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

บทที่ 1

เรื่อง การตรวจสอบกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูลและการประเมินความเสี่ยง

(เอกสารประกอบการเตรียมตัวเป็นผู้สอบบัญชีรับอนุญาต)

โดย ดร.เยาวลักษณ์ ชาติบัญชาชัย
คณะผู้ทรงคุณวุฒิเกี่ยวกับการทดสอบการปฏิบัติงานสอบบัญชี
ด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์
สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

บทที่ 1
เรื่อง การตรวจสอบกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูลและการประเมินความเสี่ยง

โดย ดร.เยาวลักษณ์ ชาติบัญชาชัย
คณะผู้ทรงคุณวุฒิเกี่ยวกับการทดสอบการปฏิบัติงานสอบบัญชี
ด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์
สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

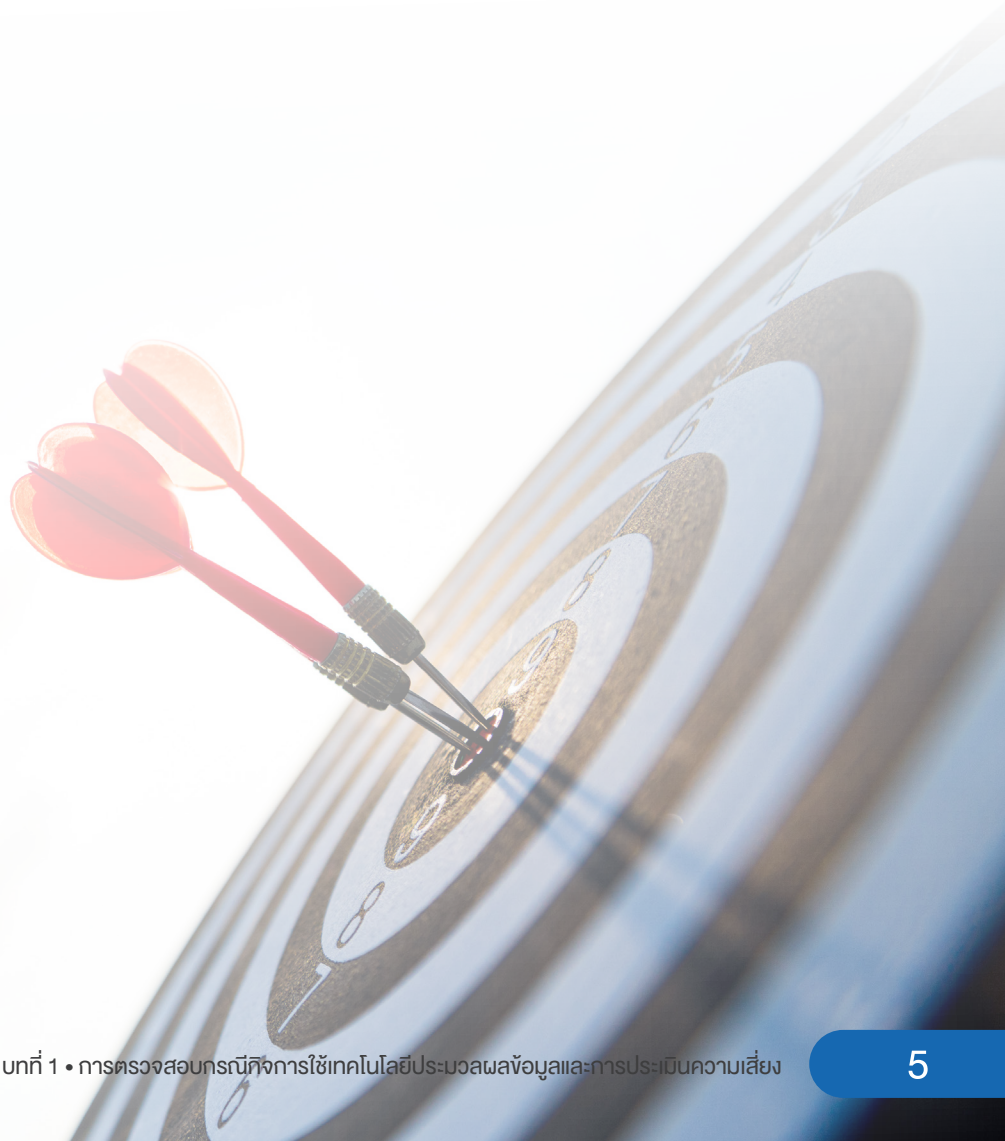
สารบัญ

	หน้า
1. สารบัญบท	4
2. วัตถุประสงค์ในการศึกษา	5
3. คำนำ	6
4. ความหมายและขอบเขตของการใช้เทคโนโลยีประมวลผลข้อมูลเพื่อการสอบบัญชี	7
5. ข้อพิจารณาในการตรวจสอบระบบสารสนเทศเพื่อการสอบบัญชี	12
6. ขอบเขตและวิธีการทำความเข้าใจสภาพแวดล้อมและการควบคุมของระบบสารสนเทศเพื่อการสอบบัญชี	19
7. การระบุและประเมินความเสี่ยงจากการใช้ระบบสารสนเทศเพื่อการสอบบัญชี	25
7.1. ความเสี่ยงที่เกิดจากการใช้ระบบสารสนเทศต่อการจัดทำรายงานทางการเงิน	26
7.2. ผลกระทบจากการใช้ระบบสารสนเทศต่อการสอบบัญชี	28
7.3. ตัวอย่างเงื่อนไขและเหตุการณ์เกี่ยวกับระบบสารสนเทศที่อาจแสดงถึงความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในรายงานทางการเงิน	30
8. การระบุและประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชี	31
8.1. ประเภทของการควบคุม	31
8.2. ความสัมพันธ์ของการควบคุมแต่ละประเภท	32
8.3. วิธีการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชี	32
8.4. การสรุปและการใช้ผลการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศ	34
9. การตรวจสอบในกรณีที่กิจการใช้บริการเกี่ยวกับระบบสารสนเทศจากองค์กรที่ให้บริการ	36
10. บทสรุป	39
11. บรรณานุกรม	41

2. วัตถุประสงค์ในการศึกษา

เมื่อได้ศึกษาเนื้อหาของบทนี้แล้ว ผู้ศึกษาควรมีความเข้าใจถึง

1. ความหมายและขอบเขตของการใช้เทคโนโลยีประมวลผลข้อมูลเพื่อการสอบบัญชี
2. ข้อพิจารณาในการตรวจสอบระบบสารสนเทศเพื่อการสอบบัญชี
3. ขอบเขตและวิธีการทำความเข้าใจสภาพแวดล้อมและการควบคุมของระบบสารสนเทศเพื่อการสอบบัญชี
4. การระบุและประเมินความเสี่ยงจากการใช้ระบบสารสนเทศที่จะมีผลต่อการจัดทำรายงานทางการเงินและการสอบบัญชี
5. การระบุและประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชี ซึ่งครอบคลุมถึงประเภทของการควบคุม ความสัมพันธ์ของการควบคุมแต่ละประเภท และวิธีการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชี
6. การสรุปและการใช้ผลการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศ
7. การตรวจสอบในกรณีที่กิจการใช้บริการเกี่ยวกับระบบสารสนเทศจากองค์กรที่ให้บริการ



3. คำนำ

การตรวจสอบกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูลและการประเมินความเสี่ยงจากการใช้เทคโนโลยีประมวลผลข้อมูล มีวัตถุประสงค์ ขอบเขต กรอบและหลักการโดยรวมของการสอบบัญชี ไม่แตกต่างกับการตรวจสอบและประเมินความเสี่ยงกรณีกิจการใช้การประมวลผลข้อมูลด้วยมือ หรือใช้การประมวลผลข้อมูลแบบอื่น ๆ เช่น ใช้การประมวลผลข้อมูลด้วยมือและที่เป็นแบบอัตโนมัติร่วมกัน อย่างไรก็ดีกิจการมักมีการใช้เทคโนโลยีเพื่อสนับสนุนการดำเนินธุรกิจอื่น ๆ นอกเหนือจากการบันทึกและประมวลผลข้อมูลทางการบัญชี และการจัดทำรายงานทางการเงินด้วย ดังนั้นในการตรวจสอบและประเมินความเสี่ยงกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูล ผู้สอบบัญชีจึงจำเป็นต้องมีความเข้าใจในประเด็นที่สำคัญต่อการสอบบัญชี โดยเฉพาะในเรื่องของขอบเขตการใช้เทคโนโลยีในการประมวลผลข้อมูลของกิจการที่เกี่ยวข้องกับการสอบบัญชี ข้อพิจารณาในการตรวจสอบระบบสารสนเทศเพื่อการสอบบัญชี สภาพแวดล้อมทางเทคโนโลยีสารสนเทศ ความเสี่ยงและการควบคุมภายในของระบบสารสนเทศที่อยู่ภายในขอบเขตที่ผู้สอบบัญชีได้ระบุไว้ แนวทางและวิธีการในการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชี การสรุปและการใช้ผลการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศ รวมถึงแนวทางและวิธีการในการตรวจสอบในกรณีที่กิจการใช้บริการเกี่ยวกับระบบสารสนเทศจากองค์กรที่ให้บริการ ทั้งนี้เพื่อให้ผู้สอบบัญชีสามารถปฏิบัติงานการตรวจสอบตามมาตรฐานการสอบบัญชีที่เกี่ยวข้อง เช่น มาตรฐานการสอบบัญชี รหัส 315 (ฉบับปรับปรุง 2564) เรื่อง “การระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ” มาตรฐานการสอบบัญชี รหัส 330 (ฉบับปรับปรุง) เรื่อง “วิธีปฏิบัติของผู้สอบบัญชีในการตอบสนองต่อความเสี่ยงที่ได้ประเมินไว้” และมาตรฐานการสอบบัญชี รหัส 402 เรื่อง “ข้อพิจารณาในกรณีที่กิจการใช้บริการขององค์กรอื่น” ได้อย่างมีประสิทธิผลและประสิทธิภาพ

4. ความหมายและขอบเขตของการใช้เทคโนโลยีประมวลผลข้อมูลเพื่อการสอบบัญชี

การใช้เทคโนโลยีประมวลผลข้อมูลเพื่อการสอบบัญชี หมายถึง การใช้ระบบสารสนเทศที่ใช้เทคโนโลยีรวมถึงคอมพิวเตอร์ในการประมวลผลข้อมูลที่เกี่ยวกับการจัดทำรายงานทางการเงินของกิจการ (ซึ่งต่อไปในบทนี้จะเรียกระบบสารสนเทศดังกล่าวโดยย่อว่า “ระบบสารสนเทศ” หรือ “ระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำงบการเงิน” หรือ “ระบบสารสนเทศเพื่อการสอบบัญชี”)

ซึ่งขอบเขตของการประมวลผลข้อมูลด้วยเทคโนโลยีเพื่อการสอบบัญชีนี้ครอบคลุมถึง

- การเกิดธุรกรรมทางธุรกิจ เช่น การขอเป็นลูกค้าเพื่อซื้อสินค้า การสั่งซื้อสินค้าจากลูกค้า
- การบันทึกรายการค้า เช่น การบันทึกรายการสั่งซื้อของลูกค้า การส่งสินค้า การตั้งยอดลูกหนี้ การรับชำระเงินจากลูกค้า และการตัดยอดลูกหนี้
- การประมวลผลข้อมูล เช่น การคำนวณเพื่อจัดชั้นลูกหนี้ การเปรียบเทียบยอดคงเหลือลูกหนี้กับวงเงินสินเชื่อก่อนอนุมัติรายการสั่งซื้อของลูกค้า
- การจัดทำรายงานทางการเงินและหลักฐานการสอบบัญชี เช่น รายงานบัญชีแยกประเภทย่อยลูกหนี้และยอดคงเหลือลูกหนี้การค้าในงบการเงิน รายงานอายุลูกหนี้
- การจัดเก็บข้อมูลที่เกี่ยวข้องทั้งที่เป็นข้อมูลหลัก (Master Data) ข้อมูลรายการค้า (Transaction Data) และข้อมูลอ้างอิง (Reference Data) ข้อมูลเกี่ยวกับข้อมูล (Metadata) ข้อมูลอดีต (Historical Data) และข้อมูลชั่วคราว (Temporary Data) ซึ่งข้อมูลที่จัดเก็บอาจมีหลายรูปแบบ เช่น เป็นตัวอักษร เป็นตัวเลข หรือเป็นมัลติมีเดีย เช่น ภาพ เสียง หรืออื่น ๆ

โดยระบบสารสนเทศนี้จะประกอบด้วยองค์ประกอบที่สำคัญ 3 องค์ประกอบ ได้แก่

- กระบวนการ (Processes) ทั้งที่เป็นกระบวนการทางธุรกิจและกระบวนการด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงนโยบายและการควบคุมต่าง ๆ ที่กิจการกำหนดให้มีภายในกระบวนการเหล่านั้น
- เทคโนโลยี (Technology) ซึ่งประกอบด้วย
  - ส่วนที่เป็นฮาร์ดแวร์ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์นำเข้าข้อมูล อุปกรณ์จัดเก็บข้อมูล
  - ส่วนที่เป็นซอฟต์แวร์ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน ซอฟต์แวร์ระบบจัดการฐานข้อมูล ซอฟต์แวร์ระบบเครือข่าย ซอฟต์แวร์เพื่อรักษาความมั่นคงปลอดภัยของระบบและข้อมูล
  - ส่วนที่เป็นข้อมูล ซึ่งรวมถึงข้อมูลที่จัดเก็บในสื่อเก็บข้อมูล ในระบบคลาวด์ และในระบบสารสนเทศที่ติดตั้งที่ศูนย์คอมพิวเตอร์สำรอง
- คน (People) ซึ่งประกอบด้วยผู้ใช้งานทั้งที่เป็นผู้ใช้งานภายในและภายนอกกิจการที่สามารถเข้าถึงและใช้งานระบบสารสนเทศของกิจการได้ เช่น ลูกค้า ผู้สอบบัญชี และบุคลากรของหน่วยงานเทคโนโลยีสารสนเทศของกิจการและของหน่วยงานภายนอกที่ให้บริการเทคโนโลยีสารสนเทศกับกิจการ โดยรวมถึงโครงสร้างองค์กร ทักษะและความสามารถ วัฒนธรรมองค์กร จริยธรรม และพฤติกรรม

ทั้งนี้การใช้เทคโนโลยีประมวลผลข้อมูลของกิจการอาจเป็นปัจจัยเสี่ยงที่ทำให้เกิดการแสดงข้อมูลในงบการเงินที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญได้ ดังตัวอย่างกรณีต่อไปนี้

- การเปลี่ยนแปลงรูปแบบการดำเนินงาน (Operating Model) โครงสร้างองค์กร หรือบุคลากรด้านเทคโนโลยีสารสนเทศ ซึ่งมีผลกระทบสำคัญต่อระดับความเสี่ยงด้านการจัดทำรายงานการเงินจากลักษณะการใช้และระดับการพึ่งพิงเทคโนโลยีในการดำเนินงานที่เปลี่ยนแปลงไป การแบ่งแยกหน้าที่ การควบคุมคุณภาพการดำเนินงานด้านเทคโนโลยีสารสนเทศ เช่น

การพัฒนาและการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ การบริหารจัดการเหตุการณ์ผิดปกติ การบริหารจัดการการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูล และการกำกับดูแลการปฏิบัติงานให้เป็นไปตามการควบคุมที่กำหนดไว้

- การมีข้อบกพร่องของการควบคุมด้านเทคโนโลยีสารสนเทศ โดยเฉพาะในกรณีที่ผู้บริหารไม่ได้ให้ความสำคัญที่จะรับทราบและจัดการ โดยข้อบกพร่องดังกล่าวมีผลกระทบที่สำคัญต่อความครบถ้วน ความถูกต้องและความสมเหตุสมผลของรายการและข้อมูลอื่นที่ประมวลผลโดยระบบสารสนเทศ โดยที่ผู้ใช้งานไม่ได้ตระหนักถึงจึงไม่ได้จัดให้มีมาตรการใดที่จะตรวจพบรายการที่ผิดปกติที่มีผลมาจากข้อบกพร่องของการควบคุมดังกล่าว
- การมีความไม่สอดคล้องกันระหว่างกลยุทธ์ด้านเทคโนโลยีสารสนเทศและกลยุทธ์ทางธุรกิจ ซึ่งมีผลทำให้ระบบสารสนเทศไม่สามารถรองรับความต้องการทางธุรกิจได้ทันเวลา และทำให้ต้องมีการทำรายการนอกระบบสารสนเทศหรือหลีกเลี่ยงกฎเกณฑ์และการควบคุมที่กำหนดไว้ เช่น ไม่บันทึกรายการตามนโยบายและหลักการบัญชีที่กำหนดไว้ ไม่มีการอนุมัติก่อนการบันทึกรายการ มีการนำซอฟต์แวร์ระบบงานที่พัฒนาขึ้นไปใช้งานจริงก่อนได้รับการทดสอบและยอมรับจากผู้ใช้งาน
- การเปลี่ยนแปลงสภาพแวดล้อมหรือโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศที่สำคัญ เช่น การเปลี่ยนแปลงหรือย้ายศูนย์คอมพิวเตอร์ การเปลี่ยนแปลงผู้ให้บริการเทคโนโลยีสารสนเทศที่สำคัญ การเปลี่ยนแปลงสถาปัตยกรรมของระบบเครือข่ายหรือระบบการรักษาความมั่นคงปลอดภัย ซึ่งมีผลทำให้การควบคุมที่กำหนดไว้เพื่อให้สามารถเชื่อมั่นในความครบถ้วน ความถูกต้องและความสมเหตุสมผลของรายการและข้อมูลอื่นที่ประมวลผลโดยระบบสารสนเทศไม่มีประสิทธิผลอีกต่อไป นอกจากนี้การเปลี่ยนแปลงดังกล่าวอาจทำให้ทรัพย์สินด้านเทคโนโลยีสารสนเทศบางส่วนไม่สามารถใช้งานต่อได้และด้อยค่าไป ในขณะที่ในรายงานการเงินยังแสดงมูลค่าของทรัพย์สินนั้นอยู่
- การนำระบบสารสนเทศใหม่มาใช้งาน ซึ่งมีผลกระทบต่อความครบถ้วน ความถูกต้องและความสมเหตุสมผลของรายการและข้อมูลอื่นที่ประมวลผลโดยระบบสารสนเทศจากการที่ระบบสารสนเทศดังกล่าวไม่ได้รับการออกแบบ การพัฒนา การตั้งค่าหรือการทดสอบที่สะท้อนความต้องการของผู้ใช้งานทั้งในแง่การทำงานและการควบคุม

ดังนั้นในการตรวจสอบกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูลเพื่อการสอบบัญชี จึงมีวัตถุประสงค์เพื่อพิจารณาว่าระบบสารสนเทศทำงานตามที่กำหนดไว้ และรายการค้าที่นำเข้าหรือสร้างขึ้นและบันทึกอยู่ในระบบสารสนเทศ การประมวลผลข้อมูล และข้อมูลออกของระบบสารสนเทศนั้น ครบถ้วน ถูกต้อง และสะท้อนสถานะทางการเงินที่แท้จริงของกิจการ โดยในเบื้องต้นผู้สอบบัญชีจะต้องพิจารณาถึงความเสี่ยงของระบบสารสนเทศที่กิจการใช้ที่เกี่ยวข้องกับการจัดทำรายงานทางการเงินเพื่อให้สามารถกำหนดลักษณะ ระยะเวลา และขอบเขตการตรวจสอบ ที่ตอบสนองต่อความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด ทั้งในระดับของงบการเงินและในระดับที่เกี่ยวกับสิ่งที่ผู้บริหารได้ให้การรับรองไว้

โดยทั่วไปปัจจัยสำคัญที่ใช้ในการพิจารณาขอบเขตการใช้เทคโนโลยีประมวลผลข้อมูลของกิจการที่ผู้สอบบัญชีต้องครอบคลุมในการสอบบัญชี มีดังนี้

- รูปแบบธุรกิจ (Business Model) และลักษณะการใช้เทคโนโลยีประมวลผลข้อมูลของกิจการ เช่น กิจการที่มีรูปแบบธุรกิจที่พึ่งพิงการใช้ดิจิทัลเทคโนโลยีในการขายสินค้าหรือบริการ เพื่อหลีกเลี่ยงหรือลดคนกลาง หรือเพื่อลดต้นทุนในการให้บริการหรือเพื่อเสนอสินค้าหรือบริการในรูปแบบที่ง่ายต่อการเข้าถึงและใช้งาน แบบที่ใช้กันในธุรกิจให้บริการทางการเงิน หรือธุรกิจค้าปลีกแบบออนไลน์ รูปแบบธุรกิจเช่นนี้ย่อมมีผลทำให้กิจการมีการทำธุรกรรมและรายการค้า การประมวลผล การบันทึกรายการและการจัดทำรายงานทางธุรกิจรวมถึงงบการเงินด้วยคอมพิวเตอร์เป็นส่วนมาก ในกรณีนี้ขอบเขตงานของผู้สอบบัญชีย่อมต้องครอบคลุมขอบเขตงานเกี่ยวกับการใช้เทคโนโลยีประมวลผลข้อมูลของกิจการ รวมถึงระบบสารสนเทศที่กิจการใช้อย่างเพียงพอต่อการวางแผนการตรวจสอบงบการเงินของกิจการ และการปฏิบัติงานตรวจสอบอย่างมีประสิทธิผลและประสิทธิภาพ

- ความซับซ้อนของระบบสารสนเทศที่กิจการใช้ ซึ่งครอบคลุมถึงสภาพแวดล้อมและโครงสร้างทางเทคโนโลยีสารสนเทศของกิจการ ตัวอย่างของลักษณะของสถาปัตยกรรมของระบบสารสนเทศที่มีผลทำให้ระบบสารสนเทศมีความซับซ้อน ได้แก่
  - มีระบบสารสนเทศที่ใช้มาเป็นเวลานานหลายระบบ โดยแต่ละระบบไม่ได้เชื่อมโยงเข้าด้วยกัน ซึ่งอาจทำให้มีการนำเข้าข้อมูลที่ซ้ำซ้อนและไม่ตรงกัน ความหมายของข้อมูลในแต่ละระบบต่างกัน ข้อมูลเดียวกันที่จัดเก็บในแต่ละระบบมีค่าต่างกัน นอกจากนี้ข้อมูลที่กิจการใช้ในการบันทึกบัญชีอาจได้จากการที่ผู้ใช้งานเอาข้อมูลในระบบงานต่าง ๆ มาจัดทำโดยใช้โปรแกรมหรือเครื่องมือที่พัฒนาหรือจัดหาและดูแลเองโดยผู้ใช้งาน
  - มีการใช้ผู้ให้บริการภายนอกสำหรับบริการด้านเทคโนโลยีที่สำคัญบางด้าน เช่น ใช้บริการโครงสร้างเทคโนโลยีสารสนเทศพื้นฐานทั้งหมดจากผู้ให้บริการภายนอกหลายราย และผู้ให้บริการบางรายอยู่ต่างประเทศ หรือใช้บริการพัฒนาและดูแลซอฟต์แวร์ระบบงานทั้งหมดจากผู้ให้บริการภายนอกหลายราย
  - สถาปัตยกรรมระบบสารสนเทศที่ใช้มีหลายรูปแบบ
  - ผู้ใช้งานระบบสารสนเทศมีจำนวนมากและมีผู้ใช้งานที่เป็นบุคคลหรือหน่วยงานภายนอกด้วย
  - มีการเชื่อมต่อระบบสารสนเทศของกิจการกับระบบงานอื่นที่อยู่ทั้งในและนอกกิจการจำนวนมาก
  - รายการที่นำเข้าและประมวลผลโดยระบบสารสนเทศมีจำนวนมากจนยากที่ผู้ใช้งานจะสามารถพบและแก้ไขข้อผิดพลาดได้
  - รายการบัญชีที่มีสาระสำคัญต่อความถูกต้องน่าเชื่อถือของงบการเงินถูกสร้างและบันทึกเข้าระบบสารสนเทศโดยระบบงานอื่นแบบอัตโนมัติ
  - ข้อมูลทางการเงินในระบบสารสนเทศเกิดจากการคำนวณที่ซับซ้อนโดยระบบและ/หรือระบบสร้างและบันทึกรายการบัญชีที่มีสาระสำคัญโดยอัตโนมัติ ทำให้ไม่สามารถหรือไม่มีการตรวจสอบความถูกต้องและเหมาะสมของรายการอย่างเป็นอิสระได้
  - รายการถูกแลกเปลี่ยนกันระหว่างองค์กรในรูปแบบอิเล็กทรอนิกส์ โดยไม่สามารถสอบทานความถูกต้องและเหมาะสมด้วยมือหรือต้องใช้วิธีการตรวจสอบทางเทคนิคที่ซับซ้อน
- ความเสี่ยงของระบบสารสนเทศ หากระบบสารสนเทศมีความเสี่ยงต่อการแสดงข้อมูลในงบการเงินที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ในกรณีนี้ขอบเขตงานของผู้สอบบัญชีย่อมต้องครอบคลุมขอบเขตงานเกี่ยวกับการใช้เทคโนโลยีประมวลผลข้อมูลของกิจการ รวมถึงระบบสารสนเทศที่กิจการใช้อย่างเพียงพอต่อการวางแผนการตรวจสอบงบการเงินของกิจการและการปฏิบัติงานตรวจสอบอย่างมีประสิทธิผลและประสิทธิภาพ เนื่องจากความเสี่ยงดังกล่าวเป็นปัจจัยสำคัญในการกำหนดการควบคุมที่ระบบสารสนเทศควรมี และการกำหนดลักษณะ ระยะเวลาและขอบเขตในการตรวจสอบที่เหมาะสม ดังนั้นผู้สอบบัญชีจึงจำเป็นต้องประเมินระดับความเสี่ยงของระบบสารสนเทศ โดยการประเมินโอกาสที่การใช้ระบบสารสนเทศนี้จะทำให้เกิดข้อผิดพลาดขึ้น หากไม่มีการควบคุมใด ๆ เลย หรือที่เรียกความเสี่ยงประเภทนี้โดยทั่วไปว่า ความเสี่ยงสืบเนื่อง (Inherent Risk) และทำการประเมินประสิทธิผลของการควบคุมที่เกี่ยวข้องกับการใช้ระบบสารสนเทศนี้ของกิจการในการป้องกัน ค้นพบและแก้ไขข้อผิดพลาดหรือรายการผิดปกติที่เกิดขึ้น ในเรื่องของความครบถ้วน มีอยู่จริง มูลค่า การแสดงรายการและความทันต่อเวลาของรายการและข้อมูลในระบบสารสนเทศ โดยผู้สอบบัญชีต้องคำนึงว่าระบบสารสนเทศมีลักษณะพิเศษบางประการที่อาจกระทบต่อความเสี่ยงต่อการแสดงข้อมูลในงบการเงินที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ และการสอบบัญชี เช่น
  - ระบบสารสนเทศที่ใช้อาจไม่สามารถให้หลักฐานในการติดตามการบันทึกรายการ (Transaction Trails) หรือร่องรอยการตรวจสอบ (Audit Trails) ที่เพียงพอต่อการค้นหาข้อผิดพลาดของการประมวลผลได้
  - ระบบสารสนเทศที่ใช้บางระบบอาจถูกออกแบบให้เก็บข้อมูลหลักฐานในการติดตามการบันทึกรายการเฉพาะในช่วงเวลาหนึ่งก่อนที่จะถูกลบจากระบบ หรือแทนค่าไป หรืออยู่ในรูปแบบที่อ่านได้ด้วยเทคโนโลยีเท่านั้น หรือไม่มีการจัดเก็บข้อมูลหลักฐานการติดตามการบันทึกรายการอย่างสมบูรณ์ทุกขั้นตอนของการประมวลผล ซึ่งทำให้ยากที่จะพบข้อผิดพลาดในตรรกะของโปรแกรม (Program Logics) ที่ทำให้ผลลัพธ์ที่ได้จากการประมวลผลผิดพลาดได้ทันเวลาโดยการใช้ขั้นตอนการค้นหาและตรวจสอบด้วยมือ

