เกณฑ์การประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี
(IT Risk Assessment : ITRA)

ปัจจุบันระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการดำเนินธุรกิจของสำนักงานสอบบัญชีไทยมากขึ้น โดยระบบเทคโนโลยีสารสนเทศถือเป็นทรัพยากรโครงสร้างพื้นฐานที่ช่วยเสริมสร้างประสิทธิภาพการดำเนินงานในด้านต่าง ๆ ของสำนักงานสอบบัญชี เช่น อำนวยความสะดวกในการติดต่อสื่อสารกับลูกค้าสอบบัญชี พัฒนาการบริหารทรัพยากรบุคคลให้มีประสิทธิภาพมากขึ้น พัฒนาระบบการปฏิบัติงานตรวจสอบรายงานทางการเงินให้มีความน่าเชื่อถือและมีประสิทธิภาพมากขึ้น รวมถึงส่งเสริมระบบการควบคุมคุณภาพของสำนักงานสอบบัญชี เป็นต้น ซึ่งการที่สำนักงานสอบบัญชีมีแนวโน้มในการนำทรัพยากรทางเทคโนโลยีมาใช้มากขึ้น ส่งผลให้เกิดความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีเพิ่มขึ้นด้วยเช่นกัน นอกจากนี้ International Auditing and Assurance Standards Board (IAASB) ได้เผยแพร่มาตรฐานเกี่ยวกับการบริหารคุณภาพสำนักงานสอบบัญชี (International Standard on Quality Management 1 “ISQM1”) โดยได้เพิ่มองค์ประกอบในเรื่องทรัพยากรทางเทคโนโลยีสารสนเทศ เพื่อตอบสนองต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีที่เพิ่มสูงขึ้น ซึ่งมาตรฐานฉบับนี้มีผลบังคับใช้กับสำนักงานสอบบัญชีในตลาดทุนตั้งแต่วันที่ 15 ธันวาคม พ.ศ. 2565 เป็นต้นไป ดังนั้น เพื่อให้ระบบบริหารคุณภาพของสำนักงานสอบบัญชีในตลาดทุนสอดคล้องตามมาตรฐาน ISQM1 และตอบสนองต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามด้านไซเบอร์ที่มีพัฒนาการด้านเทคนิคและวิธีการที่หลากหลายมากขึ้น สำนักงาน ก.ล.ต. จึงได้ออกหลักเกณฑ์ในการกำกับดูแลด้านเทคโนโลยีสารสนเทศและการตรวจสอบด้านเทคโนโลยีสารสนเทศสำหรับสำนักงานสอบบัญชีในตลาดทุน โดยมีเกณฑ์ในการประเมินระดับความเสี่ยงของเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี เพื่อนำไปใช้ในการกำหนดรอบระยะเวลาในการจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยมีขั้นตอนการประเมิน ดังนี้

ขั้นตอนที่ 1 : การประเมินความซับซ้อนของระบบเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี

สำนักงาน ก.ล.ต. ได้จัดทำแนวทางการประเมินความซับซ้อนของระบบเทคโนโลยีสารสนเทศในแต่ละหัวข้อย่อยเพื่อใช้เป็นแนวทางในการประเมินความเสี่ยง ซึ่งมีรายละเอียดดังนี้

