ปรับปรุงวันที่ 30 พฤษภาคม 2568

ประเด็นคำถามที่ถามบ่อย (FAQ) (ฉบับประมวล)

Document version :

Version	วันที่การจัดทำ	ข้อมูลการแก้ไขปรับปรุงเอกสาร FAQ
1.0	26 เมษายน 2566	จัดทำเอกสาร FAQ ประกาศ สธ. 38/2565 และ นป. 7/2565
2.0	15 มีนาคม 2567	เพิ่มเติมข้อคำถาม-คำตอบ
3.0	30 พฤษภาคม 2568	เพิ่มเติมข้อคำถาม-คำตอบ และปรับปรุงเนื้อหาตามประกาศ สธ. 33/2567 และ นป. 6/2567

หมายเหตุ :

[New] **แสดงคำถาม/คำตอบ ที่มีการเพิ่มเติมหรือปรับปรุงจาก FAQ ฉบับก่อนหน้า (ปรับปรุงจากฉบับประมวล เมื่อวันที่ 15 มีนาคม 2567)**

ลำดับ	คำถาม	คำตอบ
1.	**ขอบเขตการบังคับใช้**	
1.1	ประกาศสำนักงาน ก.ล.ต. เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบ IT ("ประกาศ IT") มีหลักการอย่างไร และผู้ประกอบธุรกิจจะทราบได้อย่างไรว่าการดำเนินการได้เป็นไปตามหลักเกณฑ์แล้ว	เนื่องด้วยประกาศ IT ฉบับนี้ได้นำมาบังคับใช้กับผู้ประกอบธุรกิจหลากหลายกลุ่มธุรกิจ ดังนั้น หลักการที่อยู่ในประกาศฉบับนี้จึงกำหนดเป็นแนว principle-based โดยมีแนวปฏิบัติที่มีรายละเอียด เพื่อให้ผู้ประกอบธุรกิจนำไปใช้เพื่อการดำเนินการได้ ด้วยความหลากหลายของธุรกิจ ระบบงานและเทคโนโลยีที่ใช้งานอาจทำให้ผู้ประกอบธุรกิจมีมาตรการควบคุม (controls) ของตนเองที่แตกต่างไปจากประกาศแนวปฏิบัติของสำนักงาน ก.ล.ต. อย่างไรก็ดี หากมาตรการควบคุมความเสี่ยงนั้น สามารถตอบวัตถุประสงค์และเป้าหมายของการควบคุมได้อย่างมีประสิทธิผล ผู้ประกอบธุรกิจก็สามารถดำเนินการได้ แต่ผู้ประกอบธุรกิจจะต้องมีภาระในการพิสูจน์หรือแสดงว่ามาตรการควบคุมที่แตกต่างนั้น ยังคงสามารถบรรลุวัตถุประสงค์ตามที่ประกาศของสำนักงาน ก.ล.ต. กำหนด ทั้งนี้ สำนักงาน ก.ล.ต. จะพิจารณาความมีประสิทธิผลของมาตรการควบคุมความเสี่ยงจากเรื่องดังต่อไปนี้ (1) การประเมินความเสี่ยงด้าน IT โดยคำนึงถึงช่องโหว่ (vulnerability) ภัยคุกคาม (threat) และผลกระทบ (impact) อย่างรอบด้าน (2) การควบคุมความเสี่ยงอย่างเหมาะสม โดยมีกระบวนการขออนุมัติแผนการบริหารจัดการความเสี่ยงจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย (3) กระบวนการติดตามและทบทวนความเสี่ยง เพื่อให้มั่นใจว่ามาตรการควบคุมความเสี่ยงที่ดำเนินการนั้น ยังคงมีประสิทธิภาพ และยังสามารถใช้ได้ในบริบทหรือสภาพแวดล้อมที่เปลี่ยนไป (4) การรายงานผลการดำเนินการหรือข้อบกพร่องต่าง ๆ ที่เกี่ยวข้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของผู้ประกอบธุรกิจ และคณะกรรมการที่เกี่ยวข้องอย่างสม่ำเสมอ
1.2	แนวปฏิบัติแต่ละหัวข้อสามารถเลือกทำได้หรือไม่ เนื่องจากใน ISO 27001 สามารถเลือกเฉพาะ control ที่ต้องการนำมาจัดการความเสี่ยงนั้น ๆ หลังจากประเมินความเสี่ยงแล้ว	ผู้ประกอบธุรกิจสามารถเลือกใช้มาตรกรควบคุมที่เหมาะสมกับความเสี่ยงของผู้ประกอบธุรกิจ โดยมาตรการควบคุมบางอย่างนั้นอาจไม่เป็นไปตามแนวปฏิบัติของสำนักงาน ก.ล.ต. ได้ อย่างไรก็ดี ผู้ประกอบธุรกิจอาจมีภาระในการพิสูจน์หรือแสดงให้เห็นว่ามาตรการควบคุมที่แตกต่างหรือไม่ครบถ้วนนั้น ยังคงบรรลุวัตถุประสงค์ตามประกาศของสำนักงาน ก.ล.ต. ตัวอย่างเช่น ผู้ประกอบธุรกิจมีนโยบายไม่อนุญาตให้พนักงานใช้อุปกรณ์ส่วนตัวของพนักงานเพื่อเข้าถึงระบบงานในบริษัท และแสดงได้ว่าอุปกรณ์

ลำดับ	คำถาม	คำตอบ
		ส่วนตัวของพนักงานไม่สามารถเข้าถึงหรือเชื่อมต่อเครือข่ายหรือระบบงานภายในบริษัทได้จริง ผู้ประกอบธุรกิจอาจยกเว้นการจัดให้มีมาตรการควบคุมอื่น ๆ ที่เกี่ยวข้องได้
1.3	ระบบที่ต้องปฏิบัติตามหลักเกณฑ์ครอบคลุมเฉพาะระบบของธุรกิจที่อยู่ภายใต้การกำกับของสำนักงาน ก.ล.ต. หรือทุกระบบของผู้ประกอบธุรกิจ เช่น ระบบของธนาคารพาณิชย์ทั้งหมด เป็นต้น	หลักเกณฑ์ใช้บังคับกับระบบ IT ที่เกี่ยวข้องกับธุรกิจที่อยู่ภายใต้การกำกับดูแลของสำนักงาน ก.ล.ต. ตามประกาศที่ สธ. 38/2565 เท่านั้น อย่างไรก็ดี ในทางปฏิบัติมีความเป็นไปได้ที่ผู้ประกอบธุรกิจยังจำเป็นต้องใช้งานหรือพึ่งพาระบบเครือข่าย และ/หรือระบบงานอื่น ๆ ที่อยู่ภายใต้การดูแลของบริษัทในเครือ/บริษัทแม่ ดังนั้น ผู้ประกอบธุรกิจต้องทำให้มั่นใจได้ว่า การดูแลระบบเครือข่าย และ/หรือระบบงานอื่น ๆ ดังกล่าว ได้รับการควบคุมดูแลความเสี่ยงได้ตามมาตรฐานอย่างน้อยที่ประกาศสำนักงาน ก.ล.ต. กำหนด
1.4	ในประกาศ สธ. 38/2565 (ซึ่งแก้ไขเพิ่มเติมโดยประกาศ สธ. 33/2567) ที่ได้ระบุไว้ว่า “ข้อ 5 เว้นแต่จะมีการกำหนดไว้แล้วเป็นการเฉพาะในประกาศอื่น ในการดำเนินการด้านเทคโนโลยีสารสนเทศ ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้” ประกาศอื่นหมายถึงอะไร	แม้ว่าประกาศ IT จะครอบคลุมและมีผลใช้บังคับกับผู้ประกอบธุรกิจหลากหลายประเภท แต่ก็มีประกาศอื่น ๆ (ประกาศคณะกรรมการ ก.ล.ต ประกาศคณะกรรมการกำกับตลาดทุน หรือประกาศสำนักงาน ก.ล.ต.) ที่ได้กล่าวถึงมาตรการควบคุมความเสี่ยงที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ เช่น การจัดทำและทดสอบแผน BCP หรือการจัดเก็บรักษาสินทรัพย์ดิจิทัล เป็นต้น **ดังนั้น ผู้ประกอบธุรกิจจึงมีความจำเป็นต้องปฏิบัติตามประกาศอื่น ๆ ที่มีข้อกำหนดเกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศเป็นการเฉพาะเพิ่มเติมด้วย** เช่น ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลให้ดำเนินการตามประกาศที่ กธ. 19/2561 ซึ่งมีข้อกำหนดเกี่ยวกับการทดสอบเจาะระบบและการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานผลการดำเนินการดังกล่าวต่อสำนักงาน ก.ล.ต. ตามเวลาที่กำหนด เป็นต้น
1.5	[New] “ผู้ประกอบธุรกิจที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ” คือผู้ประกอบธุรกิจประเภทใด	“สาขาของธนาคารพาณิชย์ต่างประเทศ” หมายถึง สาขาของธนาคารพาณิชย์ต่างประเทศที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์ในประเทศไทย ตามคำจำกัดความในข้อกำหนดของธนาคารแห่งประเทศไทย ทั้งนี้ มิได้นับรวมถึงธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ ซึ่งเป็นบริษัทมหาชนจำกัดที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์ ตามข้อกำหนดของธนาคารแห่งประเทศไทย
2.	**คำศัพท์**	
2.1	ขอให้อธิบาย และยกตัวอย่างของ (1) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) (2) การปฏิบัติงานจากเครือข่าย	1. การใช้งานอุปกรณ์เคลื่อนที่ (mobile device): การนำอุปกรณ์เคลื่อนที่ทุกชนิดเชื่อมต่อระบบเครือข่ายขององค์กรเพื่อเข้าถึงระบบ IT ที่มีนัยสำคัญ โดยครอบคลุมอุปกรณ์เคลื่อนที่ทั้งที่เป็นขององค์กรหรือของพนักงาน

ลำดับ	คำถาม	คำตอบ
	ภายนอก (teleworking) และ (3) การใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD)	2. การปฏิบัติงานจากเครือข่ายภายนอก (teleworking): การนำอุปกรณ์ใด ๆ ก็ตามเชื่อมต่อเข้าถึงระบบ IT ที่มีนัยสำคัญขององค์กรจากเครือข่ายภายนอกขององค์กร เช่น การใช้งานอุปกรณ์ Laptop/PC หรือ แท็บเล็ต เชื่อมต่อเครือข่ายจากที่บ้าน/นอกที่ทำการ เพื่อเข้าถึงระบบสารสนเทศที่มีนัยสำคัญขององค์กร ทั้งที่ผ่าน VPN หรือไม่ผ่าน VPN เป็นต้น 3. การใช้งานอุปกรณ์ส่วนตัว" (Bring Your Own Device : BYOD): ผู้ปฏิบัติงานใช้อุปกรณ์ส่วนตัว เช่น โทรศัพท์มือถือ แท็บเล็ต และคอมพิวเตอร์ส่วนตัว เป็นต้น เพื่อเข้าถึงระบบสารสนเทศขององค์กร โดยมีรายละเอียดดังภาคผนวก 1 ของเอกสาร FAQ ทั้งนี้ นโยบายของผู้ประกอบธุรกิจอาจมีนิยามของ mobile device, teleworking และ BYOD ที่แตกต่างจากนิยามของสำนักงาน ก.ล.ต. ได้ อย่างไรก็ดี ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการควบคุมอย่างเหมาะสมและครอบคลุมขอบเขตตามที่สำนักงาน ก.ล.ต. กำหนด
2.2	"การเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง" หมายถึง การเชื่อมต่อแบบใดบ้าง	การใช้อุปกรณ์ทุกชนิดไม่ว่าจะเป็นอุปกรณ์ขององค์กร หรืออุปกรณ์ส่วนตัวของพนักงาน เชื่อมต่อกับระบบเครือข่ายภายในขององค์กร (internal network) เพื่อวัตถุประสงค์ในการปฏิบัติงาน หรือกิจกรรมส่วนตัว โดยครอบคลุมทั้งรูปแบบการเชื่อมต่อผ่านสายเคเบิล (Ethernet) หรือการเชื่อมต่อแบบไร้สาย (Wi-Fi) ทั้งนี้ หากเป็นการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในขององค์กร ผ่านเข้ามาทางเครือข่ายอินเทอร์เน็ต (รวมถึง VPN) หรือ untrusted network จะไม่นับว่าเป็นการเชื่อมต่อโดยตรง
2.3	ระบบอีเมลถือเป็นระบบ IT ที่มีนัยสำคัญหรือไม่	ผู้ประกอบธุรกิจแต่ละรายมีการนำระบบ IT มาเป็นเครื่องมือในการประกอบธุรกิจที่แตกต่างกัน หากระบบอีเมลหยุดชะงักแล้วส่งผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานหรือความต่อเนื่องในการดำเนินงาน ชื่อเสียง หรือฐานะของผู้ประกอบธุรกิจ หรือการใช้บริการของลูกค้า ระบบอีเมลดังกล่าวเข้าข่ายเป็นระบบ IT ที่มีนัยสำคัญ ทั้งนี้ ไม่ว่าผู้ประกอบธุรกิจจะพิจารณาว่าระบบอีเมลเป็นระบบงานสำคัญหรือไม่ ผู้ประกอบธุรกิจมีหน้าที่ต้องจัดเก็บบันทึกข้อมูล (log/audit trails) สำหรับการสื่อสารผ่านทางอีเมลอย่างครบถ้วน ตามที่ประกาศ IT และประกาศอื่น ๆ ที่เกี่ยวข้องได้กำหนดไว้ เช่น แนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการและระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้าของบริษัทหลักทรัพย์ และการลงทุนเพื่อเป็นทรัพย์สินของบริษัทหลักทรัพย์ เป็นต้น

ลำดับ	คำถาม	คำตอบ
2.4	ผู้ใช้งานที่ได้รับสิทธิในการใช้งานในระดับสูง (privileged user) หมายถึงสิทธิระดับใดบ้าง	privileged user หมายถึง user ที่มีสิทธิเหนือกว่าผู้ใช้งานทั่วไป โดยสามารถเข้าถึงการตั้งค่าความปลอดภัยของระบบ กำหนดสิทธิของ user อื่น ๆ หรือลบบันทึกข้อมูลสำหรับการตรวจสอบ (audit trails) บนระบบได้ โดยมีตัวอย่างดังนี้ • root account • superuser account • system account • domain administrator • database administrator • network administrator • system administrator • application administrator • emergency account เป็นต้น
2.5	ขอทราบตัวอย่างแนวทางการพิจารณา “ความมีนัยสำคัญ”	การพิจารณาความมีนัยสำคัญ ให้คำนึงถึงกรอบหลักการของความเสี่ยง (inherent risk) และผลกระทบต่อการให้บริการ หรือดำเนินธุรกิจในวงกว้าง (enterprise-wide impact) โดยยังไม่นำมาตรการควบคุม (controls) มาประกอบการพิจารณาความเสี่ยงนั้น <u>ตัวอย่างการพิจารณาความมีนัยสำคัญ</u> • บุคคลภายนอกที่มีนัยสำคัญ (critical 3rd party) ความมีนัยสำคัญของบุคคลภายนอกอาจพิจารณาจากระดับความสำคัญของงานที่ใช้บริการจากบุคคลภายนอก ความสำคัญของระบบที่เชื่อมต่อกับบุคคลภายนอก ความสำคัญของข้อมูลที่อนุญาตให้บุคคลภายนอกเข้าถึง ตลอดจนจำนวนลูกค้าที่อาจได้รับผลกระทบกรณีบุคคลภายนอกไม่สามารถให้บริการ หรือถูกโจมตีทางไซเบอร์ • การเปลี่ยนแปลงที่มีนัยสำคัญ (critical system change) ความมีนัยสำคัญของการเปลี่ยนแปลงระบบหรือเทคโนโลยี สามารถพิจารณาจากระยะเวลาหยุดชะงักหรือจำนวนลูกค้าที่จะได้รับผลกระทบ เช่น กรณีการเปลี่ยนแปลงระบบเกิดปัญหา หรือจำนวนระบบที่เชื่อมต่อกับระบบที่มีการเปลี่ยนแปลง เป็นต้น • ระบบสารสนเทศที่มีนัยสำคัญ (critical IT system) ความมีนัยสำคัญของระบบสารสนเทศที่ให้บริการ สามารถพิจารณาจากผลกระทบที่อาจจะเกิดขึ้นหากระบบหรือเทคโนโลยีดังกล่าวหยุดชะงักหรือไม่สามารถให้บริการได้
2.6	“สื่อบันทึกข้อมูล” ครอบคลุมสิ่งใดบ้าง	สื่อบันทึกข้อมูล (media) ครอบคลุม สื่อหรืออุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลทั้งหมด เช่น hard disk, flash drive, tape drive, memory card และ disc เป็นต้น

ลำดับ	คำถาม	คำตอบ
3.	**การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**	
3.1	**บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ**	
3.1.1	“ผู้บริหารระดับสูง” หมายถึง บุคลากรตั้งแต่ระดับใด	ผู้บริหารระดับสูง หมายถึง พนักงานของผู้ประกอบธุรกิจระดับผู้บริหารหน่วยงาน (head of department) และตำแหน่งที่เทียบเท่าที่ชื่อเรียกอย่างอื่นขึ้นไป
3.1.2	[New] “กรรมการ” ควรเป็นผู้ที่มีอำนาจจัดการ หรือเป็นกรรมการอื่นได้	“กรรมการ” หมายถึง กรรมการผู้มีอำนาจควบคุม กรรมการผู้ไม่มีอำนาจควบคุม และกรรมการอิสระ ซึ่งผู้ประกอบธุรกิจแต่งตั้งให้ทำหน้าที่เป็นคณะกรรมการของผู้ประกอบธุรกิจ หรือได้รับมอบหมายอย่างเป็นทางการให้มีบทบาทหน้าที่อื่น ๆ เพิ่มเติมตามความเหมาะสม
3.1.3	[New] ข้อกำหนดประกาศ IT ในส่วนของแนวปฏิบัติ เรื่อง “กรรมการของผู้ประกอบธุรกิจควรได้รับการสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT อย่างเพียงพอตามระยะเวลาที่เหมาะสม” จะทราบอย่างไรว่าได้ดำเนินการสร้างความรู้และความตระหนักต่อกรรมการอย่าง “เพียงพอ” แล้ว ● กรรมการทุกท่านในองค์คณะ board of directors จำเป็นต้องได้รับการฝึกอบรมหรือเข้าร่วมสัมมนาเสริมสร้างความตระหนักด้านความเสี่ยงด้าน IT หรือไม่ ● สำนักงานกำหนดชั่วโมงขั้นต่ำในการฝึกอบรมหรือเข้าร่วมสมนาหรือไม่ ● จำเป็นต้องการเข้าฝึกอบรมเป็นหลักสูตรหรือไม่ หรือเป็นการสัมมนาแบบครั้งคราวได้ ● สามารถให้ phishing test ประจำปีเข้าข่ายว่ากรรมการได้รับการสร้างความตระหนักอย่างเพียงพอแล้วได้หรือไม่	ข้อกำหนดดังกล่าวมิได้กำหนดรูปแบบและจำนวนชั่วโมง “การสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT” เป็นการเฉพาะผู้ประกอบธุรกิจสามารถจัดทำ คัดเลือกหลักสูตร เลือกรูปแบบหรือวิธีการ เพื่อสร้างรู้และความตระหนักได้ตามความเหมาะสม เพื่อให้เป็นไปตามวัตถุประสงค์ที่ทำให้กรรมการทุกท่านของผู้ประกอบธุรกิจมีความรู้/ความตระหนักต่อความเสี่ยงด้าน IT ที่เพียงพอต่อการตัดสินใจและบริหารจัดการความเสี่ยงด้าน IT และมีความรู้เท่าทันสภาพแวดล้อมด้าน IT ที่เปลี่ยนแปลงไปในปัจจุบัน ทั้งนี้ การสร้างความรู้/ความตระหนักดังกล่าว ควรมีเนื้อหาและจำนวนชั่วโมงที่เพียงพอเพื่อให้เข้าใจต่อเนื้อหาและใจความสำคัญได้ (comprehensive understanding) โดย ผู้ประกอบธุรกิจสามารถจัดการอบรมภายในให้แก่กรรมการได้ด้วยตนเอง ● การทดสอบ phishing เป็นการสร้างความตระหนักรู้ได้ อย่างไรก็ดีอาจยังไม่เพียงพอต่อการนำไปใช้เพื่อการตัดสินใจและบริหารจัดการความเสี่ยงด้าน IT ดังนั้น ผู้ประกอบธุรกิจจึงควรพิจารณาดำเนินการสร้างความรู้และความตระหนักโดยการจัดอบรมหรือการสัมมนาที่เหมาะสมและเพียงพอด้วย ● สำนักงานสนับสนุนให้กรรมการของผู้ประกอบธุรกิจ เข้าร่วมในกิจกรรมของสำนักงาน อาทิ Capital Market Board Awareness โดยสำนักงานจะพิจารณาว่า การเข้าร่วมในงานอบรมหรือสัมมนาด้าน IT ของสำนักงานนั้น สามารถเข้าข่ายด้านการสร้างความรู้และความตระหนักอย่างเพียงพอ ● การนำเสนอวาระที่เกี่ยวข้องกับภัยคุกคามไซเบอร์ เช่น update cybersecurity trend อย่างน้อยไตรมาสละครั้งให้กับคณะกรรมการบริษัท ก็ถือเป็นส่วนหนึ่งในการสร้างความตระหนักรู้ให้แก่

ลำดับ	คำถาม	คำตอบ
		คณะกรรมการบริษัท
3.1.4	[New] ข้อกำหนดประกาศแนวปฏิบัติที่ นป. 6/2567 ข้อ 1.6.2 (3) ซึ่งระบุให้ผู้ประกอบธุรกิจรายงาน “ผลการตรวจสอบด้าน IT (IT audit) และความคืบหน้าในการดำเนินการแก้ไขข้อบกพร่อง” ต่อคณะกรรมการของผู้ประกอบธุรกิจ (หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ) “อย่างน้อยปีละ 1 ครั้ง” สำหรับรอบปีที่สำนักงานมิได้กำหนดให้มีการตรวจสอบด้าน IT สำหรับผู้ประกอบธุรกิจขนาดเล็กหรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ผู้ประกอบธุรกิจในกลุ่มดังกล่าวจะต้องรายงาน “ผลการตรวจสอบด้าน IT” ในรอบปีนั้นต่อคณะกรรมการอย่างไร	ผู้ประกอบธุรกิจอาจไม่ต้องดำเนินการสำหรับรอบปีที่หลักเกณฑ์มิได้กำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบด้าน IT และรายงานผลการตรวจสอบ IT ต่อสำนักงาน‡ อย่างไรก็ดี หากผู้ประกอบธุรกิจจัดให้มีการตรวจสอบด้าน IT ในรอบปีดังกล่าวแล้ว สามารถรายงานผลการตรวจสอบดังกล่าวต่อคณะกรรมการของผู้ประกอบธุรกิจเพื่อให้มีข้อมูลที่เพียงพอต่อการตัดสินใจและบริหารจัดการความเสี่ยงด้าน IT ได้ แต่ไม่ต้องรายงานผลดังกล่าวต่อสำนักงาน
3.2	**โครงสร้างการกำกับดูแล**	
3.2.1	ในกรณีที่งานด้าน IT compliance และ IT risk รวมอยู่ด้วยกันภายใต้ทีมของ IT security ซึ่งเป็น 1st line นั้น ผู้ประกอบธุรกิจจะต้องแยกหน่วยงานด้าน IT compliance และ IT risk ออกมาเป็นโครงสร้าง 2nd line ที่ชัดเจนหรือไม่	ประกาศ IT ให้ความสำคัญเรื่องการแยกบทบาทหน้าที่ในการปฏิบัติงานอย่างชัดเจนและเป็นอิสระ โดยมิได้กำหนดเรื่องการแบ่งแยกตามโครงสร้างองค์กรเป็นการเฉพาะ ดังนั้น หากงานด้าน IT risk หรือ IT compliance มีการแบ่งแยกหน้าที่จาก 1st line ตามหลัก segregation of duties อย่างชัดเจน และมีความเป็นอิสระเพียงพอ เช่น ผู้ปฏิบัติงานด้าน IT compliance สามารถกำกับดูแลการปฏิบัติงานของทีม IT security ซึ่งเป็น 1st line และสามารถรายงานข้อเสนอแนะหรือข้อสังเกต (ถ้ามี) ต่อ CEO หรือคณะกรรมการ

‡ **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล** เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล (Digital Asset Advisory Service) ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Digital Asset Exchange) เป็นต้น มีหน้าที่ในการปฏิบัติตามข้อกำหนดของประกาศ **กธ. 19/2561** เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจึงยังคงต้องจัดให้มีการตรวจสอบทุกปี และต้องนำส่งรายงานต่อสำนักงานตามเงื่อนไขของประกาศ กธ. 19/2561** คือ

(1) จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ก่อนเริ่มให้บริการและภายหลังเริ่มให้บริการแล้ว**อย่างน้อยปีละ 1 ครั้ง** *และ*

(2) รายงานผลต่อสำนักงานภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการทดสอบ

แม้ว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล เป็นต้น ได้ผลการประเมินแบบ RLA เป็นผู้ประกอบธุรกิจขนาดเล็ก ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง เพื่อให้เป็นไปตามข้อกำหนดของประกาศ กธ. 19/2561

ลำดับ	คำถาม	คำตอบ
		ได้อย่างเป็นอิสระ เป็นต้น ทั้งนี้ ผู้ประกอบธุรกิจสามารถพิจารณาจัดโครงสร้างองค์กรได้ตามความเหมาะสม โดยยังคงรักษาไว้ซึ่งความเป็นอิสระในการปฏิบัติงาน
3.2.2	ตามข้อกำหนดในประกาศ IT “ผู้ประกอบธุรกิจควรจัดให้มีกรรมการของผู้ประกอบธุรกิจ หรือที่ปรึกษาของผู้ประกอบธุรกิจ อย่างน้อย 1 ท่าน ที่มีความรู้หรือประสบการณ์ด้าน IT” มีวิธีการพิจารณาคุณสมบัติของกรรมการอย่างไร เพื่อให้การปฏิบัติสอดคล้องกับเจตนารมณ์ของหลักเกณฑ์	วัตถุประสงค์ของข้อกำหนดดังกล่าว คือ ให้ผู้ประกอบธุรกิจจัดให้มี (1) กรรมการอย่างน้อย 1 ท่าน หรือ (2) ที่ปรึกษา (บุคคลหรือคณะกรรมการชุดย่อย) ที่มีความรู้ หรือประสบการณ์ด้าน IT เพื่อทำหน้าที่ให้คำปรึกษาต่อคณะกรรมการของผู้ประกอบธุรกิจในการกำกับดูแลการบริหารจัดการด้าน IT (IT governance) ที่ดี ผู้ประกอบธุรกิจสามารถพิจารณาคุณสมบัติของกรรมการ หรือที่ปรึกษาที่มีความรู้หรือประสบการณ์ด้าน IT ได้จากเรื่องดังต่อไปนี้ (1) จบการศึกษาในสาขา IT หรือสาขาที่เกี่ยวข้อง หรือ (2) มีประสบการณ์ในตำแหน่งหัวหน้าหน่วยงานด้าน IT หรือมีหน้าที่รับผิดชอบเป็นผู้บริหารงานที่เกี่ยวข้องกับด้าน IT หรือมีประสบการณ์ในด้านการให้คำปรึกษาที่เกี่ยวข้องกับด้าน IT ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้ปัจจัยอื่น ๆ เพิ่มเติมได้ตามความเหมาะสม อย่างไรก็ดี การพิจารณาเฉพาะประวัติการอบรมหรือการสัมมนาด้าน IT (เช่น การอบรมเพื่อสร้างความตระหนักด้านภัยไซเบอร์ เป็นต้น) อาจไม่เพียงพอที่สำหรับการพิจารณาคุณสมบัติด้านความรู้ความสามารถของกรรมการหรือที่ปรึกษา
3.2.3	กรณีที่กรรมการของบริษัทแม่มีความรู้ความสามารถด้าน IT อยู่แล้ว บริษัทไม่ทำการแต่งตั้งกรรมการหรือที่ปรึกษาด้าน IT ภายในบริษัทได้หรือไม่	หลักเกณฑ์กำหนดให้ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูงต้องจัดให้มีกรรมการ หรือที่ปรึกษาของบริษัทอย่างน้อย 1 ท่าน ที่มีความรู้หรือประสบการณ์ด้าน IT เพื่อมีส่วนร่วมหรือให้คำปรึกษาในการกำกับดูแลด้าน IT ในองค์กรอย่างมีประสิทธิผล การกำหนดโครงสร้างการกำกับดูแลโดยอาศัยคณะกรรมการของบริษัทแม่ที่มีความรู้หรือประสบการณ์ด้าน IT อาจไม่เป็นไปตามวัตถุประสงค์ของหลักเกณฑ์ เนื่องจากผู้ประกอบธุรกิจ และบริษัทแม่เป็นคนละองค์กร กรรมการของบริษัทแม่จึงไม่มีความรับผิดชอบและอำนาจหน้าที่โดยตรงในการกำกับดูแลผู้ประกอบธุรกิจ อย่างไรก็ดี ผู้ประกอบธุรกิจอาจแต่งตั้งกรรมการหรือที่ปรึกษาซึ่งเป็นบุคลากรจากบริษัทแม่ เพื่อดำรงตำแหน่งกรรมการหรือที่ปรึกษาด้าน IT ของผู้ประกอบธุรกิจได้ โดยในกรณีของการแต่งตั้งกรรมการผู้ประกอบธุรกิจยังคงต้องตรวจสอบคุณสมบัติของกรรมการเพื่อให้

