บทที่ 2
แนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้อง

แนวคิดและทฤษฎีที่เกี่ยวข้อง

ผู้ศึกษาได้ทำการศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องกับการประเมินความเสี่ยงในการสอบบัญชีของระบบสารสนเทศที่ใช้คอมพิวเตอร์ตามลำดับ ดังนี้

1. แนวคิดเกี่ยวกับการสอบบัญชี
2. แนวคิดเกี่ยวกับการสอบบัญชีในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์
3. การควบคุมภายในของระบบสารสนเทศที่ใช้คอมพิวเตอร์
4. การประเมินความเสี่ยงในการสอบบัญชี

1. แนวคิดเกี่ยวกับการสอบบัญชี (นิพันธ์ เห็นโชคชัยชนะ และศิลปพร ศรีจั่นเพชร, 2550)

1.1 ความหมายของการสอบบัญชี

สมาคมการบัญชีอเมริกัน (The American Accounting Association: AAA) ได้ให้คำนิยามของการสอบบัญชี (Auditing) ไว้ดังนี้ การสอบบัญชี คือ กระบวนการของการรวบรวมและการประเมินหลักฐานเกี่ยวกับสารสนเทศ เพื่อระบุและรายงานเกี่ยวกับระดับความสอดคล้องต้องกันของสารสนเทศนั้นกับหลักเกณฑ์ที่กำหนดไว้และการสื่อสารผลลัพธ์ให้ผู้ใช้ที่สนใจ การสอบบัญชีควรปฏิบัติโดยบุคคลที่มีความรู้ความสามารถและมีความเป็นอิสระ

1.2 วัตถุประสงค์ของการสอบบัญชี

มาตรฐานการสอบบัญชีรหัส 200 เรื่อง วัตถุประสงค์และหลักการพื้นฐานของการสอบบัญชี ระบุว่า การตรวจสอบงบการเงินมีวัตถุประสงค์เพื่อให้ผู้สอบบัญชีสามารถแสดงความเห็นต่องบการเงินว่า งบการเงินนั้นได้จัดทำในส่วนสาระสำคัญเป็นไปตามแม่บทการบัญชีในการรายงานทางการเงินหรือไม่ ดังนั้นวัตถุประสงค์ของการตรวจสอบงบการเงิน คือ การแสดงความเห็นว่างบการเงินนั้นได้แสดงฐานะการเงิน ผลการดำเนินงาน และกระแสเงินสดของกิจการโดยถูกต้องตามควรในสาระสำคัญตามหลักการบัญชีที่รับรองทั่วไปหรือไม่

2. แนวคิดเกี่ยวกับการสอบบัญชีในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์

2.1 ความหมายของการสอบบัญชีในระบบสารสนเทศที่ใช้คอมพิวเตอร์

การตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ หมายถึง การตรวจเพื่อแสดงความเห็นต่อระบบการควบคุมสารสนเทศที่องค์กรใช้ว่าเหมาะสมและเป็นไปตามวัตถุประสงค์ของการควบคุมที่กำหนดไว้หรือไม่ ทั้งนี้ต้องเข้าใจว่าวัตถุประสงค์ของการควบคุมอาจกำหนดโดยผู้บริหารหรือผู้ออกแบบระบบ แต่ผู้ตรวจสอบจะตรวจสอบเพื่อให้ความมั่นใจว่าระบบที่ออกแบบไว้นั้นยังคงเพียงพอ เหมาะสม มีการปฏิบัติตาม และได้ผลตามวัตถุประสงค์ที่กำหนดไว้อย่างไรหรือไม่ (อุษณา ภัทรมนตรี, 2544)

มาตรฐานการสอบบัญชี รหัส 401 เรื่อง การสอบบัญชีในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ได้ให้คำนิยามของสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ไว้ดังนี้ สภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์เกิดขึ้นเมื่อมีการใช้คอมพิวเตอร์ไม่ว่าประเภทใดหรือขนาดใดในการประมวลผลข้อมูลทางการเงินซึ่งมีความสำคัญต่อการสอบบัญชี ทั้งนี้ไม่ว่าการประมวลผลนั้นจะดำเนินการโดยกิจการหรือมอบหมายให้บุคคลภายนอกดำเนินการ (สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์, 2549ค)

2.2 วัตถุประสงค์ของการตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์

การตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์โดยผู้สอบบัญชี มีวัตถุประสงค์เพื่อพิจารณาว่า ระบบสารสนเทศที่กิจการใช้ในการประมวลผลข้อมูลที่จำเป็นต่อการจัดทำงบการเงินและการตรวจสอบมีการทำงานตามที่กำหนดไว้หรือไม่ และรายการทางบัญชีที่บันทึกอยู่ในระบบและข้อมูลออกของระบบมีความถูกต้อง ครบถ้วน และสะท้อนสถานะทางการเงินที่แท้จริงของกิจการหรือไม่ (สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย, 2543)

2.3 ความแตกต่างระหว่างระบบสารสนเทศที่ใช้คอมพิวเตอร์กับไม่ใช้คอมพิวเตอร์

ลักษณะของความแตกต่างระหว่างระบบสารสนเทศที่ใช้คอมพิวเตอร์กับระบบสารสนเทศที่ไม่ใช้คอมพิวเตอร์ มีดังนี้ (สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์, 2549ง)

(1) โครงสร้างการจัดองค์การ

แนวปฏิบัติงานสอบบัญชี รหัส 1008 เรื่อง การประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายใน-ระบบสารสนเทศที่ใช้คอมพิวเตอร์ ระบุว่า ในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ กิจการจะกำหนดโครงสร้างขององค์การและวิธีการปฏิบัติงาน เพื่อบริหารกิจกรรมด้านระบบสารสนเทศที่ใช้คอมพิวเตอร์ ลักษณะโครงสร้างขององค์การด้านระบบสารสนเทศที่ใช้คอมพิวเตอร์ดังกล่าว รวมถึง

– **การรวมหน้าที่งานและความรู้เข้าด้วยกัน**

ถึงแม้ว่าระบบงานส่วนใหญ่ที่ใช้คอมพิวเตอร์ยังมีการปฏิบัติงานด้วยมืออยู่ส่วนหนึ่งก็ตาม แต่โดยทั่วไปแล้วจำนวนบุคลากรที่เกี่ยวข้องในการประมวลผลข้อมูลทางการเงินมักจะมีจำนวนลดลงมาก ยิ่งไปกว่านั้นบุคลากรที่ทำหน้าที่ประมวลผลข้อมูลจะเป็นผู้ที่มีความรู้ในรายละเอียดเกี่ยวกับความสัมพันธ์ระหว่างแหล่งที่มาของข้อมูล วิธีการประมวลผล ตลอดจนการนำเสนอและการใช้ผลที่ได้จากการประมวลผลนั้น โดยส่วนใหญ่บุคคลเหล่านี้จะทราบถึงจุดอ่อนของระบบการควบคุมภายใน และอาจอยู่ในฐานะที่จะเปลี่ยนแปลงแก้ไขโปรแกรมและข้อมูลได้ ไม่ว่าข้อมูลนั้นจะอยู่ระหว่างการเก็บรักษาหรือระหว่างการดำเนินการประมวลผลก็ตาม ดังนั้นการควบคุมแบบเดิมโดยใช้การแบ่งแยกหน้าที่จึงอาจไม่เกิดขึ้น หรืออาจมีประสิทธิผลลดน้อยลง หากไม่มีการควบคุมการเข้าถึงระบบคอมพิวเตอร์และการควบคุมอื่นๆ

– **การจัดเก็บโปรแกรมและข้อมูลไว้ด้วยกัน**

แฟ้มข้อมูลรายการและแฟ้มข้อมูลหลักมักจัดเก็บไว้ด้วยกัน โดยปกติจะเก็บอยู่ในรูปแบบที่อ่านได้โดยใช้คอมพิวเตอร์ และอาจจัดเก็บไว้ในระบบคอมพิวเตอร์ที่ส่วนกลางระบบเดียว หรืออาจจัดเก็บไว้ในระบบคอมพิวเตอร์หลายระบบซึ่งกระจายอยู่ทั่วกิจการ การเรียกใช้หรือเปลี่ยนแปลงข้อมูลดังกล่าวจำเป็นต้องใช้โปรแกรมคอมพิวเตอร์ซึ่งกิจการส่วนใหญ่จะเก็บโปรแกรมไว้ในสถานที่เดียวกับข้อมูล ดังนั้นหากไม่มีการควบคุมอย่างเหมาะสมแล้ว จะเป็นการเพิ่มโอกาสในการเข้าถึงและเปลี่ยนแปลงแก้ไขทั้งข้อมูลและโปรแกรมโดยไม่ได้รับอนุมัติ

(2) ลักษณะของการประมวลผล

แนวปฏิบัติงานสอบบัญชี รหัส 1008 เรื่อง การประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายใน-ระบบสารสนเทศที่ใช้คอมพิวเตอร์ ระบุว่า การนำคอมพิวเตอร์มาใช้มีผลให้ระบบงานมีรูปแบบ ซึ่งให้หลักฐานที่มองเห็นได้น้อยกว่าในระบบงานที่ไม่ใช้คอมพิวเตอร์ นอกจากนั้นจำนวนคนที่สามารถเรียกใช้ข้อมูลจากระบบงานก็มีมากขึ้นด้วย วิธีการประมวลผลโดยคอมพิวเตอร์จึงอาจส่งผลให้ระบบงานมีลักษณะดังต่อไปนี้

– **การไม่มีเอกสารที่ใช้ในการนำข้อมูลเข้าคอมพิวเตอร์**

ข้อมูลอาจนำเข้าสู่เครื่องคอมพิวเตอร์โดยตรงโดยไม่มีเอกสารประกอบการบันทึกรายการในบางระบบที่ข้อมูลถูกส่งมาตามสาย หลักฐานที่เป็นลายลักษณ์อักษรของการอนุมัติรายการและข้อมูลที่นำเข้าคอมพิวเตอร์อาจใช้วิธีการปฏิบัติอย่างอื่นแทน เช่น การนำเรื่องการควบคุมการอนุมัติเข้าไปรวมไว้ในโปรแกรมคอมพิวเตอร์ตั้งแต่แรก และให้คอมพิวเตอร์ควบคุมการอนุมัติโดยตรง ตัวอย่างเช่น การนำเกณฑ์ในการอนุมัติคำสั่งซื้อจากลูกค้าเข้าไปรวมไว้ในคอมพิวเตอร์ล่วงหน้า เมื่อ