- ระบบสารสนเทศที่ใช้จะประมวลผลรายการประเภทเดียวกันด้วยคำสั่งและขั้นตอนแบบเดียวกัน ทำให้โอกาสที่จะเกิดความผิดพลาดจากการปฏิบัติงานของพนักงาน (Human Errors) ในลักษณะสุ่มที่มักเกิดในการประมวลผลที่ใช้มือน้อยมาก แต่หลักการในการทำงานของระบบสารสนเทศในลักษณะนี้ ทำให้เกิดความเสี่ยงที่การประมวลผลของรายการทุกรายการในประเภทเดียวกันจะผิดพลาดทั้งหมด หากมีข้อผิดพลาดในตรรกะของโปรแกรมระบบงาน หรือมีข้อผิดพลาดในการทำงานของฮาร์ดแวร์ หรือมีข้อผิดพลาดในการทำงานของซอฟต์แวร์ระบบ ที่เกี่ยวข้องกับการประมวลผล
- การแบ่งแยกหน้าที่โดยการแยกผู้ปฏิบัติงานอาจไม่สามารถทำได้ในระบบสารสนเทศที่ประมวลผลด้วยเทคโนโลยี ซึ่งตามหลักการแบ่งแยกหน้าที่ที่ดี กำหนดให้ต้องมีการแบ่งแยกหน้าที่การดูแลรักษาสินทรัพย์ การอนุมัติรายการ การบันทึกรายการและการตรวจสอบรายการออกจากกัน เพื่อป้องกันไม่ให้มีบุคคลใดบุคคลหนึ่งสามารถปกปิดข้อผิดพลาดหรือรายการผิดปกติได้ ซึ่งการจัดให้มีการแบ่งแยกหน้าที่ตามหลักการนี้ในระบบสารสนเทศที่ประมวลผลด้วยมือ สามารถทำได้โดยแยกหน้าที่หลักดังกล่าวให้บุคคลต่างคนกันรับผิดชอบ อย่างไรก็ตามในกรณีที่กิจการใช้เทคโนโลยีในการประมวลผลหน้าที่ที่ต้องแบ่งแยกกันในระบบสารสนเทศที่ประมวลผลด้วยมืออาจทำโดยเทคโนโลยีทั้งหมด เช่น การใช้เทคโนโลยีในการประมวลผลระบบลูกหนี้และรับเงิน ระบบสารสนเทศอาจทำหน้าที่ในการจัดทำเอกสารใบเบิกของจากเอกสารการสั่งซื้อของลูกค้าที่ได้รับอนุมัติ จัดทำใบแจ้งหนี้ และบันทึกรายการลูกหนี้ในบัญชีแยกประเภทย่อยทันทีที่มีการบันทึกรายการเบิกและส่งของ และส่งข้อมูลไปยังธนาคารเพื่อโอนเงินจากบัญชีธนาคารของลูกหนี้เข้าบัญชีธนาคารของกิจการโดยอัตโนมัติทันทีที่ยอดหนี้นั้นถึงกำหนดชำระ ซึ่งจุดนี้อาจก่อให้เกิดความเสี่ยงในการควบคุมได้หากมีผู้สามารถเข้าถึงโปรแกรมชุดคำสั่งการประมวลผล หรือข้อมูลได้ เช่น การที่โปรแกรมเมอร์สามารถเข้าถึงโปรแกรมระบบงานที่ใช้ในการประมวลผลจริงและข้อมูลจริงของระบบสารสนเทศ ทำให้สามารถเปลี่ยนแปลงและแก้ไขยอดลูกหนี้ หรือข้อมูลส่วนลดที่ลูกหนี้พึงได้รับซึ่งมีผลให้กิจการไม่ได้รับเงินหรือได้รับน้อยกว่าที่ควร เป็นต้น ดังนั้นการใช้ระบบงานสารสนเทศในการประมวลผลยังจำเป็นต้องมีการแบ่งแยกหน้าที่ที่เหมาะสม แต่รูปแบบการแบ่งแยกหน้าที่จะมีรายละเอียดที่แตกต่างไป เช่น การแบ่งแยกหน้าที่ภายในหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ และระหว่างหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและหน่วยงานผู้ใช้งาน โดยไม่ให้มีบุคคลใดบุคคลหนึ่งรับผิดชอบทั้งการพัฒนาระบบสารสนเทศ การจัดการและรักษาความปลอดภัยของระบบสารสนเทศ การปฏิบัติการด้านเทคโนโลยีสารสนเทศ การนำเข้าข้อมูล การอนุมัติรายการ และการตรวจสอบข้อมูล
- โอกาสที่ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานจะไม่พบข้อผิดพลาดและรายการผิดปกติในช่วงการทดสอบระบบสารสนเทศก่อนใช้งานจริงจะมีสูงขึ้นหากระบบสารสนเทศที่พัฒนาขึ้นหรือที่จะนำมาใช้งานมีความซับซ้อนและข้อผิดพลาดและรายการผิดปกตินั้นอาจยังมีอยู่ในระบบเป็นเวลานานหลังจากนำระบบสารสนเทศมาใช้งานกว่ากิจการจะตรวจพบ
- โอกาสที่จะมีผู้ที่ไม่ได้รับอนุมัติสามารถเข้าถึงระบบสารสนเทศ และทำการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ทิ้งร่องรอยที่สามารถมองเห็นและตรวจสอบได้สูงกว่าของระบบสารสนเทศที่ประมวลผลด้วยมือ
- ประสิทธิผลของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศอาจมีผลกระทบต่อประสิทธิผลของการควบคุมอื่น เช่น การควบคุมด้วยผู้ใช้งานหรือการปฏิบัติด้วยมือ ที่จำเป็นต้องใช้รายงานหรือข้อมูลออกของระบบสารสนเทศ (IT-Dependent Manual Controls) ดังนั้นการควบคุมอื่นเหล่านี้จะมีประสิทธิผลเมื่อระบบสารสนเทศสามารถประมวลผลและจัดทำรายงานหรือข้อมูลออกที่ผู้ใช้งานต้องการใช้ในการควบคุมได้ครบถ้วนและถูกต้อง ทั้งนี้เนื่องจากระบบสารสนเทศจะสามารถประมวลผลได้อย่างน่าเชื่อถือและมีประสิทธิผล หากระบบสารสนเทศที่ใช้นั้นมีการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เช่น การควบคุมการเข้าถึงและการควบคุมการพัฒนาและเปลี่ยนแปลงระบบสารสนเทศที่มีประสิทธิผล
- ระบบสารสนเทศอาจมีเครื่องมือสำหรับการวิเคราะห์ข้อมูล ซึ่งผู้บริหารสามารถใช้ช่วยในการสอบทานและควบคุมดูแลการปฏิบัติงานของพนักงานให้มีประสิทธิผลและประสิทธิภาพมากขึ้น เช่น เครื่องมือที่ช่วยให้ผู้บริหารสามารถดึงข้อมูลจากระบบสารสนเทศเพื่อใช้ในการติดตามผลการปฏิบัติงานของพนักงานได้โดยง่าย ซึ่งการใช้เครื่องมือเหล่านี้อาจช่วยให้การควบคุมโดยรวมของกิจการดีขึ้น

- การตรวจสอบระบบที่ใช้เทคโนโลยีที่ประมวลผลและวิเคราะห์ข้อมูลอาจเปิดโอกาสให้ผู้สอบบัญชีสามารถใช้เทคนิคการตรวจสอบโดยใช้เทคโนโลยีได้อย่างมีประสิทธิผลและประสิทธิภาพมากขึ้น เนื่องจากข้อมูลที่ต้องการใช้ในการทดสอบจะอยู่ในรูปอิเล็กทรอนิกส์แล้ว และอาจมีรูปแบบที่สามารถใช้ได้กับเครื่องมือที่ผู้สอบบัญชีมี เช่น โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป (Generalized Audit Software หรือ GAS) หรือโปรแกรมที่เขียนขึ้นโดยเฉพาะ (Specialized Audit Software)

ผู้สอบบัญชีพิจารณาปัจจัยข้างต้นร่วมกับปัจจัยอื่นที่สำคัญ เช่น ประเภทและลักษณะของธุรกิจ สภาพแวดล้อมทางเทคโนโลยีสารสนเทศ การควบคุมของกิจการ และทรัพยากรของผู้สอบบัญชี ในการกำหนดกลยุทธ์และแนวทางที่ผู้สอบบัญชีจะใช้ในการตรวจสอบ ซึ่งกลยุทธ์และแนวทางดังกล่าว จะทำให้ผู้สอบบัญชีสามารถกำหนดขอบเขตการใช้เทคโนโลยีประมวลผลข้อมูลของกิจการที่ควรครอบคลุมในการสอบบัญชี เช่น

- ผู้สอบบัญชีพิจารณาที่จะใช้กลยุทธ์และแนวทางการตรวจสอบที่ไม่อิงการควบคุมที่รวมถึงการควบคุมด้านเทคโนโลยีสารสนเทศ ในกรณีนี้ ขอบเขตงานของผู้สอบบัญชีจะครอบคลุมเพียงการทำความเข้าใจธุรกิจ รวมถึงสภาพแวดล้อมและการควบคุมของระบบสารสนเทศที่กิจการใช้ และการระบุความเสี่ยงที่สำคัญของระบบสารสนเทศที่กิจการใช้ต่อความถูกต้องและน่าเชื่อถือของข้อมูลทางการค้าและบัญชี รายงานการเงิน และหลักฐานการสอบบัญชี
- ผู้สอบบัญชีพิจารณาที่จะใช้กลยุทธ์และแนวทางการตรวจสอบที่อิงการควบคุมที่รวมถึงการควบคุมด้านเทคโนโลยีสารสนเทศเฉพาะประเภทของรายการบางประเภท เช่น รายการที่เป็นการซื้อและเจ้าหนี้ และรายการขายและลูกหนี้ ซึ่งกิจการมีการใช้ระบบสารสนเทศที่พัฒนาขึ้นเองชื่อ Logistics AccPlus ในการประมวลผลรายการดังกล่าว ส่วนรายการประเภทอื่นผู้สอบบัญชีจะใช้กลยุทธ์และแนวทางการตรวจสอบที่ไม่อิงการควบคุมในการตรวจสอบ แม้ว่ากิจการจะมีการใช้ระบบสารสนเทศอื่นในการประมวลผลข้อมูลรายการประเภทเหล่านั้น ในกรณีนี้ขอบเขตงานของผู้สอบบัญชีจะครอบคลุมการทำความเข้าใจสภาพแวดล้อมทางเทคโนโลยีและการควบคุมของระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำรายงานทางการเงินที่กิจการใช้ การระบุความเสี่ยงที่สำคัญของระบบสารสนเทศที่กิจการใช้ต่อความถูกต้องและน่าเชื่อถือของข้อมูลทางการค้าและบัญชี รายงานการเงิน และหลักฐานการสอบบัญชี และการประเมินประสิทธิผลของการออกแบบและการปฏิบัติตามการควบคุมของเฉพาะที่เกี่ยวกับระบบสารสนเทศ Logistics AccPlus ทั้งที่ระดับกิจการ ระดับการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ และระดับระบบงาน

ทั้งนี้ ขอบเขตและความซับซ้อนของระบบสารสนเทศที่กิจการใช้ อาจทำให้การตรวจสอบโดยใช้แนวทางการตรวจสอบรอบระบบ ซึ่งเป็นการตรวจสอบข้อมูลนำเข้าและผลลัพธ์ของระบบสารสนเทศ เพื่องานสอบบัญชีและไม่อิงการควบคุมด้านเทคโนโลยีสารสนเทศ เป็นแนวทางการตรวจสอบที่ไม่มีประสิทธิผลหรือไม่มีประสิทธิภาพ ดังนั้นแนวทางการตรวจสอบผ่านระบบหรือการตรวจสอบการประมวลผลของระบบและอิงการควบคุม โดยเฉพาะการควบคุมระบบงาน จึงอาจเป็นแนวทางที่ให้ประสิทธิผลและประสิทธิภาพมากกว่า

แม้ว่าในปัจจุบันผู้สอบบัญชีอาจมีเครื่องมือและเทคนิคอัตโนมัติ ที่ช่วยให้สามารถวิเคราะห์และตรวจสอบความครบถ้วน ความถูกต้องและความสมเหตุสมผลของรายการและข้อมูลอื่นที่นำเข้าระบบสารสนเทศ ของการประมวลผล และของการจัดทำผลลัพธ์โดยระบบสารสนเทศ ที่สามารถช่วยให้ผู้สอบบัญชีสามารถตรวจสอบรายการและข้อมูลจำนวนมากในเวลาอันรวดเร็ว ผู้สอบบัญชีอาจยังจำเป็นต้องประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศที่ระดับกิจการ (IT Entity-Level Controls) และการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ (IT General Controls) เพื่อให้สามารถเชื่อมั่นว่าข้อมูลจากระบบสารสนเทศที่นำมาใช้ในการวิเคราะห์และตรวจสอบด้วยเครื่องมือและเทคนิคอัตโนมัติ มีความครบถ้วน ความถูกต้อง ความสมเหตุสมผล และความน่าเชื่อถือตลอดช่วงระยะเวลาที่ผู้สอบบัญชีต้องการได้ความเชื่อมั่นหรือตั้งใจที่จะเชื่อถือในความครบถ้วน ความถูกต้อง ความสมเหตุสมผลและความน่าเชื่อถือของข้อมูลดังกล่าว

5. ข้อพิจารณาในการตรวจสอบระบบสารสนเทศเพื่อการสอบบัญชี

การใช้ระบบสารสนเทศในการบันทึกรายการค้า การประมวลผลข้อมูลทางการเงินและการจัดทำงบการเงินของกิจการ ทำให้ผู้สอบบัญชีต้องมีความเข้าใจเกี่ยวกับลักษณะและขอบเขตของสภาพแวดล้อมทางเทคโนโลยีสารสนเทศของกิจการ รวมถึงอาจต้องตรวจสอบระบบสารสนเทศที่กิจการใช้เพื่อวัตถุประสงค์การสอบบัญชีด้วย ซึ่งในการตรวจสอบระบบสารสนเทศนั้น ผู้สอบบัญชีต้องสามารถที่จะระบุและประเมินความเสี่ยงจากการใช้ระบบสารสนเทศของกิจการต่อความถูกต้องครบถ้วนและน่าเชื่อถือข้อมูลทางการเงิน งบการเงิน และหลักฐานการสอบบัญชีที่จัดเก็บหรือจัดทำโดยระบบสารสนเทศที่เกี่ยวข้อง ในกรณีที่ผู้สอบบัญชีตัดสินใจให้ต้องมีการตรวจสอบระบบสารสนเทศเป็นส่วนหนึ่งของงานสอบบัญชีของกิจการ ข้อพิจารณาที่ผู้สอบบัญชีควรคำนึงถึงมีดังต่อไปนี้

5.1. ความชำนาญและความรู้ความสามารถ

ในการสอบบัญชีในกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูลและการตรวจสอบระบบสารสนเทศ ผู้สอบบัญชีต้องมีความชำนาญและความรู้ความสามารถอย่างเพียงพอ เพื่อให้สามารถวางแผน สั่งการ ควบคุมดูแล และสอบทานงานสอบบัญชีได้อย่างมีประสิทธิผล โดยทั่วไปผู้สอบบัญชีต้องมีความรู้และความสามารถในเรื่องต่อไปนี้

- ความรู้และความเข้าใจเกี่ยวกับสภาพแวดล้อมทางเทคโนโลยีเพื่อการสอบบัญชีและองค์ประกอบหลักของระบบสารสนเทศ อันได้แก่ กระบวนการ เทคโนโลยี และคน ตามรายละเอียดที่ได้อธิบายในหัวข้อที่ 4 ความหมายและขอบเขตของการใช้เทคโนโลยีประมวลผลข้อมูลเพื่อการสอบบัญชี ตลอดถึงความสัมพันธ์ระหว่างองค์ประกอบหลักเหล่านั้นที่มีผลต่อความครบถ้วน ความถูกต้องความสมเหตุสมผลของรายการและความน่าเชื่อถือข้อมูลในงบการเงิน
- ความรู้และความเข้าใจเกี่ยวกับความเสี่ยงสืบเนื่องของระบบสารสนเทศของกิจการ ความสามารถและความชำนาญในการวิเคราะห์ข้อมูลที่รวบรวมได้เพื่อระบุความเสี่ยงสืบเนื่องและประเมินผลกระทบของความเสี่ยงเหล่านั้นต่อยอดคงเหลือในบัญชีและรายการแต่ละประเภทของกิจการ รวมถึงสิ่งที่ผู้บริหารได้ให้การรับรองไว้
- ความรู้เกี่ยวกับลักษณะและวิธีการควบคุมสำหรับระบบสารสนเทศของกิจการความสามารถและความชำนาญในการวิเคราะห์ที่จะระบุการควบคุมและประเมินประสิทธิผลของการควบคุมของกิจการ
- ความรู้เกี่ยวกับวิธีการและเทคนิคการตรวจสอบระบบสารสนเทศ ความสามารถและความชำนาญในการใช้วิธีการและเทคนิคการตรวจสอบเหล่านั้นอย่างเพียงพอที่จะออกแบบและดำเนินการทดสอบการควบคุมและการตรวจสอบเนื้อหาสาระ รวมถึงการสรุปผลการทดสอบและการตรวจสอบอย่างเหมาะสม
- ความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศและระบบสารสนเทศ เช่น
  - ประเภทและลักษณะที่สำคัญของสถาปัตยกรรมของระบบสารสนเทศ ซึ่งมีการจัดประเภทในหลายแบบ อีกทั้งสถาปัตยกรรมของระบบสารสนเทศที่กิจการใช้อาจมีได้หลากหลายรูปแบบ เช่น
    1. ระบบแบบชั้นเดียว (1-Tier System Architecture) ซึ่งระบบสารสนเทศที่ใช้สถาปัตยกรรมแบบนี้ ได้แก่ ระบบงานแบบเดี่ยว (Stand-Alone Application System) ที่การนำข้อมูลเข้า การประมวลผลข้อมูล การจัดเก็บข้อมูล และการแสดงผลจะทำอยู่ในเครื่องคอมพิวเตอร์เพียงเครื่องเดียวและระบบงานรวมศูนย์ที่เครื่องแม่ข่าย (Host-Based Application System) ที่การประมวลผล การจัดการและการจัดเก็บข้อมูลทั้งหมดจะทำที่เครื่องแม่ข่าย ส่วนเครื่องลูกข่าย (Client) จะทำหน้าที่เป็นเพียงอุปกรณ์นำเข้าข้อมูลจากผู้ใช้งานและแสดงข้อมูลออกให้ผู้ใช้งานเท่านั้น

2. ระบบแบบหลายชั้น (N-Tier System Architecture หรือ Multi-Tier System Architecture) ซึ่งระบบสารสนเทศที่ใช้กันทั่วไปที่มีสถาปัตยกรรมแบบนี้ คือ ระบบรับ-ให้บริการหรือที่เรียกกันว่า ระบบไคลเอนต์/เซิร์ฟเวอร์ (Client-Server System Architecture) ซึ่งเป็นระบบที่มีเครื่องคอมพิวเตอร์ที่เป็นเครื่องให้บริการต่าง ๆ ขึ้นกับการร้องขอบริการจากเครื่องรับบริการ เช่น บริการประมวลผลซอฟต์แวร์ระบบงาน บริการฐานข้อมูล โดยระบบดังกล่าวอาจออกแบบให้เป็นระบบแบบสองชั้น (2-Tier System Architecture) เช่น สถาปัตยกรรมแบบกระจายที่เครื่องลูกข่าย (Client-Based Architecture) ที่การทำงานทุกอย่างจะอยู่ที่เครื่องลูกข่าย และเครื่องแม่ข่ายจะทำหน้าที่เป็นที่เก็บข้อมูลเท่านั้น หรือ 3-Tier System Architecture หรือมากกว่านั้น ขึ้นอยู่กับว่าจะมีการแยกการแสดงผล (Presentation) การประมวลผล (Application Processing) การจัดการข้อมูล (Data Management) และการจัดเก็บข้อมูล (Data Storage) ออกจากกันเป็นกี่ชั้น
3. ระบบคลาวด์ (Cloud System Architecture) เป็นรูปแบบหนึ่งของสถาปัตยกรรมแบบระบบไคลเอนต์/เซิร์ฟเวอร์ ซึ่งระบบคลาวด์นี้อาจมีได้หลายรูปแบบ เช่น เป็นแบบ Public Cloud แบบ Private Cloud แบบ Hybrid Cloud แบบ Multi-Cloud หรือ แบบ Community Cloud และมีรูปแบบการให้บริการหลายรูปแบบ เช่น บริการแพลตฟอร์ม (Platform-as-a-Service หรือเรียกอย่างย่อว่า PaaS) บริการโครงสร้างพื้นฐาน (Infrastructure-as-a-Service หรือเรียกอย่างย่อว่า IaaS) บริการซอฟต์แวร์ (Software-as-a-Service หรือเรียกอย่างย่อว่า SaaS) โดยรายละเอียดเกี่ยวกับระบบคลาวด์นี้สามารถศึกษาได้ในบทที่ 5 เรื่อง ความเสี่ยง การควบคุม และการตรวจสอบการใช้เทคโนโลยีสมัยใหม่
4. ระบบเชิงเว็บ (N-Tier Web-Based System Architecture) เป็นอีกรูปแบบหนึ่งของสถาปัตยกรรมแบบระบบไคลเอนต์/เซิร์ฟเวอร์ ซึ่งอาจเป็นแบบ 2-Tier หรือ N-Tier ก็ได้ โดยมีลักษณะสำคัญที่การเรียกใช้บริการจะทำผ่านทางเว็บบราว์เซอร์ (Web Browser) และผู้ใช้งานสามารถเข้าถึงระบบและใช้บริการของระบบสารสนเทศทางเครือข่ายอินเทอร์เน็ตหรือเครือข่ายอินทราเน็ตของกิจการ
5. ระบบเพียร์ทูเพียร์หรือพีทูพี (Peer-To-Peer System Architecture หรือ P2P System Architecture) เป็นรูปแบบที่เครื่องคอมพิวเตอร์ในระบบสารสนเทศจะเชื่อมต่อกันเอง โดยทุกเครื่องจะเหมือนกันหรือเท่าเทียมกัน และแต่ละเครื่องจะทำหน้าที่ทั้งหมดไม่ว่าจะเป็นการแสดงผล การประมวลผล การจัดการข้อมูล และการจัดเก็บข้อมูล รวมถึงจะเป็นได้ทั้งเครื่องแม่ข่ายและเครื่องลูกข่าย ซึ่งทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของเครื่องคอมพิวเตอร์ใดก็ได้ แทนที่จะต้องใช้จากเครื่องแม่ข่ายเท่านั้น
6. ระบบเชิงบริการ (Services-Oriented System Architecture หรือเรียกอย่างย่อว่า SOA) เป็นรูปแบบหนึ่งของการออกแบบสถาปัตยกรรมระบบสารสนเทศ ที่แยกส่วนการทำงานของระบบออกเป็นองค์ประกอบ (Components) โดยที่แต่ละองค์ประกอบจะประกอบไปด้วยบริการต่าง ๆ ซึ่งทำงานอย่างใดอย่างหนึ่ง และมีการกำหนดเกณฑ์วิธี (Protocol) ในการสื่อสารระหว่างองค์ประกอบไว้ด้วย ตัวอย่างของสถาปัตยกรรมแบบนี้ คือ Microservices System Architecture ที่จะแยกระบบตามแต่ละบริการของระบบออกจากกันโดยชัดเจน ซึ่งแต่ละบริการสามารถทำงานได้อย่างเป็นอิสระ มีฐานข้อมูลเป็นของตัวเอง และหากจำเป็นต้องใช้ข้อมูลที่อยู่ในบริการอื่น ก็สามารถเรียกใช้ผ่าน Application Programming Interface หรือที่เรียกโดยย่อว่า API ได้

