ภาคผนวก 2 ของประกาศแนวปฏิบัติ ที่ นป. /2567

การประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี
(IT Risk Assessment: ITRA)

ปัจจุบันระบบงานเทคโนโลยีสารสนเทศ (“ระบบงาน IT”) เข้ามามีบทบาทสำคัญในการดำเนินธุรกิจของสำนักงานสอบบัญชีไทยมากขึ้น โดยระบบงาน IT ถือเป็นทรัพยากรโครงสร้างพื้นฐานที่ช่วยเสริมสร้างประสิทธิภาพการดำเนินงานในด้านต่าง ๆ ของสำนักงานสอบบัญชี เช่น อำนวยความสะดวกในการติดต่อสื่อสารกับลูกค้าสอบบัญชี พัฒนาการบริหารทรัพยากรบุคคลให้มีประสิทธิภาพมากขึ้น พัฒนาระบบการปฏิบัติงานตรวจสอบรายงานทางการเงินให้มีความน่าเชื่อถือและมีประสิทธิภาพมากขึ้น รวมถึงส่งเสริมระบบการบริหารคุณภาพของสำนักงานสอบบัญชี เป็นต้น ซึ่งการที่สำนักงานสอบบัญชีมีแนวโน้มในการนำทรัพยากรทางเทคโนโลยีมาใช้มากขึ้น ส่งผลให้เกิดความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีเพิ่มขึ้นด้วยเช่นกัน นอกจากนี้ International Auditing and Assurance Standards Board (IAASB) ได้เผยแพร่มาตรฐานเกี่ยวกับการบริหารคุณภาพสำนักงานสอบบัญชี (International Standard on Quality Management 1 “ISQM 1”) โดยได้เพิ่มองค์ประกอบในเรื่องทรัพยากรทางเทคโนโลยี เพื่อตอบสนองต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีที่เพิ่มสูงขึ้น ซึ่งมาตรฐานฉบับนี้มีผลบังคับใช้กับสำนักงานสอบบัญชีในตลาดทุนตั้งแต่วันที่ 15 ธันวาคม พ.ศ. 2565 เป็นต้นไป ดังนั้น เพื่อให้ระบบการบริหารคุณภาพของสำนักงานสอบบัญชีในตลาดทุนสอดคล้องตามมาตรฐาน ISQM 1 และตอบสนองต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามด้านไซเบอร์ที่มีพัฒนาการด้านเทคนิคและวิธีการที่หลากหลายมากขึ้น สำนักงาน ก.ล.ต. จึงได้ออกหลักเกณฑ์ในการกำกับดูแลด้านเทคโนโลยีสารสนเทศและการตรวจสอบด้านเทคโนโลยีสารสนเทศสำหรับสำนักงานสอบบัญชีในตลาดทุน โดยมีหลักเกณฑ์ในการประเมินระดับความเสี่ยงของเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี เพื่อนำไปใช้ในการกำหนดรอบระยะเวลาในการจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยมีขั้นตอนการประเมิน ดังนี้

ขั้นตอนที่ 1: การประเมินความซับซ้อนของระบบงาน IT ของสำนักงานสอบบัญชี

สำนักงาน ก.ล.ต. ได้จัดทำแนวทางการประเมินความซับซ้อนของระบบงาน IT ในแต่ละหัวข้อย่อยเพื่อใช้เป็นแนวทางในการประเมินความเสี่ยง ซึ่งมีรายละเอียดดังนี้

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
ระบบงาน IT				
1. โปรแกรมหรือระบบงาน IT ที่ใช้สนับสนุนการบริหารงานการปฏิบัติงานสอบบัญชี (ทั้งระบบหน้าบ้าน (front end) และระบบหลังบ้าน (back end))	โปรแกรมหรือระบบงานที่เกี่ยวข้องกับทรัพยากรทางเทคโนโลยีของสำนักงานสอบบัญชีที่มีวัตถุประสงค์เกี่ยวข้องกับระบบการบริหารคุณภาพของสำนักงานสอบบัญชีอ้างอิงตามมาตรฐานการบริหารคุณภาพ (TSQM1) ย่อหน้าที่ 32 (ฉ) ก99 ให้นำมาพิจารณาในข้อนี้	ใช้โปรแกรมหรือระบบพื้นฐานทั่วไป เช่น Microsoft office **และ** ไม่ได้มีการเปลี่ยนแปลงการทำงานของโปรแกรม (customization) ตามความต้องการเฉพาะของสำนักงานสอบบัญชี	- ใช้โปรแกรมหรือระบบเฉพาะสำหรับงานสอบบัญชีซึ่งได้จากการซื้อมา (off the shelf) เช่น audit software **หรือ** - ใช้โปรแกรมหรือระบบพื้นฐานทั่วไปที่ได้ปรับเปลี่ยนตามความต้องการของสำนักงานสอบบัญชีโดยเฉพาะก่อนนำมาใช้งาน (customization)	สำนักงานสอบบัญชีมีการใช้โปรแกรมหรือระบบที่ได้พัฒนาขึ้นภายในสำนักงานสอบบัญชีเองไม่ว่าจะเป็นการจ้างผู้ผลิตภายนอกพัฒนาหรือ พัฒนาเองโดยหน่วยงานภายในสำนักงานสอบบัญชี รวมถึงสำนักงานเครือข่าย (network firm) หรือกรณีอื่นใดนอกเหนือจากการใช้โปรแกรมหรือระบบที่ถูกกำหนดไว้เป็นระดับต่ำหรือระดับปานกลาง
2. การจัดเก็บและเรียกใช้ข้อมูล	-	จัดเก็บและเรียกใช้ข้อมูลในเครื่องคอมพิวเตอร์ของสำนักงานสอบบัญชี รวมถึง Server หรือ ระบบเครือข่ายคอมพิวเตอร์แบบเชื่อมโยงระยะใกล้ (LAN) ของสำนักงานสอบบัญชี หรือจัดเก็บในรูปแบบกระดาษ	มีการจัดเก็บและเรียกใช้ข้อมูล**บางส่วนจาก cloud** (สัดส่วนการจัดเก็บและเรียกใช้ข้อมูลจาก cloud **ต่ำกว่า 50%** ของข้อมูลทั้งหมดของสำนักงานสอบบัญชี) หรือ มีการใช้storage ในการจัดเก็บข้อมูลและเรียกใช้ข้อมูลที่ดำเนินการโดยผู้ให้บริการ	มีการจัดเก็บและเรียกใช้ข้อมูล**ส่วนใหญ่จากcloud** (สัดส่วนการจัดเก็บและเรียกใช้ข้อมูลจาก cloud **50% ขึ้นไป**ของข้อมูลทั้งหมดของสำนักงานสอบบัญชี)
3. จำนวน laptop PC tablet, mobile devices, removeable storage หรือ อุปกรณ์อื่น ๆ ซึ่งเป็นอุปกรณ์ส่วนตัวของพนักงาน (Bring Your Own Device) ที่สามารถเชื่อมต่อเครือข่ายภายในของสำนักงานสอบบัญชี หรือเข้าถึงข้อมูลหรือฐานข้อมูลภายในของสำนักงานสอบบัญชีได้ (รวมถึง email ด้วย)	-	0 - 500 อุปกรณ์	501 – 1000 อุปกรณ์	ตั้งแต่ 1001 อุปกรณ์ขึ้นไป
4. สิทธิ์ในการเข้าถึงระบบงาน หรือฐานข้อมูลของสำนักงานสอบบัญชีด้วยอุปกรณ์ส่วนตัวของพนักงาน	เลือกจากระดับสิทธิ์สูงสุดที่สำนักงานสอบบัญชีอนุญาตให้พนักงานเข้าถึงระบบได้ เช่น อุปกรณ์ส่วนตัวของพนักงานทั่วไปได้สิทธิ์เข้าถึง email เท่านั้น ในขณะที่	ไม่สามารถเข้าถึงระบบงานหรือฐานข้อมูลของสำนักงานสอบบัญชีได้	สามารถเข้าถึง email ได้เท่านั้น	สามารถเข้าถึง email และระบบงานและฐานข้อมูลของสำนักงานสอบบัญชีได้ หรือไม่มีข้อจำกัดในการเข้าถึงเสมือนใช้อุปกรณ์ของสำนักงาน