ลำดับ	คำถาม	คำตอบ
		เป็นไปตามประกาศอื่น ๆ ที่เกี่ยวข้องของสำนักงาน (ถ้ามี) ด้วย
3.2.4	หากจำเป็นต้องแต่งตั้งตำแหน่ง CISO สามารถใช้วิธีให้บุคลากรจากบริษัทแม่ทำหน้าที่ในลักษณะ secondment ได้หรือไม่	กรณีของบริษัทที่มีความเสี่ยงระดับสูง ผู้ประกอบธุรกิจต้องจัดให้มี CISO ของตนเองไว้ในโครงสร้างองค์กรอย่างเป็นทางการ โดยกำหนดบทบาทหน้าที่และความรับผิดชอบของ CISO อย่างชัดเจน ทั้งนี้ หลักเกณฑ์ไม่มีข้อห้ามในการใช้บุคลากรจากบริษัทแม่ (secondment) อย่างไรก็ดี บุคลากรดังกล่าวต้องสามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพและประสิทธิผล
3.2.5	การแต่งตั้ง CIO เพียงอย่างเดียวสามารถทดแทนการแต่งตั้ง CISO ได้หรือไม่	ไม่สามารถทดแทนกันได้ เนื่องจากบทบาทหน้าที่ของ CIO มุ่งเน้นการบริหารจัดการด้าน IT เพื่อสนับสนุนทางธุรกิจ แต่บทบาทหน้าที่ของ CISO มุ่งเน้นการบริหารจัดการความมั่นคงปลอดภัยด้าน IT โดยเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านการพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development)
3.2.6	CISO สามารถเป็นบุคคลเดียวกับ CTO หรืออยู่ในหน่วยงานด้าน security ที่อยู่ภายใต้ CTO ได้หรือไม่ เป็นต้น	CISO ควรมีความเป็นอิสระจากหน่วยงานที่ปฏิบัติงานด้าน IT (IT operation) และงานด้านพัฒนาระบบ IT (IT development) เพื่อให้สอดคล้องตามหลักการถ่วงดุลที่ดี (check and balance) โดยบทบาทหน้าที่และตำแหน่งตามโครงสร้างองค์กรของ CISO ควรสนับสนุนให้เกิดการปฏิบัติหน้าที่ได้อย่างเป็นอิสระและมีประสิทธิภาพ เช่น สามารถรายงานปัญหา และให้ความเห็นด้านความมั่นคงปลอดภัย ต่อผู้บริหารสูงสุดขององค์กรและคณะกรรมการที่เกี่ยวข้องได้โดยตรง
3.2.7	ความเป็นอิสระของ CISO พิจารณาจากตำแหน่งงานในโครงสร้างองค์กรหรือบทบาทหน้าที่ความรับผิดชอบ	
3.2.8	กรณีผู้ประกอบธุรกิจที่มีโครงสร้างกำกับดูแลในกลุ่มธุรกิจแบบรวมศูนย์มีแนวทางดำเนินการตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense : 3 LoDs) อย่างไร	กรณีผู้ประกอบธุรกิจมีโครงสร้างการกำกับดูแลความเสี่ยงด้าน IT แบบรวมศูนย์สำหรับบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องกัน การพิจารณาโครงสร้างการกำกับดูแลตาม 3 LoDs ให้พิจารณาโดยดูจากภาพรวมทั้งหมดของกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องได้ อย่างไรก็ดี คณะกรรมการของผู้ประกอบธุรกิจยังคงต้องรับผิดชอบต่อการกำกับดูแลความเสี่ยงด้าน IT เสมือนผู้ประกอบธุรกิจดำเนินการเอง
3.2.9	ผู้ประกอบธุรกิจจำเป็นต้องจัดให้มีตำแหน่ง IT compliance โดยเฉพาะซึ่งแยกจากตำแหน่ง compliance หรือไม่	หลักเกณฑ์มิได้กำหนดให้มี IT Compliance แยกออกจาก Compliance ไว้เป็นการเฉพาะ ผู้ประกอบธุรกิจสามารถพิจารณาการมอบหมายหน้าที่ได้ตามความเหมาะสมกับการจัดโครงสร้างองค์กร ขนาด และความซับซ้อนในการประกอบธุรกิจ ทั้งนี้ ผู้ประกอบธุรกิจควรพิจารณาจัดสรรบุคลากรให้เพียงพอต่อเพื่อการกำกับดูแลการปฏิบัติตามกฎระเบียบด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิผล
3.3	**นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT**	

ลำดับ	คำถาม	คำตอบ
3.3.1	ผู้ประกอบธุรกิจสามารถใช้นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ของกลุ่มบริษัทซึ่งได้รับอนุมัติจากคณะกรรมการของกลุ่ม ได้หรือไม่	ผู้ประกอบธุรกิจสามารถนำนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ที่บริษัทแม่หรือบริษัทในกลุ่มกำหนดไว้มาปรับใช้ได้ โดยต้องมั่นใจว่านโยบายดังกล่าวครอบคลุมและสอดคล้องตามหลักเกณฑ์ที่สำนักงาน ก.ล.ต. กำหนดอย่างครบถ้วน และเหมาะสมกับลักษณะของธุรกิจในตลาดทุน นอกจากนี้ คณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจยังคงต้องอนุมัตินโยบายดังกล่าวด้วย
3.3.2	ในกรณีที่ผู้ประกอบธุรกิจใช้นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ซึ่งกำหนดโดยบริษัทแม่ที่อยู่ในต่างประเทศ ผู้ประกอบธุรกิจต้องจัดให้มีการอนุมัตินโยบายดังกล่าวโดยคณะกรรมการของบริษัท (subsidiary ประจำประเทศไทย) อีกหรือไม่	
3.3.3	กรณีที่มีการทบทวนนโยบาย ขั้นตอนปฏิบัติ หรือแผนงานต่าง ๆ แต่มิได้มีการแก้ไขเปลี่ยนแปลงรายละเอียด ควรดำเนินการอย่างไร	กรณีผู้ประกอบธุรกิจมีการทบทวนนโยบายหรือเอกสารต่าง ๆ แล้วตัดสินใจว่าจะไม่ทำการแก้ไขเปลี่ยนแปลงใดๆ ผู้ประกอบธุรกิจควรบันทึกหลักฐานของการทบทวน ซึ่งอาจประกอบข้อมูล เช่น วันที่ทำการทบทวน ประเด็นหรือข้อสังเกตที่พบ และเหตุผลในการตัดสินใจไม่แก้ไขเปลี่ยนแปลง เป็นต้น บันทึกหลักฐานดังกล่าวจะเป็นประโยชน์ต่อการทบทวนในอนาคต
4.	**การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ**	
4.1	**โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT**	
4.1.1	ผู้ประกอบธุรกิจต้องดำเนินการอย่างไร ในกรณีที่มีบุคลากรไม่เพียงพอที่จะแบ่งแยกหน้าที่ความรับผิดชอบในการปฏิบัติงานด้าน IT (IT operations) ได้	ผู้ประกอบธุรกิจอาจจัดให้มีมาตรการหรือวิธีการควบคุมอื่นใดที่แสดงให้เห็นได้ว่าสามารถสอบทานการปฏิบัติงานได้อย่างมีประสิทธิภาพ เช่น มีการจัดเก็บหลักฐาน (log) ของการปฏิบัติงาน รวมทั้งจัดให้มีการติดตามวิเคราะห์ log ดังกล่าวอย่างสม่ำเสมอโดยบุคคลที่เป็นอิสระจากผู้ปฏิบัติหน้าที่ เป็นต้น อย่างไรก็ดี การขาดแคลนทรัพยากรในการสอบทานการปฏิบัติงานที่สำคัญเป็นระยะเวลานานอาจสร้างความเสี่ยงต่อการปฏิบัติงานขององค์กรได้ รวมทั้งอาจสะท้อนได้ว่าองค์กรไม่ได้ให้ความสำคัญในเรื่องการบริหารจัดการทรัพยากรด้าน IT อย่างเพียงพอ
4.2	**การบริหารจัดการบุคลากร และบุคคลภายนอก**	
4.2.1	**การบริหารจัดการบุคลากร**	

ลำดับ	คำถาม	คำตอบ
4.2.1.1	กรณีที่หน่วยงานมีข้อจำกัดด้านบุคลากร สามารถให้ผู้ปฏิบัติหน้าที่บริหารความเสี่ยงด้าน IT (IT risk) และผู้ตรวจสอบด้าน IT (IT audit) เป็นบุคคลคนเดียวกันได้หรือไม่	ไม่สามารถเป็นบุคคลคนเดียวกันได้ เนื่องจากตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 LoDs) บุคคลที่ทำหน้าที่ 2nd line และ 3rd line of defense ควรเป็นอิสระต่อกัน เนื่องจากหน้าที่หนึ่งของ 3rd line คือ การตรวจสอบการดำเนินการของ 2nd line ด้วย
4.2.2	**การบริหารจัดการบุคคลภายนอก (third party)**	
4.2.2.1	เนื่องจากแนวปฏิบัติในการควบคุมเกี่ยวกับบุคคลภายนอก (third-party) มีขอบเขตค่อนข้างกว้าง ทำให้มีบุคคลภายนอกหลายประเภท การบริหารจัดการบุคคลภายนอก เช่น การประเมินความเสี่ยง การคัดเลือก และการจัดทำข้อตกลงหรือสัญญา เป็นต้น จะต้องดำเนินการตามที่กำหนดไว้ในแนวปฏิบัติอย่างครบถ้วนกับบุคคลภายนอกทุกรายหรือไม่	วัตถุประสงค์ของแนวปฏิบัติในเรื่องการบริหารจัดการบุคคลภายนอก คือการรวบรวมสิ่งที่ควรปฏิบัติและสิ่งที่ควรคำนึงถึง เมื่อมีการใช้บริการงานด้าน IT เชื่อมต่อระบบ IT หรืออนุญาตให้บุคคลภายนอกเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าได้ ผู้ประกอบธุรกิจสามารถบริหารจัดการบุคคลภายนอกแต่ละประเภทแตกต่างกันตามความเสี่ยงและความมีนัยสำคัญ โดยพิจารณาความเหมาะสมของการนำแนวปฏิบัติไปใช้งาน ตัวอย่างเช่น • การเชื่อมต่อระบบชำระเงินกับธนาคารพาณิชย์ อาจมีการ due diligence ที่เข้มงวดต่ำกว่าการใช้บริการ cloud service • การใช้บริการ IT support ทั่วไป ซึ่งไม่เกี่ยวข้องกับระบบงานสำคัญอาจไม่มีความจำเป็นต้องระบุรายละเอียดเกี่ยวกับ RTO และ RPO ลงในสัญญาการใช้งาน
4.2.2.2	[New] การที่ผู้ประกอบธุรกิจใช้บริการจากผู้ให้บริการจากบุคคลภายนอก กรณีที่เป็นการใช้บริการในงานที่มี **ผู้ให้บริการแบบรวมศูนย์ซึ่งได้รับความเห็นชอบจากสำนักงาน ก.ล.ต.** ผู้ประกอบธุรกิจยังต้องจัดให้มีมาตรการบริหารจัดการบุคคลภายนอกตามข้อกำหนดของหลักเกณฑ์ สธ. 38/2565 อีกหรือไม่ (IT Third Party Risk Management)	ผู้ประกอบธุรกิจยังคงมีหน้าที่ในการบริหารจัดการบุคคลภายนอกเพื่อให้บุคคลภายนอกสามารถให้บริการหรือส่งมอบงานได้ตามที่ได้ตกลงในสัญญาที่ได้จัดทำกับผู้ประกอบธุรกิจ เช่น ข้อตกลงระดับการให้บริการด้าน IT (SLA) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การรักษาความลับของข้อมูล เป็นต้น สำหรับผู้ให้บริการแบบรวมศูนย์ซึ่งได้รับความเห็นชอบจากสำนักงาน ก.ล.ต. เช่น ผู้ให้บริการระบบสนับสนุนงานที่เกี่ยวข้องกับการซื้อขายหน่วยลงทุนและการจัดการกองทุน เป็นต้น สำนักงานเป็นเพียงผู้กำกับดูแลให้ผู้ให้บริการดังกล่าว ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยระบบด้าน IT เป็นไปตามที่หลักเกณฑ์กำหนด ซึ่งอาจมิได้ครอบคลุมตามข้อตกลงระดับการให้บริการของแต่ละรายที่แตกต่างกัน
	นิยามขอบเขต “บุคคลภายนอก”	
4.2.2.3	ผู้ประกอบธุรกิจมีการเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ (data center) โดยผู้ให้เช่าทำหน้าที่ในการบริหาร	การเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ โดยผู้ให้เช่าทำหน้าที่บริหารจัดการระบบสาธารณูปโภคด้วย เข้าข่ายเป็นการใช้บริการงานด้าน IT

ลำดับ	คำถาม	คำตอบ
	จัดการระบบสาธารณูปโภคต่าง ๆ ภายในศูนย์คอมพิวเตอร์ (facility) ด้วย เช่น ระบบไฟฟ้า ระบบทำความเย็นและควบคุมความชื้น ระบบป้องกันและระงับอัคคีภัย เป็นต้น เพื่อให้อยู่ในสภาพที่พร้อมใช้งานอย่างต่อเนื่อง เข้าข่ายเป็นการใช้บริการ third party หรือไม่	จาก third party เนื่องจากการบริหารจัดการระบบสาธารณูปโภคถือเป็นปัจจัยสำคัญที่มีผลต่อการดำเนินการอย่างต่อเนื่องของศูนย์คอมพิวเตอร์ ดังนั้น ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยง กำหนดวิธีการคัดเลือกผู้ให้เช่า กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้เช่า และติดตามผลการให้บริการของผู้ให้เช่าอย่างเพียงพอด้วย
4.2.2.4	[New] ตัวอย่างการเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือการให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญตามนิยามของบุคคลภายนอก	ตัวอย่างการเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก เช่น การเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับพันธมิตรทางธุรกิจเพื่อให้บริการร่วมกัน การเชื่อมต่อกับผู้ให้บริการระบบชำระเงิน หรือการเชื่อมต่อผ่าน Application Programming Interface (API) ทั้งที่ดำเนินการผ่าน private network หรือ public network เป็นต้น
4.2.2.5	[New] กรณี ● ผู้ให้บริการพิมพ์เอกสาร ● ผู้ให้บริการจัดเก็บเอกสารในรูปแบบกระดาษ ● ผู้ให้บริการรับส่งเอกสาร ที่สามารถเข้าถึงข้อมูลของลูกค้าได้ เช่น การเข้าถึงข้อมูลของลูกค้าของผู้ประกอบธุรกิจจากข้อมูลส่วนบุคคลของลูกค้าลงบนเอกสาร เป็นต้น ในกรณีนี้ เข้าข่ายเป็นบุคคลภายนอกตามประกาศการจัดให้มีระบบ IT หรือไม่	สำหรับการเข้าถึงข้อมูลสำคัญโดยบุคคลภายนอกนั้น ให้จำกัด scope ที่ข้อมูลประเภทอิเล็กทรอนิกส์ เช่น การเข้าถึง (Inbound) ข้อมูลลูกค้าของผู้ประกอบธุรกิจและนำไปพิมพ์ใบยืนยันรายการซื้อขาย (confirmation statement) หรือรายงานยอดสินทรัพย์คงเหลือสิ้นเดือน (monthly statement report) เป็นต้น ทั้งนี้ กรณีข้อมูลของลูกค้าที่มิได้อยู่ในรูปแบบอิเล็กทรอนิกส์ เช่น ข้อมูลที่อยู่ในรูปแบบกระดาษ (paper) โดยให้ messenger หรือไปรษณีย์นำส่งจดหมายแจ้งที่มีชื่อและที่อยู่ของลูกค้า เป็นต้น ไม่ได้อยู่ในขอบเขตเป็นบุคคลภายนอกภายใต้ประกาศการจัดให้มีระบบเทคโนโลยีสารสนเทศ อย่างไรก็ดี ผู้ประกอบธุรกิจควรจัดให้มีการบริหารจัดการความเสี่ยงและจัดให้มีมาตรการควบคุมด้านความปลอดภัย ตามประกาศหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นต้น
4.2.2.6	การเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ ครอบคลุมเฉพาะขา inbound เข้ามาในระบบของบริษัท หรือรวมถึงขา outbound ที่บริษัทส่งข้อมูลออกไปยังหน่วยงานภายนอก	ข้อกำหนดเรื่องบุคคลภายนอกตามประกาศจะครอบคลุมเฉพาะกรณีที่หน่วยงานภายนอกเข้าถึงข้อมูลบนระบบของบริษัท (เฉพาะขา Inbound เข้ามา Access ระบบหรือข้อมูลของบริษัท) ยกเว้นการเข้าถึงในฐานะลูกค้า อย่างไรก็ดี กรณีบริษัทมีการส่งข้อมูลสำคัญไปยังหน่วยงานภายนอก บริษัทควรมีการจัดการความเสี่ยงด้านธุรกิจ และคำนึงถึงกฎหมายที่เกี่ยวข้องด้วย

ลำดับ	คำถาม	คำตอบ
4.2.2.7	บุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลขององค์กร หมายความรวมถึงผู้ให้บริการที่เข้ามา on-site เป็นครั้งคราวด้วยหรือไม่	บุคคลภายนอกให้รวมถึงผู้ให้บริการที่เข้ามา on-site เป็นครั้งคราว ซึ่งสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจได้
4.2.2.8	กรณีที่ผู้ให้บริการงานด้าน IT ผู้เชื่อมต่อระบบ IT หรือผู้ที่สามารถเข้าถึงข้อมูลสำคัญ เป็นบริษัทในเครือ ถือว่าเป็นบุคคลภายนอกตามหลักเกณฑ์หรือไม่	บริษัทในเครือ เช่น บริษัทแม่ หรือบริษัทลูก เป็นต้น ที่มีสถานะเป็นคนละหน่วยงานหรือคนละนิติบุคคลกัน ถือเป็นบุคคลภายนอกที่ผู้ประกอบธุรกิจต้องจัดให้มีการบริหารจัดการความเสี่ยง และปฏิบัติตามข้อกำหนดของหลักเกณฑ์ เช่น การประเมินความเสี่ยง การกำหนดบทบาทหน้าที่ความรับผิดชอบของแต่ละหน่วยงานที่ชัดเจน และการจัดให้มีสัญญา/ข้อตกลงในการให้บริการ (SLA) ระหว่างหน่วยงาน เป็นต้น
4.2.2.9	การดำเนินการดังต่อไปนี้ เข้าข่ายเป็นบุคคลภายนอกที่ต้องปฏิบัติตามหลักเกณฑ์ หรือไม่ ● การจัดซื้อและติดตั้งโปรแกรมสำเร็จรูปที่พร้อมใช้งาน เช่น Office suite เป็นต้น ● การจัดซื้อ ติดตั้งและบำรุงรักษาฮาร์ดแวร์ ● การจ้างผู้เชี่ยวชาญภายนอกเพื่อแก้ปัญหาฉุกเฉิน	ผู้ให้บริการงานด้าน IT ผู้เชื่อมต่อระบบ IT หรือผู้ที่สามารถเข้าถึงข้อมูลสำคัญได้ ถือว่าบุคคลภายนอกที่ต้องปฏิบัติตามหลักเกณฑ์ <u>แต่ไม่รวมถึง</u> กรณีดังนี้ ● การจัดซื้อและติดตั้งโปรแกรมสำเร็จรูปที่พร้อมใช้งาน ที่บริษัทเป็นผู้ดำเนินการจัดซื้อเอง เช่น Office suite และโปรแกรมป้องกันไวรัส เป็นต้น <u>ยกเว้น</u> การบำรุงรักษาซอฟต์แวร์ หรือแอปพลิเคชันที่สามารถดำเนินการเองได้ แต่บริษัทมีการจัดซื้อจัดหาบริการดังกล่าวเพิ่มเติม ● การจัดซื้อ ติดตั้งและบำรุงรักษาฮาร์ดแวร์ ที่บริษัทเป็นผู้ดำเนินการจัดซื้อเอง <u>ยกเว้น</u> การบำรุงรักษาฮาร์ดแวร์ที่สามารถดำเนินการเองได้ แต่บริษัทมีการจัดซื้อจัดหาบริการดังกล่าวเพิ่มเติม ● **<u>การตรวจสอบด้าน IT ตามเกณฑ์สำนักงาน หรือการตรวจสอบเพื่อรับรองมาตรฐาน</u>** ● การจ้างผู้เชี่ยวชาญภายนอกเพื่อแก้ปัญหาฉุกเฉิน
	การประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก	
4.2.2.10	ความเสี่ยงจากการกระจุกตัว (concentration risk) ครอบคลุมกรณีใดบ้าง	ความเสี่ยงจากการกระจุกตัว (concentration risk) ซึ่งผู้ประกอบธุรกิจควรคำนึงถึงในกระบวนการคัดเลือกบุคคลภายนอก สามารถครอบคลุมได้หลายกรณี โดยมีตัวอย่างที่สำคัญ เช่น ● การใช้บริการจากบุคคลภายนอกเพียงรายเดียว (single provider) สำหรับระบบงานสำคัญทั้งหมด ซึ่งหากบุคคลภายนอกมีปัญหาในการให้บริการ อาจส่งผลกระทบต่อการดำเนินธุรกิจอย่างมีนัยสำคัญ ● การใช้บริการจากบุคคลภายนอกที่ให้บริการกับผู้ประกอบธุรกิจหลายราย หากมีเหตุขัดข้องเกิดขึ้น บุคคลภายนอกอาจต้องจัดลำดับความสำคัญในการแก้ไขปัญหา โดยจัดสรรทรัพยากรเพื่อแก้ไขปัญหาให้กับผู้ประกอบธุรกิจรายใดรายหนึ่งก่อน เป็นต้น

ลำดับ	คำถาม	คำตอบ
4.2.2.11	ยกตัวอย่างวิธีการประเมินระดับความมีนัยสำคัญของบุคคลภายนอก	วัตถุประสงค์หลักของการประเมินบุคคลภายนอกคือ การเข้าใจความเสี่ยงของ (1) การใช้บริการงานด้าน IT จากบุคคลภายนอก (2) การเชื่อมต่อระบบ IT กับบุคคลภายนอก และ (3) การอนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแล และจัดให้มีการคัดเลือกบุคคลภายนอกที่สอดคล้องกับความเสี่ยงหรือความมีนัยสำคัญของบุคคลภายนอก ทั้งนี้ เพื่อให้ขั้นตอนการประเมินบุคคลภายนอกเป็นไปอย่างมีมาตรฐานและสอดคล้องกับนโยบายที่กำหนดไว้ ผู้ประกอบธุรกิจอาจจัดให้มีแบบฟอร์มมาตรฐานที่ใช้ในการประเมินและคัดเลือกบุคคลภายนอก โดยมีตัวอย่างตามภาคผนวก 2 ของเอกสาร FAQ
	การประเมินศักยภาพบุคคลภายนอก (due diligence)	
4.2.2.12	ผู้ประกอบธุรกิจสามารถใช้วิธีการตรวจสอบรายการใบรับรอง (certificate list) ที่บุคคลภายนอกได้รับแทนการกำหนดสิทธิในการเข้าตรวจสอบการดำเนินงานด้าน IT ของบุคคลภายนอกที่ให้บริการงานด้าน IT รายที่มีนัยสำคัญ เพื่อลดภาระในการตรวจสอบได้หรือไม่	การตรวจสอบจากรายการใบรับรอง (certificate list*) เพียงอย่างเดียวอาจไม่เพียงพอในการพิจารณาความเสี่ยงของผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญ ผู้ประกอบธุรกิจควรพิจารณารายละเอียดของรายงานผลการตรวจสอบด้าน IT (IT audit report) โดยผู้ตรวจสอบที่เป็นอิสระ เช่น System and Organization Control (SOC) Report เป็นต้น โดยคำนึงถึงขอบเขตการตรวจสอบ ระยะเวลาที่ครอบคลุมในรายงานการตรวจสอบผลการตรวจสอบและประเด็นสำคัญ (major findings) ในผลการตรวจสอบและความสามารถและความน่าเชื่อถือของผู้ตรวจสอบ นอกจากนี้ ผู้ประกอบธุรกิจควรพิจารณาความเสี่ยงอื่น ๆ จากการใช้บริการจากบุคคลภายนอก เช่น ความเสี่ยงในด้าน concentration risk / vendor locked-in เป็นต้น เพิ่มเติมด้วย
	การจัดทำสัญญาหรือข้อตกลงกับบุคคลภายนอก	
4.2.2.13	[New] “(7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องกับการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจหรือสอดคล้องกับ*มาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป*”	ตัวอย่าง ของมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป - ISO/IEC 27001 - ISO/IEC 27017 (แนวทางความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์) - CSA STAR Certification/Attestation (Cloud Security Alliance – Security, Trust & Assurance Registry) - NIST Cybersecurity Framework (NIST CSF)

ลำดับ	คำถาม	คำตอบ
	• คำว่า “มาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป” หมายถึงมาตรฐานใด • การประเมินความสอดคล้องกับมาตรฐานสากลของบุคคลภายนอกควรให้ผู้ประกอบธุรกิจดำเนินการในรูปแบบใด เช่น การประเมินด้วยตนเอง (self-assessment) หรือจำเป็นต้องให้บุคคลภายนอกมีใบรับรองมาตรฐาน (certification) จากหน่วยงานที่เชื่อถือได้ เป็นต้น	- SOC 2 (System and Organization Controls Type 2) - PCI-DSS (Payment Card Industry Data Security Standard) - COBIT (Control Objectives for Information and Related Technologies) - ENISA Guidelines • การปรับปรุงข้อกำหนดดังกล่าว มีจุดประสงค์เพื่อให้ผู้ประกอบธุรกิจมี**ความยืดหยุ่น**ในการดำเนินงานมากยิ่งขึ้น และสามารถบริหารจัดการกรณีการใช้บริการ การเชื่อมต่อ หรือการอนุญาตให้บุคคลภายนอกเข้าถึงข้อมูลได้อย่าง**เหมาะสมกับบริบทของตนเอง** โดยยังคงรักษาระดับความมั่นคงปลอดภัยด้าน IT ให้อยู่ในระดับที่เพียงพอและเป็นที่ยอมรับ • ในกรณีที่ผู้ประกอบธุรกิจไม่สามารถกำหนดแนวปฏิบัติให้บุคคลภายนอกดำเนินการตามมาตรฐานขององค์กรได้โดยตรง เช่น กรณีการใช้บริการจาก Cloud Service Provider (CSP) ที่ไม่สามารถปรับการควบคุมตามความต้องการขององค์กรได้ทั้งหมด ผู้ประกอบธุรกิจสามารถพิจารณาเลือกใช้ บุคคลภายนอกที่ได้รับรองมาตรฐานสากลในระดับที่ยอมรับได้ เช่น CSP ที่ได้รับการรับรอง CSA STAR Certification และพิจารณาผลการตรวจสอบจากรายงาน SOC Type 2 ประกอบการตัดสินใจรวมด้วยได้ โดยต้องพิจารณาว่ามาตรฐานดังกล่าวมีความเพียงพอต่อความเสี่ยงของตนเอง เป็นต้น • ทั้งนี้ หลักเกณฑ์**ไม่ได้กำหนดว่าบุคคลภายนอกจำเป็นต้องได้รับใบรับรองมาตรฐานสากลเฉพาะเจาะจง**
4.2.2.14	[New] กรณีข้อตกลง/สัญญาที่ได้จัดทำขึ้นก่อนที่ประกาศมีผลใช้บังคับ หรือกรณีผู้ประกอบธุรกิจไม่สามารถกำหนด SLA ในข้อตกลงหรือสัญญาการให้บริการได้ เช่น ผู้ให้บริการต่างประเทศบางราย เป็นต้น ผู้ประกอบธุรกิจควรปฏิบัติอย่างไร	ผู้ประกอบธุรกิจควรพิจารณาปรับปรุงข้อตกลง/สัญญาที่ได้จัดทำขึ้นก่อนประกาศมีผลใช้บังคับ ให้มีความสอดคล้องตามเจตนารมณ์ที่ประกาศกำหนด เพื่อลดความเสี่ยงที่อาจกระทบต่อผู้ประกอบธุรกิจ โดยทั่วไปข้อตกลง/สัญญา จะมีการกำหนดอายุ หรือระบุวันครบกำหนดสัญญา ดังนั้น ในทางปฏิบัติผู้ประกอบธุรกิจอาจจัดให้มีการทบทวนข้อตกลง/สัญญาให้เป็นไปตามที่ประกาศกำหนดได้ แต่ขึ้นการความยินยอมของคู่สัญญาด้วย กรณีที่ไม่สามารถกำหนด SLA ในข้อตกลงหรือสัญญาการให้บริการได้ ผู้ประกอบธุรกิจสามารถขออนุมัติยกเว้น (exception) จากคณะกรรมการของผู้ประกอบธุรกิจ พร้อมทั้งจัดให้มีพิจารณาแนวทางการควบคุมความเสี่ยงที่เพียงพอเหมาะสมได้

ลำดับ	คำถาม	คำตอบ
		<u>ตัวอย่างเช่น</u> ● ผู้ประกอบธุรกิจมีข้อจำกัดในการระบุข้อตกลงระดับการให้บริการด้าน IT (SLA) ลงในสัญญาที่จัดทำกับ vendor บางประเภท เช่น Cloud Service Provider ต่างประเทศ เป็นต้น ● หากผู้ประกอบธุรกิจยังคงต้องการใช้บริการ vendor รายดังกล่าวแม้จะไม่สามารถกำหนดข้อตกลง SLA ลงในสัญญาได้ ผู้ประกอบธุรกิจควรรายงานเหตุจำเป็น ความเสี่ยง และมาตรการที่เลือกใช้เพิ่มเติมเพื่อให้ผู้มีอำนาจของผู้ประกอบธุรกิจ เช่น คณะกรรมการของผู้ประกอบธุรกิจ เป็นต้น ให้ได้รับทราบถึงความเสี่ยงที่ cloud provider ดังกล่าว อาจจะไม่สามารถปฏิบัติได้ตาม SLA ที่องค์กรกำหนดได้ และตัดสินใจว่าจะยังคงต้องการใช้งาน vendor รายดังกล่าวหรือไม่
	การประเมินผลการปฏิบัติงานหรือผลการให้บริการของบุคคลภายนอก	
4.2.2.15	กรณีที่ใช้บริการโครงสร้างพื้นฐานจาก cloud service provider จะสามารถประเมินมาตรการรักษาความมั่นคงปลอดภัยได้อย่างไร	ผู้ประกอบธุรกิจสามารถประเมินมาตรการรักษาความมั่นคงปลอดภัยของ cloud service provider ได้จากรายงานผลการตรวจสอบที่ดำเนินการโดยผู้ที่มีความเป็นอิสระ เช่น รายงานผลการตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 Type 2) เป็นต้น นอกจากนี้ สำนักงานได้เผยแพร่แนวทางการกำกับดูแลและบริหารจัดการ cloud computing บนเว็บไซต์สำนักงาน ผู้ประกอบธุรกิจสามารถศึกษาเพิ่มเติมและปรับใช้เป็นแนวทางเพื่อกำกับดูแลและบริหารความปลอดภัยจากการใช้งาน cloud computing ได้
4.3	**การบริหารจัดการทรัพย์สินด้าน IT**	
4.3.1	การจัดทำทะเบียนทรัพย์สินด้าน IT ควรมีข้อมูลใดบ้าง	วัตถุประสงค์หลักของการจัดทำทะเบียนทรัพย์สินด้าน IT ทั้ง hardware และ software นั้น เพื่อให้ผู้ประกอบธุรกิจทราบถึงทรัพย์สินด้าน IT ที่ผู้ประกอบธุรกิจมีอยู่ทั้งหมด สามารถจัดให้มีมาตรการควบคุมความเสี่ยงของทรัพย์สินแต่ละรายการได้อย่างเหมาะสม และบริหารจัดการทรัพย์สินดังกล่าวได้อย่างมีประสิทธิผล เช่น การติดตามช่องโหว่ การติดตั้ง patch และการวางแผนบำรุงรักษาหรือการจัดหาทรัพย์สินทดแทน เป็นต้น ดังนั้น ทะเบียนทรัพย์สินควรมีข้อมูลที่สามารถช่วยให้ผู้ประกอบธุรกิจสามารถบรรลุวัตถุประสงค์ดังกล่าว โดยแนวปฏิบัติของสำนักงาน ก.ล.ต. ได้ให้ตัวอย่างรายการข้อมูลในทะเบียนทรัพย์สิน เพื่อให้ผู้ประกอบธุรกิจสามารถพิจารณานำไปปรับใช้ได้