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
ระบบเทคโนโลยี				
1. โปรแกรมหรือระบบเทคโนโลยีสารสนเทศที่ใช้สนับสนุนการบริหารงานการปฏิบัติงานสอบบัญชี (ทั้งระบบหน้าบ้าน (front end) และระบบหลังบ้าน (back end))	-	ใช้โปรแกรมหรือระบบพื้นฐานทั่วไป เช่น Microsoft office **และ** ไม่ได้มีการเปลี่ยนแปลงการทำงานของโปรแกรม (customization) ตามความต้องการเฉพาะของสำนักงานสอบบัญชี	- ใช้โปรแกรมหรือระบบเฉพาะสำหรับงานสอบบัญชีซึ่งได้จากการซื้อมา (off the shelf) เช่น audit software **หรือ** - ใช้โปรแกรมหรือระบบพื้นฐานทั่วไป ที่ได้ปรับเปลี่ยนตามความต้องการของสำนักงานสอบบัญชีโดยเฉพาะ (customization) ก่อนนำมาใช้งาน	ใช้โปรแกรมหรือระบบที่ได้พัฒนาขึ้นภายในสำนักงานสอบบัญชีเอง ไม่ว่าจะเป็นการจ้างผู้ผลิตภายนอกพัฒนา หรือพัฒนาเองโดยหน่วยงานภายในสำนักงานสอบบัญชี รวมถึงสำนักงานเครือข่าย (network firm)
2. การจัดเก็บและเรียกใช้ข้อมูล	-	จัดเก็บและเรียกใช้ข้อมูลในเครื่องคอมพิวเตอร์ของสำนักงานสอบบัญชี รวมถึง Server หรือ ระบบเครือข่ายคอมพิวเตอร์แบบเชื่อมโยงระยะใกล้ (LAN) ของสำนักงานสอบบัญชี	มีการจัดเก็บและเรียกใช้ข้อมูล**บางส่วนจาก cloud** (สัดส่วนการจัดเก็บและเรียกใช้ข้อมูลจาก cloud **ต่ำกว่า 50%** ของข้อมูลทั้งหมดของสำนักงานสอบบัญชี)	มีการจัดเก็บและเรียกใช้ข้อมูล**ส่วนใหญ่จาก cloud** (สัดส่วนการจัดเก็บและเรียกใช้ข้อมูลจาก cloud **50% ขึ้นไป** ของข้อมูลทั้งหมดของสำนักงานสอบบัญชี)
3. จำนวน laptop PC tablet และ mobile ซึ่งเป็นอุปกรณ์ส่วนตัวของพนักงาน (Bring Your Own Device) ที่สามารถเชื่อมต่อเครือข่ายภายในของสำนักงานสอบบัญชี หรือเข้าถึงข้อมูลหรือฐานข้อมูลภายในของสำนักงานสอบบัญชีได้	-	น้อยกว่า 100 อุปกรณ์	100 – 500 อุปกรณ์	มากกว่า 500 อุปกรณ์ หรือ ไม่สามารถระบุได้
4. จำนวน removeable storage หรืออุปกรณ์อื่น ๆ ที่ไม่ได้กล่าวในข้อ 3. ซึ่งเป็นอุปกรณ์ส่วนตัวของพนักงาน (Bring Your Own Device) ที่สามารถเชื่อมต่อเครือข่ายภายในของสำนักงานสอบบัญชี หรือเข้าถึงข้อมูลหรือฐานข้อมูลภายในของสำนักงานสอบบัญชีได้	-	น้อยกว่า 100 อุปกรณ์	100 – 500 อุปกรณ์	มากกว่า 500 อุปกรณ์ หรือ ไม่สามารถระบุได้
5. สิทธิ์ในการเข้าถึงระบบงาน หรือฐานข้อมูลของสำนักงานสอบบัญชีด้วยอุปกรณ์ส่วนตัวของพนักงาน	เลือกจากระดับสิทธิสูงสุดที่สำนักงานสอบบัญชีอนุญาตให้พนักงานเข้าถึงระบบได้ เช่น อุปกรณ์ส่วนตัวของพนักงานทั่วไปได้สิทธิ์เข้าถึง email เท่านั้น ในขณะที่	ไม่สามารถเข้าถึงระบบงานหรือฐานข้อมูลของสำนักงานสอบบัญชีได้	สามารถเข้าถึง email ได้เท่านั้น	สามารถเข้าถึง email และระบบงานและฐานข้อมูลของสำนักงานสอบบัญชีได้หรือไม่มีข้อจำกัดในการเข้าถึง เสมือนใช้อุปกรณ์

