระดับความเสี่ยงจะยิ่งสูงหากสินทรัพย์นั้นมีความอ่อนแอต่อถูกขโมยหรือสูญหายสูง เช่น เงินสดหรือสินค้าที่สามารถขายได้ง่ายมีความอ่อนแอต่อสูญหายสูงจึงมีระดับความเสี่ยงสูง

4.4 แนวทางการประเมินความเสี่ยงในระบบสารสนเทศ

การใช้คอมพิวเตอร์ในการประมวลข้อมูลก่อให้เกิดความเสี่ยงนอกเหนือจากที่เกิดในระบบที่ประมวลข้อมูลด้วยมือหรือเครื่องจักรหลายประการ เช่น

- การประมวลข้อมูลด้วยคอมพิวเตอร์อาจทำให้หลักฐานในการติดตามเพื่อการตรวจสอบ (Audit Trail) ขาดหายไป ทั้งนี้เนื่องมาจากมีการรวมขั้นตอนบางขั้นตอนเข้าเป็นขั้นตอนเดียว
- โดยทั่วไปการใช้คอมพิวเตอร์ในการประมวลข้อมูลสืบเนื่องมาจากรายการที่ต้องประมวลมีจำนวนมาก เมื่อมีรายการที่เกี่ยวข้องมาก โอกาสที่จะเกิดข้อผิดพลาดก็จะมีมากตามไปด้วย
- การใช้คอมพิวเตอร์ในการประมวลข้อมูลอาจสืบเนื่องมาจากรายการที่ต้องประมวลมีความซับซ้อนในการคำนวณมาก ดังนั้นโอกาสที่จะเกิดข้อผิดพลาดก็จะมีมาก
- ในระบบที่ใช้คอมพิวเตอร์ประมวลข้อมูล ข้อมูลจะถูกเก็บไว้ในหน่วยความจำชั่วคราวและสื่อแม่เหล็ก ซึ่งโอกาสที่ข้อมูลจะสูญหายหรือเสียหายจะมีมากกว่าระบบที่ประมวลข้อมูลด้วยมือหรือเครื่องจักร
- โอกาสที่จะมีการใช้ข้อมูลผิดในการประมวลข้อมูลจะสูงในระบบที่ใช้คอมพิวเตอร์
- ทางเดินของเอกสารและขั้นตอนการควบคุมภายในจะแตกต่างไปเมื่อมีการใช้คอมพิวเตอร์ในการประมวลข้อมูล
- ผู้ใช้ข้อมูลอาจเชื่อถือผลจากระบบคอมพิวเตอร์มากเกินไป ซึ่งในทางปฏิบัติแล้วผลที่ได้จากระบบคอมพิวเตอร์อาจผิดพลาดได้ หากข้อมูลเข้า ขั้นตอนในการประมวลข้อมูล หรือวิธีการและเงื่อนไขที่ใช้ในการประมวลข้อมูล (Logic) ไม่ถูกต้อง

อย่างไรก็ตามในการตรวจสอบกรณีกิจการใช้คอมพิวเตอร์ประมวลผล ผู้สอบบัญชีไม่ควรประเมินความเสี่ยงของระบบส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูลแยกต่างหากจากระบบส่วนอื่นที่ไม่ได้ใช้คอมพิวเตอร์ เนื่องจากระบบส่วนที่ประมวลข้อมูลด้วยคอมพิวเตอร์ยังคงมีความเกี่ยวข้องและต่อเนื่องกับกิจกรรมต่างๆขององค์กรและการประมวลข้อมูลของส่วนอื่นๆ ที่ทำด้วยมือ

โดยมากความเสี่ยงจากข้อผิดพลาดและความผิดปกติในระบบที่ใช้คอมพิวเตอร์ประมวลข้อมูลมักจะเกี่ยวเนื่องกับระบบงานเฉพาะแต่ละระบบงาน อย่างไรก็ตามการใช้ระบบคอมพิวเตอร์อาจจะมีข้อผิดพลาดหรือความผิดปกติในตัวเองโดยไม่เกี่ยวเนื่องกับระบบงานใดเลย เช่น

ข้อผิดพลาดหรือเหตุการณ์ที่ผิดปกติ	ผลกระทบ
การเลิกใช้ฮาร์ดแวร์หรือซอฟต์แวร์โดยไม่ได้รับการอนุมัติหรือไม่มีการบันทึกรายการ	สินทรัพย์แสดงมูลค่าที่สูงกว่าความเป็นจริง
ไม่มีการบันทึกหนี้สินที่เกิดขึ้นจากการซื้อหรือเช่าฮาร์ดแวร์หรือซอฟต์แวร์	หนี้สินแสดงยอดที่ต่ำกว่าความเป็นจริง
ใช้ฮาร์ดแวร์หรือซอฟต์แวร์เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้รับอนุมัติ	งบการเงินถูกต้อง แต่ค่าใช้จ่ายบางรายการจะไม่เกี่ยวข้องกับธุรกิจของกิจการ
การใช้บุคลากร วัสดุสิ้นเปลือง และอุปกรณ์ ในกิจกรรมการพัฒนาระบบที่ไม่ได้ผ่านการอนุมัติ	งบการเงินถูกต้อง แต่ค่าใช้จ่ายเกินจากที่อนุมัติ
การทำสำเนาข้อมูลหรือโปรแกรมเพื่อใช้ส่วนตัวหรือเพื่อใช้ในทางมิชอบ	ไม่มีผลโดยตรงต่องบการเงิน แต่อาจก่อให้เกิดผลเสียที่ร้ายแรงต่อบริษัทในอนาคต

ดังนั้นในการประเมินความเสี่ยงจึงอาจแยกทำได้เป็น 2 ระดับ คือ ระดับระบบ (System Level) และระดับระบบงาน (Application Level)

1. การประเมินความเสี่ยงในระดับระบบ

เป็นการวิเคราะห์และประเมินความเสี่ยงในระดับภาพรวมของการประมวลข้อมูลด้วยคอมพิวเตอร์ทั้งระบบ ซึ่งครอบคลุมถึงการวิเคราะห์ความเสี่ยงที่เกี่ยวข้องกับการใช้ทรัพยากรในการพัฒนาระบบ และการใช้ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลและอุปกรณ์ต่างๆ ในระบบ

โดยในการประเมินความเสี่ยงของระบบส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูลนี้ ผู้สอบบัญชีจะต้องระบุความเสี่ยงที่เป็นสาระสำคัญและโอกาสที่จะเกิดผลเสียหาย (Material Risks and Exposures) ในส่วนที่เกี่ยวกับ

- การวางแผนในส่วนที่เกี่ยวกับระบบสารสนเทศและการจัดองค์กรของหน่วยงานระบบสารสนเทศ
- การพัฒนาระบบและการนำระบบไปใช้งานจริง

- การใช้งานระบบในเรื่องของการเข้าถึงทั้งด้านตรรกะและด้านกายภาพ (Logical and Physical Access Controls) รวมถึงการจัดการเกี่ยวกับแผนสำรองเผื่อฉุกเฉินและการสำรองทรัพยากรสารสนเทศอย่างเหมาะสมต่อการฟื้นฟูระบบในกรณีที่เกิดเหตุฉุกเฉิน
- การติดตามและตรวจสอบในส่วนต่างๆ ข้างต้น

ซึ่งรายละเอียดของการประเมินความเสี่ยงในระดับระบบได้อธิบายเพิ่มเติมในบทที่ 3 การควบคุมทั่วไปและการประเมินความเสี่ยง

2. การประเมินความเสี่ยงในระดับระบบงาน

ผู้สอบบัญชีควรประเมินความเสี่ยงที่เกี่ยวข้องกับกลุ่มของกิจกรรมและรายการที่รวมกันเป็นระบบงาน โดยผู้สอบบัญชีจะต้องวิเคราะห์ความสำคัญของระบบงานแต่ละระบบงานต่อความถูกต้องและน่าเชื่อถือของงบการเงินและโอกาสที่สินทรัพย์สารสนเทศจะถูกนำไปใช้อย่างไม่เหมาะสม ซึ่งความสำคัญของระบบงานหนึ่งๆ จะแตกต่างไปในกิจการที่ต่างกัน นอกจากนี้ผู้สอบบัญชีจำเป็นต้องระบุรายการ (Transactions) ที่สำคัญๆ ที่ประมวลผลภายในแต่ละระบบงานด้วย โดยผู้สอบบัญชีต้องทำการวิเคราะห์ความเสี่ยงในด้านต่างๆ ในรายละเอียด เช่น ความเสี่ยงที่จะเกิดรายการที่ไม่ถูกต้อง (Invalid Transactions) รายการที่ไม่ได้รับการอนุมัติ (Unauthorized Transactions) หรือรายการที่ไม่ได้รับการบันทึก (Unrecorded Transactions) ความเสี่ยงที่จะประเมินมูลค่าไม่ถูกต้อง (Improper Valuation) ความเสี่ยงที่จะบันทึกรายการล่าช้า (Untimely Recording) ความเสี่ยงที่จะจัดประเภทรายการไม่ถูกต้อง (Improper Classification) และความเสี่ยงที่จะผ่านรายการไม่ถูกต้อง (Incorrect Posting)

ผู้สอบบัญชีจะต้องประเมินโอกาสที่จะเกิดความเสี่ยงเหล่านี้ ความถี่ที่จะเกิดและผลเสียหายที่จะเกิดตามมาเพื่อพิจารณาถึงระดับความเสี่ยงจากข้อผิดพลาดและความผิดปกติที่เกี่ยวข้องกับรายการแต่ละประเภท โดยปกติผลของข้อผิดพลาดหรือความผิดปกติจะจำกัดเพียงรายการหนึ่งๆ เท่านั้น แต่ผลดังกล่าวจะซับซ้อนมากขึ้นหากรายการที่ถูกกระทบนั้นก่อให้เกิดรายการอื่นๆ ต่อไป นอกจากนี้จะเห็นว่ารายการที่มียอดเงินสูงย่อมก่อให้เกิดความเสี่ยงมากกว่ารายการที่ยอดเงินต่ำ และข้อผิดพลาดหรือความผิดปกติในการประมวลข้อมูลของบางระบบงานมีโอกาสที่จะถูกพบโดยบุคคลภายนอกมีสูงกว่าระบบงานอื่น เช่น รายการยอดค้างชำระของลูกหนี้และเจ้าหนี้ เป็นต้น

นอกจากนี้ผู้สอบบัญชีต้องพิจารณาถึงความเสี่ยงในระดับข้อมูลด้วยเนื่องจากข้อมูลแต่ละรายการมีความสำคัญต่องบการเงินและความเสี่ยงที่จะเกิดข้อผิดพลาดต่างกัน และในปัจจุบันระบบงานโดยมากจะเก็บข้อมูลในลักษณะฐานข้อมูล ดังนั้นการประเมินความเสี่ยงของข้อมูลแต่ละรายการในฐานข้อมูลจึงควรจะพิจารณาเพิ่มเติมจากการประเมินความเสี่ยงของระบบงานและรายการค้า ในการวิเคราะห์ผู้สอบบัญชีควรทำความเข้าใจและพิจารณาถึงการใช้รายการข้อมูลนั้นๆ โดยระบบงานที่มีผลกระทบที่เป็นสาระสำคัญต่องบการเงิน แหล่งที่มาของข้อมูล จุดที่ก่อให้เกิดการปรับปรุงข้อมูลและขอบเขตการสอบทานและประเมินคุณภาพของข้อมูลที่มีอยู่

ทั้งนี้รายละเอียดของการประเมินความเสี่ยงในระดับระบบงานได้อธิบายเพิ่มเติมในบทที่ 4 การควบคุมระบบงานและการประเมินความเสี่ยง

4.5 การจัดการและการควบคุมความเสี่ยง (Risk Management and Controls)