นำคำสั่งซื้อจากลูกค้าเข้าเครื่องคอมพิวเตอร์ และคำสั่งซื้อนั้นอยู่ในเกณฑ์ที่กำหนด คอมพิวเตอร์จะอนุมัติและดำเนินการในขั้นตอนต่อไป เป็นต้น

– **การไม่มีหลักฐานการติดตามการบันทึกรายการที่สามารถมองเห็นได้**

ข้อมูลบางอย่างอาจจัดเก็บไว้ในแฟ้มข้อมูลคอมพิวเตอร์เท่านั้น โดยปกติในระบบที่จัดทำด้วยมือจะมีความเป็นไปได้ในการติดตามรายการตลอดระบบงาน โดยตรวจสอบจากเอกสารขั้นต้น สมุดบัญชี และรายงานทางการเงิน อย่างไรก็ตามในระบบงานที่ใช้คอมพิวเตอร์ หลักฐานที่ใช้ในการติดตามรายการนั้น บางส่วนอาจอยู่ในรูปแบบที่อ่านได้โดยใช้คอมพิวเตอร์ นอกจากนี้ข้อมูลดังกล่าวอาจจัดเก็บไว้เพียงช่วงเวลาที่กำหนดเท่านั้น

– **การไม่มีผลลัพธ์จากการประมวลผลที่สามารถมองเห็นได้**

รายการหรือผลที่ได้จากการประมวลผลบางอย่างอาจไม่ได้มีการพิมพ์ออกมาใช้ ในระบบที่จัดทำด้วยมือและระบบสารสนเทศที่ใช้คอมพิวเตอร์บางระบบ ผู้สอบบัญชีสามารถตรวจสอบผลลัพธ์จากการประมวลผลได้ด้วยตา แต่ในระบบสารสนเทศที่ใช้คอมพิวเตอร์บางระบบอาจไม่มีการพิมพ์ผลที่ได้จากการประมวลผลออกมาหรืออาจพิมพ์เฉพาะข้อมูลสรุปเท่านั้น ดังนั้นการไม่มีผลลัพธ์ที่สามารถมองเห็นได้ดังกล่าวอาจทำให้จำเป็นต้องเรียกข้อมูลที่จัดเก็บอยู่ในแฟ้มข้อมูล ซึ่งสามารถอ่านได้โดยใช้คอมพิวเตอร์เท่านั้น

– **การเข้าถึงข้อมูลและโปรแกรมคอมพิวเตอร์ทำได้ง่าย**

ข้อมูลและโปรแกรมคอมพิวเตอร์อาจมีการเข้าถึงหรือเปลี่ยนแปลงแก้ไข ณ สถานที่ตั้งคอมพิวเตอร์ หรือโดยผ่านการใช้อุปกรณ์คอมพิวเตอร์จากสถานที่อื่นได้ ดังนั้นการขาดการควบคุมที่เหมาะสมจะเป็นการเพิ่มโอกาสให้บุคคลที่ไม่ได้รับการอนุมัติทั้งภายในและภายนอกกิจการสามารถเข้าถึง หรือเปลี่ยนแปลงแก้ไขข้อมูลและโปรแกรมคอมพิวเตอร์ได้

(3) การออกแบบและวิธีปฏิบัติงาน

แนวปฏิบัติงานสอบบัญชี รหัส 1008 เรื่อง การประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายใน-ระบบสารสนเทศที่ใช้คอมพิวเตอร์ ระบุว่า โดยทั่วไปการพัฒนาระบบสารสนเทศที่ใช้คอมพิวเตอร์ จะมีผลต่อลักษณะของการออกแบบและการกำหนดวิธีการปฏิบัติงาน ซึ่งจะแตกต่างจากที่พบในระบบงานซึ่งจัดทำด้วยมือ ลักษณะของการออกแบบและการกำหนดวิธีการปฏิบัติงานที่แตกต่างออกไปของระบบสารสนเทศที่ใช้คอมพิวเตอร์ดังกล่าว รวมถึง

– **ความสม่ำเสมอของการปฏิบัติงาน**

เนื่องจากระบบสารสนเทศที่ใช้คอมพิวเตอร์จะกำหนดให้รายการทุกรายการผ่านวิธีการและการควบคุมตามที่เขียนไว้ในโปรแกรมคอมพิวเตอร์เหมือนกันหมด หากมีการกำหนดชนิดของรายการและเงื่อนไขต่างๆ ที่อาจเกิดขึ้นทั้งหมดไว้ในระบบแล้ว การปฏิบัติงานโดยใช้คอมพิวเตอร์

จึงมีแนวโน้มน่าเชื่อถือมากกว่าระบบที่จัดทำด้วยมือ ในทางตรงกันข้ามหากโปรแกรมคอมพิวเตอร์ที่เขียนและทดสอบไม่ถูกต้อง การปฏิบัติงานตามโปรแกรมดังกล่าวอาจก่อให้เกิดรายการหรือข้อมูลอื่นที่ผิดพลาดอย่างต่อเนื่อง

– **วิธีการควบคุมโดยโปรแกรมในระบบงาน**

ลักษณะของการประมวลผลโดยคอมพิวเตอร์สามารถที่จะออกแบบให้มีวิธีการควบคุมภายในรวมอยู่ในโปรแกรมคอมพิวเตอร์ วิธีการควบคุมเหล่านี้อาจไม่สามารถมองเห็นได้ เช่น การป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุมัติอาจทำได้โดยการกำหนดให้ทุกระบบงานมีการตรวจสอบการผ่านเข้าไปใช้งาน โดยต้องระบุรหัสผู้ใช้งานร่วมกับรหัสผ่านที่ถูกต้องเท่านั้น เป็นต้น นอกจากนี้ยังสามารถออกแบบวิธีการปฏิบัติงานอื่นให้ใช้ร่วมกับส่วนงานที่ทำด้วยมือก็ได้ เช่น การสอบทานรายงานเกี่ยวกับรายการที่ผิดปกติซึ่งพิมพ์จากคอมพิวเตอร์ และการตรวจสอบความสมเหตุสมผลและข้อจำกัดของข้อมูล เป็นต้น

– **รายการทางบัญชีรายการเดียวอาจนำไปปรับปรุงฐานข้อมูลหรือแฟ้มข้อมูลคอมพิวเตอร์ได้มากกว่าหนึ่งแฟ้ม**

ข้อมูลรายการเดียวที่นำเข้าระบบบัญชีอาจปรับปรุงข้อมูลทางบัญชีที่เกี่ยวข้องกับรายการนั้นได้พร้อมกันทั้งหมดโดยอัตโนมัติ เช่น เอกสารประกอบการส่งสินค้าอาจใช้ปรับปรุงแฟ้มข้อมูลขาย ลูกหนี้ และสินค้าคงเหลือ เป็นต้น ดังนั้นโอกาสที่จะเกิดความผิดพลาดในการปรับปรุงข้อมูลดังกล่าวจะลดลง ในทางตรงกันข้ามถ้าข้อมูลที่นำเข้าคอมพิวเตอร์ผิดพลาด รายการบัญชีนั้นอาจก่อให้เกิดความผิดพลาดต่อข้อมูลทางบัญชีมากกว่าหนึ่งรายการได้เช่นเดียวกัน

– **รายการที่สร้างขึ้นจากระบบงาน**

รายการบางรายการอาจสร้างจากระบบสารสนเทศที่ใช้คอมพิวเตอร์โดยไม่ต้องใช้เอกสารเป็นสื่อในการนำข้อมูลเข้าคอมพิวเตอร์ การอนุมัติรายการดังกล่าวอาจไม่มีเอกสารหลักฐาน ซึ่งจะแตกต่างจากการอนุมัติรายการที่ไม่ได้ใช้คอมพิวเตอร์ เช่น การคำนวณดอกเบี้ยแล้วผ่านรายการไปยังบัญชีลูกค้าโดยอัตโนมัติตามคำสั่งที่กำหนดเงื่อนไขการอนุมัติไว้แล้วในโปรแกรมคอมพิวเตอร์ ดังนั้นจึงจำเป็นต้องมีการควบคุมการออกแบบระบบงานและวิธีการปฏิบัติงานให้เป็นไปตามที่อนุมัติไว้

– **สื่อที่ใช้ในการเก็บโปรแกรมและข้อมูลมีโอกาสเสียหายได้ง่าย**

ข้อมูลจำนวนมากและโปรแกรมคอมพิวเตอร์ที่ใช้ในการประมวลผลข้อมูลอาจเก็บอยู่ในสื่อที่เคลื่อนย้ายได้หรือไม่ได้ เช่น แผ่นดิสก์หรือเทปแม่เหล็ก สื่อข้อมูลเหล่านี้อาจถูกโจรกรรม สูญหาย หรือถูกทำลายได้ง่ายทั้งโดยเจตนาและไม่เจตนา ดังนั้นจึงจำเป็นต้องมีการออกแบบมาตรการรักษาความปลอดภัยของสื่อเหล่านี้โดยรัดกุม

3. การควบคุมภายในของระบบสารสนเทศที่ใช้คอมพิวเตอร์ (สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย, 2543)

3.1 วัตถุประสงค์ของการควบคุมภายในของระบบสารสนเทศที่ใช้คอมพิวเตอร์

การควบคุมภายในของระบบสารสนเทศที่ใช้คอมพิวเตอร์มีวัตถุประสงค์ไม่แตกต่างจากวัตถุประสงค์ของการควบคุมภายในสำหรับระบบที่ประมวลผลด้วยมือ กล่าวคือ การควบคุมภายในของระบบสารสนเทศเป็นกระบวนการที่ออกแบบขึ้นโดยมีวัตถุประสงค์เพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผล (Reasonable Assurance) ว่ากิจการจะบรรลุวัตถุประสงค์ในเรื่องต่อไปนี้

(1) ประสิทธิผลและประสิทธิภาพในการปฏิบัติงาน

(2) ความน่าเชื่อถือของรายงานทางการเงิน

(3) การปฏิบัติตามกฎหมายและกฎระเบียบที่มีผลบังคับใช้

วัตถุประสงค์ของการควบคุมภายในที่ผู้สอบบัญชีเน้นในการตรวจสอบงบการเงินของกิจการ ได้แก่ วัตถุประสงค์ข้อที่สอง และวัตถุประสงค์ข้อที่สามเฉพาะส่วนที่มีผลกระทบต่อความถูกต้องและการเปิดเผยข้อมูลของงบการเงิน