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
	อุปกรณ์ส่วนตัวของหัวหน้าสำนักงานสอบบัญชี ไม่มีข้อจำกัดในการใช้งานสำนักงานสอบบัญชีต้องเลือกประเมินข้อนี้เป็นระดับสูง			สอบบัญชี
5. จำนวนหน่วยงานภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบงานหรือฐานข้อมูลของสำนักงานสอบบัญชี เช่น ลูกค้า หน่วยงานกำกับดูแล sub-contract และ outsource (ไม่รวมบริษัทในเครือของสำนักงานสอบบัญชี)	เช่น ลูกค้า 100 บริษัท นับเป็น 100 แห่ง หรือ หน่วยงานกำกับดูแล 10 องค์กร นับเป็น 10 แห่ง เป็นต้น	0 - 5 แห่ง	6 -10 แห่ง	ตั้งแต่ 11 แห่งขึ้นไป
6. ช่องทางในการเข้าถึงระบบงานหรือฐานข้อมูลของสำนักงานสอบบัญชี โดยหน่วยงานภายนอก (ไม่รวมบริษัทในเครือของสำนักงานสอบบัญชี)	-	ไม่สามารถเข้าถึงระบบงานหรือฐานข้อมูลได้	สามารถเข้าถึงระบบงานหรือฐานข้อมูลได้ผ่าน leased line (การเชื่อมต่อสายอินเทอร์เน็ตโดยตรงโดยไม่ผ่านเครือข่ายวงนอก) หรือผ่าน VPN over leased line (เชื่อมต่ออุปกรณ์ด้วยเครือข่ายส่วนตัวเสมือนผ่านสายอินเทอร์เน็ตแบบเช่าใช้)	สามารถเข้าถึงระบบงานหรือฐานข้อมูลผ่านการเชื่อมต่ออุปกรณ์ผ่านอินเทอร์เน็ตทั่วไปที่ไม่ได้ต่อสายอินเทอร์เน็ตแบบเช่าใช้ (leased line)
7. การเชื่อมต่อระบบงาน IT ของสำนักงานสอบบัญชีกับระบบงานของหน่วยงานภายนอกที่ไม่รวมบริษัทในเครือของสำนักงานสอบบัญชี (นอกเหนือจากการส่ง email)	เช่น หากฝ่ายใดฝ่ายหนึ่งมีการสร้างข้อมูลในระบบ ข้อมูลนั้นจะถูกส่งไปยังอีกฝ่ายอัตโนมัติ เช่น ลูกค้า A มีการบันทึกบัญชีขายรายวัน และสำนักงานสอบบัญชีสามารถเรียกดูได้จากระบบของสำนักงานสอบบัญชีได้เองแบบทันที (real-time)	**ไม่มี**การเชื่อมต่อระบบงาน IT ที่ใช้ในการรับส่งรายการธุรกรรม หรือเชื่อมต่อข้อมูลในระบบโดยตรงกับบุคคล/กิจการภายนอกผ่านเครือข่ายอินเทอร์เน็ต	**มี**การเชื่อมต่อระบบงาน IT ที่ใช้ในการรับส่งรายการธุรกรรม หรือเชื่อมต่อข้อมูลในระบบโดยตรงกับบุคคล/กิจการภายนอกผ่านเครือข่ายอินเทอร์เน็ต โดยหน่วยงานที่มีการเชื่อมต่อกับสำนักงานสอบบัญชี **มีจำนวน 1 - 10 ราย**	**มี**การเชื่อมต่อระบบงาน IT ที่ใช้ในการรับส่งรายการธุรกรรม หรือเชื่อมต่อข้อมูลในระบบโดยตรงกับบุคคล/กิจการภายนอกผ่านเครือข่ายอินเทอร์เน็ต โดยหน่วยงานที่มีการเชื่อมต่อกับสำนักงานสอบบัญชี**มีจำนวนตั้งแต่ 11 รายขึ้นไป**
8. ช่องทางการแบ่งปันข้อมูล (shared drive) กับหน่วยงานภายนอกที่ไม่รวมบริษัทในเครือของสำนักงานสอบบัญชี (นอกเหนือจาก email)	-	**ไม่มี** shared drive หรือ platform ไว้ใช้แบ่งปันข้อมูลกับหน่วยงานภายนอก	**ใช้** shared drive หรือ platform ของ service provider สำหรับแบ่งปันข้อมูลให้กับหน่วยงานภายนอก เช่น OneDrive, Google Drive หรือ Dropbox เป็นต้น	**ใช้** shared drive หรือ platform ที่สำนักงานสอบบัญชีพัฒนาขึ้นมาเอง เช่น - พัฒนาโดยoutsource - พัฒนาโดยหน่วยงานภายในสำนักงานสอบบัญชี - พัฒนาโดยสำนักงานเครือข่าย (network firms)