ลำดับ	คำถาม	คำตอบ
4.3.2	ทะเบียนทรัพย์สินประเภทซอฟต์แวร์ควรมีข้อมูลของ freeware ด้วยหรือไม่	วัตถุประสงค์สำคัญอย่างหนึ่งของการจัดทำทะเบียนทรัพย์สินประเภทซอฟต์แวร์คือ เพื่อให้ผู้ประกอบธุรกิจสามารถติดตามช่องโหว่ของระบบสารสนเทศได้อย่างมีประสิทธิผล ดังนั้น ทะเบียนทรัพย์สินประเภทซอฟต์แวร์ควรครอบคลุมซอฟต์แวร์ทุกประเภท (ทั้ง freeware open source และ licensed software) ที่ติดตั้งบนระบบสารสนเทศที่มีนัยสำคัญ หรือมีความเสี่ยงต่อการถูกใช้เป็นช่องทางการโจมตีทางไซเบอร์
4.3.3	ผู้ประกอบธุรกิจสามารถจัดทำทะเบียนทรัพย์สินในกรณีที่ใช้บริการ cloud service provider ได้อย่างไร	วัตถุประสงค์ของการจัดทำทะเบียนทรัพย์สินด้าน IT ทั้ง hardware และ software คือเพื่อให้ผู้ประกอบธุรกิจทราบถึงทรัพย์สินด้าน IT ที่มีอยู่ทั้งหมด และสามารถจัดให้มีมาตรการควบคุมความเสี่ยงได้อย่างมีประสิทธิผล เช่น การติดตามช่องโหว่ การติดตั้ง patch และการวางแผนบำรุงรักษาหรือการจัดหาทรัพย์สินทดแทน เป็นต้น ดังนั้น ผู้ประกอบธุรกิจจึงควรจัดทำทะเบียนทรัพย์สินให้ครอบคลุมทรัพย์สินที่ใช้งานจาก cloud service provider ด้วย ทั้งนี้ ผู้ประกอบธุรกิจสามารถจัดทำทะเบียนทรัพย์สินให้สอดคล้องกับประเภทของบริการที่ใช้งาน ตัวอย่างเช่น ● infrastructure as a service (IaaS) และ platform as a service (PaaS) อาจจัดทำทะเบียนทรัพย์สินของฮาร์ดแวร์หรือซอฟต์แวร์บน cloud เช่น ชื่อ virtual server, virtual network, virtual resources, VM เป็นต้น ● software as a service (SaaS) อาจจัดทำทะเบียนซอฟต์แวร์ที่ใช้บริการบน cloud
4.4	**การรักษาความมั่นคงปลอดภัยของข้อมูล**	
4.4.1	หากผู้ประกอบธุรกิจมีการจัดทำ ROPA (records of processing activity) สามารถใช้แทนทะเบียนทรัพย์สินประเภทข้อมูลได้หรือไม่	วัตถุประสงค์ของการจัดทำ ROPA คือการบันทึกรายการประมวลผลข้อมูลส่วนบุคคล ซึ่งอาจไม่ครอบคลุมข้อมูลอื่น ๆ ที่มิใช่ข้อมูลส่วนบุคคล ดังนั้น กรณีที่ผู้ประกอบธุรกิจมีการจัดทำ ROPA แล้ว ผู้ประกอบธุรกิจยังคงต้องจัดให้มีทะเบียนข้อมูลเพิ่มเติม เพื่อให้ครอบคลุมข้อมูลอื่น ๆ ขององค์กร และกำหนดมาตรการรักษาความปลอดภัยของข้อมูลดังกล่าวอย่างเหมาะสมด้วย
4.4.2	การจัดทำทะเบียนทรัพย์สินประเภทข้อมูลควรครอบคลุมข้อมูลใดบ้าง และรวมถึงข้อมูลที่อยู่ในรูปแบบ unstructured data ด้วยหรือไม่	การจัดทำทะเบียนทรัพย์สินประเภทข้อมูล มีวัตถุประสงค์เพื่อให้ผู้ประกอบธุรกิจสามารถบริหารจัดการข้อมูลที่มีอยู่ในองค์กรได้อย่างครบถ้วน (ทั้งข้อมูลแบบ structured และ unstructured) มีความเหมาะสม และมีประสิทธิภาพ สามารถลดความเสี่ยงของเหตุการณ์ที่ส่งผลกระทบต่อความมั่งคงปลอดภัยของข้อมูลได้ ดังนั้น ทะเบียนทรัพย์สินประเภทข้อมูลควรมีข้อมูลที่เพียงพอที่จะบรรลุวัตถุประสงค์ดังกล่าว

ลำดับ	คำถาม	คำตอบ
		ทั้งนี้ ในกรณีของข้อมูลส่วนบุคคล ผู้ประกอบธุรกิจควรคำนึงถึงการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างครบถ้วน โดยสามารถอธิบายวัตถุประสงค์ของการเก็บ รวบรวม ใช้งาน และประมวลผลข้อมูลนั้น รวมทั้งมีการขอความยินยอมจากเจ้าของข้อมูล (data subject) (แล้วแต่กรณี) นอกจากนี้ การจัดทำทะเบียนข้อมูลให้ครอบคลุมยังสามารถช่วยให้ผู้ประกอบธุรกิจสามารถบริหารจัดการความเสี่ยงของข้อมูลต่าง ๆ ให้เหมาะสมและมีประสิทธิภาพและประสิทธิผลด้วย
4.4.3	data owner ต้องระบุเป็นระดับบุคคล หรือเป็นชื่อหน่วยงาน/ฝ่ายงาน	ผู้ประกอบธุรกิจสามารถกำหนดบุคคล หรือหน่วยงาน/ฝ่ายงานให้เป็น data owner ขึ้นอยู่กับรูปแบบการบริหารจัดการภายใน
4.4.4	จำเป็นหรือไม่ที่ต้องระบุ data owner สำหรับข้อมูลทั้งหมด	ข้อมูลทั้งหมดควรมีการกำหนด data owner เพื่อให้มีผู้รับผิดชอบต่อข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย
4.5	**การควบคุมการเข้าถึงข้อมูลและระบบ IT**	
4.5.1	ขอทราบที่มาของแนวปฏิบัติ ดังนี้ – การจำกัดการยืนยันตัวตนผิดพลาดติดต่อกันไม่เกิน 10 ครั้ง – การใช้รหัสผ่านที่ไม่ซ้ำกับรหัสที่เคยใช้งานอย่างน้อย 4 ครั้งล่าสุด หรือไม่ซ้ำกับรหัสผ่านที่เคยใช้งานในช่วง 1 ปีที่ผ่านมา	แนวปฏิบัติดังกล่าวอ้างอิงจากมาตรฐาน Payment Card Industry Data Security Standard (PCI DSS v4.0) อย่างไรก็ดี ผู้ประกอบธุรกิจสามารถอ้างอิงหรือใช้งานมาตรฐานอื่น ๆ ได้
4.5.2	หากระบบงานหรือเทคโนโลยีที่ใช้งานมีข้อจำกัด ทำให้จำเป็นต้องใช้วิธีการยืนยันตัวตนที่มีความเข้มงวดต่ำกว่าแนวปฏิบัติที่สำนักงาน ก.ล.ต. กำหนด ผู้ประกอบธุรกิจควรดำเนินการอย่างไร	หากระบบงานหรือเทคโนโลยีที่ผู้ประกอบธุรกิจใช้งานมีข้อจำกัด ผู้ประกอบธุรกิจควรประเมินความเสี่ยง และจัดให้มีมาตรการควบคุมทดแทนที่เหมาะสมและสอดคล้องกับความเสี่ยง เช่น กรณีระบบไม่สามารถระงับการเข้าสู่ระบบ (login) ด้วยรหัสผ่านที่ผิดพลาดต่อเนื่องได้ อาจใช้วิธีการอื่น ๆ เพื่อตรวจจับความผิดปกติและตอบสนองได้อย่างทันการ เป็นต้น อย่างไรก็ดี เนื่องจากข้อจำกัดดังกล่าวอาจส่งผลให้ผู้ประกอบธุรกิจไม่สามารถปฏิบัติตามนโยบายขององค์กร หรือแนวปฏิบัติของสำนักงาน ผู้ประกอบธุรกิจจึงควรระบุความเสี่ยงดังกล่าวและประเมินผลกระทบที่อาจจะเกิดขึ้นในกรณีที่เลวร้ายที่สุด (worst case) พร้อมทั้งวางแผนปรับปรุงระบบตามลำดับความเสี่ยง ทั้งนี้ ในระยะสั้นผู้ประกอบธุรกิจควรรายงานและขออนุมัติยกเว้น (exception) จากผู้มีอำนาจอนุมัติและดำเนินการตามแผนที่ได้วางไว้ต่อไป

ลำดับ	คำถาม	คำตอบ
4.5.3	แนวปฏิบัติของผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูงซึ่งควรจัดให้มีระบบอัตโนมัติในการตรวจสอบและแจ้งเตือนพฤติกรรมการยืนยันตัวตนที่ผิดปกติหรือต้องสงสัย การแจ้งเตือนที่กล่าวถึงนั้น เป็นการแจ้งเตือนต่อผู้ประกอบธุรกิจ หรือเป็นแจ้งเตือนต่อผู้ใช้งาน (ลูกค้า)	แนวปฏิบัติมิได้กำหนดรูปแบบการแจ้งเตือนไว้เป็นการเฉพาะ หลักการที่สำคัญคือการจัดให้มีระบบอัตโนมัติในการตรวจสอบและแจ้งเตือนพฤติกรรมการยืนยันตัวตนที่ผิดปกติหรือต้องสงสัย ซึ่งช่วยให้ผู้ที่เกี่ยวข้อง (ไม่ว่าจะเป็นผู้ประกอบธุรกิจ หรือลูกค้า) สามารถตอบสนองหรือแก้ไขเหตุภัยคุกคามได้อย่างทันท่วงที
4.5.4	หากบัญชี privileged user ถูกกำหนดให้ใช้งานเป็นรายบุคคล (assigned to individual) ผู้ประกอบธุรกิจยังจำเป็นต้องสอบทาน log การยืนยันตัวตนและการเข้าถึง หรือ log การดำเนินงานหรือไม่	การสร้างบัญชี privileged user สำหรับผู้ใช้งานแต่ละราย จะช่วยให้บริษัทสามารถระบุผู้ใช้งานได้อย่างมีประสิทธิผล อย่างไรก็ดี ผู้ประกอบธุรกิจยังควรดำเนินการสอบทาน log ที่เกี่ยวกับ privileged user (เช่น authentication log, access log และ activity log เป็นต้น) เพื่อช่วยให้สามารถตรวจพบพฤติกรรมที่อาจมีความผิดปกติ (potential security breaches) และดำเนินการตรวจสอบ (investigate) เพิ่มเติมได้อย่างเหมาะสม
4.5.5	กรณีผู้ประกอบธุรกิจระดับความเสี่ยงสูงซึ่งควรจัดให้มีระบบอัตโนมัติในการตรวจสอบและแจ้งเตือนพฤติกรรมการยืนยันตัวตนที่ผิดปกติหรือต้องสงสัย การใช้งานอุปกรณ์ IPS หรือ IDS ถือว่าเป็นไปตามแนวปฏิบัติแล้วหรือไม่	หากอุปกรณ์ IPS หรือ IDS มีการตั้งค่าให้มีการตรวจสอบและแจ้งเตือนพฤติกรรมการยืนยันตัวตนที่ผิดปกติหรือพฤติกรรมต้องสงสัยจากการใช้งานบัญชีผู้ใช้งาน ถือว่าเป็นไปตามแนวปฏิบัติของสำนักงาน
4.6	**การควบคุมการเข้ารหัส**	
4.6.1	มาตรฐานการเข้ารหัสข้อมูล (cryptographic algorithm) ควรกำหนดอย่างไร เช่น สามารถใช้งาน 128bit key encryption ได้หรือไม่ เป็นต้น	ผู้ประกอบธุรกิจควรเลือกใช้ algorithm ในการเข้ารหัสที่ปลอดภัยตามมาตรฐานสากลหรือเป็นที่ยอมรับได้ เช่น National Institute of Standards and Technology (NIST) หรือ National Security Agency (NSA) เป็นต้น ทั้งนี้ algorithm ที่ใช้งาน ควรมีความเหมาะสมกับระดับความสำคัญและความเสี่ยงของข้อมูล และไม่ควรใช้ algorithm และ key length ที่ปัจจุบันไม่ปลอดภัย
4.6.2	การควบคุมการเข้ารหัส ครอบคลุมการเข้ารหัสในส่วนใดบ้าง เช่น การเข้ารหัสฐานข้อมูล หรือการเข้ารหัสของช่องทางเชื่อมต่อ API เป็นต้น	กรณีที่ผู้ประกอบธุรกิจมีการใช้เทคโนโลยีการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูล (confidentiality, integrity และ authenticity) ตามนโยบาย data security ขององค์กร กุญแจและกระบวนการเข้ารหัสทั้งหมดที่นำมาใช้งานต้องได้รับการควบคุมที่เพียงพอเหมาะสม เพื่อให้สามารถบรรลุวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลตามที่องค์กรกำหนดไว้
4.7	**การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม**	
4.7.1	หากผู้ประกอบธุรกิจย้ายระบบจาก on-	การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

ลำดับ	คำถาม	คำตอบ
	premises ไปบน Cloud ทั้งหมดแล้ว ยังจำเป็นต้องกำหนดนโยบายและแนวปฏิบัติ เรื่อง การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical security) หรือไม่	(Physical security) ควรครอบคลุมถึงศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ ในกรณีที่บริเวณสำนักงาน (office) เป็นสถานที่ตั้งของอุปกรณ์หรือเครือข่ายที่ใช้เพื่อเข้าถึง (remote access) ระบบ IT ที่มีนัยสำคัญซึ่งอยู่บน Cloud บริษัทควรพิจารณาความเสี่ยงที่เกี่ยวข้อง เพื่อกำหนดมาตรการควบคุมที่จำเป็นด้วยเช่นกัน
4.8	**การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT**	
4.8.1	**การบริหารจัดการการตั้งค่าระบบ (system configuration management)**	
4.8.1.1	กรณีบริษัทมีอุปกรณ์จำนวนมากและมีระบบปฏิบัติการและระบบฐานข้อมูลที่แตกต่างกัน จำเป็นต้องสอบทานครบทุกอุปกรณ์หรือสุ่มสอบทานได้	บริษัทสามารถกำหนดแผนในการสอบทานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) โดยแบ่งรอบการสอบทานและความถี่ ได้ตามระดับความสำคัญของระบบ รวมถึงสามารถกำหนดวิธีการสุ่มสอบทานเพื่อให้มั่นใจว่าตัวอย่างที่ใช้ตรวจสอบสามารถใช้แทนประชากรทั้งหมดได้ ในระดับความเชื่อมั่นที่เหมาะสม
4.8.2	**การบริหารจัดการการเปลี่ยนแปลง (change management)**	
4.8.2.1	เสนอให้อธิบายเพิ่มเติมถึงความแตกต่างระหว่าง standard change และ normal change	standard change และ normal change ที่กำหนดในแนวปฏิบัติเป็นเพียงตัวอย่างของประเภทการเปลี่ยนแปลง โดยมีความหมายที่ใช้ทั่วไปดังนี้ ● <u>การเปลี่ยนแปลงมาตรฐานที่ได้รับอนุมัติเป็นการทั่วไป (standard change)</u> คือ การเปลี่ยนแปลงที่ได้รับการอนุมัติจากผู้มีอำนาจไว้ล่วงหน้าเพื่อให้มีการดำเนินงานตามเงื่อนไขที่กำหนดไว้ (pre-authorized) ซึ่งมักเป็นการเปลี่ยนแปลงที่มีความเสี่ยงต่ำ เกิดขึ้นบ่อยครั้ง และมีขั้นตอนการดำเนินการที่ชัดเจน เช่น การเพิ่ม memory เป็นต้น ● <u>การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการปกติ (normal change)</u> คือ การเปลี่ยนแปลงที่ไม่ได้การอนุมัติไว้ล่วงหน้า และไม่ใช่การเปลี่ยนแปลงกรณีเร่งด่วน จึงต้องดำเนินการตามขั้นตอนการขอเปลี่ยนแปลงตามปกติ
4.8.2.2	ข้อกำหนดสำหรับผู้ประกอบธุรกิจระดับความเสี่ยงสูง ซึ่งกำหนดให้มี change advisory board (CAB) นั้น จำเป็นต้องเสนอ CAB สำหรับทุก change request หรือไม่ หรือเฉพาะ change request ที่ส่งผลกระทบระดับสูงเท่านั้น	ผู้ประกอบธุรกิจสามารถกำหนดหลักเกณฑ์หรือเงื่อนไขของการเปลี่ยนแปลงที่ต้องเสนอต่อ CAB ได้ โดยคำนึงถึงระดับความสำคัญและผลกระทบของการเปลี่ยนแปลง ในการนี้ ปัจจัยที่ผู้ประกอบธุรกิจควรนำมาคำนึงถึงเป็นอย่างน้อย เพื่อให้สามารถประเมินผลกระทบได้ชัดเจนขึ้น เช่น ระบบหรือ function ที่ได้รับผลกระทบ / ระยะเวลาที่ใช้ในการเปลี่ยนแปลง / downtime ที่เกิดขึ้น / ประสบการณ์ในการเปลี่ยนแปลงในอดีต (กรณีมีลักษณะเป็น case เดียวกัน) / โอกาสที่การเปลี่ยนแปลงนั้นไม่เป็นไปตามแผน /

ลำดับ	คำถาม	คำตอบ
		แผนสำรองหรือ workaround / ผลการทดลองหรือทดสอบก่อนเริ่มการเปลี่ยนแปลง เป็นต้น
4.8.3	**การบริหารจัดการขีดความสามารถของระบบ IT (capacity management)**	
	-	-
4.8.4	**การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน(endpoint)**	
4.8.4.1	-	-
4.8.5	**การรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD)**	
4.8.5.1	ในการปฏิบัติงานที่มีการใช้ mobile device จะต้องกำหนดให้มีการลงทะเบียนอุปกรณ์ เช่น ยี่ห้อ รุ่น , OS , serial number , MAC address เป็นต้น การลงทะเบียนนั้น ใช้เฉพาะกับพนักงานของบริษัทที่นำอุปกรณ์มาใช้ หรือว่ารวมไปถึงลูกค้าและบุคคลภายนอก (third party) ด้วย	การลงทะเบียนอุปกรณ์เคลื่อนที่นั้น ควรพิจารณาจากความเสี่ยงในการเข้าถึงระบบงานโดยไม่ได้รับอนุญาต และความเสี่ยงจากการเข้าถึงระบบงานโดยอุปกรณ์ที่มีการรักษาความมั่นคงปลอดภัยที่ไม่เพียงพอ ดังนั้น ผู้ประกอบธุรกิจควรลงทะเบียนอุปกรณ์ให้ครอบคลุมทุกอุปกรณ์ที่สามารถใช้เพื่อเข้าถึงระบบ IT ที่มีนัยสำคัญ สำหรับในส่วนของลูกค้า และบุคคลภายนอกที่ไม่สามารถเข้าถึงระบบ IT ที่มีนัยสำคัญ และผู้ประกอบธุรกิจมีมาตรการแบ่งแยกเครือข่ายของระบบ IT ที่มีนัยสำคัญออกจากระบบอื่น ๆ อย่างเหมาะสม ผู้ประกอบธุรกิจอาจไม่จำเป็นต้องกำหนดให้มีการลงทะเบียนอุปกรณ์เคลื่อนที่ อย่างไรก็ดี ผู้ประกอบธุรกิจควรจัดให้มีการลงทะเบียนผู้ใช้งาน และการจัดเก็บ log การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายภายในของผู้ประกอบธุรกิจ เพื่อให้ผู้ประกอบธุรกิจสามารถระบุตัวบุคคลผู้ใช้งานอินเทอร์เน็ตผ่านเครือข่ายของผู้ประกอบธุรกิจได้อย่างถูกต้องและเป็นประโยชน์ในการติดตามตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่ผิดวัตถุประสงค์ขององค์กร หรือไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้องต่อไป
4.8.5.2	กรณีอุปกรณ์สูญหาย ซึ่งการลบข้อมูลจากระยะไกล (remote wipe-out)	เพื่อป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) ซึ่งถูกจัดเก็บในอุปกรณ์เคลื่อนที่จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต

ลำดับ	คำถาม	คำตอบ
	ดำเนินการได้ยาก หากผู้ประกอบธุรกิจมีการควบคุมเรื่องของรหัสผ่านในการเข้าเครื่องและการ lock screen จะสามารถทดแทนการลบข้อมูลได้หรือไม่	ผู้ประกอบธุรกิจสามารถจัดให้มีมาตรการป้องกันข้อมูลกรณีที่อุปกรณ์เกิดการสูญหายที่เหมาะสมอื่น ๆ ได้ เช่น การเข้ารหัสข้อมูล (data encryption) หรืออาจเข้ารหัส drive ข้อมูลเพิ่มเติมสำหรับกรณีที่ไม่สามารถทำ remote wipe-out ได้ เป็นต้น
4.8.5.3	การตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์ส่วนตัวของพนักงาน (BYOD) เช่น ตรวจสอบการ root หรือ jailbroken อาจปฏิบัติได้ยาก สามารถใช้มาตรการควบคุมอื่น ๆ ทดแทนได้หรือไม่	หลักการของข้อกำหนดคือ ผู้ประกอบธุรกิจไม่ควรอนุญาตให้อุปกรณ์ที่ไม่น่าเชื่อถือ (untrusted device) เชื่อมต่อหรือเข้าถึงระบบเครือข่ายภายในขององค์กร เพื่อป้องกันการถูกโจมตีทางไซเบอร์ผ่านอุปกรณ์ BYOD ซึ่งอาจมีการรักษาความมั่นคงปลอดภัยที่ไม่เพียงพอ ดังนั้น ในกรณีที่ผู้ประกอบธุรกิจมีข้อจำกัดในการตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์ BYOD ผู้ประกอบธุรกิจอาจใช้วิธีการปฏิเสธการเชื่อมต่อหรือการเข้าถึงระบบเครือข่าย หรืออนุญาตให้เข้าถึงระบบเครือข่ายที่จัดเป็น untrusted zone หรืออนุญาตให้เข้าถึงได้เฉพาะระบบและข้อมูลที่มีความเสี่ยงต่ำเท่านั้น นอกจากนี้ ผู้ประกอบธุรกิจควรจัดให้มีมาตรการควบคุมเพิ่มเติมสำหรับการรักษาความปลอดภัยของระบบงานและเครือข่ายที่ถูกเข้าถึงผ่าน BYOD ด้วย
4.8.5.4	ข้อกำหนด BYOD ให้รวมถึงการใช้งาน BYOD เพื่อเข้าถึงข้อมูลหรือระบบ IT ใดบ้าง หากไม่ใช่ข้อมูลหรือระบบสำคัญต้องปฏิบัติตามหลักเกณฑ์หรือไม่ เช่น การใช้งาน BYOD เพื่อเข้าใช้งานอีเมล เป็นต้น	ข้อกำหนด BYOD ให้รวมถึงการใช้งาน BYOD เพื่อเข้าถึงระบบ IT ทั้งหมด ทั้งระบบ IT ที่มีนัยสำคัญ และระบบ IT อื่น ๆ เช่น การเข้าถึงระบบอีเมลและตารางการประชุมของผู้ประกอบธุรกิจ ไม่ว่าจะกระทำผ่านแอปพลิเคชัน เว็บบราวเซอร์ หรือช่องทางใด ๆ เป็นต้น ดังนั้น หากผู้ประกอบธุรกิจมีนโยบายหรือมีความจำเป็นที่ต้องให้บุคลากรขององค์กรสามารถนำอุปกรณ์ส่วนตัวมาเชื่อมต่อเพื่อให้สามารถเข้าถึงระบบ IT ขององค์กร ผู้ประกอบธุรกิจต้องมีมาตรการควบคุมความเสี่ยงที่อาจจะเกิดขึ้นอย่างเหมาะสม เช่น ความเสี่ยงจากข้อมูลรั่วไหล อุปกรณ์สูญหาย หรือการถูกโจมตีผ่านช่องโหว่บนอุปกรณ์ที่ไม่มีความมั่นคงปลอดภัย เป็นต้น
4.8.5.5	กรณีที่ลูกค้าใช้อุปกรณ์ส่วนตัวเพื่อเข้าถึงข้อมูลที่ผู้ประกอบธุรกิจให้บริการ เช่น แอปพลิเคชันหรือเว็บไซต์ เป็นต้น นับว่าเข้าข่ายเป็น BYOD และต้องจัดให้มีมาตรการรักษาความปลอดภัยสำหรับการใช้งานอุปกรณ์ส่วนตัวหรือไม่	BYOD ครอบคลุมเฉพาะการนำอุปกรณ์เคลื่อนที่ทุกชนิดของพนักงาน เชื่อมต่อระบบ IT ขององค์กร ไม่รวมถึงการใช้งานอุปกรณ์ส่วนตัวของลูกค้า
4.8.5.6	ในกรณีที่ผู้ประกอบธุรกิจมีการใช้งาน Virtual Desktop Infrastructure (VDI)	แม้ว่า VDI จะช่วยให้ผู้ประกอบธุรกิจสามารถรักษาความปลอดภัยของคอมพิวเตอร์ที่ใช้ปฏิบัติงานผ่านส่วนกลางได้ แต่ VDI ยังมีความเสี่ยง

ลำดับ	คำถาม	คำตอบ
	จำเป็นต้องมีการรักษาความปลอดภัยอื่น ๆ เช่น BYOD security เป็นต้นด้วยหรือไม่	ด้านอื่น ๆ ที่ไม่สามารถจัดการได้ผ่าน virtualization ได้โดยตรงทั้งหมด เช่น การโจมตีข้อมูลและแอปพลิเคชันที่ใช้เพื่อเข้าถึง VDI ซึ่งอยู่บนอุปกรณ์ BYOD เป็นต้น ดังนั้น การใช้งาน VDI ควรมีการคำนึงถึงความเสี่ยงที่เกี่ยวข้องอย่างรอบด้านและจัดให้มีมาตรการควบคุมอย่างเพียงพอ แม้ว่า Virtual Desktop Infrastructure (VDI) จะช่วยรักษาความปลอดภัยของระบบปฏิบัติการและแอปพลิเคชันที่อยู่บนเซิร์ฟเวอร์ได้ในระดับหนึ่ง แต่ VDI ยังมีความเสี่ยงด้านความปลอดภัยอื่นๆ ที่ต้องคำนึงถึง โดยเฉพาะอย่างยิ่งความเสี่ยงที่เกี่ยวข้องกับอุปกรณ์ปลายทาง (End-point devices) ที่ใช้เข้าถึง VDI เช่น ● Bring Your Own Device (BYOD) Security: อุปกรณ์ส่วนตัวที่พนักงานนำมาใช้งานอาจถูกโจมตี และทำให้ผู้โจมตีได้รับข้อมูลในการเข้าถึง VDI หรือ สามารถดักจับข้อมูลบน VDI ผ่านอุปกรณ์ BYOD ได้ ● Network Security: การเข้าถึง VDI ผ่านเครือข่ายที่ไม่ปลอดภัย อาจทำให้ข้อมูลการสื่อสารถูกดักจับได้ จึงควรใช้ VPN หรือการเข้ารหัสข้อมูลเพื่อป้องกัน
4.8.6	**การสำรองข้อมูล (data backup)**	
4.8.6.1	รายละเอียดข้อมูลหรือระบบที่ควรนำมาทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูล หมายถึงการทดสอบข้อมูลสำรองของระบบใด เช่น critical system, application system หรือ ทุก system เป็นต้น	หลักการของข้อกำหนดคือ ผู้ประกอบธุรกิจต้องมีข้อมูลสำรองที่พร้อมนำมาใช้งานเสมอเมื่อเกิดเหตุการณ์ที่ไม่คาดคิด (unexpected event) การทดสอบข้อมูลเป็นกระบวนการที่ทำให้ผู้ประกอบธุรกิจมั่นใจได้ว่าข้อมูลที่ได้สำรองไว้มีความพร้อมใช้งานเมื่อจำเป็นต้องใช้ เนื่องจากผู้ประกอบธุรกิจแต่ละรายมีระบบและวิธีการจัดเก็บข้อมูลที่แตกต่างกัน ดังนั้น ผู้ประกอบธุรกิจสามารถกำหนดขอบเขตของการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลให้เหมาะสมกับความเสี่ยงของข้อมูลและความมีนัยสำคัญของระบบที่เกี่ยวข้อง ทั้งนี้ การทดสอบควรคำนึงถึง Recovery Point Objective (RPO) และ Recovery Time Objective (RTO) ที่กำหนดไว้ด้วย
4.8.7	**การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log)**	
4.8.7.1	log ของการเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล หมายถึงอะไร	log การเปลี่ยนแปลงโครงสร้างฐานข้อมูล หรือตาราง (table) ของฐานข้อมูล เช่น การ create / alter / drop table เป็นต้น
4.8.7.2	กรณีที่ระบบ instant messaging บางระบบ เช่น ระบบ chat ใน Lotus Note หรือ Bloomberg เป็นต้น ไม่สามารถบันทึกและจัดเก็บหลักฐาน	สามารถใช้ได้เฉพาะกรณีที่ผู้ใช้งานไม่สามารถเข้าถึงข้อมูลภายในที่ไม่ได้เปิดเผยเป็นการทั่วไป หรือผู้ใช้งานไม่จัดเป็น access person ตามที่ระบุในประกาศแนวปฏิบัติที่ นป. 1/2562 เรื่อง แนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับ

