บริษัท [ชื่อบริษัท]

รายงานผลการตรวจประเมินทางด้านเทคโนโลยีสารสนเทศ

ปี พ.ศ. 25xx

สารบัญ

1. บทสรุปสำหรับผู้บริหาร

ตามที่สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต. หรือ สำนักงาน) มีวัตถุประสงค์เพื่อให้ผู้ประกอบธุรกิจภายใต้การกำกับดูแลของสำนักงาน มีการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและเป็นระบบ รวมทั้งมีการควบคุมและรักษา ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม สอดคล้องกับมาตรฐานสากลนั้น บริษัท [ชื่อบริษัท] (บริษัท) ได้ให้ความสำคัญในเรื่องการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ จึงจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นการตรวจประเมินโดย หน่วยงานตรวจสอบภายในของบริษัท/การจัดจ้างผู้เชี่ยวชาญภายนอก/จัดทำรายงานเพื่อให้ความเชื่อมั่นตามมาตรฐานสากล/อื่น ๆ

การตรวจประเมินดำเนินการในระหว่างวันที่ [dd mmmm yyyy] ถึงวันที่ [dd mmmm yyyy] โดยขอบเขตการตรวจประเมินครอบคลุมระบบสารสนเทศสำคัญ ได้แก่ ระบบ XXX, XXX, XXX โดยเป็นการประเมินความเพียงพอเหมาะสมของการออกแบบการควบคุม (Control design effectiveness) และ การประเมินการควบคุมที่มีการดำเนินการ (Control operating effectiveness) ในระยะเวลา xx เดือน ตั้งแต่วันที่ [dd mmmm yyyy] ถึงวันที่ [dd mmmm yyyy] ผลการตรวจประเมินโดยสรุป เป็นดังนี้

หัวข้อการตรวจสอบ	**ประเด็นข้อตรวจพบ**		
	ระดับสูง	**ระดับปานกลาง**	**ระดับต่ำ**
(1) การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยี			
1.1 บทบาทหน้าที่คณะกรรมการของผู้ประกอบธุรกิจ	[หัวข้อตรวจพบ]	[หัวข้อตรวจพบ]	[หัวข้อตรวจพบ]
1.2. โครงสร้างการกำกับดูแลในระดับองค์กร			
1.3. การกำหนดนโยบายด้าน IT			
(2) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยี			
2.1. โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT			
2.2 การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT			

หัวข้อการตรวจสอบ	ประเด็นข้อตรวจพบ		
	ระดับสูง	ระดับปานกลาง	ระดับต่ำ
2.3 การบริหารจัดการทรัพย์สินด้าน IT			
2.4 การรักษาความมั่นคงปลอดภัยของข้อมูล			
2.5 การควบคุมการเข้าถึงข้อมูลและระบบ IT			
2.6 การบริหารจัดการการเข้ารหัสข้อมูล			
2.7 การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม			
2.8 มาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT			
2.9 มาตรการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์			
2.10. การบริหารจัดการโครงการด้าน IT มาตรการการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ			
2.11. การบริหารจัดการบุคคลภายนอก			
2.12. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้าน IT			
2.13. แผนฉุกเฉินด้าน IT			

โดยประเด็นข้อตรวจพบข้างต้น รวมทั้งแผนการดำเนินการแก้ไข ได้ถูกรายงานไปยังคณะกรรมการบริษัทเพื่อพิจารณาเห็นชอบแล้วในวันที่ [dd mmmm yyyy]

2. วัตถุประสงค์และขอบเขต

บริษัทจัดทำเอกสารฉบับนี้ขึ้นเพื่อรายงานผลการตรวจประเมินด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องตามประกาศที่ สธ. xx/25xx เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ และ ประกาศ ที่ นป. x/25xx เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ โดยบริษัทสามารถนำผลการตรวจประเมินมาใช้เป็นแนวทางปรับปรุงการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงส่งเสริมและสนับสนุนการดำเนินงาน เพื่อนำไปสู่กา รยกระดับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรต่อไป