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
	อุปกรณ์ส่วนตัวของหัวหน้าสำนักงานสอบบัญชี ไม่มีข้อจำกัดในการใช้งาน สำนักงานสอบบัญชีต้องเลือกประเมินข้อนี้เป็นระดับสูง			ของสำนักงานสอบบัญชี
6. จำนวนหน่วยงานภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบงานหรือฐานข้อมูลของสำนักงานสอบบัญชี เช่น ลูกค้า หน่วยงานกำกับดูแล sub-contract และ outsource (ไม่รวมบริษัทในเครือของสำนักงานสอบบัญชี)	-	มีจำนวนน้อยกว่า 5 แห่ง	มีจำนวน 5 -10 แห่ง	มีจำนวนมากกว่า 10 แห่ง
7. ช่องทางในการเข้าถึงระบบงานหรือฐานข้อมูลของสำนักงานสอบบัญชีโดยหน่วยงานภายนอก	-	ไม่สามารถเข้าถึงระบบงานหรือฐานข้อมูลได้	สามารถเข้าถึงระบบงานหรือฐานข้อมูลได้ผ่าน leased line (การเชื่อมต่อสาย internet โดยตรง โดยไม่ผ่านเครือข่ายวงนอก) หรือผ่าน VPN over leased line (เชื่อมต่ออุปกรณ์ด้วยเครือข่ายส่วนตัวเสมือนผ่านสายอินเทอร์เน็ตแบบเช่าใช้)	สามารถเข้าถึงระบบงานหรือฐานข้อมูลผ่านการเชื่อมต่ออุปกรณ์ผ่านอินเตอร์เน็ตทั่วไป ที่ไม่ได้ต่อสายอินเทอร์เน็ตแบบเช่าใช้ (leased line)
8. การเชื่อมต่อระบบงานของสำนักงานสอบบัญชีกับระบบงานของหน่วยงานภายนอก (นอกเหนือจากการส่ง email)	เช่น หากฝ่ายใดฝ่ายหนึ่งมีการสร้างข้อมูลในระบบ ข้อมูลนั้นจะถูกส่งไปยังอีกฝ่ายอัตโนมัติ เช่น ลูกค้า A มีการบันทึกบัญชีขายรายวัน และสำนักงานสอบบัญชีสามารถเรียกดูได้จากระบบของสำนักงานสอบบัญชีได้เองแบบทันที (real-time)	**ไม่มี**การเชื่อมต่อระบบเทคโนโลยีสารสนเทศที่ใช้ในการรับส่งรายการธุรกรรมหรือเชื่อมต่อข้อมูลในระบบโดยตรงกับบุคคล/กิจการภายนอกผ่านเครือข่ายอินเทอร์เน็ต	**มี**การเชื่อมต่อระบบเทคโนโลยีสารสนเทศที่ใช้ในการรับส่งรายการธุรกรรมหรือเชื่อมต่อข้อมูลในระบบโดยตรงกับบุคคล/กิจการภายนอกผ่านเครือข่ายอินเทอร์เน็ต โดยหน่วยงานที่มีการเชื่อมต่อกับสำนักงานสอบบัญชีมี**จำนวนน้อยกว่า 10 ราย**	**มี**การเชื่อมต่อระบบเทคโนโลยีสารสนเทศที่ใช้ในการรับส่งรายการธุรกรรม หรือเชื่อมต่อข้อมูลในระบบโดยตรงกับบุคคล/กิจการภายนอกผ่านเครือข่ายอินเทอร์เน็ต โดยหน่วยงานที่มีการเชื่อมต่อกับสำนักงานสอบบัญชีมี**จำนวนตั้งแต่ 10 รายขึ้นไป**
9. ช่องทางการแบ่งปันข้อมูล (shared drive) กับหน่วยงานภายนอก (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 - พัฒนาโดย outsource - พัฒนาโดยหน่วยงานภายในสำนักงานสอบบัญชี - พัฒนาโดยสำนักงาน