3.2 องค์ประกอบของการควบคุมภายใน

โครงสร้างของการควบคุมภายใน (Internal Control Structure) ของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ประกอบด้วยนโยบายและขั้นตอนต่างๆ ที่กำหนดขึ้นเพื่อให้สามารถมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ในเรื่องของการดำเนินงานอย่างมีประสิทธิผลและประสิทธิภาพ การจัดทำรายงานทางการเงินที่น่าเชื่อถือ และการปฏิบัติตามกฎหมายและระเบียบข้อบังคับอย่างถูกต้อง ซึ่งมาตรฐานการสอบบัญชีระหว่างประเทศ ฉบับที่ 400 ซึ่งเป็นต้นแบบของมาตรฐานการสอบบัญชี รหัส 400 เรื่อง การประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายใน ได้แบ่งนโยบายและขั้นตอนเหล่านี้เป็น 3 ส่วน ดังนี้

(1) สภาพแวดล้อมของการควบคุม (Control Environment)

สภาพแวดล้อมของการควบคุมเป็นองค์ประกอบสำคัญที่มีผลต่อประสิทธิผลของการควบคุมภายใน เนื่องจากสภาพแวดล้อมของการควบคุมเป็นตัวกำหนดบรรยากาศของกิจการที่มีต่อการควบคุมภายใน ซึ่งเป็นพื้นฐานสำหรับองค์ประกอบอื่นของโครงสร้างการควบคุมภายใน ปัจจัยสำคัญของสภาพแวดล้อมของการควบคุม ได้แก่

- นโยบายและวิธีปฏิบัติเกี่ยวกับบุคลากร
- โครงสร้างองค์กรและวิธีการมอบหมายอำนาจหน้าที่และความรับผิดชอบ
- ปรัชญาและรูปแบบการดำเนินงานของผู้บริหาร

(2) ระบบบัญชี (Accounting System)

ระบบบัญชีประกอบด้วยวิธีการและบันทึกที่จัดทำขึ้น เพื่อบันทึก ประมวลผล รวมยอด และรายงานเกี่ยวกับรายการค้า สินทรัพย์ หนี้สิน และทุนของกิจการ ดังนั้นระบบบัญชีจึงประกอบด้วย 2 องค์ประกอบหลัก ดังนี้

– วิธีการของระบบบัญชี

– เอกสารและบันทึก ได้แก่ เอกสารประกอบระบบ เอกสารประกอบโปรแกรม และเอกสารประกอบการปฏิบัติงาน

(3) กิจกรรมการควบคุม หรือวิธีการควบคุม (Control Activities or Control Procedures)

กิจกรรมการควบคุมเป็นนโยบายและขั้นตอนที่กำหนดขึ้น เพื่อช่วยให้แน่ใจว่ากิจกรรมต่างๆ ที่จำเป็นต่อการลดความเสี่ยงเพื่อให้กิจการสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ได้มีการปฏิบัติตาม กิจกรรมการควบคุมของกิจการอาจมีวัตถุประสงค์หลายหลากและหลายรูปแบบ โดยปกติกิจกรรมการควบคุมที่เกี่ยวข้องโดยตรงกับการตรวจสอบสามารถแยกได้ดังนี้

– การแบ่งแยกหน้าที่

– การควบคุมทางกายภาพ

– การประมวลผลรายการ

– การตรวจสอบผลการปฏิบัติงานอย่างอิสระ

3.3 ประเภทของการควบคุม

การควบคุมภายในของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ประกอบด้วย การควบคุมทั่วไป (General Controls) และการควบคุมระบบงาน (Application Controls) ซึ่งมีรายละเอียดดังนี้

(1) การควบคุมทั่วไป (General Controls)

การควบคุมทั่วไปในระบบสารสนเทศ หมายถึง การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุมภายใน (Internal Control Environment) นโยบายและวิธีการในการควบคุมระบบสารสนเทศ การจัดแบ่งส่วนงานและหน้าที่รวมทั้งวิธีการปฏิบัติงานของผู้ที่เกี่ยวข้องกับระบบสารสนเทศ การควบคุมความปลอดภัยระบบ การควบคุมการพัฒนาและปรับปรุงระบบและการป้องกันความเสียหายหรือลดความเสียหายของระบบ การควบคุมทั่วไปเป็นการควบคุมภายในสำหรับระดับองค์การ หรือการควบคุมที่ควรมีในทุกๆ ส่วนของระบบสารสนเทศโดยมีวัตถุประสงค์เพื่อให้เกิดความมั่นใจว่าระบบคอมพิวเตอร์โดยรวมขององค์กรมีความเสถียร (Stable) มีการจัดการที่ดี และเป็นส่วนหนึ่งที่จะก่อให้เกิดบูรณภาพ (Integrity) ของระบบสารสนเทศของกิจการ การควบคุมทั่วไปในระบบสารสนเทศที่ใช้คอมพิวเตอร์ ประกอบด้วยกิจกรรมต่างๆ ดังนี้

– **การกำหนดนโยบายการใช้สารสนเทศ**

การรักษาความปลอดภัยของข้อมูลและสารสนเทศเป็นการควบคุมที่สำคัญอย่างหนึ่ง จึงต้องมีการกำหนดเป็นนโยบายโดยมีการทบทวนเพื่อทำการปรับปรุงอย่างต่อเนื่อง ในการกำหนดนโยบายเกี่ยวกับความปลอดภัยของข้อมูลและการใช้งานนั้น เริ่มจากการพิจารณาว่าใคร ต้องเข้าถึงข้อมูลอะไร เมื่อไร และข้อมูลนั้นอยู่ในระบบงานใด ซึ่งการพิจารณาดังกล่าวจะเป็นปัจจัยในการระบุภัยคุกคาม (Threats) ความเสี่ยง (Risks) และผลของความเสี่ยง (Exposures) ที่จะมีต่อระบบสารสนเทศ เพื่อให้สามารถเลือกวิธีการรักษาความปลอดภัยที่เหมาะสมที่สุดและคุ้มค่ากับการลงทุน (Cost-Effective) โดยผู้บริหารระดับสูงควรมีหน้าที่ในการกำหนดนโยบาย กำกับดูแล และควบคุมให้เป็นไปตามนโยบายที่กำหนดไว้ โดยมีการทบทวนและปรับปรุงอย่างต่อเนื่องรวมทั้งชี้แจงให้ผู้ปฏิบัติงานที่เกี่ยวข้องทุกคนรับทราบ

– **การแบ่งแยกหน้าที่งานในระบบสารสนเทศที่ใช้คอมพิวเตอร์**

วิธีการหนึ่งในการควบคุมระบบสารสนเทศขององค์กร คือ การแบ่งแยกหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานระบบคอมพิวเตอร์ให้ชัดเจน เพื่อลดโอกาสที่จะเกิดความผิดพลาดจากการปฏิบัติงานและโอกาสการทุจริตของผู้ปฏิบัติงานที่ไม่ถูกจำกัดสิทธิในการเข้าถึงระบบงานโปรแกรมและข้อมูล โดยมีประเภทงานที่ควรมีการแบ่งแยกผู้ปฏิบัติงาน ได้แก่ งานวิเคราะห์ระบบ (System Analysis) งานเขียนโปรแกรม (Programming) งานปฏิบัติการคอมพิวเตอร์ (Computer Operation) งานของผู้ใช้ (User) งานบรรณารักษ์ระบบ (System Library) และงานควบคุมข้อมูล (Data Control) ทั้งนี้การอนุญาตให้ผู้ปฏิบัติงานทำงานได้หลายประเภทงานจะเป็นการเปิดโอกาสให้มีการทุจริตได้ง่าย ตัวอย่างเช่น นักปฏิบัติการคอมพิวเตอร์ที่สามารถเข้าถึงโปรแกรมที่ติดตั้งในระดับตรรกะ (Logic) อาจทำการแก้ไขเปลี่ยนแปลงโปรแกรมเพื่อให้ประมวลผลเพิ่มเงินค่าจ้างของตนเอง เป็นต้น

– **การควบคุมโครงการการพัฒนาระบบสารสนเทศ (Project Development Controls)**

การพัฒนาระบบสารสนเทศที่ขาดการควบคุมการบริหารจัดการที่ดี ก่อให้เกิดความเสี่ยงในการที่ระบบไม่สามารถตอบสนองความต้องการทางธุรกิจ และระบบงานที่พัฒนาขึ้นอาจไม่มีการควบคุมภายในที่เพียงพอทำให้การทำงานผิดพลาด นอกจากนั้นยังเป็นผลให้กิจการสูญเสียเงินลงทุนจำนวนมากในโครงการพัฒนาระบบสารสนเทศ การควบคุมโครงการพัฒนาระบบสารสนเทศประกอบด้วย แผนแม่บทระยะยาว (Long-Range Master Plan) แผนงานพัฒนาระบบ (Project Development Plan) กำหนดการประมวลผลข้อมูล (Data Processing Schedule) การมอบหมายหน้าที่และความรับผิดชอบ (Assignment of Responsibility) การประเมินผลงานระหว่างการดำเนินโครงการ (Periodic Performance Evaluation) การสอบทานภายหลังการติดตั้งระบบและ

นำระบบมาใช้งาน (Post Implementation Review) และการวัดผลการดำเนินงานของระบบ (System Performance Measurements)

– **การควบคุมการเปลี่ยนแปลงแก้ไขระบบ**

การแก้ไขเปลี่ยนแปลงระบบโดยไม่ได้รับอนุญาตอาจมีผลให้เกิดความผิดพลาดในโปรแกรม การทุจริต หรือมีข้อมูลที่ไม่ถูกต้องในงบการเงินและรายงานต่างๆ และอาจทำให้ระบบล้มเหลวหรือหยุดชะงักการทำงานได้ การเปลี่ยนแปลงแก้ไขระบบหรือโปรแกรมที่ใช้อยู่จึงควรมีการกำหนดเป็นขั้นตอนโดยมีการอนุมัติและจัดทำเอกสารประกอบ โดยผู้สอบบัญชีควรมีการสอบทานความเพียงพอของการควบคุมภายในของระบบงานหรือโปรแกรมที่มีการเปลี่ยนแปลงแก้ไขนั้น การควบคุมการเปลี่ยนแปลงแก้ไขระบบประกอบด้วย การกำหนดระเบียบวิธีการปฏิบัติในการเปลี่ยนแปลงแก้ไขระบบที่เป็นลายลักษณ์อักษร และมีการอนุมัติจากเจ้าของระบบงาน มีการศึกษาผลกระทบต่างๆ ทั้งผลกระทบทางด้านเทคนิค ผลกระทบที่มีต่อระบบอื่น และความเสี่ยงจากการเปลี่ยนแปลง มีการทดสอบระบบที่แก้ไขแล้วก่อนนำมาใช้งาน จัดทำเอกสารคู่มือประกอบการแก้ไขเปลี่ยนแปลงทั้งหมด และมีการแก้ไขเอกสารที่เกี่ยวข้อง เช่น คู่มือการใช้งาน คู่มือระบบ ข้อมูลเกี่ยวกับการรักษาความปลอดภัยระบบ และตารางการทำงานของผู้ปฏิบัติงานคอมพิวเตอร์ เป็นต้น และมีการประเมินและสอบทานระบบงานหรือโปรแกรมภายหลังจากเริ่มใช้งานในระยะเวลาหนึ่ง