มาตรการและวิธีการที่สำคัญในการจัดการและควบคุมความเสี่ยงคือ การประเมินความเสี่ยงของระบบสารสนเทศและผลกระทบและการกำหนดให้มีการควบคุมภายในที่เหมาะสมซึ่งจะช่วยลดระดับความเสี่ยงที่จะเกิดข้อผิดพลาดหรือความผิดปกติที่มีผลต่อความถูกต้องของงบการเงินอย่างมีสาระสำคัญได้ อย่างไรก็ตามการควบคุมภายในที่กำหนดไว้จะมีประสิทธิผลก็ต่อเมื่อมีการปฏิบัติตามอย่างเหมาะสมและมีการปรับเปลี่ยนให้เหมาะสมกับสภาพแวดล้อมของระบบสารสนเทศและธุรกิจที่เปลี่ยนแปลงไป

5. การประเมินการควบคุมภายในของระบบสารสนเทศ

การตรวจสอบกรณีกิจการใช้ระบบที่ประมวลข้อมูลด้วยคอมพิวเตอร์จำเป็นอย่างยิ่งที่ผู้สอบบัญชีจะต้องทำการสอบบัญชีอย่างมีระบบ เนื่องจากในระบบคอมพิวเตอร์ผู้สอบบัญชีจะไม่สามารถเห็นและติดตามขั้นตอนและข้อมูลที่อยู่ในแฟ้มข้อมูลต่างๆ ด้วยตาเปล่า ดังนั้นการตรวจสอบที่ไม่มีแผนและขั้นตอนที่เหมาะสมอาจทำให้ผู้สอบบัญชีข้ามการตรวจสอบขั้นตอนการประมวลข้อมูลหรือแฟ้มข้อมูลที่สำคัญไป นอกจากนี้การควบคุมของระบบที่ใช้คอมพิวเตอร์ยังมีความซับซ้อนมากกว่าระบบที่ประมวลข้อมูลด้วยมือ ซึ่งทำให้ยากที่จะพิจารณาว่าโปรแกรมคอมพิวเตอร์และแฟ้มข้อมูลที่ให้ผู้สอบบัญชีตรวจสอบเป็นสำเนาที่ใช้ในการประมวลข้อมูลจริง

การสอบทานและประเมินประสิทธิผลการควบคุมมีความเกี่ยวข้องโดยตรงกับการประเมินระดับของความเสี่ยงจากการควบคุม (Assessed Level of Control Risk) หรือความน่าจะเป็นที่จะไม่สามารถป้องกัน ตรวจพบและแก้ไขการแสดงข้อมูลบัญชีที่ไม่ถูกต้องอย่างทันการณ์ ซึ่งความผิดพลาดนี้อาจเป็นได้ทั้งที่ไม่เจตนาหรือเจตนา เช่น การทุจริตก็ได้ ซึ่งความเสี่ยงจากการควบคุมนี้เป็นปัจจัยสำคัญหนึ่งในการกำหนดขอบเขตการตรวจสอบ ดังนั้นในการตรวจสอบกิจการที่ใช้คอมพิวเตอร์ประมวลผล ผู้สอบบัญชีจึงต้องมีการปฏิบัติงานในเรื่องต่อไปนี้

1. ทำความเข้าใจโครงสร้างการควบคุม

การที่ผู้สอบบัญชีจะมีข้อมูลที่เพียงพอต่อการวางแผนการตรวจสอบอย่างมีประสิทธิผล ผู้สอบบัญชีจะต้องมีความเข้าใจในองค์ประกอบที่สำคัญของโครงสร้างการควบคุมและบันทึกข้อมูลที่เกี่ยวข้องไว้ในกระดาษทำการ โดยสรุปวัตถุประสงค์ที่ผู้สอบบัญชีต้องทำความเข้าใจโครงสร้างการควบคุมของกิจการมีดังนี้

- เพื่อให้ทราบถึงประเภทของความผิดพลาดที่อาจเกิดขึ้นได้
- เพื่อพิจารณาถึงปัจจัยที่มีผลต่อความเสี่ยงที่จะทำให้เกิดความผิดพลาดที่เป็นสาระสำคัญ
- เพื่อใช้ในการออกแบบการทดสอบเนื้อหาสาระ

2. ประเมินความเสี่ยงจากการควบคุม

การประเมินความเสี่ยงจากการควบคุมเป็นกระบวนการในการประเมินประสิทธิผลของการควบคุมในการที่จะป้องกันหรือค้นพบข้อผิดพลาดที่เป็นสาระสำคัญของรายงานการเงิน โดยการประเมินจะใช้วิธีการทดสอบการควบคุม (Test of Controls) ในกรณี

ที่ระบบมีการควบคุมที่ดี ผู้สอบบัญชีจะทำการทดสอบว่าระบบมีการปฏิบัติตามที่ควรจะเป็นหรือไม่ ถ้าผลออกมาว่าระบบเป็นไปตามที่คาดไว้ ผู้สอบบัญชีอาจลดขอบเขตการตรวจสอบลงได้ ในกรณีที่ผู้สอบบัญชีพบว่าระบบมีจุดอ่อนในการควบคุมหรือไม่มีการควบคุมตามที่ควรจะเป็น หรือผู้สอบบัญชีเลือกที่จะไม่อิงการควบคุมที่มีอยู่ในระบบ ผู้สอบบัญชีจำเป็นต้องขยายขอบเขตการตรวจสอบ

3. การทดสอบเนื้อหาสาระ

การทดสอบเนื้อหาสาระประกอบด้วยการตรวจสอบยอด (Tests of Balances) และขั้นตอนการวิเคราะห์ข้อมูลการเงิน ในการทดสอบผู้สอบบัญชีจะต้องพิจารณาว่าโปรแกรมคอมพิวเตอร์ประมวลข้อมูลตามที่ควรจะเป็นหรือไม่ และในการตรวจสอบยอดผู้สอบบัญชีจะต้องตรวจสอบข้อมูลที่ได้จากการประมวลข้อมูลทั้งที่อยู่ในแฟ้มหลักและแฟ้มรายการ ส่วนในการวิเคราะห์ข้อมูลทางการเงินนั้น จะมีประสิทธิภาพมากกว่าหากใช้คอมพิวเตอร์ช่วยเนื่องจากวิธีการที่ใช้ในการวิเคราะห์ส่วนใหญ่จะเป็นการวิเคราะห์อัตราส่วนและแนวโน้ม

ในการตรวจสอบระบบประมวลข้อมูลด้วยคอมพิวเตอร์ผู้สอบบัญชีจะต้องรวบรวมและประเมินหลักฐานเพื่อให้แน่ใจในความน่าเชื่อถือของการควบคุมและข้อมูลที่ประมวลขึ้นโดยคอมพิวเตอร์ การรวบรวมหลักฐานจะกระทำโดยการทดสอบจุดควบคุมต่างๆ ว่าสามารถควบคุมตามที่กำหนดไว้หรือไม่ และโดยการทดสอบรายการและยอดคงเหลือว่าข้อมูลที่อยู่ในแฟ้มข้อมูลสะท้อนถึงรายการค้าของกิจการอย่างเหมาะสม

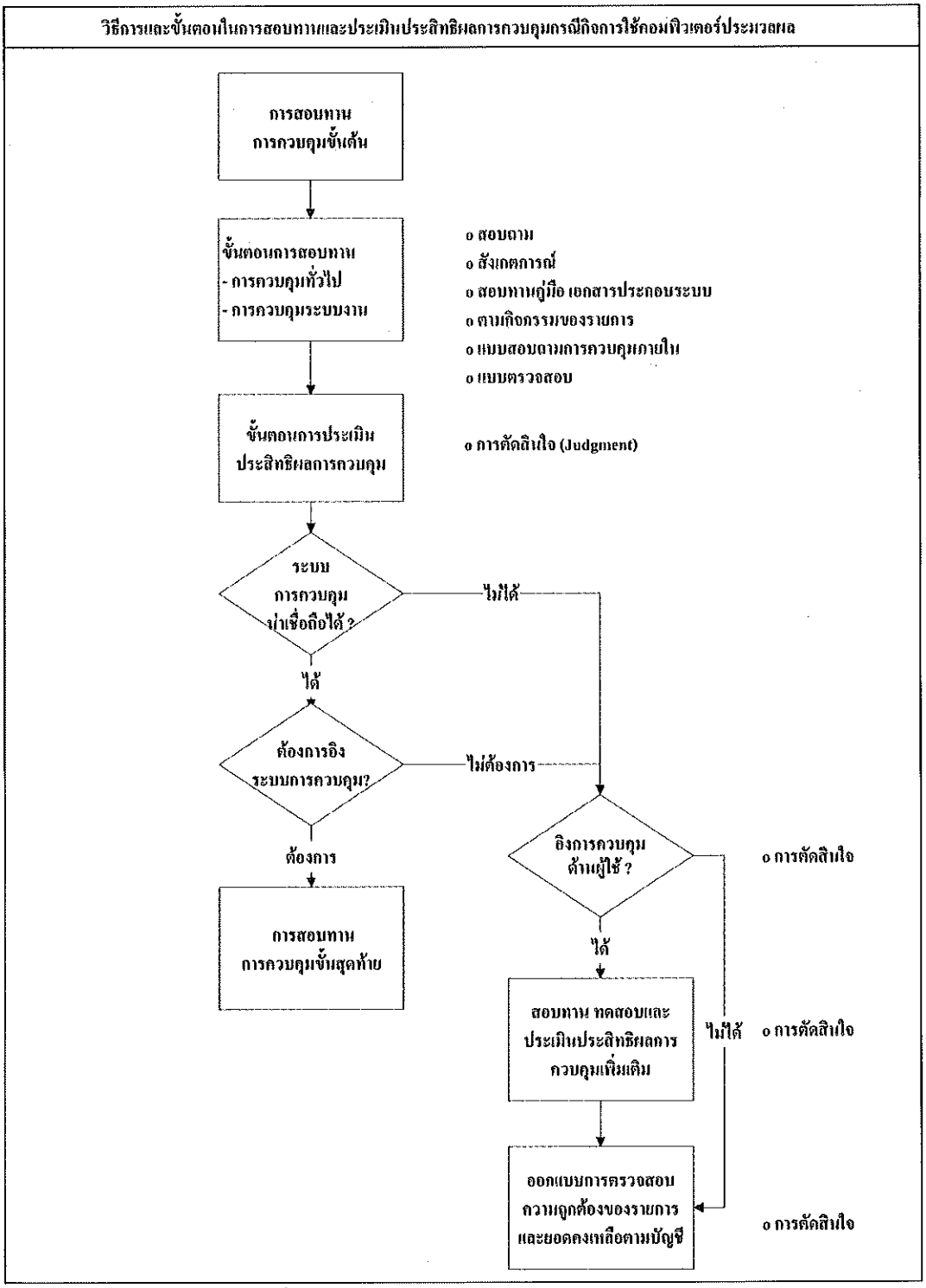
ทั้งนี้ผู้สอบบัญชีมีความรับผิดชอบที่จะต้องรายงานผลการประเมินความเสี่ยงและการควบคุมภายในแก่ผู้ที่เกี่ยวข้อง อันได้แก่ ผู้สอบบัญชีในทีม และลูกค้า ด้วย