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
				เครือข่าย (network firms)
10. การนำเทคโนโลยีอุบัติใหม่ (“emerging technologies”) มาใช้ในสำนักงานสอบบัญชี ในรอบระยะเวลา 3 ปีที่ผ่านมา	เช่น artificial intelligence (AI) machine learning (ML) robotics หรือ blockchain เป็นต้น (รอบ 3 ปีที่ผ่านมา หมายถึง 3 ปี ย้อนหลังนับจากวันที่จัดทำการประเมิน เช่น สำนักงานสอบบัญชีจัดทำการประเมินความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี ในวันที่ 1 มกราคม 2566 ดังนั้น รอบ 3 ปีที่ผ่านมาคือ ตั้งแต่ 1 มกราคม 2563 ถึง 31 ธันวาคม 2565)	**ไม่มี**การนำ emerging technologies มาช่วยในการทำงาน	**มี**การนำ emerging technologies มาช่วยในการทำงาน แต่**น้อยกว่า 3 โครงการ (project) ในรอบระยะเวลา 3 ปี**	**มี**การนำ emerging technologies มาช่วยในการทำงาน **ตั้งแต่ 3 โครงการ (project) เป็นต้นไป ในรอบระยะเวลา 3 ปี**
11. การนำเทคโนโลยี หรือ application ที่มาใช้เป็นครั้งแรก ในรอบระยะเวลา 3 ปีที่ผ่านมา ไม่รวมเทคโนโลยีอุบัติใหม่ (emerging technologies)	-	**ไม่มี**การนำเทคโนโลยี หรือ application มาใช้เป็นครั้งแรก ในรอบระยะเวลา 3 ปีที่ผ่านมา	**มี**การนำ 1-2 เทคโนโลยี หรือ application มาใช้เป็นครั้งแรก ในรอบระยะเวลา 3 ปีที่ผ่านมา	**มี**การนำ มากกว่า 2 เทคโนโลยีหรือ application ขึ้นไป มาใช้เป็นครั้งแรก ในรอบระยะเวลา 3 ปีที่ผ่านมา
12. จำนวนโปรแกรมสำเร็จรูป หรือระบบปฏิบัติการ ที่หมดอายุหรือตกรุ่น 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 Oracle 11g ซึ่งทั้งสองระบบไม่ได้รับการสนับสนุนจากผู้พัฒนาแล้ว นับเป็น 2 ระบบ	น้อยกว่า 2 โปรแกรมหรือระบบ	3-7 โปรแกรมหรือระบบ	มากกว่า 7 โปรแกรมหรือระบบ
13. จำนวนงานบริการด้านเทคโนโลยีสารสนเทศ ที่สำนักงานสอบบัญชีใช้บริการจากผู้ให้บริการภายนอก ภายในรอบระยะเวลา 3 ปีที่ผ่านมา	**<u>ตัวอย่างการนับจำนวนงานที่ใช้บริการจากผู้ให้บริการภายนอก (outsource)</u>** หากผู้ให้บริการจากภายนอกให้การบริการที่แตกต่างกัน สำหรับงานแต่ละงานให้นับแยกงานกัน เช่น - ว่าจ้างวางระบบเครือข่าย (network) นับเป็น 1 บริการ - ดูแลระบบserver/website/security นับเป็น 3 บริการ	น้อยกว่า 5 งานบริการ	5 -10 งานบริการ	มากกว่า 10 งานบริการ
14. จำนวนบริษัทในเครือ หรือเครือข่ายของสำนักงานสอบบัญชี ทั้งในประเทศและต่างประเทศทั้งหมด		น้อยกว่า 5 แห่ง	จำนวน 5-10 แห่ง	มากกว่า 10 แห่ง

หัวข้อ	ตัวอย่าง/รายละเอียด	ระดับต่ำ	ระดับปานกลาง	ระดับสูง
ที่เชื่อมต่อกับระบบงานของกับสำนักงานสอบบัญชีได้ เช่น มีสิทธิ์เข้าถึงระบบข้อมูลของลูกค้า ระบบข้อมูลพนักงาน เป็นต้น				
15. อัตรากำลังคนตามโครงสร้างของสำนักงานสอบบัญชี ณ วันที่ทำการประเมิน	ได้แก่ จำนวนพนักงานประจำ ลูกจ้างประจำ และ ลูกจ้างชั่วคราวของบริษัท รวมถึงหุ้นส่วนและผู้บริหาร และพนักงานบริษัทในเครือ หรือ สำนักงานเครือข่ายที่มาทำงานให้สำนักงานสอบบัญชีและมีสิทธิ์เข้าถึงระบบของสำนักงานสอบบัญชี (ไม่รวม outsource)	น้อยกว่า 100 คน	100-500 คน	มากกว่า 500 คน
16. อัตราการลาออกของ IT staff (turnover rate) ณ วันที่ทำการประเมิน	<u>ตัวอย่างการคำนวณอัตราการลาออก</u> อัตราการลาออก = จำนวนบุคลากรที่ลาออกทั้งหมดในรอบปีนั้นๆ/ จำนวนบุคลากรเฉลี่ยในปีนั้น <u>เช่น</u> จำนวนพนักงาน IT ทั้งหมด รวมลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ outsource - ณ 1 มกราคม 2565 = 100 คน - ณ 31 ธันวาคม 2565 = 70 คน 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 %	น้อยกว่า 20 %	20% - 50%	มากกว่า 50%
การถูกคุกคามทางไซเบอร์				
17. จำนวนครั้งที่ระบบเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีถูกโจมตีในรอบ 3 ปีที่ผ่านมา	เช่น phishing email หรือ phishing phone หรือ ransomware เป็นต้น	ไม่มี	1 – 2 ครั้ง	มากกว่า 2 ครั้ง
18. จำนวนครั้งที่ระบบเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีถูกโจมตีในรอบ 3 ปีที่ผ่านมา และที่มีผลเสียหายเกิดขึ้น (monetary and non-monetary)	เช่น โดนเรียกค่าไถ่ข้อมูล (ransomware) หรือ ทำให้เกิดความเข้าใจผิดจากการที่ผู้โจมตีใช้ Deepfake หลอกเอาข้อมูลจากบุคลากรของสำนักงานสอบบัญชี เป็นต้น	ไม่มี	1 – 2 ครั้ง	มากกว่า 2 ครั้ง