– **การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์**

ศูนย์คอมพิวเตอร์เป็นหน่วยงานที่ให้บริการคอมพิวเตอร์แก่หน่วยงานอื่น การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์ประกอบด้วย การประมวลผลระบบงาน การสำรองข้อมูล (Data Backup) และการจัดการปัญหาของระบบ

– **การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ (Physical Access Controls)**

การเข้าถึงอุปกรณ์คอมพิวเตอร์ หมายถึง ความสามารถในการเข้าถึงตัวเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ขององค์กร วิธีการควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์เพื่อรักษาความปลอดภัยของอุปกรณ์คอมพิวเตอร์ เช่น สถานที่ติดตั้งอุปกรณ์คอมพิวเตอร์ควรอยู่ในห้องที่มีกุญแจปิด และจำกัดให้ใช้งานได้เฉพาะผู้ที่ได้รับอนุญาต ผู้ปฏิบัติงานต้องติดเครื่องหมายหรือบัตรประจำตัวผู้ผ่านเข้าออกในห้องคอมพิวเตอร์ ติดตั้งระบบเตือนภัยกรณีมีผู้บุกรุก จำกัดสิทธิการใช้โทรศัพท์และเครื่องคอมพิวเตอร์ปลายทาง (Terminal) และเครื่องคอมพิวเตอร์ส่วนบุคคลสำหรับงานส่วนตัว การควบคุมสภาพแวดล้อมในการทำงานของเครื่องคอมพิวเตอร์ โดยมีการควบคุมอุณหภูมิ ความชื้น ฝุ่นละออง มีการติดตั้งระบบป้องกันเพลิงไหม้ เช่น เครื่องตรวจควัน (Smoke Detector) เป็นต้น

– **การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ (Resource)**

ในระบบแฟ้มข้อมูล (Flat File System) ผู้ใช้ข้อมูลต่างก็ดูแลรักษาแฟ้มข้อมูลที่เป็นของตนเอง ระบบดังกล่าวจึงมีสภาพแวดล้อมของการควบคุมที่เอื้ออำนวยต่อการควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ ในทางตรงกันข้ามในระบบฐานข้อมูล (Database System) ซึ่งเน้นความสำคัญของบูรณภาพของข้อมูลและความจำเป็นในการใช้ข้อมูลร่วมกันจะเพิ่มความเสี่ยงในการควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ ตัวอย่างเช่น ความเสี่ยงจากการทุจริต การขโมยข้อมูล การนำข้อมูลไปใช้ในทางที่ผิด การทำลายข้อมูล เป็นต้น ความเสี่ยงเหล่านี้อาจเกิดขึ้นจากการที่มีผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล หรือการที่ผู้ใช้ที่ได้รับอำนาจมีการเข้าถึงข้อมูลที่เกินกว่าขอบเขตที่ได้รับ การควบคุมการเข้าถึงข้อมูลในฐานข้อมูลมีหลายลักษณะ ได้แก่ ทรรศนะของผู้ใช้ (User Views หรือ Subschema) ตารางการอนุญาตให้เข้าถึงฐานข้อมูล (Database Authorization Table) การเข้ารหัสข้อมูล (Data Encryption) การควบคุมการอนุมานข้อมูล (Inference Controls)

– **การควบคุมการเข้าถึงระบบงาน (Logical Access Controls)**

การเข้าถึงระบบงาน หมายถึง ความสามารถในการเข้าถึงโปรแกรมและข้อมูลในระบบงาน การควบคุมความสามารถดังกล่าวเพื่อรักษาความปลอดภัยของโปรแกรมและข้อมูลในระบบงาน ผู้ใช้ระบบจะได้รับอนุญาตให้เข้าถึงข้อมูลได้ เพื่อทำการอ่าน ทำสำเนา เพิ่ม และลบเฉพาะส่วนที่ตนเองมีสิทธิในการใช้งานเท่านั้น และการป้องกันข้อมูลจากบุคคลภายนอกก็มีความสำคัญเช่นเดียวกัน การจำกัดการเข้าถึงระบบงานนั้น ตัวระบบงานเองจะต้องมีความสามารถแยกข้อแตกต่างระหว่างการใช้งานของผู้ได้รับอนุญาตและผู้ไม่ได้รับอนุญาต ข้อมูลใดที่ผู้ใช้ระบบงานทราบหรือเป็นเจ้าของ สถานที่ที่ผู้ใช้ระบบงานเข้าใช้ระบบงาน หรือคุณลักษณะของแต่ละบุคคล วิธีการที่นิยมโดยทั่วไปสำหรับการควบคุมการเข้าถึงจะใช้การตรวจสอบจากสิ่งที่ผู้ใช้งานทราบ ตัวอย่างเช่น ให้เครื่องคอมพิวเตอร์แจ้งให้ผู้ใช้ป้อนรหัสประจำตัวบุคคล เป็นต้น การควบคุมการเข้าถึงระบบงาน ประกอบด้วย การตรวจสอบความแท้จริง (Authentication) การกำหนดสิทธิ (Authorization) การบันทึกกิจกรรมต่างๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)

– **การควบคุมการจัดเก็บข้อมูล (Data Storage Controls)**

สารสนเทศเป็นสิ่งที่สร้างทั้งความได้เปรียบคู่แข่งขันและมูลค่าแก่องค์กร เนื่องจากเป็นทรัพยากรที่ทรงคุณค่า จึงต้องป้องกันผู้ไม่ได้รับอนุญาตมาเปิดเผยหรือทำลาย ซึ่งองค์กรจะต้องกำหนดประเภทของข้อมูลที่จะต้องบำรุงรักษาและระดับการป้องกันที่จำเป็นสำหรับข้อมูลแต่ละประเภท โดยขั้นตอนต่างๆ ในการป้องกันต้องจัดทำเป็นเอกสาร มีการรวบรวมข้อมูลเหตุการณ์ต่างๆ ในการรักษาความปลอดภัย มีการดูแลเอกสาร ข้อมูลประเภทรายการ และแฟ้มข้อมูลลับ และ

มีการเก็บข้อมูลการเข้าไปใช้ข้อมูลลับเหล่านั้นเพื่อให้สามารถตรวจสอบได้ โดยพนักงานจะต้องทำสัญญาว่าจะไม่เปิดเผยข้อมูลที่เป็นความลับของบริษัท

การกำกับดูแลด้วยสารบบแฟ้มข้อมูล (File Library) ที่เหมาะสม เป็นส่วนที่สำคัญในการป้องกันข้อมูลสูญหาย หน่วยงานที่มีหน้าที่จัดเก็บแฟ้มข้อมูล (File Storage) จะต้องเก็บรักษาแฟ้มข้อมูลให้พ้นจากเพลิงไหม้ ฝุ่นผง ความร้อน ความชื้น หรือสถานการณ์ที่สร้างความเสียหายให้กับข้อมูลที่จัดเก็บไว้

การติดป้ายชื่อแฟ้มข้อมูล (File Label) จะช่วยป้องกันการนำไปใช้ผิดประเภทโดยไม่ได้ตั้งใจ ป้ายชื่อภายนอก (External Label) เป็นป้ายกระดาษที่ติดไว้กับอุปกรณ์ที่เป็นหน่วยเก็บ (Storage Device) ซึ่งจะต้องมีชื่อ เนื้อหา และวันที่ประมวลผล ส่วนป้ายชื่อภายใน (Internal Label) เป็นป้ายชื่อที่เครื่องคอมพิวเตอร์อ่านได้จากแบบฟอร์มในสื่อบันทึกข้อมูล ซึ่งจะมีอยู่ 3 ประเภท คือ ป้ายหมวด (Volume Label) ป้ายหัวเรื่อง (Header Label) และป้ายชื่อท้ายแฟ้ม (Trailer Data)

กลไกการป้องกันการเขียนทับ (Write Protection Mechanism) จะช่วยป้องกันผู้ใช้ระบบงานเขียนข้อมูลทับหรือลบข้อมูลโดยไม่ตั้งใจ เช่น ในแผ่นดิสก์เก็ต (Diskette) จะมีสวิตช์เปิด/ปิดให้เลือกป้องกันการเขียนทับได้ แต่เป็นที่น่าเสียดายที่กลไกนี้ยกเลิกได้ง่ายมาก

ในระบบฐานข้อมูล (Database System) จะใช้ผู้บริหารฐานข้อมูล (Database Administrator) พจนานุกรมข้อมูล (Data Dictionary) และการควบคุมการปรับปรุงข้อมูล เพื่อป้องกันข้อมูล โดยผู้บริหารฐานข้อมูลจะเป็นผู้สร้างและควบคุมให้การเข้าถึงและการปรับปรุงฐานข้อมูลเป็นไปตามวิธีการที่กำหนด พจนานุกรมข้อมูลจะสร้างความมั่นใจว่ารายการข้อมูลมีการกำหนดและใช้อย่างถูกต้อง ส่วนการควบคุมการปรับปรุงข้อมูลจะช่วยป้องกันรายการข้อมูลจากข้อผิดพลาดที่เกิดขึ้นจากผู้ใช้หลายคนปรับปรุงฐานข้อมูลรายการเดียวกันพร้อมๆ กัน ซึ่งการควบคุมนี้จะช่วยล็อกข้อมูลรายการนั้นให้ปรับปรุงได้ทีละคน โดยจะปลดล็อกภายหลังจากปรับปรุงเรียบร้อย ผู้ใช้รายอื่นจึงจะสามารถเข้ามาทำการปรับปรุงต่อไป

– การควบคุมการสื่อสารข้อมูล (Data Transmission Controls)