5.1 ขั้นตอนในการประเมินการควบคุมของระบบสารสนเทศ

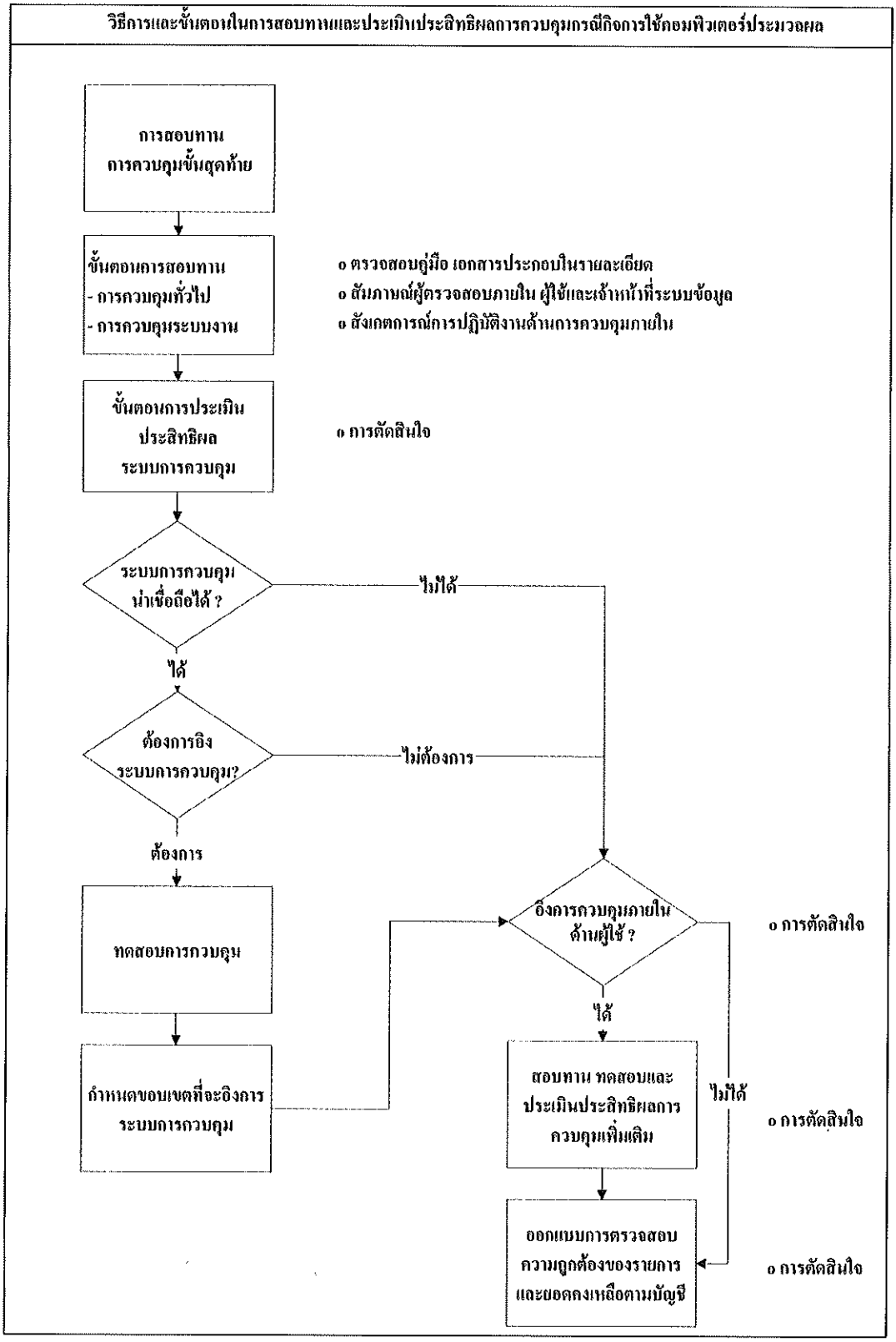
การสอบทานและประเมินการควบคุมของระบบที่ประมวลข้อมูลด้วยคอมพิวเตอร์จะสามารถแบ่งออกได้เป็นสองขั้นตอนคือ การสอบทานและประเมินประสิทธิผลการควบคุมขั้นต้น (Preliminary Phase of the Review) และการสอบทานและประเมินประสิทธิผลการควบคุมขั้นสุดท้าย (Completion Phase of the Review) โดยในแต่ละขั้นตอนผู้สอบบัญชีจะต้องพิจารณาทั้งการควบคุมทั่วไปและการควบคุมระบบงานของระบบที่ตรวจสอบ อย่างไรก็ตามระดับและรายละเอียดของการสอบทานในแต่ละขั้นตอนจะแตกต่างกันอย่างมาก ทั้งนี้ในการประเมินว่าการควบคุมที่กำหนดไว้มีอยู่จริงหรือไม่นั้น ผู้สอบบัญชีสามารถใช้วิธีการเช่นเดียว

กับการประเมินการควบคุมของระบบที่ประมวลข้อมูลด้วยมือ เช่น ใช้วิธีการสังเกตการณ์การปฏิบัติงานเพื่อให้แน่ใจว่ามีการแบ่งแยกหน้าที่ตามที่กำหนดไว้หรือไม่ ในกรณีที่การควบคุมถูกสร้างไว้ในระบบคอมพิวเตอร์ ผู้สอบบัญชีอาจจำเป็นต้องใช้คอมพิวเตอร์ช่วยในการประเมิน เช่น ผู้สอบบัญชีอาจประมวลผลข้อมูลทดสอบ (Test Data) ผ่านระบบเพื่อให้แน่ใจว่าระบบจะไม่รับรายการที่ไม่ถูกต้องตรงตามที่กำหนดไว้ เป็นต้น โดยในปีแรกของการตรวจสอบ ผู้สอบบัญชีจำเป็นต้องรวบรวมข้อมูลในรายละเอียด และในกรณีที่เหมาะสมทำการสอบทานและประเมินประสิทธิผลการควบคุมของระบบ ส่วนในปีถัดไปของการตรวจสอบ ผู้สอบบัญชีไม่จำเป็นต้องทำการสอบทานและประเมินการควบคุมของระบบในรายละเอียดซ้ำกับที่ได้ทำไปแล้วในปีแรก หากระบบไม่มีการเปลี่ยนแปลงจากเดิมในจุดที่เป็นสาระสำคัญ ในกรณีที่ระบบมีการเปลี่ยนแปลงไปจากเดิม ผู้สอบบัญชีจำเป็นต้องเก็บข้อมูลเกี่ยวกับการเปลี่ยนแปลงดังกล่าวและประเมินความเสี่ยงและผลกระทบตลอดถึงสอบทานประเมินประสิทธิผลการควบคุมของระบบที่เปลี่ยนแปลงไป

วิธีการและขั้นตอนในการสอบทานและประเมินประสิทธิผลการควบคุมกรณีกิจการใช้คอมพิวเตอร์ประมวลผลได้สรุปในภาพ 2-2



ภาพ 2-2 *วิธีการและขั้นตอนในการสอบทานและประเมินประสิทธิผลการควบคุมกรณีกิจการใช้คอมพิวเตอร์ประมวลผล*



ภาพ 2-2 วิธีการและขั้นตอนในการสอบทานและประเมินประสิทธิผลการควบคุมกรณีกิจการใช้คอมพิวเตอร์ประมวลผล (ต่อ)

5.2 การสอบทานการควบคุมของระบบสารสนเทศขั้นต้น

การสอบทานและการประเมินประสิทธิผลการควบคุมขั้นต้นมีวัตถุประสงค์เพื่อพิจารณาถึงผลของการควบคุมของระบบคอมพิวเตอร์ในส่วนที่มีสาระสำคัญต่อการตรวจสอบว่า ผู้สอบบัญชีจะสามารถอิงการควบคุมของระบบได้มากน้อยเพียงใดและจะต้องขยายขอบเขตการสอบทานเพิ่มเติมหรือไม่ ซึ่งปริมาณงานที่ผู้สอบบัญชีจะต้องทำเพื่อให้บรรลุวัตถุประสงค์ของขั้นตอนนี้ขึ้นอยู่กับลักษณะและความซับซ้อนของระบบประมวลข้อมูล โดยในขั้นตอนนี้จะประกอบด้วยขั้นตอนย่อย 2 ขั้นตอนคือขั้นตอนการสอบทานการควบคุมและขั้นตอนการประเมินประสิทธิผลการควบคุม

5.2.1 ขั้นตอนการสอบทานการควบคุม

ในขั้นตอนนี้ผู้สอบบัญชีจะสอบทานการควบคุมทั่วไปและการควบคุมระบบงานเพื่อระบุและทำความเข้าใจในเรื่องต่อไปนี้

- ขอบเขตของการใช้คอมพิวเตอร์ในการประมวลข้อมูลในแต่ละระบบงานบัญชีที่สำคัญ
- ทางเดินของรายการและเอกสารในภาพรวม (High-Level Diagram)
- โครงสร้างการควบคุมภายในที่กำหนดไว้ในระบบ

ผู้สอบบัญชีระบุและทำความเข้าใจเกี่ยวกับระบบสารสนเทศและการควบคุมโดยการรวบรวมข้อมูลเกี่ยวกับระบบคอมพิวเตอร์และการควบคุมที่เกี่ยวกับกิจกรรมของหน่วยงานระบบสารสนเทศ เช่น

- ขอบเขตการใช้คอมพิวเตอร์ในการประมวลข้อมูล เช่น จำนวนและประเภทของรายการที่ประมวลข้อมูลด้วยคอมพิวเตอร์ ยอดเงินรวมของรายการแต่ละประเภท ขอบเขตและลักษณะของการประมวลข้อมูลที่ทำด้วยคอมพิวเตอร์
- การจัดองค์การและการแบ่งสายงานและหน้าที่
- ลักษณะและการทำงานของคอมพิวเตอร์ อุปกรณ์ ชุดคำสั่งงานกลาง ระบบและโปรแกรมที่ใช้
- วิธีการจัดเก็บและนโยบายการรักษาข้อมูลและโปรแกรม
- การพัฒนาและดูแลรักษาระบบงาน
- การนำข้อมูลเข้าคอมพิวเตอร์และโปรแกรมคำสั่งงาน

- การกำหนดขั้นตอนการปฏิบัติงานฉุกเฉิน
- นโยบายการจัดหาเครื่องคอมพิวเตอร์สำรองไว้ภายนอกกิจการ
- เอกสารประกอบระบบ

5.2.1.1 การสอบทานการควบคุมทั่วไป

ในขั้นตอนนี้ผู้สอบบัญชีจะต้องหาข้อมูลเพื่อทำความเข้าใจเกี่ยวกับการออกแบบการควบคุมทั่วไปของกิจการ (General Control Design) ในเรื่องต่อไปนี้

- การควบคุมทางด้านการจัดองค์การของหน่วยงานระบบสารสนเทศว่ามีการควบคุมดูแลและแบ่งแยกงานอย่างเหมาะสมภายในหน่วยงานประมวลข้อมูลและระหว่างหน่วยงานประมวลข้อมูลกับผู้ใช้หรือไม่
- การควบคุมในส่วนของการพัฒนาระบบ การเข้าถึงเอกสารประกอบระบบและการบำรุงรักษาและปรับปรุงระบบและโปรแกรม
- การควบคุมในด้านการปฏิบัติการของคอมพิวเตอร์และการเข้าถึงแฟ้มข้อมูลและโปรแกรมที่ใช้งานจริง และการฟื้นฟูแฟ้มข้อมูลและระบบประมวลข้อมูล
- การสอบทานและตรวจสอบระบบควบคุมภายในทางด้านคอมพิวเตอร์

ผู้สอบบัญชีอาจใช้วิธีการต่อไปนี้ในการสอบทาน

- สอบถามบุคคลากรของกิจการ
- สอบทานคู่มือปฏิบัติงานของกิจการ คำบรรยายลักษณะงาน ผังทางเดินเอกสาร ตารางการตัดสินใจ และเอกสารอื่นๆ นโยบายหรือขั้นตอนต่างๆ ที่มีผลต่อการควบคุมภายใน
- เลือกและติดตามดูการปฏิบัติในการบันทึกรายการบัญชีตามระบบที่วางไว้โดยการตรวจตลอด (System Walkthrough)

ซึ่งรายละเอียดของการสอบทานการควบคุมทั่วไปในขั้นตอนนี้ได้อธิบายเพิ่มเติมในบทที่ 3 การควบคุมทั่วไปและการประเมินความเสี่ยง