ลำดับ	คำถาม	คำตอบ
	การสนทนาได้ ผู้ประกอบธุรกิจสามารถใช้ระบบงานดังกล่าวได้หรือไม่	การกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้าของบริษัทจัดการและการลงทุนเพื่อเป็นทรัพย์สินของบริษัทจัดการ
4.8.7.3	[New] กรณีผู้ประกอบธุรกิจที่มิได้มีระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ผู้ประกอบธุรกิจจะจัดเก็บข้อมูลตามรูปแบบบันทึกการทำธุรกรรม (transaction log) ตามที่หลักเกณฑ์กำหนดอย่างไร เช่น หมายเลขบริษัทสมาชิก (broker No. 4 หลัก) เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET Order ID) เป็นต้น	ข้อกำหนดบันทึกการทำธุรกรรม (transaction log) ซึ่งระบุให้มีการบันทึกข้อมูล transaction ในรูปแบบ (format) ตามที่หลักเกณฑ์กำหนดนั้น หมายถึง กรณีที่ผู้ประกอบธุรกิจที่เป็นบริษัทสมาชิกของศูนย์ซื้อขายหลักทรัพย์ ที่มีการใช้งานระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) เช่น บริษัทหลักทรัพย์ (บล.) เป็นต้น กรณีผู้ประกอบธุรกิจประเภทอื่น ๆ เช่น บลจ. บลน. บลป. เป็นต้น ให้จัดให้มีการบันทึก transaction log เป็นระยะเวลาอย่างน้อย 1 ปี แต่จะมีรูปแบบใดก็ได้ตามความเหมาะสม ทั้งนี้ การจัดเก็บ transaction log ดังกล่าวต้องยึดหลักการความถูกต้อง (accuracy) เชื่อถือได้ (reliability) และสามารถตรวจสอบย้อนกลับได้ (auditability) **สรุปข้อกำหนดแนวปฏิบัติเรื่องบันทึกการทำธุรกรรม (transaction log)** **[ทุกระบบ]** บันทึกการทำธุรกรรม (transaction log) ควรมีระยะเวลาจัดเก็บขั้นต่ำ 1 ปี **[สำหรับผู้ประกอบธุรกิจที่ใช้งานระบบ trading system เช่น บล. เป็นต้น]** โดยในกรณีที่เป็นระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ให้บันทึกบัญชีผู้ใช้งาน / ข้อมูลรายละเอียดชื่อย่อหลักทรัพย์ (securities symbol) / หมายเลขบริษัทสมาชิก (broker No. 4 หลัก : xxxx) / เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order ID) / เลขที่บัญชีซื้อขายหลักทรัพย์ (account ID) / วันและเวลาในการส่งคำสั่งซื้อขายหลักทรัพย์ (yyyy/mm/dd – hh:mm:ss:sss) / หมายเลข public และ local IP address ต้นทาง (source) / หมายเลข IP address ปลายทาง (destination) / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) / terminal type (ถ้ามี) เช่น mobile, PC, iPad, iPhone เป็นต้น **[สำหรับผู้ประกอบธุรกิจที่ใช้งานระบบ trading system เช่น บล. เป็นต้น]** ให้ผู้ประกอบธุรกิจจัดทำและนำส่งข้อมูลเพิ่มเติมต่อสำนักงานตามรูปแบบและวิธีการที่สำนักงานกำหนดโดยไม่ชักช้าเมื่อสำนักงานร้องขอ โดยข้อมูลบันทึกการทำธุรกรรมเพิ่มเติม (additional transaction log) ที่ผู้ประกอบธุรกิจควรพร้อมจัดทำและนำส่งต่อสำนักงานเมื่อสำนักงานร้องขอ โดยมีรายละเอียดขั้นต่ำ ดังนี้ ... (รายละเอียดตามที่กำหนดใน นป. 6/2567)

ลำดับ	คำถาม	คำตอบ
4.8.7.4	ผู้ประกอบธุรกิจจะต้องจัดเก็บบันทึกการทำธุรกรรม (transaction log) สำหรับระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ในส่วนของ source IP และ destination IP รวมถึง full URL อย่างไร จึงจะเป็นไปตามความคาดหวังตามประกาศของสำนักงาน ก.ล.ต.	ให้ผู้ประกอบธุรกิจจัดเก็บ source IP และ destination IP โดยจำแนกตามลักษณะการใช้งานของลูกค้า ดังนี้ (พิจารณาประกอบกับแผนภาพตามภาคผนวก 3 ของเอกสาร FAQ) 1. กรณีลูกค้าซื้อขายหลักทรัพย์ผ่านอุปกรณ์ที่ผู้ประกอบธุรกิจจัดไว้ภายในที่ทำการของผู้ประกอบธุรกิจ (เช่น desktop ในห้องค้า เป็นต้น) 1.1 หากส่งคำสั่งผ่าน trading application ที่ผู้ประกอบธุรกิจพัฒนาขึ้น / จ้างพัฒนาหรือเช่าระบบของ vendor โดยที่ application ดังกล่าว host อยู่ในที่ทำการของผู้ประกอบธุรกิจ รวมถึงกรณีลูกค้าส่งคำสั่งผ่านพนักงาน IC ให้ผู้ประกอบธุรกิจจัดเก็บ private IP address ตามคู่ A-A' และ full URL ให้ครบถ้วน (<u>ยกเว้น</u>กรณี non web-based application ไม่ต้องจัดเก็บ full URL) 1.2 หากส่งคำสั่งผ่าน SETTRADE application หรือ application อื่นที่มิได้ host อยู่ในที่ทำการของผู้ประกอบธุรกิจ (โดยการเชื่อมต่อ internet) ผู้ประกอบธุรกิจต้องจัดเก็บ private IP address (source) ของเครื่องที่ทำการส่งคำสั่ง พร้อมกับจัดให้ผู้ให้บริการ application ดำเนินการจัดเก็บ public IP address ตามคู่ B-B' และ full URL ให้ครบถ้วน ทั้งนี้ เพื่อให้ผู้ประกอบธุรกิจมีข้อมูลเพียงพอยืนยันตัวตนของลูกค้าที่ส่งคำสั่งได้ 2. กรณีลูกค้าซื้อขายหลักทรัพย์ผ่านอุปกรณ์ที่มิใช่ทรัพย์สินของผู้ประกอบธุรกิจผ่าน internet (เช่น mobile phone / internet café / personal laptop เป็นต้น) 2.1 หากส่งคำสั่งผ่าน trading application ที่ผู้ประกอบธุรกิจพัฒนาขึ้น / จ้างพัฒนาหรือเช่าระบบของ vendor โดยที่ application ดังกล่าว host อยู่ในที่ทำการของผู้ประกอบธุรกิจ ให้ผู้ประกอบธุรกิจจัดเก็บ IP address ตามคู่ C-C' และ full URL (<u>ยกเว้น</u>กรณี mobile application หรือ non-web-based application ไม่ต้องจัดเก็บ full URL) <u>ทั้งนี้ ผู้ประกอบธุรกิจควรจัดให้มีระบบงานที่จะช่วย correlate log ที่เกิดจาก trading application และ log จากคู่ C-C' เพื่อประโยชน์ในการยืนยันตัวตนลูกค้าผู้ส่งคำสั่ง (ดูตัวอย่าง log ได้จากภาคผนวก 3)</u> 2.2 หากส่งคำสั่งผ่าน SETTRADE application หรือ application อื่นที่มิได้ host อยู่ในที่ทำการของผู้ประกอบธุรกิจ ให้ดำเนินการเช่นเดียวกับข้อ 1.2 (<u>ยกเว้น</u>กรณี mobile application ไม่ต้องจัดเก็บ full URL)
4.8.7.5	บริษัทหลักทรัพย์สามารถจัดเก็บ log ในส่วนของ order number ที่สร้างขึ้นมาเองแทนการเก็บ SET order	บริษัทหลักทรัพย์ไม่สามารถจัดเก็บ order number ที่สร้างขึ้นเองได้ เนื่องจากในการตรวจสอบตัวตนของลูกค้าผู้ส่งคำสั่ง สำนักงาน ก.ล.ต. หรือหน่วยงานบังคับใช้กฎหมายอื่น ๆ จำเป็นต้องใช้ SET order number

ลำดับ	คำถาม	คำตอบ
	number ได้หรือไม่	ประกอบการพิจารณา เพื่อให้สามารถตรวจสอบ log เทียบกับข้อมูลซื้อขายที่ได้จากระบบของ SET ซึ่งการใช้ข้อมูลแวดล้อมอื่น ๆ ในการพิจารณา เช่น order time หรือข้อมูล login / logout time อาจทำให้การตรวจสอบมีความคลาดเคลื่อนได้ เป็นต้น
4.8.7.6	ข้อมูล log ตามประกาศ อาจไม่สามารถจัดเก็บทั้งหมดให้อยู่ใน centralized log เดียวกันได้ เนื่องจากในทางปฏิบัติ log ของแต่ละอุปกรณ์จะจัดเก็บแยกกัน เช่น firewall, load balancer, proxy server, web server และ application server เป็นต้น	หลักการของข้อกำหนดคือ เมื่อมีเหตุที่ทำให้ผู้ประกอบธุรกิจต้องดำเนินการตรวจสอบเพื่อหาข้อเท็จจริง ผู้ประกอบธุรกิจต้องมีข้อมูล log ของอุปกรณ์ต่าง ๆ ที่ครบถ้วน โดยมีวันและเวลาที่ตรงกัน (time sync) และมีข้อมูลเพียงพอต่อการดำเนินการตรวจสอบข้อเท็จจริง และเป็นไปตามกฎหมาย ผู้ประกอบธุรกิจสามารถจัดเก็บ log ไว้แตกต่างสถานที่ (location) กันได้ ขึ้นอยู่กับวิธีการบริหารจัดการ log ภายในองค์กร อย่างไรก็ดี ผู้ประกอบธุรกิจควรจัดให้มีระบบงานที่ช่วยให้ correlate log ระหว่างอุปกรณ์เพื่อประโยชน์ในการตรวจสอบกิจกรรมของลูกค้า เมื่อสำนักงาน ก.ล.ต. หรือหน่วยงานบังคับใช้กฎหมายอื่น ๆ ร้องขอ
4.8.7.7	ผู้ประกอบธุรกิจควรเก็บข้อมูลบันทึกเหตุการณ์การใช้งานอินเทอร์เน็ตเฉพาะสำหรับพนักงาน หรือรวมถึงบุคคลภายนอก (ลูกค้า) ที่เข้ามาใช้งานอินเทอร์เน็ตของบริษัท	การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานอินเทอร์เน็ต ควรครอบคลุมการใช้งานทั้งหมดของพนักงานและบุคคลภายนอก เพื่อให้สามารถระบุตัวตนผู้ใช้งานและกิจกรรมที่เกิดขึ้นได้ เพื่อป้องกันไม่ให้ผู้ไม่หวังดีใช้ระบบเครือข่ายขององค์กรทำการโจมตี ก่อกวน นำเข้า หรือเผยแพร่ข้อมูลสารสนเทศที่เข้าข่ายเป็นการกระทำผิดกฎหมาย ทั้งนี้ ข้อมูลที่จัดเก็บต้องสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นต้น
4.8.7.8	การทำงานของ firewall (network firewall log) หมายถึงอะไร ควรมีข้อมูลใดบ้าง	network firewall log หมายถึง log ข้อมูลการจัดการ traffic ของ firewall เช่น เหตุการณ์ที่มีการ deny/drop packet เป็นต้น เพื่อให้สามารถใช้เป็นข้อมูลในการตรวจสอบย้อนหลังกรณีที่เครือข่ายถูกโจมตีได้ โดยใน log ควรบันทึกข้อมูล วันและเวลาที่ตรงกับระบบงานอื่น ๆ (clock synchronization) / IP address ต้นทาง (source) และปลายทาง (destination) / firewall action / port ที่ใช้ติดต่อ
4.8.8	**การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring)**	
4.8.8.1	-	-
4.8.9	**การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment)**	

ลำดับ	คำถาม	คำตอบ
4.8.9.1	-	-
4.8.10	**การทดสอบเจาะระบบงาน (penetration test)**	
4.8.10.1	ผู้ประกอบธุรกิจสามารถเข้าร่วมโครงการ bug bounty เพื่อค้นหาช่องโหว่ แทนการจัดทำ penetration test ได้หรือไม่	การเข้าร่วมโครงการ bug bounty แม้จะเป็นการช่วยให้สามารถค้นหาและแจ้งเตือนช่องโหว่ ซึ่งอาจนำไปสู่การดำเนินการแก้ไขได้ อย่างไรก็ดี การเข้าร่วมโครงการดังกล่าวไม่ได้เป็นการรับประกันว่าจะมีผู้ดำเนินการทดสอบหรือค้นหาช่องโหว่ของบริษัทในระหว่างที่เข้าร่วมโครงการ อีกทั้งยังไม่รับประกันว่าช่องโหว่ดังกล่าวจะถูกรายงานให้กับผู้เข้าร่วมโครงการอย่างเหมาะสม ดังนั้น การจัดทำ penetration test จึงยังคงมีความจำเป็น โดยควรเป็นรูปแบบมาตรฐานที่ใช้ในการทดสอบและค้นหาช่องโหว่ต่าง ๆ ของระบบงานตามขอบเขตที่กำหนดเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงระบบงานอย่างมีนัยสำคัญ ทั้งนี้ การทำโครงการ bug bounty ควบคู่ไปกับการทำ penetration test จะยิ่งช่วยให้ผู้ประกอบธุรกิจได้รับความมั่นใจมากยิ่งขึ้นว่าระบบงานสำคัญทั้งภายในและภายนอกจะได้รับการทดสอบและได้รับการรายงานช่องโหว่อย่างเหมาะสม
4.8.10.2	ผู้จัดทำ penetration test เป็นบุคลากรภายในองค์กร ได้หรือไม่	ผู้ประกอบธุรกิจสามารถจัดให้มี penetration test โดยบุคลากรภายในองค์กรได้ อย่างไรก็ดี บุคลากรดังกล่าวต้องมีความรู้ความสามารถโดยมีความเป็นอิสระจากหน่วยงานเจ้าของระบบ และเป็นอิสระจากการพัฒนาระบบดังกล่าว
4.8.10.3	ผู้ประกอบธุรกิจสามารถใช้เครื่องมือทดสอบ หรือเครื่องมือ scan ระบบ เช่น Web Application Scan เป็นต้น เพื่อทดแทนการจัดทำ penetration testing ได้หรือไม่	การใช้เครื่องมือทดสอบ หรือเครื่องมือ scan เช่น Web Application Scan เป็นต้น ถือเป็นเพียงการประเมินช่องโหว่ทางเทคนิค (vulnerability assessment) ในขั้นต้นเท่านั้น ไม่สามารถทดแทนการทดสอบการเจาะระบบได้ เนื่องจากช่องโหว่บางชนิดอาจไม่สามารถตรวจพบได้โดยเครื่องมือสแกนช่องโหว่อัตโนมัติเพียงอย่างเดียว ต้องอาศัยผู้เชี่ยวชาญในการทดสอบเจาะระบบร่วมด้วย ทั้งนี้ ในการทดสอบเจาะระบบงานซึ่งดำเนินการโดยผู้เชี่ยวชาญ (penetration tester) นั้น สามารถใช้เครื่องมือ (tools) ต่าง ๆ สนับสนุนการดำเนินการได้
4.8.10.4	ในกรณีที่บริษัทใช้บริการระบบ/โปรแกรม จากผู้ให้บริการ (vendor) บริษัทสามารถให้ vendor จัดทำ penetration test ระบบดังกล่าวแทนการดำเนินการโดยบริษัท	ผู้ประกอบธุรกิจสามารถใช้ผลการจัดทำ penetration test ของ vendor ได้ ในกรณีที่ผู้ประกอบธุรกิจนำระบบ/โปรแกรมที่เป็นผลิตภัณฑ์สำเร็จรูปมาใช้งาน โดยที่ไม่สามารถดัดแปลงหรือแก้ไขผลิตภัณฑ์ได้เอง และต้องปฏิบัติตามเงื่อนไขการใช้งานของผลิตภัณฑ์นั้น เพื่อป้องกันผลกระทบที่อาจเกิดต่อระบบการรักษาความปลอดภัยของ

ลำดับ	คำถาม	คำตอบ
	ได้หรือไม่	ผลิตภัณฑ์ดังกล่าว รวมถึงเมื่อนำผลิตภัณฑ์มาเชื่อมต่อกับระบบและเครือข่ายของผู้ประกอบธุรกิจแล้ว จะไม่ก่อให้เกิดช่องโหว่เพิ่มเติมจาก environment หรือ operation ของผู้ประกอบธุรกิจ ซึ่งจะส่งผลให้การทำ penetration test นั้นไม่ถูกต้อง
4.8.10.5	สำนักงาน ก.ล.ต. มีการกำหนดรูปแบบรายงานผลการทดสอบการเจาะระบบหรือไม่	สำนักงาน ก.ล.ต. ไม่ได้กำหนดรูปแบบ (template) สำหรับการจัดทำรายงานผลทดสอบการเจาะระบบ อย่างไรก็ดี รายงานผลการทดสอบการเจาะระบบควรครอบคลุมรายละเอียดที่สำคัญ เพื่อให้ผู้ประกอบธุรกิจเข้าใจถึงความเสี่ยงของช่องโหว่ และสามารถดำเนินการป้องกันแก้ไขอย่างเหมาะสม ตัวอย่างเช่น ผู้ทำการทดสอบ วันที่ทดสอบ ขอบเขตการทดสอบ รายการช่องโหว่ที่ตรวจพบ วิธีการทดสอบซึ่งทำให้ตรวจพบช่องโหว่ ความเสี่ยงของช่องโหว่ และแนวทางป้องกันแก้ไขช่องโหว่ เป็นต้น
4.8.10.6	กรณีระบบ IT ที่มีนัยสำคัญ แต่ไม่ได้เชื่อมต่อกับเครือข่ายสาธารณะ ผู้ประกอบธุรกิจจำเป็นต้องจัดให้มีการทดสอบการเจาะระบบอย่างน้อยปีละ 1 ครั้งหรือไม่	กรณีดังกล่าว ให้ผู้ประกอบธุรกิจพิจารณาความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เช่น การโจมตีผ่าน intranet โดยผู้ไม่ประสงค์ดี (internal user/malicious insider) หรือการแพร่กระจายของมัลแวร์ผ่าน intranet เป็นต้น และกำหนดขอบเขตการทดสอบการเจาะระบบได้ตามความเหมาะสม
4.8.10.7	กรณีระบบที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ แต่ไม่ได้เป็นระบบ IT ที่มีนัยสำคัญ ผู้ประกอบธุรกิจจำเป็นต้องจัดให้มีการทดสอบการเจาะระบบ (penetration test) อย่างน้อยปีละ 1 ครั้ง หรือไม่	ผู้ประกอบธุรกิจต้องดำเนินการทดสอบการเจาะระบบที่เชื่อมต่อกับเครือข่ายสาธารณะอย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ เนื่องจากระบบที่เชื่อมกับเครือข่ายสาธารณะหรืออินเทอร์เน็ตมีโอกาสที่จะตกเป็นเป้าหมายของการโจมตีทางไซเบอร์และส่งผลกระทบต่อการปฏิบัติงานหรือความน่าเชื่อถือขององค์กร นอกจากนี้ จากข้อมูลเหตุการณ์ที่เกิดขึ้นในอดีต ผู้ไม่หวังดีมักจะโจมตีองค์กรผ่านระบบที่มีช่องโหว่เป็นลำดับแรก โดยไม่คำนึงว่าเป็นระบบที่มีความสำคัญหรือไม่ หลังจากนั้นผู้ไม่ประสงค์จะเข้าควบคุมระบบดังกล่าวเพื่อใช้เป็นฐานในการโจมตีระบบ IT ที่มีนัยสำคัญอื่น ๆ หรืออาจใช้ระบบงานของผู้ประกอบธุรกิจเป็นฐานโจมตีหน่วยงานภายนอกต่อไปได้ (รายละเอียดเพิ่มเติมตามแผนภาพในภาคผนวก 4) อย่างไรก็ดี กรณีที่ผู้ประกอบธุรกิจมีเว็บไซต์เพื่อการให้ข้อมูลลูกค้า ไม่รองรับการ upload ข้อมูลใด ๆ และไม่รองรับการทำธุรกิจอิเล็กทรอนิกส์ เพื่อเป็นการลดภาระค่าใช้จ่าย ผู้ประกอบธุรกิจสามารถประเมินความเสี่ยงด้านต่าง ๆ รวมถึงความเสี่ยงด้านชื่อเสียงกรณีเว็บไซต์ถูกโจมตี หากความเสี่ยงอยู่ในระดับที่ยอมรับได้ ผู้ประกอบธุรกิจ

ลำดับ	คำถาม	คำตอบ
		สามารถขออนุมัติยกเว้นการทำ penetration test ประจำปีจากผู้มีอำนาจขององค์กรได้
4.8.10.8	กรณีระบบ IT ที่เชื่อมต่อโดยตรงกับระบบของหน่วยงานอื่น เช่น SET ธนาคารหรือสถาบันการเงินอื่น ๆ เป็นต้น ผ่าน private network ผู้ประกอบธุรกิจต้องทำการทดสอบการเจาะระบบดังกล่าวหรือไม่	หลักเกณฑ์ได้ให้ความสำคัญกับการทดสอบการเจาะระบบของระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะสูงกว่าระบบอื่น ๆ เพื่อให้สอดคล้องกับความเสี่ยงจากการถูกโจมตีทางไซเบอร์ สำหรับระบบ IT มีเพียงการเชื่อมต่อแบบ private network ผู้ประกอบธุรกิจสามารถพิจารณาความเสี่ยงที่เกี่ยวข้อง เช่น การโจมตีผ่านช่องโหว่บนระบบที่เชื่อมต่อกัน และช่องโหว่บน private network เป็นต้น และกำหนดขอบเขตของการทดสอบการเจาะระบบที่เหมาะสมเพิ่มเติมได้
4.8.10.9	การทดสอบการเจาะระบบต้องดำเนินการในรูปแบบใด (black box, grey box หรือ white box)	ผู้ประกอบธุรกิจสามารถเลือกใช้วิธีการทดสอบการเจาะระบบที่สอดคล้องกับความเสี่ยงของระบบงานและเป้าหมายของการทดสอบ ทั้งนี้ ผู้ทดสอบการเจาะระบบควรมีความรู้ความสามารถและเชี่ยวชาญในการทดสอบการเจาะระบบ รวมทั้งมีความเป็นอิสระจากหน่วยงานเจ้าของระบบ และเป็นอิสระจากการพัฒนาระบบดังกล่าว
4.8.10.10	ผู้ประกอบธุรกิจจำเป็นต้องดำเนินการแก้ไขทุกช่องโหว่ที่พบจากการทำ vulnerability assessment และ penetration testing หรือไม่	ผู้ประกอบธุรกิจต้องมีการบริหารจัดการและแก้ไขช่องโหว่ที่ตรวจพบทุกประเภทตามความเสี่ยงของช่องโหว่ ซึ่งรวมถึงช่องโหว่ที่มีระดับความเสี่ยงต่ำ ซึ่งยังคงมีความเสี่ยงและสามารถพัฒนาเป็นภัยคุกคามร้ายแรงในอนาคตได้หากไม่ได้รับการติดตาม เฝ้าระวัง และแก้ไขอย่างเหมาะสม
4.8.10.11	ผู้ที่ทดสอบการเจาะระบบควรเป็นอิสระจากหน่วยงานเจ้าของระบบ และเป็นอิสระจากการพัฒนาระบบดังกล่าวหมายความว่าอย่างไร	วัตถุประสงค์ของข้อกำหนดคือการจัดให้มีการรายงานช่องโหว่ที่ตรวจพบถึงผู้บริหารระดับสูงอย่างครบถ้วน และมีการแก้ไขช่องโหว่อย่างเหมาะสม ดังนั้น เพื่อให้มีการ check and balance ที่ดี ผู้ที่ทดสอบเจาะระบบจึงควรมีความเป็นอิสระตามตัวอย่างดังนี้ • ผู้ทดสอบการเจาะระบบ ไม่ใช่บุคคลเดียวกันกับผู้พัฒนาโปรแกรม • ผู้ทดสอบการเจาะระบบ ไม่ได้อยู่ภายใต้การบังคับบัญชาของผู้พัฒนาโปรแกรม หรืออยู่ภายใต้ผู้บังคับบัญชาเดียวกันกับผู้พัฒนาโปรแกรม หรือถูกประเมินผลการปฏิบัติงานโดยผู้บังคับบัญชาเดียวกันกับผู้พัฒนาโปรแกรม • ผู้ทดสอบการเจาะระบบไม่มีส่วนได้ส่วนเสียกับความสำเร็จของโปรแกรมโดยตรง เช่น ไม่ได้เป็นสมาชิกของทีมที่รับผิดชอบในการพัฒนาระบบ เป็นต้น ทั้งนี้ กรณีที่มีข้อจำกัด ผู้ประกอบธุรกิจสามารถจัดให้มีการควบคุมอื่น ๆ ทดแทนได้ เช่น ให้ผู้ทดสอบการเจาะระบบรายงานผลการตรวจสอบต่อ CEO หรือคณะกรรมการที่เกี่ยวข้องได้โดยตรง

<table>
<tr><th>ลำดับ</th><th>คำถาม</th><th>คำตอบ</th></tr>
<tr><td>4.8.10.12</td><td>ผู้ประกอบธุรกิจที่มีการใช้ระบบ IT ที่บริหารจัดการโดยบริษัทแม่ สามารถใช้ผลการทดสอบเจาะระบบของบริษัทแม่ได้หรือไม่</td><td>สามารถใช้ผลการทดสอบของบริษัทแม่ได้ หากการทดสอบที่เกิดขึ้นมีขอบเขตครอบคลุมระบบ IT ทั้งหมดที่ใช้ในธุรกิจภายใต้ประกาศที่ สธ. 38/2565 ซึ่งมีการเชื่อมต่อกับอินเทอร์เน็ต</td></tr>
<tr><td>4.8.10.13</td><td>[New] ผู้ประกอบธุรกิจขนาดเล็กต้องจัดให้มีการทดสอบการเจาะระบบและการประเมินช่องโหว่ทางเทคนิคอย่างไร‡</td><td><u>การทดสอบการเจาะระบบ (penetration testing)</u>
ผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการทดสอบการเจาะระบบที่ครอบคลุมระบบงาน (application system) และระบบเครือข่ายที่มีช่องทางเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) <u>อย่างน้อยทุก 3 ปี</u>‡ และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ โดยผู้ประกอบธุรกิจสามารถเลือกปีที่จะต้องจัดทำ penetration testing ได้ตามความเหมาะสม (ไม่จำเป็นต้องเป็นปีเดียวกันกับปีที่ทำการตรวจสอบด้าน IT)

<u>การประเมินช่องโหว่ทางเทคนิค (vulnerability assessment)</u>
ผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการประเมินช่องโหว่ทางเทคนิคสำหรับระบบ IT ที่มีนัยสำคัญและระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะทุกระบบ <u>อย่างน้อยปีละ 1 ครั้ง</u> และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ

ความแตกต่างระหว่างการทำ Pen-Test และ VA
<table>
<tr><th>หัวข้อ</th><th>Penetration Testing (Pen-Test)</th><th>Vulnerability Assessment (VA)</th></tr>
<tr><td>วัตถุประสงค์</td><td>ทดสอบการโจมตีเพื่อดูว่าสามารถเข้าถึงระบบได้หรือไม่</td><td>ค้นหาช่องโหว่ในระบบเพื่อระบุและประเมินความเสี่ยง</td></tr>
<tr><td>แนวทางการทำงาน</td><td>การจำลองการโจมตีจริงเพื่อหาวิธีเจาะระบบ</td><td>การ scan ระบบเพื่อค้นหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ</td></tr>
<tr><td>ระดับความลึก</td><td>มุ่งเน้นเจาะลึกในบางจุดหรือระบบที่สำคัญ</td><td>การประเมินภาพรวมของระบบทั้งหมด</td></tr>
<tr><td>ผลลัพธ์ที่ได้</td><td>รายงานช่องโหว่ที่สามารถถูกโจมตีได้จริง พร้อมแนวทางป้องกัน</td><td>รายงานช่องโหว่ทั้งหมด พร้อมระดับความเสี่ยงและคำแนะนำทั่วไป</td></tr>
<tr><td>ตัวอย่างเครื่องมือ</td><td>Metasploit, Burp Suite, Cobalt Strike</td><td>Nessus, OpenVAS, Qualys</td></tr>
<tr><td>ผู้ใช้งาน</td><td>มักใช้โดยองค์กรที่ต้องการทดสอบการโจมตีจริง</td><td>มักใช้ในกระบวนการตรวจสอบและปรับปรุงความปลอดภัยทั่วไป</td></tr>
</table>
</td></tr>
</table>

‡ **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล** เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล (Digital Asset Advisory Service) ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Digital Asset Exchange) เป็นต้น มีหน้าที่ในการปฏิบัติตามข้อกำหนดของประกาศ **กธ. 19/2561** เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล เพื่อให้เป็นไปตามข้อกำหนดของประกาศ กธ. 19/2561 **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจึงยังคงต้อง**

(1) **จัดให้มีการทดสอบการเจาะระบบ (penetration test)** กับระบบงานสำคัญก่อนเริ่มให้บริการและภายหลังจากเริ่มให้บริการ **<u>อย่างน้อยปีละ 1 ครั้ง</u>** *และ*

(2) **รายงานผลการทดสอบการเจาะระบบต่อสำนักงาน ภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการทดสอบ**

ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่ได้ผลการประเมินแบบ RLA เป็นผู้ประกอบธุรกิจขนาดเล็ก เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล (Digital Asset Advisory Service) เป็นต้น ยังมีหน้าที่ในการทดสอบการเจาะระบบ อย่างน้อยปีละ 1 ครั้ง

ลำดับ	คำถาม	คำตอบ
4.8.10.14	**การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)**	
	-	-
4.9	**การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร**	
	-	-
4.10	**การบริหารจัดการโครงการด้าน IT การจัดหา พัฒนา และบำรุงรักษาระบบ IT**	
4.10.1	การดำเนินการลักษณะใดบ้างที่ต้องทำในรูปแบบของโครงการ	ในการจัดหา พัฒนา หรือแก้ไขเปลี่ยนแปลงระบบ IT ที่มีผลกระทบอย่างมีนัยสำคัญต่อการให้บริการ แนวทางหรือรูปแบบการดำเนินธุรกิจ หรือโครงสร้างพื้นฐาน (infrastructure) ด้าน IT ผู้ประกอบธุรกิจควรจัดทำในรูปแบบของโครงการ ซึ่งมีการกำหนดเป้าหมาย แผนงาน และกรอบระยะเวลา เพื่อให้มีการบริหารจัดการความเสี่ยงของโครงการที่เหมาะสมและสามารถบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้ โดยมีตัวอย่างของโครงการ เช่น การเปลี่ยนแปลงระบบจับคู่คำสั่งซื้อขาย การเปลี่ยนแปลงเทคโนโลยีของโครงสร้างพื้นฐาน เป็นต้น
4.10.2	กรณีผู้ประกอบธุรกิจขนาดเล็กที่มีข้อจำกัดด้านบุคลากร โครงสร้างการควบคุมและกำกับดูแลโครงการจำเป็นต้องมีผู้รับผิดชอบครบทุกบทบาทหรือไม่ เช่น project steering committee, project owner, project management office และ project manager เป็นต้น	ผู้ประกอบธุรกิจสามารถกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการได้ตามความเหมาะสม ไม่จำเป็นต้องมีหน่วยงานครบตามที่ยกตัวอย่างในแนวปฏิบัติ อย่างไรก็ดี ผู้ประกอบธุรกิจควรกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการอย่างชัดเจน และมีผู้รับผิดชอบในบทบาทหน้าที่อย่างเพียงพอ เพื่อให้มั่นใจได้ว่าการบริหารจัดการความเสี่ยงของโครงการด้าน IT นั้นเป็นไปอย่างมีประสิทธิภาพและมีประสิทธิผล ครบถ้วน และสามารถบรรลุตามวัตถุประสงค์ของเป้าหมายโครงการ
4.10.3	หน่วยงานหรือทีมงานดูแลภาพรวมโครงการ (project management office : PMO) สามารถเป็นหน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการครอบคลุมทั้งด้าน IT และ non-IT ได้หรือไม่ และผู้ประกอบธุรกิจซึ่งเป็นบริษัทลูกของบริษัทแม่ต่างประเทศสามารถใช้หน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการจากสำนักงานใหญ่ประจำภูมิภาค (regional) แทนการจัดตั้งหน่วยงาน	PMO สามารถเป็นหน่วยงานหรือทีมงานที่ดูแลภาพรวมทั้งโครงการด้าน IT และโครงการที่เป็น non-IT ได้ และสามารถใช้ PMO ของสำนักงานใหญ่ประจำภูมิภาค (regional) ได้ อย่างไรก็ดี PMO ของสำนักงานใหญ่ประจำภูมิภาคต้องติดตามความคืบหน้าและภาพรวมของโครงการด้าน IT ที่สำคัญของผู้ประกอบธุรกิจ และรายงานต่อคณะกรรมการกำกับดูแลโครงการ (project steering committee) หรือผู้บริหารระดับสูงที่เกี่ยวข้องทราบอย่างครบถ้วน เพื่อให้การบริหารความเสี่ยงของโครงการเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล รวมทั้งโครงการสามารถบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้