การลดความเสี่ยงจากความล้มเหลวในการสื่อสารข้อมูล องค์กรจะต้องตรวจตราระบบเครือข่ายเพื่อหาจุดอ่อน รวมทั้งการบำรุงรักษาส่วนประกอบที่ใช้ในการสำรอง และออกแบบเครือข่ายให้มีขีดความสามารถเพียงพอที่จะรองรับความต้องการในช่วงเวลาที่มีการใช้งานเต็มที่ และจะต้องสร้างเส้นทางการสื่อสารภายในเครือข่ายไว้หลายๆ เส้นทาง เพื่อให้ระบบสามารถทำงานต่อเนื่องได้แม้ว่าจะมีบางเส้นทางที่ล้มเหลว และนอกจากการบำรุงรักษาอุปกรณ์ในการสื่อสารแล้วควรจะมีการปรับปรุงระบบ เช่น เปลี่ยนสายโทรศัพท์ไปใช้ชนิดที่เร็วกว่าหรือมีประสิทธิภาพมากกว่า เป็นต้น

การเติบโตของอินเทอร์เน็ต (Internet) และพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) ทำให้การเข้ารหัสลับข้อมูล (Data Encryption) เป็นการควบคุมที่สำคัญมาก วิทยาการการเข้ารหัสลับ (Cryptography) เป็นวิทยาการเกี่ยวกับรหัสลับที่มีการนำมาใช้ในการสื่อสารข้อมูลและการพาณิชย์อิเล็กทรอนิกส์ เพื่อให้มั่นใจว่ามีการรักษาความปลอดภัยที่สำคัญ 3 ประการ ได้แก่ ความลับ (Confidentiality) บูรณภาพของข้อมูล (Integrity) และความเป็นตัวตนที่แท้จริง (Authenticity)

การควบคุมการสื่อสารข้อมูลสำหรับการสับเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange: EDI) ในองค์กรที่มีการใช้ประโยชน์จากการสับเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์จะต้องเพิ่มการควบคุมในด้านนี้เป็นการเฉพาะ เนื่องจากมีความเสี่ยงที่ผู้ไม่ได้รับอนุญาตจะเข้าถึงข้อมูลได้ง่าย ในการป้องกันจึงต้องนำเอาการเข้ารหัสข้อมูลมาใช้ในการควบคุม ข้อมูลรายการทุกรายการจะต้องบันทึกการใช้งาน และมีการตรวจตราบันทึกตามรอบระยะเวลาเพื่อให้ทราบว่ามีรายการที่ไม่ถูกต้องเกิดขึ้นหรือไม่

– **การกำหนดมาตรฐานเอกสารระบบสารสนเทศ (Documentation Standards)**

การควบคุมทั่วไปที่สำคัญวิธีการหนึ่งคือ วิธีการและมาตรฐานในการจัดทำเอกสารระบบสารสนเทศ เพื่อให้มั่นใจว่ามีความชัดเจนและรัดกุม การจัดทำเอกสารที่มีคุณภาพทำให้การติดต่อสื่อสารและการติดตามความก้าวหน้าในการพัฒนาระบบงานสะดวกขึ้น และใช้เป็นเอกสารอ้างอิงและเป็นเครื่องมือฝึกอบรมพนักงาน รวมทั้งช่วยให้การบำรุงรักษาและแก้ไขปรับปรุงโปรแกรมประยุกต์สามารถทำได้ง่ายขึ้น การจัดทำเอกสารระบบงานดังกล่าวแยกเป็น 3 ประเภท ได้แก่ การจัดทำเอกสารทางการบริหาร (Administrative Documentation) การจัดทำเอกสารระบบงาน (System Documentation) และการจัดทำเอกสารประกอบการปฏิบัติงาน (Operating Documentation)

– **การลดความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ (Minimizing System Downtime)**

ฮาร์ดแวร์ (Hardware) หรือซอฟต์แวร์ (Software) ที่ทำงานล้มเหลวอาจสร้างความสูญเสียทางการเงินที่สำคัญได้ วิธีการต่างๆ ที่จะลดความเสียหาย ได้แก่ การบำรุงรักษาในเชิงป้องกัน (Preventive Maintenance) อุปกรณ์ไฟฟ้าสำรอง (Uninterrupted Power System: UPS) และระบบที่ทนต่อความบกพร่อง (Fault Tolerant)

– **การวางแผนแก้ไขความเสียหายจากเหตุฉุกเฉิน (Disaster Recovery Plan)**

ทุกองค์กรควรมีแผนแก้ไขความเสียหายจากเหตุฉุกเฉินต่างๆ เพื่อให้การนำข้อมูลกลับมาใช้เป็นไปอย่างเรียบร้อยและรวดเร็วที่สุดเมื่อเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหาย ประกอบด้วยรายการต่างๆ ดังต่อไปนี้ การจัดลำดับความสำคัญของการกู้คืนระบบ (Priority for the Recovery

Process) การสำรองข้อมูลและโปรแกรม (Backup Data and Program Files) การมอบหมายหน้าที่เป็นการเฉพาะ (Specific Assignments) การจัดทำเอกสารประกอบที่สมบูรณ์ (Complete Documentation) เครื่องคอมพิวเตอร์และระบบโทรคมนาคมสำรอง (Backup Computer and Telecommunication Facilities)

(2) การควบคุมระบบงาน (Application Controls)

การควบคุมระบบงานแบ่งโดยพิจารณาตามองค์ประกอบของระบบหรือวงจรของรายการ (Transaction Cycles) ได้เป็น 3 ประเภท คือ

– การควบคุมการนำข้อมูลเข้าสู่ระบบงาน (Input Controls)

จุดมุ่งหมายของการจัดให้มีการควบคุมการนำข้อมูลเข้าสู่ระบบงานเป็นเช่นเดียวกัน ไม่ว่าจะเป็นระบบการประมวลผลข้อมูลด้วยมือหรือด้วยคอมพิวเตอร์ นั่นคือควบคุมเพื่อให้มั่นใจว่าข้อมูลรายการที่ต้องการประมวลผลได้รับการบันทึกอย่างถูกต้องครบถ้วนในงวดบัญชีที่เกิดรายการ และข้อมูลที่ผิดพลาดได้รับการตรวจพบและแก้ไขให้ถูกต้องก่อนส่งกลับเข้าประมวลผลอีกครั้งหนึ่งภายในงวดที่ถูกต้อง ตัวอย่างเช่น ในการนำข้อมูลรายการจากใบสั่งซื้อเข้าประมวลผล ระบบการควบคุมการนำเข้าข้อมูลที่ดีควรสามารถตรวจพบข้อผิดพลาดต่างๆ ในใบสั่งซื้อ เช่น รหัสลูกค้าที่ขาดหายไป และจำนวนสั่งซื้อที่ไม่สมเหตุสมผล และต้องมีการติดตามแก้ไขข้อมูลรายการสั่งซื้อนั้นให้ถูกต้อง เพื่อส่งกลับเข้าประมวลผลภายในงวดเวลาที่ถูกต้องด้วย นอกจากนี้ในกรณีที่มีการส่งข้อมูลผ่านสายสื่อสาร (Communication Lines) ระบบการควบคุมการนำข้อมูลเข้าที่ดีควรก่อให้เกิดความมั่นใจได้ว่า ข้อมูลที่รวบรวมมาเพื่อการประมวลผลได้รับการส่งผ่านสายสื่อสาร และแปลงให้อยู่ในสภาพที่เครื่องคอมพิวเตอร์อ่านได้อย่างถูกต้องครบถ้วน

การควบคุมการนำข้อมูลเข้ามีความสำคัญต่อระบบการประมวลผลข้อมูลด้วยคอมพิวเตอร์มาก ด้วยเหตุผลที่ว่าข้อผิดพลาดต่างๆ สามารถแก้ไขให้ถูกต้องได้ง่ายและสะดวกในขั้นตอนการนำเข้ามากกว่าในขั้นตอนอื่น และถ้าข้อมูลที่นำเข้าถูกต้อง ข้อมูลที่ใช้ในการประมวลผลและบันทึกไว้ในแฟ้มข้อมูลก็จะปราศจากข้อผิดพลาดด้วย ข้อพิจารณานี้มีความสำคัญยิ่งขึ้นในระบบที่มีการประมวลผลแบบเชื่อมตรง (On-line Processing) ซึ่งข้อผิดพลาดจะกระจายไปทั่วระบบอย่างรวดเร็วและยากที่จะตรวจพบหลังจากผ่านขั้นตอนการนำเข้าข้อมูลไปแล้ว ข้อมูลรายการที่ผิดพลาดเพียงรายการเดียวสามารถส่งผลกระทบถึงแฟ้มข้อมูลที่เกี่ยวข้องหลายแฟ้ม และทำให้ข้อมูลส่งออกและรายงานการประมวลผลไม่ถูกต้อง นอกจากนี้ยังอาจทำให้เกิดการปฏิบัติที่ไม่พึงประสงค์อีกด้วย เช่น จำนวนสั่งซื้อที่สูงเกินไปในใบสั่งซื้อที่มีข้อผิดพลาด จะทำให้ปริมาณสินค้าในมือ (Quantity on Hand) สำหรับสินค้าชนิดนั้นลดต่ำลงกว่าจุดสั่งซื้อ (Reorder Point) ซึ่งถ้ากิจการใช้ระบบสั่งซื้อ

อัตโนมัติ รายการที่ผิดพลาดนี้จะทำให้ระบบสั่งซื้อจัดเตรียมใบสั่งซื้อ (Purchase Order) และซื้อสินค้าเข้ามาเพิ่มทั้งๆ ที่กิจการมีสินค้าชนิดนั้นอยู่ในมืออย่างเพียงพอ

ผู้สอบบัญชีส่วนใหญ่เห็นความสำคัญและให้เวลาค่อนข้างมากในการประเมินความเชื่อถือได้ของระบบการควบคุมการนำข้อมูลเข้า ด้วยเหตุผลที่ว่ากิจกรรมการนำข้อมูลเข้าเป็นกิจกรรมที่ปฏิบัติอยู่เป็นประจำโดยคน และบางกรณีเป็นการปฏิบัติโดยคนคนเดียวซึ่งไม่มีผู้อื่นรู้เห็น จึงเสี่ยงต่อการเกิดข้อผิดพลาดได้มาก ซึ่งสอดคล้องกับผลการศึกษาวิจัยในอดีตที่ระบุว่าการทุจริตเกี่ยวกับคอมพิวเตอร์มักจะเกิดขึ้นในขั้นตอนการนำข้อมูลเข้าสู่ระบบงานคอมพิวเตอร์ โดยพิจารณาตามขั้นตอนทั่วไปของการปฏิบัติในการนำข้อมูลรายการเข้าประมวลผล ได้แก่ การอนุมัติรายการ (Authorization of Transactions) การบันทึกรายการ (Recording of Transaction) การรวมข้อมูลรายการ (Batch of Transaction Data) การแปลงสภาพข้อมูลรายการ (Conversion of Transaction Data) การตรวจทานความถูกต้องของข้อมูลรายการ (Editing of Transaction Data) และการส่งผ่านข้อมูลรายการ (Transaction of Transaction Data)