ทั้งนี้ สถาปัตยกรรมระบบสารสนเทศแต่ละรูปแบบจะมีปัจจัยเสี่ยง ความเสี่ยงสืบเนื่อง ระดับความเสี่ยง และการควบคุมส่วนหนึ่งที่ต่างกัน เช่น ระบบสารสนเทศที่มีสถาปัตยกรรมรวมศูนย์แบบชั้นเดียว จะมีปัจจัยเสี่ยงและความเสี่ยงที่ซับซ้อนน้อยกว่าระบบสารสนเทศที่มีสถาปัตยกรรมแบบหลายชั้น และมีแนวโน้มจะมีความเสี่ยงสืบเนื่องที่จะมีการเข้าถึงข้อมูลและการเปลี่ยนแปลงแก้ไขระบบสารสนเทศจากบุคคลภายนอกที่ต่ำกว่าระบบสารสนเทศที่มีสถาปัตยกรรมแบบระบบคลาวด์

- ซอฟต์แวร์ระบบงานหรือเครื่องมือที่นิยมใช้ในการนำเข้า ประมวลผล จัดทำรายงาน และจัดเก็บข้อมูล เช่น ซอฟต์แวร์สำหรับช่วยสร้างรายงาน ทั้งนี้เนื่องจากในกรณีที่กิจการมีการใช้ซอฟต์แวร์ระบบงานหรือเครื่องมือดังกล่าว ผู้สอบบัญชีอาจจำเป็นต้องพิจารณาถึงความเสี่ยงที่เกิดขึ้นจากการใช้ซอฟต์แวร์ระบบงานหรือเครื่องมือนั้น
- แหล่งที่มาของซอฟต์แวร์ระบบงาน เช่น เป็นซอฟต์แวร์ที่กิจการพัฒนาขึ้นเอง โดยบุคลากรของกิจการ เป็นซอฟต์แวร์ที่กิจการจ้างบุคคลภายนอกพัฒนาขึ้นเป็นซอฟต์แวร์สำเร็จรูปที่ใช้โดยไม่ได้ปรับแต่ง เป็นซอฟต์แวร์สำเร็จรูปที่กิจการมีการปรับแต่งเป็นซอฟต์แวร์ของหน่วยงานภายนอก เป็นซอฟต์แวร์แบบบริการคลาวด์ (Software-as-a-Services) หรือเป็นซอฟต์แวร์แบบฟรีแวร์
- องค์ประกอบด้านฮาร์ดแวร์ของระบบสารสนเทศ เช่น หน้าที่ของหน่วยประมวลผลส่วนกลางและตัวอย่างของหน่วยจัดเก็บข้อมูล อุปกรณ์นำเข้าข้อมูลและอุปกรณ์นำข้อมูลออก
- องค์ประกอบด้านซอฟต์แวร์ของระบบสารสนเทศ เช่น หน้าที่ของและความแตกต่างระหว่างซอฟต์แวร์ระบบและซอฟต์แวร์ระบบงาน
- วิธีการในการประมวลผล เช่น ลักษณะและความแตกต่างระหว่างการประมวลผลแบบรวมกลุ่มและแบบเชื่อมตรง และ ลักษณะและความแตกต่างระหว่างการประมวลผลแบบรวมศูนย์ แบบแยกจากศูนย์และแบบกระจาย
- การกำกับดูแล การบริหารจัดการข้อมูล และรูปแบบของการจัดเก็บข้อมูล เช่น ข้อดีและข้อเสียของการจัดเก็บข้อมูลแบบฐานข้อมูล ในบางกรณีกิจการอาจมีระบบคลังข้อมูล (Data Warehouse) ซึ่งสามารถเข้าถึงได้โดยผู้ใช้งานเพื่อจัดทำรายงานหรือเพื่อวิเคราะห์ข้อมูล หรือโดยบุคลากรด้านเทคโนโลยีสารสนเทศที่มีสิทธิพิเศษ ซึ่งผู้สอบบัญชีอาจพิจารณาให้คลังข้อมูล (Data Warehouse) เป็นระบบสารสนเทศที่ตรวจสอบเพื่อการสอบบัญชีด้วย หากผู้สอบบัญชีพิจารณาแล้ว เห็นว่ามีผลกระทบต่อหลักฐานการสอบบัญชีหรือความครบถ้วน ความถูกต้องและความสมเหตุสมผลของรายการและข้อมูลทางการเงินและงบการเงินของกิจการอย่างมีสาระสำคัญ
- เทคโนโลยีอื่น ๆ ที่สำคัญในธุรกิจ เช่น ลักษณะและความแตกต่างระหว่างระบบเครือข่ายแบบ LAN, WAN, VAN, Internet, Intranet และ Extranet ลักษณะและข้อดี ข้อเสียของระบบรับ-ให้บริการ (Client-Server Systems) ลักษณะและข้อดี ข้อเสียของระบบพาณิชยธุรกิจ (e-Commerce) ลักษณะและข้อดี ข้อเสียของระบบคลาวด์
- ศัพท์เทคโนโลยีและชื่อผลิตภัณฑ์เทคโนโลยีที่สำคัญ
- ความเสี่ยงสืบเนื่องของระบบสารสนเทศ ซึ่งอาจเกิดจากหลายปัจจัยเสี่ยง เช่น จากการใช้บริการระบบคลาวด์จากผู้ให้บริการ จากการใช้ระบบสารสนเทศที่พัฒนาขึ้นเอง จากการเชื่อมต่อระบบสารสนเทศของกิจการกับระบบของหน่วยงานภายนอก หรือจากการที่กิจการให้บุคคลภายนอกเข้ามาใช้ระบบสารสนเทศของกิจการ ซึ่งตัวอย่างของความเสี่ยงสืบเนื่องที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศมีดังนี้

    1. การเข้าถึงข้อมูลและเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ซึ่งรวมถึงการบันทึกรายการที่ไม่ได้รับอนุญาตหรือไม่มีอยู่จริง จากการที่ระบบสารสนเทศไม่สามารถให้สิทธิตามบทบาทหน้าที่ได้ หรือจากการที่บุคลากรด้านการพัฒนาระบบสารสนเทศได้รับสิทธิในการเข้าถึงระบบสารสนทศที่ใช้งานจริงได้ เนื่องจากข้อจำกัดด้านทรัพยากรของกิจการ
    2. การบันทึกรายการที่ไม่ถูกต้องและครบถ้วนจากการที่ผู้ใช้งานหลายคนสามารถเข้าถึงและเปลี่ยนแปลงฐานข้อมูลที่ใช้ร่วมกันในเวลาเดียวกัน
    3. การเข้าถึงข้อมูลและเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือการประมวลผลที่ผิดพลาดจากการเปลี่ยนแปลงระบบสารสนเทศหรือด้านอื่นของสภาพแวดล้อมทางเทคโนโลยีสารสนเทศซึ่งผู้ให้บริการจากภายนอกไม่ได้แจ้งให้ทราบหรือแจ้งให้ทราบแต่กิจการไม่ทราบถึงผลกระทบต่อการควบคุมหรือต่อการประมวลผลข้อมูลของระบบสารสนเทศจึงไม่ได้ดำเนินการใด ๆ
    4. การสูญเสียข้อมูลหรือการไม่สามารถเข้าถึงข้อมูลของระบบสารสนเทศได้ตามต้องการจากการถูกโจมตีทางไซเบอร์ผ่านทางระบบเครือข่ายที่ระบบสารสนเทศเชื่อมต่ออยู่

- การควบคุมด้านเทคโนโลยีสารสนเทศของระบบสารสนเทศ เช่น ความหมายและวิธีการของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศและการควบคุมระบบงาน ซึ่งการควบคุมที่กิจการใช้มักจะประกอบด้วยการควบคุมที่ปฏิบัติด้วยมือและการควบคุมโดยอัตโนมัติ แต่การออกแบบการควบคุมของแต่ละกิจการว่าจะมีการควบคุมที่เป็นอัตโนมัติมากน้อยเพียงใดจะขึ้นอยู่กับลักษณะและความซับซ้อนของการใช้เทคโนโลยีสารสนเทศของกิจการ อย่างไรก็ดีจะเห็นว่าการควบคุมโดยอัตโนมัติอาจเชื่อถือได้มากกว่าการควบคุมที่ปฏิบัติด้วยมือ เนื่องจากการควบคุมโดยอัตโนมัติที่ได้รับการออกแบบและฝังหรือตั้ง ค่าในระบบสารสนเทศที่ใช้งานจริงอย่างมีประสิทธิผลจะลดปัญหาที่สำคัญของของการควบคุมที่ปฏิบัติด้วยมือ คือ การผิดพลาดจากผู้ปฏิบัติงานทั้งที่ตั้งใจและไม่ตั้งใจได้
- การตรวจสอบโดยใช้คอมพิวเตอร์ช่วย ซึ่งรายละเอียดในเรื่องนี้สามารถศึกษาได้ในบทที่ 4 เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (CAAT)

5.2. การใช้ผู้เชี่ยวชาญด้านการตรวจสอบระบบสารสนเทศในงานสอบบัญชี

การตรวจสอบระบบสารสนเทศอาจดำเนินการโดยผู้สอบบัญชีที่ทำการตรวจสอบระบบสารสนเทศเป็นส่วนหนึ่งของการตรวจสอบเพื่อแสดงความเห็นต่องบการเงินของกิจการ โดยเฉพาะในกรณีที่ระบบสารสนเทศที่กิจการใช้ไม่มีความซับซ้อนและการควบคุมหลักของกิจการยังเป็นการควบคุมที่ปฏิบัติด้วยมือ ตลอดถึงหลักฐานการสอบบัญชีที่สำคัญส่วนมากยังอยู่ในรูปกระดาษ ในกรณีที่ผู้สอบบัญชีจำเป็นต้องตรวจสอบระบบสารสนเทศของกิจการที่มีความซับซ้อน ผู้สอบบัญชีอาจไม่มีความรู้ความสามารถ และความชำนาญด้านเทคโนโลยีสารสนเทศอย่างเพียงพอที่จะปฏิบัติงานตรวจสอบระบบสารสนเทศได้เองอย่างมีประสิทธิผล ผู้สอบบัญชีจึงจำเป็นต้องพิจารณาใช้ผู้เชี่ยวชาญที่มีทักษะ ความรู้และประสบการณ์ด้านการตรวจสอบเทคโนโลยีสารสนเทศมาช่วยงาน ทั้งนี้ในการใช้ผู้เชี่ยวชาญดังกล่าว ผู้สอบบัญชีจำเป็นต้องมีหลักฐานการสอบบัญชีที่เพียงพอและเหมาะสมว่างานของผู้เชี่ยวชาญนั้นเพียงพอสำหรับวัตถุประสงค์การตรวจสอบและเป็นไปตามมาตรฐานการสอบบัญชี รหัส 620 เรื่อง “การใช้ผลงานของผู้เชี่ยวชาญของผู้สอบบัญชี” เช่น ผู้สอบบัญชีควรประเมินความเพียงพอและเหมาะสมของความสามารถของผู้เชี่ยวชาญ หากผู้สอบบัญชีวางแผนที่จะใช้ผลงานของผู้เชี่ยวชาญนั้น เป็นต้น

5.3. เทคโนโลยีอุบัติใหม่

กิจการอาจมีการใช้เทคโนโลยีอุบัติใหม่ เช่น ระบบคลาวด์ บล็อกเชน วิทยาการหุ่นยนต์ ปัญญาประดิษฐ์ เงินหรือสินทรัพย์ดิจิทัล หรือโดรน ในระบบสารสนเทศที่เกี่ยวข้องกับการประมวลผลข้อมูลและรายการค้าและการจัดทำรายงานทางการเงิน รวมถึงหลักฐานการสอบบัญชีที่สำคัญ ดังตัวอย่างต่อไปนี้

- การใช้ระบบงานบัญชีแบบคลาวด์
- การใช้ระบบบล็อกเชนในการทำรายการค้ากับคู่ค้าตั้งแต่การเกิดรายการ ไปจนถึงการรับชำระเงินหรือการจ่ายเงินผ่านสถาบันการเงิน
- การใช้วิทยาการหุ่นยนต์ในการตรวจสอบเอกสารบัญชี และการบันทึกรายการบัญชีที่มีสาระสำคัญต่องบการเงิน
- การใช้ปัญญาประดิษฐ์ในการอนุมัติการให้หรือเพิ่มวงเงินสินเชื่อ การตั้งประมาณการต่าง ๆ เช่น ประมาณการหนี้สงสัยจะสูญและประมาณการอายุการให้ประโยชน์ของสินทรัพย์ แทนการใช้คน
- การใช้เงินดิจิทัลหรือสินทรัพย์ดิจิทัลเป็นอีกรูปแบบหนึ่งในการทำธุรกรรมของกิจการ ซึ่งระบบหรือแพลตฟอร์มที่เกี่ยวข้องอาจเป็นของบุคคลภายนอกหรือของกิจการเองก็ได้ นอกจากนี้กิจการอาจเป็นผู้ออกเงินดิจิทัลหรือสินทรัพย์ดิจิทัลนั้นเองด้วยก็ได้
- การใช้โดรนในการตรวจสอบสภาพและตรวจนับสินค้าคงคลังหรือทรัพย์สินที่มีสาระสำคัญต่องบการเงินในกรณีที่วิธีการอื่นมีประสิทธิผลและประสิทธิภาพน้อยกว่าหรือไม่สามารถใช้ได้

เมื่อกิจการมีการใช้เทคโนโลยีอุบัติใหม่ในระบบสารสนเทศที่เกี่ยวข้องกับการประมวลผลข้อมูลและรายการค้า รวมถึงการจัดทำรายงานทางการเงิน และหลักฐานการสอบบัญชีที่สำคัญ ผู้สอบบัญชีจึงอาจจำเป็นต้องรวมเทคโนโลยีอุบัติใหม่ดังกล่าวเป็นส่วนหนึ่งของขอบเขตงานการตรวจสอบระบบสารสนเทศภายใต้งานสอบบัญชี เช่น การทำความเข้าใจสภาพแวดล้อมของเทคโนโลยีอุบัติใหม่นั้น การระบุความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีอุบัติใหม่ดังกล่าว และการประเมินประสิทธิผลการควบคุมที่เกี่ยวข้อง แม้ว่าเทคโนโลยีอุบัติใหม่อาจมีความซับซ้อนมากกว่าเทคโนโลยีที่มีอยู่ในปัจจุบันมาระยะหนึ่งมาก ความรับผิดชอบของผู้สอบบัญชีในการตรวจสอบการใช้เทคโนโลยีอุบัติใหม่ดังกล่าวยังคงไม่เปลี่ยนแปลงหรือมีข้อยกเว้น เช่น ผู้สอบบัญชีไม่สามารถเลือกใช้แนวทางการตรวจสอบที่ไม่อิงการควบคุม หรือเลือกทดสอบการควบคุมที่ปฏิบัติด้วยมือแทนการควบคุมแบบอัตโนมัติ ในกรณีที่กิจการมีการใช้ระบบสารสนเทศและเทคโนโลยีอุบัติใหม่ที่มีความซับซ้อนเกินกว่าการควบคุมที่ปฏิบัติด้วยมือหรือการตรวจสอบเนื้อหาสาระจะมีประสิทธิผลหรือประสิทธิภาพได้ เพียงเพราะผู้สอบบัญชีไม่มีทรัพยากรหรือความรู้ความสามารถเพียงพอในการตรวจสอบ

5.4. ขอบเขตที่ผู้สอบบัญชีสามารถปฏิบัติงานได้

ในกรณีที่กิจการใช้ซอฟต์แวร์ของระบบสารสนเทศเป็นซอฟต์แวร์สำเร็จรูปทางบัญชีเชิงพาณิชย์ ซึ่งกิจการไม่มีสิทธิเข้าถึงรหัสโปรแกรมต้นฉบับเพื่อทำการเปลี่ยนแปลงใด ๆ ขอบเขตที่ผู้สอบบัญชีสามารถปฏิบัติงานได้ในการตรวจสอบระบบสารสนเทศ คือ การทำความเข้าใจลักษณะของซอฟต์แวร์สำเร็จรูปทางบัญชีเชิงพาณิชย์ในเรื่องต่อไปนี้

- ระดับการยอมรับและความมีชื่อเสียงในด้านความน่าเชื่อถือของซอฟต์แวร์
- ระดับความเป็นไปได้ที่กิจการจะแก้ไขหรือปรับเปลี่ยนการทำงานของซอฟต์แวร์สำเร็จรูปทางบัญชีเชิงพาณิชย์ เช่น การเพิ่มโปรแกรมหรือชุดคำสั่งเสริมเข้ากับซอฟต์แวร์สำเร็จรูปทางบัญชีเชิงพาณิชย์ รวมถึงความเสี่ยงต่อความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของข้อมูลทางการเงิน หลักฐานการสอบบัญชี และงบการเงิน
- ลักษณะและขอบเขตของการแก้ไขที่สามารถดำเนินการได้โดยกิจการ ซึ่งซอฟต์แวร์สำเร็จรูปทางบัญชีเชิงพาณิชย์ส่วนมากจะอนุญาตให้ทำการตั้งค่าได้ ผู้สอบบัญชีจึงต้องพิจารณาขอบเขตที่กิจการสามารถตั้งค่าซอฟต์แวร์ดังกล่าวได้ รวมถึงความเสี่ยงต่อความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของข้อมูลทางการเงิน หลักฐานการสอบบัญชี และงบการเงินที่เกิดจากความสามารถในการตั้งค่าในซอฟต์แวร์ดังกล่าว
- ระดับความเป็นไปได้ที่จะเพิ่ม แก้ไข หรือลบข้อมูลในระดับฐานข้อมูลของระบบสารสนเทศได้โดยตรงโดยไม่ผ่านซอฟต์แวร์สำเร็จรูปทางบัญชีเชิงพาณิชย์ รวมถึงความเสี่ยงต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผลและความน่าเชื่อของข้อมูลทางการเงิน หลักฐานการสอบบัญชี และงบการเงิน หากความเป็นไปได้และขอบเขตที่สามารถดำเนินการกับข้อมูลที่สำคัญต่องบการเงินและการสอบบัญชีมาก ผู้สอบบัญชีต้องประเมินประสิทธิผลของการควบคุมของกิจการที่ตอบสนองต่อการรักษาความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของข้อมูล ซึ่งอาจประกอบด้วยการควบคุมทั่วไปของเทคโนโลยีสารสนเทศด้านการเข้าถึงและการเปลี่ยนแปลง ข้อมูลและการควบคุมระบบงาน

นอกจากนี้ในกรณีที่กิจการใช้บริการจากผู้ให้บริการจากภายนอกเพื่อจัดการงานบางส่วนของสภาพแวดล้อมของระบบสารสนเทศที่ผู้สอบบัญชีต้องครอบคลุมในการตรวจสอบ หรือดำเนินการกระบวนการด้านเทคโนโลยีสารสนเทศบางกระบวนการที่เกี่ยวข้องกับระบบสารสนเทศดังกล่าว เช่น การใช้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (Infrastructure-as-a-service หรือ IaaS) ผู้สอบบัญชีต้องทำความเข้าใจผลกระทบของการใช้บริการเหล่านั้นต่อขอบเขตที่ผู้สอบบัญชีสามารถปฏิบัติงานได้ และพิจารณาหาแนวทางที่เหมาะสมเพื่อให้ผู้สอบบัญชีปฏิบัติงานได้อย่างเพียงพอต่อการแสดงความเห็นต่องบการเงิน ซึ่งหัวข้อที่ 9 การตรวจสอบในกรณีที่กิจการใช้บริการเกี่ยวกับระบบสารสนเทศจากองค์กรที่ให้บริการ ได้อธิบายรายละเอียดเพิ่มเติมในเรื่องนี้

5.5. โปรแกรม ชุดคำสั่ง หรือเครื่องมือที่พัฒนาหรือจัดหาและดูแลโดยผู้ใช้งาน

หลักฐานการสอบบัญชีอาจมาในรูปแบบของผลลัพธ์ที่ระบบสารสนเทศสร้างขึ้นแล้วนำไปคำนวณโดยใช้โปรแกรม ชุดคำสั่ง หรือเครื่องมือที่พัฒนาหรือจัดหาและดูแลโดยผู้ใช้งาน เช่น กระดาษคำนวณอิเล็กทรอนิกส์ หรือโปรแกรมที่พัฒนาโดยผู้ใช้งาน แต่โปรแกรม ชุดคำสั่ง หรือเครื่องมือเหล่านี้มักไม่ได้ถูกระบุให้เป็นระบบสารสนเทศที่ครอบคลุมในการตรวจสอบระบบสารสนเทศของผู้สอบบัญชี เนื่องจากการออกแบบและการนำการควบคุมไปปฏิบัติสำหรับการเข้าถึงและการเปลี่ยนแปลงโปรแกรม ชุดคำสั่ง หรือเครื่องมือที่พัฒนาหรือจัดหาและดูแลโดยผู้ใช้งานมักจะไม่ครอบคลุมอยู่ในการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ดูแลรับผิดชอบโดยหน่วยงานเทคโนโลยีสารสนเทศของกิจการ ผู้สอบบัญชีจึงจำเป็นต้องทำความเข้าใจและระบุความเสี่ยงสืบเนื่องจากการใช้โปรแกรม ชุดคำสั่ง หรือเครื่องมือที่พัฒนาหรือจัดหาและดูแลโดยผู้ใช้งาน โดยคำนึงถึงวัตถุประสงค์และความซับซ้อนของโปรแกรม ชุดคำสั่ง หรือเครื่องมือที่พัฒนาหรือจัดหาและดูแลโดยผู้ใช้งานที่เกี่ยวข้อง ในกรณีที่ผู้สอบบัญชีสรุปว่าการใช้โปรแกรม ชุดคำสั่ง หรือเครื่องมือที่พัฒนาหรือจัดหาและดูแลโดยผู้ใช้งานมีผลกระทบต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผลและความน่าเชื่อถือของงบการเงินและหลักฐานการสอบบัญชีอย่างมีสาระสำคัญ การสอบบัญชีอาจจำเป็นต้องประเมินประสิทธิผลของการควบคุมที่เกี่ยวข้อง เช่น

- การควบคุมโดยอัตโนมัติหรือการควบคุมแบบอื่นที่กิจการนำมาใช้เพื่อให้มั่นใจว่าข้อมูลที่ดึงออกมาจากคลังข้อมูลหรือจากระบบงานสารสนเทศและโอนเข้าโปรแกรมที่พัฒนาโดยผู้ใช้งานเพื่อประมวลผลต่อถูกต้องและครบถ้วน เช่น การกระทบยอดรายงานกับข้อมูลที่ได้มา การเปรียบเทียบกับข้อมูลแต่ละรายการจากรายงานไปยังแหล่งที่มาและในทางกลับกัน การกระทบยอดจำนวนรายการและขนาดของข้อมูลและให้มีการดึงและโอนข้อมูลใหม่หากพบข้อผิดพลาดโดยอัตโนมัติ การจำกัดสิทธิไม่ให้สามารถแก้ไขข้อมูลที่โอนมาได้
- การควบคุมที่ตรวจสอบว่าตรรกะของโปรแกรมที่พัฒนาโดยผู้ใช้งานทำงานตามที่ตั้งใจไว้ เช่น การควบคุมที่มีการทดสอบสูตรการคำนวณหรือชุดคำสั่งที่ใช้ทำงานอัตโนมัติก่อนนำโปรแกรมที่พัฒนาโดยผู้ใช้งานไปใช้งานจริงโดยผู้พัฒนาโปรแกรมและผู้ใช้งานคนอื่นที่มีความรู้ความสามารถที่เหมาะสม หรือการควบคุมโดยการใช้เครื่องมือที่ตรวจสอบความถูกต้องของการประมวลผลข้อมูลแบบอัตโนมัติ เช่น การสร้างสูตรการคำนวณหรือชุดคำสั่งที่ทำการกระทบยอดที่ประมวลผลได้โดยอัตโนมัติในกระดาษคำนวณอิเล็กทรอนิกส์