5.2.1.2 การสอบทานการควบคุมระบบงาน

สำหรับการสอบทานการควบคุมระบบงาน ซึ่งเป็นการควบคุมที่มีผลต่อความสมบูรณ์และถูกต้องของข้อมูลในแต่ละระบบงาน ผู้สอบบัญชีจะต้องรวบรวมข้อมูลของแต่ละระบบงานในเรื่องต่อไปนี้

- การออกแบบการควบคุมด้านข้อมูลเข้าที่ทำให้แน่ใจได้ว่า ข้อมูลที่เข้าสู่ระบบเพื่อประมวลข้อมูลผ่านการอนุมัติที่เหมาะสม มีความสมบูรณ์ ถูกต้อง ไม่ซ้ำซ้อน หรือถูกเปลี่ยนแปลง
- การออกแบบการควบคุมด้านการประมวลข้อมูลที่ทำให้แน่ใจได้ว่าการประมวลข้อมูลเป็นไปตามที่ควรจะเป็น รายการทุกรายการที่ประมวลเป็นรายการที่ได้รับการอนุมัติและไม่มีรายการที่ได้รับอนุมัติรายการใดไม่ถูกประมวล
- การออกแบบการควบคุมด้านข้อมูลออกที่ทำให้แน่ใจว่า ผลของการประมวลถูกต้องและผู้ที่ได้รับข้อมูลออกเป็นผู้ที่ได้รับอนุมัติเท่านั้น

โดยในการสอบทานการควบคุมระบบงานในขั้นตอนนี้ ผู้สอบบัญชีสามารถใช้วิธีการเดียวกับที่ใช้ในการสอบทานการควบคุมทั่วไป ทั้งนี้รายละเอียดของการสอบทานการควบคุมระบบงานได้อธิบายเพิ่มเติมในบทที่ 4 การควบคุมระบบงานและการประเมินความเสี่ยง

5.2.2 ขั้นตอนการประเมินประสิทธิผลการควบคุม

เมื่อผู้สอบบัญชีทำการสอบทานการควบคุมของระบบแล้ว ผู้สอบบัญชีจะนำข้อมูลที่ได้มาใช้ในการประเมินประสิทธิผลการควบคุม ในขั้นตอนนี้ผู้สอบบัญชีจะต้องประเมินถึงความสำคัญของการควบคุมของระบบคอมพิวเตอร์เปรียบเทียบกับการควบคุมของระบบบัญชีทั้งระบบ ทั้งนี้เพื่อระบุถึงขอบเขตการสอบทานการควบคุมภายในของระบบสารสนเทศ ซึ่งในการประเมินผู้สอบบัญชีอาจสรุปว่า

1. การควบคุมภายในของระบบส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูลมีข้อบกพร่องทำให้ไม่สามารถเชื่อถือการควบคุมได้ ในกรณีนี้ผู้สอบบัญชีไม่จำเป็นต้องทำการสอบทานเพิ่มเติม และไม่ต้องทำการทดสอบการควบคุม ทั้งนี้ผู้สอบบัญชีต้องประเมินผลกระทบของจุดอ่อนดังกล่าวต่อความถูกต้องของงบการเงินและใช้วิธีการอื่นแทนเพื่อให้บรรลุวัตถุประสงค์ของการตรวจสอบ เช่น การทดสอบสาระสำคัญเพื่อทดสอบความถูกต้องของรายการบัญชี

2. การควบคุมภายในของระบบส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูลตามที่กำหนดไว้มีประสิทธิผลพอเพียงที่จะเชื่อถือ และสามารถเอาไปใช้ประโยชน์ในการปฏิบัติงานสอบบัญชีและลดขอบเขตการทดสอบรายการได้ ในกรณีนี้ผู้สอบบัญชีจะต้องทำการสอบทานการควบคุมภายในของระบบให้เสร็จสิ้นและจดบันทึกข้อมูลเกี่ยวกับระบบบัญชีส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูลเพื่อใช้ในการประเมินประสิทธิผลขั้นสุดท้ายและทดสอบการควบคุมต่อไป
3. ผู้สอบบัญชีอาจเลือกที่จะไม่ทำการสอบทานการควบคุมภายในเพิ่มเติม และไม่ทำการทดสอบการควบคุมในส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูล แม้ว่าผู้สอบบัญชีจะสรุปว่าการควบคุมภายในของระบบที่มีอยู่เพียงพอ ในกรณีนี้ผู้สอบบัญชีจะไม่สามารถอิงขั้นตอนการควบคุมภายในของระบบส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูลในการสอบบัญชีได้ สถานการณ์ที่ผู้สอบบัญชีตัดสินใจที่จะเลือกปฏิบัติเช่นนี้อาจเนื่องจาก
    - ผู้สอบบัญชีสรุปว่าทรัพยากรที่ต้องใช้ในการสอบทานและทดสอบการควบคุมเพิ่มเติมมากกว่าทรัพยากรที่สามารถประหยัดได้เนื่องจากผู้สอบบัญชีสามารถลดขอบเขตการตรวจสอบบัญชีโดยการอิงการควบคุมภายในของระบบในส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูล
    - ผู้สอบบัญชีสรุปว่าการควบคุมภายในของระบบในส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูลบางส่วนซ้ำซ้อนกับการควบคุมภายในที่มีอยู่แล้วในส่วนอื่นของระบบรวม

5.3 การสอบทานการควบคุมของระบบสารสนเทศขั้นสุดท้าย

หากในการสอบทานและการประเมินประสิทธิผลการควบคุมขั้นต้นชี้ว่าการควบคุมของระบบส่วนที่ใช้คอมพิวเตอร์ประมวลข้อมูลเชื่อถือได้ และผู้สอบบัญชีตัดสินใจที่จะอิงการควบคุมเหล่านั้น ผู้สอบบัญชีจะต้องทำการสอบทานและประเมินประสิทธิผลการควบคุมขั้นสุดท้าย ซึ่งจะประกอบด้วยการสอบทานการควบคุมทั่วไปและการควบคุมระบบงาน การทดสอบการควบคุม และการประเมินประสิทธิผลการควบคุม โดยผลที่ได้จากขั้นตอนนี้จะใช้ในการระบุขอบเขตของการทดสอบสาระสำคัญต่อไป

ในขั้นตอนนี้ผู้สอบบัญชีควรจะพิจารณาถึงประเภทของข้อผิดพลาดและความผิดปกติที่อาจเกิดขึ้นในรายละเอียด และระบุขั้นตอนการควบคุมที่สามารถป้องกันหรือค้นพบข้อผิดพลาดหรือความผิดปกติดังกล่าวด้วย

5.3.1 ขั้นตอนการสอบทาน

5.3.1.1 การสอบทานการควบคุมทั่วไป

การสอบทานการควบคุมทั่วไปในขั้นสุดท้ายนี้ ผู้สอบบัญชีควรจะระบุจุดอ่อนและจุดแข็งที่สำคัญที่จะต้องพิจารณาเมื่อทำการประเมินประสิทธิผลการควบคุมระบบงาน ในขั้นตอนนี้ผู้สอบบัญชีควรหาข้อมูลเพิ่มเติมจากที่ได้ในขั้นตอนแรกจากการสอบถาม สังเกตการณ์ และตรวจสอบเอกสาร คู่มือและผังองค์กร ทั้งนี้ผู้สอบบัญชีควรจะรวบรวมรายละเอียดในเรื่องต่อไปนี้

- วิธีการจัดองค์กรของหน่วยงานระบบสารสนเทศที่ทำให้เกิดการควบคุมดูแลและการแบ่งแยกงานอย่างเหมาะสมภายในหน่วยงานและระหว่างหน่วยงานกับผู้ใช้
- ขั้นตอนที่ทำให้เกิดการควบคุมที่เหมาะสมในการพัฒนาระบบและการเข้าถึงเอกสารประกอบระบบ
- ขั้นตอนที่ทำให้เกิดการควบคุมที่เหมาะสมในการบำรุงรักษาและปรับปรุงโปรแกรมและระบบ
- ขั้นตอนที่ทำให้เกิดการควบคุมที่เหมาะสมในการปฏิบัติการของคอมพิวเตอร์และการเข้าถึงแฟ้มข้อมูลและโปรแกรม
- ขั้นตอนที่ทำให้แน่ใจว่าการสร้างแฟ้มข้อมูลใหม่และการประมวลข้อมูลซ้ำใหม่เป็นไปอย่างสมบูรณ์
- ขอบเขตที่ผู้ตรวจสอบภายในทำการสอบทานและประเมินกิจกรรมการประมวลข้อมูลด้วยคอมพิวเตอร์

ซึ่งรายละเอียดของการสอบทานการควบคุมทั่วไปในขั้นตอนนี้ได้อธิบายเพิ่มเติมในบทที่ 3 การควบคุมทั่วไปและการประเมินความเสี่ยง

5.3.1.2 การสอบทานการควบคุมระบบงาน

ในการสอบทานการควบคุมระบบงาน ผู้สอบบัญชีจะต้องคำนึงถึงจุดอ่อนและจุดแข็งของการควบคุมภายในที่พบในระหว่างการสอบทานการควบคุมทั่วไป ในขั้นตอนนี้ผู้สอบบัญชีควรจะเก็บข้อมูลเพิ่มเติมจากที่ได้ทำไปแล้วในขั้นตอนการสอบทานขั้นต้น โดยการสอบถาม สังเกตการณ์ และตรวจสอบเอกสาร คู่มือ และผังทางเดินเอกสาร ในระหว่างการสอบทานผู้สอบบัญชีควรรวบรวมรายละเอียดในเรื่องต่อไปนี้

- รายละเอียดขั้นตอนและวิธีการด้านข้อมูลเข้าที่ทำให้แน่ใจได้ว่า ข้อมูลที่ได้รับมาเพื่อประมวลข้อมูลโดยคอมพิวเตอร์ได้รับการอนุมัติที่เหมาะสม มีความสมบูรณ์ ถูกต้อง ไม่ซ้ำซ้อน หรือถูกเปลี่ยนแปลง
- รายละเอียดขั้นตอนและวิธีการด้านการประมวลข้อมูลที่ทำให้แน่ใจว่า การประมวลข้อมูลเป็นไปตามที่ควรจะเป็น รายการทุกรายการที่ประมวลเป็นรายการที่ได้รับการอนุมัติและไม่มีรายการที่ได้รับอนุมัติรายการใดไม่ถูกประมวล
- รายละเอียดขั้นตอนและวิธีการด้านข้อมูลออกที่ทำให้แน่ใจว่า ผลของการประมวลถูกต้องและผู้ที่ได้รับข้อมูลออกเป็นผู้ที่ได้รับอนุมัติเท่านั้น

ซึ่งรายละเอียดของการสอบทานการควบคุมระบบงานได้อธิบายเพิ่มเติมในบทที่ 4 การควบคุมระบบงานและการประเมินความเสี่ยง

ในขั้นตอนสุดท้ายของการสอบทาน ผู้สอบบัญชีอาจพบว่าระบบการควบคุมมีจุดอ่อนทำให้ไม่สามารถอิงการควบคุมภายในดังกล่าวในการตรวจสอบได้ หรือการทดสอบการปฏิบัติตามของจุดควบคุมเฉพาะจุด (Specific Controls) ไม่สามารถทำได้อย่างมีประสิทธิภาพ ผู้สอบบัญชีอาจเปลี่ยนแปลงการตัดสินใจที่จะอิงการควบคุมภายในของระบบและตัดสินใจที่จะหยุดการสอบทาน ทั้งนี้ผู้สอบบัญชีจะต้องประเมินผลกระทบของจุดอ่อนในการควบคุมภายในที่พบต่อความถูกต้องของงบการเงิน และใช้วิธีการอื่นทดแทนในการตรวจสอบ การที่ผู้สอบบัญชีตัดสินใจที่จะไม่ทำการสอบทานต่อไปอาจทำได้ใน 2 ระดับคือ