– **การควบคุมการประมวลผลและแฟ้มข้อมูล (Processing and File Controls)**

การควบคุมการประมวลผลข้อมูล (Processing Control) ถูกจัดให้มีขึ้นเพื่อให้มั่นใจได้ว่ารายการต่างๆ ที่นำเข้ารวมทั้งรายการที่สร้างขึ้นโดยระบบงานได้รับการประมวลผลอย่างถูกต้องครบถ้วน แฟ้มข้อมูลและโปรแกรมที่เกี่ยวข้องมีความเหมาะสม รายการต่างๆ ภายหลังจากนำเข้าหรือสร้างขึ้นโดยระบบงานแล้วจะไม่สูญหาย มีการเพิ่มเติม ถูกประมวลผลซ้ำ หรือมีการเปลี่ยนแปลงโดยไร้เหตุผล และข้อผิดพลาดจากการประมวลผลจะถูกรายงานและแก้ไขทันเวลา

การควบคุมเกี่ยวกับแฟ้มข้อมูล (File Control) กิจการสามารถนำเทคนิคในการควบคุมข้อมูลนำเข้าและการประมวลผลมาประยุกต์ใช้ในการควบคุมการเปลี่ยนแปลงข้อมูลที่มีลักษณะถาวร นอกจากนี้การเปลี่ยนแปลงข้อมูลต้องมีการอนุมัติอย่างเหมาะสม บุคคลที่มีสิทธิในการแก้ไขเปลี่ยนแปลงควรจำกัดอยู่เฉพาะคนจำนวนน้อยซึ่งมีหน้าที่เกี่ยวข้องกับการปฏิบัติงานเท่านั้น และควรมีการบันทึกและพิมพ์รายงานการแก้ไขเปลี่ยนแปลงข้อมูลที่มีลักษณะถาวรเพื่อการสอบทานด้วย ส่วนการควบคุมข้อมูลรายการนั้น ควรจัดให้มีบัญชีคุมยอดเพื่อให้มั่นใจว่ายอดรวมของรายการเหล่านั้นถูกต้อง และมีการกระทบยอดรวมของบัญชีคุมยอดด้วย นอกจากนั้นควรมีการตรวจทานความถูกต้องของยอดต่างๆ ที่เป็นบัญชีย่อยหรือรายการย่อยของยอดรวมเหล่านั้น การตรวจทานจะมากน้อยเพียงใดย่อมขึ้นอยู่กับความสำคัญของรายการและการควบคุมอื่นที่มีอยู่ในระบบการประมวลผลรายการเหล่านี้

– **การควบคุมข้อมูลส่งออก (Output Controls)**

การควบคุมข้อมูลส่งออกมีวัตถุประสงค์เพื่อสร้างความมั่นใจว่าผลลัพธ์จากการประมวลผลถูกต้อง ครบถ้วน ได้รับการนำส่งถึงผู้รับที่ได้รับอนุมัติภายในเวลาที่กำหนด และมีการเก็บรักษาและทำลายอย่างเหมาะสม การควบคุมข้อมูลส่งออกเป็นความรับผิดชอบร่วมกันของบุคลากรทั้งภายในและภายนอกหน่วยงานคอมพิวเตอร์ การควบคุมข้อมูลส่งออกอาจแยกได้เป็น 3 ส่วน ได้แก่ การสอบทานสิ่งที่ได้จากการประมวลผล การควบคุมการแจกจ่ายผลลัพธ์จากการประมวลผล และการเก็บรักษาและทำลายสิ่งที่ได้จากการประมวลผล

4. การประเมินความเสี่ยงในการสอบบัญชี

4.1 ความหมายและประเภทของความเสี่ยงในการสอบบัญชี

มาตรฐานการสอบบัญชี รหัส 400 เรื่อง การประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายใน ระบุว่า ความเสี่ยงในการสอบบัญชี (Audit Risk: AR) หมายถึง ความเสี่ยงที่ผู้สอบบัญชีแสดงความเห็นที่ไม่เหมาะสมเมื่องบการเงินแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ความเสี่ยงในการสอบบัญชี ได้แก่ (สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์, 2549ข)

(1) ความเสี่ยงสืบเนื่อง (Inherent Risk: IR)

คือ โอกาสที่ยอดคงเหลือของบัญชี หรือประเภทของรายการแสดงข้อมูลที่ขัดต่อข้อเท็จจริง ซึ่งอาจมีสาระสำคัญในแต่ละรายการ หรือมีสาระสำคัญเมื่อรวมกับการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงในยอดคงเหลืออื่น หรือประเภทของรายการอื่น โดยไม่คำนึงถึงการควบคุมภายในที่อาจมีอยู่ ซึ่งอาจป้องกันหรือตรวจพบ และแก้ไขการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงดังกล่าวได้

(2) ความเสี่ยงจากการควบคุม (Control Risk: CR)

คือ ความเสี่ยงที่ระบบบัญชีหรือระบบการควบคุมภายในไม่สามารถป้องกัน หรือตรวจพบและแก้ไขการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงได้อย่างทันเวลา การแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอาจเกิดขึ้นในยอดคงเหลือของบัญชีหรือประเภทของรายการ และอาจมีสาระสำคัญในแต่ละรายการหรือมีสาระสำคัญเมื่อรวมกับการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงในยอดคงเหลืออื่นหรือประเภทของรายการอื่น

(3) ความเสี่ยงจากการตรวจสอบ (Detection Risk: DR)

คือ ความเสี่ยงที่วิธีการตรวจสอบเนื้อหาสาระซึ่งผู้สอบบัญชีใช้จะไม่สามารถตรวจพบการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงที่มีอยู่ในยอดคงเหลือของบัญชีหรือประเภทของรายการ โดยการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงนั้นอาจมีสาระสำคัญในแต่ละรายการ หรือมีสาระสำคัญเมื่อรวมกับการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงในยอดคงเหลืออื่นหรือประเภทของรายการอื่น

4.2 วัตถุประสงค์ของการประเมินความเสี่ยงในระบบสารสนเทศที่ใช้คอมพิวเตอร์

ผู้สอบบัญชีประเมินความเสี่ยงของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการประมวลผลข้อมูล เพื่อที่จะระบุถึงโอกาสที่จะเกิดผลเสียหายแก่สินทรัพย์และทรัพยากรด้านสารสนเทศของกิจการอันมีผลกระทบต่อความถูกต้องและน่าเชื่อถือต่องบการเงินอย่างมีสาระสำคัญ

กิจกรรมที่ผู้สอบบัญชีทำเพื่อให้เกิดความเข้าใจในความเสี่ยงสืบเนื่องของระบบสารสนเทศและโครงสร้างการควบคุมภายในจะเป็นพื้นฐานแก่ผู้สอบบัญชีในการประเมินระดับความเสี่ยงจากการควบคุม โดยผู้สอบบัญชีจะใช้ข้อมูลดังกล่าวในการประเมินประสิทธิผลหรือความเพียงพอของนโยบายการควบคุมภายในที่เกี่ยวข้องกับระบบสารสนเทศของกิจการ (Internal Control Structure Policies) ในการป้องกัน ค้นพบ และแก้ไขข้อผิดพลาดที่มีสาระสำคัญที่ทำให้เกิดผลเสียหายแก่สินทรัพย์และทรัพยากรสารสนเทศของกิจการอันมีผลกระทบต่อความถูกต้องและน่าเชื่อถือของงบการเงินอย่างมีสาระสำคัญ โดยเฉพาะในเรื่องของความครบถ้วน มีอยู่จริง สิทธิและภาระผูกพัน มูลค่า การแสดงรายการและการเปิดเผยข้อมูล ซึ่งผู้สอบบัญชีจะใช้ผลจากการประเมินความเพียงพอของการประเมินประสิทธิผลของการควบคุมภายในหรือความเสี่ยงจากการควบคุมนี้ในการกำหนดกลยุทธ์และแผนการตรวจสอบว่าผู้สอบบัญชีควรจัดสรรเวลาและทรัพยากรอย่างไรระหว่างการประเมินประสิทธิผลการควบคุมภายในเพิ่มเติม (Additional Control Evaluation Procedures) กับการทดสอบเนื้อหาสาระ (Substantive Tests) ตลอดจนถึงการกำหนดลักษณะและขอบเขตการตรวจสอบ และการทดสอบรายการที่เหมาะสมเพียงพอในการแสดงความเห็นต่องบการเงิน (สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย, 2543)

4.3 ปัจจัยที่มีผลกระทบต่อระดับความเสี่ยงในระบบสารสนเทศที่ใช้คอมพิวเตอร์

การพิจารณาปัจจัยความเสี่ยงในระบบสารสนเทศมักพิจารณาจากสิ่งต่อไปนี้ (อุษณา ภัทรมนตรี, 2544)

(1) ความซับซ้อนของปัจจัยความเสี่ยง

ความซับซ้อนของปัจจัยความเสี่ยงประกอบด้วย ความเสี่ยงจากความซับซ้อนของระบบงาน ความเสี่ยงจากความซับซ้อนของระบบประมวลผล ความเสี่ยงจากการควบคุมทั่วไป และความเสี่ยงจากการบริหาร

(2) โอกาสที่น่าจะเกิดของความเสี่ยง

นอกจากการประเมินตามลักษณะความเสี่ยง สถานการณ์ต่อไปนี้ถือว่ามีโอกาสสูงที่จะเกิดความเสี่ยงในระบบหรือในบัญชีที่พบ ได้แก่ ข้อตรวจพบสำคัญที่ยังไม่ได้รับการแก้ไข ความถี่ในการเข้าตรวจสอบ ความรู้และทักษะของผู้ตรวจสอบ จำนวนปริมาณงานสูงที่ยากต่อการตรวจพบ ระดับความเกี่ยวข้องของคนในระบบงานสูง ระบบงานที่เกี่ยวข้องกับสินทรัพย์สภาพคล่อง เช่น

ระบบการรับ-จ่ายเงิน กิจกรรมการควบคุมการปฏิบัติงานประจำวันที่ไม่เพียงพอ และจำนวนการเข้ามาแก้ไขระบบงานสูง