บริษัทกำหนดขอบเขตในการตรวจประเมินให้ครอบคลุมการประเมินความเพียงพอเหมาะสมของการออกแบบการควบคุม (Control design effectiveness) และ การประเมินการควบคุมที่มีการดำเนินการ (Control operating effectiveness) ในระยะเวลา xx เดือน ตั้งแต่วันที่ [dd mmmm yyyy] ถึงวันที่ [dd mmmm yyyy] โดยครอบคลุมระบบงานสำคัญของบริษัท ดังนี้

ลำดับ	ชื่อระบบงาน

<อ้างอิงรายละเอียดของระบบงานในภาคผนวก 1>

การตรวจประเมินดำเนินการในระหว่างวันที่ [dd mmmm yyyy] ถึงวันที่ [dd mmmm yyyy] โดยหน่วยงานตรวจสอบภายในของบริษัท/ผู้เชี่ยวชาญภายนอกจากบริษัท XXX โดยได้รายงานข้อตรวจพบข้างต้น รวมทั้งแผนการดำเนินการแก้ไขไปยังคณะกรรมการบริษัทเพื่อพิจารณาเห็นชอบแล้วในวันที่ [dd mmmm yyyy]

3. การยืนยันการดำเนินงานตรวจสอบ

ในการตรวจสอบในครั้งนี้ บริษัทให้หน่วยงานตรวจสอบภายในของบริษัท / ผู้ตรวจสอบภายนอกจากบริษัท XXXXXX ที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญในการดำเนินงาน และมีรายชื่อผู้ดำเนินงานตรวจสอบ ดังนี้

ผู้ตรวจสอบ

1. นาย/นาง/น.ส. ..... นามสกุล ..... ตำแหน่ง ..... โดยมีประสบการณ์ในการตรวจสอบด้าน IT รวม xx ปี และมีใบประกาศนียบัตรรับรอง CISA, CISM, CISSP, ISO/IEC 27001Lead Auditor, xxxxx

ผู้สอบทาน

2. นาย/นาง/น.ส. ..... นามสกุล ..... ตำแหน่ง ..... โดยมีประสบการณ์ในการตรวจสอบด้าน IT รวม xx ปี และมีใบประกาศนียบัตรรับรอง CISA, CISM, CISSP, ISO/IEC 27001Lead Auditor, xxxxx

ข้าพเจ้าขอรับรองว่าข้อมูลที่อยู่ในรายงานฉบับนี้ถูกต้องเป็นความจริงทุกประการ จึงได้ลงลายมือชื่อไว้เป็นหลักฐาน

ลงชื่อ.....ผู้รับผิดชอบงานตรวจสอบ

(นาย/นาง/น.ส. XXXXX XXXXXXXX)

ตำแหน่ง XXXXXXXXXXXXXXXXXX

ลงชื่อ..... กรรมการผู้มีอำนาจหรือผู้รับมอบอำนาจของบริษัทฯ

(นาย/นาง/น.ส. XXXXX XXXXXXXX)

ตำแหน่ง XXXXXXXXXXXXXXXXXX

4. ภาพรวมทางด้านเทคโนโลยีสารสนเทศ

(1) การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยี
คณะกรรมการบริษัทฯอนุมัติ ทบทวนนโยบายและแผนกลยุทธ์ด้าน IT มีคณะอนุกรรมการพัฒนาระบบ IT (IT Steering Committee) กำกับดูแลการดำเนินงานและการรักษาความมั่นคงปลอดภัยด้าน IT xxxxxxxx
(2) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยี
มีการระบุการบริหารจัดการทรัพย์สินสารสนเทศตามนโนบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy)

5. สรุปผลการตรวจสอบ

จากการตรวจประเมินพบข้อตรวจพบ รวมทั้งสิ้น xx ข้อ และข้อสังเกตุเพิ่มเติมอื่น ๆ xx ข้อ โดยข้อตรวจพบถูกจำแนกตามระดับความสำคัญเพื่อให้มีการปรับปรุงแก้ไขตามความเสี่ยง ซึ่งแบ่งเป็น 3 ระดับ ได้แก่

หัวข้อการควบคุม	ข้อตรวจพบ	ระดับความสำคัญ[1]
การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร	1. xx	สูง
	2. xx	ต่ำ
นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	3. xx	ปานกลาง
การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ	4. xx	สูง