- เมื่อผู้สอบบัญชีไม่สามารถอิงการควบคุมภายในของระบบงานบัญชีระบบใดระบบหนึ่ง ทำให้ผู้สอบบัญชีเลือกที่จะไม่ทำการสอบทานการควบคุมภายในของทั้งระบบ
- เมื่อผู้สอบบัญชีไม่สามารถอิงการควบคุมภายในของระบบงานบัญชีที่มีสาระสำคัญระบบหนึ่งหรือมากกว่า ทำให้ผู้สอบบัญชีตัดสินใจที่จะหยุดทำการสอบทานการควบคุมภายในของระบบนั้นๆ แต่ยังคงทำการสอบทานการควบคุมภายในของระบบงานอื่นที่เหลืออยู่ต่อไป

หากผู้สอบบัญชีตัดสินใจที่จะอิงการควบคุมของระบบส่วนที่ใช้คอมพิวเตอร์ประมวลผลในการตรวจสอบ ผู้สอบบัญชีจะต้องพิจารณาว่าขั้นตอนต่างๆ ที่กำหนดไว้ได้มีการปฏิบัติตามในระดับที่เหมาะสมหากผู้สอบบัญชีพบว่าการปฏิบัติงานไม่เป็นไปตามระบบการควบคุมภายใน

ที่วางไว้ ผู้สอบบัญชีจะต้องใช้วิธีการทดสอบความถูกต้องของรายการบัญชีในการตรวจสอบแทน ในการทดสอบการปฏิบัติตามมุ่งเน้นที่จะตอบคำถามต่อไปนี้

- ได้มีการปฏิบัติขั้นตอนต่างๆ ที่จำเป็นหรือไม่
- ขั้นตอนเหล่านี้ได้ถูกปฏิบัติอย่างไร
- ใครเป็นผู้ปฏิบัติขั้นตอนเหล่านี้

ผู้สอบบัญชีควรตรวจสอบหลักฐานของการปฏิบัติตามขั้นตอนการควบคุมภายใน เช่น ลายเซ็นอนุมัติ ยอดคุม (Control Totals) และรายงานแสดงรายการแก้ไขหรือข้อผิดพลาด (Edit or Error Listings) สำหรับการควบคุมบางประเภทจะไม่มีหลักฐาน เช่น การแบ่งแยกงาน ผู้สอบบัญชีควรใช้วิธีสังเกตการณ์และสอบถามแทน โดยสรุปวิธีการทดสอบการปฏิบัติงานตามระบบอาจทำได้โดยการสอบถาม การสังเกตการณ์ การตรวจสอบหลักฐาน และการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ

5.3.2 ขั้นตอนการประเมินประสิทธิผลการควบคุม

การประเมินประสิทธิผลการควบคุมในขั้นตอนนี้ ผู้สอบบัญชีควรจะพิจารณาถึงประเภทของข้อผิดพลาดและความผิดปกติที่อาจเกิดขึ้น ระบุขั้นตอนการควบคุมที่สามารถป้องกันหรือค้นพบข้อผิดพลาดหรือความผิดปกติดังกล่าว พิจารณาว่ามีการกำหนดขั้นตอนการควบคุมที่จำเป็นไว้และมีการปฏิบัติตามอย่างเหมาะสม และประเมินจุดอ่อนต่างๆ อันได้แก่ ประเภทของข้อผิดพลาดหรือความผิดปกติที่อาจเกิดขึ้นได้และระบุผลกระทบต่อลักษณะ ระยะเวลา และขอบเขตของขั้นตอนการตรวจสอบที่จะต้องใช้ และข้อเสนอแนะที่จะต้องแจ้งต่อลูกค้า

การจัดทำกระดาษทำการจะต้องเพียงพอที่จะชี้ให้เห็นว่า ผู้สอบบัญชีได้ทำการศึกษาและประเมินระบบการควบคุมของลูกค้าในขอบเขตที่จำเป็นต่อการกำหนดลักษณะ ขอบเขต และระยะเวลาของขั้นตอนการตรวจสอบอื่นที่จะต้องใช้ในตรวจสอบงบการเงิน ซึ่งกระดาษทำการดังกล่าวอาจประกอบด้วย

- คำบรรยาย ผังทางเดินเอกสาร หรือเอกสารอื่นที่บรรยายถึงทางเดินของข้อมูลในระบบบัญชี
- คำบรรยายและหลักฐานของจุดควบคุมต่างๆ ในระบบ
- แบบสอบถามหรือ Checklists ที่ใช้ในการตรวจสอบ
- คำบรรยายของแฟ้มคอมพิวเตอร์ที่สำคัญ
- เอกสารหรือบทวิเคราะห์แสดงผลของการทดสอบการควบคุม

- ตัวอย่างแบบฟอร์มและรายงานคอมพิวเตอร์
- รายงานการสัมภาษณ์บุคลากรของลูกค้า
- รายงานการวิเคราะห์ ประเมิน และบทสรุปเกี่ยวกับความเพียงพอของการควบคุมภายใน
- ข้อวิจารณ์จุดควบคุมภายในที่มีผลกระทบต่อลักษณะ ขอบเขตและระยะเวลาของขั้นตอนการตรวจสอบอื่น

6. เทคนิคและวิธีการตรวจสอบระบบสารสนเทศ

การตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลอย่างมีประสิทธิผลและประสิทธิภาพอาจจำเป็นต้องใช้เทคนิคและวิธีการที่แตกต่างจากการตรวจสอบระบบที่ประมวลผลด้วยมือ บทที่ 9 เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์และบทที่ 15 กรณีศึกษาและการสาธิตการปฏิบัติงานโดยใช้คอมพิวเตอร์ช่วยในการจัดทำบัญชีและสอบบัญชีให้รายละเอียดเพิ่มเติมของเทคนิคและวิธีการที่จะกล่าวถึงต่อไปนี้

6.1 เทคนิคและวิธีการทดสอบการควบคุม

การทดสอบการการควบคุมมีวัตถุประสงค์เพื่อให้แน่ใจว่าการควบคุมที่จำเป็นมีอยู่จริงและมีการทำงานและปฏิบัติตามอย่างเหมาะสมตามที่กำหนดไว้ ตลอดถึงเพื่อบันทึกเกี่ยวกับวิธีการ เวลาและผู้ปฏิบัติงานที่ทำให้เกิดการควบคุมนั้นๆ วิธีการในการทดสอบการควบคุมจึงประกอบด้วยการตรวจสอบบันทึก การทดสอบการทำงานของการควบคุมภายใน การสอบถามบุคลากรที่เกี่ยวข้อง และการสังเกตการณ์การปฏิบัติงาน ซึ่งเทคนิคสำคัญที่ผู้สอบบัญชีสามารถใช้ในการปฏิบัติงานเพื่อให้มั่นใจว่าการประมวลผลของระบบและการทำงานของการควบคุมเป็นไปตามที่กำหนดไว้ ได้แก่ การทดสอบโดยใช้ข้อมูลสมมติ การทดสอบแบบไอทีเอฟ การทดสอบโดยการใช้โปรแกรมในการติดตามรายการ การทดสอบโดยการสอบทานเงื่อนไขและตรรกะของโปรแกรม การทดสอบโดยการใช้โปรแกรมเพื่อเปรียบเทียบคำสั่งโปรแกรม การทดสอบโดยการใช้โปรแกรมอรรถประโยชน์ การทดสอบโดยการใช้โปรแกรมจำลอง การทดสอบโดยการใช้โปรแกรมตรวจสอบฝังตัว

6.1.1 การทดสอบโดยใช้ข้อมูลสมมติ (Test Data)

การใช้การทดสอบโดยใช้ข้อมูลสมมติมีวัตถุประสงค์เพื่อให้ผู้สอบบัญชีสามารถพิสูจน์อย่างเป็นอิสระว่าโปรแกรมระบบงานมีการทำงานตามที่ควรจะเป็น โดยโปรแกรมระบบงานต้องสามารถประมวลข้อมูลที่ถูกต้องได้อย่างถูกต้องและต้องสามารถที่จะระบุและปฏิเสธที่จะรับข้อมูลที่ไม่ถูกต้องในการประมวลผล

ในการทดสอบโดยใช้ข้อมูลสมมติ ผู้สอบบัญชีจะต้องกำหนดข้อมูลสมมติที่จะใช้ในการทดสอบขึ้น ซึ่งข้อมูลสมมติดังกล่าวควรจะประกอบด้วยรายการที่มีข้อมูลถูกต้องและรายการที่มีข้อมูลไม่ถูกต้องสำหรับกรณีต่างๆ ครบทุกกรณี ดังนั้นวิธีการนี้จึงเหมาะสมและมีประโยชน์ในกรณีที่จำนวนเงื่อนไขที่ต้องทดสอบมีไม่มาก นอกจากนี้ผู้สอบบัญชีจำเป็นจะต้องทราบผลลัพธ์ที่ถูกต้องของรายการที่ใช้ในการทดสอบด้วย ในการทดสอบผู้สอบบัญชีจะนำข้อมูลสมมติที่กำหนดขึ้นนี้เข้าสู่ระบบเพื่อประมวลผลโดยโปรแกรมระบบงานที่กิจการใช้จริง โดยการทดสอบจะทำในสภาพแวดล้อมที่ไม่ใช่สภาพแวดล้อมที่กิจการประมวลผลข้อมูลจริง ผลลัพธ์ที่ได้จากการประมวลผลจะต้องนำไปเปรียบเทียบกับผลลัพธ์ที่ผู้สอบบัญชีระบุไว้ล่วงหน้าแล้ว ผู้สอบบัญชีสามารถสรุปว่าการทำงานของการควบคุมเป็นไปตามที่กำหนดไว้หากผลลัพธ์ที่ได้จากการประมวลผลไม่แตกต่างจากผลลัพธ์ที่ผู้ตรวจสอบระบุไว้ล่วงหน้า

6.1.2 การทดสอบแบบไอทีเอฟ (Integrated Test Facility or ITF)

การทดสอบแบบไอทีเอฟมีวัตถุประสงค์เช่นเดียวกับการทดสอบโดยใช้ข้อมูลสมมติ แต่จะมีวิธีการที่แตกต่างกัน เนื่องจากการใช้ข้อมูลสมมติในการทดสอบอาจจะทำให้ข้อมูลจริงที่อยู่ในระบบเสียหายได้ การทดสอบแบบไอทีเอฟใช้การเพิ่มหน่วยธุรกิจปลอม (Dummy Entity) เข้าไปในระบบเพื่อให้ผู้สอบบัญชีสามารถทดสอบการทำงานของโปรแกรมระบบงานโดยข้อมูลที่ใช้ในการทดสอบจะอยู่ที่หน่วยธุรกิจปลอมนี้แยกต่างหากจากข้อมูลจริงของระบบ หน่วยธุรกิจปลอมและข้อมูลอื่นที่เกี่ยวข้องจะต้องถูกลบออกจากระบบภายหลังจากการทดสอบเสร็จสิ้นลง ข้อดีของการทดสอบแบบไอทีเอฟคือผู้สอบบัญชีสามารถแน่ใจว่าโปรแกรมระบบงานที่ใช้ในการทดสอบเป็นโปรแกรมระบบงานที่ใช้จริงในการประมวลข้อมูลของระบบสารสนเทศที่ตรวจสอบ

6.1.3 การทดสอบโดยการใช้โปรแกรมในการติดตามรายการ (Program Tracing)