5.6. ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กิจการมีความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ในกรณีที่ระบบสารสนเทศที่ใช้ในการดำเนินธุรกิจของกิจการซึ่งรวมถึงระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำรายงานทางการเงิน สามารถเข้าถึงได้ผ่านทางอินเทอร์เน็ตหรือเครือข่ายสาธารณะอื่นไม่ว่าโดยทางตรงหรือทางอ้อม เช่น กิจการมีซอฟต์แวร์ระบบงานของกิจการที่ติดตั้งบนมือถือ และระบบงานที่เข้าผ่านเว็บไซต์ของกิจการเพื่อให้ลูกค้าสามารถสั่งสินค้าและชำระเงินได้ หรือกิจการมีการใช้ระบบอีเมล ซึ่งทำให้มีโอกาสที่จะมีการส่งอีเมลที่เป็นภัยต่อกิจการมายังผู้ใช้งานของกิจการได้ ความเสี่ยงนี้อาจส่งผลกระทบต่อรายงานทางการเงิน เช่น การโอนเงินของกิจการไปยังบัญชีธนาคารของเจ้าหนี้ที่ไม่ถูกต้อง แต่ได้มีการตัดยอดเจ้าหนี้แล้ว หรือการสูญเสียทรัพย์สินของกิจการ เช่น ข้อมูลที่ไม่สามารถเข้าถึงและกู้คืนได้ ผู้สอบบัญชีจึงจำเป็นต้องมีความเข้าใจเกี่ยวกับสภาพแวดล้อมทางเทคโนโลยีสารสนเทศของกิจการที่เพียงพอต่อการระบุภัยคุกคามอาจเข้ามาผ่านทางขอบเครือข่ายรอบนอกที่เชื่อมต่อกับอินเทอร์เน็ตหรือเครือข่ายสาธารณะ และเข้าสู่เครือข่ายภายในที่อาจมีช่องทางเชื่อมต่อกับระบบสารสนเทศ ฐานข้อมูล และระบบปฏิบัติการที่กระทบต่อการจัดทำงบการเงินได้ รวมถึงต่อการระบุและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกิจการด้วย ในกรณีที่ผู้สอบบัญชีพบว่ามีเหตุการณ์การละเมิดการรักษาความมั่นคงปลอดภัย ผู้สอบบัญชีควรพิจารณาในประเด็นต่อไปนี้

- โอกาสที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อการรายงานทางการเงิน หากผู้สอบบัญชีประเมินว่าการรายงานทางการเงินมีโอกาสที่จะได้รับผลกระทบในระดับที่เป็นสาระสำคัญ ผู้สอบบัญชีอาจพิจารณาและตัดสินใจที่จะทำความเข้าใจและทดสอบการควบคุมที่เกี่ยวข้องเพื่อระบุระดับของผลกระทบต่อการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงที่อาจเกิดขึ้นในงบการเงิน
- ความจำเป็นและความเพียงพอของการเปิดเผยข้อมูลเกี่ยวกับเหตุการณ์การละเมิดการรักษาความมั่นคงปลอดภัยในงบการเงิน

5.7. กฎหมายและข้อบังคับที่อาจมีผลกระทบทางตรงหรือทางอ้อมต่องบการเงินของกิจการ

มาตรฐานการสอบบัญชี รหัส 250 (ปรับปรุง) กำหนดความรับผิดชอบของผู้สอบบัญชีในการพิจารณากฎหมายและข้อบังคับในการตรวจสอบงบการเงิน โดยผู้สอบบัญชีต้องระบุการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญต่องบการเงินจากการไม่ปฏิบัติตามกฎหมายและข้อบังคับ แต่ผู้สอบบัญชีไม่ได้มีความรับผิดชอบในการป้องกันการไม่ปฏิบัติตามกฎหมายและข้อบังคับ และไม่ได้ถูกคาดหวังให้ตรวจพบการไม่ปฏิบัติตามกฎหมายและข้อบังคับทั้งหมด นอกจากนี้การไม่ปฏิบัติตามกฎหมายและข้อบังคับอาจทำให้กิจการต้องชำระค่าปรับ ถูกฟ้องร้อง หรือเกิดผลกระทบอื่น ๆ ที่ตามมาต่อกิจการซึ่งอาจมีผลกระทบที่เป็นสาระสำคัญต่องบการเงินด้วย

ผู้สอบบัญชีอาจต้องพิจารณากฎหมายและข้อบังคับในการตรวจสอบระบบสารสนเทศด้วย เพราะมีกฎหมายและข้อบังคับอื่นที่ไม่มีผลกระทบโดยตรงต่อการกำหนดจำนวนเงินและการเปิดเผยข้อมูลในงบการเงิน แต่การปฏิบัติตามกฎหมายและข้อบังคับเหล่านี้อาจเป็นพื้นฐานในการดำเนินธุรกิจ เพื่อให้กิจการสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง หรือเพื่อหลีกเลี่ยงค่าปรับที่มีสาระสำคัญ ซึ่งกฎหมายและข้อบังคับเหล่านี้บางฉบับอาจเกี่ยวข้องกับการใช้เทคโนโลยีและระบบสารสนเทศของกิจการ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ทั้งนี้ผู้สอบบัญชีจะต้องพิจารณาลักษณะทางธุรกิจของกิจการว่ากฎหมายที่กิจการต้องปฏิบัติตามนั้นรวมถึงกฎหมายของต่างประเทศด้วยหรือไม่ เช่น กิจการไทยที่มีการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในสหภาพยุโรป มีความเป็นไปได้สูงที่จะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลของสหภาพยุโรปด้วย การพิจารณาการปฏิบัติตามกฎหมายหรือข้อบังคับที่เกี่ยวข้องกับการใช้เทคโนโลยีและระบบสารสนเทศของกิจการตามที่กล่าวข้างต้น ทำให้ผู้สอบบัญชีอาจต้องมีความเข้าใจเกี่ยวกับกระบวนการด้านเทคโนโลยีสารสนเทศและการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่กิจการนำไปปฏิบัติเพื่อตอบสนองตามข้อกำหนดของกฎหมายหรือข้อบังคับที่เกี่ยวข้อง นอกจากนี้มาตรฐานการสอบบัญชี รหัส 250 (ปรับปรุง) ยังให้ตัวอย่างข้อบ่งชี้ว่ามีการไม่ปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับการใช้เทคโนโลยีและระบบสารสนเทศของกิจการ เช่น ระบบสารสนเทศที่ไม่ให้ร่องรอยการตรวจสอบที่เหมาะสม หรือไม่ให้หลักฐานที่เพียงพอไม่ว่าจะโดยจงใจหรือไม่ก็ตาม

6. ขอบเขตและวิธีการทำความเข้าใจสภาพแวดล้อมและการควบคุมของระบบสารสนเทศเพื่อการสอบบัญชี

โดยทั่วไปขั้นตอนแรกของการปฏิบัติงานสอบบัญชี คือ การวางแผนการตรวจสอบ โดยการวางแผนการตรวจสอบกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูลอาจจะต้องครอบคลุมถึงการวางแผนการตรวจสอบระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำรายงานการเงินของกิจการ โดยอาจต้องครอบคลุมถึงเรื่องอื่น ๆ ที่ได้รับผลกระทบจากการใช้ระบบสารสนเทศดังกล่าวที่เป็นสาระสำคัญต่อความถูกต้อง ครบถ้วน และน่าเชื่อถือของงบการเงินด้วย เช่น การตรวจสอบระบบสารสนเทศและกระบวนการของผู้ให้บริการด้านเทคโนโลยีสารสนเทศ การตรวจสอบการใช้ซอฟต์แวร์ที่ผิดกฎหมาย ซึ่งการระบุขอบเขตและวิธีการทำความเข้าใจสภาพแวดล้อมและการควบคุมของระบบสารสนเทศเพื่อการสอบบัญชี เป็นขั้นตอนหลักที่สำคัญของการวางแผนการตรวจสอบระบบสารสนเทศเพื่อการสอบบัญชี เพราะจะทำให้ผู้สอบบัญชีได้มาซึ่งข้อมูลและความเข้าใจเพียงพอต่อการระบุและประเมินความเสี่ยงจากการใช้ระบบสารสนเทศเพื่อการสอบบัญชี การระบุการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชี และการกำหนดวัตถุประสงค์และขอบเขตของการตรวจสอบระบบสารสนเทศเพื่อการสอบบัญชี รวมถึงงบประมาณที่คาดว่าจะใช้ในการตรวจสอบต่อไปได้

ในการทำความเข้าใจสภาพแวดล้อมและการควบคุมของระบบสารสนเทศเพื่อการสอบบัญชี ผู้สอบบัญชีต้องรวบรวมและสอบทานข้อมูล รวมทั้งบันทึกวิธีการและขั้นตอนที่ใช้ เพื่อให้ได้มาซึ่งความเข้าใจในระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำงบการเงินในเรื่องต่อไปนี้

6.1. ข้อมูลทั่วไปเกี่ยวกับกิจการและการบริหารจัดการเทคโนโลยีสารสนเทศที่กิจการใช้

- ลักษณะ ประเภทธุรกิจ รูปแบบทางธุรกิจ รูปแบบการดำเนินงานของกิจการและสภาพแวดล้อมทางธุรกิจของกิจการ ซึ่งเป็นปัจจัยหนึ่งที่กระทบต่อความซับซ้อนของระบบสารสนเทศ และความเสี่ยงสืบเนื่องด้านเทคโนโลยีสารสนเทศ เช่น ระบบสารสนเทศของกิจการในธุรกิจ ธนาคาร สื่อสารโทรคมนาคม โรงพยาบาล หรือค้าปลีก จะมีความซับซ้อนและมีความเสี่ยงสืบเนื่องด้านเทคโนโลยีสารสนเทศที่สูงกว่าของธุรกิจอื่น เช่น ค้าส่ง ผลิต โรงแรม ก่อสร้าง นอกจากนี้ กิจการที่มีรูปแบบธุรกิจและรูปแบบการดำเนินงานที่อิงการใช้เทคโนโลยีดิจิทัลสูงจะมีระบบสารสนเทศที่ซับซ้อนและมีความเสี่ยงสืบเนื่องด้านเทคโนโลยีสารสนเทศที่สูงกว่ากิจการที่มีรูปแบบธุรกิจและรูปแบบการดำเนินงานแบบดั้งเดิม
- บทบาทของเทคโนโลยีสารสนเทศและระบบสารสนเทศที่สนับสนุนวิสัยทัศน์ กลยุทธ์ และวัตถุประสงค์ของกิจการ รวมถึงบทบาท กระบวนการ และกลยุทธ์ของหน่วยงานเทคโนโลยีสารสนเทศต่อการกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสนับสนุนวิสัยทัศน์ กลยุทธ์ และวัตถุประสงค์ของกิจการ รวมถึงการจัดการเกี่ยวกับเทคโนโลยีสารสนเทศและทรัพยากรที่ได้รับการจัดสรร เช่น กิจการมีการลงทุนในสภาพแวดล้อมทางเทคโนโลยีสารสนเทศที่เหมาะสมหรือสำหรับการปรับปรุงที่จำเป็น หรือมีการว่าจ้างบุคลากรที่มีทักษะเหมาะสมอย่างเพียงพอต่อการพัฒนาและนำระบบสารสนเทศมาใช้งานอย่างมีประสิทธิผลและประสิทธิภาพ
- เทคโนโลยีและระบบสารสนเทศที่กิจการใช้เพื่อสนับสนุนกระบวนการทางธุรกิจ การดำเนินงาน และการประมวลผลข้อมูลของกิจการ หากกิจการมีการใช้เทคโนโลยี และระบบสารสนเทศสูง ความเสี่ยงสืบเนื่องด้านเทคโนโลยีสารสนเทศย่อมสูงตามไปด้วย
- ปัจจัยเสี่ยงและความเสี่ยงที่สำคัญจากการใช้เทคโนโลยีของกิจการ โดยเฉพาะความเสี่ยงที่มีผลกระทบต่อกระบวนการทางธุรกิจ การรักษาความมั่นคงปลอดภัยของข้อมูล และความครบถ้วน ความถูกต้อง ความสมเหตุสมผลและความน่าเชื่อถือของงบการเงินและหลักฐานการสอบบัญชีซึ่งอาจรวมถึงความเสี่ยงทางไซเบอร์ ความเสี่ยงจากหน่วยงานภายนอกที่มีความสัมพันธ์เป็นผู้ให้บริการ คู่ค้า หรืออื่น ๆ ตลอดถึงกลยุทธ์และกระบวนการที่กิจการใช้ในการจัดการความเสี่ยง

- ภัยคุกคาม จุดอ่อนหรือช่องโหว่และเหตุการณ์ผิดปกติที่สำคัญของระบบสารสนเทศของกิจการและสภาพแวดล้อมการควบคุมภายในของกิจการ ที่มีผลต่อความมั่นคงปลอดภัยของข้อมูล และต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผลของข้อมูลทางการค้า การบัญชี และรายงานการเงิน ที่อาจทำให้เกิดการแสดงข้อมูลในงบการเงินที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ

ผู้สอบบัญชีอาจบันทึกข้อมูลที่รวบรวมได้เกี่ยวกับข้อมูลทั่วไปนี้ในลักษณะการบรรยายความ หรือการใช้แบบฟอร์ม ดังตัวอย่างแบบฟอร์มประเมินองค์ประกอบของการควบคุมภายในกิจการและแบบฟอร์มทำความเข้าใจระดับการใช้เทคโนโลยีของกิจการที่จัดทำและเผยแพร่โดยสภาวิชาชีพบัญชี ซึ่งสามารถเข้าถึงได้ที่ สภาวิชาชีพบัญชี: มาตรฐาน (www.tfac.or.th)

6.2. ข้อมูลเกี่ยวกับระบบสารสนเทศเพื่อการสอบบัญชี

- ลักษณะและความซับซ้อนของสภาพแวดล้อมของระบบสารสนเทศ รวมทั้งกระบวนการและกิจกรรมด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับรายงานทางการเงิน โดยพิจารณาจากข้อมูลด้านเทคโนโลยีที่สำคัญ เช่น สถาปัตยกรรมของระบบสารสนเทศ ประเภทและลักษณะของฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ วิธีการในการประมวลผลของระบบสารสนเทศ จำนวนระบบสารสนเทศที่ใช้ การเชื่อมต่อระบบสารสนเทศของกิจการกับระบบเทคโนโลยีสารสนเทศอื่นที่อยู่ทั้งในและนอกกิจการ รูปแบบของการจัดเก็บข้อมูลและระบบจัดการฐานข้อมูลที่ใช้ สถาปัตยกรรมของระบบเครือข่าย จำนวนผู้ใช้งาน จำนวนบุคลากรของหน่วยงานเทคโนโลยีสารสนเทศ จำนวนรายการที่นำเข้าและประมวลผลโดยระบบสารสนเทศ ซึ่งผู้สอบบัญชีอาจบันทึกข้อมูลที่รวบรวมได้เกี่ยวกับความสำคัญและความซับซ้อนของกิจกรรมระบบสารสนเทศ และการมีอยู่ของข้อมูลที่จะนำมาใช้ในการตรวจสอบ ในลักษณะการบรรยายความ หรือการใช้แบบฟอร์ม หรือเป็นรูปภาพที่ออกแบบมาให้ง่ายต่อการทำความเข้าใจและวิเคราะห์ เช่น เป็นรูปภาพที่แสดงองค์ประกอบที่สำคัญของระบบสารสนเทศ การเชื่อมต่อของระบบสารสนเทศกับระบบอื่น เช่น ระบบงานที่ใช้สนับสนุนการดำเนินธุรกิจ ระบบของธนาคาร และการไหลของข้อมูลจากแหล่งข้อมูลเข้าต้นทาง เช่น จากมือถือของลูกค้าหรือจากเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นของผู้ใช้งานภายใน ไปจนถึงรายงานทางการเงิน
- โครงสร้างพื้นฐานของระบบสารสนเทศ (Information System Infrastructure) ที่อยู่ในขอบเขตงานเพื่อวัตถุประสงค์ของการสอบบัญชี เช่น ทรัพยากรสารสนเทศที่ใช้สถาปัตยกรรมของโครงสร้างพื้นฐานและระบบงาน เช่น ระบบสารสนเทศแบบหลายชั้นที่เป็นแบบบูรณาการ (Integrated ERP System) หรือระบบสารสนเทศแบบ SaaS รวมถึงฮาร์ดแวร์ ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน ซอฟต์แวร์ระบบจัดการฐานข้อมูล ฐานข้อมูลเครือข่าย เทคโนโลยีแบบเคลื่อนที่ และอื่น ๆ ที่กิจการใช้ทั้งที่เป็นของกิจการเองหรือของหน่วยงานภายนอกที่ให้บริการ เช่น ผู้ให้บริการด้านซอฟต์แวร์ผู้ให้บริการระบบคลาวด์ ตลอดถึงข้อดี ข้อเสีย ความเสี่ยง และประเด็นพิจารณาที่ผู้สอบบัญชีต้องให้ความสนใจ
- กระบวนการและกิจกรรมด้านเทคโนโลยีสารสนเทศที่กิจการใช้ในการจัดการ การเข้าถึงสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ การจัดการการเปลี่ยนแปลงโปรแกรมและชุดคำสั่งหรือเปลี่ยนแปลงสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ และการจัดการการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บุคลากรที่เกี่ยวข้องและทรัพยากรอื่นที่ใช้ในกระบวนการเหล่านั้น ขอบเขตของความเข้าใจของผู้สอบบัญชีเกี่ยวกับกระบวนการและกิจกรรมด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงขอบเขตของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศของกิจการ จะแตกต่างกันไปตามลักษณะและสถานการณ์ของกิจการและสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ รวมทั้งขึ้นอยู่กับลักษณะและขอบเขตของการควบคุมที่ผู้สอบบัญชีระบุไว้ ซึ่งระบบสารสนเทศที่อาจมีความเสี่ยงเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศจะแตกต่างกันไปตามปัจจัยข้างต้นด้วย เช่น

    ก. กิจการที่ใช้ซอฟต์แวร์เชิงพาณิชย์และไม่สามารถเข้าถึงรหัสโปรแกรมต้นฉบับเพื่อทำการเปลี่ยนแปลงโปรแกรมใด ๆ ได้ อาจไม่จำเป็นต้องมีกระบวนการสำหรับการเปลี่ยนแปลงโปรแกรม แต่อาจต้องมีกระบวนการหรือวิธีปฏิบัติที่ใช้ในการตั้งค่าซอฟต์แวร์เหล่านั้น เช่น การกำหนดผังบัญชี การตั้งค่าพารามิเตอร์สำหรับการผ่านรายการ การตั้งค่าพารามิเตอร์สำหรับระดับที่ยอมรับได้ในการบันทึกรายการ หรือการกำหนดลำดับชั้นของสิทธิในการเข้าถึง

    ข. กิจการที่มีระบบงานเทคโนโลยีสารสนเทศหลายระบบและกระบวนการในการจัดการสภาพแวดล้อมทางเทคโนโลยีสารสนเทศอาจมีความซับซ้อน กิจการอาจจำเป็นที่ต้องมีกระบวนการด้านเทคโนโลยีสารสนเทศที่เป็นทางการและเป็นไปตามแนวปฏิบัติที่ดี

- ผลกระทบของสภาพแวดล้อมและกิจกรรมด้านเทคโนโลยีสารสนเทศของระบบสารสนเทศที่เกี่ยวข้องกับรายงานทางการเงินต่อการประเมินความเสี่ยงสืบเนื่องและความเสี่ยงจากการควบคุมในแง่ความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของงบการเงิน โดยเน้นความเสี่ยงที่มีผลทำให้มีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ซึ่งผู้สอบบัญชีอาจบันทึกข้อมูลเกี่ยวกับผลกระทบนี้ในลักษณะการบรรยายความ หรือการใช้แบบฟอร์มที่ได้ออกแบบให้ง่ายต่อการทำความเข้าใจและวิเคราะห์
- ความมีอยู่ของข้อมูลที่ผู้สอบบัญชีต้องการใช้ในการสอบบัญชี เช่น เอกสารประกอบรายการ แฟ้มข้อมูลระบบสารสนเทศที่สามารถดาวน์โหลดออกมาเพื่อนำมาใช้งานเพื่อการสอบบัญชีได้ ร่องรอยการตรวจสอบที่มีในระบบสารสนเทศ รายงานและหลักฐานการสอบบัญชีอื่นซึ่งอาจเป็นเอกสารสนับสนุนการทำและบันทึกรายการค้าที่อาจมีการจัดเก็บในระบบสารสนเทศเท่านั้น เนื่องจากข้อมูลเหล่านี้อาจมีอยู่เฉพาะในช่วงเวลาหนึ่งก่อนที่จะถูกลบจากระบบหรือแทนค่าไป หรืออยู่ในรูปแบบที่อ่านได้ด้วยคอมพิวเตอร์เท่านั้น การที่ผู้สอบบัญชีมีความเข้าใจเกี่ยวกับข้อมูลที่มีของระบบสารสนเทศยังทำให้ผู้สอบบัญชีสามารถระบุรายงานภายในของกิจการที่สามารถนำมาใช้เพื่อช่วยในการทดสอบเนื้อหาสาระ และพิจารณาความเป็นไปได้ในการนำเอาเทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (Computer-Assisted Audit Techniques – CAAT) มาใช้เพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน หรือช่วยให้สามารถทำการตรวจสอบบางขั้นตอนกับรายการทุกรายการในบัญชีหรือประเภทรายการที่ต้องการได้แทนการตรวจสอบโดยใช้วิธีสุ่มตัวอย่าง ซึ่งช่วยผู้สอบบัญชีได้ความเชื่อมั่นในผลการตรวจสอบเพิ่มมากขึ้นแต่ใช้ทรัพยากรที่น้อยกว่า
- ประเภทของรายการในการดำเนินงานของกิจการ ยอดคงเหลือทางบัญชี และการเปิดเผยข้อมูลที่มีสาระสำคัญต่องบการเงิน และระบบสารสนเทศที่ใช้สนับสนุนการประมวลผล รวมถึงการให้ได้มาซึ่งยอดคงเหลือทางบัญชีแต่ละรายการและการเปิดเผยข้อมูลแต่ละเรื่องที่มีสาระสำคัญต่องบการเงิน รวมถึงการควบคุมโดยอัตโนมัติที่ทำโดยระบบสารสนเทศ หรือการควบคุมที่ปฏิบัติด้วยมือที่อิงข้อมูลจากระบบสารสนเทศสำหรับรายการแต่ละประเภท ยอดคงเหลือทางบัญชี และการเปิดเผยข้อมูลที่มีสาระสำคัญต่องบการเงิน ที่กิจการกำหนดไว้เป็นการควบคุมหลัก ในกรณีที่ผู้สอบบัญชีต้องการพึ่งพิงการควบคุมดังกล่าวในการปฏิบัติงาน โดยเฉพาะในกรณีที่การควบคุมที่ตอบสนองต่อความเสี่ยงที่วิธีการตรวจสอบเนื้อหาสาระเพียงอย่างเดียวไม่สามารถให้หลักฐานการสอบบัญชีที่เหมาะสมอย่างเพียงพอ ผู้สอบบัญชีควรต้องรวมระบบสารสนเทศนั้นในขอบเขตการตรวจสอบระบบสารสนเทศ อย่างไรก็ดีในบางกรณีผู้สอบบัญชีอาจไม่ได้วางแผนที่จะพึ่งพิงการควบคุมสำหรับรายงานหรือหลักฐานการสอบบัญชีที่จัดทำโดยระบบสารสนเทศและวางแผนที่จะทดสอบข้อมูลนำเข้าและข้อมูลผลลัพธ์ของรายงานหรือหลักฐานการสอบบัญชีดังกล่าวโดยตรงแทน ผู้สอบบัญชีอาจไม่รวมระบบสารสนเทศที่เกี่ยวข้องในขอบเขตการตรวจสอบระบบสารสนเทศ ดังนั้นความเข้าใจในเรื่องนี้จึงสำคัญมากต่อการกำหนดขอบเขตของระบบสารสนเทศที่ควรจะต้องครอบคลุมในการตรวจสอบระบบสารสนเทศของผู้สอบบัญชี
- ขอบเขตการใช้ระบบสารสนเทศของกิจการในส่วนที่เกี่ยวกับการทำให้เกิดรายการการบันทึกข้อมูลและรายการบัญชี การประมวลผลและการแก้ไขรายการในกรณีที่จำเป็น การผ่านรายการไปยังสมุดบัญชีแยกประเภท และการจัดทำรายงานทางการเงิน รวมถึงวิธีการที่ระบบสารสนเทศใช้ในการรวบรวมข้อมูล เหตุการณ์และเงื่อนไข นอกเหนือจากรายการต่าง ๆ ที่มีสาระสำคัญต่องบการเงิน