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
9. การนำเทคโนโลยีอุบัติใหม่ (“emerging technologies”) มาใช้งานในสำนักงานสอบบัญชีจริงในปีที่ผ่านมา	- พิจารณาเฉพาะงานที่เกี่ยวข้องกับทรัพยากรทางเทคโนโลยีของสำนักงานสอบบัญชีที่มีวัตถุประสงค์เกี่ยวข้องกับระบบการบริหารคุณภาพของสำนักงานสอบบัญชี โดยอ้างอิงตามมาตรฐานการบริหารคุณภาพ (TSQM1) ย่อหน้า 32 (ฉ) ก99 - ตัวอย่าง emerging technologies ที่มีการนำมาใช้ในงานข้างต้น เช่น artificial intelligence (AI) machine learning (ML) robotics หรือ blockchain เป็นต้น **<u>ตัวอย่าง</u>** สำนักงานสอบบัญชีมีการนำเอา robotic process automation มาใช้ในการตรวจสอบในทุก ๆ engagements ที่ถูกประเมินว่ามีความเสี่ยงที่เกี่ยวเนื่องกับการทุจริต โดยนำมาใช้จริงในปี 2566 เป็นต้นไป กรณีเช่นนี้ให้นับเป็น 1 โครงการนับแต่วันที่มีการใช้จริง	**ไม่มี**การนำ emerging technologies มาช่วยในการทำงานในปีที่ผ่านมา	**มี**การนำ emerging technologies มาช่วยในการทำงาน จำนวน 1-3 **โครงการ (project) ในปีที่ผ่านมา**	**มี**การนำ emerging technologies มาช่วยในการทำงาน **ตั้งแต่ 4 โครงการ (project) ขึ้นไปในปีที่ผ่านมา**
10. การนำเทคโนโลยี หรือ application มาใช้เป็นครั้งแรกในปีที่ผ่านมา ไม่รวมเทคโนโลยีอุบัติใหม่ (emerging technologies)	- พิจารณาเฉพาะงานที่เกี่ยวข้องกับทรัพยากรทางเทคโนโลยีของสำนักงานสอบบัญชีที่มีวัตถุประสงค์เกี่ยวข้องกับระบบการบริหารคุณภาพของสำนักงานสอบบัญชี โดยอ้างอิงตามมาตรฐานการบริหารคุณภาพ (TSQM1) ย่อหน้าที่ 32 (ฉ) ก99	**ไม่มี**การนำเทคโนโลยี หรือ application มาใช้เป็นครั้งแรกในปีที่ผ่านมา	**มี**การนำ 1-2 เทคโนโลยี หรือ application มาใช้เป็นครั้งแรกในปีที่ผ่านมา	**มี**การนำตั้งแต่ 3 เทคโนโลยี หรือ application ขึ้นไป มาใช้เป็นครั้งแรกในปีที่ผ่านมา
11. จำนวนโปรแกรมสำเร็จรูป หรือระบบปฏิบัติการที่หมดอายุหรือตกรุ่น หรือไม่ได้รับการสนับสนุนจากผู้พัฒนา (End-of-life หรือ End-of-support) แต่สำนักงานสอบบัญชียังคงใช้งานอยู่ในปัจจุบัน	**<u>ตัวอย่าง</u>** - เครื่องคอมพิวเตอร์ จำนวน 13 เครื่อง ติดตั้ง Window XP ให้นับจำนวนระบบงานที่ End of Life/ End of Support นับเป็น 1 ระบบ - เครื่องคอมพิวเตอร์ จำนวน 1 เครื่อง ติดตั้ง Window XP และ	0 - 2 โปรแกรมหรือระบบ	3-7 โปรแกรมหรือระบบ	ตั้งแต่ 8 โปรแกรมหรือระบบขึ้นไป

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
	Oracle 11g ซึ่งทั้งสองระบบไม่ได้รับการสนับสนุนจากผู้พัฒนาแล้ว นับเป็น 2 ระบบ			
12. จำนวนงานบริการด้านเทคโนโลยีสารสนเทศ ที่สำนักงานสอบบัญชีใช้บริการจากผู้ให้บริการภายนอกที่ไม่รวมบริษัทในเครือของสำนักงานสอบบัญชี ภายในรอบระยะเวลา 3 ปีที่ผ่านมา	**ตัวอย่างการนับจำนวนงานที่ใช้บริการจากผู้ให้บริการภายนอก (outsource)** หากผู้ให้บริการจากภายนอกให้การบริการที่แตกต่างกันสำหรับงานแต่ละงาน ให้นับแยกงาน เช่น - ว่าจ้างวางระบบเครือข่าย (network) นับเป็น 1 บริการ - ดูแลระบบ server/website/ security นับเป็น 3 บริการ	0 - 5 งานบริการ	6 -10 งานบริการ	ตั้งแต่ 11 งานบริการขึ้นไป
13. จำนวนบริษัทในเครือ หรือเครือข่ายของสำนักงานสอบบัญชีทั้งในประเทศและต่างประเทศทั้งหมด ที่เชื่อมต่อกับระบบงานของสำนักงานสอบบัญชีได้ เช่น มีสิทธิ์เข้าถึงระบบข้อมูลของลูกค้า ระบบข้อมูลพนักงาน เป็นต้น	-	0 - 5 แห่ง	6 -10 แห่ง	ตั้งแต่ 11 แห่งขึ้นไป
14. อัตรากำลังคนตามโครงสร้างของสำนักงานสอบบัญชี ณ วันที่ทำการประเมิน (หรือจากการประมาณการที่ดีที่สุด)	ได้แก่ จำนวนพนักงานประจำ ลูกจ้างประจำ และ ลูกจ้างชั่วคราวของบริษัท รวมถึงหุ้นส่วนและผู้บริหาร และพนักงานบริษัทในเครือหรือ สำนักงานเครือข่ายที่มาทำงานให้สำนักงานสอบบัญชีและมีสิทธิ์เข้าถึงระบบของสำนักงานสอบบัญชี (ไม่รวม outsource)	0 - 100 คน	101-500 คน	ตั้งแต่ 501 คนขึ้นไป
15. อัตราการลาออกของ IT staff (turnover rate) ณ วันที่ทำการประเมิน หมายเหตุ: ให้รวมเจ้าหน้าที่ outsource ที่ทำงานเต็มเวลากับสำนักงานสอบบัญชี	ตัวอย่างการคำนวณอัตราการลาออก อัตราการลาออก = จำนวนบุคลากรที่ลาออกทั้งหมดในรอบปีนั้น ๆ / จำนวนบุคลากรเฉลี่ยในปีนั้น เช่น จำนวนพนักงาน IT ทั้งหมด รวมลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ outsource - ณ 1 มกราคม 2565 = 100 คน - ณ 31 ธันวาคม 2565 = 70 คน	0 - 20 %	21% - 50%	ตั้งแต่ 51% ขึ้นไป