ลำดับ	คำถาม	คำตอบ
	หรือทีมงานใหม่ในประเทศเพื่อทำหน้าที่ดังกล่าวได้หรือไม่	
4.10.4	การสอบทานคำสั่งในการเขียนโปรแกรม (source code review) มีความถี่ในการจัดทำอย่างไร	ผู้ประกอบธุรกิจควรจัดให้มี source code review ในรูปแบบ automated หรือแบบ manual เมื่อมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ที่มีนัยสำคัญ และมีความเสี่ยงในด้านความมั่นคงปลอดภัยของระบบ ซึ่งดำเนินการโดยบุคคลที่มีความเป็นอิสระ เช่น ผู้สอบทานไม่ใช่ทีมที่เป็นผู้พัฒนาโปรแกรมเอง เป็นต้น ทั้งนี้ ในกรณีของผู้ประกอบธุรกิจที่มีระดับความเสี่ยงสูง ให้ใช้วิธีการสอบทานแบบ manual เมื่อมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ที่มีนัยสำคัญ ซึ่งมีความเสี่ยงด้านความมั่นคงปลอดภัย
4.11	แนวปฏิบัติในการสอบทานคำสั่งของการเขียนโปรแกรม (source code review) ของผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูงมีรายละเอียดของการปฏิบัติที่แตกต่างจากแนวปฏิบัติของผู้ประกอบธุรกิจอื่น ๆ อย่างไร	ข้อแตกต่างของการแนวปฏิบัติมีรายละเอียด ดังนี้ **ผู้ที่<u>ไม่ใช่</u>ผู้ประกอบธุรกิจระดับความเสี่ยงสูง** สามารถสอบทาน source code เพื่อระบุข้อบกพร่องและแก้ไขก่อนนำขึ้นระบบเพื่อใช้งานจริงได้ 2 วิธี ได้แก่ (1) สอบทานโดยใช้ระบบอัตโนมัติ (automated tool) ซึ่งอาจดำเนินการโดยผู้พัฒนาโปรแกรมเอง หรือ (2) ให้บุคคลที่ไม่ใช่ผู้พัฒนาโปรแกรม เป็นผู้สอบทาน source code (manual source code review) **ผู้ประกอบธุรกิจระดับความเสี่ยงสูง** ให้บุคคลที่มีความเชี่ยวชาญและเป็นอิสระจากผู้พัฒนาโปรแกรมเป็นผู้สอบทาน source code (manual source code review หรือ white-box testing) ทั้งนี้ การตรวจสอบโดยผู้เชี่ยวชาญสามารถใช้เครื่องมือ (tool) สนับสนุนการดำเนินการได้
4.11.1	ข้อกำหนดสำหรับผู้ประกอบธุรกิจความเสี่ยงสูง ซึ่งกำหนดให้มีการสอบทานคำสั่งในการเขียนโปรแกรมแบบ manual โดยผู้เชี่ยวชาญที่มีความเป็นอิสระจากผู้พัฒนาโปรแกรม จะทราบได้อย่างไรว่าบุคลากรดังกล่าวมีความเป็นอิสระและมีความเชี่ยวชาญครบถ้วนแล้ว	<u>ความเชี่ยวชาญของผู้ที่สอบทานคำสั่งของโปรแกรม</u>: ผู้ประกอบธุรกิจสามารถกำหนดรายละเอียดคุณสมบัติของบุคลากรได้ตามความเหมาะสม เช่น ความรู้และประสบการณ์ในการเขียนโปรแกรม วุฒิการศึกษา เป็นต้น <u>ความเป็นอิสระของผู้สอบทานคำสั่งของโปรแกรม</u>: ผู้ประกอบธุรกิจสามารถพิจารณาความเป็นอิสระตามตัวอย่างดังนี้ เพื่อให้มีการ check and balance ในการพัฒนาโปรแกรมที่ดี ● ผู้สอบทานคำสั่งของโปรแกรมไม่ใช่บุคคลเดียวกันกับผู้พัฒนาโปรแกรม ● ผู้สอบทานคำสั่งของโปรแกรมไม่ได้อยู่ภายใต้การบังคับบัญชาของผู้พัฒนาโปรแกรม ● ผู้สอบทานคำสั่งของโปรแกรมไม่มีส่วนได้ส่วนเสียกับความสำเร็จของโปรแกรมโดยตรง เช่น ไม่ได้เป็นสมาชิกของทีมที่รับผิดชอบในการพัฒนาระบบ เป็นต้น

ลำดับ	คำถาม	คำตอบ
4.11.2	การตรวจสอบหรือสอบทานชุดคำสั่งคอมพิวเตอร์ (source code review) ในส่วนของซอฟต์แวร์ที่ใช้บริการจากผู้ให้บริการ เช่น Off-the-shelf software เป็นต้น จะดำเนินการอย่างไร	ผู้ประกอบธุรกิจควรพิจารณาการควบคุมอื่นทดแทน (compensate control) กรณีที่ไม่มีสิทธิเข้าถึงและสามารถสอบทาน source code ได้ เช่น จัดให้มีกระบวนการคัดเลือกซอฟต์แวร์ที่ดี เพื่อให้ซอฟต์แวร์ที่นำมาใช้งานภายในองค์กรมีความมั่นคงปลอดภัย หรือตรวจสอบข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาซอฟต์แวร์ของผู้ให้บริการหรือเจ้าของผลิตภัณฑ์ เป็นต้น
4.11.3	การดำเนินการทดสอบ Unit test จะต้องมีการจัดทำ Unit test script หรือไม่ เพื่อเป็นหลักฐานที่แสดงได้ว่ามีการทดสอบจริง	วัตถุประสงค์ของการทดสอบระบบในขั้นตอนต่าง ๆ เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน การตรวจประเมินเกี่ยวกับมาตรการควบคุมในกระบวนการพัฒนาระบบสามารถใช้หลักฐานที่รวบรวมได้จากหลายแหล่งหรือหลายวิธีการ เช่น การตรวจสอบบันทึกข้อมูลเกี่ยวกับการทดสอบระบบ การตรวจสอบขั้นตอนการปฏิบัติงาน (documented procedure) การสัมภาษณ์งานผู้ปฏิบัติงาน และการสังเกตกระบวนการทำงาน (walk through) เป็นต้น ดังนั้น หากบริษัทไม่มีการจัดเก็บหรือจัดทำ unit test script ผู้ตรวจสอบยังคงสามารถใช้หลักฐานอื่นเพื่อการตรวจสอบได้
4.12	**การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT**	
4.12.1	กรณีที่พบไวรัสบนเครื่องคอมพิวเตอร์หรือพบการโจมตี ซึ่งไม่ก่อให้เกิดผลกระทบใด ๆ กับผู้ประกอบธุรกิจ ต้องรายงานสำนักงาน ก.ล.ต. หรือไม่	ผู้ประกอบธุรกิจรายงานเหตุการณ์ดังกล่าวเฉพาะในกรณีที่มีส่งผลกระทบต่อการดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของผู้ประกอบธุรกิจหรือลูกค้าในวงกว้าง อย่างไรก็ดี ผู้ประกอบธุรกิจควรติดตาม และสืบหาข้อเท็จจริงของการตกเป็นเป้าหมายในการโจมตี เพื่อเตรียมแผนการรับมือหรือขอความช่วยเหลือจากหน่วยงานต่าง ๆ ได้ทันการณ์ ทั้งนี้ ผู้ประกอบธุรกิจสามารถสรุปเหตุการณ์ หรือแจ้งเตือนเหตุการณ์ดังกล่าวต่อผู้ประกอบธุรกิจรายอื่น ๆ ในอุตสาหกรรมตลาดทุนได้ ผ่านช่องทางการแลกเปลี่ยนข้อมูลภัยคุกคามของ TCM-CERT
4.12.2	[New] “ทรัพย์สินของลูกค้า” ในข้อกำหนดการรายงานเหตุการณ์ผิดปกติด้าน IT ให้รวมถึงทรัพย์สินประเภทใด หรือของบุคคลใดบ้าง	“ทรัพย์สินของลูกค้า” หมายรวมถึง ทรัพย์สินด้าน IT และทรัพย์สินอื่น ๆ ของลูกค้า อาทิ สินทรัพย์ดิจิทัล เงินสด หรือทรัพย์สินทางการเงินประเภทอื่น ๆ ที่อยู่ภายใต้ความดูแลของผู้ประกอบธุรกิจ หากเกิดเหตุการณ์ผิดปกติที่ส่งผลให้ทรัพย์สินเหล่านี้สูญหายหรือเสียหาย ผู้ประกอบธุรกิจต้องรายงานเหตุการณ์ดังกล่าวต่อสำนักงาน ก.ล.ต. **<u>ตัวอย่างเหตุการณ์ที่ควรเข้าข่ายต้องรายงาน</u>** • การสูญหายของสินทรัพย์ดิจิทัลที่ส่งผลกระทบต่อลูกค้า

ลำดับ	คำถาม	คำตอบ
		• บัญชีลูกค้าภายใต้การดูแลของผู้ประกอบธุรกิจ ถูกโจมตีหรือถูกเข้าควบคุมโดยผู้ไม่ประสงค์ดี
4.12.3	ผู้ประกอบธุรกิจจำเป็นต้องรายงานเฉพาะกรณีเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญเท่านั้น หรือต้องรายงานเหตุการณ์ที่ส่งผลกระทบกับระบบสารสนเทศอื่น ๆ ด้วย	เหตุการณ์ที่ต้องรายงานต่อสำนักงาน ก.ล.ต. ไม่ได้จำกัดเพียงเหตุการณ์ที่เกิดขึ้นต่อระบบที่มีความสำคัญเท่านั้น แต่ให้รวมถึงระบบอื่น ๆ ที่เกี่ยวข้องด้วย หากเหตุการณ์นั้นอาจส่งผลกระทบต่อลูกค้า การดำเนินการ ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินการของผู้ประกอบธุรกิจ
4.12.4	กรณีเหตุการณ์ด้าน IT แม้จะเป็นเหตุการณ์ดังต่อไปนี้ แต่มิได้ส่งผลกระทบต่อลูกค้าในวงกว้าง ผู้ประกอบธุรกิจจำเป็นต้องรายงานเหตุการณ์ต่อสำนักงาน ก.ล.ต. หรือไม่ (1) การละเมิดต่อข้อมูลส่วนบุคคลที่เกิดจากเหตุการณ์ผิดปกติด้าน IT (2) ทรัพย์สินของลูกค้าสูญหาย หรือเสียหาย (3) การบุกรุกเข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (4) เหตุการณ์ที่ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement) เป็นต้น (5) การหยุดชะงักของระบบงาน (system disruption) ตามระยะเวลาที่กำหนดในแนวปฏิบัติ	ผู้ประกอบธุรกิจควรรายงานสำนักงาน ในกรณีที่มีเหตุการณ์ด้าน IT ซึ่งอาจส่งผลกระทบต่อธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของผู้ประกอบธุรกิจ หรือต่อลูกค้าในวงกว้าง โดยครอบคลุมเหตุการณ์อย่างน้อยดังต่อไปนี้ ● กรณีเหตุการณ์ที่ระบุในข้อ (1) – (4) : ผู้ประกอบธุรกิจควรมีการพิจารณาว่า เหตุการณ์ได้ส่งผลกระทบต่อธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของผู้ประกอบธุรกิจ หรือต่อลูกค้าในวงกว้างหรือไม่ โดยใช้หลักเกณฑ์การรายงานสำนักงานที่บริษัทได้จัดทำขึ้นภายในองค์กร ทั้งนี้ เพื่อให้เกิดความสอดคล้องในการปฏิบัติ ผู้ประกอบธุรกิจสามารถกำหนดเงื่อนไขหรือแนวทางการรายงานเหตุการณ์ต่อสำนักงาน โดยเทียบเคียงกับการรายงานเหตุการณ์ดังกล่าวต่อผู้บริหารระดับสูงขององค์กรได้ เช่น เหตุการณ์ใดที่เข้าเงื่อนไขต้องรายงานเหตุให้ผู้บริหารระดับสูงขององค์กรทราบก็รายงานเหตุการณ์นั้น ให้สำนักงานทราบด้วยเช่นกัน ● กรณีเหตุการณ์ที่ระบุในข้อ (5) : ให้อ้างอิงระยะเวลาระบบหยุดชะงักที่เข้าข่ายต้องรายงานสำนักงาน ซึ่งกำหนดไว้ในแนวปฏิบัติ นป. 6/2567
4.12.5	[New] กรณีที่ผู้ประกอบธุรกิจต้องปิดปรับปรุงระบบเพื่อ system maintenance ทำให้ระบบงานไม่สามารถใช้งานได้เป็นระยะเวลาต่อเนื่องเกินจากที่ข้อกำหนดได้ระบุไว้ (เช่น หน้าเว็บไซต์หลักไม่สามารถใช้งานได้เกิน 60 นาที เป็นต้น) ผู้ประกอบธุรกิจต้องรายงานสำนักงานหรือไม่	ผู้ประกอบธุรกิจไม่ต้องรายงานเหตุการณ์ดังกล่าวต่อสำนักงาน หากเป็นการปิดปรับปรุงระบบ (system maintenance) ที่มีการแจ้งให้ลูกค้าทราบล่วงหน้าแล้ว ● ทั้งนี้ system maintenance ที่ไม่ต้องรายงานต่อสำนักงาน ควรเป็นการปิดปรับปรุงระบบที่มีการวางแผนไว้ล่วงหน้า (planned downtime) เช่น การบำรุงรักษาระบบ การอัปเกรดซอฟต์แวร์หรือฮาร์ดแวร์ การทดสอบระบบ หรือเปลี่ยนโครงสร้างพื้นฐาน เป็นต้น ● กรณีที่เป็นการปิดปรับปรุงระบบแบบกระทันหัน หรือไม่ได้วางแผนไว้ล่วงหน้า (unplanned downtime) แม้จะมีการแจ้งให้ลูกค้าทราบล่วงหน้า หากเป็นการแจ้งให้ลูกค้าทราบแบบกระชั้นชิด เช่น 1-2 ชั่วโมง

ลำดับ	คำถาม	คำตอบ
		ระบบจะต้องปิดปรับปรุง เนื่องจากพบเจอปัญหาเทคนิค เป็นต้น การปิดปรับปรุงระบบแบบกระทันหันนั้น อาจส่งผลกระทบต่อผู้ใช้งานได้ ในกรณีนี้ ควรต้องรายงานเหตุการณ์ดังกล่าวต่อสำนักงาน หากการปิดปรับปรุงระบบดังกล่าวส่งผลให้ระบบงานไม่สามารถใช้งานได้เกินกรอบระยะเวลาที่หลักเกณฑ์กำหนด
4.12.6	กรณีบริษัทที่มีขนาดเล็ก ทำให้มีการรายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้บริหารระดับสูงทุกเหตุการณ์ แม้ว่าเหตุการณ์ดังกล่าวจะมีผลกระทบเพียงเล็กน้อย ในกรณีนี้ บริษัทสามารถกำหนดเงื่อนไขในการรายงานผู้บริหารระดับสูง แยกกันกับเงื่อนไขในการรายงานสำนักงาน ก.ล.ต. ได้หรือไม่	ผู้ประกอบธุรกิจสามารถจัดทำหลักเกณฑ์ในการรายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้บริหารระดับสูง แยกจากหลักเกณฑ์ในการรายงานสำนักงานได้ อย่างไรก็ดี หลักเกณฑ์ดังกล่าวต้องได้รับความเห็นชอบจากผู้บริหารระดับสูงหรือคณะกรรมการบริษัทด้วย
4.12.7	กรณี website defacement ที่ต้องรายงานสำนักงาน และต้องจัดให้มีการตรวจสอบด้าน IT แบบเต็มรูปแบบ หมายถึงกรณีใด	การโดนปลอมแปลงหน้าเว็บไซต์ (website defacement) และการถูกสร้างเว็บไซต์ปลอม (imposter/fake website) เป็นเหตุการณ์ที่แตกต่างกัน โดยมีความแตกต่างกัน ดังนี้ • **website defacement** เป็นการโจมตีที่เว็บไซต์ที่อยู่ภายใต้การควบคุมของผู้ประกอบธุรกิจที่อาจถูกผู้ไม่ประสงค์ดี hack หรือ compromised เพื่อเปลี่ยนแปลงลักษณะการแสดงผลหรือเนื้อหาข้อมูลบนเว็บไซต์ ซึ่งผู้โจมตีมีวัตถุประสงค์เพื่อ (1) ปรับเปลี่ยนหน้าเว็บไซต์เป้าหมายไปเป็นหน้าเว็บไซต์ใหม่ หรือ (2) เพิ่มเติมเนื้อหา (content) ที่ไม่พึงประสงค์ลงบนหน้าเว็บไซต์เดิม เช่น วางข้อความหรือลิงก์ที่ไม่เหมาะสม เป็นต้น กรณีที่เว็บไซต์ถูก defacement ผู้ประกอบธุรกิจต้องรายงานสำนักงานในช่องทาง incident report • **imposter/fake website** คือการที่ผู้ไม่ประสงค์ดีสร้างเว็บไซต์หลอกลวงลูกค้าที่มีหน้าตาเสมือนเว็บไซต์จริง ซึ่งอาจถูกใช้เพื่อให้ผู้ใช้งานสำคัญผิดว่าเป็นเว็บไซต์ของผู้ประกอบธุรกิจและขโมยข้อมูลสำคัญ เช่น ข้อมูลเข้าสู่ระบบ ข้อมูลบัตรเครดิต เป็นต้น เว็บไซต์เลียนแบบ/เว็บไซต์ปลอมเหล่านี้ อยู่นอกเหนือการควบคุมของผู้ประกอบธุรกิจ ทั้งนี้ กรณีพบเจอเว็บไซต์เลียนแบบ/เว็บไซต์ปลอม ผู้ประกอบธุรกิจสามารถแจ้งเบาะแสหรือเหตุการณ์ต่อสำนักงาน ก.ล.ต. ที่ SEC Scam Alert หน่วยงานที่เกี่ยวข้อง และลูกค้าของผู้ประกอบธุรกิจได้ แต่ไม่ต้องรายงานสำนักงานผ่านระบบ incident report
4.12.8	กรณีที่ผู้ประกอบธุรกิจพบเจอการที่บุคคลอื่นทำการปลอมเว็บไซต์ขึ้นมาใหม่ให้เหมือนหรือคล้ายกับเว็บไซต์ของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องรายงานเหตุการณ์ดังกล่าวในช่องทาง incident report ภายในกรอบระยะเวลาที่ประกาศกำหนดหรือไม่	

ลำดับ	คำถาม	คำตอบ
4.12.9	กรณีที่ผู้ประกอบธุรกิจพบว่ามีบุคคลแอบอ้างชื่อของบริษัทเพื่อทำการหลอกลวงลูกค้าหรือประชาชน เช่น เว็บไซต์ปลอม บัญชี social media ปลอม เป็นต้น สามารถแจ้งเหตุการณ์ดังกล่าวต่อสำนักงาน ก.ล.ต. อย่างไร	ผู้ประกอบธุรกิจสามารถแจ้งเบาะแสการหลอกลงทุนในตลาดทุนผ่านช่องทาง SEC Scam Alert ซึ่งเป็นช่องทางที่สำนักงาน ก.ล.ต. จัดทำขึ้นเพื่อดำเนินการตรวจสอบข้อมูลที่ได้รับแจ้งอย่างเร่งด่วนและแจ้งไปยังหน่วยงานที่เกี่ยวข้องเพื่อปิดกั้นเนื้อหาหรือช่องทางการหลอกลงทุนเพื่อป้องกันประชาชนไม่ให้เสียหายเพิ่มขึ้น
4.12.10	กรณีพบข้อมูลลูกค้า 10 รายรั่วไหล ต้องรายงานสำนักงานหรือไม่	ให้ผู้ประกอบธุรกิจดำเนินการ ดังนี้ (1) พิจารณาจากหลักเกณฑ์การรายงานเหตุการณ์ของบริษัทต่อผู้บริหารระดับสูงหรือคณะกรรมการบริษัท ว่ามีการกำหนดเงื่อนไขของเหตุการณ์เช่นนี้ไว้อย่างไร หากกำหนดให้รายงานผู้บริหารระดับสูงหรือคณะกรรมการบริษัท ก็ควรรายงานสำนักงาน ก.ล.ต. ด้วย หากไม่ได้กำหนดไว้ ให้พิจารณาจาก (2) (2) ในกรณีนี้ ให้ผู้ประกอบธุรกิจตรวจสอบระบบเพิ่มเติมว่ามีร่องรอยการโจมตีระบบ (indicator of compromise) หรือตรวจสอบ log ต่าง ๆ หากเชื่อได้ว่า เหตุการณ์ที่เกิดขึ้นนี้เกิดจากระบบของบริษัท ซึ่งอาจส่งผลกระทบในวงกว้าง/ส่งผลกระทบต่อชื่อเสียงองค์กร ให้รายงานสำนักงานด้วย อย่างไรก็ดี ผู้ประกอบธุรกิจควรพิจารณารายงานกรณี Data Breach ตามที่กฎหมายอื่นกำหนดด้วย เช่น สคส. เป็นต้น
4.12.11	ผู้ประกอบธุรกิจสามารถพิจารณาระดับความรุนแรงของเหตุการณ์ที่ควรรายงานต่อสำนักงาน ก.ล.ต. เพิ่มเติมจาก “กรอบระยะเวลาหยุดชะงัก ก่อนที่จะรายงานสำนักงาน” ได้หรือไม่	กรณีของเหตุการณ์ระบบหยุดชะงัก (ระบบจับคู่คำสั่งซื้อขาย ระบบจัดการคำสั่งซื้อขาย ระบบรับส่งคำสั่งซื้อขาย หน้าเว็บไซต์หลัก และระบบฝากและถอนทรัพย์สิน) ผู้ประกอบธุรกิจควรอ้างอิงกรอบระยะเวลาที่ระบบหยุดชะงักซึ่งต้องรายงานสำนักงาน ก.ล.ต. ตามที่กำหนดในแนวปฏิบัติ เพื่อให้ผู้ประกอบธุรกิจในตลาดทุนมีมาตรฐานการรายงานเหตุการณ์ที่สอดคล้องกัน สำหรับเหตุการณ์ผิดปกติด้าน IT อื่น ๆ ผู้ประกอบธุรกิจสามารถกำหนดหลักเกณฑ์การพิจารณาความรุนแรงของเหตุการณ์ซึ่งต้องรายงานสำนักงาน ก.ล.ต. เพิ่มเติมได้ตามความเหมาะสม
4.12.12	กรณีที่ระบบรวมศูนย์ (เช่น ระบบของ SET เป็นต้น) หยุดชะงัก ผู้ประกอบธุรกิจทุกรายที่ใช้ระบบดังกล่าวต้องรายงานต่อสำนักงานหรือไม่	หากมีข้อเท็จจริงว่าปัญหามิได้เกิดจากระบบงานของผู้ประกอบธุรกิจ แต่เกิดจากระบบของหน่วยงานซึ่งอยู่ภายใต้การกำกับดูแลของสำนักงาน ก.ล.ต. ผู้ประกอบธุรกิจไม่จำเป็นต้องรายงานสำนักงาน ทั้งนี้ หากปัญหาเกิดขึ้นจากหน่วยงานภายนอกที่ไม่ได้อยู่ภายใต้การกำกับดูแลของสำนักงาน ก.ล.ต. ผู้ประกอบธุรกิจมีหน้าที่ต้องรายงานเหตุการณ์ดังกล่าวด้วย

<table>
<tr><th>ลำดับ</th><th>คำถาม</th><th>คำตอบ</th></tr>
<tr><td>4.12.13</td><td>กรณีที่ระบบหยุดชะงัก และผู้ประกอบธุรกิจมีช่องทางให้บริการที่หลากหลาย ซึ่งลูกค้าสามารถใช้บริการได้ทันที (เช่น มีระบบรับส่งคำสั่งซื้อขายมากกว่า 1 ระบบ) ผู้ประกอบธุรกิจต้องรายงานต่อสำนักงาน ก.ล.ต. หรือไม่</td><td>แม้ว่าผู้ประกอบธุรกิจจะมีระบบหรือช่องทางอื่น ๆ ทดแทน ซึ่งลูกค้าสามารถเปลี่ยนไปใช้บริการได้ทันที แต่ลูกค้าหลายรายอาจไม่ได้รับความสะดวกในการใช้บริการ หรือได้รับผลกระทบจากการเปลี่ยนแปลงลักษณะการใช้บริการปกติของตน เช่น ต้องเปลี่ยนแอปพลิเคชันที่ใช้งาน หรือเปลี่ยนเป็นการส่งคำสั่งผ่านทางโทรศัพท์หรืออีเมล กรณีนี้ให้ผู้ประกอบธุรกิจรายงานสำนักงาน ก.ล.ต. แต่หากกรณีที่ระบบหยุดชะงัก และผู้ประกอบธุรกิจมีระบบ IT สำรอง ทำให้ลูกค้ากลับมาใช้บริการได้ปกติก่อนถึงระยะเวลาที่ต้องรายงานต่อสำนักงาน ผู้ประกอบธุรกิจไม่จำเป็นต้องรายงานสำนักงาน ก.ล.ต.</td></tr>
<tr><td>4.12.14</td><td>กรณีที่ระบบหยุดชะงัก และผู้ประกอบธุรกิจเปลี่ยนไปใช้ระบบ IT สำรอง ทำให้ลูกค้ากลับมาใช้บริการได้ปกติ (ลูกค้าใช้งานผ่านแอปพลิเคชันหรือระบบเดิม) ก่อนถึงระยะเวลาที่ต้องรายงานสำนักงาน ก.ล.ต. ผู้ประกอบธุรกิจต้องรายงานต่อสำนักงานหรือไม่</td><td>ในกรณีที่ผู้ประกอบธุรกิจมีระบบ IT สำรองทำให้ลูกค้ากลับมาใช้บริการได้ปกติก่อนถึงระยะเวลาที่ต้องรายงานสำนักงาน ผู้ประกอบธุรกิจไม่จำเป็นต้องรายงานสำนักงาน ก.ล.ต.</td></tr>
<tr><td>4.12.15</td><td>กรณีระบบของสาขาผู้ประกอบธุรกิจล่ม ซึ่งอาจส่งผลกระทบต่อการให้บริการลูกค้าบางราย หรือบางสาขานั้น ผู้ประกอบธุรกิจจำเป็นต้องรายงานสำนักงาน ก.ล.ต. หรือไม่</td><td>หากเหตุการณ์นั้นไม่ได้ส่งผลกระทบต่อลูกค้าในวงกว้าง (ตามหลักเกณฑ์การพิจารณาที่บริษัทกำหนด) ผู้ประกอบธุรกิจไม่จำเป็นต้องรายงานเหตุการณ์ต่อสำนักงาน ก.ล.ต.</td></tr>
<tr><td>4.12.16</td><td>กรณีเหตุการณ์หยุดชะงักเกิดขึ้นระหว่างนอกเวลาทำการของสำนักงาน ก.ล.ต. เช่น
– เวลา night session ของ TFEX
– เวลากลางคืนสำหรับผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่เปิดทำการ 24 ชั่วโมงทุกวัน
– เหตุการณ์หยุดชะงักในวันเสาร์-อาทิตย์ ซึ่งเป็นเวลาทำการของผู้ประกอบธุรกิจ เป็นต้น
ผู้ประกอบธุรกิจต้องรายงานสำนักงานในเวลาใด</td><td>กรณีพบเหตุการณ์ที่เข้าเงื่อนไขต้องรายงานสำนักงาน นอกวันทำการของสำนักงาน ก.ล.ต. หรือนอกเวลา 8:30 น.– 16:30 น.
(1) ให้รายงานโดยไม่ชักช้า ภายในเวลา 10:00 น. ของวันทำการถัดไป (วันทำการของสำนักงาน ก.ล.ต.) ยกตัวอย่างเช่น
<table>
<tr><th>ตัวอย่างเวลาหยุดชะงัก</th><th>เวลาที่ต้องรายงานสำนักงาน</th></tr>
<tr><td>เวลา 21:00 น. ของวันพฤหัสบดี</td><td>ภายใน 10:00 น. ของวันศุกร์</td></tr>
<tr><td>เวลา 3:30 น. ของวันศุกร์</td><td>ภายใน 10:00 น. ของวันศุกร์</td></tr>
<tr><td>เวลา 9:00 น. ของวันเสาร์</td><td>ภายใน 10:00 น. ของวันจันทร์</td></tr>
<tr><td>เวลา 9:00 น. วันหยุดทำการของสำนักงาน ก.ล.ต. (สามารถดูรายละเอียดเพิ่มเติมได้ที่เว็บไซต์ของสำนักงาน https://www.sec.or.th/TH/Pages/ABOUTUS/HOLIDAY.aspx)</td><td>ภายใน 10:00 น. ของวันทำการถัดไป</td></tr>
</table>
(2) รายงานความคืบหน้า เมื่อมีการเปลี่ยนแปลงสถานการณ์ หรือตามที่สำนักงานร้องขอ จนกว่าระบบ IT จะกลับสู่การให้บริการได้อย่างเป็นปกติ</td></tr>
</table>