นอกจากนี้ ข้อสังเกตุเพิ่มเติมอื่น ๆ ที่บริษัทอาจพิจารณาดำเนินการในภายหลังเพื่อเป็นแนวทางการปฏิบัติที่ดีทางด้านสารสนเทศ ได้แก่

1. การxxx

[เพิ่มเติม อื่นๆที่ผู้ตรวจสอบอยากนำเสนอ]

[1] อ้างอิงภาคผนวก 8.3 แนวทางในการประเมินระดับความสำคัญของข้อตรวจพบจากการตรวจสอบการบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ

6. รายละเอียดประเด็นขอตรวจพบ

หมายเลข	ประเด็นข้อตรวจพบ	ระดับความสำคัญและความเสี่ยง	ข้อเสนอแนะของผู้ตรวจสอบ	ความคิดเห็นของผู้บริหารและแนวทางการแก้ไข	Control no.
	ข้อตรวจพบ สาเหตุของข้อตรวจพบ	**ระดับความสำคัญ** **ความเสี่ยง**		เห็นด้วย/ไม่เห็นด้วย ผู้รับผิดชอบ: แนวทางการดำเนินการ: ระยะเวลาที่คาดว่าจะแล้วเสร็จตามระดับความสำคัญ[2]:	

[2] ระยะเวลาที่คาดว่าจะแล้วเสร็จตามระดับความสำคัญ เพื่อให้มีการปรับปรุงแก้ไขตามระดับความเสี่ยงโดยมี 3 ระดับ ได้แก่

1) ระดับความสำคัญสูง บริษัทควรดำเนินการแก้ไขให้แล้วเสร็จภายในภายใน 3 เดือน

2) ระดับความสำคัญปานกลาง บริษัทควรดำเนินการแก้ไขให้แล้วเสร็จภายในภายใน 3-6 เดือน

3) ระดับความสำคัญต่ำ บริษัทควรดำเนินการแก้ไขเมื่อมีความพร้อมของทรัพยากรในด้านต่าง ๆ หากได้รับการแก้ไขจะช่วยเพิ่มประสิทธิภาพการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

7. สถานะการติดตามประเด็นข้อตรวจพบในปีที่ผ่านมา

หมายเลข	ประเด็นข้อตรวจพบคงค้าง	อ้างอิงผลการตรวจสอบ	ความคิดเห็นของผู้บริหารและแนวทางการแก้ไข	ผลการดำเนินการแก้ไขของบริษัทในปัจจุบัน	Control no.
	ข้อตรวจพบ สาเหตุของข้อตรวจพบ ระดับความสำคัญ	ผลการตรวจสอบปี 25xx	เห็นด้วย/ไม่เห็นด้วย ผู้รับผิดชอบ แนวทางการดำเนินการ ระยะเวลาที่คาดว่าจะแล้วเสร็จตามระดับความสำคัญ:		