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
	ดังนั้น จำนวนบุคลากรเฉลี่ยของปี 2565 = (100+70) ÷ 2 = **85 คน** - จำนวนบุคลากรที่ลาออกรวม ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ outsource ที่ลาออกหรือย้ายไป ทั้งหมดในรอบปี 2565 = 40 คน ดังนั้น **อัตราการลาออกของ IT staff** = (40 ÷ 85) * 100 = 47%			
การถูกคุกคามทางไซเบอร์				
16. จำนวนครั้งที่ระบบงาน IT ของสำนักงานสอบบัญชีถูกโจมตีในรอบปีที่ผ่านมา	เช่น virus/malware, phishing email หรือ phishing phone หรือ ransomware เป็นต้น โดยให้หารเฉลี่ยต่อวันของจำนวนที่ถูกโจมตีในรอบหนึ่งปีที่ผ่านมา สำหรับกรณีมีผลเสียหายและไม่มีผลเสียหาย (นับเป็น incident ที่เกิด)	0 - 5 ครั้งต่อวัน	6 – 50 ครั้งต่อวัน	ตั้งแต่ 51 ครั้งต่อวัน
17. จำนวนครั้งที่ระบบงาน IT ของสำนักงานสอบบัญชีถูกโจมตีในรอบปีที่ผ่านมา และที่มีผลเสียหายเกิดขึ้น (monetary and non-monetary)	เช่น โดน virus/malware โจมตีทำให้ข้อมูลเสียหาย, โดนเรียกค่าไถ่ข้อมูล (ransomware) หรือทำให้เกิดความเข้าใจผิดจากการที่ผู้โจมตีใช้ Deepfake หลอกเอาข้อมูลจากบุคลากรของสำนักงานสอบบัญชี เป็นต้น	ไม่มี	1 - 2 ครั้งต่อปี	ตั้งแต่ 3 ครั้งต่อปีขึ้นไป

หมายเหตุ: ในการตอบแบบประเมินข้างต้น หากสำนักงานสอบบัญชีไม่สามารถหาจำนวนของคำตอบที่แน่นอนได้ ให้ใช้การประมาณการที่ดีที่สุดแทน หรือหากเป็นการคำนวณให้ใช้การปัดเศษทศนิยมขึ้นหากทศนิยมที่ได้มากกว่าเท่ากับ 0.5 หรือปัดทศนิยมลงหากทศนิยมที่ได้น้อยกว่า 0.5

จากการประเมินความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีข้างต้น ให้สำนักงานสอบบัญชีหาผลรวมของจำนวนข้อในแต่ละระดับเพื่อประเมินผลความซับซ้อนทางเทคโนโลยีในภาพรวม ดังนี้

1. ความซับซ้อนทางเทคโนโลยีสารสนเทศระดับต่ำ
    a. จำนวนข้อที่ประเมินอยู่ในระดับต่ำ >= 9 ข้อ **และ** ไม่มีข้อใดได้ระดับสูง
2. ความซับซ้อนทางเทคโนโลยีสารสนเทศระดับกลาง
    a. จำนวนข้อที่ประเมินอยู่ในระดับต่ำ >= 9 ข้อ **แต่** มีอย่างน้อย 1 ข้อได้ระดับสูง
    b. จำนวนข้อที่ประเมินอยู่ในระดับกลางและระดับสูง >= 9 ข้อ **และ** จำนวนข้อที่ประเมินอยู่ในระดับกลาง > ระดับสูง
3. ความซับซ้อนทางเทคโนโลยีสารสนเทศระดับสูง
    a. จำนวนข้อที่ประเมินอยู่ในระดับกลางและระดับสูง >= 9 ข้อ **และ** จำนวนข้อที่ประเมินอยู่ในระดับสูง >= กลาง

ตัวอย่างที่ 1

สำนักงานสอบบัญชี A ทำแบบประเมินความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีได้ผลดังนี้

ระดับต่ำ 9 ข้อ ระดับกลาง 3 ข้อ และ ระดับสูง 5 ข้อ

พบว่า จำนวนข้อที่ประเมินอยู่ในระดับต่ำ = 9 ข้อ **และ** มีจำนวนข้อที่ประเมินอยู่ในระดับสูงอย่างน้อย 1 ข้อ ดังนั้น ความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี A อยู่ใน**ระดับกลาง**

ตัวอย่างที่ 2

สำนักงานสอบบัญชี B ทำแบบประเมินความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีได้ผลดังนี้

ระดับต่ำ 8 ข้อ ระดับกลาง 4 ข้อ และ ระดับสูง 5 ข้อ

พบว่า จำนวนข้อที่ประเมินอยู่ในระดับกลางและระดับสูง (9 ข้อ) >= 9 ข้อ และ และจำนวนข้อที่ประเมินอยู่ในระดับสูง > ระดับกลาง ดังนั้น ความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี B อยู่ใน**ระดับสูง**

โดยผลของความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี ในขั้นตอนที่ 1 จะนำไปคำนวณในขั้นตอนที่ 3: ประเมินความเสี่ยงเกี่ยวกับระบบงาน IT ในภาพรวมของสำนักงานสอบบัญชีต่อไป

ขั้นตอนที่ 2: การประเมินผลกระทบต่อตลาดทุนโดยการพิจารณามูลค่าหลักทรัพย์ตามราคาตลาด (market capitalization) ของลูกค้าสอบบัญชีที่เป็นบริษัทจดทะเบียน ณ วันสิ้นปีปฏิทินล่าสุด

โดยพิจารณาจากมูลค่าหลักทรัพย์ตามราคาตลาดรวมของลูกค้าสอบบัญชี ณ วันสิ้นปีปฏิทินล่าสุด อ้างอิงจากตารางด้านล่างนี้

ระดับผลกระทบต่อตลาดทุน (X)	**มูลค่าหลักทรัพย์ตามราคาตลาดรวมของลูกค้าสอบบัญชี ณ วันสิ้นปีปฏิทินล่าสุด (y)** หน่วย:บาท
ระดับสูง (H)	y >= 1 ล้านล้าน
ระดับกลางค่อนไปทางสูง (MH)	2 แสนล้าน <= y < 1 ล้านล้าน
ระดับกลางค่อนไปทางต่ำ (ML)	2 หมื่นล้าน <= y < 2 แสนล้าน
ระดับต่ำ (Low)	y < 2 หมื่นล้าน