ลำดับ	คำถาม	คำตอบ
		(3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ
4.12.17	การรายงานเหตุการณ์ผิดปกติด้าน IT ผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด หมายถึงช่องทางใด	ช่องทางรายงานเหตุการณ์ผิดปกติด้าน IT ที่สำนักงานกำหนด คือ การรายงานผ่านเว็บไซต์ https://web-incident.sec.or.th/ ทั้งนี้ สำหรับผู้ประกอบธุรกิจที่ยังไม่เคยลงทะเบียน สามารถดูรายละเอียดการลงทะเบียนและการเข□าใช□งาน ได้ที่ https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-INCIDENTREPORT.aspx **หมายเหตุ:** ในกรณีที่มีเหตุขัดข้องในการรายงานผ่านเว็บไซต์ข้างต้น ผู้ประกอบธุรกิจสามารถรายงานทางวาจาต่อเจ้าหน้าที่ที่เกี่ยวข้อง หรือรายงานผ่านอีเมล incident-report@sec.or.th หลังจากนั้น ให้ผู้ประกอบธุรกิจรายงานข้อมูลผ่านเว็บไซต์อีกครั้งโดยไม่ชักช้าเมื่อไม่พบเหตุขัดข้องแล้ว
4.12.18	กรณีที่เป็นบริษัทในเครือ หรือใช้ infrastructure เดียวกันกับธนาคารพาณิชย์ จะสามารถใช้ผลทดสอบร่วมกันได้หรือไม่	หากผู้บริหารและบุคลากรของผู้ประกอบธุรกิจมีส่วนร่วมในการฝึกซ้อมร่วมกับบริษัทแม่หรือบริษัทในเครือ และได้นำผลการฝึกซ้อมดังกล่าวมาทบทวนและปรับปรุงแผนการบริหารจัดการเหตุการณ์ผิดปกติขององค์กรแล้ว การฝึกซ้อมดังกล่าวก็เป็นไปตามวัตถุประสงค์ของหลักเกณฑ์ ทั้งนี้ หากผู้บริหารและบุคลากรของผู้ประกอบธุรกิจไม่ได้มีส่วนร่วมในการฝึกซ้อม จะไม่สามารถนำผลการทดสอบของบริษัทแม่หรือบริษัทในเครือมาใช้อ้างอิงได้
4.12.19	การจัดทำ cyber security drill ต้องจัดทำถึงระดับใด และกรณีที่เป็นบริษัทในเครือ หรือใช้ infrastructure เดียวกันกับธนาคารพาณิชย์ จะสามารถใช้ผลทดสอบร่วมกันได้หรือไม่	วัตถุประสงค์ของการจัดทำ cyber security drill เพื่อให้ผู้บริหารและบุคลากรที่เกี่ยวข้องภายในบริษัทในทุกระดับชั้น ไม่เฉพาะแต่เพียงฝ่ายงาน IT ได้มีส่วนร่วม ในการทดสอบแผนการบริหารจัดการเหตุการณ์ด้าน cyber ซึ่งจะช่วยให้บุคลากรที่เกี่ยวข้องภายในบริษัท สามารถปฏิบัติงานตามแผนเมื่อเกิดเหตุการณ์ได้อย่างมีประสิทธิภาพ และประสิทธิผล และยังสามารถนำผลการทดสอบที่ได้กลับมาทบทวนความถูกต้องเหมาะสมของแผนที่วางไว้ได้ ทั้งนี้ ผู้ประกอบธุรกิจสามารถพิจารณาจัดทำได้ทั้งรูปแบบ table-top exercise หรือ full live ตามที่เห็นสมควร
4.13	**แผนฉุกเฉินด้าน IT**	
4.13.1	สำนักงานมีตัวอย่างการจัดทำแผนฉุกเฉินด้าน IT หรือไม่	ผู้ประกอบธุรกิจสามารถศึกษาแนวทางการจัดทำแผนฉุกเฉินด้าน IT ที่ดีได้จาก NIST Special Publication 800-34 Contingency Planning Guide for Federal Information Systems
4.13.2	ในกรณีที่ผู้ประกอบธุรกิจมีแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ที่ครอบคลุมการจัดทำแผนฉุกเฉินด้าน IT และได้รับความเห็นชอบจาก	ผู้ประกอบธุรกิจสามารถใช้แผน BCP แทนการจัดทำแผนฉุกเฉินด้าน IT ได้ หากแผน BCP ดังกล่าว ครอบคลุมและมีเนื้อหาในเรื่องการจัดทำแผนฉุกเฉินด้าน IT เพียงพอต่อการดำเนินการ และเป็นไปตามข้อกำหนดเรื่องแผนฉุกเฉินด้าน IT ที่หลักเกณฑ์กำหนดอย่างครบถ้วน

ลำดับ	คำถาม	คำตอบ
	คณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายแล้ว ผู้ประกอบธุรกิจสามารถใช้แผน BCP ดังกล่าวแทนการจัดทำแผนฉุกเฉินด้าน IT ได้หรือไม่	
4.13.3	ผู้ประกอบธุรกิจสามารถกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ (Recovery Time Objective : RTO) ได้ด้วยตนเอง ซึ่งสอดคล้องกับ RTO ของกระบวนการทางธุรกิจ (business process) แต่ไม่สอดคล้องกับข้อกำหนดของสำนักงาน ก.ล.ต. ได้หรือไม่	หลักการของการกำหนด RTO ที่เหมาะสม เริ่มต้นจากการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) เพื่อให้ทราบถึงผลกระทบเมื่อระบบงานใดระบบงานหนึ่งหยุดชะงัก และนำข้อมูลดังกล่าวมาวิเคราะห์เพื่อกำหนดกรอบเป้าหมาย RTO และ RPO ให้กับองค์กร พร้อมทั้งจัดให้มีแผนงานและทรัพยากรที่จำเป็นต่าง ๆ เพื่อให้สามารถกู้คืนระบบได้ภายในกรอบเป้าหมายที่กำหนดไว้ อย่างไรก็ดี ประกาศแนวปฏิบัติของสำนักงาน ก.ล.ต. มีการกำหนดกรอบเป้าหมายของ RTO ให้ไม่ควรเกิน 4 ชั่วโมง <u>สำหรับระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญ</u> (ระบบงานอื่น ๆ สามารถพิจารณาได้ตามความเหมาะสม) เพื่อให้ผู้ประกอบธุรกิจในตลาดทุนมีการบริหารจัดการระบบ IT ซึ่งสนับสนุนกระบวนการทางธุรกิจที่สำคัญภายใต้กรอบระยะเวลาเป้าหมายในการกู้คืนระบบที่เป็นมาตรฐานเดียวกัน ในกรณีที่ผู้ประกอบธุรกิจมีข้อจำกัด ผู้ประกอบธุรกิจสามารถจัดให้มีการให้บริการในลักษณะ manual เพื่อให้ลูกค้าสามารถกลับมาใช้บริการได้อย่างต่อเนื่องแทนการกู้คืนระบบ IT ภายในระยะเวลาดังกล่าวได้ ทั้งนี้ การกำหนด RTO ที่ไม่เหมาะสม เช่น RTO ที่นานเกินจริง เป็นต้น อาจส่งผลให้เกิดการจัดสรรหรือเตรียมทรัพยากรที่ไม่เพียงพอ อีกทั้งอาจไม่สอดคล้องกับเป้าหมายในการดำเนินธุรกิจขององค์กรได้
4.13.4	ขอบเขต (scope) ในการทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินมีข้อกำหนดอย่างไรบ้าง ผู้ประกอบธุรกิจสามารถกำหนดได้เองหรือไม่ เช่น ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินเฉพาะระบบ IT ที่มีนัยสำคัญ ปีละ 1 ครั้ง และระบบอื่น ๆ ได้ตามความเหมาะสม เป็นต้น	ผู้ประกอบธุรกิจควรทดสอบและทบทวนการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง ซึ่งสามารถกำหนดขอบเขตและเหตุการณ์ที่ใช้ในการทดสอบประจำปีได้ตามความเหมาะสม อย่างไรก็ดี ควรเลือกทดสอบเหตุการณ์ที่มีโอกาสที่จะเกิดขึ้น (likelihood) และอาจส่งผลกระทบให้กระบวนการทางธุรกิจที่สำคัญหยุดชะงัก (impact) เช่น การหยุดชะงักของระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญ เป็นต้น กรณีระบบอื่น ๆ ผู้ประกอบธุรกิจสามารถพิจารณาขอบเขตเพื่อทำการทบทวนและทดสอบการปฏิบัติตามแผนได้ตามความเหมาะสม
4.13.5	การทดสอบแผนฉุกเฉินด้าน IT สามารถดำเนินการแบบ table-top exercise ได้หรือไม่	ผู้ประกอบธุรกิจสามารถกำหนดรูปแบบการทดสอบแผนฉุกเฉิน (เช่น walkthrough, table top หรือ technical exercise เป็นต้น) ให้สอดคล้องกับวัตถุประสงค์ของการทดสอบ อย่างไรก็ดี วิธีการทดสอบ

ลำดับ	คำถาม	คำตอบ
		ที่ใช้ควรมีความเหมาะสมกับสภาพแวดล้อมและความเสี่ยง โดยครอบคลุมเหตุการณ์ (scenario) ที่อาจส่งผลกระทบต่อกระบวนการทางธุรกิจที่สำคัญ เพื่อให้มั่นใจได้ว่าจะสามารถใช้งานแผนฉุกเฉินด้าน IT ได้อย่างมีประสิทธิผลเมื่อเกิดเหตุการณ์ที่ส่งผลต่อการดำเนินธุรกิจ
4.13.6	การทดสอบแผนฉุกเฉินด้าน IT ครอบคลุมถึงการทดสอบแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ด้วยหรือไม่	แผนฉุกเฉินด้าน IT และแผน BCP มีวัตถุประสงค์ที่แตกต่างกัน กล่าวคือ ● แผน BCP มีวัตถุประสงค์เพื่อกำหนดกิจกรรม กระบวนการ หรือขั้นตอนเพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง เมื่อเกิดเหตุการณ์ฉุกเฉิน เช่น ภัยธรรมชาติ อัคคีภัย และภัยคุกคามทางไซเบอร์ เป็นต้น ● แผนฉุกเฉินด้าน IT มีวัตถุประสงค์เพื่อกำหนดกิจกรรม กระบวนการหรือขั้นตอนเพื่อการกู้คืนระบบ IT ที่มีนัยสำคัญ (critical IT functions) ให้กลับมาใช้งานได้เป็นปกติ ตามที่บริษัทได้กำหนดเป้าหมายของ Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) ไว้ อย่างไรก็ดี แผนฉุกเฉินด้าน IT มักถูกกำหนดไว้เป็นส่วนหนึ่งของแผน BCP ดังนั้น ผู้ประกอบธุรกิจสามารถทดสอบแผนฉุกเฉินด้าน IT ควบคู่กับแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ได้ (รายละเอียดเพิ่มเติมตามแผนภาพในภาคผนวก 5)
4.13.7	การทดสอบให้พนักงานสามารถปฏิบัติงานจากสถานที่ใดก็ได้ (work from anywhere) นับว่าเป็นการทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT หรือไม่	วัตถุประสงค์ของการทดสอบแผนฉุกเฉินด้าน IT คือ การทำให้มั่นใจได้ว่าแผนฉุกเฉินด้าน IT ที่กำหนดไว้ สามารถใช้งานเพื่อกู้คืนระบบ IT ที่มีนัยสำคัญ (critical IT functions) ให้กลับมาใช้งานได้เป็นปกติอย่างมีประสิทธิผล อย่างไรก็ดี การอนุญาตให้พนักงาน work form anywhere (WFA) อาจไม่ใช่วิธีการทดสอบแผนฉุกเฉินด้าน IT ที่ดี เนื่องจากไม่ได้แสดงให้เห็นถึงการทดสอบขั้นตอนการกู้คืนระบบงานที่มีนัยสำคัญให้กลับมาใช้งานได้เป็นปกติ
4.13.8	กรณีระบบงานของบริษัทอยู่บนระบบคลาวด์ (Cloud) ทั้งหมด จำเป็นต้องจัดทำขั้นตอนการกู้คืนระบบด้วยหรือไม่	การใช้งาน Cloud แต่ละประเภท (SaaS PaaS หรือ IaaS) มีขอบเขตความรับผิดชอบของผู้ใช้งาน และผู้ให้บริการ Cloud ที่แตกต่างกัน ผู้ประกอบธุรกิจควรพิจารณาถึงสถานการณ์ (scenario) ที่จะส่งผลกระทบต่อระบบ IT ของบริษัทและจัดให้มีขั้นตอนการกู้คืนระบบอย่างเพียงพอ ตัวอย่าง กรณีผู้ประกอบธุรกิจใช้บริการ Cloud ในรูปแบบ Infra as a Service (IaaS) เช่น กรณีใช้งาน Virtual machine (Compute Engine) ที่ผู้ประกอบธุรกิจมีหน้าที่ในการรักษาความปลอดภัยของระบบด้วยตนเอง ผู้ประกอบธุรกิจควรคำนึงถึงกรณีระบบถูกโจมตีโดย

ลำดับ	คำถาม	คำตอบ
		ransomware ซึ่งในกรณีนี้หน้าที่ในการกู้คืนระบบจะอยู่ที่ผู้ประกอบธุรกิจทั้งหมด
4.13.9	[New] กรณีของผู้ประกอบธุรกิจขนาดเล็กที่อาจมีข้อจำกัดในการจัดสรรทรัพยากรด้านการบริหารจัดการแผนฉุกเฉินด้าน IT หากผู้ประกอบธุรกิจขนาดเล็กต้องการจัดให้มีแผนฉุกเฉินด้าน IT ที่มีประสิทธิภาพในองค์กร ผู้ประกอบธุรกิจควรดำเนินการอย่างไร	ผู้ประกอบธุรกิจขนาดเล็กสามารถจัดทำแผนบริหารจัดการกรณีฉุกเฉินด้าน IT ได้อย่างมีประสิทธิภาพ ภายใต้ทรัพยากรที่จำกัด โดยสามารถพิจารณาแนวทางต่าง ๆ ได้ดังตัวอย่างต่อไปนี้ ● จัดลำดับความสำคัญของระบบ โดยมุ่งเน้นระบบสำคัญที่กระทบต่อการดำเนินธุรกิจและลูกค้า ซึ่งทราบได้จากการวิเคราะห์ผลกระทบทางธุรกิจ (business impact assessment) ● ใช้บริการจากผู้เชี่ยวชาญภายนอก เช่น ระบบสำรองข้อมูล หรือบริการกู้คืนระบบจากเหตุฉุกเฉินผ่านผู้ให้บริการที่มีความเชี่ยวชาญ ● จัดทำแผนฉุกเฉินอย่างกระชับและใช้งานได้จริง มีการระบุขั้นตอน ช่องทางการติดต่อ (call tree) และบทบาทที่ชัดเจน ● มีขั้นตอนการดำเนินงานแบบ manual ชั่วคราว เช่น หากระบบไม่สามารถใช้งานได้ ให้พนักงานสามารถดำเนินงานแบบ manual ชั่วคราวได้ ● เข้าฝึกซ้อม Cyber Resilience Exercise ที่หน่วยงานต่าง ๆ ได้จัดทำขึ้น เช่น กิจกรรม Capital Market Cyber Exercise (CMX) เป็นต้น ● เข้าร่วมกลุ่มความร่วมมือหรือเครือข่ายต่าง ๆ เช่น กลุ่มความร่วมมือด้านไซเบอร์ หรือกลุ่มภายใต้การสนับสนุนของหน่วยงานกำกับดูแล เป็นต้น
5.	**การตรวจสอบด้านเทคโนโลยีสารสนเทศ (information technology audit)**	
5.1	ธนาคารพาณิชย์, บริษัทประกันชีวิต, สถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ซึ่งเป็นผู้ประกอบธุรกิจประเภท LBDU ต้องนำส่งรายงานผลการตรวจสอบด้าน IT ใช่หรือไม่	ผู้ประกอบธุรกิจทุกรายซึ่งอยู่ภายใต้การบังคับใช้ตามประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 มีหน้าที่ในการนำส่งรายงานผลการตรวจสอบด้าน IT (IT Audit report) <u>เว้นแต่</u>กรณีธนาคารพาณิชย์ ประกันชีวิต หรือสถาบันการเงิน ซึ่งได้รับเพียงใบอนุญาตประกอบธุรกิจตราสารหนี้ และ/หรือ กิจการการยืมและให้ยืมหลักทรัพย์ (SBL) เท่านั้น ที่ไม่ต้องส่งนำส่งรายงานดังกล่าว
5.2	การเลือกระบบงานที่อยู่ในขอบเขตของการตรวจสอบควรพิจารณาอย่างไร	ระบบ IT ที่ควรอยู่ในขอบเขตของการทำ IT audit ควรครอบคลุมดังนี้ (1) ระบบ IT ที่มีความเสี่ยงสูง (พิจารณาจาก inherent risk) (2) ระบบ IT ที่มีนัยสำคัญ : ซึ่งมีนิยามไว้ว่า ระบบคอมพิวเตอร์หรือระบบเครือข่ายที่หากมีการหยุดชะงักจะส่งผลกระทบอย่างมีนัยสำคัญ (enterprise-wide impact) ต่อการดำเนินงานหรือความต่อเนื่องในการดำเนินงาน ชื่อเสียง หรือฐานะของผู้ประกอบธุรกิจ หรือการใช้บริการของลูกค้า เช่น ระบบซื้อขาย ระบบสนับสนุนการปฏิบัติการ (back office system) ระบบจัดเก็บและบริหารจัดการข้อมูลลูกค้า ระบบ

ลำดับ	คำถาม	คำตอบ
		จัดการลงทุน หรือระบบจัดเก็บทรัพย์สิน เป็นต้น ทั้งนี้ ในการประเมินความเสี่ยงอาจพบระบบที่มี impact สูงมาก แต่ likelihood ต่ำ ซึ่งในกรณีนี้ ระบบดังกล่าวควรอยู่ในขอบเขตของการตรวจสอบ เนื่องจากหากข้อบกพร่องของระบบดังกล่าวไม่ได้รับการตรวจพบและแก้ไขอย่างทันท่วงที จะทำให้เกิดผลกระทบอย่างมีนัยสำคัญต่อผู้ประกอบธุรกิจและลูกค้า กรณีที่ผู้ประกอบธุรกิจมีธุรกิจหลายประเภท ควรจัดให้มีแผนการตรวจสอบที่ผ่านการอนุมัติจากผู้มีอำนาจ โดยกำหนดขอบเขตการตรวจสอบที่เหมาะสมเพื่อให้ระบบ IT ที่มีความเสี่ยงสูงและระบบ IT ที่มีนัยสำคัญได้รับการตรวจสอบในรอบความถี่ที่เพียงพอ และเพื่อให้มั่นใจว่าคณะกรรมการบริษัทจะมีข้อมูลที่เพียงพอต่อการกำกับดูแลการบริหารจัดการความเสี่ยงด้าน IT ที่ดีและเพื่อให้การดำเนินธุรกิจตามแผนกลยุทธ์ทางธุรกิจได้อย่างต่อเนื่อง ทั้งนี้ สำนักงานได้จัดทำรายชื่อระบบ IT ที่มีนัยสำคัญเพื่อให้ผู้ประกอบธุรกิจพิจารณาขอบเขตของการตรวจสอบได้อย่างเป็นมาตรฐานเดียวกัน อย่างไรก็ดี ผู้ประกอบธุรกิจแต่ละรายอาจมีระบบ IT ที่มีนัยสำคัญซึ่งแตกต่างหรือมากกว่ารายชื่อที่สำนักงานกำหนดไว้ ในกรณีนี้ ผู้ประกอบธุรกิจควรกำหนดขอบเขตการตรวจสอบให้ครอบคลุมระบบงานเหล่านั้นด้วย
5.3	การตรวจสอบด้าน IT ในปี 2567 เป็นต้นไป ผู้ตรวจสอบต้องได้รับวุฒิบัตรก่อนวันที่เริ่มการตรวจสอบหรือไม่	วัตถุประสงค์ของข้อกำหนดด้านวุฒิบัตรของผู้ตรวจสอบ คือการช่วยให้มั่นใจได้ว่าการตรวจสอบและรายงานผลการตรวจสอบนั้นได้เป็นไปอย่างมีมาตรฐาน และมีความน่าเชื่อถือ ดังนั้น ผู้ตรวจสอบต้องได้รับวุฒิบัตรก่อนวันแรกที่เริ่มดำเนินการตรวจสอบ
5.4	ผู้ตรวจสอบในทีมตรวจสอบ จำเป็นต้องมีวุฒิบัตร (certificate) ครบทุกคนหรือไม่	ข้อกำหนดในเกณฑ์มิได้กำหนดให้ทีมผู้ตรวจสอบต้องได้รับ certificate อย่างครบถ้วนทุกคน และมิได้กำหนดให้ผู้ที่ได้รับ certificate ต้องได้รับ certificate ครบถ้วนทุกใบตามรายชื่อที่กำหนด ผู้ประกอบธุรกิจสามารถจัดให้มีผู้ตรวจสอบหรือผู้ควบคุมการตรวจรายใดรายหนึ่งในทีมตรวจสอบที่ได้รับ certificate ตามรายชื่อที่กำหนดอย่างน้อย 1 ใบ
5.5	ผู้ตรวจสอบที่วุฒิบัตร (certificate) หมดอายุ ยังคงถือว่ามีคุณสมบัติตามที่หลักเกณฑ์กำหนดหรือไม่	การคงสถานะของ certificate เป็นการช่วยให้มั่นใจได้ว่าผู้ตรวจสอบรายดังกล่าวยังคงมีกระบวนการพัฒนาองค์ความรู้ให้เท่าทันอยู่สม่ำเสมอ และเป็นส่วนสำคัญที่ยืนยันได้ว่าการตรวจสอบและรายงานผล

ลำดับ	คำถาม	คำตอบ
		การตรวจสอบนั้นได้เป็นไปอย่างมีมาตรฐาน และมีความน่าเชื่อถือ การใช้งานผู้ตรวจสอบที่ certificate หมดอายุ อาจส่งผลให้มีข้อสังเกตด้านการพัฒนาองค์ความรู้อย่างต่อเนื่อง ทั้งในด้านเทคโนโลยีหรือมาตรฐานการตรวจสอบซึ่งอาจมีการเปลี่ยนแปลงไปได้
5.6	ผู้ตรวจสอบตามประกาศจำเป็นต้องเป็นผู้ตรวจสอบภายในหรือไม่	ผู้ตรวจสอบด้าน IT สามารถเป็นได้ทั้งผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีคุณสมบัติครบถ้วนตามที่หลักเกณฑ์กำหนด ได้แก่ (1) ผ่านการรับรองและมีวุฒิบัตรที่กำหนด และ (2) มีความเป็นอิสระจากผู้ที่ทำหน้าที่ 1st line และ 2nd line
5.7	ผู้ตรวจสอบสามารถรับผิดชอบงานด้านการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ (compliance function) หรืออยู่ในหน่วยงานเดียวกันกับ compliance ได้หรือไม่	ผู้ตรวจสอบด้าน IT ต้องมีความเป็นอิสระจากผู้ทำหน้าที่ในระดับ 1st line และ 2nd line ดังนั้น ผู้ตรวจสอบจึงไม่สามารถปฏิบัติงานด้าน compliance ซึ่งเป็นงานของ 2nd line ได้ ในกรณีที่มีข้อจำกัดทำให้ไม่สามารถแบ่งแยกหน่วยงานที่ปฏิบัติหน้าที่ 2nd line และ 3rd line ตามโครงสร้างขององค์กรได้ ผู้ประกอบธุรกิจควรกำหนดวิธีปฏิบัติที่ทำให้ผู้ตรวจสอบสามารถปฏิบัติหน้าที่ได้อย่างเป็นอิสระและมีประสิทธิภาพ เช่น ผู้ตรวจสอบต้องสามารถรายงานผลการตรวจสอบและให้ความเห็นที่เกี่ยวข้องต่อคณะกรรมการตรวจสอบ หรือคณะกรรมการของผู้ประกอบธุรกิจได้โดยตรง เป็นต้น
5.8	หากธุรกิจหลักของผู้ประกอบธุรกิจอยู่ภายใต้การกำกับดูแลของหน่วยงานอื่น โดยมีธุรกิจเพียงส่วนน้อยที่อยู่ภายใต้การกำกับดูแลของสำนักงาน ก.ล.ต. เช่นนี้ สามารถกำหนดขอบเขตการตรวจสอบเฉพาะระบบที่เกี่ยวข้องกับธุรกิจที่อยู่ภายใต้การกำกับดูแลของสำนักงาน ก.ล.ต. ใช่หรือไม่	การจัดส่งผลประเมินตามแบบ RLA และการนำส่งแบบรายงาน IT Audit report มีขอบเขตครอบคลุมเฉพาะระบบงานด้าน IT ที่ใช้ประกอบธุรกิจที่อยู่ภายใต้ประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 เท่านั้น
5.9	กรณีผู้ประกอบธุรกิจได้รับใบอนุญาตประกอบธุรกิจหลายประเภท เช่น ได้รับใบอนุญาตแบบ ข และใบอนุญาตแบบ ง เป็นต้น ผู้ประกอบธุรกิจต้องรายงานผลการตรวจสอบของทุกระบบงานที่เกี่ยวข้องกับใบอนุญาตทั้ง 2 ประเภทใช่หรือไม่ และจัดทำรายงานผลการตรวจสอบแยกตามประเภทใบอนุญาตหรือไม่	ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบทุกระบบ IT ที่มีนัยสำคัญซึ่งใช้เพื่อประกอบธุรกิจที่ได้รับใบอนุญาตจากสำนักงาน ก.ล.ต. และเป็นธุรกิจภายใต้การบังคับใช้ตามประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 ทั้งนี้ ให้ผู้ประกอบธุรกิจนำส่งรายงานผลการตรวจสอบ โดยรวมผลการตรวจสอบของทุกใบอนุญาตเป็น full report ฉบับเดียว (1 รายงาน ต่อ 1 บริษัท)

<table>
<tr><th>ลำดับ</th><th>คำถาม</th><th>คำตอบ</th></tr>
<tr><td>5.10</td><td>[New] ขอบเขตการตรวจสอบด้าน IT มีความสัมพันธ์กับ RLA อย่างไร
* ตามข้อกำหนดที่ปรับปรุงใหม่ ประกาศที่ สธ. 38/2565 ที่แก้ไขเพิ่มเติมโดยประกาศที่ สธ. 33/2567 (หรือ ประกาศที่ สธ. 38/2565 ฉบับประมวล) และ นป. 6/2567 ซึ่งมีผลใช้บังคับเมื่อวันที่ 1 มกราคม 2568</td><td>ผลการประเมินระดับความเสี่ยงจากแบบ RLA จะเป็นการกำหนดขอบเขตหลักเกณฑ์ที่ผู้ประกอบธุรกิจต้องปฏิบัติ และจัดให้มีการตรวจสอบด้าน IT โดยผลการประเมิน RLA จะกำหนดขอบเขตการตรวจสอบ ดังนี้
<table><tr><th>รอบนำส่ง RLA</th><th>ช่วงข้อมูลในการจัดทำ RLA</th><th>รอบการตรวจสอบ</th></tr><tr><td>ปี 2567</td><td>1 ต.ค. 2566 – 30 ก.ย. 2567</td><td>2568</td></tr><tr><td>ปี 2569</td><td>1 ม.ค. 2568 – 31 ธ.ค. 2568</td><td>2569</td></tr><tr><td>ปี 2570</td><td>1 ม.ค. 2569 – 31 ธ.ค. 2570</td><td>2570</td></tr></table>โดยมีข้อกำหนดซึ่งต้องครอบคลุมในขอบเขตการตรวจสอบ ดังนี้
<table><tr><th>ระดับความเสี่ยง</th><th>ขอบเขตการตรวจสอบ</th></tr><tr><td>ขนาดเล็ก*</td><td>เฉพาะแนวปฏิบัติ (control) ขั้นต้น (Cyber Hygiene)</td></tr><tr><td>ระดับต่ำ*</td><td>แนวปฏิบัติทั้งหมด ยกเว้นข้อที่ระบุ [ความเสี่ยงสูง]*</td></tr><tr><td>ระดับปานกลาง</td><td>แนวปฏิบัติทั้งหมด ยกเว้นข้อที่ระบุ [ความเสี่ยงสูง]</td></tr><tr><td>ระดับสูง</td><td>แนวปฏิบัติทั้งหมด</td></tr></table>หมายเหตุ: * จัดให้มีการตรวจสอบแบบ full scope อย่างน้อยทุก 3 ปี ตามรอบปีที่สำนักงานกำหนด‡ รวมทั้งมีการตรวจสอบเพิ่มเติมในปีที่ผู้ประกอบธุรกิจเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ แม้ว่าปีนั้นจะเป็นปีที่สำนักงานไม่ได้กำหนดให้มีการตรวจสอบด้าน IT (รอบปีที่สำนักงานกำหนด และรายละเอียดเพิ่มเติม สามารถตรวจสอบได้ที่เอกสารหนังสือเวียนที่ กลต.ตท.(ว) 5225/2567 และเอกสารแนบหนังสือเวียน หรือ ภาคผนวก 6 ของเอกสาร FAQ)

ตัวอย่าง
● ผู้ประกอบธุรกิจ ก. ประเมิน RLA ปี 2567 ได้ผลการประเมินเป็นความเสี่ยงระดับต่ำ ในการตรวจสอบด้าน IT รอบปี 2568 ผู้ประกอบธุรกิจไม่ต้องดำเนินการตรวจสอบด้าน IT และไม่ต้องนำส่งแบบรายงานผลการตรวจสอบด้าน IT ของรอบปีดังกล่าว ทั้งนี้ หากในปี 2568 ผู้ประกอบธุรกิจเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ เช่น ระบบของผู้ประกอบธุรกิจถูก ransomware</td></tr>
</table>

‡ **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล** เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล (Digital Asset Advisory Service) ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Digital Asset Exchange) เป็นต้น มีหน้าที่ในการปฏิบัติตามข้อกำหนดของประกาศ **กธ. 19/2561** เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจึงยังคงต้องจัดให้มีการตรวจสอบทุกปี และต้องนำส่งรายงานต่อสำนักงานตามเงื่อนไขของประกาศ กธ. 19/2561** คือ

(1) จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ก่อนเริ่มให้บริการและภายหลังเริ่มให้บริการแล้ว**อย่างน้อยปีละ 1 ครั้ง** *และ*

(2) รายงานผลต่อสำนักงานภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการทดสอบ

แม้ว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล เป็นต้น ได้ผลการประเมินแบบ RLA เป็นผู้ประกอบธุรกิจขนาดเล็ก ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง เพื่อให้เป็นไปตามข้อกำหนดของประกาศ กธ. 19/2561

ลำดับ	คำถาม	คำตอบ
		เป็นต้น ในปี 2568 นั้น ผู้ประกอบธุรกิจ จำเป็นต้องตรวจสอบให้ครอบคลุมแนวปฏิบัติทั้งหมด (ยกเว้นข้อที่ระบุ *[ความเสี่ยงสูง]*) ● ในปีถัดมา ผู้ประกอบธุรกิจ ก. ประเมิน RLA ปี 2569 ได้ผลการประเมินเป็นความเสี่ยงระดับต่ำเช่นเดิม อย่างไรก็ดี เนื่องด้วยปี 2569 เป็นปีที่สำนักงานกำหนดให้มีการตรวจสอบด้าน IT สำหรับผู้ประกอบธุรกิจ ดังนั้น ผู้ประกอบธุรกิจ ก. ต้องจัดให้มีการตรวจสอบภายในปี 2569 ซึ่งครอบคลุมแนวปฏิบัติทั้งหมด (ยกเว้นข้อที่ระบุ *[ความเสี่ยงสูง]*) และมีหน้าที่ต้องนำส่งแบบรายงานผลการตรวจสอบดังกล่าวให้ทันกำหนดการณ์ภายในวันที่ 31 มีนาคม 2570
5.11	[New] กรณีที่ผู้ประกอบธุรกิจเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญขึ้นในปีที่ไม่ได้ถูกกำหนดให้มีการตรวจสอบด้าน IT เช่น ปี 2568 2570 2571 เป็นต้น ซึ่งทำให้ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบด้าน IT เพิ่มเติม (special audit) ภายในปีนั้น ข้อกำหนดที่ระบุว่า “special audit ต้องทำใน 4 เดือน” 4 เดือนนั้นหมายความว่าต้องตรวจสอบเสร็จและได้รายงานสรุปจากทางผู้ตรวจสอบแล้ว หรือว่าอยู่ระหว่างดำเนินการตรวจสอบได้	สำหรับรอบปีที่ไม่ได้กำหนดให้ผู้ประกอบธุรกิจขนาดเล็กหรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำต้องจัดให้มีการตรวจสอบด้าน IT หากปีใดเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญที่ทำให้ต้องดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ แต่ผู้ประกอบธุรกิจไม่สามารถดำเนินการตรวจสอบได้ภายในปีที่เกิดเหตุการณ์เนื่องด้วยเหตุสุดวิสัยที่รับฟังได้ เช่น เหตุการณ์เกิดในช่วงเดือนธันวาคมใกล้สิ้นปี เป็นต้น ผู้ประกอบธุรกิจต้องดำเนินการดังต่อไปนี้ ภายใน 4 เดือน นับแต่วันที่ทราบเหตุการณ์ดังกล่าว (1) รายงานเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ได้ภายในปีที่เกิดเหตุการณ์ดังกล่าว และแผนการตรวจสอบด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ เฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ รวมทั้งรายงานเหตุจำเป็นดังกล่าวต่อสำนักงาน *และ* (2) ดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ข้อ (1) ต้องดำเนินการให้แล้วเสร็จภายในปีที่เกิดเหตุการณ์ ข้อ (2) ผู้ประกอบธุรกิจต้องจัดให้มีการดำเนินการตรวจสอบ (เริ่ม audit engagement) โดยระยะเวลา 4 เดือน สำนักงานได้พิจารณาว่าเป็นระยะเวลาที่เพียงพอต่อการจัดหาผู้ตรวจสอบด้าน IT หากใช้ระยะเวลาที่เกินกว่านั้น อาจทำให้ความเสี่ยงที่เป็นสาเหตุให้เกิดเหตุการณ์ร้ายแรงไม่ได้รับการแก้ไขอย่างทันการณ์ ทั้งนี้ รายงานผล IT Audit ให้บริษัทนำส่งไม่เกินวันที่ 31 มีนาคม ตามรอบ