การทดสอบโดยการใช้โปรแกรมในการติดตามรายการมีวัตถุประสงค์เพื่อช่วยผู้สอบบัญชีในการระบุขั้นตอนที่เกิดขึ้นในการประมวลรายการ โปรแกรมติดตามรายการจะจัดทำรายงานแสดงขั้นตอนการประมวลผลรายการของโปรแกรมระบบงาน ซึ่งโปรแกรมติดตามรายการนี้อาจเป็นส่วนหนึ่งของโปรแกรมระบบงานหรืออาจเป็นโปรแกรมพิเศษที่ต้องซื้อหรือพัฒนาขึ้นเพิ่มเติม

6.1.4 การทดสอบโดยการสอบทานเงื่อนไขและตรรกะของโปรแกรม (Program Logic Review)

การทดสอบโดยการสอบทานเงื่อนไขและตรรกะของโปรแกรมมีวัตถุประสงค์เพื่อสอบทานขั้นตอนการประมวลผลที่ทำโดยระบบคอมพิวเตอร์ โดยผู้สอบบัญชีควรเริ่มจากการรวบรวมและสอบทานเอกสารประกอบโปรแกรมเพื่อให้ทราบถึงภาพรวมของโปรแกรมระบบงาน วัตถุประสงค์และหน้าที่งานของระบบงาน จากนั้นผู้ตรวจสอบจึงตรวจสอบโปรแกรมต้นฉบับ (Source Codes) เพื่อระบุการทำงานของโปรแกรมโดยละเอียด การทดสอบโดยวิธีการนี้จำเป็นที่ผู้สอบบัญชีจะต้องมีความรู้เกี่ยวกับการเขียนโปรแกรมอย่างดีและวิธีนี้จะใช้เวลาในการทดสอบมากหากระบบงานมีความซับซ้อนมาก

6.1.5 การทดสอบโดยการใช้โปรแกรมเพื่อเปรียบเทียบคำสั่งโปรแกรม (Program Code Checking)

การทดสอบโดยการใช้โปรแกรมเพื่อเปรียบเทียบคำสั่งโปรแกรมมีวัตถุประสงค์เพื่อให้แน่ใจว่าโปรแกรมระบบงานที่ตรวจสอบเป็นชุดที่ใช้งานจริง หรือเพื่อให้แน่ใจว่าโปรแกรมระบบงานที่ตรวจสอบเป็นชุดเดียวกับที่เคยตรวจสอบแล้ว การทดสอบโดยการใช้โปรแกรมเพื่อเปรียบเทียบคำสั่งโปรแกรมเริ่มจากการที่ผู้สอบบัญชีใช้โปรแกรมเพื่อเปรียบเทียบคำสั่งโปรแกรมในการเปรียบเทียบคำสั่งโปรแกรมต้นฉบับชุดที่ตรวจสอบกับชุดที่ใช้จริงในระบบสารสนเทศทางการบัญชี โปรแกรมเพื่อเปรียบเทียบคำสั่งโปรแกรมจะระบุรายละเอียดความแตกต่างของคำสั่งงานทั้งสองชุดถ้ามีความแตกต่างกัน ในกรณีที่ไม่มีความแตกต่าง ผู้สอบบัญชีจะใช้โปรแกรมเพื่อเปรียบเทียบคำสั่งโปรแกรมในการเปรียบเทียบคำสั่งโปรแกรมชุดที่ตรวจสอบฉบับที่แปลเป็นภาษาเครื่องแล้วกับชุดที่ใช้งานจริง โปรแกรมเพื่อเปรียบเทียบคำสั่งโปรแกรมจะระบุรายละเอียดความแตกต่างของคำสั่งงานฉบับที่แปลเป็นภาษาเครื่องทั้งสองชุดถ้ามีความแตกต่างกัน

6.1.6 การทดสอบโดยการใช้โปรแกรมอรรถประโยชน์ (Utility Programs)

โปรแกรมอรรถประโยชน์เป็นโปรแกรมที่ใช้เพื่อวัตถุประสงค์ทั่วไป เช่น ใช้จัดลำดับแฟ้มข้อมูล การโอนข้อมูลจากสื่อของข้อมูลหนึ่งไปจัดเก็บในอีกสื่อข้อมูลหนึ่ง เป็นต้น การใช้โปรแกรมอรรถประโยชน์ในการทดสอบโดยทั่วไปมักมีวัตถุประสงค์เพื่อโอนย้ายข้อมูล จัดเรียงข้อมูล จัดเตรียมข้อมูล ทำสำเนาข้อมูล จัดพิมพ์ข้อมูลที่ต้องการหรือจัดการข้อมูลที่จำเป็นต้องใช้ในการตรวจสอบ โปรแกรมอรรถประโยชน์มักมาพร้อมกับโปรแกรมประยุกต์ที่กิจการใช้ในระบบสารสนเทศ ซึ่งโปรแกรมอรรถประโยชน์เหล่านี้มักสามารถทำงานได้อย่างรวดเร็ว

6.1.7 การทดสอบโดยการใช้โปรแกรมจำลอง (Simulation Programs)

การทดสอบโดยการใช้โปรแกรมจำลองมีวัตถุประสงค์เพื่อให้ผู้ตรวจสอบสามารถพิสูจน์ผลลัพธ์ออกจากระบบงานได้อย่างเป็นอิสระ โดยผู้สอบบัญชีจะต้องทำการพัฒนาโปรแกรมที่สามารถทำงานหลักๆ ได้เช่นเดียวกับระบบงานที่ตรวจสอบ จากนั้นจึงนำข้อมูลจริงที่เกิดขึ้นมาประมวลผลโดยโปรแกรมที่พัฒนาขึ้น แล้วนำผลลัพธ์ที่ได้ไปเปรียบเทียบกับผลลัพธ์ออกของระบบงานที่ตรวจสอบ ผู้สอบบัญชีอาจใช้การทดสอบวิธีนี้หากโปรแกรมระบบงานที่ต้องตรวจสอบมีความซับซ้อนมากจนผู้สอบบัญชีไม่สามารถพิสูจน์ความถูกต้องของผลลัพธ์ออกได้ด้วยมือ

6.1.8 การทดสอบโดยการใช้โปรแกรมตรวจสอบฝังตัว (Embedded Codes)

การทดสอบโดยการใช้โปรแกรมตรวจสอบฝังตัวมีวัตถุประสงค์เพื่อระบุรายการที่เข้าเงื่อนไขที่กำหนดไว้ โดยโปรแกรมตรวจสอบฝังตัวนี้อาจเป็นโปรแกรมที่มาพร้อมกับโปรแกรมระบบงานหรือเป็นโปรแกรมที่พัฒนาขึ้นแล้วฝังเข้าเป็นส่วนหนึ่งของโปรแกรมระบบงาน ซึ่งโปรแกรมฝังตัวนี้จะทำหน้าที่ในการระบุรายการที่เข้าเงื่อนไขที่กำหนดไว้แล้วจัดเก็บรายการเหล่านั้นในแฟ้มข้อมูลรายการเพื่อให้ผู้สอบบัญชีสามารถดึงข้อมูลจากแฟ้มข้อมูลรายการนี้ไปใช้งานได้เมื่อต้องการ แฟ้มข้อมูลรายการที่เก็บข้อมูลรายการที่สามารถนำไปใช้ในการตรวจสอบนี้จะเรียกกันโดยทั่วไปว่าสคาร์ฟ (SCARF) ซึ่งย่อมาจาก System Control Audit Review File

6.2 เทคนิคและวิธีการทดสอบเนื้อหาสาระ

การทดสอบเนื้อหาสาระมีวัตถุประสงค์เพื่อให้แน่ใจว่ายอดคงเหลือตามบัญชีถูกต้องครบถ้วนและเหมาะสม ระบบสารสนเทศที่ใช้คอมพิวเตอร์ประมวลผลมักมีข้อมูลจำนวนมากทำให้การทดสอบความถูกต้องของรายการและยอดคงเหลือตามบัญชีด้วยมือต้องใช้เวลาและทรัพยากรมาก การใช้คอมพิวเตอร์ช่วยในการทดสอบจึงมีประสิทธิภาพมากกว่า ซึ่งเทคนิคที่ใช้ในการทดสอบการควบคุมที่กล่าวถึงในหัวข้อแรก อาจนำมาใช้ในการทดสอบเนื้อหาสาระได้ อย่างไรก็ตามเทคนิคสำคัญที่ใช้สำหรับการทดสอบเนื้อหาสาระที่นิยมใช้ทั่วไป ได้แก่ การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบและการใช้โปรแกรมที่เขียนขึ้นโดยเฉพาะ ซึ่งในบางกรณีผู้ตรวจสอบอาจใช้เทคนิคนี้ในการทดสอบการควบคุมได้เช่นกัน

6.2.1 การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป

โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป (Generalized Audit Software หรือ GAS) ประกอบด้วยโปรแกรมหนึ่งหรือมากกว่าหนึ่งชุดที่พัฒนาขึ้นเพื่อใช้ในการตรวจสอบเรื่องต่างๆ ของธุรกิจได้เกือบทุกรูปแบบ ตัวอย่างของโปรแกรมสำเร็จรูปสำหรับการตรวจสอบที่ใช้กันอย่างแพร่หลายในปัจจุบัน ได้แก่ IDEA (Interactive

Data Extraction and Analysis) และ ACL (Audit Command Language) โปรแกรมสำเร็จรูปสำหรับการตรวจสอบสามารถช่วยผู้สอบบัญชีในการปฏิบัติงานในเรื่องต่อไปนี้

- การอ่านข้อมูลในแฟ้มข้อมูลและดึงข้อมูลจากแฟ้มข้อมูลในระบบสารสนเทศทางการบัญชีตามเงื่อนไขที่ผู้ตรวจสอบต้องการ เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบในการอ่านรายการในแฟ้มข้อมูลหลักลูกหนี้และดึงรายการที่มียอดคงเหลือติดลบเก็บแยกไว้ในอีกแฟ้มข้อมูลหนึ่งเพื่อใช้งานต่อไป เป็นต้น
- การคำนวณยอดคงเหลือของบัญชี เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบรวมยอดคงเหลือของสินค้าคงเหลือแต่ละรายการในแฟ้มข้อมูลหลักสินค้าคงเหลือแล้วนำยอดรวมที่ได้ไปกระทบยอดกับบัญชีคุมสินค้าคงเหลือเพื่อให้แน่ใจว่ารายละเอียดของบัญชีสินค้าคงเหลือครบถ้วนและถูกต้องก่อนที่จะนำแฟ้มข้อมูลดังกล่าวไปใช้งานต่อไป เป็นต้น
- การเปรียบเทียบข้อมูลรายการค้า เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบเปรียบเทียบรายการค้าในแฟ้มข้อมูลรายการสั่งซื้อกับแฟ้มข้อมูลรายการรับของและแฟ้มข้อมูลรายการใบแจ้งหนี้เพื่อให้แน่ใจว่าการบันทึกหนี้สินถูกต้องและครบถ้วนในแง่ของปริมาณ ราคาและงวดเวลา เป็นต้น
- การรวมยอด เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบรวมยอดขายในแฟ้มข้อมูลรายการขาย การรวมยอดซื้อในแฟ้มข้อมูลใบแจ้งหนี้ เป็นต้น
- การวิเคราะห์และจัดกลุ่มข้อมูล เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบจัดกลุ่มรายการในแฟ้มข้อมูลรายการขายตามรหัสลูกค้าแล้วหายอดขายรวมสำหรับลูกค้าแต่ละราย การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบจัดกลุ่มรายการในแฟ้มข้อมูลรายการขายตามรหัสสินค้าแล้วหายอดขายรวมสำหรับสินค้าแต่ละราย การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบวิเคราะห์ปริมาณการซื้อของลูกค้าแต่ละรายในช่วงเวลาหนึ่งๆ เป็นต้น
- การจัดเรียงข้อมูลตามเงื่อนไขที่ต้องการ เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบในการจัดลำดับรายการในแฟ้มข้อมูลหลักเจ้าหนี้ตามยอดคงเหลือจากมากไปน้อย การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบในการจัดลำดับรายการในแฟ้มข้อมูลรายการรับของตามวันที่ที่รับของจากก่อนไปหลัง เป็นต้น
- การคัดเลือกรายการเพื่อทดสอบ เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบในการเลือกรายการในแฟ้มข้อมูลหลักสินค้าคงเหลือที่มียอดคงเหลือมากกว่า 50,000 บาทเพื่อใช้ในการสังเกตการตรวจนับ การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบในการเลือกรายการในแฟ้มข้อมูลหลักเจ้าหนี้การค้าที่มียอดคงเหลือมากกว่า 500,000