ตัวอย่าง: ณ วันที่ 1 มกราคม 2569 สำนักงานสอบบัญชี A ประเมินผลกระทบต่อตลาดทุนโดยการพิจารณามูลค่าหลักทรัพย์ตามราคาตลาดรวมของลูกค้าสอบบัญชีทั้งหมด ณ วันที่ 30 ธันวาคม 2568 (วันสุดท้ายของปีล่าสุดที่ตลาดหลักทรัพย์แห่งประเทศไทยเปิดให้มีการซื้อขายหลักทรัพย์) ซึ่งประกอบไปด้วยลูกค้าบริษัทจดทะเบียน 2 ราย คือ บมจ. A และ บมจ. B จากฐานข้อมูลของตลาดหลักทรัพย์แห่งประเทศไทยแสดงข้อมูล ดังนี้

- มูลค่าหลักทรัพย์ตามราคาตลาดรวมของลูกค้าสอบบัญชี บมจ. A และ บมจ. B ณ วันที่ 30 ธันวาคม 2568 = 1.9 แสนล้านบาท
- ระดับของผลกระทบต่อตลาดทุนจากมูลค่าหลักทรัพย์ตามราคาตลาด ณ วันสิ้นปีล่าสุด คือระดับกลางค่อนไปทางต่ำ (ML)

ขั้นตอนที่ 3: ประเมินความเสี่ยงเกี่ยวกับระบบงาน IT ในภาพรวมของสำนักงานสอบบัญชี

การประเมินความเสี่ยงในภาพรวมของระบบงาน IT ของสำนักงานสอบบัญชี มีผลต่อการกำหนดความถี่ในการตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีโดยผู้เชี่ยวชาญ ตามหลักเกณฑ์ในการกำกับดูแลและตรวจสอบด้าน IT สำหรับสำนักงานสอบบัญชี ซึ่งความเสี่ยงดังกล่าวจะพิจารณาจากผลการประเมินที่ได้จาก 2 ขั้นตอนแรก คือ

ขั้นตอนที่ 1: ผลการประเมินความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี

ขั้นตอนที่ 2: ระดับของผลกระทบต่อตลาดทุนจากมูลค่าหลักทรัพย์ตามราคาตลาด ณ วันสิ้นปีล่าสุด

โดยมีรายละเอียด ดังนี้

ระดับของผลกระทบต่อตลาดทุน	ผลการประเมินความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี		
	ต่ำ	กลาง	สูง
ระดับสูง (H)	ทุกปี	ทุกปี	ทุกปี
ระดับกลางค่อนไปทางสูง (MH)	2 ปี/ครั้ง	2 ปี/ครั้ง	ทุกปี
ระดับกลางค่อนไปทางต่ำ (ML)	3 ปี/ครั้ง	3 ปี/ครั้ง	2 ปี/ครั้ง
ระดับต่ำ (Low)	3 ปี/ครั้ง	3 ปี/ครั้ง	3 ปี/ครั้ง

โดยรอบความถี่ของระยะเวลาที่คำนวณข้างต้น คือ ความถี่ของระยะเวลาที่สำนักงานสอบบัญชีจะต้องจัดให้มีการตรวจสอบด้าน IT แบบเต็มรูปแบบ (“full-scope”)[1] ตามการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี โดยผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ ซึ่งรอบการตรวจสอบให้เป็นไปตามนโยบายและแนวปฏิบัติที่สำนักงานสอบบัญชีกำหนด

<u>การกำหนดรอบการตรวจสอบและกรณีมีการเปลี่ยนรอบตรวจสอบ</u>

สำนักงานสอบบัญชีควรกำหนดรอบการตรวจสอบครอบคลุมระยะเวลาอย่างน้อย 12 เดือน และรอบการตรวจถัดไปควรมีวันที่เริ่มต้นและสิ้นสุดสอดคล้องกับรอบการตรวจครั้งก่อนหน้าที่เคยนำส่งรายงานผลการตรวจสอบระบบงาน IT ให้สำนักงาน ก.ล.ต.

กรณีสำนักงานสอบบัญชีมีความประสงค์จะเปลี่ยนแปลงรอบการตรวจในปัจจุบัน สำนักงานสอบบัญชีต้องแจ้งการเปลี่ยนแปลงรอบการตรวจใหม่ภายใน 30 วันนับแต่มีการเปลี่ยนแปลงแก่สำนักงาน ก.ล.ต.

อย่างไรก็ดี หากสำนักงานสอบบัญชีมีการเปลี่ยนแปลงรอบการตรวจสอบใหม่ สำนักงานสอบบัญชีต้องจัดให้มีกระบวนการตรวจสอบเพื่อให้มาซึ่งหลักฐานที่สามารถให้ความเชื่อมั่นว่าระบบทรัพยากรทางเทคโนโลยีตามมาตรฐานการบริหารคุณภาพและการควบคุมที่เกี่ยวข้องระหว่างรอบการตรวจสอบเดิมและรอบการตรวจสอบใหม่ยังคงมีอยู่ และมีประสิทธิภาพ

<u>ตัวอย่าง</u> ณ ตอนปี 2568 สำนักงานสอบบัญชีได้ทำการตรวจสอบด้าน IT แบบ full-scope ครั้งแรก ครอบคลุมระยะเวลา ตั้งแต่ 1 มิถุนายน 2567 ถึง 31 พฤษภาคม 2568 และทำการประเมิน ITRA ครั้งแรกในปีเดียวกันได้รอบการตรวจ 3 ปี/ครั้ง ดังนั้น สำนักงานสอบบัญชีต้องจัดให้มีการตรวจสอบด้าน IT แบบ full-scope โดยผู้เชี่ยวชาญอีกครั้งภายในปี 2571 โดยครอบคลุมระยะเวลา 1 มิถุนายน 2570 ถึง 31 พฤษภาคม 2571 ทั้งนี้สำหรับปีที่ไม่ได้ตรวจแบบ full-scope ให้ดำเนินการตามหัวข้อ **แนวปฏิบัติสำหรับปีที่สำนักงานสอบบัญชีไม่ได้ถูกกำหนดให้ดำเนินการตรวจแบบ full-scope**

[1] อ้างอิง การกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี คำจำกัดความข้อที่ 2

<u>การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง</u>[2]

1. สำนักงานสอบบัญชีต้องนำส่งเอกสารดังต่อไปนี้ที่ผ่านการอนุมัติจากหัวหน้าสำนักงานสอบบัญชีแล้วต่อสำนักงาน ก.ล.ต. ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ก.ล.ต. ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบของสำนักงานสอบบัญชีที่ต้องถูกตรวจสอบด้านเทคโนโลยีสารสนเทศตาม ITRA หรือภายในระยะเวลาที่ได้รับการผ่อนผันจากสำนักงาน ก.ล.ต.
    - รายงานผลการตรวจสอบระบบงาน IT แบบ full-scope โดยผู้เชี่ยวชาญ
    - root cause analysis และ remediation plan กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง
    - ITRA ที่ประเมินใหม่ เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง
2. จัดเก็บเอกสารตามข้อ 1. เป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