ลำดับ	คำถาม	คำตอบ
		การนำส่งแบบรายงานผลการตรวจสอบด้าน IT ตัวอย่างเช่น บริษัทเกิด major IT security incident วันที่ 20 ธันวาคม 2568 ผู้ประกอบธุรกิจต้องดำเนินการทั้ง (1) และ (2) ให้เสร็จสิ้นภายในวันที่ 30 เมษายน 2569 และต้องนำส่งแบบรายงานผลการตรวจสอบดังกล่าวในระบบ E-Submission ได้ตลอดเวลา ทั้งนี้ ไม่เกินวันที่ 31 มีนาคม 2570
5.12	[New] หากบริษัทเริ่มประกอบธุรกิจในปี 2568 บริษัทต้องจัดให้มีการตรวจสอบด้าน IT สำหรับรอบปี 2568 ด้วยหรือไม่[‡]	เนื่องด้วยปี 2568 บริษัทได้เริ่มประกอบธุรกิจและมีสถานะต้องปฏิบัติตามข้อกำหนดของสำนักงานแล้ว บริษัทต้องจัดให้มีการตรวจสอบด้าน IT สำหรับรอบปี 2568 และนำส่งรายงานผล IT Audit รอบปี 2568 ภายในวันที่ 31 มีนาคม 2569 ทั้งนี้ ให้บริษัทดำเนินการประเมินแบบ RLA ย้อนหลัง (ประเมินโดยใช้แบบ RLA รอบปี 2567 ซึ่งดาวน์โหลดได้จากเว็บไซต์ของสำนักงาน) หากบริษัทได้ผลการประเมินเป็น <u>กรณีที่ 1</u> ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ หรือผู้ประกอบธุรกิจขนาดเล็ก เนื่องด้วยสำนักงานมิได้กำหนดให้ปี 2568 ต้องมีการตรวจสอบด้าน IT ในกรณีนี้ บริษัทสามารถใช้ดุลยพินิจได้ตามความเหมาะสม ทั้งนี้ • หากเป็นผู้ประกอบธุรกิจภายใต้ประกาศที่ กธ. 19/2561 บริษัทต้องจัดให้มีการตรวจสอบด้วย ตามข้อกำหนดที่ 19 ของประกาศที่ กธ. 19/2561 *หรือ* • หากในปี 2568 บริษัทเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ต้องมีหน้าที่ในการตรวจสอบด้าน IT ในปี 2568 ด้วย <u>กรณีที่ 2</u> ผู้ประกอบธุรกิจที่มีความเสี่ยงปานกลาง หรือผู้ประกอบธุรกิจที่มีความเสี่ยงสูง บริษัทต้องจัดให้มีการตรวจสอบด้าน IT ในปี 2568 และต้องนำส่งแบบรายงานผลการตรวจสอบดังกล่าวภายในวันที่ 31 มีนาคม 2569

[‡] **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล** เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล (Digital Asset Advisory Service) ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Digital Asset Exchange) เป็นต้น มีหน้าที่ในการปฏิบัติตามข้อกำหนดของประกาศ **กธ. 19/2561** เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจึงยังคงต้องจัดให้มีการตรวจสอบทุกปี และต้องนำส่งรายงานต่อสำนักงานตามเงื่อนไขของประกาศ กธ. 19/2561** คือ

(1) จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ **ก่อนเริ่มให้บริการ**และภายหลังเริ่มให้บริการแล้ว**อย่างน้อยปีละ 1 ครั้ง** *และ*

(2) รายงานผลต่อสำนักงานภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการทดสอบ

แม้ว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล เป็นต้น ได้ผลการประเมินแบบ RLA เป็นผู้ประกอบธุรกิจขนาดเล็ก ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง เพื่อให้เป็นไปตามข้อกำหนดของประกาศ กธ. 19/2561

ลำดับ	คำถาม	คำตอบ
5.13	ระดับ Maturity level ในแบบรายงานผล IT Audit report มีความสัมพันธ์กับผลการประเมินในแบบ RLA หรือไม่	ระดับ Maturity level ในแบบรายงานผล IT Audit report ไม่ได้มีความสัมพันธ์กับผลประเมินในแบบ RLA โดยตรง เนื่องจากแบบ RLA เป็นการประเมินระดับความเสี่ยงเกี่ยวกับระบบ IT ของผู้ประกอบธุรกิจเพื่อใช้กำหนดหลักเกณฑ์ที่ผู้ประกอบธุรกิจต้องปฏิบัติ รวมทั้งกำหนดขอบเขตของการตรวจสอบด้าน IT (IT audit) ในขณะที่ Maturity level เป็นผลการประเมินของแต่ละมาตรการควบคุมตามหลักเกณฑ์ โดยสำนักงานมุ่งหวังให้ผู้ประกอบธุรกิจทุกรายมีระดับ Maturity level อยู่ในระดับ M3 หรือเทียบเท่ากับผลการประเมินเป็น Yes อย่างไรก็ดี หากผู้ประกอบธุรกิจมีระดับความเสี่ยงสูง ผู้ประกอบธุรกิจสามารถตั้งเป้าหมายที่ระดับ Maturity level 4 หรือ 5 เพื่อให้การกำกับดูแลความเสี่ยงด้าน IT ขององค์กรมีประสิทธิภาพมากยิ่งขึ้น
5.14	การตรวจสอบแบบเต็มรูปแบบ (full scope) ให้ตรวจสอบเฉพาะระบบ IT ที่มีนัยสำคัญ (critical system) เท่านั้น หรือรวมถึงระบบอื่น ๆ ด้วย	การตรวจสอบแบบเต็มรูปแบบ หมายถึง การตรวจสอบตามหลักเกณฑ์และแนวปฏิบัติทุกหัวข้อ โดยมีขอบเขตอย่างน้อยครอบคลุมระบบ IT ที่มีนัยสำคัญ สำหรับระบบอื่น ๆ ผู้ประกอบธุรกิจสามารถพิจารณาจัดให้มีการตรวจสอบเพิ่มเติมได้ (optional)
5.15	กรณีที่ผู้ประกอบธุรกิจมีระบบ IT ที่มีนัยสำคัญ 15 ระบบ ผู้ประกอบธุรกิจจำเป็นต้องตรวจสอบทั้งหมด 15 ระบบนั้นภายใน 1 ปี หรือไม่	สำนักงานได้จัดทำรายชื่อระบบ IT ที่มีนัยสำคัญเพื่อให้ผู้ประกอบธุรกิจพิจารณาใช้กำหนดเป็นขอบเขตของการตรวจสอบประจำปี (อ้างอิงเอกสาร “คำอธิบายประกอบการจัดทำแบบรายงานผล IT Audit” บน website ของสำนักงาน https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-REGULATIONS.aspx) โดยผู้ประกอบธุรกิจสามารถวางแผนการตรวจสอบเพื่อให้ทุกระบบ IT ที่มีนัยสำคัญได้รับการตรวจสอบในรอบความถี่ที่เหมาะสม (รายละเอียดเพิ่มเติมตามภาคผนวก 7)
5.16	กรณีมีระบบรับส่งคำสั่งซื้อขาย (OMS) หลายระบบ (เช่น OMS ส่งคำสั่งในประเทศ / OMS ส่งคำสั่งไปต่างประเทศ) โดยบางระบบมีปริมาณการใช้งานน้อยเมื่อเทียบกับระบบอื่น ๆ ในการตรวจสอบต้องครอบคลุม OMS ที่มีปริมาณการใช้งานน้อยด้วยหรือไม่	ขอบเขตในการตรวจสอบตามข้อกำหนดของสำนักงานนั้นต้องครอบคลุมระบบ IT ที่มีนัยสำคัญ ซึ่งใช้เพื่อการประกอบธุรกิจที่ได้รับใบอนุญาตจากสำนักงาน ก.ล.ต. และอยู่ภายใต้การบังคับใช้ตามประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 กรณีที่ผู้ประกอบธุรกิจมีระบบ OMS หลายระบบ ผู้ประกอบธุรกิจไม่จำเป็นต้องตรวจครบทุกระบบในปีเดียวกัน แต่สามารถพิจารณากำหนดแผนการตรวจสอบให้ครอบคลุมทุกระบบ และนำเสนอแผนดังกล่าวต่อคณะกรรมการตรวจสอบเพื่อพิจารณาอนุมัติการนำไปใช้งานได้
5.17	กรณีที่มีการเปลี่ยนแปลงระบบ (system) และ/หรือกระบวนการทำงาน (process) ซึ่งกระทบต่อการ	วัตถุประสงค์ของการตรวจสอบด้าน IT คือการประเมินประสิทธิผล ประสิทธิภาพ และความปลอดภัยด้าน IT ขององค์กร หากระบบ/กระบวนการเดิมไม่ได้ใช้งานอีกต่อไปหรือถูกแทนที่ด้วยระบบ/

ลำดับ	คำถาม	คำตอบ
	ควบคุม (controls) ในระหว่างปีจะสามารถตรวจสอบตามกระบวนการปฏิบัติงานแบบใหม่ โดยไม่ต้องทำการตรวจสอบในกระบวนการปฏิบัติงานเดิมได้หรือไม่	กระบวนการใหม่ทั้งหมด อาจไม่จำเป็นต้องรวมระบบ/กระบวนการเดิมไว้ในขอบเขตการตรวจสอบ อย่างไรก็ดี หากการเปลี่ยนแปลงที่เกิดขึ้นนั้น ยังทำให้ระบบ/กระบวนการเก่ายังมีการใช้งานอยู่ ผู้ประกอบธุรกิจควรรวมระบบ/กระบวนการเก่า ไว้ในขอบเขตการตรวจสอบด้วย
5.18	ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบด้าน IT ในส่วนของงานที่รับผิดชอบโดยบุคคลภายนอกด้วยหรือไม่	ผู้ประกอบธุรกิจสามารถกำหนดวิธีการกำกับดูแล และตรวจสอบตามขอบเขตงานที่รับผิดชอบโดยบุคคลภายนอกได้ตามความเหมาะสม โดยพิจารณาจากความเสี่ยงและขอบเขตของงานที่มีการมอบหมาย เช่น การให้ผู้ตรวจสอบของผู้ประกอบธุรกิจเข้าดำเนินการตรวจสอบการดำเนินการด้าน IT ของผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญ หรือการใช้รายงานผลการตรวจสอบของผู้ให้บริการที่ดำเนินการโดยผู้ที่มีความเป็นอิสระ (third-party assurance report) มีความน่าเชื่อถือ และมีขอบเขตและวิธีการตรวจสอบสอดคล้องกับหลักเกณฑ์การจัดให้มีระบบ IT เป็นต้น
5.19	ในกรณีการตรวจสอบแยกเป็นหัวข้อย่อย ๆ แล้วแบ่งการตรวจตามช่วงเวลาหรือแบ่งเป็นหลายทีมตรวจสอบ ซึ่งจะทำให้การตรวจแต่ละหัวข้อแล้วเสร็จไม่พร้อมกัน ผู้ประกอบธุรกิจสามารถรวบรวมผลการตรวจสอบทั้งหมดในรอบปี (ครบทุกหัวข้อการตรวจสอบ) เพื่อรายงานสำนักงานครั้งเดียวได้หรือไม่	ผู้ประกอบธุรกิจสามารถรวบรวมผลการตรวจสอบทุกระบบงานและทุกหัวข้อการตรวจสอบ แล้วรายงานครั้งเดียวหลังการตรวจครั้งสุดท้ายของปีเสร็จสิ้น โดยการนับวันรายงานผลการตรวจสอบต่อสำนักงาน ก.ล.ต. ให้อ้างอิงจากวันได้รับ final report ฉบับสุดท้าย เช่น domain สุดท้าย ของระบบสุดท้าย เป็นต้น ทั้งนี้ ผู้ประกอบธุรกิจต้องนำส่งภายในเงื่อนไขเวลาที่หลักเกณฑ์กำหนด
5.20	กรณีผู้ประกอบธุรกิจเป็นสาขาของบริษัทต่างชาติ (centralized systems) ซึ่งมีโครงสร้างในการตรวจสอบที่ดำเนินการโดยสำนักงานใหญ่ต่างประเทศ อาจมีข้อจำกัดในการดำเนินการตรวจสอบตามข้อกำหนดของสำนักงาน ก.ล.ต. ผู้ประกอบธุรกิจสามารถใช้รายงานการตรวจสอบ (shared audit report) ของกลุ่มบริษัทได้หรือไม่	ในกรณีที่ผู้ประกอบธุรกิจมีขั้นตอนการตรวจสอบ (IT audit program) หรือรูปแบบรายงานผลการตรวจสอบของตนเอง ของกลุ่มธุรกิจในเครือหรือของหน่วยงานกำกับดูแลอื่น ๆ อยู่แล้ว ผู้ประกอบธุรกิจสามารถใช้แนวทางดังกล่าวในการตรวจสอบได้ โดยต้องนำข้อมูลสรุปผลการตรวจสอบนั้นกรอกข้อมูลลงในแบบรายงานที่สำนักงาน ก.ล.ต. กำหนด และภายในเงื่อนไขเวลาที่หลักเกณฑ์กำหนด ทั้งนี้ หากการตรวจสอบตามแนวทางของกลุ่มธุรกิจในเครือ หรือหน่วยงานกำกับดูแลอื่น ๆ มีข้อมูลไม่เพียงพอที่จะกรอกลงในรายงานที่สำนักงาน ก.ล.ต. กำหนดอย่างครบถ้วน ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบเพื่อให้ได้ข้อมูลเพิ่มเติมอย่างเพียงพอ
5.21	เนื่องจากหัวข้อในการตรวจสอบ	

ลำดับ	คำถาม	คำตอบ
	มีความคล้ายคลึงกับข้อกำหนด IT Risk ของ ธปท. ผู้ประกอบธุรกิจสามารถอ้างอิงผลการตรวจสอบในเรื่องเดียวกันจากการตรวจตาม IT ธปท. ได้หรือไม่ โดยจัดทำรายงานตามรูปแบบที่สำนักงาน ก.ล.ต. กำหนด	
5.22	กรณีที่ผู้ประกอบธุรกิจมี audit program ในรูปแบบของตนเองอยู่แล้ว สามารถใช้ audit program นั้นเพื่อนำส่งสำนักงานได้หรือไม่	
5.23	การสุ่มตัวอย่างในการตรวจสอบมีกำหนดกรอบระยะเวลาและจำนวนของกลุ่มตัวอย่างที่ใช้อย่างไร	การสุ่มตัวอย่างในการตรวจสอบ (audit sampling) มีวัตถุประสงค์เพื่อให้ผู้ตรวจสอบมีข้อมูลเพียงพอในการสรุปผลการประเมินอย่างสมเหตุสมผล (reasonable assurance) ในขณะที่ลดเวลาและค่าใช้จ่ายของการตรวจสอบจากประชากร (population) ทั้งหมด ดังนั้น ในการเลือกกลุ่มตัวอย่าง ผู้ตรวจสอบควรพิจารณากรอบระยะเวลา (sample period) และขนาดของกลุ่มตัวอย่าง (sample size) ที่เพียงพอสำหรับการสรุปผลการประเมินกิจกรรมด้าน IT ที่เกิดขึ้นในรอบ 1 ปีที่ผ่านมา โดยให้ความเชื่อมั่นอย่างสมเหตุสมผล แม้ว่าสำนักงานมิได้กำหนดช่วงวันที่ในการเลือกกลุ่มตัวอย่าง อย่างไรก็ดี ผู้ประกอบธุรกิจควรกำหนดช่วงวันที่ (audit period) ที่เหมาะสมกับแผนการตรวจสอบขององค์กร เช่น ในรอบปี 2566 ผู้ประกอบธุรกิจจะจัดให้มีการตรวจสอบด้าน IT ในเดือนกรกฎาคม โดยเป็นการตรวจสอบกิจกรรมที่เกิดขึ้น ในช่วงวันที่ 1 กรกฎาคม 2565 ถึง 30 มิถุนายน 2566 ในกรณีนี้ การตรวจสอบในรอบปีถัดไปควรกำหนดช่วงวันที่ที่มีรูปแบบเดียวกันเพื่อให้การตรวจสอบประชากร (population) มีความต่อเนื่องและเป็นไปในทิศทางเดียวกัน ทั้งนี้ การกำหนด audit period ควรคำนึงถึงการปฏิบัติอย่างสม่ำเสมอ (consistency) ด้วย เช่น หากกำหนด audit period เป็นช่วงระหว่างวันที่ 1 กรกฎาคม 2565 ถึง 30 มิถุนายน 2566 ในปีถัดไป การกำหนด audit period ก็ควรต้องเป็นช่วงเวลาเดียวกันไปตลอด เพื่อลดโอกาส หรือ bias ที่กลุ่มตัวอย่างในช่วง audit period อาจจะไม่ถูกเลือก ทั้งนี้ ผู้ประกอบธุรกิจสามารถดูแนวทางการสุ่มตัวอย่าง ได้จาก เอกสาร “คำอธิบายประกอบการจัดทำแบบรายงานผล IT Audit” บน website
5.24	หากเริ่มทำการตรวจสอบในช่วงกลางปี จำนวนประชากร (Population) ต้องกำหนดให้ครบในช่วง 1 ปีหรือไม่ หรือต้องกำหนดอย่างไรจึงจะเพียงพอ	
5.25	การตรวจสอบจากประชากร (population) ผู้ประกอบธุรกิจต้องใช้ข้อมูลย้อนหลังถึงเมื่อใด	

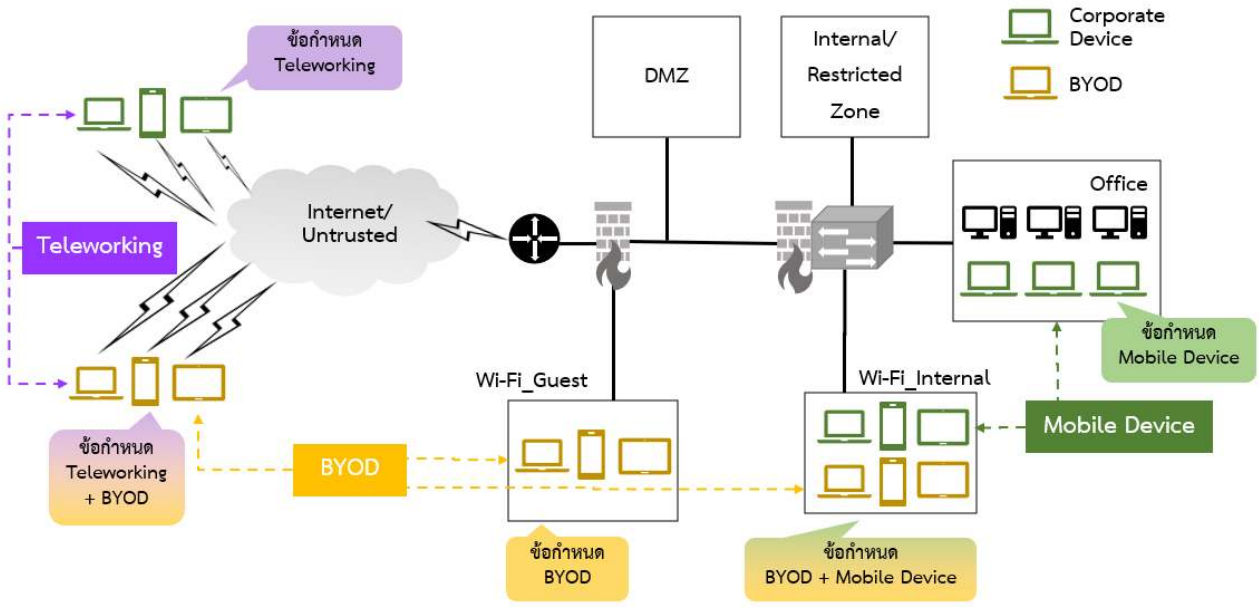
ลำดับ	คำถาม	คำตอบ
		ของสำนักงาน https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-REGULATIONS.aspx
5.26	ในรายงานผลการตรวจประเมินทางด้านเทคโนโลยีสารสนเทศ ซึ่งได้ทำการแยกความสำคัญของประเด็นข้อบกพร่องให้อิงตามเกณฑ์ของสำนักงานหรือของผู้ประกอบธุรกิจ	การประเมินระดับความสำคัญของข้อบกพร่องให้เป็นไปตามรายละเอียดในแบบรายงานผลการตรวจประเมินทางด้านเทคโนโลยีสารสนเทศที่สำนักงาน ก.ล.ต. กำหนด เพื่อให้ผู้ประกอบธุรกิจสามารถจัดระดับความสำคัญของข้อบกพร่องได้อย่างเป็นมาตรฐานเดียวกัน
5.27	กรณีที่ผู้ประกอบธุรกิจมีบริษัทแม่ซึ่งดูแลบริษัทย่อยหลายแห่ง โดยบริษัทย่อยแต่ละแห่งประกอบธุรกิจภายใต้กำกับของสำนักงาน ผู้ประกอบธุรกิจต้องนำส่งรายงานผลการตรวจประเมินด้านเทคโนโลยีสารสนเทศแยกบริษัท หรือนำส่งเป็นฉบับเดียว	ผู้ประกอบธุรกิจแต่ละราย (แต่ละนิติบุคคล) มีหน้าที่รายงานผลการตรวจสอบด้าน IT ด้วยตนเอง เพื่อให้สำนักงาน ก.ล.ต. สามารถนำข้อมูลดังกล่าวมาประมวลผลได้อย่างถูกต้อง และนำส่งข้อมูลผลการวิเคราะห์ภาพรวมให้กับผู้ประกอบธุรกิจเพื่อนำไปใช้ประโยชน์ต่อไป
5.28	หากบริษัทมีแผนตรวจสอบประจำปีในช่วงไตรมาส 1 - 2 ของทุกปี สำหรับปี 2568 บริษัทจะสามารถใช้ ผลตรวจในช่วงไตรมาส 1 - 2 และส่งสำนักงาน ก.ล.ต. ช่วงไตรมาส 3 ได้หรือไม่	ในปี 2568 ผู้ประกอบธุรกิจสามารถดำเนินการตรวจสอบในช่วงใดของปีก็ได้ แต่ต้องนำส่งผลการตรวจสอบภายในเดือนมีนาคม 2569
5.29	วันที่สิ้นสุดการตรวจสอบ หมายถึงวันใด	วันที่สิ้นสุดการตรวจสอบให้ใช้วันที่ผู้ตรวจสอบ (auditor) นำส่งรายงานผลการตรวจสอบฉบับสมบูรณ์แก่ผู้ประกอบธุรกิจ (final audit report)
5.30	ผู้ประกอบธุรกิจจำเป็นต้องนำส่งกระดาษทำการ (working paper) เมื่อนำส่งรายงานผลการตรวจสอบด้าน IT ต่อสำนักงานหรือไม่	ผู้ประกอบธุรกิจไม่จำเป็นต้องนำส่งกระดาษทำการเมื่อนำส่งรายงานผลการตรวจสอบด้าน IT ต่อสำนักงาน อย่างไรก็ดี ควรจัดเก็บกระดาษทำการและหลักฐานประกอบการตรวจไม่น้อยกว่า 2 ปี นับแต่วันที่ดำเนินการตรวจสอบ ในรูปแบบที่สามารถพร้อมให้สำนักงานเรียกดูและตรวจสอบได้โดยไม่ชักช้า
5.31	ผู้ประกอบธุรกิจจำเป็นต้องจัดเก็บกระดาษทำการด้วยตนเอง หรือสามารถขอกระดาษทำการจากผู้ตรวจสอบเพื่อนำส่งให้กับสำนักงานเมื่อสำนักงานร้องขอ	หลักการของข้อกำหนดคือ ผู้ประกอบธุรกิจสามารถแสดงข้อมูลเกี่ยวกับการตรวจสอบ (เช่น บันทึกกระดาษทำการ เป็นต้น) เมื่อสำนักงานเรียกดูและตรวจสอบได้โดยไม่ชักช้า ดังนั้น ผู้ประกอบธุรกิจสามารถ (1) เก็บกระดาษทำการไว้เอง หรือ (2) ให้ผู้ตรวจสอบเป็นผู้เก็บกระดาษทำการก็ได้ อย่างไรก็ดี การที่ผู้ประกอบธุรกิจเก็บกระดาษทำการไว้กับตนเองจะทำให้มั่นใจได้ว่ามีการรวบรวมและจัดเก็บหลักฐานการตรวจสอบไว้อย่างครบถ้วนเป็นระยะเวลาไม่น้อยกว่า 2 ปี และพร้อมให้สำนักงานเรียกดูได้ตามข้อกำหนดของสำนักงาน

ลำดับ	คำถาม	คำตอบ
5.32	กระดาษทำการจำเป็นต้องมี template ตามที่สำนักงานกำหนดหรือไม่	สำนักงานมิได้กำหนด template ของกระดาษทำการหรือหลักฐานประกอบการตรวจ อย่างไรก็ดี กระดาษทำการและหลักฐานประกอบการตรวจควรมีข้อมูลที่เพียงพอที่แสดงให้เห็นว่าผู้ตรวจสอบได้รวบรวมข้อมูล และสรุปผลการตรวจสอบโดยให้ความเชื่อมั่นอย่างสมเหตุสมผล
5.33	การรายงานผลการตรวจสอบด้าน IT สามารถจัดทำเป็นภาษาอังกฤษได้หรือไม่	สำนักงานได้จัดทำแบบรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและแผนการปรับปรุงแก้ไขข้อบกพร่อง (แบบรายงานผล IT Audit) ในรูปแบบ Excel ที่เป็นมาตรฐานในการรายงานข้อมูลต่อสำนักงาน โดยปัจจุบันมีเพียงเวอร์ชันภาษาไทยเท่านั้น ทั้งนี้ การจัดทำ working paper โดยผู้ตรวจสอบ หรือการกรอกข้อมูลลงในแบบรายงานผล IT Audit เช่น ข้อมูลสรุปประเด็นข้อบกพร่อง/ข้อตรวจพบ ผู้ประกอบธุรกิจสามารถระบุข้อมูลลงในแบบรายงานโดยใช้ภาษาอังกฤษได้
5.34	การใช้บริการผู้ตรวจสอบด้าน IT ภายนอก (external IT auditor) ต้องปฏิบัติตามประกาศที่เกี่ยวข้องกับการมอบหมายให้บุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวข้องกับการประกอบธุรกิจ (outsource) เช่น ทธ. 60/2561 หรือไม่	การมอบหมายการตรวจสอบด้าน IT ให้แก่ external IT auditor ไม่นับว่าเป็นการ outsource เนื่องจากผู้ตรวจสอบด้าน IT (IT auditor) จะทำหน้าที่ตรวจสอบการควบคุมและการปฏิบัติงานด้าน IT ตามขอบเขตและแผนการตรวจที่ผู้ประกอบธุรกิจกำหนด นอกจากนี้ ผู้ประกอบธุรกิจยังคงมีหน้าที่ตัดสินใจในส่วนสำคัญของกระบวนการตรวจสอบ เช่น การพิจารณาดำเนินการเกี่ยวกับข้อตรวจพบ เป็นต้น
5.35	หากผู้ตรวจสอบพบความบกพร่องเกี่ยวกับมาตรการควบคุมที่บริษัทรับรู้ก่อนการตรวจสอบ และอยู่ระหว่างดำเนินการตามแผนงานแก้ไขที่ชัดเจนและได้รับอนุมัติแผนจากผู้บริหารแล้ว กรณีนี้ยังคงพิจารณาเป็นประเด็นข้อตรวจพบหรือไม่	หากการแก้ไขข้อตรวจพบหรือข้อบกพร่องยังไม่แล้วเสร็จก่อนการเข้าตรวจประเมินตามเกณฑ์ของสำนักงานนั้น ในการควบคุมข้อนั้นๆ จะยังคงเป็นประเด็นข้อตรวจพบ เนื่องจากยังมีความเสี่ยงจากการขาดการควบคุมหรือมีการควบคุมเพียงบางส่วน
5.36	การกรอกผลการประเมินเป็น “N/A” กับไม่กรอกข้อมูลมีความแตกต่างกันอย่างไร และใช้งานเมื่อใด	การเว้นว่างโดยไม่กรอก จะมีผลเท่ากับผู้ตรวจสอบไม่ได้ตรวจสอบตามหัวข้อการควบคุมนั้น ๆ แต่หากผู้ตรวจสอบได้ดำเนินการตรวจสอบตามหัวข้อการควบคุมนั้นแล้ว แต่เข้าเงื่อนไข ดังนี้ (1) บริษัทไม่มีความเสี่ยงที่เกี่ยวข้องกับการควบคุม *หรือ* (2) การควบคุมไม่สามารถใช้ได้กับระบบ IT ของบริษัท เนื่องจากมีข้อจำกัดบางประการ และมีการขอยกเว้น (exception) จากผู้มีอำนาจอนุมัติ เช่น ผู้บริหารระดับสูง หรือคณะกรรมการบริษัท เป็นต้น ให้ผู้ตรวจสอบสามารถระบุผลการประเมินเป็น “N/A” ได้