6.3. ข้อมูลเกี่ยวกับกิจกรรมการควบคุมของระบบสารสนเทศเพื่อการสอบบัญชี

องค์ประกอบของสภาพแวดล้อมการควบคุมของกิจการที่เกี่ยวข้องกับระบบสารสนเทศที่ต้องครอบคลุมเพื่อการสอบบัญชี ประกอบด้วยการควบคุมด้านเทคโนโลยีสารสนเทศในระดับกิจการ (IT Entity-Level Controls) การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ (IT General Controls) และการควบคุมระบบงาน (Application Controls) ไม่ว่าจะอยู่ในรูปของการควบคุมที่ปฏิบัติด้วยมือ (Manual Controls) การควบคุมด้วยระบบงานเทคโนโลยีสารสนเทศหรือการควบคุมโดยอัตโนมัติ (IT Application Controls หรือ Automated Controls) หรือการควบคุมที่ปฏิบัติด้วยมือที่อิงเทคโนโลยีสารสนเทศ (IT-Dependent Manual Controls) ทั้งที่เป็นการควบคุมเชิงป้องกัน เชิงค้นหา และเชิงแก้ไข ในส่วนของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศจะเน้นถึงความเข้าใจในเรื่องการควบคุมในการคัดเลือก การพัฒนา และการนำไปใช้ของระบบสารสนเทศใหม่ การควบคุมการเข้าถึงทั้งเชิงตรรกะและกายภาพ (Logical and Physical Access Controls) เช่น การให้สิทธิตามบทบาทหน้าที่และการแบ่งแยกหน้าที่ การควบคุมเพื่อปกป้องข้อมูลที่อ่อนไหวและสำคัญ การควบคุมเพื่อตอบสนองต่อเหตุการณ์ที่ก่อให้เกิดความเสี่ยงสูง ทั้งนี้การทำความเข้าใจความเสี่ยงที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศและการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่นำไปปฏิบัติโดยกิจการเพื่อตอบสนองต่อความเสี่ยงเหล่านั้น อาจส่งผลต่อการกลยุทธ์และวิธีการของผู้สอบบัญชีในการตรวจสอบ เช่น

- การตรวจสอบโดยพึ่งพิงการควบคุมระบบงานที่เป็นการควบคุมโดยอัตโนมัติ และการควบคุมที่ปฏิบัติด้วยมือที่อิงข้อมูลจากระบบสารสนเทศ และทดสอบความมีประสิทธิผลของการปฏิบัติตามการควบคุมทั่วไปของเทคโนโลยีสารสนเทศและการควบคุมระบบงาน เพื่อตอบสนองต่อความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในระดับที่เกี่ยวกับสิ่งที่ผู้บริหารได้ให้การรับรองไว้ หรือการตรวจสอบโดยไม่พึ่งพิงการควบคุมระบบงานที่เป็นการควบคุมโดยอัตโนมัติและการควบคุมที่ปฏิบัติด้วยมือที่อิงข้อมูลจากระบบสารสนเทศและไม่ทดสอบความมีประสิทธิผลของการออกแบบและการปฏิบัติตามการควบคุมทั่วไปของเทคโนโลยีสารสนเทศและการควบคุมระบบงาน
- การทดสอบข้อมูลที่ประมวลผลหรือจัดทำโดยระบบสารสนเทศที่กิจการใช้ หรือจัดทำจากการใช้ข้อมูลจากระบบสารสนเทศดังกล่าว ที่ผู้สอบบัญชีจะนำมาใช้เป็นหลักฐานการสอบบัญชี ผู้สอบบัญชีอาจพิจารณาทดสอบการควบคุมโดยอัตโนมัติสำหรับหลักฐานการสอบบัญชีนั้น รวมถึงการระบุและการทดสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ตอบสนองต่อความเสี่ยงที่เกิดจากการเปลี่ยนแปลงโปรแกรมและชุดคำสั่ง หรือการเปลี่ยนแปลงข้อมูลโดยตรงในรายงานอย่างไม่เหมาะสมหรือไม่ได้รับอนุญาต
- การออกแบบวิธีการตรวจสอบเพิ่มเติมในกรณีที่ผู้สอบบัญชีพบจากการประเมินประสิทธิผลการออกแบบหรือการปฏิบัติตามการควบคุมทั่วไปของเทคโนโลยีสารสนเทศว่ามีการควบคุมในบางเรื่องหรือในบางระบบไม่มีประสิทธิผล ผู้สอบบัญชีอาจพิจารณาทดสอบประสิทธิผลของการควบคุมอื่นที่สามารถช่วยลดความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศต่อการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในระดับที่เกี่ยวกับสิ่งที่ผู้บริหารได้ให้การรับรองไว้ หรือรวบรวมและสอบทานข้อมูลเพิ่มเติมว่ามีสถานการณ์หรือเงื่อนไขใดของกิจการที่ทำให้การควบคุมที่ไม่มีประสิทธิผลนี้ ไม่ก่อให้เกิดความเสี่ยงดังกล่าว หรือในกรณีที่ผู้สอบบัญชีตัดสินใจที่จะไม่ทดสอบความมีประสิทธิผลของการปฏิบัติตามการควบคุมทั่วไปของเทคโนโลยีสารสนเทศหรือคาดการณ์ว่าการควบคุมทั่วไปของเทคโนโลยีสารสนเทศไม่มีประสิทธิผลในทุกเรื่องและทุกระบบ โดยผู้สอบบัญชีต้องพิจารณาถึงความเป็นไปได้ที่จะเกิดความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศต่อการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในระดับที่เกี่ยวกับสิ่งที่ผู้บริหารได้ให้การรับรองไว้ และออกแบบวิธีการตรวจสอบเนื้อหาสาระให้ตอบสนองต่อความเสี่ยงที่อาจเกิดขึ้นนี้ อย่างไรก็ตาม ในกรณีที่ความเสี่ยงดังกล่าวเป็นความเสี่ยงที่วิธีการตรวจสอบเนื้อหาสาระเพียงอย่างเดียวไม่สามารถให้หลักฐานการสอบบัญชีที่เหมาะสมอย่างเพียงพอ ผู้สอบบัญชีอาจพิจารณาถึงผลกระทบต่อการแสดงความเห็นของผู้สอบบัญชี

6.4. ข้อมูลเกี่ยวกับลักษณะของข้อมูลหรือสารสนเทศที่เกี่ยวข้อง

ผู้สอบบัญชีต้องมีความเข้าใจถึงลักษณะของข้อมูลหรือสารสนเทศที่เกี่ยวข้องกับรายการ เหตุการณ์และเงื่อนไขอื่น ๆ ที่ต้องประมวลผล และวิธีการที่ข้อมูลเดินทางผ่านระบบสารสนเทศของกิจการ สำหรับประเภทของรายการ ยอดคงเหลือทางบัญชี และการเปิดเผยข้อมูลที่มีนัยสำคัญ ตั้งแต่ที่มาของรายการค้าและข้อมูลเกี่ยวกับเหตุการณ์และเงื่อนไขต่าง ๆ (นอกเหนือจากรายการค้า) การจับข้อมูลของรายการค้า การบันทึก การจัดเก็บข้อมูล การประมวลผลข้อมูล การแก้ไขข้อมูล (ในกรณีที่จำเป็น) การผ่านรายการไปยังบัญชีแยกประเภท ไปจนถึงการจัดทำรายงานทางการเงินและการเปิดเผยข้อมูลในงบการเงิน

6.5. การควบคุมระบบงานที่สำคัญ

การควบคุมระบบงานที่สำคัญที่มีอยู่ในทางเดินของรายการค้า (Business Transaction Flow) ของกิจการ ซึ่งครอบคลุมตั้งแต่การนำข้อมูลเข้า (Input) การจัดเก็บข้อมูล (Storage) การประมวลผล (Processing) และการแสดงผลลัพธ์ (Output) สำหรับกระบวนการธุรกิจที่สำคัญ (Significant Business Processes) ของกิจการ ตลอดถึงผลกระทบของการควบคุมเหล่านั้นต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผลของข้อมูลและความน่าเชื่อถือของงบการเงินของกิจการ

6.6. การใช้หน่วยงานภายนอกในการให้บริการ

ผู้สอบบัญชีต้องมีความเข้าใจถึงการใช้หน่วยงานภายนอกในการให้บริการ ซึ่งครอบคลุมถึงวัตถุประสงค์และความสำคัญของการใช้หน่วยงานภายนอกในการให้บริการ ระยะเวลาและเงื่อนไขในการให้บริการ การควบคุมส่วนเสริมของกิจการ (Complementary User Entity Controls) ที่เกี่ยวข้อง รายงานการประเมินการควบคุมของหน่วยงานภายนอกในการให้บริการในการสอบบัญชีของกิจการ เช่น ประเภทของรายงาน ระยะเวลาที่ครอบคลุม ส่วนของระบบสารสนเทศที่ครอบคลุม ตลอดถึงผลกระทบจากการใช้รายงานการประเมินการควบคุมของหน่วยงานภายนอกที่ให้บริการแก่กิจการเพื่อการตรวจสอบงบการเงินของกิจการ เช่น รายงานของผู้สอบบัญชีขององค์กรที่ให้บริการประเภท 1 ซึ่งเป็นรายงานที่เกี่ยวกับคำอธิบาย และการออกแบบการควบคุม ณ องค์กรที่ให้บริการ หรือรายงานของผู้สอบบัญชีขององค์กรที่ให้บริการประเภท 2 ซึ่งเป็นรายงานเกี่ยวกับคำอธิบาย การออกแบบการควบคุม และความมีประสิทธิผลของการปฏิบัติตามการควบคุม ณ องค์กรที่ให้บริการ

6.7. งานการตรวจสอบภายในหรืองานของผู้เชี่ยวชาญอื่น

กิจการอาจจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบภายในหรือผู้เชี่ยวชาญอื่น หรือกิจการอาจได้รับการตรวจสอบดังกล่าวโดยหน่วยงานกำกับดูแลที่เกี่ยวข้อง เช่น ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ หรือคู่ค้า หรือหน่วยรับรองระบบมาตรฐานที่ได้รับการรับรอง (Accredited Certification Body) เช่น หน่วยงานรับรองมาตรฐานการจัดการการรักษาความมั่นคงปลอดภัยของสารสนเทศ - ISO 27001 ผู้สอบบัญชีจึงควรมีความเข้าใจถึงการตรวจสอบด้านเทคโนโลยีสารสนเทศของกิจการ รวมถึงประเด็นที่พบจากการตรวจสอบ และการจัดการประเด็นที่พบเหล่านั้นของกิจการ ในส่วนที่มีผลกระทบต่อการสอบบัญชี ทั้งนี้ผู้สอบบัญชีอาจพิจารณานำผลงานการตรวจสอบเหล่านั้นมาใช้ประกอบกับการสอบบัญชีด้วย

วิธีการที่ผู้สอบบัญชีใช้เพื่อให้มีความเข้าใจเกี่ยวกับสภาพแวดล้อมและการควบคุมของระบบสารสนเทศมีหลายวิธี เช่น

- การสอบถามบุคลากรที่เกี่ยวข้องกับวิธีปฏิบัติที่ใช้ในกระบวนการทางธุรกิจและกระบวนการด้านเทคโนโลยีสารสนเทศของกิจการ รวมถึงปัจจัยเสี่ยงและความเสี่ยงที่สำคัญ การควบคุมที่เกี่ยวข้อง การเปลี่ยนแปลงที่เกี่ยวกับระบบสารสนเทศที่สำคัญ และเหตุการณ์ผิดปกติที่มีสาระสำคัญ
- การสอบทานนโยบาย ระเบียบปฏิบัติ คู่มือปฏิบัติงาน หรือเอกสารอื่น ๆ ของระบบสารสนเทศของกิจการ
- การสังเกตการณ์การปฏิบัติตามนโยบายหรือระเบียบปฏิบัติของบุคลากรของกิจการ
- การเลือกรายการและติดตามรายการเหล่านั้นผ่านกระบวนการต่าง ๆ ที่เกี่ยวข้องในระบบสารสนเทศ
- การใช้เครื่องมือและเทคนิคอัตโนมัติในการรวบรวมวิเคราะห์หรือตรวจสอบข้อมูลเพื่อยืนยันความเข้าใจเกี่ยวกับสภาพแวดล้อมและการควบคุมของระบบสารสนเทศของกิจการ

ตัวอย่างของข้อมูลที่ควรจัดเก็บเพื่อให้ผู้สอบบัญชีมีความเข้าใจเกี่ยวกับสภาพแวดล้อมและการควบคุมของระบบสารสนเทศของกิจการที่ดีขึ้นเพื่อให้สามารถวางแผนการตรวจสอบอย่างมีประสิทธิผลและประสิทธิภาพ ได้แก่

1. รายละเอียดเกี่ยวกับระบบฐานข้อมูลของกิจการ เช่น ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในการจัดการฐานข้อมูล
2. รายละเอียดและผังระบบโครงข่ายและการเชื่อมต่อ (Network & Communication Diagram) ซึ่งระบุถึงการเชื่อมต่อกับ Internet ด้วย (ถ้ามี)
3. การเปลี่ยนแปลงที่สำคัญเพิ่งเกิดขึ้นหรือที่คาดว่าจะดำเนินการที่เกี่ยวข้องกับระบบสารสนเทศของกิจการ
4. รายละเอียดเกี่ยวกับจำนวนผู้ใช้ จำนวนเจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ
5. รายละเอียดเกี่ยวกับวิธีการที่ใช้ในการนำเข้าข้อมูลและการประมวลผล เช่น ใช้การประมวลผลแบบรวมกลุ่ม (Batch Processing) หรือแบบเชื่อมตรงทันที (Online, Real-time Processing) และความซับซ้อนของการประมวลผลและจำนวนรายการที่เกี่ยวข้อง
6. นโยบายและขั้นตอนในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกิจการ เช่น นโยบายในการรักษาความลับข้อมูลของกิจการ นโยบายในการใช้ทรัพยากรสารสนเทศของกิจการ ขั้นตอนในการขอเข้าถึงระบบ ขั้นตอนในการขอเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลง แก้ไขหรือพัฒนาระบบ และขั้นตอนในการสอบทานผู้ใช้และสิทธิในการเข้าถึง ขั้นตอนในการสำรองข้อมูลและฟื้นฟูระบบ
7. มาตรการและวิธีการในการสอบทานเหตุการณ์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัย (Security Events Review)
8. มาตรฐานในการพิสูจน์ตัวตน (Authentication) และการกำหนดและจัดการรหัสผู้ใช้งานและรหัสผ่าน
9. วิธีการกำหนดสิทธิในการเข้าถึง (Access Authorization)
10. มาตรการและวิธีการในการรักษาความมั่นคงปลอดภัยด้านกายภาพของศูนย์คอมพิวเตอร์
11. รายละเอียดเกี่ยวกับเอกสารประกอบระบบสารสนเทศที่มี

7. การระบุและประเมินความเสี่ยงจากการใช้ระบบสารสนเทศเพื่อการสอบบัญชี

ความเสี่ยงจากการใช้ระบบสารสนเทศเพื่อการสอบบัญชี หมายถึง ความเสี่ยงที่มีผลต่อบูรณภาพ (Integrity) หรือ ความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของรายการ ข้อมูลและสารสนเทศทางการเงินที่นำเข้า ประมวลผล จัดเก็บ และแสดงผลโดยระบบสารสนเทศ ซึ่งผู้สอบบัญชีต้องมีความเข้าใจเกี่ยวกับลักษณะและสภาพแวดล้อมทางธุรกิจ กระบวนการทางธุรกิจ และสภาพแวดล้อมของระบบสารสนเทศที่กิจการใช้ เพื่อให้สามารถที่จะระบุและประเมินความเสี่ยงจากการใช้ระบบสารสนเทศดังต่อไปนี้

1. ความเสี่ยงสืบเนื่อง (Inherent Risk) คือ ความเป็นไปได้ของการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญอันเนื่องจากลักษณะเฉพาะของประเภทของรายการยอดคงเหลือทางบัญชี หรือ การเปิดเผยข้อมูล ซึ่งในการประเมินความเสี่ยงสืบเนื่องนี้ผู้สอบบัญชีจะต้องระบุโอกาสที่จะเกิดเหตุการณ์กับรายการค้า ข้อมูลและสารสนเทศทางการเงินที่นำเข้า ประมวลผล จัดเก็บและแสดงผลโดยระบบสารสนเทศ ที่มีผลทำให้เกิดหรือมีข้อผิดพลาดในยอดคงเหลือ หรือรายการค้าประเภทหนึ่ง ๆ ซึ่งเมื่อรวมพิจารณากับข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทอื่นแล้ว มีสาระสำคัญต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผลและความน่าเชื่อถือของงบการเงิน หากไม่มีการควบคุมภายใน หรือยังไม่พิจารณาถึงการควบคุมที่กิจการกำหนดไว้เลย
2. ความเสี่ยงในการควบคุม (Control Risk) คือ ความเป็นไปได้หรือโอกาสที่จะเกิดเหตุการณ์กับรายการ ข้อมูลและสารสนเทศทางการเงินที่นำเข้า ประมวลผล จัดเก็บ และแสดงผลโดยระบบสารสนเทศ ที่มีผลทำให้เกิดหรือมีข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทหนึ่ง ๆ ซึ่งเมื่อรวมพิจารณากับข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทอื่นแล้วมีสาระสำคัญต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผลและความน่าเชื่อถือของงบการเงิน แม้ว่ากิจการจะมีการกำหนดและให้ถือปฏิบัติตามการควบคุมแล้ว หรือเมื่อพิจารณาถึงการควบคุมที่กิจการกำหนดไว้และถือปฏิบัติแล้ว ทั้งนี้ความเสี่ยงจากการควบคุมอาจเกิดจากการควบคุมที่ออกแบบไว้ไม่มีประสิทธิผล หรือการนำการควบคุมที่ออกแบบไว้ไปปฏิบัติไม่มีประสิทธิผล หรือการละเลยที่จะปฏิบัติตามการควบคุมที่ออกแบบไว้
3. ความเสี่ยงในการตรวจพบ (Detection Risk) คือ ความเป็นไปได้หรือโอกาสที่ผู้สอบบัญชีจะตรวจไม่พบประเด็นจุดอ่อนของการควบคุมที่สำคัญ การไม่ปฏิบัติตามการควบคุมที่ออกแบบไว้ที่สำคัญ และข้อผิดพลาดหรือความผิดปกติของข้อมูลและสารสนเทศทางการเงินที่นำเข้า ประมวลผล จัดเก็บ และแสดงผลโดยระบบสารสนเทศที่สำคัญ

ความเสี่ยงทั้งสามประเภทข้างต้นเป็นองค์ประกอบของความเสี่ยงในการตรวจสอบ (Audit Risk) ซึ่งหมายถึงความเป็นไปได้หรือโอกาสที่ผู้สอบบัญชีจะสรุปผลจากการตรวจสอบว่ากิจการไม่มีประเด็นจุดอ่อนของการควบคุมที่สำคัญ การไม่ปฏิบัติตามการควบคุมที่ออกแบบไว้ที่สำคัญ หรือข้อผิดพลาดหรือความผิดปกติของข้อมูลและสารสนเทศทางการเงินที่นำเข้า ประมวลผล จัดเก็บ และแสดงผลโดยระบบสารสนเทศที่มีผลทำให้เกิดหรือมีข้อผิดพลาดในยอดคงเหลือ หรือรายการประเภทหนึ่ง ๆ ซึ่งเมื่อพิจารณารวมกับข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทอื่นแล้วมีสาระสำคัญต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผลและความน่าเชื่อถือของงบการเงิน ทั้งที่ตามความเป็นจริงแล้วมีประเด็นจุดอ่อนของการควบคุมที่สำคัญ การไม่ปฏิบัติตามการควบคุมที่ออกแบบไว้ที่สำคัญ หรือข้อผิดพลาดหรือความผิดปกติของข้อมูลและสารสนเทศทางการเงินที่นำเข้า ประมวลผล จัดเก็บ และแสดงผลโดยระบบสารสนเทศที่มีผลทำให้เกิดหรือมีข้อผิดพลาดในยอดคงเหลือ หรือรายการประเภทหนึ่ง ๆ ซึ่งเมื่อพิจารณารวมกับข้อผิดพลาดในยอดคงเหลือหรือรายการประเภทอื่นแล้วที่มีสาระสำคัญต่อความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของงบการเงิน โดยความเสี่ยงในการตรวจสอบ มีความสัมพันธ์กับองค์ประกอบความเสี่ยงแต่ละประเภท ดังนี้

Audit Risk = Inherent Risk x Control Risk x Detection Risk

การที่ผู้สอบบัญชีจะลดความเสี่ยงในการที่จะแสดงความเห็นต่องบการเงินของกิจการผิดพลาดอย่างมีสาระสำคัญ ผู้สอบบัญชีต้องประเมินระดับของ Inherent Risk และ Control Risk ประกอบกับการวางแผนการสอบบัญชีตามที่จำเป็นเพื่อให้ Detection Risk อยู่ในระดับที่ต้องการ ซึ่งเมื่อพิจารณาแล้วจะเห็นว่าผู้สอบบัญชีไม่สามารถควบคุมระดับของ Inherent Risk และ Control Risk ได้ แต่ผู้สอบบัญชีสามารถควบคุมระดับของ Detection Risk ให้อยู่ในระดับที่ต้องการได้ เนื่องจากระดับของ Detection Risk มีความสัมพันธ์โดยตรงกับกลยุทธ์และแนวทางในการตรวจสอบ รวมถึงขอบเขตและวิธีการในตรวจสอบและการทดสอบรายการของผู้สอบบัญชี

การระบุและประเมินความเสี่ยงจากการใช้ระบบสารสนเทศเพื่อการสอบบัญชี มีวัตถุประสงค์เพื่อให้ผู้สอบบัญชีสามารถกำหนดแผนการตรวจสอบและขอบเขตการทดสอบรายการที่เหมาะสมเพียงพอในการแสดงความเห็นต่องบการเงิน ซึ่งการระบุและประเมินความเสี่ยงดังกล่าวจะเกี่ยวข้องโดยตรงกับการประเมินประสิทธิผลของการควบคุมของระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำรายงานทางการเงินของกิจการ ในการป้องกันหรือค้นพบข้อผิดพลาดที่มีสาระสำคัญในรายงานทางการเงิน โดยเฉพาะในเรื่องของความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของงบการเงินและการเปิดเผยข้อมูล

ผู้สอบบัญชีประเมินความเสี่ยงที่กิจการใช้ระบบสารสนเทศประมวลผลข้อมูลและรายการค้าและจัดทำรายงานทางการเงินโดยการระบุปัจจัยเสี่ยงและเหตุการณ์ที่จะทำให้มีการแสดงข้อมูลทางการเงินที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญที่เกิดจากการใช้ระบบสารสนเทศนั้น โอกาสที่จะเกิดเหตุการณ์นั้น ๆ และระดับของผลกระทบของเหตุการณ์ดังกล่าว โดยทั่วไปปัจจัยที่มีผลกระทบต่อระดับความเสี่ยง ได้แก่ คุณภาพของบุคลากร ลักษณะกิจกรรมและการใช้ระบบสารสนเทศของกิจการ และสภาพแวดล้อมและลักษณะของระบบสารสนเทศและการควบคุมขององค์กร

1. คุณภาพของบุคลากร ได้แก่ ระดับการศึกษา ทักษะ ความสามารถ ทัศนคติในการทำงานและความซื่อสัตย์
2. ลักษณะกิจกรรมและการใช้ระบบสารสนเทศของกิจการ ได้แก่ ประเภทธุรกิจของกิจการ ลักษณะและปริมาณของกิจกรรมที่ต้องปฏิบัติ ความถี่ของการเกิดรายการ ขนาดของรายการ วิธีการปฏิบัติภายในองค์กร วัฒนธรรมและลักษณะขององค์กร ความซับซ้อนของรายการค้าและวิธีการบัญชีที่ถือปฏิบัติ ลักษณะความซับซ้อนของระบบสารสนเทศ และระบบข้อมูล เช่น
   - รายการหรือเหตุการณ์ที่เกิดขึ้นบ่อยย่อมมีความเสี่ยงที่จะเกิดข้อผิดพลาดหรือรายการผิดปกติสูงกว่ารายการหรือเหตุการณ์ที่เกิดขึ้นไม่บ่อย เช่น กิจการค้าปลีกที่มีรายการขายจำนวนมาก ย่อมมีความเสี่ยงที่ข้อมูลรายการขายจะมีข้อผิดพลาดสูงกว่ากิจการที่มีรายการขายจำนวนน้อย หากข้อมูลส่วนลดราคาสินค้าในแฟ้มข้อมูลหลักไม่ถูกต้อง หรือระบบสารสนเทศคำนวณส่วนลดสำหรับสมาชิกไม่ถูกต้อง
   - ระดับความเสี่ยงจะยิ่งสูงหากการสูญเสียที่อาจเกิดขึ้นเกี่ยวข้องกับรายการที่มีมูลค่าเป็นจำนวนเงินมาก เช่น ธุรกิจอสังหาริมทรัพย์ ธุรกิจจำหน่ายรถยนต์ หรือโรงพยาบาลเอกชน จะมีรายการขายหรือให้บริการที่มีมูลค่าสูงและองค์ประกอบของรายการขายแต่ละรายการที่ซับซ้อน หากกิจการใช้ระบบสารสนเทศในการประมวลผลและจัดทำเอกสารการขาย โดยข้อมูลที่ต้องใช้ในการประมวลผลไม่ถูกต้อง หรือตรรกะของโปรแกรมและชุดคำสั่งที่ใช้ในการประมวลผลไม่ถูกต้อง ระดับความเสียหายที่เกิดขึ้นอาจจะสูงตามไปด้วย
3. สภาพแวดล้อมและลักษณะของการควบคุมขององค์กร ได้แก่ บรรยากาศในการควบคุมภายในของกิจการ ซึ่งเป็นผลมาจากทัศนคติของผู้บริหารและพนักงานที่มีต่อการควบคุมภายในมาตรการการควบคุมภายในที่มี และมาตรการที่ใช้เมื่อไม่มีการปฏิบัติตามมาตรการการควบคุมภายในที่กำหนดไว้