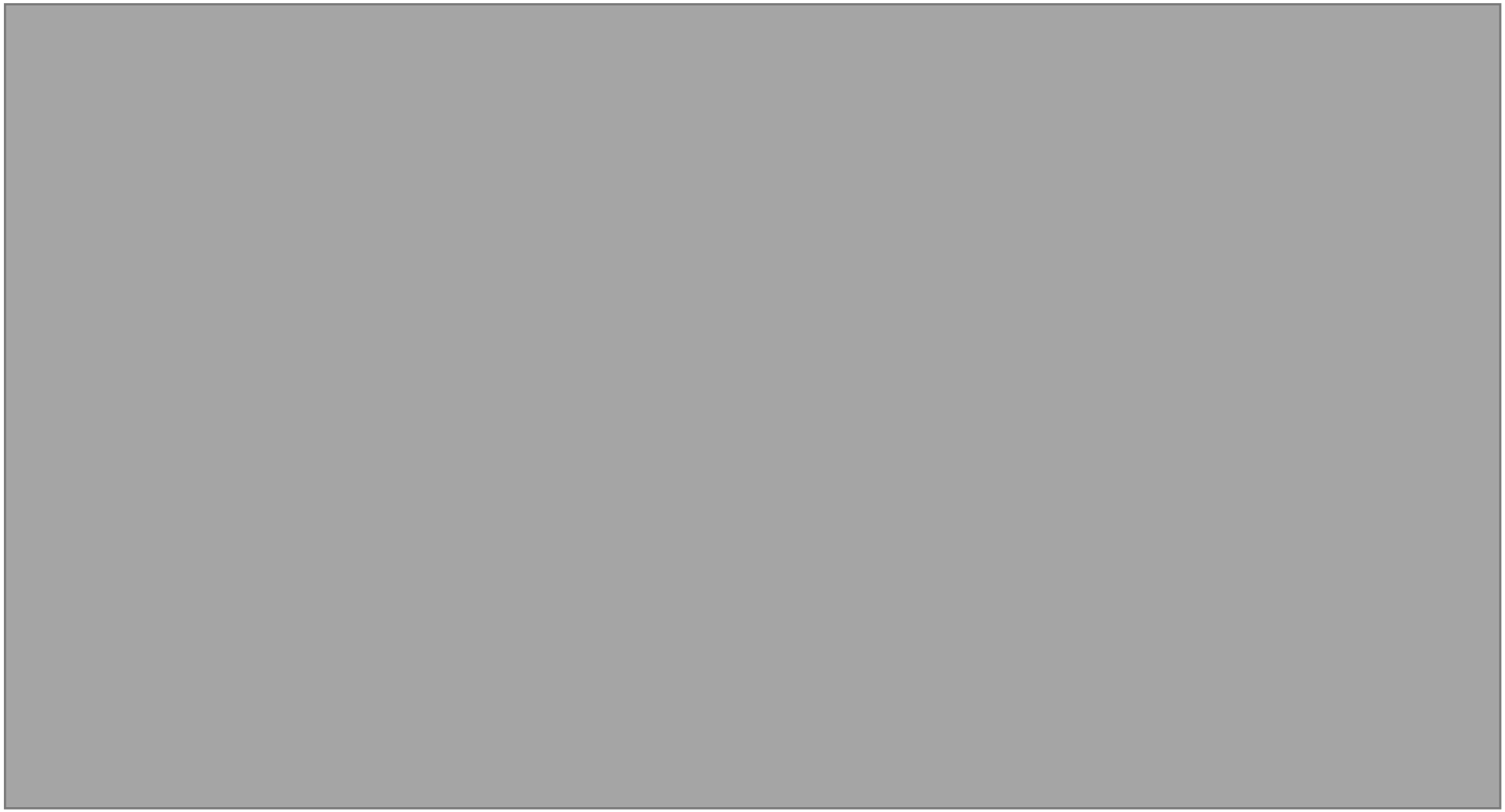
<u>หมายเหตุ</u>

1. ความเสี่ยง หมายถึง ความเสี่ยงของข้อตรวจพบ ซึ่งมีผลกระทบต่อ (1) ระบบหรือการปฏิบัติงานของผู้ประกอบธุรกิจ (2) ความมั่นคงปลอดภัยด้านสารสนเทศ (Information security) และข้อมูล หรือ (3) ความเชื่อมั่นของตลาดทุน ซึ่งรวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threat)
2. ข้อเสนอแนะของผู้ตรวจสอบ หมายถึง การให้ข้อเสนอแนะจากผู้ตรวจสอบที่มีความครบถ้วนตั้งแต่ต้นจนจบกระบวนการ (End to End Process) เพื่อแก้ไขปรับปรุงข้อบกพร่องในการควบคุม หรือปรับปรุงให้มีประสิทธิภาพ สามารถจัดการกับความเสี่ยงทางไซเบอร์ได้
3. แนวทางการแก้ไข ควรระบุแนวทางการแก้ไขข้อตรวจพบที่สาเหตุ หรือ root cause ครอบคลุมทุกข้อสังเกตที่ตรวจพบ และกำหนดผู้รับผิดชอบ (Owner) ในการแก้ไขข้อตรวจพบ รวมถึงกำหนดระยะเวลาในการแก้ไขให้ชัดเจนและสอดคล้องกับความสำคัญและความเสี่ยง กรณีถ้ามีระยะเวลาดำเนินการยาวนานควรมีแผนการบรรเทาความเสี่ยง (Risk Treatment Plan) ด้วย