บาทเพื่อทำหนังสือยืนยันยอดคงเหลือ เป็นต้น

- การคำนวณค่าสถิติต่างๆ ของข้อมูลในแฟ้มข้อมูล เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบในการคำนวณอัตราหมุนของสินค้าคงเหลือ อายุเฉลี่ยของลูกหนี้ อายุเฉลี่ยของเจ้าหนี้ เป็นต้น
- การพิมพ์หนังสือยืนยันยอดและรายงานในรูปแบบต่างๆ โดยใช้ข้อมูลที่อยู่ในระบบ เช่น การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบในการพิมพ์หนังสือยืนยันยอดเจ้าหนี้การค้า เป็นต้น

6.2.2 การใช้โปรแกรมที่เขียนขึ้นโดยเฉพาะ

โปรแกรมที่เขียนขึ้นโดยเฉพาะ (Specialized Audit Software) ประกอบด้วยโปรแกรมหนึ่งหรือมากกว่าหนึ่งชุดที่พัฒนาขึ้นสำหรับใช้ในการตรวจสอบเฉพาะกรณีหรือเพื่อการตรวจสอบเฉพาะเรื่อง ตัวอย่างเช่น

- การตรวจสอบความถูกต้องของรายการค้าของธุรกิจที่มีระบบสารสนเทศที่มีลักษณะเฉพาะซึ่งทำให้ไม่สามารถใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบช่วยในการตรวจสอบได้ เช่น แฟ้มข้อมูลในระบบสารสนเทศอาจไม่สามารถโอนมาอยู่ในสื่อในรูปแบบที่สามารถใช้กับโปรแกรมสำเร็จรูปสำหรับการตรวจสอบได้ จึงจำเป็นต้องใช้โปรแกรมที่เขียนขึ้นโดยเฉพาะในการดึงข้อมูลที่ต้องการมาจัดเก็บในสื่อในรูปแบบที่สามารถประมวลผลต่อได้ หรือแฟ้มข้อมูลอาจมีขนาดใหญ่มากทำให้ต้องใช้โปรแกรมที่เขียนขึ้นโดยเฉพาะทำการประมวลผลและวิเคราะห์แฟ้มข้อมูลดังกล่าวภายในระบบสารสนเทศทางการบัญชีแทนที่จะใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทำการประมวลผลและวิเคราะห์แฟ้มข้อมูลดังกล่าวนอกระบบสารสนเทศเป็นต้น
- การตรวจสอบความถูกต้องของรายการค้าของธุรกิจที่มีเงื่อนไขในการบันทึกรายการหรือเงื่อนไขในการคำนวณยอดที่ซับซ้อนทำให้ไม่สามารถใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบช่วยในการตรวจสอบได้ เช่น การคำนวณต้นทุนของสินค้าที่มีสูตรในการผลิตและการปันส่วนต้นทุนที่ซับซ้อน การคำนวณยอดรายได้ตามสัญญาว่าจ้างงานที่มีเงื่อนไขที่ซับซ้อน เป็นต้น

การใช้โปรแกรมที่เขียนขึ้นโดยเฉพาะไม่เป็นที่นิยมใช้ในการทดสอบเนื้อหาสาระสำหรับระบบสารสนเทศ เนื่องจากค่าใช้จ่ายและเวลาที่ใช้ในการพัฒนาโปรแกรมดังกล่าวค่อนข้างสูงและประโยชน์ใช้สอยจะจำกัดเฉพาะกรณีและอาจยากต่อการแก้ไขโปรแกรมในกรณีที่สถานการณ์เปลี่ยนแปลงไป

7. บทสรุป

แม้ว่าการตรวจสอบและการประเมินความเสี่ยงกรณีกิจการใช้คอมพิวเตอร์ประมวลผลข้อมูลมีหลักการพื้นฐานเดียวกับการตรวจสอบและการประเมินความเสี่ยงกรณีกิจการใช้ระบบประมวลข้อมูลแบบอื่นๆ ผู้สอบบัญชีจะต้องตระหนักว่าระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการประมวลผลมีลักษณะสำคัญและความเสี่ยงสืบเนื่องที่แตกต่างไปจากระบบที่ประมวลผลด้วยมือ ดังนั้นวิธีการและเทคนิคที่ใช้ในการตรวจสอบซึ่งรวมถึงการประเมินความเสี่ยงและการประเมินประสิทธิผลการควบคุมภายในจะมีความแตกต่างกันในรายละเอียด

ร่างมาตรฐานการสอบบัญชี รหัส 400 และ 401 เป็นเอกสารอ้างอิงที่สำคัญในการปฏิบัติงานของผู้สอบบัญชีในการตรวจสอบกิจการที่ใช้คอมพิวเตอร์ประมวลผล ดังนั้นผู้สอบบัญชีจึงควรทำความเข้าใจหลักการและวิธีการต่างๆ ที่ระบุในร่างมาตรฐานทั้งสองฉบับนี้ โดยเฉพาะในเรื่องของลักษณะสำคัญของระบบสารสนเทศที่ใช้ในการประมวลผลซึ่งมีผลกระทบต่อความเสี่ยงและการควบคุมภายในของระบบ โครงสร้างของการควบคุมและวัตถุประสงค์ของการควบคุมแต่ละประเภท ตลอดถึงวิธีการและขั้นตอนในการประเมินความเสี่ยงและประสิทธิผลของการควบคุมของระบบสารสนเทศและเทคนิคที่สามารถใช้ช่วยในการตรวจสอบ ทั้งนี้เพื่อให้ผู้สอบบัญชีสามารถปฏิบัติงานการตรวจสอบตามมาตรฐานการสอบบัญชีได้อย่างมีประสิทธิผลและประสิทธิภาพ นอกจากนี้ผู้สอบบัญชีควรทำความเข้าใจเกี่ยวกับมาตรฐานสอบบัญชีระหว่างประเทศ รหัส 1008 ซึ่งเป็นมาตรฐานที่ให้หลักเกณฑ์ในการยกร่างมาตรฐานการสอบบัญชี รหัส 1008 โดยมาตรฐานฉบับนี้ให้หลักการในการประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายในของระบบสารสนเทศที่ใช้คอมพิวเตอร์

8. เอกสารและหัวข้อที่แนะนำให้อ่านเพิ่มเติม

1) สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย. 2543. **ร่างมาตรฐานการสอบบัญชี รหัส 400 เรื่อง การประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายใน.** กรุงเทพมหานคร.

2) สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย. 2543. **ร่างมาตรฐานการสอบบัญชี รหัส 401 เรื่อง การตรวจสอบในสภาพแวดล้อมของระบบสารสนเทศที่ประมวลผลด้วยคอมพิวเตอร์.** กรุงเทพมหานคร.

3) สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย. 2533. **มาตรฐานการสอบบัญชี ฉบับที่ 28 เรื่อง การสอบบัญชีในธุรกิจที่ใช้คอมพิวเตอร์.** กรุงเทพมหานคร.

4) สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย. 2533. **มาตรฐานการสอบบัญชี ฉบับที่ 29 เรื่อง การประเมินประสิทธิภาพการควบคุมภายในกรณีกิจการใช้คอมพิวเตอร์.** กรุงเทพมหานคร.

5) Gallegos, Frederick, Manson, Daniel P., and Allen-Senft, Sandra. 1999. **Information Technology Control and Audit.** Boca Raton: CRC Press LLC.

   หัวข้อ

   A Foundation for IT Auditability and Control, pp. 1-65

6) Hall, James A. 2000. **Information Systems Auditing and Assurance.** South-Western College Publishing.

   หัวข้อ

   Auditing, Assurance, and Internal Control, pp. 1-24

7) International Federation of Accountants. 2534. **International Auditing Practice Statement 1008 : Risk Assessments and Internal Control - CIS Characteristics and Considerations.** New York.

8) Wilkinson, Joseph W., et. al. 2000. Accounting Information Systems: Essential Concepts and Applications. 4th ed. New York: John Wiley & Sons, Inc.

   หัวข้อ

   Risk Exposures and the Internal Control Structure, pp. 233-255

   Auditing of Information Systems, pp. 341-361

9. แบบฝึกหัดปรนัย และแนวคำตอบ

1. ข้อใดต่อไปนี้เป็นลักษณะสำคัญของระบบสารสนเทศ
   ก. หลักการแบ่งแยกหน้าที่ไม่มีความสำคัญสำหรับระบบที่ประมวลผลด้วยคอมพิวเตอร์
   ข. เอกสารขั้นต้นที่ใช้ในการนำข้อมูลเข้าต้องมีรูปแบบเฉพาะ
   ค. ระบบคอมพิวเตอร์มีวัตถุประสงค์ในการควบคุมที่แตกต่างจากระบบที่ประมวลผลด้วยมือ
   ง. หน้าที่ต่างๆอาจรวมเข้าด้วยกันเมื่อใช้ระบบคอมพิวเตอร์ในการประมวลผล

2. ข้อใดต่อไปนี้ไม่ใช่วัตถุประสงค์ของการควบคุมสำหรับระบบสารสนเทศ
   ก. เพื่อให้มั่นใจอย่างสมเหตุสมผลว่าการปฏิบัติงานภายในองค์กรเป็นไปอย่างมีประสิทธิผลและประสิทธิภาพ
   ข. เพื่อให้มั่นใจอย่างสมเหตุสมผลว่ารายงานทางการเงินน่าเชื่อถือได้
   ค. เพื่อให้มั่นใจอย่างสมเหตุสมผลว่าการปฏิบัติงานภายในองค์กรสอดคล้องกับกฎหมายและกฎระเบียบที่มีผลบังคับใช้
   ง. เพื่อให้มั่นใจอย่างสมเหตุสมผลว่าการปฏิบัติงานภายในองค์กรบรรลุเป้าหมายทั้งหมดที่ผู้บริหารกำหนดไว้

3. ข้อใดต่อไปนี้ไม่ใช่องค์ประกอบหลักของโครงสร้างของการควบคุมของระบบสารสนเทศ
   ก. สภาพแวดล้อมของการควบคุม
   ข. กฎ ระเบียบและข้อบังคับตามกฎหมาย
   ค. ระบบบัญชี
   ง. กิจกรรมการควบคุม

4. ข้อใดต่อไปนี้ไม่ใช่ปัจจัยที่สำคัญของสภาพแวดล้อมของการควบคุม
   ก. การแบ่งแยกหน้าที่
   ข. นโยบายด้านบุคลากร
   ค. ปรัชญาในการบริหารงานของผู้บริหาร
   ง. การปฏิบัติหน้าที่และบทบาทของผู้ตรวจสอบภายใน

5. ข้อใดต่อไปนี้ไม่ใช่ปัจจัยที่มีผลกระทบต่อระดับของความเสี่ยง
   ก. ขนาดของรายการ
   ข. ประเภทของรายการค้า
   ค. ความถี่ของการเกิดรายการ
   ง. ลักษณะของสินทรัพย์ที่ง่ายต่อการถูกขโมยหรือสูญหาย