(3) การพิจารณาผลกระทบ

จะพิจารณาจากสาระสำคัญที่มีต่องบการเงินหรือระบบสารสนเทศขององค์กรโดยรวม ถ้าเป็นสาระสำคัญถือว่ามีความเสี่ยงสูง

แนวปฏิบัติการประเมินความเสี่ยงในการสอบบัญชี รหัส 1008 สรุปว่าให้พิจารณาปัจจัยความเสี่ยงที่เกิดจากความซับซ้อนและปริมาณงานมีผลกระทบต่อการประมวลผลของแต่ละระบบงานและต่องบการเงินโดยรวมอย่างมีสาระสำคัญ ความเสี่ยงดังกล่าวนี้มีทั้งความเสี่ยงที่เป็นความเสี่ยงแฝงจากสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ความเสี่ยงจากการควบคุมทั่วไป และความเสี่ยงจากการควบคุมระบบงาน (สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์, 2549ง)

4.4 การประเมินความเสี่ยงในการสอบบัญชี

มาตรฐานการสอบบัญชี รหัส 400 เรื่อง การประเมินความเสี่ยงในการสอบบัญชีกับการควบคุมภายใน ระบุว่า ในการตรวจสอบงบการเงิน ผู้สอบบัญชีจะคำนึงถึงนโยบายและวิธีการปฏิบัติในระบบบัญชีและระบบการควบคุมภายในเฉพาะที่เกี่ยวกับสิ่งที่ผู้บริหารได้ให้การรับรองไว้เกี่ยวกับงบการเงิน ความเข้าใจในระบบบัญชีและระบบการควบคุมภายในควบคู่ไปกับการประเมินความเสี่ยงสืบเนื่องและความเสี่ยงจากการควบคุมและข้อพิจารณาอื่น จะทำให้ผู้สอบบัญชีสามารถระบุถึงประเภทของข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญซึ่งอาจแสดงอยู่ในงบการเงิน พิจารณาปัจจัยซึ่งมีผลกระทบต่อความเสี่ยงที่อาจมีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ และกำหนดวิธีการตรวจสอบที่เหมาะสม

ในการกำหนดแผนการสอบบัญชีโดยรวม ผู้สอบบัญชีควรประเมินความเสี่ยงสืบเนื่องในระดับงบการเงิน และในการกำหนดแนวการสอบบัญชี ผู้สอบบัญชีควรพิจารณาความสัมพันธ์ระหว่างผลการประเมินดังกล่าวกับสิ่งที่ผู้บริหารได้ให้การรับรองไว้เกี่ยวกับยอดคงเหลือในบัญชีและประเภทของรายการที่มีสาระสำคัญ หลังจากที่ได้มาซึ่งความเข้าใจในระบบบัญชีและระบบการควบคุมภายในแล้ว ผู้สอบบัญชีควรประเมินความเสี่ยงจากการควบคุมในเบื้องต้น สำหรับแต่ละยอดคงเหลือในบัญชีหรือแต่ละประเภทของรายการที่มีสาระสำคัญซึ่งผู้บริหารได้ให้การรับรองไว้ และผู้สอบบัญชีควรได้มาซึ่งหลักฐานการสอบบัญชีโดยการทดสอบการควบคุมเพื่อสนับสนุนผลการประเมินความเสี่ยงจากการควบคุมที่มีระดับที่ต่ำกว่าระดับสูง ความเสี่ยงจากการควบคุมที่ได้ประเมินมีระดับยิ่งต่ำลงเท่าใด ผู้สอบบัญชียิ่งต้องการหลักฐานสนับสนุนมากขึ้นเท่านั้น ทั้งนี้เพื่อให้แน่ใจว่าระบบบัญชีและระบบการควบคุมภายในมีการออกแบบอย่างเหมาะสมและมีการปฏิบัติตามอย่างมีประสิทธิผล ส่วนระดับของความเสี่ยงจากการตรวจสอบมีความสัมพันธ์โดยตรงกับวิธีการ

ตรวจสอบเนื้อหาสาระที่ผู้สอบบัญชีใช้ ดังนั้นผู้สอบบัญชีควรพิจารณาระดับของความเสี่ยงสืบเนื่องและความเสี่ยงจากการควบคุมที่ได้ประเมินไว้ในการกำหนดลักษณะ ระยะเวลา และขอบเขตของวิธีการตรวจสอบเนื้อหาสาระที่จำเป็น เพื่อที่จะลดความเสี่ยงของการสอบบัญชีให้อยู่ในระดับต่ำพอที่จะยอมรับได้ (สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์, 2549ข)

มาตรฐานการสอบบัญชี รหัส 401 เรื่อง การสอบบัญชีในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ระบุให้ผู้สอบบัญชีควรพิจารณาถึงผลกระทบของสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ที่มีต่อการสอบบัญชีโดยผู้สอบบัญชีควรมีความรู้เกี่ยวกับระบบสารสนเทศที่ใช้คอมพิวเตอร์อย่างเพียงพอ เพื่อวางแผน สั่งการ ควบคุมดูแล และสอบทานงานที่ได้ปฏิบัติ ผู้สอบบัญชีควรพิจารณาว่าจำเป็นต้องใช้ผู้เชี่ยวชาญด้านระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการตรวจสอบหรือไม่ หากมีการใช้ผู้เชี่ยวชาญดังกล่าว ผู้สอบบัญชีควรได้มาซึ่งหลักฐานการสอบบัญชีที่เพียงพอและเหมาะสมว่างานซึ่งผู้เชี่ยวชาญปฏิบัติเพียงพอสำหรับวัตถุประสงค์ในการตรวจสอบ และเป็นไปตามมาตรฐานการสอบบัญชีรหัส 620 เรื่องการใช้ผลงานของผู้เชี่ยวชาญ

การวางแผนการตรวจสอบในส่วนที่ได้รับผลกระทบจากสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ผู้สอบบัญชีควรได้มาซึ่งความเข้าใจเกี่ยวกับความสำคัญและความซับซ้อนของกิจกรรมระบบสารสนเทศที่ใช้คอมพิวเตอร์ และข้อมูลที่จะนำมาใช้ในการตรวจสอบความเข้าใจดังกล่าวรวมถึงเรื่องต่อไปนี้

(1) ความสำคัญและความซับซ้อนของการประมวลผลด้วยคอมพิวเตอร์ในแต่ละระบบงานบัญชีที่สำคัญ ความสำคัญในที่นี้เกี่ยวข้องกับความมีสาระสำคัญของสิ่งที่ผู้บริหารได้ให้การรับรองไว้เกี่ยวกับงบการเงิน ซึ่งได้รับผลกระทบจากการประมวลผลข้อมูลด้วยคอมพิวเตอร์

(2) โครงสร้างการจัดองค์กรของกิจกรรมระบบสารสนเทศที่ใช้คอมพิวเตอร์ของลูกค้าและขอบเขตของการรวมหรือการกระจายการประมวลผลด้วยคอมพิวเตอร์ของทั้งกิจการโดยเฉพาะอย่างยิ่งในกรณีที่ปัจจัยเหล่านี้อาจมีผลกระทบต่อการแบ่งแยกหน้าที่

(3) การมีข้อมูลให้ตรวจสอบ เอกสารประกอบรายการ แฟ้มข้อมูลคอมพิวเตอร์ และเรื่องอื่นที่เกี่ยวกับหลักฐานการตรวจสอบ ซึ่งผู้สอบบัญชีต้องการใช้ในการสอบบัญชี โดยอาจเป็นข้อมูลที่มีอยู่เพียงช่วงระยะเวลาอันสั้นหรืออาจเป็นข้อมูลในรูปแบบที่อ่านได้ด้วยคอมพิวเตอร์เท่านั้น ระบบสารสนเทศที่ใช้คอมพิวเตอร์ของกิจการอาจก่อให้เกิดรายงานภายในซึ่งเป็นประโยชน์ต่อการใช้วิธีการทดสอบเนื้อหาสาระ และการใช้เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (Computer-Assisted Audit Techniques-CAAT) อาจช่วยเพิ่มประสิทธิภาพในการปฏิบัติงานสอบบัญชี หรืออาจทำให้ผู้สอบบัญชีสามารถใช้วิธีการตรวจสอบบางอย่างสำหรับบัญชีหรือรายการทั้งหมดได้อย่างประหยัด

ในกรณีที่ระบบสารสนเทศที่ใช้คอมพิวเตอร์มีความสำคัญ ผู้สอบบัญชีควรได้มาซึ่งความเข้าใจเกี่ยวกับสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ซึ่งอาจมีอิทธิพลต่อการประเมินความเสี่ยงสืบเนื่องและความเสี่ยงจากการควบคุม โดยความเสี่ยงสืบเนื่องและความเสี่ยงจากการควบคุมในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์อาจส่งผลกระทบอย่างกว้างขวาง และส่งผลกระทบต่อบัญชีใดบัญชีหนึ่งโดยเฉพาะที่จะเกิดการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอย่างมีสาระสำคัญดังต่อไปนี้

(1) ความเสี่ยงซึ่งอาจเป็นผลมาจากข้อบกพร่องในกิจกรรมระบบสารสนเทศที่ใช้คอมพิวเตอร์ที่ส่งผลกระทบอย่างกว้างขวาง เช่น การพัฒนาและการบำรุงรักษาโปรแกรม การสนับสนุนและการปฏิบัติงานของซอฟแวร์ระบบ การรักษาความปลอดภัยทางกายภาพของระบบสารสนเทศที่ใช้คอมพิวเตอร์ และการควบคุมเกี่ยวกับการเข้าถึงโปรแกรมอรรถประโยชน์ (Utility Program) ซึ่งให้สิทธิพิเศษแก่ผู้ใช้ ข้อบกพร่องเหล่านี้มีแนวโน้มที่จะส่งผลกระทบอย่างกว้างขวางต่อทุกระบบงานที่ประมวลผลด้วยคอมพิวเตอร์

(2) ความเสี่ยงเหล่านี้อาจเพิ่มโอกาสที่จะก่อให้เกิดข้อผิดพลาดหรือการทุจริตโดยเฉพาะในบางระบบงาน บางฐานข้อมูลหรือแฟ้มข้อมูลหลัก หรือบางกิจกรรมประมวลผลเท่านั้น ตัวอย่างเช่น ข้อผิดพลาดอาจพบทั่วไปในระบบซึ่งมีการคำนวณหรือมีขั้นตอนการปฏิบัติที่ซับซ้อนหรือที่ต้องเกี่ยวข้องกับเงื่อนไขที่เป็นข้อยกเว้นต่างๆ ระบบซึ่งควบคุมเกี่ยวกับการเบิกจ่ายเงินสดหรือสินทรัพย์ที่มีสภาพคล่องมักจะล่อแหลมต่อการทุจริตโดยผู้ใช้ระบบงานหรือโดยบุคลากรด้านระบบสารสนเทศที่ใช้คอมพิวเตอร์