7.1. ความเสี่ยงที่เกิดจากการใช้ระบบสารสนเทศต่อการจัดทำรายงานทางการเงิน

ในการตรวจสอบกิจการที่ใช้ระบบสารสนเทศประมวลผลข้อมูล ผู้สอบบัญชีจำเป็นต้องสามารถระบุความเสี่ยงที่สำคัญของระบบได้ ซึ่งโดยทั่วไปความเสี่ยงของกิจการ ซึ่งรวมถึงความเสี่ยงจากการใช้ระบบสารสนเทศ มักเกิดจากปัจจัยเสี่ยง ดังนี้

1. ความเสี่ยงจากการทำข้อผิดพลาดที่ไม่ตั้งใจ

ข้อผิดพลาดอาจปรากฏในข้อมูลเข้าเนื่องจากพนักงานขาดความรู้ เหนื่อยล้า เลินเล่อ หรือขาดการควบคุมดูแลจากผู้บังคับบัญชาหรือขาดการควบคุมระบบงานที่เพียงพอ ทำให้มีการนำข้อมูลเข้าที่ไม่ถูกต้องเข้าสู่ระบบ ซึ่งข้อผิดพลาดเช่นนี้มักจะเกิดขึ้นในลักษณะสุ่ม (Random) และเกิดขึ้นเป็นครั้งคราว เช่น การนำข้อมูลเข้าที่ผิดพลาดเนื่องจากการเลือกหรือพิมพ์รหัสรายการผิดพลาดโดยไม่ตั้งใจของพนักงานขาย นอกจากนี้ข้อผิดพลาดอาจเกิดขึ้นในช่วงของการประมวลผลของระบบเนื่องจากโปรแกรมที่ใช้ในการประมวลผลมีเงื่อนไขในการประมวลผลที่ไม่ถูกต้อง เนื่องจากผู้พัฒนาโปรแกรมขาดความรู้และความเข้าใจเกี่ยวกับความต้องการของผู้ใช้อย่างเพียงพอและผู้ใช้งานไม่ได้ทดสอบโปรแกรมอย่างรอบคอบก่อนใช้งานจริง ทำให้ผลลัพธ์ (Outputs) ที่ได้จากการประมวลผลไม่ถูกต้องทุกครั้งที่ระบบใช้โปรแกรมนี้ในการประมวลผล

2. ความเสี่ยงจากการทำข้อผิดพลาดที่ตั้งใจ

ความเสี่ยงจากการทำข้อผิดพลาดที่ตั้งใจเกิดจากความตั้งใจของพนักงานของกิจการหรือบุคคลภายนอกที่จะทำรายการที่ผิดพลาด ทำการทุจริต หรือทำการฉ้อฉลเพื่อผลประโยชน์ส่วนตัว หรือเหตุผลอื่น เช่น พนักงานรับเงินอาจไม่บันทึกรายการรับเงินเข้าระบบแล้วนำเงินที่ได้รับจากลูกค้าไปใช้ส่วนตัว หรือผู้บริหารอาจสั่งการให้มีการจัดประเภทรายการที่ไม่ถูกต้อง เพื่อให้งบการเงินแสดงยอดกำไรที่สูงไป เจ้าหน้าที่ของหน่วยงานที่ให้บริการด้านเทคโนโลยีสนเทศจากภายนอกอาจลักลอบเข้าระบบสารสนเทศของกิจการเพื่อเปลี่ยนแปลงข้อมูลในระบบ เช่น เปลี่ยนเลขที่บัญชีธนาคารของผู้ขายเป็นเลขที่บัญชีธนาคารของตน

3. ความเสี่ยงจากการสูญหายหรือสูญเสียสินทรัพย์ที่ไม่ตั้งใจ

สินทรัพย์อาจจะสูญหายหรือถูกจัดเก็บผิดที่โดยไม่ตั้งใจ เช่น อุปกรณ์ระบบสารสนเทศอาจถูกจัดเก็บไว้ผิดที่ทำให้หาไม่พบเมื่อต้องการใช้หรือจัดเก็บในสถานที่ที่ไม่เหมาะสมทำให้เสื่อมสภาพ ไม่สามารถทำงานได้อย่างน่าเชื่อถือ หรือข้อมูลที่จัดเก็บในสื่ออาจถูกลบทิ้งไปโดยไม่ตั้งใจในระหว่างที่พนักงานปฏิบัติการใช้เทปแม่เหล็กที่มีข้อมูลอยู่แล้วในการทำข้อมูลสำรองชุดใหม่

4. ความเสี่ยงจากการขโมยสินทรัพย์

สินทรัพย์ของกิจการอาจถูกขโมยโดยบุคคลภายนอกหรือภายในของกิจการ เช่น บุคคลภายนอกอาจลักลอบหรือบุกรุกเข้ามาในสำนักงานหรือศูนย์คอมพิวเตอร์แล้วขโมยเครื่องหรืออุปกรณ์คอมพิวเตอร์ไป พนักงานอาจนำเครื่องหรืออุปกรณ์คอมพิวเตอร์หรือซอฟต์แวร์ของกิจการไปใช้เพื่อประโยชน์ส่วนตัว พนักงานอาจทำสำเนาข้อมูลทางการค้าที่สำคัญโดยไม่ได้รับอนุมัติแล้วนำสำเนาดังกล่าวไปให้กับคู่แข่งขันของกิจการ หรือเข้าถึงข้อมูลของลูกค้าของกิจการ เช่น ข้อมูลบัตรประชาชน ข้อมูลบัตรเครดิต บัญชีธนาคาร และนำข้อมูลไปใช้ประโยชน์ในทางมิชอบ การขโมยสินทรัพย์โดยพนักงานหรือบุคคลภายนอกในบางกรณีจะเกิดควบคู่กับการทำข้อผิดพลาดโดยตั้งใจ เช่น การยักยอกเงินโดยพนักงานรับเงินจะเกิดควบคู่กับการไม่บันทึกรายการรับเงินเข้าระบบ

5. ความเสี่ยงจากการฝ่าฝืนการรักษาความมั่นคงความปลอดภัยและภัยคุกคามทางไซเบอร์

การฝ่าฝืนการรักษาความมั่นคงความปลอดภัยและภัยคุกคามทางไซเบอร์ อาจทำให้บุคคลที่ไม่ได้รับอนุมัติสามารถเปลี่ยนแปลงแก้ไขหรือทำลายข้อมูลในระบบสารสนเทศ หรือเข้าถึงรายงานที่สำคัญของกิจการ หรือเปลี่ยนแปลงแก้ไขโปรแกรมหรือชุดคำสั่งของระบบสารสนเทศทำให้การประมวลผลข้อมูลเกิดข้อผิดพลาด เช่น พนักงานที่ไม่ได้รับอนุมัติอาจเข้าถึงข้อมูลเงินเดือนของผู้อื่นโดยใช้รหัสผู้ใช้และรหัสผ่านของพนักงานเงินเดือน บุคคลภายนอกหรือแฮ็คเกอร์อาจเข้าถึงระบบผ่านทางอินเทอร์เน็ตแล้วขโมยข้อมูลที่เป็นความลับของกิจการไปหรือทำให้กิจการไม่สามารถเปิดแฟ้มข้อมูลที่สำคัญได้

6. ความเสี่ยงจากภัยธรรมชาติหรือเหตุการณ์ที่รุนแรง

เหตุการณ์ที่รุนแรงที่ทำให้สูญเสียสินทรัพย์อาจทำโดยบุคคลภายนอกหรือภายใน เช่น การจลาจล การที่พนักงานหรืออดีตพนักงานที่มีปัญหากับกิจการนำโปรแกรมไปไว้ในระบบสารสนเทศเพื่อลบข้อมูลทั้งหมดเมื่อเงื่อนไขที่กำหนดไว้ในโปรแกรมเป็นจริง แต่ถ้าเงื่อนไขที่กำหนดไว้ในโปรแกรมยังไม่เป็นจริงโปรแกรมดังกล่าวก็จะยังไม่ทำงาน นอกจากนี้เหตุการณ์ที่รุนแรงที่อาจทำให้สูญเสียสินทรัพย์หรือทรัพยากรด้านเทคโนโลยีสารสนเทศ รวมถึงข้อมูลของระบบสารสนเทศ อาจเกิดจากสาเหตุที่ไม่เกี่ยวข้องกับคนหรือเป็นภัยธรรมชาติ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือพายุ

ทั้งนี้โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยงจากการใช้ระบบสารสนเทศ อันเนื่องจากแต่ละปัจจัยเสี่ยงนั้นขึ้นอยู่กับระดับของความเสี่ยงสืบเนื่องของระบบสารสนเทศ และประสิทธิผลของการควบคุมของระบบสารสนเทศของกิจการในการป้องกันค้นพบ และแก้ไขข้อผิดพลาดหรือรายการผิดปกติที่เกิดขึ้นกับข้อมูลและสารสนเทศทางการเงินที่นำเข้า ประมวลผล จัดเก็บ และแสดงผลโดยระบบสารสนเทศของกิจการ

7.2. ผลกระทบจากการใช้ระบบสารสนเทศต่อการสอบบัญชี

การใช้ระบบสารสนเทศของกิจการอาจมีผลกระทบต่อระดับความเสี่ยงต่อการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในระดับที่เกี่ยวกับสิ่งที่ผู้บริหารได้ให้การรับรองไว้ วิธีการควบคุม และวิธีการประเมินประสิทธิผลการควบคุมและการตรวจสอบของผู้สอบบัญชี เนื่องจากการใช้ระบบสารสนเทศจะมีลักษณะพิเศษบางประการที่แตกต่างจากการประมวลผลและจัดทำงบการเงินด้วยมือ เช่น

- การประมวลผลข้อมูลด้วยระบบสารสนเทศอาจทำให้หลักฐานในการติดตามเพื่อการตรวจสอบ (Audit Trails) ขาดหายไป ทั้งนี้เนื่องมาจากมีการรวมขั้นตอนบางขั้นตอนเข้าเป็นขั้นตอนเดียว โดยบางส่วนของขั้นตอนนั้นระบบจะทำโดยอัตโนมัติ หรือระบบสารสนเทศอาจไม่ได้ออกแบบให้มีการจัดเก็บหลักฐานนั้น เช่น ในการคำนวณต้นทุนสินค้าที่ผลิต ผู้ปฏิบัติงานอาจนำเข้าข้อมูลการเบิกวัตถุดิบและข้อมูลจำนวนสินค้าที่ผลิตได้ แต่ข้อมูลค่าแรงทางตรงและต้นทุนทางอ้อมจะคำนวณหรือปันส่วนเข้าสินค้าโดยอัตโนมัติ
- กิจการมักใช้ระบบสารสนเทศในการประมวลผลข้อมูล เนื่องจากรายการที่ต้องประมวลผลมีจำนวนมาก ดังนั้นโอกาสที่จะเกิดข้อผิดพลาดก็จะมีมากตามไปด้วย หากระบบสารสนเทศไม่มีการควบคุมทั่วไปของเทคโนโลยีสารสนเทศและการควบคุมระบบงานที่มีประสิทธิผล
- กิจการอาจใช้ระบบสารสนเทศในการประมวลผลข้อมูล เนื่องจากรายการที่ต้องประมวลมีความซับซ้อนในการคำนวณมาก ดังนั้นโอกาสที่จะเกิดข้อผิดพลาดก็จะมีมาก หากการควบคุมทั่วไปของเทคโนโลยีสารสนเทศเกี่ยวกับการพัฒนาและเปลี่ยนแปลงแก้ไขระบบสารสนเทศไม่มีประสิทธิผล
- ในระบบที่ใช้เทคโนโลยีสารสนเทศประมวลผลข้อมูล ข้อมูลจะถูกเก็บไว้ในหน่วยความจำชั่วคราวและสื่อแม่เหล็ก ซึ่งโอกาสที่ข้อมูลจะสูญหายหรือเสียหายจะมีมากกว่าระบบที่ประมวลผลข้อมูลด้วยมือ
- โอกาสที่จะมีการใช้ข้อมูลผิดในการประมวลผลข้อมูลจะสูงในระบบที่ใช้เทคโนโลยีสารสนเทศ
- ทางเดินของเอกสารและขั้นตอนการควบคุมจะแตกต่างไปเมื่อมีการใช้เทคโนโลยีสารสนเทศในการประมวลผลข้อมูล
- ผู้ใช้ข้อมูลอาจเชื่อถือผลจากระบบสารสนเทศมากเกินไป ซึ่งในทางปฏิบัติแล้วผลที่ได้จากระบบสารสนเทศอาจผิดพลาดได้ หากข้อมูลเข้าขั้นตอนในการประมวลผลข้อมูล หรือวิธีการและเงื่อนไขที่ใช้ในการประมวลผลข้อมูล (Logic) ไม่ถูกต้อง

โดยทั่วไปความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงจากปัจจัยเสี่ยงที่เกี่ยวกับการใช้เทคโนโลยีสารสนเทศของกิจการมักจะเกี่ยวเนื่องกับระบบสารสนเทศที่ใช้ อย่างไรก็ดีการใช้เทคโนโลยีสารสนเทศนอกเหนือจากระบบสารสนเทศของกิจการ อาจมีผลกระทบต่อการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในระดับที่เกี่ยวกับสิ่งที่ผู้บริหารได้ให้การรับรองไว้ได้ เช่น

ข้อบกพร่อง	ผลกระทบ
การเลิกใช้ฮาร์ดแวร์หรือซอฟต์แวร์โดยไม่ได้รับการอนุมัติหรือไม่มีการบันทึกรายการ	สินทรัพย์อาจแสดงมูลค่าที่สูงกว่าความเป็นจริง
การบันทึกค่าใช้จ่ายที่เกี่ยวข้องจากการใช้ระบบงานแบบระบบคลาวด์ที่เป็น SaaS จากผู้ให้บริการจากภายนอกเป็นสินทรัพย์ทั้งจำนวน	สินทรัพย์อาจแสดงมูลค่าที่สูงกว่าความเป็นจริง
การใช้ฮาร์ดแวร์หรือซอฟต์แวร์เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้รับอนุมัติ	งบการเงินถูกต้อง แต่ค่าใช้จ่ายบางส่วนจะไม่เกี่ยวข้องกับธุรกิจของกิจการ
การใช้บุคลากร วัสดุสิ้นเปลือง และอุปกรณ์ในกิจกรรมการพัฒนาระบบที่ไม่ได้ผ่านการอนุมัติ	งบการเงินถูกต้อง แต่ค่าใช้จ่ายบางส่วนอาจจะไม่เกี่ยวข้องกับธุรกิจของกิจการ
การทำสำเนาแฟ้มข้อมูลที่ได้รับจากการให้บริการลูกค้าเพื่อใช้ส่วนตัวหรือเพื่อใช้ในทางมิชอบโดยบุคลากรของกิจการ	อาจไม่มีผลโดยตรงต่อตัวเลขในงบการเงินแต่อาจก่อให้เกิดเหตุการณ์ที่สร้างความเสียหายที่ร้ายแรงต่อกิจการได้ เช่น ถูกฟ้องร้องและดำเนินคดีจากการละเมิดเงื่อนไขการรักษาความลับในสัญญากับลูกค้าซึ่งเป็นคู่สัญญา ซึ่งอาจจำเป็นให้ต้องมีการเปิดเผยข้อมูลในงบการเงิน หรือในรายงานของผู้สอบบัญชี
การใช้ซอฟต์แวร์ที่สิ้นสุดการสนับสนุน (End of Support) จากผู้ขาย	ไม่มีผลโดยตรงต่อตัวเลขในงบการเงิน แต่อาจก่อให้เกิดเหตุการณ์ที่สร้างความเสียหายที่ร้ายแรงต่อกิจการได้ เช่น การหยุดชะงักของกระบวนการทางธุรกิจหรือกิจกรรมทางธุรกิจบางส่วน เนื่องจากซอฟต์แวร์ที่ใช้สนับสนุนการดำเนินงานนั้นเกิดปัญหาไม่สามารถทำงานได้ตามปกติ
การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์	อาจไม่มีผลโดยตรงต่อตัวเลขในงบการเงิน แต่อาจก่อให้เกิดเหตุการณ์ที่สร้างความเสียหายที่ร้ายแรงต่อกิจการได้ เช่น ถูกฟ้องร้องและดำเนินคดีโดยเจ้าของลิขสิทธิ์ซอฟต์แวร์ และเกิดปัญหากับการส่งออกสินค้าของกิจการไปยังคู่ค้าที่อยู่ต่างประเทศบางประเทศ ซึ่งอาจจำเป็นให้ต้องมีการเปิดเผยข้อมูลในงบการเงิน หรือในรายงานของผู้สอบบัญชี
การรั่วไหลของข้อมูลส่วนบุคคลจากการถูกโจมตีระบบโดยผู้ไม่ประสงค์ดี	อาจไม่มีผลโดยตรงต่อตัวเลขในงบการเงิน แต่อาจก่อให้เกิดเหตุการณ์ที่สร้างความเสียหายที่ร้ายแรงต่อกิจการได้ เช่น ถูกฟ้องร้องและดำเนินคดีตามกฎหมาย คุ้มครองข้อมูลส่วนบุคคล ซึ่งจะจำเป็นให้ต้องมีการเปิดเผยข้อมูลในงบการเงิน หรือในรายงานของผู้สอบบัญชี

จากข้างต้น ผู้สอบบัญชีจึงอาจวิเคราะห์และระบุความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ แยกเป็น 3 ระดับ คือ ระดับกิจการ (Entity Level) ระดับระบบเทคโนโลยีสารสนเทศ (IT System Level) ระดับระบบสารสนเทศ (Application System Level) ซึ่งบทที่ 2 การควบคุมทั่วไปของเทคโนโลยีสารสนเทศของคู่มือฉบับนี้ ได้อธิบายรายละเอียดและให้ตัวอย่างเกี่ยวกับความเสี่ยงที่ระดับกิจการ และระดับระบบเทคโนโลยีสารสนเทศ ส่วนบทที่ 3 การควบคุมระบบงาน ของคู่มือฉบับนี้ได้อธิบายรายละเอียดและให้ตัวอย่างเกี่ยวกับความเสี่ยงที่ระบบสารสนเทศ

7.3. ตัวอย่างเงื่อนไขและเหตุการณ์เกี่ยวกับระบบสารสนเทศที่อาจแสดงถึงความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในรายงานทางการเงิน

ในการระบุและประเมินความเสี่ยงจากการใช้ระบบสารสนเทศเพื่อการสอบบัญชี ผู้สอบบัญชีต้องพิจารณาถึงเหตุการณ์ รายการหรือสถานการณ์ ทั้งภายในและภายนอกกิจการที่เกี่ยวกับระบบสารสนเทศที่เกิดขึ้นและอาจส่งผลทางลบต่อความสามารถของกิจการในการเกิดรายการ บันทึกรายการ ประมวลผล และรายงานข้อมูลทางการเงินให้เป็นไปตามสิ่งที่ผู้บริหารได้ให้การรับรองไว้ในงบการเงิน เช่น

- การเปลี่ยนแปลงบุคลากรที่สำคัญ รวมถึงการลาออกของผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ
- ข้อบกพร่องของการควบคุมด้านเทคโนโลยีสารสนเทศ โดยเฉพาะข้อบกพร่องที่ผู้บริหารมิได้กล่าวถึงหรือเพิกเฉยที่จะแก้ไข
- ภัยคุกคามทางไซเบอร์และอาชญากรรมทางคอมพิวเตอร์ที่ก่อให้เกิดผลกระทบต่อความถูกต้องน่าเชื่อถือของงบการเงิน เช่น การจู่โจมระบบสารสนเทศด้วยโปรแกรมเรียกค่าไถ่ การทุจริตหรือการยักยอกสินทรัพย์ของกิจการด้วยการเปลี่ยนแปลงข้อมูลในระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำงบการเงินเพื่อประโยชน์อันมิชอบ การหลอกลวงผู้ใช้งานให้โอนเงินของกิจการไปยังบัญชีธนาคารที่ไม่ใช่บัญชีธนาคารที่ถูกต้องของเจ้าหนี้
- ความไม่สอดคล้องระหว่างกลยุทธ์ทางเทคโนโลยีสารสนเทศของกิจการกับกลยุทธ์ทางธุรกิจ
- การเปลี่ยนแปลงสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศ รวมถึงการนำเทคโนโลยีใหม่มาใช้ในระบบสารสนเทศ ซึ่งอาจทำให้กระทบต่อความเสี่ยงและประสิทธิผลของควบคุมด้านเทคโนโลยีสารสนเทศของกิจการ
- การติดตั้งระบบสนเทศที่เกี่ยวข้องกับการรายงานทางการเงินที่สำคัญใหม่ หรือการปรับปรุงหรือเปลี่ยนแปลงของระบบสารสนเทศที่มีนัยสำคัญ

8. การระบุและประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชี

ผู้สอบบัญชีจะต้องระบุและประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชีอย่างมีระบบ กล่าวคือ ผู้สอบบัญชีต้องมีความเข้าใจในวัตถุประสงค์การใช้งานของระบบสารสนเทศ และต้องสามารถระบุปัจจัยเสี่ยงและความเสี่ยงสืบเนื่องจากการใช้งานระบบสารสนเทศนั้นต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผล และความน่าเชื่อถือของงบการเงินและหลักฐานการสอบบัญชีอย่างมีสาระสำคัญ รวมถึงการระบุการควบคุมที่กิจการกำหนดให้มีเพื่อตอบสนองต่อความเสี่ยงเหล่านั้น เนื่องจากระบบสารสนเทศที่ใช้เทคโนโลยีมีความเสี่ยงในบางเรื่องที่นอกเหนือจากความเสี่ยงของระบบสารสนเทศที่ประมวลผลด้วยมือ และมีการควบคุมในหลายด้านเพิ่มเติมจากการควบคุมที่จำเป็นสำหรับระบบสารสนเทศที่ประมวลผลด้วยมือ นอกจากนี้การควบคุมด้านเทคโนโลยีสารสนเทศยังมีความซับซ้อนมากกว่าด้วย

การระบุและประเมินประสิทธิผลการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชีมีความเกี่ยวข้องโดยตรงกับการประเมินระดับของ Control Risk หรือความเป็นไปได้ที่การควบคุมจะไม่สามารถป้องกัน ตรวจพบ และแก้ไขการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในงบการเงิน

8.1. ประเภทของการควบคุม

การจัดประเภทของการควบคุมตามลักษณะของการควบคุมเป็นการจัดประเภทของการควบคุมที่นิยมมากแบบหนึ่งสำหรับการระบุและประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศ ซึ่งการจัดประเภทของการควบคุมแบบนี้แบ่งการควบคุมออกเป็น 3 ประเภทหลัก คือ การควบคุมด้านเทคโนโลยีสารสนเทศที่ระดับกิจการ การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ และการควบคุมระบบงาน

- การควบคุมด้านเทคโนโลยีสารสนเทศที่ระดับกิจการ (IT Entity-Level Controls) เป็นการควบคุมที่เป็นส่วนหนึ่งของสภาพแวดล้อมการควบคุมของกิจการ เพื่อให้กิจการมีสภาพแวดล้อมการควบคุมที่ช่วยให้การควบคุมที่ระดับเทคโนโลยีสารสนเทศ และระดับระบบสารสนเทศมีประสิทธิผล โดยประกอบด้วยกระบวนการกำกับดูแลด้านเทคโนโลยีสารสนเทศ กระบวนการในการติดตามตรวจสอบ และกระบวนการในการรายงานผล ซึ่งตัวอย่างของการควบคุมประเภทนี้ ได้แก่ กลยุทธ์และแผนงานด้านเทคโนโลยีสารสนเทศ นโยบายและขั้นตอนด้านเทคโนโลยีสารสนเทศที่มีผลบังคับใช้ทั้งองค์กร กิจกรรมประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ การอบรมและให้ความรู้เกี่ยวกับด้านเทคโนโลยีสารสนเทศทั้งในแง่การใช้งานและการรักษาความมั่นคงปลอดภัยแก่บุคลากร และบุคคลภายนอกที่สามารถเข้าถึงทรัพยากรเทคโนโลยีสารสนเทศของกิจการ การติดตามตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น การตรวจสอบคุณภาพบริการด้านเทคโนโลยีสารสนเทศของหน่วยงานเทคโนโลยีสารสนเทศหรือขององค์กรที่ให้บริการจากภายนอก การตรวจภายในด้านเทคโนโลยีสารสนเทศ การตรวจสอบการปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับ
- การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ (IT General Controls) เป็นการควบคุมที่เกี่ยวข้องกับกระบวนการและกิจกรรมด้านเทคโนโลยีสารสนเทศของกิจการที่จะช่วยให้การควบคุมที่ระดับระบบสารสนเทศมีประสิทธิผล เช่น กระบวนการควบคุมการเข้าถึง กระบวนการจัดการการเปลี่ยนแปลงโปรแกรมและชุดคำสั่งหรือการเปลี่ยนแปลงอื่นในสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ กระบวนการจัดการการปฏิบัติการด้านเทคโนโลยีสารสนเทศ ซึ่งรายละเอียดเกี่ยวกับการควบคุมทั่วไปของเทคโนโลยีสารสนเทศนี้ได้อธิบายในบทที่ 2 การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ของคู่มือฉบับนี้
- การควบคุมระบบงาน (Application Controls) เป็นการควบคุมที่เกี่ยวข้องกับกิจกรรมแต่ละกิจกรรม หรือประเภทรายการใดรายการหนึ่ง หรือรายการบัญชีเฉพาะรายการ ดังนั้นในบางครั้งการควบคุมประเภทนี้จึงเรียกว่า การควบคุมรายการ (Transaction Controls) โดยมีวัตถุประสงค์เพื่อให้กิจการมั่นใจในความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของข้อมูลและรายการค้าที่นำเข้า ประมวลผล แสดงผล และจัดเก็บโดยระบบสารสนเทศซึ่งรายละเอียดเกี่ยวกับการควบคุมระบบงานนี้ได้อธิบายในบทที่ 3 การควบคุมระบบงาน ของคู่มือฉบับนี้