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 4 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 6 ข้อ

พบว่า จำนวนข้อที่ประเมินอยู่ในระดับกลางและระดับสูง (10 ข้อ) > 9 ข้อ และ และจำนวนข้อที่ประเมินอยู่ในระดับสูง > ระดับกลาง ดังนั้น ความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี B อยู่ใน**ระดับสูง**

โดยผลของความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี ในขั้นตอนที่ 1 จะนำไปคำนวณในขั้นตอนที่ 3 : ประเมินความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศในภาพรวมของสำนักงานสอบบัญชีต่อไป

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 คือ ระดับกลางค่อนไปทางต่ำ (ML)

ขั้นตอนที่ 3 : ประเมินความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศในภาพรวมของสำนักงานสอบบัญชี

การประเมินความเสี่ยงในภาพรวมของระบบเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี มีผลต่อการกำหนดความถี่ในการตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีโดยผู้เชี่ยวชาญตามหลักเกณฑ์ในการกำกับดูแลและตรวจสอบด้าน 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 ปีครั้ง	2 ปีครั้ง	ทุกปี
ระดับกลางค่อนไปทางต่ำ (ML)	3 ปีครั้ง	3 ปีครั้ง	2 ปีครั้ง
ระดับต่ำ (Low)	3 ปีครั้ง	3 ปีครั้ง	3 ปีครั้ง

ทั้งนี้ รอบความถี่ที่คำนวณได้ข้างต้น คือ รอบความถี่ที่สำนักงานสอบบัญชีจะต้องจัดให้มีการตรวจสอบด้าน IT แบบเต็มรูปแบบ (“full-scope”) และนำส่งผลการตรวจสอบดังกล่าวให้กับสำนักงาน ก.ล.ต. รวมถึงจัดให้มีการประเมิน ITRA ใหม่เพื่อหารอบระยะเวลาถัดไปที่จะจัดให้มีการตรวจสอบแบบ full-scope อีกครั้ง โดย

- ผู้รับผิดชอบต้องนำเสนอรายงานผลการตรวจสอบ root cause analysis และ remediation plan ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีภายใน 30 วัน หลังวันสุดท้ายที่สิ้นสุดการตรวจสอบ
- รายงานผลการตรวจสอบ root cause analysis และ remediation plan ที่ผ่านการพิจารณาจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีข้างต้น รวมถึง ITRA ที่ประเมินใหม่ต่อสำนักงาน ก.ล.ต. ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ก.ล.ต. ภายใน 90 หลังวันที่นำเสนอเอกสารดังกล่าวต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี

ทั้งนี้ หากรอบปีใด สำนักงานสอบบัญชีมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนแปลงในระบบงาน IT สำนักงานสอบบัญชีต้องทบทวนการประเมิน ITRA ใหม่ในปีนั้น และนำส่งผลการประเมินไปยังสำนักงาน ก.ล.ต. ภายใน 30 วัน นับจากวันที่มีการเปลี่ยนแปลงที่สำคัญ