8. ภาคผนวก

8.1 รายละเอียดของระบบงาน

1) แผนภาพการเชื่อมต่อ และ ส่งผ่านของมูลของระบบงาน



2) ตารางแสดงรายละเอียดระบบงาน

No	ระบบงานสำคัญ	รายละเอียดการใช้งาน	ประเภทระบบงาน	ผู้พัฒนาระบบ	ผู้ดูแลระบบ (application / OS / DB level)	ศูนย์หลัก	ศูนย์สำรอง
	(e.g. SBA)	(e.g. Back office สำหรับ หุ้น และอนุพันธ์)	(e.g. Off-the-shelf with customization)	(e.g. Freewill)	(e.g. บริษัท AIRA ส่วนงาน IT - Back office)	(e.g. AIRA head office)	(e.g. CX Loxinfo)
	(e.g. Streaming)	(e.g. ช่องทางซื้อขายหุ้นและอนุพันธ์ (Retail))	(e.g. Off-the-shelf without customization)	(e.g. SETTRADE.COM)	(e.g. SETTRADE.COM)	(e.g. SET colo)	(e.g. บริหารจัดการโดย SETTRADE.COM)
1							
2							
3							

8.2. การประเมิน

ให้ผู้ประกอบธุรกิจตรวจประเมินตามมาตรการควบคุมที่พึงมีทุกหัวข้อ กรณีหัวข้อที่มีการแบ่งระดับการควบคุมเป็น 5 ระดับ (maturity model) การประเมินระดับ 3 คือระดับที่ถือว่าผู้ประกอบธุรกิจได้ปฏิบัติตามการควบคุมที่พึงมีตามข้อกำหนดในประกาศสำนักงาน

Control no.	การควบคุมที่พึงมี	คำอธิบาย	ผลประเมิน	หมายเหตุ
1.1	[ความเสี่ยงสูง] คณะกรรมการของผู้ประกอบธุรกิจควรจัดให้มีกรรมการของผู้ประกอบธุรกิจ หรือที่ปรึกษาของผู้ประกอบธุรกิจ อย่างน้อย 1 ท่าน ที่มีความรู้หรือประสบการณ์ด้าน IT	**Yes:** มีการดำเนินการ **Partial:** มีการดำเนินการเพียงบางส่วน **No:** ไม่มีการดำเนินการ	Out of scope	บริษัทไม่จำเป็นต้องดำเนินการควบคุมข้อดังกล่าว เนื่องจากเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง
1.3	คณะกรรมการมีการกำกับดูแลให้มีการกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT อย่างเป็นลายลักษณ์อักษร	**Yes:** มีการดำเนินการ **Partial:** มีการดำเนินการเพียงบางส่วน **No:** ไม่มีการดำเนินการ	Yes	
2.3.5	มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ประเภทอุปกรณ์ (hardware)	**LV1:** ไม่มีการจัดทำทะเบียนรายการทรัพย์สินด้าน IT **LV2:** มีการจัดทำทะเบียนรายการทรัพย์สินด้าน IT แต่ไม่ครบถ้วน **LV3:** มีการจัดทำทะเบียนรายการทรัพย์สินด้าน IT อย่างครบถ้วน **LV4:** มีการจัดทำทะเบียนรายการทรัพย์สินด้าน IT อย่างครบถ้วน รวมถึงมีการติดตามให้เป็นปัจจุบัน	LV 1	