8.2. ความสัมพันธ์ของการควบคุมแต่ละประเภท

ผู้สอบบัญชีจะประเมินประสิทธิผลของการควบคุมระบบงานใด ขึ้นอยู่กับกลยุทธ์และแนวทางที่ผู้สอบบัญชีจะใช้ในการตรวจสอบประเภทของรายการแต่ละประเภทที่มีนัยสำคัญในงบการเงิน (Significant Class of Transactions) ในกรณีที่การควบคุมที่กิจการใช้ในประเภทรายการที่ผู้สอบบัญชีใช้แนวทางที่อิงการควบคุมในการตรวจสอบเป็นการควบคุมระบบงาน ผู้สอบบัญชีจะต้องพิจารณาถึงผลกระทบของข้อบกพร่องที่พบจากการประเมินประสิทธิผลการควบคุมทั่วไปของเทคโนโลยีสารสนเทศต่อประสิทธิผลของการควบคุมระบบงานด้วย เช่น

- ผู้สอบบัญชีสรุปผลว่าการควบคุมทั่วไปของเทคโนโลยีสารสนเทศเกี่ยวกับกระบวนการจัดการการเปลี่ยนแปลงโปรแกรมและชุดคำสั่งไม่มีประสิทธิผล และผู้สอบบัญชีได้ทำการตรวจสอบเพิ่มเติมและพบว่ากิจการไม่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศที่ใช้ในการประมวลผลประเภทรายการที่ผู้สอบบัญชีต้องการอิงการควบคุมระบบงานในการตรวจสอบเลยตั้งแต่นำระบบดังกล่าวมาใช้งาน 3 ปีที่แล้ว ซึ่งครอบคลุมถึงช่วงเวลาที่ผู้สอบบัญชีต้องการได้ความเชื่อมั่นในกรณีนี้ ผู้สอบบัญชีสามารถสรุปว่าการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ไม่มีประสิทธิผลนี้ไม่มีผลกระทบต่อประสิทธิผลของการควบคุมระบบงาน และผู้สอบบัญชีสามารถเชื่อมั่นว่าการควบคุมระบบงานที่ผู้สอบบัญชีประเมินแล้วว่ามีประสิทธิผลจะมีประสิทธิผลตลอดช่วงเวลาที่ผู้สอบบัญชีต้องการได้ความเชื่อมั่น
- ผู้สอบบัญชีสรุปผลว่าการควบคุมทั่วไปของเทคโนโลยีสารสนเทศเกี่ยวกับกระบวนการควบคุมการเข้าถึงไม่มีประสิทธิผล เนื่องจากการให้สิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศจะให้ตามที่ผู้ใช้งานขอ โดยไม่มีการกำหนดขอบเขตของสิทธิที่ผู้ใช้งานจะได้รับตามบทบาทหน้าที่ และมีการให้สิทธิในการเข้าถึงระบบที่สูงแก่ผู้ใช้งานจำนวนมาก รวมถึงผู้ใช้งานของระบบสารสนเทศที่ใช้ในการประมวลผลประเภทรายการที่ผู้สอบบัญชีต้องการอิงการควบคุมระบบงานด้วย ในกรณีนี้ผู้สอบบัญชีอาจจำเป็นต้องสรุปว่าการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ไม่มีประสิทธิผลนี้มีผลกระทบต่อประสิทธิผลของการควบคุมระบบงาน
- ผู้สอบบัญชีสรุปผลว่าการควบคุมทั่วไปของเทคโนโลยีสารสนเทศเกี่ยวกับกระบวนการควบคุมการเข้าถึง กระบวนการจัดการการเปลี่ยนแปลงโปรแกรมและชุดคำสั่งหรือการเปลี่ยนแปลงอื่นในสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ กระบวนการจัดการการปฏิบัติการด้านเทคโนโลยีสารสนเทศมีประสิทธิผล ในกรณีนี้ผู้สอบบัญชีสามารถสรุปว่าการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่มีประสิทธิผลนี้จะมีผลให้ผู้สอบบัญชีสามารถเชื่อมั่นว่าการควบคุมระบบงานที่ผู้สอบบัญชีประเมินแล้วว่ามีประสิทธิผล จะมีประสิทธิผลตลอดช่วงเวลาที่ผู้สอบบัญชีต้องการได้ความเชื่อมั่น

นอกจากนี้ข้อบกพร่องของการควบคุมด้านเทคโนโลยีสารสนเทศที่ระดับกิจการอาจมีผลกระทบต่อประสิทธิผลของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศและการควบคุมระบบงานได้ โดยเฉพาะในกรณีที่มีข้อบกพร่องที่เกิดจากการฝ่าฝืนหรือแทรกแซงระบบการควบคุมโดยผู้บริหารของกิจการ วัฒนธรรมองค์กรที่ไม่ให้ความสำคัญกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ การควบคุมและจริยธรรมในการใช้ทรัพยากรเทคโนโลยีสารสนเทศและข้อมูล และการกำกับดูแลการบริหารจัดการด้านเทคโนโลยีสารสนเทศ หากผู้สอบบัญชีพบข้อบกพร่องดังกล่าวจากการประเมินประสิทธิผลการควบคุมด้านเทคโนโลยีสารสนเทศที่ระดับกิจการ ผู้สอบบัญชีอาจสรุปว่าการควบคุมด้านเทคโนโลยีสารสนเทศที่ระดับกิจการที่ไม่มีประสิทธิผลนี้มีผลกระทบต่อประสิทธิผลของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศและการควบคุมระบบงาน และตัดสินใจใช้แนวทางที่ไม่อิงการควบคุมในการตรวจสอบงบการเงินของกิจการ

8.3. วิธีการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อการสอบบัญชี

การประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศ สามารถแบ่งออกได้เป็นสองขั้นตอนเช่นเดียวกับการประเมินประสิทธิผลของการควบคุมอื่นที่ไม่ใช่การควบคุมด้านเทคโนโลยีสารสนเทศ คือ การประเมินประสิทธิผลการออกแบบการควบคุม (Control Design Effectiveness Evaluation) และการควบคุมดังกล่าวมีการนำไปปฏิบัติจริง และการประเมินประสิทธิผลการปฏิบัติตามการควบคุมที่ออกแบบไว้ (Control Operating Effectiveness Evaluation) โดยวิธีการที่ผู้สอบบัญชีสามารถใช้ในการประเมินประสิทธิผลมีได้หลายวิธีการ เช่น ใช้วิธีการสังเกตการณ์การปฏิบัติงานเพื่อให้แน่ใจว่ามีการแบ่งแยกหน้าที่ตามที่กำหนดไว้หรือไม่ ในกรณีที่การควบคุมทำโดยระบบสารสนเทศ ผู้สอบบัญชีอาจจำเป็นต้องใช้เครื่องมือเทคนิคอัตโนมัติช่วยในการประเมิน เช่น ผู้สอบบัญชีอาจใช้โปรแกรมตรวจสอบในการทดสอบผ่านระบบเพื่อให้แน่ใจว่าระบบจะไม่รับรายการที่ไม่ถูกต้องตรงตามที่กำหนดไว้ เป็นต้น

8.3.1 การประเมินประสิทธิผลการออกแบบการควบคุม

การประเมินประสิทธิผลการออกแบบการควบคุม เป็นการประเมินว่าการควบคุมที่กำหนดไว้มีประสิทธิผลที่จะช่วยให้บรรลุวัตถุประสงค์ของการควบคุมที่กำหนดไว้หรือไม่ เช่น กิจการมีการกำหนดมาตรฐานในการตั้งค่ารหัสผ่านเพื่อให้มั่นใจว่าผู้ที่สามารถเข้าถึงระบบเทคโนโลยีสารสนเทศเป็นผู้ที่ได้รับอนุมัติเท่านั้น ซึ่งการควบคุมที่ผู้สอบบัญชีจะรวมอยู่ในขอบเขตการประเมินประสิทธิผลจะต้องเป็นการควบคุมที่มีวัตถุประสงค์ที่มีความสัมพันธ์โดยตรงกับการลดความเสี่ยงที่จะเกิดการแสดงข้อมูลในงบการเงินที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ในสิ่งที่ผู้บริหารได้ให้การรับรองไว้ ตัวอย่างของวิธีการที่ผู้สอบบัญชีอาจใช้ในการประเมินประสิทธิผลการออกแบบการควบคุม ได้แก่

- สอบถามบุคลากรของกิจการ
- สอบทานนโยบายด้านเทคโนโลยีสารสนเทศ คู่มือปฏิบัติงานของกิจการ คำบรรยายลักษณะงาน ผังทางเดินเอกสารและข้อมูล ตารางการให้สิทธิในการเข้าถึงระบบสารสนเทศ ตารางอำนาจอนุมัติ เอกสารระเบียบหรือขั้นตอนปฏิบัติงานต่าง ๆ และเอกสารอื่นที่มีผลต่อการควบคุม
- ติดตามดูการปฏิบัติงานตามการควบคุมที่กำหนดไว้ (Walk-through)
- ระบุข้อบกพร่องของการควบคุมที่ออกแบบและผลกระทบต่อประสิทธิผลของการควบคุม
- ประเมินความสำคัญของการควบคุมเปรียบเทียบกับการควบคุมด้านเทคโนโลยีสารสนเทศทั้งหมดของระบบสารสนเทศ ทั้งนี้เพื่อระบุถึงขอบเขตการทดสอบการควบคุม ซึ่งในการประเมินผู้สอบบัญชีอาจสรุปว่า
  - การควบคุมด้านเทคโนโลยีสารสนเทศที่ออกแบบไว้มีข้อบกพร่อง ทำให้ไม่สามารถเชื่อถือการควบคุมได้ ในกรณีนี้ผู้สอบบัญชีไม่จำเป็นต้องทำการสอบทานใดเพิ่มเติม และไม่ต้องทำการทดสอบการปฏิบัติตามระบบ ทั้งนี้ผู้สอบบัญชีต้องประเมินผลกระทบของข้อบกพร่องดังกล่าวต่อความครบถ้วน ความถูกต้อง ความสมเหตุสมผลและความน่าเชื่อถือของงบการเงิน และใช้วิธีการอื่นแทนเพื่อให้บรรลุวัตถุประสงค์ของการตรวจสอบ เช่น การทดสอบเนื้อหาสาระ
  - การควบคุมที่กำหนดไว้มีประสิทธิผลเพียงพอ และอาจสามารถเอาไปใช้ประโยชน์ในการปฏิบัติงานสอบบัญชีและลดขอบเขตการทดสอบรายการได้ ในกรณีนี้ผู้สอบบัญชีจะต้องทำการประเมินประสิทธิผลการปฏิบัติตามการควบคุมที่ออกแบบไว้ต่อไป ยกเว้นในกรณีที่ผู้สอบบัญชีตัดสินใจที่จะไม่อิงการควบคุมในการสอบบัญชีได้ ซึ่งอาจเนื่องจากผู้สอบบัญชีพิจารณาแล้วว่าทรัพยากรที่ต้องใช้ในการทดสอบการปฏิบัติตามการควบคุมสูงกว่าทรัพยากรที่สามารถประหยัดได้จากการที่ผู้สอบบัญชีสามารถลดขอบเขตการตรวจสอบบัญชี หรือการควบคุมด้านเทคโนโลยีสารสนเทศนี้มีเพื่อวัตถุประสงค์เดียวกับการควบคุมในส่วนอื่นที่ผู้สอบบัญชีได้ทำการทดสอบแล้ว

8.3.2 การประเมินประสิทธิผลการปฏิบัติตามการควบคุมที่ออกแบบไว้

หากผู้สอบบัญชีสรุปผลการประเมินประสิทธิผลการออกแบบการควบคุมว่าการควบคุมด้านเทคโนโลยีสารสนเทศที่ออกแบบไว้มีประสิทธิผล และผู้สอบบัญชีตัดสินใจที่จะอิงการควบคุมเหล่านั้น ผู้สอบบัญชีจะต้องทำการประเมินประสิทธิผลการปฏิบัติตามการควบคุมที่ออกแบบไว้ โดยการทดสอบการปฏิบัติตามการควบคุม โดยผลที่ได้จากขั้นตอนนี้จะใช้ในการระบุขอบเขตของการตรวจสอบเนื้อหาสาระต่อไป ซึ่งตัวอย่างของวิธีการที่ผู้สอบบัญชีอาจใช้ในขั้นตอนนี้ ได้แก่

- ตรวจสอบการแบ่งแยกหน้าที่ระหว่างหน่วยงานเทคโนโลยีสารสนเทศกับผู้ใช้งาน และการแบ่งแยกหน้าที่ภายในหน่วยงานเทคโนโลยีสารสนเทศว่าเป็นไปตามนโยบายที่กำหนดไว้
- ตรวจสอบการให้สิทธิที่สำคัญในการเข้าถึงระบบตามที่กำหนดในระบบสารสนเทศว่าเป็นไปตามตารางการให้สิทธิที่อิงบทบาทหน้าที่ที่กำหนดไว้
- สังเกตการณ์การปฏิบัติการด้านเทคโนโลยีสารสนเทศในการการควบคุมการเข้าถึงอุปกรณ์ โปรแกรม ชุดคำสั่ง และข้อมูล การพัฒนาระบบและการเข้าถึงเอกสารประกอบระบบการบำรุงรักษาและปรับปรุงโปรแกรม ชุดคำสั่ง และระบบ

สำหรับการออกแบบลักษณะ ขอบเขต และระยะเวลาในการประเมินประสิทธิผลการควบคุมเทคโนโลยีสารสนเทศ ผู้สอบบัญชีต้องพิจารณาผลกระทบของการเปลี่ยนแปลงด้านเทคโนโลยีที่มีสาระสำคัญที่เกิดขึ้นในระหว่างช่วงเวลาที่ผู้สอบบัญชีต้องการความเชื่อมั่นในประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศด้วย เช่น การเปลี่ยนระบบสารสนเทศที่ใช้ในการประมวลผลและจัดทำงบการเงิน การเปลี่ยนแปลงกระบวนการและวิธีการในการควบคุมการเข้าถึง การเปลี่ยนแปลงกระบวนการและวิธีการจัดการการเปลี่ยนแปลงโปรแกรมและชุดคำสั่ง การเปลี่ยนแปลงอื่นในสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกระบวนการและวิธีการจัดการการปฏิบัติการด้านเทคโนโลยีสารสนเทศ หากผู้สอบบัญชีพิจารณาแล้วเห็นว่าการเปลี่ยนแปลงที่เกิดขึ้นมีผลกระทบทำให้การควบคุมที่ผู้สอบบัญชีต้องการอิงในการตรวจสอบเปลี่ยนแปลงไป ผู้สอบบัญชีจำเป็นต้องประเมินประสิทธิผลของการควบคุมที่ได้รับผลกระทบนั้นทั้งก่อนและหลังการเปลี่ยนแปลง เช่น กิจการมีการเปลี่ยนระบบงานที่ใช้สนับสนุนกระบวนการขายและรับเงินจากระบบ Sales One เป็นระบบ New Sales ผู้สอบบัญชีจำเป็นต้องทดสอบการปฏิบัติตามการควบคุมทั่วไปของเทคโนโลยีสารสนเทศและการควบคุมระบบงานของทั้งระบบ Sales One เป็นระบบ New Sales ที่ได้รับผลกระทบจากการเปลี่ยนแปลง เช่น การให้สิทธิในการเข้าถึงระบบ Sales One และระบบ New Sales ตามที่กำหนดในระบบเป็นไปตามนโยบายที่กำหนดไว้

8.4. การสรุปและการใช้ผลการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศ

เมื่อผู้สอบบัญชีทำการตรวจสอบระบบสารสนเทศแล้วเสร็จ ผู้สอบบัญชีจะต้องสรุปผลการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศ โดยการวิเคราะห์ระดับของผลกระทบและโอกาสที่จะเกิด และการระบุระดับความเสี่ยงของแต่ละประเด็นที่พบและของทุกประเด็นร่วมกัน ต่อความครบถ้วน ความถูกต้อง และความสมเหตุสมผลของข้อมูลและรายการค้าในระบบสารสนเทศและในหลักฐานการสอบบัญชี และการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในงบการเงิน

โดยทั่วไปประเด็นที่เป็นข้อบกพร่องจากการออกแบบการควบคุมที่ไม่มีประสิทธิผล มีแนวโน้มที่จะมีระดับความเสี่ยงที่สูงกว่าข้อบกพร่องในการปฏิบัติตามการควบคุมที่กำหนดไว้ เพราะข้อบกพร่องจากการออกแบบการควบคุมจะมีผลที่แผ่กระจายมากกว่า เช่น กิจการไม่มีการกำหนดให้มีการระงับรหัสผู้ใช้งานทันทีที่พนักงานพ้นสภาพการจ้างงานกับกิจการ โดยฝ่ายบุคคลจะต้องแจ้งให้หน่วยงานเทคโนโลยีสารสนเทศทราบล่วงหน้า 5 วันทำการก่อนวันดังกล่าว ในกรณีนี้หน่วยงานเทคโนโลยีสารสนเทศอาจไม่เคยได้รับแจ้งและทำการระงับรหัสผู้ใช้งานของพนักงานที่พ้นสภาพการจ้างงานแล้วทั้งหมดในทางตรงกันข้าม หากกิจการมีการกำหนดเป็นนโยบายไว้ ผู้สอบบัญชีอาจพบประเด็นว่ามีรายการบางรายการที่ฝ่ายบุคคลไม่ได้แจ้งให้หน่วยงานเทคโนโลยีสารสนเทศทราบหรือทราบล่าช้า หรือบางรายการที่หน่วยงานเทคโนโลยีสารสนเทศไม่ได้ดำเนินการตามนโยบาย แต่มีรายการส่วนหนึ่งได้รับการดำเนินการตามที่นโยบายกำหนดไว้ นอกจากนี้ประเด็นที่เป็นข้อบกพร่องของการควบคุมโดยอัตโนมัติมีแนวโน้มที่จะมีระดับความเสี่ยงที่สูงกว่าการควบคุมที่ปฏิบัติด้วยมือ เพราะจะมีผลที่แผ่กระจายมากกว่า เช่น กิจการอาจจะมีการกำหนดการควบคุมโดยให้มีการผ่านรายการโดยอัตโนมัติ แต่ผู้ปฏิบัติงานตั้งค่าเลขที่บัญชีที่ต้องการให้ผ่านรายการในแฟ้มข้อมูลหลักลูกหนี้ไม่ถูกต้อง ทำให้ทุกครั้งที่เกิดรายการขึ้น ระบบจะทำการผ่านรายการไปยังบัญชีที่ตั้งค่าไว้แทนที่จะผ่านรายการไปยังบัญชีที่ถูกต้อง

ผู้สอบบัญชีจะใช้ผลจากการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศในการวางแผนงานและการตรวจสอบบัญชี เพื่อให้การตรวจสอบบัญชีเป็นไปอย่างมีประสิทธิผลและประสิทธิภาพ เนื่องจากการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศจะช่วยให้ผู้สอบบัญชีมีความเข้าใจในการควบคุมของกิจการที่เพียงพอ เช่น ประเภทและลักษณะของความผิดพลาดที่ทำให้มีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอย่างมีสาระสำคัญที่อาจเกิดขึ้นได้ ปัจจัยที่มีผลต่อความเสี่ยงที่จะทำให้เกิดความผิดพลาดที่เป็นสาระสำคัญ ซึ่งความเข้าใจนี้จะช่วยในการออกแบบลักษณะ ช่วงเวลาและขอบเขตของการตรวจสอบเนื้อหาสาระ ในกรณีที่ผู้สอบบัญชีใช้แนวทางการตรวจสอบที่อิงการควบคุมของกิจการ และจากการประเมินประสิทธิผลการควบคุมของกิจการประกอบกับการควบคุมอื่นที่ไม่ใช่การควบคุมด้านเทคโนโลยีสารสนเทศพบว่า การควบคุมของกิจการมีประสิทธิผล ผู้สอบบัญชีอาจลดขอบเขตการตรวจสอบเนื้อหาสาระของประเภทรายการที่เกี่ยวข้องลงได้ ในกรณีที่ผู้สอบบัญชีพบว่าการควบคุมด้านเทคโนโลยีสารสนเทศไม่มีประสิทธิผลไม่ว่าจะเป็นที่ระดับการออกแบบการควบคุมหรือระดับการปฏิบัติตามการควบคุมที่กำหนดไว้ และกิจการไม่มีการควบคุมอื่นที่มีประสิทธิผลเพียงพอที่จะทดแทนการควบคุมด้านเทคโนโลยีสารสนเทศที่บกพร่อง หรือผู้สอบบัญชีเลือกที่จะใช้แนวทางการตรวจสอบที่ไม่อิงการควบคุมที่มี ผู้สอบบัญชีจำเป็นต้องขยายขอบเขตการตรวจสอบเนื้อหาสาระของประเภทรายการที่เกี่ยวข้องให้เพียงพอที่จะให้ความเชื่อมั่นในระดับที่สมเหตุสมผลว่า งบการเงินของกิจการไม่มีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอย่างมีสาระสำคัญ ทั้งนี้ หัวข้อที่ 7 ผลกระทบจากการขาดการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ดี ของบทที่ 2 การควบคุมทั่วไปของเทคโนโลยีสารสนเทศได้อธิบายในรายละเอียดเพิ่มเติมเกี่ยวกับผลกระทบของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศต่อการจัดทำงบการเงินและต่อการสอบบัญชี รวมถึงตัวอย่างแนวทางการตรวจสอบในกรณีที่พบข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

9. การตรวจสอบในกรณีที่กิจการใช้บริการเกี่ยวกับระบบสารสนเทศจากองค์กรที่ให้บริการ

การใช้บริการด้านเทคโนโลยีสารสนเทศที่ผู้สอบบัญชีต้องกำหนดให้อยู่ในขอบเขตงานสอบบัญชี คือ การใช้บริการด้านเทคโนโลยีสารสนเทศที่มีผลกระทบต่อเรื่องใดเรื่องหนึ่งดังต่อไปนี้

- การประมวลผลข้อมูลของประเภทของรายการค้าที่มีความสำคัญต่องบการเงินของกิจการ
- ขั้นตอนการปฏิบัติงาน (ทั้งที่อยู่ในระบบเทคโนโลยีสารสนเทศและระบบที่ปฏิบัติด้วยมือ) ของกิจการเมื่อมีรายการค้าเกิดขึ้น มีการบันทึก ประมวลผล แก้ไข รวมถึงการผ่านรายการไปยังสมุดบัญชีแยกประเภททั่วไป และการจัดทำรายงานในงบการเงิน
- บันทึกทางบัญชีที่เกี่ยวข้อง (ไม่ว่าจะอยู่ในรูปแบบทางอิเล็กทรอนิกส์หรือการเขียน) ข้อมูลประกอบงบการเงิน และรายการในงบการเงินของกิจการที่เกิดขึ้นมีการบันทึก การประมวลผลและการรายงานรายการค้าของกิจการ รวมถึงการแก้ไขข้อมูลที่ไม่ถูกต้องและการผ่านรายการไปยังสมุดบัญชีแยกประเภททั่วไป
- วิธีการที่ระบบสารสนเทศของกิจการใช้ในการตรวจจับเหตุการณ์และเงื่อนไขต่าง ๆ (นอกเหนือจากรายการค้า) ที่มีความสำคัญต่องบการเงิน
- กระบวนการที่ใช้ในการจัดเตรียมงบการเงินของกิจการ รวมถึงการประมาณการทางบัญชี และการเปิดเผยข้อมูลที่สำคัญ
- การควบคุมเกี่ยวกับการจัดทำสมุดรายวันทั่วไป รวมถึงสมุดรายวันที่ไม่ได้อยู่ในรูปแบบมาตรฐานที่ใช้บันทึกรายการที่ไม่ได้เกิดขึ้นเป็นประจำ รายการทางการค้าที่ไม่ปกติ หรือการปรับปรุงรายการ