<u>การขอผ่อนผัน</u>

กรณีมีเหตุผลจำเป็นและสมควรที่ทำให้สำนักงานสอบบัญชีไม่สามารถดำเนินการตรวจสอบระบบงาน IT ได้ภายในรอบระยะเวลาตามที่ผล ITRA ล่าสุดกำหนดไว้ หรือสำนักงานสอบบัญชีไม่สามารถนำส่งเอกสารประกอบการตรวจสอบระบบงาน IT ได้ภายในระยะเวลาตามที่หัวข้อ **การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้องกำหนด** สำนักงานสอบบัญชีต้องยื่นหนังสือขอผ่อนผันการดำเนินการตรวจสอบระบบงาน IT ต่อสำนักงาน ก.ล.ต. ตามคู่มือสำหรับประชาชนก่อนสิ้นสุดระยะเวลาที่กำหนดให้สำนักงานสอบบัญชีต้องจัดทำและส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้องให้แก่สำนักงาน ก.ล.ต. อ้างอิงรอบการตรวจปัจจุบัน พร้อมทั้งชี้แจงเหตุผลและความจำเป็นในการขอผ่อนผันและแจ้งกำหนดระยะเวลาใหม่ที่จะดำเนินการตรวจสอบด้าน IT หรือ จัดส่งเอกสารนั้น ซึ่งสำนักงาน ก.ล.ต. จะพิจารณาผ่อนผันเป็นรายกรณีตามความจำเป็นและสมควร

<u>ตัวอย่าง</u> ณ ตอนปี 2568 สำนักงานสอบบัญชีได้ทำการประเมิน ITRA ครั้งแรกได้รอบการตรวจ 3 ปี/ครั้ง ดังนั้น สำนักงานสอบบัญชีต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศแบบ full-scope โดยผู้เชี่ยวชาญอีกครั้งภายในปี 2571 โดยสำนักงานสอบบัญชีได้กำหนดรอบการตรวจสอบเริ่ม 1 มกราคม 2571 – 31 ธันวาคม 2571 อย่างไรก็ดี หากสำนักงานสอบบัญชีไม่สามารถดำเนินการตรวจสอบตามรอบการตรวจสอบที่กำหนดและไม่สามารถนำส่งรายงานได้ภายใน 31 พฤษภาคม 2572 สำนักงานสอบบัญชีจะต้องยื่นหนังสือขอผ่อนผันการดำเนินการตรวจสอบระบบงาน IT ต่อสำนักงาน ก.ล.ต. ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบล่าสุดที่จะต้องจัดทำและส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้องให้แก่สำนักงาน ก.ล.ต. พร้อมทั้งชี้แจง

[2] อ้างอิง การกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี
หมวดที่ 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) ข้อ 5 การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง

เหตุผลและความจำเป็นในการขอผ่อนผันและแจ้งกำหนดระยะเวลาใหม่ที่จะดำเนินการตรวจสอบด้าน IT

<u>วิธีปฏิบัติในช่วงเปลี่ยนแปลง (transitional period):</u> สำหรับสำนักงานสอบบัญชีในตลาดทุนที่มีผู้สอบบัญชีในสังกัดได้รับความเห็นชอบจากสำนักงาน ก.ล.ต. ก่อนหน้าที่ประกาศฉบับนี้จะมีผลบังคับใช้

การเริ่มใช้หลักเกณฑ์ในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) เป็นครั้งแรก สำนักงานสอบบัญชีในตลาดทุนต้องดำเนินการตรวจสอบระบบงาน IT แบบเต็มรูปแบบ (“full-scope”) โดยผู้เชี่ยวชาญภายในปี 2569 เป็นครั้งแรกและนำส่งเอกสาร ได้แก่

- รายงานผลการตรวจสอบระบบงาน IT แบบ full-scope โดยผู้เชี่ยวชาญ
- root cause analysis และ remediation plan กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง
- ITRA ที่ประเมินครั้งแรก เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง

โดยสำนักงานสอบบัญชีจะต้องจัดเตรียมและนำส่งเอกสารข้างต้น ภายในระยะเวลาที่หัวข้อ **การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง** กำหนดไว้ และไม่เกินวันที่ 31 พฤษภาคม 2570

<u>วิธีปฏิบัติสำหรับสำนักงานสอบบัญชีใหม่ที่จะเข้ามาปฏิบัติงานในตลาดทุนเป็นครั้งแรก ให้ดำเนินการตามข้อกำหนดด้านล่างตั้งแต่วันที่ประกาศมีผลบังคับใช้</u>

สำนักงานสอบบัญชีใหม่ต้องจัดให้มีการดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) เป็นครั้งแรก และจัดส่งเอกสารตามด้านล่างมายังสำนักงาน ก.ล.ต. เพื่อเป็นเอกสารประกอบการแสดงคุณสมบัติของผู้สอบบัญชีในสังกัดสำนักงานสอบบัญชีที่จะยื่นขอความเห็นชอบเป็นผู้สอบบัญชีในตลาดทุนเป็นครั้งแรก

- รายงานผลการตรวจสอบระบบงาน IT แบบ full-scope โดยผู้เชี่ยวชาญ
- root cause analysis และ remediation plan กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง
- ITRA ที่ประเมินครั้งแรก เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง

โดยเอกสารที่นำส่งข้างต้น ณ วันที่นำส่ง ต้องมีอายุไม่เกิน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบ

<u>แนวปฏิบัติสำหรับปีที่สำนักงานสอบบัญชีไม่ได้ถูกกำหนดให้ดำเนินการตรวจแบบ full-scope</u>

ในรอบปีที่ไม่ได้ถูกกำหนดให้ตรวจสอบด้าน IT แบบ full-scope โดยผู้เชี่ยวชาญ สำนักงานสอบบัญชีต้องกำหนดขอบเขตของการตรวจสอบภายในด้าน IT ให้เหมาะสมกับความเสี่ยงที่เกี่ยวข้องกับสำนักงานสอบบัญชี