ลำดับ	คำถาม	คำตอบ
		สามารถตรวจสอบรายละเอียดเพิ่มเติมเรื่องการประเมินผลการตรวจสอบด้าน IT ข้อแตกต่างระหว่าง N/A และเว้นว่าง ได้ที่เอกสารคำอธิบายประกอบการจัดทำแบบรายงานผล IT Audit
5.37	[New] ส่วนงานใดในองค์กรที่เป็นผู้มีหน้าที่นำส่งแบบรายงานผลการตรวจสอบด้าน IT หรือแบบ RLA ต่อสำนักงาน ก.ล.ต. เช่น หน่วยงานตรวจสอบภายใน (internal audit) หน่วยงาน compliance หรือหน่วยงานด้าน IT เป็นต้น	สำนักงานมิได้กำหนดส่วนงานใดเป็นการเฉพาะ ผู้ประกอบธุรกิจสามารถกำหนดให้ส่วนงานใดเป็นผู้นำส่งรายงานเข้าสู่ระบบ E-submission ตามแบบ EF-3 ได้ตามความเหมาะสม ทั้งนี้ ต้องเป็นไปตามที่สำนักงานได้กำหนดในหนังสือเวียน ที่ กลต.ตท.(ว) 8/2566 เรื่อง ซักซ้อมความเข้าใจเกี่ยวกับการจัดส่งข้อมูลตามข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ● ผู้นำส่งรายงานต้องเป็นบุคลากรของผู้ประกอบธุรกิจเท่านั้น เพื่อให้สำนักงานสามารถติดตามและสอบถามข้อมูลได้ ● สำนักงานจะอนุโลมให้ผู้รับดำเนินการด้านงานสนับสนุน (outsourcee) สามารถเป็นผู้นำส่งได้ กรณีที่ outsorcee นั้น เป็น Head of Compliance ของบริษัทในกลุ่มหรือบริษัทในเครือของผู้ประกอบธุรกิจเท่านั้น

ภาคผนวก

ภาคผนวก 1 : แผนภาพแสดง mobile device, teleworking และ BYOD (ขยายความ FAQ ข้อ 2.1)



ภาคผนวก 2 : ตัวอย่างแบบประเมินบุคคลภายนอก (Third-party assessment checklist)
(ขยายความ FAQ ข้อ 4.2.2.11)

แบบประเมินนี้มีวัตถุประสงค์เพื่อให้ตัวอย่างรายการสิ่งที่ควรพิจารณาเมื่อมีการ (1) ใช้บริการงานด้าน IT จากบุคคลภายนอก (2) เชื่อมต่อระบบ IT กับบุคคลภายนอก และ (3) อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแล ไม่ได้มีวัตถุประสงค์เพื่อกำหนดรายการสิ่งที่ควรพิจารณาทั้งหมดที่ผู้ประกอบธุรกิจต้องนำไปใช้ปฏิบัติ ผู้ประกอบธุรกิจควรนำแบบประเมินนี้ไปปรับปรุงเพิ่มเติมให้เหมาะสมและสอดคล้องนโยบายของผู้ประกอบธุรกิจ และระดับความมีนัยสำคัญของบุคคลภายนอก

ชื่อบุคคลภายนอก:		**วันที่ประเมิน:**
ประเภท	☐ ผู้ให้บริการงานด้าน IT ☐ ผู้ที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ ☐ ผู้ที่สามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้า	
รายละเอียดของงาน:		
ผู้ประเมิน: **1.**	**ตำแหน่ง**	
2.	**ตำแหน่ง**	

ส่วนที่ 1: การประเมินความเสี่ยงของบุคคลภายนอก

ความเสี่ยงของบุคคลภายนอก[5]	**ระดับความเสี่ยง**				**หมายเหตุ**
	1 **ต่ำ**	2 **กลาง**	3 **สูง**	N/A	
ความเสี่ยงด้านกลยุทธ์ – เช่น ทักษะและประสบการณ์ของผู้บริหารที่ไม่เพียงพออาจนำไปสู่การขาดความเข้าใจ ขาดการควบคุมความเสี่ยงที่สำคัญ และตัดสินใจเชิงกลยุทธ์ที่ผิดพลาด หรือความเสี่ยงที่การดำเนินการของบุคคลภายนอกไม่สามารถตอบสนองหรือไม่สอดคล้องกับเป้าหมายและกลยุทธ์ของผู้ประกอบธุรกิจ					
ความเสี่ยงด้านกฎหมาย – เช่น กิจกรรมที่ดำเนินการโดยบุคคลภายนอกไม่เป็นไปตามกฎระเบียบและอาจส่งผลกระทบต่อผู้ประกอบธุรกิจซึ่งอาจมีความผิดทางกฎหมาย					
ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่รัดกุมเพียงพอ – เช่น การไม่สามารถตรวจสอบการดำเนินงานของบุคคลภายนอกได้ด้วยตนเอง					

[5] ประเภทความเสี่ยงที่ระบุในตาราง เป็นการให้ตัวอย่างความเสี่ยงสำคัญที่ผู้ประกอบธุรกิจควรคำนึงถึง ทั้งนี้ ผู้ประกอบธุรกิจอาจพิจารณาความเสี่ยงอื่น ๆ เพิ่มเติมได้ตามความเหมาะสม

ความเสี่ยงของบุคคลภายนอก[5]	ระดับความเสี่ยง				หมายเหตุ
	1 ต่ำ	2 กลาง	3 สูง	N/A	
ความเสี่ยงจากการกระจุกตัว – เช่น บุคคลภายนอกให้ความสำคัญกับผู้ประกอบธุรกิจรายอื่นสูงกว่า (higher priority) ในกรณีที่เกิดเหตุการณ์ผิดปกติ ซึ่งบุคคลภายนอกมีลูกค้าที่ต้องแก้ปัญหาให้ลูกค้าหลายราย					
ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก (third party/vendor locked-in) – เช่น ข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยีผู้ให้บริการ หรือข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเองเป็นต้น					
ความเสี่ยงด้าน IT และภัยทางไซเบอร์ – เช่น ระบบที่ให้บริการโดยบุคคลภายนอกเกิดขัดข้อง ระบบของบุคคลภายนอกมีช่องโหว่ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล เป็นต้น					
ความเสี่ยงกรณีบุคคลภายนอกให้ผู้อื่นดำเนินการแทน (sub-contracting) – เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น					

ผลการประเมิน : เป็นบุคคลภายนอกที่ ☐ **มี** ☐ **ไม่มีนัยสำคัญ**[6]

ส่วนที่ 2: การประเมินคุณสมบัติของบุคคลภายนอก

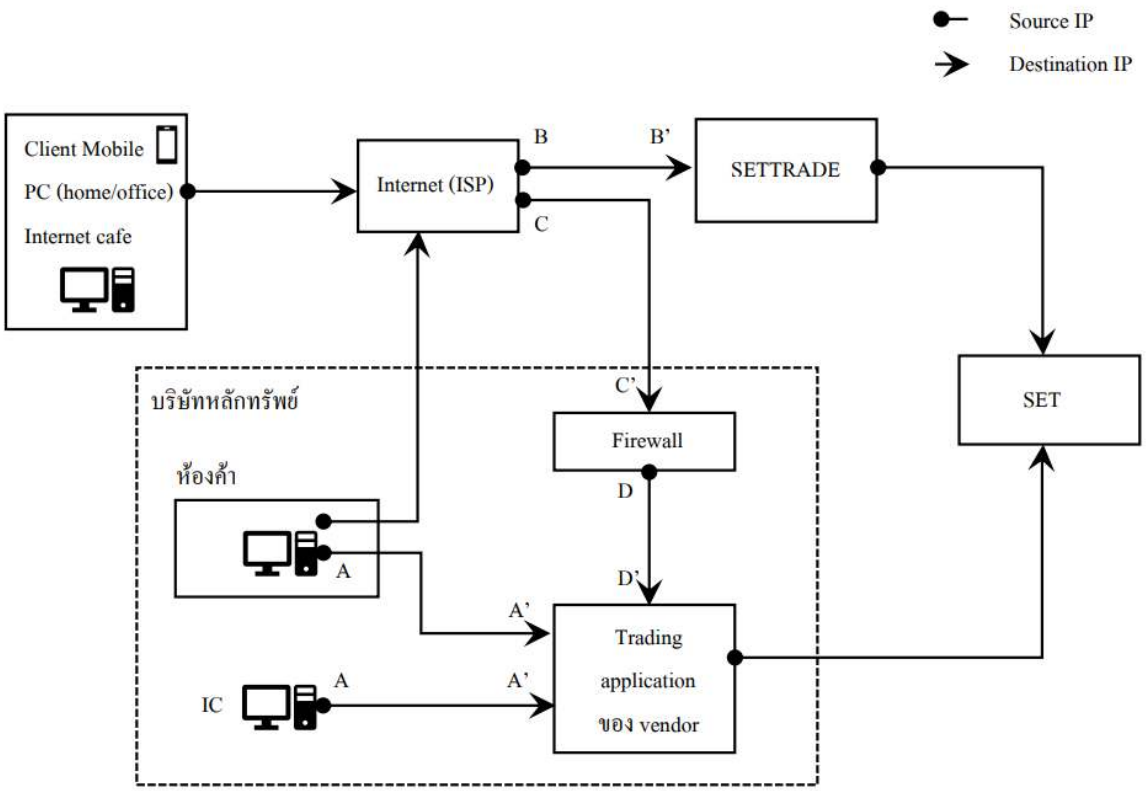
ปัจจัยการประเมิน	ผลการประเมิน			หมายเหตุ
	ผ่าน	ไม่ผ่าน	N/A	
1. ข้อมูลทั่วไป				
1.1 การจดทะเบียนตั้งบริษัท / ใบอนุญาตประกอบธุรกิจที่เกี่ยวข้อง				
1.2 ที่ตั้งบริษัท (proof of location)				
1.3 ฐานะทางการเงิน				
1.4 ชื่อเสียงของบริษัท				
1.5 ประวัติของผู้บริหาร				
1.6 ความเชี่ยวชาญ/ประสบการณ์ในการให้บริการ				
1.7 โครงสร้างองค์กร				
1.8 ประวัติเกี่ยวกับการกระทำความผิดทางกฎหมาย				
1.9 กฎหมายที่มีผลใช้บังคับกับบุคคลภายนอก (*กรณีบุคคลภายนอกเป็นบริษัทต่างประเทศ ควรพิจารณาถึงความเพียงพอ				

[6] ผู้ประกอบธุรกิจสามารถกำหนดวิธีการพิจารณาความมีนัยสำคัญของบุคคลภายนอกจากผลการประเมินความเสี่ยงด้านต่าง ๆ

ปัจจัยการประเมิน	ผลการประเมิน			หมายเหตุ
	ผ่าน	ไม่ผ่าน	N/A	
เหมาะสมของกฎหมายที่บังคับใช้กับบุคคลภายนอก เช่น การคุ้มครองข้อมูลส่วนบุคคล เป็นต้น)				
1.10 ช่องทางการติดต่อ และการรับแจ้งปัญหา				
2. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์				
2.1 ประวัติเกี่ยวกับการรั่วไหลของข้อมูล (data breach history)				
2.2 ประวัติเกี่ยวกับการถูกโจมตีทางไซเบอร์อย่างมีนัยสำคัญ (significant cyber-attack history)				
2.3 นโยบาย/มาตรการรักษาความมั่นคงปลอดภัยด้าน IT				
2.4 นโยบาย/มาตรการรักษาความมั่นคงปลอดภัยของข้อมูล รวมถึงข้อมูลส่วนบุคคล				
2.5 การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน				
2.6 แผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident response plan)				
2.7 การรายงานเหตุการณ์ผิดปกติหรือปัญหาด้าน IT ต่อบริษัท				
2.8 ระบบงานสำรอง (disaster recovery site) และแผนกู้คืนระบบ IT (disaster recovery plan)				
2.9 คุณสมบัติในด้านความต่อเนื่องในการบริการ อาทิ Uptime SLA, Recovery Time Objective (RTO) และ Recovery Point Objective (RPO)				
2.10 ผลการทดสอบด้านประสิทธิภาพ และความมั่นคงปลอดภัยของระบบ เช่น performance test และ penetration test report เป็นต้น				
2.11 แนวทางการบริหารจัดการ sub-contract (การจ้างช่วงงานต่อ) เช่น – การแจ้งผู้ประกอบธุรกิจ เมื่อมีการใช้งานหรือเปลี่ยนแปลง sub-contract – ความรับผิดชอบของผู้ให้บริการ ในกรณีที่มีการใช้งาน sub-contract				
2.12 ความสามารถในการเปลี่ยนแปลงบุคคลภายนอก (alternative third party) ในกรณีที่บุคคลภายนอกไม่สามารถให้บริการต่อได้				
2.13 การจัดให้มีผลการตรวจสอบด้าน IT โดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น การตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 Type 2 Report) หรือ PCI-DSS Attestation of Compliance (AOC) เป็นต้น / การกำหนดสิทธิ์ในการเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอก				

ปัจจัยการประเมิน	ผลการประเมิน			หมายเหตุ
	ผ่าน	ไม่ผ่าน	N/A	
3. คุณสมบัติทางด้านเทคโนโลยี				
3.1 การนำระบบหรือข้อมูลไปใช้งานกับระบบงานอื่น หรือสามารถเชื่อมโยงกับระบบอื่นได้ (interoperability)				
3.2 ความมั่นคงปลอดภัยของวิธีการยืนยันตัวตน (authentication)				
3.3 ประสิทธิภาพและความเพียงพอของระบบ (capacity)				
3.4 วิธีการเข้ารหัสของข้อมูล (encryption)				
3.5 วิธีการควบคุมการเข้าถึงข้อมูล (data access)				
3.6 ความน่าเชื่อของเทคโนโลยีที่ใช้				

ภาคผนวก 3 : แผนภาพแสดงการเก็บ application log (ขยายความ FAQ ข้อ 4.8.7.4)



ตารางตัวอย่างการเก็บ application log (ขยายความ FAQ ข้อ 4.8.7.4)

1. Authentication part	User ID	Date/time	IP address (Source)		
2. Trading part	Broker ID/No.	Symbol	SET order ID	Account ID	Date & order time
3. Source - IP part	IP address (Source)	IP address (Destination)	Full URL		

การ corelate log ระหว่างอุปกรณ์

กรณี 1.1 (1) + (2) + (3) (1),(3) Private IP
Trading app

กรณี 2.1 (1) + (2) + (3) (1),(3) public IP
Trading app Network Firewall

กรณี 1.2 (1) (2) + (3) (1) Private IP (3) Public IP
เครื่องของ บล. SETTRADE

กรณี 2.2 (1) + (2) + (3) (1),(3) public IP
SETTRADE

ภาคผนวก 4 : แผนภาพระบบซึ่งต้องจัดให้มีการทดสอบการเจาะระบบ (penetration test) อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ (ขยายความ FAQ ข้อ 4.8.10.7)

	เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing)	ไม่ได้เชื่อมต่อกับเครือข่ายสาธารณะ
ระบบงาน (application system)	☑ VA ☑ Penetration test	☑ VA ☑ Penetration test
ระบบ IT ที่มีนัยสำคัญ (critical system)	☑ VA ☑ Penetration test	☑ VA ☐ Penetration test
ระบบอื่น ๆ รวมถึงระบบเครือข่าย	☑ VA ☑ Penetration test	☐ VA ☐ Penetration test

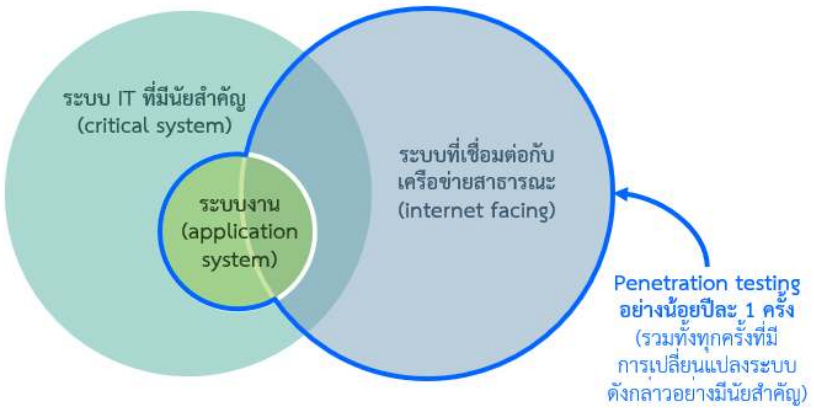
โดย

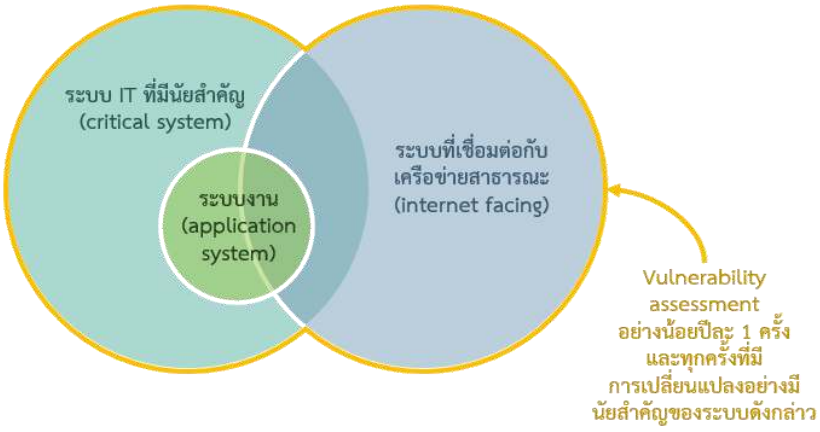
☑ VA : ต้องจัดให้มี technical vulnerability assessment อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ

☐ VA : สามารถจัดทำ vulnerability assessment ได้ตามความเหมาะสม

☑ Penetration test ต้องจัดให้มี penetration testing อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ

☐ Penetration test สามารถกำหนดขอบเขตและจัดทำ Penetration Testing ได้ตามความเหมาะสมกับความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายภายใน





ภาคผนวก 5 – ข้อแตกต่างระหว่าง IRP, DRP, ITCP และ BCP (ขยายความ FAQ ข้อ 4.13.6)

ชนิดของแผน	วัตถุประสงค์	ขอบเขต
Incident Response Plan (IRP)	กำหนดวิธีปฏิบัติเพื่อบรรเทาผลกระทบ และแก้ไขเหตุการณ์ผิดปกติด้าน IT เช่น cyber attack เป็นต้น	บรรเทาผลกระทบ และป้องกันความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น กำหนดวิธีการแยกเครื่องที่ติดไวรัสออกจากระบบ และ cleanup ระบบ เป็นต้น ทั้งนี้ IRP อาจเป็นจุดเริ่มต้นในการ activate แผน ITCP และ DRP ต่อไป ขึ้นอยู่กับความรุนแรงของสถานการณ์
Disaster Recovery Plan (DRP)	กำหนดวิธีปฏิบัติในการเปลี่ยนแปลงการใช้ระบบ IT ไปยังสถานที่สำรอง (relocating IT systems to an alternate location)	ประกาศใช้หลังจากมีเหตุการณ์ที่ส่งผลกระทบให้ระบบ IT ที่มีนัยสำคัญหยุดชะงัก และต้องการระยะเวลาในการแก้ไข
IT Contingency Plan (ITCP)	กำหนดวิธีปฏิบัติในการกู้คืนระบบ IT ให้สามารถนำกลับมาใช้งานได้ภายในระยะเวลาเป้าหมายที่กำหนด	แผนการกู้คืนระบบที่ไม่ขึ้นกับสถานที่ (location-independent plan) ที่มุ่งเน้นวิธีการกู้คืนระบบไม่ว่าจะที่ primary site หรือ alternate site
Business Continuity Plan (BCP)	กำหนดวิธีปฏิบัติที่ช่วยให้กระบวนการทางธุรกิจที่สำคัญสามารถดำเนินการต่อไปได้อย่างต่อเนื่องเมื่อเกิดเหตุการณ์หยุดชะงัก	แผนที่ใช้งานเพื่อทำให้องค์กรสามารถดำเนินกระบวนการทางธุรกิจ (business process) ที่สำคัญได้อย่างต่อเนื่อง โดยไม่ขึ้นอยู่กับเทคโนโลยีที่ใช้ ทั้งนี้ BCP อาจมีการอ้างอิง DRP และ ITCP เพื่อสนับสนุนช่วยให้กระบวนการทางธุรกิจกลับสู่การให้บริการปกติได้

หมายเหตุ: นิยาม วัตถุประสงค์ และขอบเขตของแผนอาจมีความแตกต่างกันในมาตรฐานต่าง ๆ คำอธิบายในตารางข้างต้นอ้างอิงจากเอกสาร NIST SP 800-34, Revision 1 – Contingency Planning Guide for Federal Information Systems

ภาคผนวก 6 – การนับรอบปีการตรวจสอบด้าน IT ตามข้อกำหนดของประกาศที่ สธ. 38/2565 ที่แก้ไขเพิ่มเติมโดยประกาศที่ สธ. 33/2567 (ขยายความ FAQ ข้อ 4.8.10.7)

หลักเกณฑ์ IT	รอบปีการตรวจสอบด้าน IT	อ้างอิงจากผลการประเมินแบบ RLA			การตรวจสอบด้าน IT ตามผล RLA		(ถ้าเข้าข่ายต้องจัดให้มีการตรวจสอบในรอบปี) นำส่งแบบรายงานผลการตรวจสอบด้าน IT และแผนปรับปรุงแก้ไขข้อบกพร่องภายในวันที่‡
		รอบ RLA	กรอบข้อมูลย้อนหลังเพื่อคำนวณ RLA	กำหนดการนำส่งผลการประเมิน RLA	(ก) "ผู้ประกอบธุรกิจขนาดเล็ก" หรือ "ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ"	(ข) "ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง" หรือ "ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง"	
ฉบับก่อนการแก้ไขเพิ่มเติม (ฉบับที่ 1)	**2567**	2566	Q4 2565 – Q3 2566	31 ธ.ค. 2566	**ต้อง** (full scope ทุก 2 ปี โดยปีที่มิได้ตรวจสอบแบบ full scope สามารถตรวจสอบแบบ partial scope ได้)	**ต้อง**	ภายในระยะเวลาดังนี้ แล้วแต่ระยะเวลาใดจะครบกำหนดก่อน - 30 วัน นับแต่วันที่เสนอต่อ BoD หรือ AC - 90 วัน นับแต่วันที่สิ้นสุดการตรวจสอบ - 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบ
ฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) (มีผลบังคับใช้ตั้งแต่วันที่ 1 ม.ค. 2568 เป็นต้นไป)	**2568**	2567	Q4 2566 – Q3 2567	31 ธ.ค. 2567	ไม่ได้กำหนด*‡	**ต้อง**	31 มี.ค. 2569‡
	2569	2569**	Q1 – Q4 2568	31 มี.ค. 2569	**ต้อง**	**ต้อง**	31 มี.ค. 2570‡
	2570	2570	Q1 – Q4 2569	31 มี.ค. 2570	ไม่ได้กำหนด*‡	**ต้อง**	31 มี.ค. 2571‡
	2571	2571	Q1 – Q4 2570	31 มี.ค. 2571	ไม่ได้กำหนด*‡	**ต้อง**	31 มี.ค. 2572‡
	2572	2572	Q1 – Q4 2571	31 มี.ค. 2572	**ต้อง**	**ต้อง**	31 มี.ค. 2573‡
	2573	2573	Q1 – Q4 2572	31 มี.ค. 2573	ไม่ได้กำหนด*‡	**ต้อง**	31 มี.ค. 2574‡
	2574	2574	Q1 – Q4 2573	31 มี.ค. 2574	ไม่ได้กำหนด*‡	**ต้อง**	31 มี.ค. 2575‡
	2575	2575	Q1 – Q4 2574	31 มี.ค. 2575	**ต้อง**	**ต้อง**	31 มี.ค. 2576‡
	2576	2576	Q1 – Q4 2575	31 มี.ค. 2576	ไม่ได้กำหนด*‡	**ต้อง**	31 มี.ค. 2577‡
	2577	2577	Q1 – Q4 2576	31 มี.ค. 2577	ไม่ได้กำหนด*‡	**ต้อง**	31 มี.ค. 2578‡
	2578	2578	Q1 – Q4 2577	31 มี.ค. 2578	**ต้อง**	**ต้อง**	31 มี.ค. 2579‡
	...	...	...	...	... *‡	...	... ‡

หมายเหตุ :

* กรณีที่เกิดเหตุการณ์ด้าน**ความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ** ผู้ประกอบธุรกิจขนาดเล็กและผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำต้องจัดให้มีการดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ดังกล่าวด้วย

** ตั้งแต่หลักเกณฑ์ฉบับแก้ไขเพิ่มเติมมีผลใช้บังคับ รอบปี RLA จะเรียกตามรอบปีที่นำส่งแบบ RLA

‡ **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล** เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล (Digital Asset Advisory Service) ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Digital Asset Exchange) เป็นต้น มีหน้าที่ในการปฏิบัติตามข้อกำหนดของประกาศ **กธ. 19/2561** เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจึงยังคง**ต้องจัดให้มีการตรวจสอบทุกปี** และ**ต้องนำส่งรายงานต่อสำนักงานตามเงื่อนไขของประกาศ กธ. 19/2561** คือ

(1) จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ก่อนเริ่มให้บริการและภายหลังเริ่มให้บริการแล้ว**อย่างน้อยปีละ 1 ครั้ง** *และ*

(2) รายงานผลต่อสำนักงานภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการทดสอบ

แม้ว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล เช่น ที่ปรึกษาสินทรัพย์ดิจิทัล เป็นต้น ได้ผลการประเมินแบบ RLA เป็นผู้ประกอบธุรกิจขนาดเล็ก ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง เพื่อให้เป็นไปตามข้อกำหนดของประกาศ กธ. 19/2561

ภาคผนวก 7 – การกำหนดขอบเขตของการตรวจสอบ (ขยายความ FAQ ข้อ 5.15)

กรณีที่ 1: การตรวจสอบแบบ full scope สำหรับบริษัท A ซึ่งมีผลการประเมินแบบ RLA เป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง บริษัท A จะต้องมี control ที่ต้องปฏิบัติจำนวนรวม 264 ข้อ หากบริษัท A มีระบบ IT ที่มีนัยสำคัญ ได้แก่ System A, System B และ System C [7]

- การทำ IT audit ต้องครอบคลุม control ครบทุก 264 ข้อ
- ในแต่ละปี บริษัทควรวางแผนและกำหนดขอบเขตของการตรวจสอบให้ครอบคลุมระบบ IT ที่มีนัยสำคัญอย่างน้อย 1 ระบบ และตรวจสอบทุกมาตรการควบคุม (ทุก control) บนระบบงานดังกล่าว เพื่อให้คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายมีข้อมูลที่เพียงพอประกอบการกำกับดูแลการปฏิบัติงานและบริหารจัดการความเสี่ยงด้าน IT ได้อย่างมีประสิทธิภาพ
- กรณีระบบ IT ที่มีนัยสำคัญซึ่งอยู่ในขอบเขตของการตรวจสอบประจำปี แต่ไม่ได้รับการตรวจสอบทุก control เช่น ปี 2568 บริษัทจะตรวจสอบ System A (ทุก control) เป็นอย่างน้อย และ System B (เฉพาะ control ใน Domain 2.2) ให้ผู้ประกอบธุรกิจแจ้งข้อมูลเพิ่มเติมสำหรับ System B ใน column B ของ Sheet 3. Scope ในแบบรายงานผล IT Audit ให้ระบุ “System B (ตรวจสอบเฉพาะ Domain ที่ 2.2)”

ตัวอย่าง วิธีการวางแผนการตรวจสอบของบริษัท A มีรายละเอียด ดังนี้

	ปีที่ X			**ปีที่ X+1**			**ปีที่ X+2**			**ปีที่ X+3**		
	System A	System B	System C	System A	System B	System C	System A	System B	System C	System A	System B	System C
Control #1	X				X				X	X		
Control #2	X				X				X	X		
Control #3	X				X				X	X		
Control #4	X				X				X	X		
Control #5	X				X				X	X		
Control #6	X				X				X	X		
...	X				X				X	X		
Control #264	X				X				X	X		

หมายเหตุ : การรายงานผลต่อคณะกรรมการหรือผู้บริหารที่เกี่ยวข้อง ควรระมัดระวังเรื่องความเข้าใจผิดในการรายงานผล/การวิเคราะห์ข้อมูล เช่น กรณีไม่พบข้อบกพร่อง (finding) สำหรับ control #2 บน System A ผู้บริหารอาจเกิดความเข้าใจผิดว่า control #2 ของ System B และ C ก็ไม่พบข้อบกพร่องเช่นกัน เป็นต้น

[7] รายชื่อระบบ IT ที่มีนัยสำคัญที่ควรอยู่ในขอบเขตของการตรวจสอบ สามารถอ้างอิง “Sheet 3.1 Critical systems” ของ “แบบรายงานผล IT Audit” สำหรับระบบ IT ที่ไม่ได้ถูกกำหนดใน Sheet ดังกล่าว บริษัทสามารถพิจารณาขอบเขตการทำ IT audit เพิ่มเติมได้ตามความเสี่ยง

กรณีที่ 2: บริษัท B เป็นผู้ประกอบธุรกิจขนาดเล็ก โดยมี control ที่ต้องปฏิบัติจำนวนรวม 62 ข้อ และมีระบบ IT ที่มีนัยสำคัญ ได้แก่ System X, System Y, และ System Z

ปีที่สำนักงานกำหนดให้มีการตรวจสอบด้าน IT เช่น ปี 2569 2572 2575 เป็นต้น

- การทำ IT audit ต้องครอบคลุม control ครบทุก 62 ข้อ
- บริษัทควรวางแผนและกำหนดขอบเขตของการตรวจสอบให้ครอบคลุมระบบ IT ที่มีนัยสำคัญอย่างน้อย 1 ระบบ และตรวจสอบทุกมาตรการควบคุม (ทุก control) บนระบบงานดังกล่าว เพื่อให้คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายมีข้อมูลที่เพียงพอประกอบการกำกับดูแลการปฏิบัติงานและบริหารจัดการความเสี่ยงด้าน IT ได้อย่างมีประสิทธิภาพ
- กรณีระบบ IT ที่มีนัยสำคัญซึ่งอยู่ในขอบเขตของการตรวจสอบประจำปี แต่ไม่ได้รับการตรวจสอบทุก control เช่น ปี 2569 บริษัทจะตรวจสอบ System X (ทุก control) และ System Y (เฉพาะ control ใน Domain 2.5) ให้ผู้ประกอบธุรกิจแจ้งข้อมูลเพิ่มเติมสำหรับระบบงาน Y ใน column B ของ Sheet 3. Scope ในแบบรายงานผล IT Audit ให้ระบุ ว่า “System Y (ตรวจสอบเฉพาะ Domain ที่ 2.5)”

ตัวอย่าง วิธีการวางแผนการตรวจสอบของบริษัท B (กรณีไม่มีการเปลี่ยนแปลงของระดับ RLA ในแต่ละปี) มีรายละเอียด ดังนี้

	ปีที่ X			**ปีที่ X+1 (กรณีไม่เกิด major IT security incident)**			**ปีที่ X+2 (กรณีไม่เกิด major IT security incident)**			**ปีที่ X+3**		
	System X	System Y	System Z	System X	System Y	System Z	System X	System Y	System Z	System X	System Y	System Z
Control #1	X										X	
Control #2	X										X	
Control #3	X										X	
Control #4	X										X	
Control #5	X										X	
Control #6	X										X	
...	X										X	
Control #62	X										X	