6. ข้อใดต่อไปนี้ไม่ใช่เหตุผลที่ผู้สอบบัญชีต้องพิจารณาถึงความเสี่ยงของระบบสารสนเทศ
   ก. ความเสี่ยงสืบเนื่องของระบบสารสนเทศเป็นปัจจัยสำคัญในการกำหนดการควบคุมที่ระบบควรมี
   ข. การประเมินความเสี่ยงของระบบสารสนเทศทำให้ทราบถึงผลเสียหายที่อาจเกิดขึ้นเนื่องจากภัยที่มีต่อระบบและจุดอ่อนของระบบ
   ค. การประเมินความเสี่ยงของระบบสารสนเทศทำให้ทราบถึงความเหมาะสมของนโยบายในการทำธุรกิจของกิจการ
   ง. ความเสี่ยงจากการควบคุมของระบบสารสนเทศเป็นปัจจัยสำคัญในการกำหนดลักษณะ ระยะเวลาและขอบเขตในการตรวจสอบที่เหมาะสม

7. การตรวจสอบความถูกต้อง ครบถ้วนของข้อมูลเข้าและผลลัพธ์หรือข้อมูลออกของระบบโดยไม่มีการตรวจสอบการประมวลผลของระบบเป็นการตรวจสอบประเภทใด
   ก. การตรวจสอบรอบระบบ
   ข. การตรวจสอบผ่านระบบ
   ค. การทดสอบการควบคุม
   ง. การทดสอบเนื้อหาสาระ

8. ข้อใดต่อไปนี้ไม่ใช่วัตถุประสงค์หลักของการสอบทานการควบคุมของระบบสารสนเทศขั้นต้น
   ก. เพื่อกำหนดลักษณะ ระยะเวลาและขอบเขตในการตรวจสอบความถูกต้องของรายการบัญชี
   ข. เพื่อทำความเข้าใจระบบสารสนเทศที่ประเมินและระบบการควบคุมโดยทั่วไปอย่างเพียงพอที่จะระบุจุดอ่อนที่อาจทำให้เกิดข้อผิดพลาดหรือทุจริตได้
   ค. เพื่อระบุและประเมินระบบการควบคุมและระดับความเสี่ยงด้านการควบคุมในเบื้องต้น
   ง. เพื่อรวบรวมจุดอ่อนของการควบคุมของระบบที่พบเพื่อเสนอแนะต่อผู้บริหารให้ปรับปรุงและแก้ไข

9. ข้อมูลเกี่ยวกับขอบเขตการใช้คอมพิวเตอร์ในการประมวลข้อมูลควรถูกรวบรวมในขั้นตอนใดของการสอบทานการควบคุมของระบบสารสนเทศ
   ก. การสอบทานการควบคุมทั่วไป
   ข. การสอบทานการควบคุมระบบงาน
   ค. การสอบทานการควบคุมขั้นต้น
   ง. การสอบทานการควบคุมขั้นสุดท้าย

10. ข้อใดต่อไปนี้เป็นวัตถุประสงค์หลักของการสอบทานการควบคุมของระบบสารสนเทศขั้นสุดท้าย
    ก. เพื่อระบุและประเมินระบบการควบคุมภายในและระดับความเสี่ยงด้านการควบคุมในเบื้องต้น
    ข. เพื่อกำหนดลักษณะ ระยะเวลาและขอบเขตในการตรวจสอบความถูกต้องของรายการบัญชี
    ค. เพื่อทำความเข้าใจระบบสารสนเทศที่ตรวจสอบและระบบการควบคุมโดยทั่วไปอย่างเพียงพอที่จะระบุจุดอ่อนที่อาจทำให้เกิดข้อผิดพลาดหรือทุจริตได้
    ง. เพื่อสรุปความเพียงพอและประสิทธิผลของโครงสร้างการควบคุมและประสิทธิภาพของการที่ผู้สอบบัญชีจะอิงการควบคุมที่มีในการตรวจสอบระบบสารสนเทศ

แนวคำตอบแบบฝึกหัดปรนัย

1. ง	2. ง	3. ข	4. ก	5. ข
6. ค	7. ก	8. ก	9. ค	10. ข

10. แบบฝึกหัดอัตนัย และแนวคำตอบ

1. ท่านได้รับแต่งตั้งให้เป็นผู้สอบบัญชีของกิจการแห่งหนึ่งซึ่งทำธุรกิจซื้อมาขายไปเป็นปีที่สาม โดยในปีนี้บริษัทได้มีการเปลี่ยนแปลงสภาพแวดล้อมในการประมวลผลข้อมูลจากเดิมที่เคยใช้คอมพิวเตอร์ประมวลผลเฉพาะระบบงานบัญชีแยกประเภททั่วไปมาเป็นระบบที่ใช้คอมพิวเตอร์สนับสนุนกระบวนการทางธุรกิจหลักของกิจการทุกกระบวนการ ให้ท่านระบุขั้นตอนและข้อมูลที่ท่านต้องรวบรวมในแต่ละขั้นตอนเพื่อใช้ในการสอบทานการควบคุมของระบบสารสนเทศขั้นต้น

แนวคำตอบแบบฝึกหัดอัตนัย

ขั้นตอน	ข้อมูลที่ต้องรวบรวม
1. ขั้นตอนการสอบทานการควบคุม	● ขอบเขตของการใช้คอมพิวเตอร์ในการประมวลข้อมูลโดยเฉพาะส่วนที่ผลกระทบต่อการประมวลข้อมูลบัญชีและการจัดทำงบการเงิน ● ทางเดินของรายการและเอกสารในภาพรวม (High-Level Diagram)
1.1 การสอบทานการควบคุมทั่วไป	● การจัดองค์การและการแบ่งสายงานและหน้าที่ ● ลักษณะและการทำงานของคอมพิวเตอร์ อุปกรณ์ ชุดคำสั่งงานกลางระบบและโปรแกรมที่ใช้ ● วิธีการจัดเก็บและนโยบายการรักษาข้อมูลและโปรแกรม ● การพัฒนาและดูแลรักษาระบบงาน ● การกำหนดขั้นตอนการปฏิบัติงานฉุกเฉิน ● นโยบายการจัดหาเครื่องคอมพิวเตอร์สำรองไว้ภายนอกกิจการ ● เอกสารประกอบระบบ

ขั้นตอน	ข้อมูลที่ต้องรวบรวม
1.2 การสอบทานการควบคุมระบบงาน	● การออกแบบการควบคุมด้านข้อมูลเข้าที่ทำให้แน่ใจได้ว่า ข้อมูลที่เข้าสู่ระบบเพื่อประมวลข้อมูลผ่านการอนุมัติที่เหมาะสม มีความสมบูรณ์ ถูกต้อง ไม่ซ้ำซ้อน หรือถูกเปลี่ยนแปลง ● การออกแบบการควบคุมด้านการประมวลข้อมูลที่ทำให้แน่ใจได้ว่า การประมวลข้อมูลเป็นไปตามที่ควรจะเป็น รายการทุกรายการที่ประมวลเป็นรายการที่ได้รับการอนุมัติ และไม่มีรายการที่ได้รับอนุมัติรายการใดไม่ถูกประมวล ● การออกแบบการควบคุมด้านข้อมูลออกที่ทำให้แน่ใจว่า ผลของการประมวลถูกต้อง และผู้ที่ได้รับข้อมูลออกเป็นผู้ที่ได้รับอนุมัติเท่านั้น
2. ขั้นตอนการประเมินประสิทธิผลการควบคุม	ในขั้นตอนนี้โดยปกติจะไม่มีการเก็บข้อมูล แต่เป็นการนำข้อมูลที่ได้จากขั้นตอนการสอบทานการควบคุมมาวิเคราะห์ความเสี่ยงสืบเนื่องและประเมินความเพียงพอของระบบการควบคุมที่กิจการกำหนดไว้ในการลดความเสี่ยงสืบเนื่องให้อยู่ในระดับที่ยอมรับได้

11. บรรณานุกรม

สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย. 2543. ร่างมาตรฐานการสอบบัญชี รหัส 400 เรื่อง การประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายใน. กรุงเทพมหานคร.

_____. 2543. ร่างมาตรฐานการสอบบัญชี รหัส 401 เรื่อง การตรวจสอบในสภาพแวดล้อมของระบบสารสนเทศที่ประมวลผลด้วยคอมพิวเตอร์. กรุงเทพมหานคร.

_____. 2533. มาตรฐานการสอบบัญชีฉบับที่ 28 เรื่อง การสอบบัญชีในธุรกิจที่ใช้คอมพิวเตอร์. กรุงเทพมหานคร.

_____. 2533. มาตรฐานการสอบบัญชีฉบับที่ 29 เรื่อง การประเมินประสิทธิภาพการควบคุมภายในกรณีกิจการใช้คอมพิวเตอร์. กรุงเทพมหานคร.

เยาวลักษณ์ ชาติบัญชาชัย. 2544. "การควบคุมภายในระบบสารสนเทศทางการบัญชี." น. 1-44. เอกสารประกอบการสอนชุดวิชาระบบสารสนเทศทางการบัญชีหน่วยที่ 8-15. (พิมพ์ครั้งที่ 1) กรุงเทพมหานคร: มหาวิทยาลัยสุโขทัยธรรมาธิราช.

_____. 2544. "การตรวจสอบระบบสารสนเทศทางการบัญชี." น. 45-83. เอกสารประกอบการสอนชุดวิชาระบบสารสนเทศทางการบัญชีหน่วยที่ 8-15. (พิมพ์ครั้งที่ 1) กรุงเทพมหานคร: มหาวิทยาลัยสุโขทัยธรรมาธิราช.

Adams, Roger. 1991. "Audit Risk." pp. 144-162. Current Issues in Auditing, 2nd ed. London: Paul Chapman Publishing Ltd.

Bodnar, George H. and William S. Hopwood. 1993. Accounting Information Systems, 5th ed. New Jersey: Prentice-Hall Inc.

Davis, Gordon B., Donald L. Adams and Carol A. Schaller. 1983. Auditing and EDP, 2nd ed. New York: American Institute of Certified Public Accountants, Inc.

Gallegos, Frederick, Manson, Daniel P., and Allen-Senft, Sandra. 1999. Information Technology Control and Audit. Boca Raton: CRC Press LLC.

Grant, Jon. 1991. "Planning for an Effective and Efficient Audit in a Computerized Environment." Current Issues in Auditing, 2nd ed. London: Paul Chapman Publishing Ltd.

Hall, James A. 2000. Information Systems Auditing and Assurance. South-Western College Publishing.

International Federation of Accountants. 2534. International Auditing Practice Statement 1008 : Risk Assessments and Internal Control - CIS Characteristics and Considerations. New York.

Page, John and Hooper, Paul. 1992. Accounting and Information Systems, 4th ed. Englewood Cliffs: Prentice-Hall, Inc.

The COBIT Steering Committee and the IT Governance Institute. 2000. COBIT Framework, 3rd ed. Rolling Meadows: Information Systems Audit and Control Foundation.

The Computer Services Executive Committee. 1977. The Auditor's Study and Evaluation of Internal Control in EDP Systems. New York: American Institute of Certified Public Accountants, Inc.

The Control Risk Audit Guide Revision Task Force. 1999. AICPA Audit Guide: Consideration of Internal Control in a Financial Statement Audit. New York: American Institute of Certified Public Accountants, Inc.

Watne, Donald A. and Peter B. B. Turney. 1990. Auditing EDP Systems, 2nd ed. New Jersey: Prentice-Hall International, Inc.,

Weber, Ron. 1988. EDP Auditing: Conceptual Foundations and Practice, 2nd ed. New York: McGraw-Hill Book Company.

Whittington, O. Ray and Pany, Kurt. 1998. Principles of Auditing, 12th ed. Singapore: The McGraw-Hills Book Company.

Wilkinson, Joseph W. and Cerullo, Michael J. 2000. Accounting Information Systems: Essential Concepts and Applications. 4th ed. New York: John Wiley & Sons, Inc.