โดยอ้างอิงจากกระบวนการบริหารจัดการความเสี่ยงด้าน IT[3] ที่กำหนดให้มีการประเมินความเสี่ยงด้านทรัพยากรทางเทคโนโลยี (risk assessment) อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญในรอบระยะเวลาที่ไม่ได้กำหนดให้ตรวจแบบ full-scope เพื่อนำไปใช้การวางแผนและดำเนินการตรวจสอบภายในด้าน IT ในปีนั้น ๆ ซึ่งการตรวจสอบในรอบการตรวจนี้อาจจะไม่ครอบคลุมทุกข้อกำหนดตามการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี ทั้งนี้ สำนักงานสอบบัญชีต้องกำหนดนโยบายและแนวปฏิบัติในการประเมินและตอบสนองต่อความเสี่ยงอย่างเหมาะสม รวมถึงพิจารณาความจำเป็นที่ต้องใช้ผู้เชี่ยวชาญในการตรวจสอบด้าน IT

อย่างไรก็ดี สำนักงานสอบบัญชีต้องจัดส่งรายงานผลการตรวจสอบด้าน IT โดยผู้เชี่ยวชาญให้กับสำนักงาน ก.ล.ต. ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบล่าสุดที่จะต้องจัดทำและส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้องให้แก่สำนักงาน ก.ล.ต. หากการตรวจสอบด้าน IT ในปีนั้นมีเหตุการณ์ที่สำคัญดังต่อไปนี้

- หากพบว่ามีประเด็นข้อสังเกตที่สำคัญ[4] ที่ต้องได้รับการแก้ไขจากผลการตรวจรอบก่อนโดยผู้เชี่ยวชาญ สำนักงานสอบบัญชีต้องรวมประเด็นข้อสังเกตที่สำคัญเข้ามาเป็นส่วนหนึ่งของขอบเขตการตรวจสอบด้าน IT และดำเนินการตรวจสอบและติดตามผลการแก้ไขในเรื่องนั้นต่อเนื่องไปทุกปีจนกว่าจะแก้ไขแล้วเสร็จ
- การเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญ
    - หากมีการปรับปรุงหรือเพิ่มระบบงาน IT ที่มีนัยสำคัญ[5] ในรอบปี และระบบดังกล่าวเริ่มใช้งานจริง (go-live) แล้วในปีนั้น ให้สำนักงานสอบบัญชีเพิ่มระบบดังกล่าว รวมถึงระบบอื่น ๆ ที่ได้รับผลกระทบเข้ามาเป็นส่วนหนึ่งของขอบเขตการตรวจสอบด้าน IT และดำเนินการตรวจสอบด้าน IT ในปีปฏิทินเดียวกันกับที่ระบบดังกล่าวเริ่มใช้งานจริง
    - หากสำนักงานสอบบัญชีมีการเปลี่ยนแปลงนโยบายหรือแนวปฏิบัติใดที่ส่งผลให้การควบคุมตามข้อกำหนดในแต่ละหัวข้อเปลี่ยนแปลงไปอย่างมีนัยสำคัญ[6] เช่น เปลี่ยนแปลงกระบวนการควบคุมหลัก (key control) เป็นต้น สำนักงานสอบบัญชีจะต้องรวมเรื่องดังกล่าวเข้ามาเป็นส่วนหนึ่งของขอบเขตการตรวจสอบด้าน IT และดำเนินการตรวจสอบด้าน IT ในปีปฏิทินเดียวกันกับที่นโยบายนั้นมีผลบังคับใช้

---

[3] หลักเกณฑ์ในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี
หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)
หัวข้อที่ 1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร
หัวข้อย่อยที่ 2.2.1 นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy)

[4] ระดับความสำคัญของข้อบกพร่อง/ข้อตรวจพบอยู่ในระดับสูงและกลาง

[5] ระบบงาน IT ที่มีนัยสำคัญ หมายถึง ระบบงานหรือทรัพยากรทางเทคโนโลยีที่เกี่ยวข้องกับวัตถุประสงค์ของมาตรฐานการบริหารคุณภาพ อ้างอิง คำจำกัดความตามการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี

[6] ขึ้นอยู่กับดุลพินิจของสำนักงานสอบบัญชีในการประเมินระดับความมีสาระสำคัญของการเปลี่ยนแปลงนโยบายหรือแนวปฏิบัติดังกล่าวว่าส่งผลต่อการควบคุมในแต่ละข้อกำหนดตามหลักเกณฑ์ในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีมากน้อยเพียงใด

ตัวอย่างของประเด็นข้อสังเกตที่สำคัญ

- มีการเข้าถึงระบบงาน IT โดยบุคคลที่ไม่ได้รับอนุญาต ซึ่งอาจส่งผลต่อความน่าเชื่อถือของสำนักงานสอบบัญชีและก่อให้เกิดผลเสียหายกับข้อมูลของลูกค้า
- มีภัยคุกคามด้านความปลอดภัยของข้อมูลสารสนเทศเกิดขึ้นในรอบการตรวจ อันเนื่องมาจากช่องโหว่ของระบบงาน IT
- ระบบงาน IT หยุดชะงัก เนื่องจากไฟฟ้าดับ หรือไฟฟ้ากระชาก ทำให้ข้อมูลสารสนเทศ หรืออุปกรณ์เทคโนโลยีสารสนเทศเสียหาย และสำนักงานสอบบัญชีไม่มีนโยบายหรือมาตรการรองรับเหตุฉุกเฉินนี้
- ระบบงานที่ถูกพัฒนาขึ้นทำงานได้ไม่ถูกต้อง ไม่เป็นไปตามวัตถุประสงค์ของระบบงาน หรือมีการทำงานที่ผิดพลาด ส่งผลให้ประมวลผลข้อมูลไม่ถูกต้อง

ทั้งนี้ประเด็นข้อสังเกตที่สำคัญอื่นที่ต้องได้รับการแก้ไข ให้ขึ้นอยู่กับดุลยพินิจของผู้เชี่ยวชาญตามประกาศฉบับนี้

หมายเหตุ: รายงานผลการตรวจสอบระบบงาน IT โดยผู้เชี่ยวชาญ root cause analysis และ remediation plan รวมถึง ITRA ปีล่าสุด จะถือเป็นส่วนประกอบหนึ่งของการตรวจการบริหารคุณภาพงานของสำนักงานสอบบัญชี (ISQM 1) ของสำนักงาน ก.ล.ต.