หากผู้สอบบัญชีพิจารณาแล้วเห็นว่า ขอบเขตงานตรวจสอบระบบสารสนเทศเพื่อการสอบบัญชีของกิจการจำเป็นต้องรวมถึงการตรวจสอบระบบสารสนเทศจากองค์กรที่ให้บริการเทคโนโลยีสารสนเทศ ซึ่งอาจจำเป็นต้องครอบคลุมถึงการตรวจสอบระบบสารสนเทศขององค์กรที่ให้บริการช่วงด้วย ผู้สอบบัญชีต้องรวบรวมข้อมูลเพื่อให้ได้มาซึ่งความเข้าใจในลักษณะของบริการ ขอบเขตความรับผิดชอบของกิจการและองค์กรที่ให้บริการ ความสำคัญของการบริการดังกล่าวต่อกิจการ และผลกระทบของการใช้บริการนั้นต่อความเสี่ยงและการควบคุมของกิจการในส่วนที่เกี่ยวข้องกับการตรวจสอบงบการเงินอย่างเพียงพอ ที่จะทำให้ผู้สอบบัญชีสามารถระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ และออกแบบและปฏิบัติตามวิธีการตรวจสอบเพื่อตอบสนองต่อความเสี่ยงเหล่านั้นได้ จากการรวบรวมข้อมูลและความเข้าใจในส่วนนี้ ผู้สอบบัญชีอาจพบสถานการณ์ที่มีผลกระทบต่อการกำหนดแนวทางและวิธีการในการตรวจสอบ เช่น

1. ผู้สอบบัญชีไม่สามารถตรวจสอบระบบสารสนเทศขององค์กรที่ให้บริการ เนื่องจากสัญญาการให้บริการที่กิจการทำไว้กับองค์กรที่ให้บริการ ไม่มีเงื่อนไขที่อนุญาตให้กิจการตรวจสอบระบบสารสนเทศจากองค์กรที่ให้บริการได้ และองค์กรที่ให้บริการ
2. ผู้สอบบัญชีสามารถตรวจสอบระบบสารสนเทศจากองค์กรที่ให้บริการ แต่มีข้อจำกัดที่สำคัญบางประการ เช่น ช่วงและระยะเวลาที่ผู้สอบบัญชีสามารถเข้าตรวจสอบ หรือทรัพยากรและค่าใช้จ่ายที่ต้องใช้ในการตรวจสอบที่อาจมีผลกระทบจากการที่ระบบสารสนเทศจากองค์กรที่ให้บริการอยู่ต่างประเทศหรือระบบสารสนเทศและกระบวนการด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องมีความซับซ้อนอย่างมาก หรือขอบเขตที่ผู้สอบบัญชีสามารถเข้าถึงข้อมูลและหลักฐานการสอบบัญชี รวมถึงการจัดทำสำเนาข้อมูลและหลักฐานการสอบบัญชี หรือการสื่อสารกับบุคลากรขององค์กรที่ให้บริการและความสามารถในการสอบทานข้อมูลและหลักฐานการสอบบัญชีที่มีผลกระทบจากภาษาที่ต้องใช้
3. ผู้สอบบัญชีสามารถตรวจสอบระบบสารสนเทศจากองค์กรที่ให้บริการอย่างเพียงพอ ที่จะทำให้ผู้สอบบัญชีสามารถระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ และออกแบบและปฏิบัติตามวิธีการตรวจสอบเพื่อตอบสนองต่อความเสี่ยงเหล่านั้นได้

ตัวอย่างของแนวทางการตรวจสอบระบบสารสนเทศขององค์กรที่ให้บริการสำหรับแต่ละสถานการณ์ข้างต้นมีดังนี้

สถานการณ์ที่พบ	ตัวอย่างแนวทางในการตรวจสอบ
ผู้สอบบัญชีไม่สามารถตรวจสอบระบบสารสนเทศขององค์กรที่ให้บริการ	ผู้สอบบัญชีระบุและประเมินประสิทธิผลของการควบคุมที่กิจการกำหนดไว้เพื่อจัดการความเสี่ยงจากการใช้บริการเทคโนโลยีสารสนเทศของกิจการที่มีผลต่อการจัดทำรายงานทางการเงินและการสอบบัญชีอย่างมีสาระสำคัญ ซึ่งอาจประกอบด้วยการควบคุมหลายประเภท เช่น การควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการบริหารจัดการองค์กรที่ให้บริการ การควบคุมระบบงาน การควบคุมส่วนเสริมของกิจการ (Complementary User Entity Controls) ซึ่งการควบคุมส่วนเสริมของกิจการนี้เป็นการควบคุมที่มีการกำหนดไว้ว่ากิจการที่ใช้บริการต้องมีการนำไปปฏิบัติจริง รวมถึงพิจารณาว่าความจำเป็นในการใช้รายงานของผู้สอบบัญชีขององค์กรที่ให้บริการ เพื่อสนับสนุนความเข้าใจในองค์กรที่ให้บริการของผู้สอบบัญชีของกิจการที่ใช้บริการ
ผู้สอบบัญชีสามารถตรวจสอบระบบสารสนเทศขององค์กรที่ให้บริการ แต่มีข้อจำกัดที่สำคัญบางประการ	ผู้สอบบัญชีอาจให้ผู้สอบบัญชีหรือผู้เชี่ยวชาญอื่นปฏิบัติตามแนวทางและวิธีการตรวจสอบเพื่อได้มาซึ่งข้อมูลที่จำเป็นเกี่ยวกับการควบคุมที่เกี่ยวข้อง ณ องค์กรที่ให้บริการ โดยในกรณีนี้ผู้สอบบัญชีจะต้องปฏิบัติงานให้เป็นไปตาม มาตรฐานฉบับที่ 402 เรื่อง “ข้อพิจารณาในกรณีที่กิจการใช้บริการขององค์กรอื่น” รวมถึงมาตรฐานฉบับที่ 620 เรื่อง “การใช้ผลงานของผู้เชี่ยวชาญของผู้สอบบัญชี” ในกรณีที่มีการใช้ผู้เชี่ยวชาญในการตรวจสอบ
ผู้สอบบัญชีสามารถตรวจสอบระบบสารสนเทศจากองค์กรที่ให้บริการอย่างเพียงพอ	ผู้สอบบัญชีใช้แนวทางและกระบวนการที่ในการทำความเข้าใจ ระบุความเสี่ยง และประเมินประสิทธิผลการควบคุมที่เกี่ยวข้อง ซึ่งอาจเป็นการควบคุมด้านเทคโนโลยีสารสนเทศระดับองค์กร การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ หรือการควบคุมระบบงานของระบบสารสนเทศขององค์กรที่ให้บริการ เช่นเดียวกับแนวทางและกระบวนการที่ผู้สอบบัญชีใช้ในการตรวจสอบระบบสารสนเทศของกิจการ

แม้ว่าแนวทางและกระบวนการที่ผู้สอบบัญชีใช้ในการทำความเข้าใจ ระบุความเสี่ยงและการควบคุมที่เกี่ยวข้องซึ่งอาจเป็นการควบคุมด้านเทคโนโลยีสารสนเทศระดับองค์กร การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ หรือการควบคุมระบบงานของระบบสารสนเทศขององค์กรที่ให้บริการ ไม่มีความแตกต่างจากแนวทางและวิธีการที่ผู้สอบบัญชีใช้ในการตรวจสอบระบบสารสนเทศของกิจการ เทคนิคและเครื่องมือที่ผู้สอบบัญชีใช้ในการตรวจสอบระบบสารสนเทศขององค์กรที่ให้บริการอาจแตกต่างไปตามปัจจัยที่สำคัญต่าง ๆ เช่น ลักษณะของกระบวนการด้านเทคโนโลยีสารสนเทศ เทคโนโลยี และการควบคุม ที่องค์กรที่ให้บริการใช้ ความมีอยู่ของข้อมูลและหลักฐานการตรวจสอบ ความสามารถในการเข้าถึงและทำสำเนาข้อมูลและหลักฐานการตรวจสอบของผู้สอบบัญชี ซึ่งผู้สอบบัญชีควรศึกษาคู่มือฉบับนี้ ควบคู่กับมาตรฐานการสอบบัญชี รหัส 402 เรื่อง “ข้อพิจารณาในกรณีที่กิจการใช้บริการขององค์กรอื่น” ที่ให้รายละเอียดเกี่ยวกับวิธีการที่ผู้สอบบัญชีจะใช้ในการได้มาซึ่งความเข้าใจในบริการที่องค์กรที่ให้บริการจัดให้รวมถึงการควบคุมภายใน ที่เกี่ยวข้องกับการตรวจสอบอย่างเพียงพอ ที่จะระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ และออกแบบและปฏิบัติงานตรวจสอบเพื่อตอบสนองต่อความเสี่ยงเหล่านั้น นอกจากนี้เอกสารประกอบคู่มือบทที่ 5 เรื่อง ความเสี่ยง การควบคุม และการตรวจสอบการใช้เทคโนโลยีสมัยใหม่ ได้ให้รายละเอียดเกี่ยวกับการประเมินการดำเนินงานโดยบริษัทผู้ให้บริการ หรือ Cloud Service Provider (CSP) ซึ่งผู้สอบบัญชีอาจนำไปประยุกต์ใช้ในการตรวจสอบในกรณีที่กิจการใช้บริการเกี่ยวกับระบบสารสนเทศจากองค์กรที่ให้บริการได้

ในกรณีที่ผู้สอบบัญชีพบสถานการณ์ที่ผู้สอบบัญชีไม่สามารถได้มาซึ่งหลักฐานการสอบบัญชี ที่เหมาะสมอย่างเพียงพอเกี่ยวกับบริการที่องค์กรที่ให้บริการจัดทำในส่วนที่เกี่ยวข้องกับการตรวจสอบงบการเงินของกิจการที่ใช้บริการ อาจถือเป็นการจำกัดขอบเขตการตรวจสอบ ซึ่งการที่ผู้สอบบัญชีจะแสดงความเห็นแบบมีเงื่อนไขหรือไม่แสดงความเห็นหรือไม่นั้นขึ้นอยู่กับข้อสรุปของผู้สอบบัญชีว่าผลกระทบที่เป็นไปได้ที่มีต่องบการเงินนั้นมีสาระสำคัญหรือเป็นผลกระทบที่แผ่กระจายหรือไม่

10. บทสรุป

สถานะปัจจุบันและแนวโน้มที่กิจการจะมีการนำเทคโนโลยีมาใช้ในการจัดทำบัญชีมากขึ้นอย่างต่อเนื่อง ทำให้ผู้สอบบัญชีต้องมีความรู้และความเข้าใจถึงเทคโนโลยีที่มีการนำมาใช้ในการจัดทำบัญชี และความเสี่ยงของการใช้เทคโนโลยีเหล่านั้นต่อจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ทั้งนี้เนื่องจากการใช้เทคโนโลยีประมวลผลข้อมูลทางการเงินและจัดทำงบการเงิน มีผลทำให้เกิดการเปลี่ยนแปลงในการจัดการข้อมูลทางบัญชี ร่องรอยการตรวจสอบ ขั้นตอนการบันทึกบัญชีตลอดถึงการกำหนดบทบาทหน้าที่ความรับผิดชอบของบุคลากรต่าง ๆ ที่เกี่ยวข้องได้ เช่น ในกรณีที่กิจการไม่มีการใช้เทคโนโลยีประมวลผลข้อมูลและจัดทำงบการเงินเลย กิจการจะไม่มีหน่วยงานเทคโนโลยีสารสนเทศ และไม่ต้องจัดให้มีการแบ่งแยกหน้าที่ภายในหน่วยงานเทคโนโลยีสารสนเทศและระหว่างหน่วยงานเทคโนโลยีสารสนเทศและผู้ใช้งาน แต่เมื่อกิจการมีการใช้เทคโนโลยีประมวลผลข้อมูลและจัดทำงบการเงินอย่างมีสาระสำคัญ การจัดให้มีการแบ่งแยกหน้าที่ภายในหน่วยงานเทคโนโลยีสารสนเทศและระหว่างหน่วยงานเทคโนโลยีสารสนเทศและผู้ใช้งานเป็นเรื่องที่กิจการต้องให้ความสำคัญ นอกจากนี้การเปลี่ยนแปลงข้างต้นยังส่งผลกระทบต่อสภาพแวดล้อมและวิธีการในการปฏิบัติงานของผู้สอบบัญชีด้วย เช่น

- ผู้สอบบัญชีต้องครอบคลุมการตรวจสอบระบบสารสนเทศเป็นส่วนหนึ่งของการสอบบัญชี เนื่องจากเอกสารหลักฐานต่าง ๆ ที่ผู้สอบบัญชีต้องใช้ในการปฏิบัติงาน อาจจะอยู่ในรูปอิเล็กทรอนิกส์เท่านั้น เช่น การอนุมัติในระบบโดยไม่มีการจัดพิมพ์เอกสารออกมาเพื่อลงนามอนุมัติ อีกทั้งในหลายองค์กรมีการรณรงค์ในการลดปริมาณการจัดทำและจัดพิมพ์เอกสารในรูปกระดาษ ยิ่งทำให้เอกสารหลักฐานที่ผู้สอบบัญชีเคยใช้สำหรับดูหลักฐานการอนุมัติรายการและการติดตามรายการหายไป
- ผู้สอบบัญชีต้องทำความเข้าใจประสิทธิผลของการปรับเปลี่ยนการควบคุมของกิจการที่ได้รับผลกระทบจากการใช้ระบบสารสนเทศ เนื่องจากมาตรการควบคุมบางประการที่เคยออกแบบไว้สำหรับระบบการประมวลผลด้วยมืออาจไม่มีประสิทธิผลในระบบสารสนเทศที่ประมวลผลโดยคอมพิวเตอร์ เช่น
  - การควบคุมเพียงการเข้าถึงทางกายภาพและบุคลากรในองค์กร แต่ไม่รวมถึงผู้ใช้งานระบบสารสนเทศภายนอกองค์กร เช่น ลูกค้าที่ทำรายการผ่านตู้เอทีเอ็มหรือผ่านเว็บของกิจการ และผู้ให้บริการเทคโนโลยีสารสนเทศ
  - การแบ่งแยกหน้าที่งานที่ไม่ครอบคลุมถึงหน่วยงานเทคโนโลยีสารสนเทศและผู้ให้บริการเทคโนโลยีสารสนเทศ
  - การตรวจสอบความครบถ้วนและถูกต้องของการประมวลผลข้อมูล โดยการคำนวณซ้ำด้วยมือหรือการกระทบยอด โดยไม่มีการควบคุมการพัฒนาและเปลี่ยนแปลงแก้ไขระบบสารสนเทศ
- กิจการอาจมีหรือไม่มีการลงทุนด้านเทคโนโลยีสารสนเทศ ซึ่งอาจกระทบต่อความอยู่รอดของกิจการ การให้บริการด้านเทคโนโลยีสนเทศที่ต่อเนื่องที่อาจมีผลกระทบต่อลูกค้า ผู้ขาย และการปฏิบัติงานสอบบัญชี มูลค่าของทรัพย์สินเทคโนโลยีสารสนเทศทั้งที่มีตัวตนและไม่มีตัวตน เช่น ในงบการเงินอาจยังบันทึกว่าเครื่องคอมพิวเตอร์ อุปกรณ์เทคโนโลยีสารสนเทศ หรือซอฟต์แวร์ของกิจการยังมีมูลค่าอยู่ ทั้งที่ทรัพย์สินดังกล่าวไม่สามารถใช้งานได้หรือไม่ได้ถูกใช้งานแล้ว ผู้สอบบัญชีจึงจำเป็นต้องมีความเข้าใจเกี่ยวกับการลงทุนด้านเทคโนโลยีสารสนเทศของกิจการด้วย และผลกระทบต่อธุรกิจและการปฏิบัติงานสอบบัญชี เพื่อให้ผู้สอบบัญชีสามารถประเมินความเสี่ยงทางธุรกิจที่สำคัญของกิจการที่อาจมีผลกระทบต่อการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญและสามารถวางแผนการสอบบัญชีให้มีประสิทธิผลและประสิทธิภาพ
- ธุรกิจบางประเภทมีปริมาณรายการค้าเป็นจำนวนมาก เช่น ธุรกิจด้านโทรคมนาคม ประกันภัย ธนาคาร และค้าปลีก เป็นต้น การตรวจสอบข้อมูลในปริมาณมาก ๆ ดังกล่าวด้วยมืออาจต้องใช้กำลังคนและเวลาในการตรวจสอบมาก และอาจไม่ได้ประสิทธิผลและประสิทธิภาพในงานตรวจสอบตามที่ควร การใช้เทคโนโลยีหรือคอมพิวเตอร์ประมวลผลข้อมูลทางการเงินและจัดทำงบการเงินของกิจการ ช่วยให้ผู้สอบบัญชีสามารถใช้เครื่องมือและเทคนิคอัตโนมัติมาช่วยในการตรวจสอบให้มีประสิทธิผลและประสิทธิภาพมากขึ้นได้
- ผู้สอบบัญชีต้องพิจารณาความจำเป็นที่ต้องใช้ผู้เชี่ยวชาญในการตรวจสอบระบบสารสนเทศ อย่างไรก็ดีผู้สอบบัญชีต้องพัฒนาความรู้และทักษะเพื่อให้มีความชำนาญและความรู้ความสามารถอย่างเพียงพอที่จะสามารถวางแผน สั่งการ ควบคุมดูแล และสอบทานงานสอบบัญชีได้อย่างมีประสิทธิผล

ขอบเขตของการตรวจสอบระบบสารสนเทศที่กิจการใช้ในการประมวลผลข้อมูลและจัดทำงบการเงินเพื่อการวางแผนการตรวจสอบ สำหรับกิจการที่ใช้ระบบสารสนเทศสำหรับการประมวลผลข้อมูลและจัดทำงบการเงิน จะประกอบด้วยการทำความเข้าใจระบบสารสนเทศที่กิจการใช้และสภาพแวดล้อมการควบคุมของกิจการที่เกี่ยวข้อง การระบุและประเมินความเสี่ยงที่เกิดจากการใช้ระบบสารสนเทศต่อการประมวลผลข้อมูลและจัดทำงบการเงิน และการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีระดับองค์กรและการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ และการประเมินประสิทธิผลการควบคุมระบบงานที่เป็นส่วนหนึ่งของการประเมินประสิทธิผลการควบคุมระบบงานในระดับกระบวนการธุรกิจและประเภทรายการ

ทั้งนี้รายละเอียดของการทำความเข้าใจระบบสารสนเทศที่กิจการใช้นี้ได้อธิบายในบทที่ 1 การตรวจสอบกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูลและการประเมินความเสี่ยง ของคู่มือฉบับนี้ และในภาคผนวก 5 ข้อพิจารณาในการทำความเข้าใจเทคโนโลยีสารสนเทศของมาตรฐานการสอบบัญชี รหัส 315 (ฉบับปรับปรุง 2564)

ในการประเมินประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศเพื่อกำหนดขอบเขตและประเภทของการตรวจสอบเนื้อหาสาระนั้น ผู้สอบบัญชีต้องพิจารณาประสิทธิผลของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศและการควบคุมระบบงานร่วมกัน เนื่องจากการทำงานของควบคุมระบบงานจะเหมาะสมเพียงพอและทำงานอยู่อย่างสม่ำเสมอเพียงใดนั้นขึ้นอยู่กับการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ดังนั้นก่อนที่ผู้สอบบัญชีจะมั่นใจในการควบคุมระบบงานได้ ผู้สอบบัญชีจะต้องประเมินประสิทธิผลของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศก่อน ในกรณีที่มีข้อบกพร่องในการควบคุมทั่วไปของเทคโนโลยีสารสนเทศหรือในการควบคุมระบบงาน ผู้สอบบัญชีจะต้องวิเคราะห์ว่า ข้อบกพร่องดังกล่าวก่อให้เกิดความเสี่ยงต่อข้อมูลในระบบและงบการเงินในแง่ใด และพิจารณาว่าข้อผิดพลาดนั้นมีสาระสำคัญต่องบการเงินหรือไม่เพียงใด และวางแผนการตรวจสอบเนื้อหาสาระให้ครอบคลุมถึงจุดอ่อนดังกล่าว

ในการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่กิจการใช้ ผู้สอบบัญชีจะพิจารณาถึงกระบวนการด้านเทคโนโลยีสารสนเทศ เช่น กระบวนการควบคุมการเข้าถึง กระบวนการจัดการการเปลี่ยนแปลงโปรแกรมและชุดคำสั่ง หรือการเปลี่ยนแปลงอื่นในสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ กระบวนการจัดการการปฏิบัติการด้านเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียดอธิบายในบทที่ 2 การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ของคู่มือฉบับนี้ และในภาคผนวก 6 ข้อพิจารณาในการทำความเข้าใจการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ของมาตรฐานการสอบบัญชี รหัส 315 (ฉบับปรับปรุง พ.ศ. 2564) สำหรับการตรวจสอบการควบคุมระบบงาน ซึ่งอาจเป็นการควบคุมที่ปฏิบัติด้วยมือ การควบคุมโดยอัตโนมัติ หรือการควบคุมที่ปฏิบัติด้วยมือที่อิงระบบสารสนเทศ ที่มีวัตถุประสงค์เพื่อป้องกัน หรือการค้นพบและแก้ไข ผู้สอบบัญชีจะพิจารณาถึงการควบคุมที่กิจการใช้ในระดับกระบวนการทางธุรกิจ ประเภทของรายการและรายการ เพื่อให้มั่นใจว่ารายการที่เกิดขึ้นและนำเข้าระบบสารสนเทศเป็นรายการที่ได้รับการอนุมัติ มีการบันทึกและประมวลผลโดยระบบสารสนเทศอย่างครบถ้วนและถูกต้อง และมีการจัดทำและแสดงข้อมูลและงบการเงินที่ไม่ขัดต่อข้อเท็จจริงอย่างมีสาระสำคัญ รวมถึงเป็นไปตามสิ่งที่ผู้บริหารได้ให้การรับรองไว้ เช่น การควบคุมการเข้าถึงและให้สิทธิในระดับระบบงาน การควบคุมข้อมูลนำเข้า การควบคุมการประมวลผล และการควบคุมผลลัพธ์ ซึ่งมีรายละเอียดอธิบายในบทที่ 3 การควบคุมระบบงาน ของคู่มือฉบับนี้

นอกจากนี้ในการตรวจสอบกรณีกิจการใช้เทคโนโลยีประมวลผลข้อมูล ผู้สอบบัญชีอาจจำเป็นต้องใช้เครื่องมือและเทคนิคอัตโนมัติช่วยในการตรวจสอบ เนื่องจากข้อมูลรายการค้าและหลักฐานการตรวจสอบอาจมีจำนวนมากและอยู่ในรูปอิเล็กทรอนิกส์ และการควบคุมหลักที่กิจการใช้อาจเป็นการควบคุมโดยอัตโนมัติ ซึ่งรายละเอียดในเรื่องการตรวจสอบโดยใช้คอมพิวเตอร์ช่วยนี้ สามารถศึกษาได้ในบทที่ 4 เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (CAAT)

ผู้สอบบัญชีจำเป็นต้องติดตามความก้าวหน้าด้านเทคโนโลยีอย่างต่อเนื่อง เพื่อให้สามารถระบุความเสี่ยงจากการที่กิจการนำเทคโนโลยีใหม่ ๆ มาใช้ในการประมวลผลข้อมูลและรายการค้า จัดทำรายงานทางการเงิน และประเมินประสิทธิผลของการควบคุมได้ ซึ่งบทที่ 5 เรื่องความเสี่ยง การควบคุม และการตรวจสอบการใช้เทคโนโลยีสมัยใหม่ได้ให้ตัวอย่างของการตรวจสอบกรณีที่กิจการใช้เทคโนโลยีใหม่ ๆ 2 กรณี คือ การตรวจสอบกรณีที่กิจการใช้ระบบคลาวด์ และกรณีที่กิจการใช้ระบบอินเทอร์เน็ตของสรรพสิ่ง (IoT หรือ Internet of Things)

11. บรรณานุกรม

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2555). *มาตรฐานการสอบบัญชี รหัส 330: วิธีปฏิบัติของผู้สอบบัญชีในการตอบสนองต่อความเสี่ยงที่ได้ประเมินไว้.*

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2555). *มาตรฐานการสอบบัญชี รหัส 402: ข้อพิจารณาในการที่ใช้บริการของผู้ให้บริการ.*

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2555). *มาตรฐานการสอบบัญชี รหัส 620: การใช้ผลงานของผู้เชี่ยวชาญของผู้สอบบัญชี.*

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2557). *มาตรฐานการสอบบัญชี รหัส 315 (ฉบับปรับปรุง): การระบุและประเมินความเสี่ยงของการผิดพลาดที่เกิดขึ้นอย่างมีสาระสำคัญ โดยการทำความเข้าใจเกี่ยวกับกิจการและสภาพแวดล้อมของกิจการ.*

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2561). *มาตรฐานการสอบบัญชี รหัส 250 (ฉบับปรับปรุง): การพิจารณากฎหมายและข้อบังคับในการตรวจสอบงบการเงิน.*

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2562). *แนวปฏิบัติตรวจสอบเทคโนโลยีสารสนเทศสำหรับผู้สอบบัญชีอาชีพ.* https://www.tfac.or.th.

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2562). *แนวทางการใช้ดุลยพินิจในการตรวจสอบบัญชีของผู้สอบบัญชี.* https://www.tfac.or.th.

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2564). *รายงานผลการตรวจสอบการควบคุมภายในขององค์กรที่ได้ว่าจ้างผู้สอบบัญชีอื่นที่ถือว่าข้อมูลของรายงานดังกล่าวเป็นสาระสำคัญ.*

ISACA. (2014). *IT control objectives for Sarbanes-Oxley* (3rd Edition).

คณะผู้ทรงคุณวุฒิจัดทำคู่มือด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์

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

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

เลขที่ 133 ถนนสุขุมวิท 21 (อโศก) แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

0 2685 2500 โทรสาร 0 2685 2501

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