วัตถุประสงค์ในการตรวจสอบของผู้สอบบัญชีจะไม่เปลี่ยนแปลง ไม่ว่าข้อมูลทางบัญชีจะประมวลผลด้วยมือหรือด้วยคอมพิวเตอร์ อย่างไรก็ตามวิธีการประมวลผลด้วยคอมพิวเตอร์จะมีผลต่อวิธีการใช้วิธีการตรวจสอบต่างๆ เพื่อรวบรวมหลักฐานการสอบบัญชี ผู้สอบบัญชีสามารถใช้วิธีการตรวจสอบด้วยมือ หรือเทคนิคการสอบบัญชีโดยใช้คอมพิวเตอร์ช่วย (CAAT) หรือใช้ทั้งสองอย่างประกอบกัน เพื่อให้ได้หลักฐานการสอบบัญชีที่เพียงพอ อย่างไรก็ตามในระบบบัญชีซึ่งใช้คอมพิวเตอร์ในการประมวลผลระบบงานที่สำคัญ ผู้สอบบัญชีจะมีความยากลำบากหรือไม่สามารถรวบรวมข้อมูลบางอย่างเพื่อการตรวจสอบ การสอบถาม หรือการยืนยันหากไม่ใช้คอมพิวเตอร์ช่วยในการตรวจสอบ (สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์, 2549ค)

4.5 การประเมินความเสี่ยงจากการควบคุม

การประเมินความเสี่ยงจากการควบคุมในระบบการควบคุมภายในทางด้านคอมพิวเตอร์ มีลักษณะเช่นเดียวกับระบบการควบคุมภายในที่ทำด้วยมือ โดยขั้นตอนการประเมินความเสี่ยงจากการควบคุมทางด้านคอมพิวเตอร์ มีดังนี้ (นิพันธ์ เห็นโชคชัยชนะ และศิลปพร ศรีจั่นเพชร, 2550)

(1) พิจารณาความรู้ที่ได้รับจากการศึกษาทำความเข้าใจเกี่ยวกับระบบบัญชีและระบบการควบคุมภายใน

(2) ระบุข้อผิดพลาดที่อาจเกิดขึ้นในระบบบัญชีและระบบการควบคุมภายใน

(3) ระบุวิธีการควบคุมภายในที่จำเป็น เพื่อป้องกัน ค้นหา หรือแก้ไขข้อผิดพลาดเหล่านั้น

(4) ปฏิบัติการทดสอบการควบคุม

(5) ประเมินหลักฐานการสอบบัญชีและสรุปผลการประเมิน

วรรณกรรมที่เกี่ยวข้อง

กรทิพย์ วาณิชวิเศษกุล (2549) ได้วิจัยเรื่อง การวิเคราะห์และประเมินความเสี่ยงทางธุรกิจในการตรวจสอบบัญชี กรณีศึกษา: บริษัทในอุตสาหกรรมกระดาษคราฟท์ โดยการสัมภาษณ์ผู้บริหารและใช้ข้อมูลจากหน่วยงานราชการต่างๆ ที่เกี่ยวข้อง ผลการวิจัยพบว่า บริษัทตัวอย่างในอุตสาหกรรมกระดาษคราฟท์อาจมีความเสี่ยงในเรื่องของรายได้อันเนื่องมาจากการเกิดภาวการณ์แข่งขันที่รุนแรงมากขึ้น ซึ่งเป็นผลมาจากการลดภาษีนำเข้ากระดาษคราฟท์ รวมทั้งผลกระทบจากการขยายกำลังการผลิตของผู้ผลิตในประเทศจีน ทั้งนี้ความเสี่ยงดังกล่าวอาจส่งผลกระทบต่อผู้ผลิตในประเทศรวมทั้งบริษัทด้วย ทั้งนี้การนำวิธีการตรวจสอบบัญชีโดยการวิเคราะห์และประเมินความเสี่ยงทางธุรกิจมาใช้จะช่วยทำให้ผู้สอบบัญชีสามารถระบุความเสี่ยงได้ชัดเจนมากยิ่งขึ้น เนื่องจากได้มีการศึกษาและทำความเข้าใจในธุรกิจที่ตรวจสอบเป็นอย่างดี และจากการศึกษาการวิเคราะห์และประเมินความเสี่ยงทางธุรกิจในการตรวจสอบบัญชี พบว่า ผู้สอบบัญชีจะต้องเข้าถึงแหล่งข้อมูลภายในโดยการเข้าไปสอบถามจากผู้บริหารระดับสูงของบริษัท เพื่อให้ได้ข้อมูลเชิงลึก ทั้งในแง่ของวัตถุประสงค์ เป้าหมายในการดำเนินงาน และกลยุทธ์ของบริษัท รวมทั้งประเด็นต่างๆ ที่ผู้บริหารระดับสูงเป็นกังวลในแง่ของการดำเนินธุรกิจ เนื่องจากสิ่งเหล่านี้มีความจำเป็นอย่างยิ่งเพื่อให้ผู้สอบบัญชีสามารถวิเคราะห์ข้อมูลและสามารถกำหนดปัจจัยเสี่ยงที่อาจส่งผลกระทบต่องบการเงินของบริษัทได้

พรรณิภา แจ้งสุวรรณ (2549) ได้วิจัยเรื่อง การศึกษาการใช้ปัจจัยและองค์ประกอบความเสี่ยงในการประเมินความเสี่ยงในการตรวจสอบของผู้สอบบัญชีรับอนุญาต โดยศึกษาปัจจัยและองค์ประกอบความเสี่ยงในการประเมินความเสี่ยงสืบเนื่องและความเสี่ยงจากการควบคุมที่คาดว่าจะเกิดขึ้น เพื่อประโยชน์ในการวางแผนการสอบบัญชี ผลการวิจัยพบว่า ความเสี่ยงที่ผู้สอบบัญชีควรให้ความสำคัญและระมัดระวังความเสี่ยงเป็นอันดับแรก ได้แก่ ปัญหาการได้มาซึ่งหลักฐานการสอบบัญชีที่เพียงพอและเหมาะสม รายการที่ผิดปกติ เช่น รายการหรือวิธีปฏิบัติที่ซ้ำซ้อน เป็นต้น ความซื่อสัตย์ จริยธรรมของผู้บริหารและยอดคงเหลือในบัญชีแยกประเภทรายการ ความกดดันที่

ผิดปกติต่อกิจการ เช่น สภาพเศรษฐกิจตกต่ำ เป็นต้น แรงกดดันที่ผิดปกติ เช่น ความเชื่อถือได้ของรายงานทางการเงิน เป็นต้น ลักษณะทางธุรกิจของกิจการ ปัจจัยที่กระทบต่อสถานการณ์ที่ดำเนินอยู่ ปัจจัยเกี่ยวกับสภาพแวดล้อมของระบบสารสนเทศ ความเชื่อมั่นและจริยธรรม ประสบการณ์และความรู้ของผู้บริหาร นอกจากนั้น พบว่า ความแตกต่างทางด้านอายุของผู้สอบบัญชี ประสบการณ์การทำงาน ปริมาณงานส่วนที่รับต่อปี จำนวนผู้ช่วยผู้สอบบัญชี และเชื้อชาติของสำนักงานที่ผู้สอบบัญชีสังกัดนั้น ไม่มีผลทำให้ผู้สอบบัญชีแสดงความเห็นต่อปัจจัยเสี่ยงสืบเนื่องและปัจจัยเสี่ยงจากการควบคุมแตกต่างกัน

งามฉวี โชติยมนตรี (2547) ได้ศึกษาการประเมินความเสี่ยงในการสอบบัญชีของผู้สอบบัญชี ในอำเภอเมือง จังหวัดเชียงใหม่ พบว่า ผู้สอบบัญชีทั้งหมดมีความเข้าใจในเรื่องของความเสี่ยงในการสอบบัญชีอยู่ในระดับสูง ทั้งในส่วนของความเสี่ยงสืบเนื่อง ความเสี่ยงจากการควบคุม และความเสี่ยงจากการตรวจสอบ ในการประเมินความเสี่ยงสืบเนื่องนั้นผู้สอบบัญชีได้ทำการประเมินความเสี่ยงสืบเนื่องในระดับงบการเงิน โดยคำนึงถึงปัจจัยเสี่ยงที่กระทบต่ออุตสาหกรรมที่กิจการดำเนินอยู่ และได้ทำการประเมินความเสี่ยงสืบเนื่องในระดับของยอดคงเหลือในบัญชีและประเภทรายการ โดยคำนึงถึงปัจจัยเสี่ยงด้านการเปลี่ยนแปลงผู้บริหารในระหว่างงวดการตรวจสอบเป็นส่วนใหญ่ ส่วนการประเมินความเสี่ยงจากการควบคุมนั้น ผู้สอบบัญชีจะมุ่งเน้นไปที่กิจการมีระบบการควบคุมภายในที่มีประสิทธิภาพหรือไม่เป็นประเด็นสำคัญ โดยวิธีการทดสอบระบบก็เป็นอีกวิธีหนึ่งที่จะทำให้ผู้สอบบัญชีสามารถทราบจุดอ่อนของระบบการควบคุมภายในของกิจการ เพื่อจะได้ตัดสินใจกำหนดลักษณะ ระยะเวลา และขอบเขตของวิธีการตรวจสอบโดยใช้วิธีตรวจสอบเนื้อหาสาระให้เหมาะสมกับสถานการณ์และขนาดของกิจการ และการประเมินความเสี่ยงจากการตรวจสอบนั้น ผู้สอบบัญชีได้ใช้ปัจจัยเสี่ยงในการเลือกตัวอย่างเพื่อนำมาใช้ในการตรวจสอบเป็นปัจจัยสำคัญที่สุด ซึ่งผู้สอบบัญชีส่วนใหญ่เห็นว่า การปฏิบัติงานสอบบัญชีในจังหวัดเชียงใหม่นั้นจะต้องเผชิญกับความเสี่ยงประเภทนี้มากที่สุด รองลงมาคือ ความเสี่ยงจากการควบคุม และความเสี่ยงสืบเนื่อง ตามลำดับ