ตัวอย่าง

สำนักงานสอบบัญชี A ที่ได้ว่าจ้างผู้เชี่ยวชาญด้าน IT มาตรวจสอบระบบงาน IT ล่าสุดคือ ปี 2568 โดยมีรอบระยะเวลาในรายงานครอบคลุมการเปลี่ยนแปลงระบบงาน IT ตั้งแต่ 1 มิถุนายน 2567 ถึง 31 พฤษภาคม 2568 และได้จัดทำ ITRA ณ วันที่ 30 กันยายน 2568 ได้ผลดังนี้

- ความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี A ณ วันที่ 30 กันยายน 2568 อยู่ใน**ระดับกลาง**
- ระดับของผลกระทบต่อตลาดทุน ณ วันสิ้นปีปฏิทินล่าสุด (31 ธันวาคม 2567) อยู่ที่**ระดับกลางค่อนไปทางต่ำ (ML)**

ดังนั้น การกำหนดความถี่ในการตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี A โดยผู้เชี่ยวชาญ ตามหลักเกณฑ์ในการกำกับดูแลด้าน IT อยู่ที่ **3 ปีครั้ง** สำนักงานสอบบัญชี A จึงต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอีกครั้งภายในปี 2571

ทั้งนี้ ผล ITRA ที่ประเมิน ณ วันที่ 30 กันยายน 2568 จะต้องถูกอนุมัติและนำส่งต่อสำนักงาน ก.ล.ต. พร้อมกับรายงานผลการตรวจสอบระบบงาน IT แบบ full-scope ที่ตรวจในปี 2568 รวมทั้ง root cause analysis และ remediation plan (กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง) ภายในระยะเวลาที่กำหนดไว้ตามหัวข้อ **การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง** กล่าวคือภายใน 31 ตุลาคม 2568

สำหรับปีที่ไม่ได้ระบุให้ตรวจสอบด้าน IT แบบ full-scope โดยผู้เชี่ยวชาญ (ระหว่าง ปี 2569 ถึง 2570)

- สำนักงานสอบบัญชี A ต้องทำการประเมินความเสี่ยง (risk assessment) อย่างน้อยปีละ 1 ครั้ง หรืออาจถี่กว่านั้นหากมีการเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญในรอบปี เพื่อนำไปใช้การวางแผนและดำเนินการตรวจสอบภายในด้าน IT ของปี 2569 และ 2570 ตามลำดับ ทั้งนี้หากไม่ใช่ปีที่กำหนดให้ตรวจสอบด้าน IT แบบ full-scope สำนักงานสอบบัญชีอาจพิจารณาใช้ผู้เชี่ยวชาญเข้ามาตรวจสอบร่วมด้วย
- หากพบว่าในรอบการตรวจปี 2569 (1 มิถุนายน 2568 ถึง 31 พฤษภาคม 2569) ไม่มีเหตุการณ์สำคัญตามหัวข้อ **แนวปฏิบัติสำหรับปีที่สำนักงานสอบบัญชีไม่ได้ถูกกำหนดให้ดำเนินการตรวจแบบ full-scope** ให้ดำเนินการดังนี้
    - ดำเนินการตรวจสอบด้าน IT ภายในสำนักงานสอบบัญชี ตามแผนการตรวจสอบที่ได้จากการประเมินความเสี่ยง (risk assessment) ของปี 2569
    - ผลการตรวจสอบดังกล่าวถือเป็นส่วนหนึ่งของกระบวนการติดตามการบริหารคุณภาพของสำนักงานสอบบัญชีในรอบปี 2569
    - สำนักงาน ก.ล.ต. อาจเรียกดูผลการตรวจสอบดังกล่าวเพิ่มเติม หากมีการเข้าตรวจการบริหารคุณภาพของสำนักงานสอบบัญชี
- อย่างไรก็ดี หากพบว่าในรอบการตรวจปี 2570 (1 มิถุนายน 2569 ถึง 31 พฤษภาคม 2570) มีเหตุการณ์สำคัญตามหัวข้อ **แนวปฏิบัติสำหรับปีที่สำนักงานสอบบัญชีไม่ได้ถูกกำหนดให้ดำเนินการตรวจแบบ full-scope** ให้ดำเนินการดังนี้
    - ดำเนินการตรวจสอบด้าน IT ภายในสำนักงานสอบบัญชี ตามแผนการตรวจสอบที่ได้จากการประเมินความเสี่ยง (risk assessment) ของปี 2570
    - จัดให้มีการตรวจสอบด้าน IT โดยผู้เชี่ยวชาญ ในเรื่องที่เกี่ยวข้องกับเหตุการณ์สำคัญตามแนวปฏิบัติสำหรับปีที่สำนักงานสอบบัญชีไม่ได้ถูกกำหนดให้ดำเนินการตรวจแบบ full-scope
    - สำนักงานสอบบัญชี A ต้องนำส่งรายงานผลการตรวจสอบระบบงาน IT รวมทั้ง root cause analysis และ remediation plan กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่องที่ผ่านการเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี ต่อสำนักงาน ก.ล.ต. ภายใน 31 ตุลาคม 2570

สำหรับในรอบถัดไปของการตรวจสอบระบบงาน IT แบบ full-scope โดยผู้เชี่ยวชาญ

- สำนักงานสอบบัญชี A ว่าจ้างผู้เชี่ยวชาญมาตรวจสอบด้าน IT ในปี 2571 รอบระยะเวลาตั้งแต่ 1 มิถุนายน 2570 ถึง 31 พฤษภาคม 2571
- สำนักงานสอบบัญชี A ต้องนำส่งเอกสารรายงานผลการตรวจสอบระบบงาน IT แบบ full-scope รวมทั้ง root cause analysis และ remediation plan กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง พร้อมทั้ง ITRA ที่ประเมินใหม่ เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง ที่ผ่านการเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี ต่อสำนักงาน ก.ล.ต. ภายในเดือนตุลาคม 2571

ตัวอย่างการนำส่งเอกสารให้กับสำนักงาน ก.ล.ต.

สถานการณ์ตัวอย่าง	แบบรายงาน IT	root cause analysis และ remediation plan (ถ้ามี)	ITRA	นำส่งสำนักงานภายใน
ดำเนินการตรวจ IT ครั้งแรกภายในปี 2569	✓	✓	✓	ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจและไม่เกิน 31 พฤษภาคม 2570
ดำเนินการตรวจ full-scope ตามรอบที่คำนวณได้ตาม ITRA ที่ได้นำส่งสำนักงานรอบล่าสุด	✓	✓	✓	ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบ
ดำเนินการตรวจในปีที่ไม่ได้ถูกกำหนดให้ตรวจแบบ full-scope กรณีการตรวจสอบด้าน IT ในปีนั้นมีเหตุการณ์ที่สำคัญ[7]	✓	✓	-	ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบ

[7] อ้างอิงหัวข้อ แนวปฏิบัติสำหรับปีที่สำนักงานสอบบัญชีไม่ได้ถูกกำหนดให้ดำเนินการตรวจแบบ full-scope