หมายเหตุ: หากวันที่นำส่งสำนักงาน ก.ล.ต. ตรงกับวันหยุดราชการ ให้นำส่งวันทำการถัดไปแทน

<u>ตัวอย่าง</u>

สำนักงานสอบบัญชี A ประเมินความซับซ้อนทางเทคโนโลยีสารสนเทศ ณ วันที่ 1 มกราคม 2569 (ครั้งล่าสุดที่ได้ว่าจ้างผู้เชี่ยวชาญด้าน IT มาตรวจ คือ ปี 2568) ได้ผลดังนี้

- ความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี A อยู่ใน**ระดับกลาง**
- ระดับของผลกระทบต่อตลาดทุน ณ วันสิ้นปีปฏิทินล่าสุด อยู่ที่**ระดับกลางค่อนไปทางต่ำ (ML)**

ดังนั้น การกำหนดความถี่ในการตรวจสอบด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี A โดยผู้เชี่ยวชาญตามหลักเกณฑ์ในการกำกับดูแลด้าน IT อยู่ที่ **3 ปีครั้ง** สำนักงานสอบบัญชี A จึงต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอีกครั้งภายในปี 2571

- หากสำนักงานสอบบัญชี A มีการว่าจ้างผู้เชี่ยวชาญมาตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) และเสร็จสิ้น field work ณ วันที่ 31 พฤษภาคม 2571
- ผู้รับผิดชอบด้าน IT รายงานผลการตรวจสอบ root cause analysis และ remediation plan ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี ภายในวันที่ 30 มิถุนายน 2571
- สำนักงานสอบบัญชี A ต้องนำส่งรายงานผลการตรวจสอบ root cause analysis และ remediation plan ที่ผ่านการเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี รวมถึง ITRA ที่ประเมินใหม่ต่อสำนักงาน ก.ล.ต. ภายในวันที่ 28 กันยายน 2571

ส่วนรอบปีที่ไม่ได้ถูกกำหนดให้ตรวจแบบ full-scope สำนักงานสอบบัญชีต้องกำหนดขอบเขตของการตรวจสอบด้าน IT ให้เหมาะสมกับความเสี่ยงที่เกี่ยวข้องของสำนักงานสอบบัญชี เช่น

- หากพบว่ามีประเด็นสำคัญที่ต้องแก้ไขจากผลการตรวจรอบก่อน สำนักงานสอบบัญชีต้องจัดให้มีการประเมินในเรื่องนั้นต่อเนื่องไปทุกปีจนกว่าจะแก้ไขแล้วเสร็จ ส่วนเรื่องอื่นที่ไม่พบประเด็น ให้ตรวจอีกครั้งตามรอบตรวจปกติ
- ตรวจสอบเฉพาะระบบงานที่มีการปรับปรุงใหม่ในรอบปี

<u>ตัวอย่างของประเด็นข้อสังเกตที่สำคัญ</u>

- มีการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยบุคคลที่ไม่ได้รับอนุญาต ซึ่งอาจส่งผลต่อความน่าเชื่อถือของสำนักงานสอบบัญชีและก่อให้เกิดผลเสียหายกับข้อมูลของลูกค้า
- มีภัยคุกคามด้านความปลอดภัยของข้อมูลสารสนเทศเกิดขึ้นในรอบการตรวจ อันเนื่องมาจากช่องโหว่ของระบบเทคโนโลยีสารสนเทศ
- ระบบเทคโนโลยีสารสนเทศหยุดชะงัก เนื่องจากไฟฟ้าดับ หรือไฟฟ้ากระชาก ทำให้ข้อมูลสารสนเทศหรืออุปกรณ์เทคโนโลยีสารสนเทศเสียหาย และสำนักงานสอบบัญชีไม่มีนโยบายหรือมาตรการรองรับเหตุฉุกเฉินนี้
- ระบบงานที่ถูกพัฒนาขึ้นทำงานได้ไม่ถูกต้อง ไม่เป็นไปตามวัตถุประสงค์ของระบบงาน หรือมีการทำงานที่ผิดพลาด ส่งผลให้ประมวลผลข้อมูลไม่ถูกต้อง