Control no.	การควบคุมที่พึงมี	คำอธิบาย	ผลประเมิน	หมายเหตุ
		LV5: มีการจัดทำทะเบียนรายการทรัพย์สินด้าน IT อย่างครบถ้วนและมีการติดตามให้เป็นปัจจุบัน รวมถึงมีการนำเครื่องมือมาใช้ในการจัดทำทะเบียนทรัพย์สิน		
2.5.4	มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication)	**LV1:** ไม่มีกระบวนการยืนยันตัวตนผู้ใช้งาน **LV2:** มีกระบวนการยืนยันตัวตนผู้ใช้งาน แต่ไม่ครอบคลุมทุกระบบสารสนเทศ **LV3:** มีกระบวนการยืนยันตัวตนผู้ใช้งาน และครอบคลุมทุกระบบสารสนเทศ **LV4:** มีกระบวนการยืนยันตัวตนผู้ใช้งาน และครอบคลุมทุกระบบสารสนเทศ รวมถึงมีการติดตามให้มีประสิทธิภาพ **LV5:** มีกระบวนการยืนยันตัวตนผู้ใช้งาน และครอบคลุมทุกระบบสารสนเทศ รวมถึงมีการติดตามให้มีประสิทธิภาพ อีกทั้งมีการนำเครื่องมือมาใช้งาน	LV 2	
2.5.6	ใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) กับบัญชีผู้ใช้งานที่มีสิทธิสูง	**LV1:** ไม่กำหนดวิธีการยืนยันตัวตนแบบ MFA กับบัญชีสิทธิสูง **LV2:** มีการกำหนดวิธีการยืนยันตัวตนแบบ MFA กับบัญชีสิทธิสูง แต่ไม่ครอบคลุมทุก O/S และ DB ที่เกี่ยวข้องกับระบบสารสนเทศที่มีความสำคัญ **LV3:** มีการกำหนดวิธีการยืนยันตัวตนแบบ MFA กับบัญชีสิทธิสูง และครอบคลุมทุก O/S และ DB ที่เกี่ยวข้องกับระบบสารสนเทศที่มีความสำคัญ	LV 3	

Control no.	การควบคุมที่พึงมี	คำอธิบาย	ผลประเมิน	หมายเหตุ
		LV4: มีการกำหนดวิธีการยืนยันตัวตนแบบ MFA กับบัญชีสิทธิสูง และครอบคลุมทุก O/S และ DB ที่เกี่ยวข้องกับระบบสารสนเทศที่มีความสำคัญ รวมถึงมีการติดตามให้มีประสิทธิภาพ **LV5:** มีการกำหนดวิธีการยืนยันตัวตนแบบ MFA กับบัญชีสิทธิสูง และครอบคลุมทุก O/S และ DB ที่เกี่ยวข้องกับระบบสารสนเทศที่มีความสำคัญ รวมถึงมีการติดตามให้มีประสิทธิภาพ อีกทั้งมีการนำเครื่องมือมาใช้งาน		
2.6.2	มีการบริหารจัดการกุญแจเข้ารหัส (key management life cycle)	**LV1:** ไม่มีการบริหารจัดการกุญแจเข้ารหัสข้อมูล **LV2:** มีการบริหารจัดการกุญแจเข้ารหัสข้อมูล แต่ไม่ครบถ้วนทุกกระบวนการ **LV3:** มีการบริหารจัดการกุญแจเข้ารหัสข้อมูล และครบถ้วนทุกกระบวนการ **LV4:** มีการบริหารจัดการกุญแจเข้ารหัสข้อมูล และครบถ้วนทุกกระบวนการ รวมถึงมีการประเมินประสิทธิภาพของการควบคุมอย่างต่อเนื่อง **LV5:** มีการบริหารจัดการกุญแจเข้ารหัสข้อมูล ครบถ้วนทุกกระบวนการ และมีการประเมินประสิทธิภาพของการควบคุมอย่างต่อเนื่อง รวมถึงมีการใช้เครื่องมือในบริหารจัดการกุญแจเข้ารหัส	LV 5	
2.8.8	มีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติ	**Yes:** มีการดำเนินการ **Partial:** มีการดำเนินการเพียงบางส่วน	No	บริษัทไม่มีการกำหนดกระบวนการในการป้องกัน

Control no.	การควบคุมที่พึงมี	คำอธิบาย	ผลประเมิน	หมายเหตุ
	ด้าน IT โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ	**No:** ไม่มีการดำเนินการ		และตรวจจับเหตุการณ์ผิดปกติด้าน IT โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์บนระบบ IT ที่มีความสำคัญ รวมถึงยังไม่มีการจัดให้มีเครื่องมือที่สนับสนุนกระบวนการข้างต้น
2.8.11.1	มีการติดตามข้อมูลข่าวสารเกี่ยวกับ patch ที่อาจมีความเสี่ยงต่อระบบ IT ของผู้ประกอบธุรกิจอย่างทันต่อเหตุการณ์ รวมทั้งจัดให้มีการตรวจสอบช่องโหว่ที่เกี่ยวข้องบนระบบ IT	**Yes:** มีการดำเนินการ **Partial:** มีการดำเนินการเพียงบางส่วน **No:** ไม่มีการดำเนินการ	Partial	บริษัทติดตามการออก Security Patch เฉพาะส่วนของระบบปฏิบัติการ (OS) เท่านั้น อย่างไรก็ดี ระบบอื่น ๆ เช่น Database เป็นต้น ผู้ประกอบธุรกิจอยู่ระหว่างจัดทำขั้นตอนการติดตามข้อมูล patch

หมายเหตุ:

(1) Out of scope: ผู้ประกอบธุรกิจไม่จำเป็นต้องดำเนินการให้สอดคล้องตามการควบคุมนั้น ๆ เนื่องจากระดับความเสี่ยงของผู้ประกอบธุรกิจไม่เข้าเงื่อนไข เช่น ผู้ประกอบธุรกิจขนาดเล็ก ดำเนินการเฉพาะการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็นเท่านั้น หรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ และปานกลางไม่จำเป็นต้องทำแนวปฏิบัติระดับสูง เป็นต้น

(2) Not applicable: กรณีที่การควบคุมนั้น ๆ ไม่เกี่ยวข้องกับผู้ประกอบธุรกิจหรือกรณีที่ผู้ประกอบธุรกิจไม่มีการใช้งานเทคโนโลยีที่เกี่ยวข้องกับการควบคุมนั้น ๆ ภายในองค์กร เช่น ไม่อนุญาตให้พนักงานใช้การใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) ซึ่งผู้ประกอบธุรกิจสามารถกรอกข้อมูลในหัวข้อการควบคุมและการใช้งานอุปกรณ์ส่วนตัวของพนักงาน (bring your own device: BYOD) เป็น N/A ได้ โดยอธิบายมาในหมายเหตุด้วย

8.3. แนวทางในการประเมินระดับความสำคัญของข้อตรวจพบจากการตรวจสอบการบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ

แนวทางในการประเมินระดับความสำคัญของประเด็นข้อตรวจพบ มีหลักเกณฑ์ในการพิจารณาดังนี้

ก. การประเมินระดับความสำคัญเบื้องต้นจะพิจารณาจากผลกระทบที่เกิดขึ้นหรืออาจเกิดขึ้นในกรณีที่ไม่มีการปรับปรุงแก้ไขประเด็นข้อตรวจพบต่อการบรรลุถึงวัตถุประสงค์ของการบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศตามที่กำหนดไว้ในมาตรฐานและหลักเกณฑ์ที่เกี่ยวข้อง จะพิจารณาจาก กิจกรรมการควบคุมที่ผู้ประกอบธุรกิจพึงจัดให้มีเพื่อให้สามารถจัดการกับความเสี่ยงต่อการบรรลุถึงวัตถุประสงค์ที่เกี่ยวข้องตามที่กำหนดไว้ในมาตรฐานและหลักเกณฑ์ที่เกี่ยวข้อง ตามแนวทางดังนี้

ข้อตรวจพบที่มีความสำคัญระดับสูง	ข้อตรวจพบที่เกิดจากการไม่มีกิจกรรมการควบคุมหรือไม่สามารถตอบสนองต่อวัตถุประสงค์ของการควบคุม โดยมีหรืออาจมี ● ผลกระทบอย่างรุนแรง หรือ มีนัยสำคัญต่อการรักษาความลับ (Confidentiality) ของข้อมูล หรือ สารสนเทศที่สำคัญ ● ผลกระทบอย่างรุนแรง หรือ มีนัยสำคัญต่อความถูกต้องครบถ้วน (Integrity) ของข้อมูล การประมวลผล หรือ การปฏิบัติการทางด้านสารสนเทศ ● ผลกระทบอย่างรุนแรง หรือ มีนัยสำคัญต่อสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ หรือ ระบบงานสำคัญ
ข้อตรวจพบที่มีความสำคัญระดับปานกลาง	ข้อตรวจพบที่เกิดจากการขาดกิจกรรมการควบคุมที่ไม่ครบถ้วนหรือไม่สามารถตอบสนองต่อวัตถุประสงค์ของการควบคุมได้ทั้งหมด โดยมีหรืออาจมี ● ผลกระทบเพียงบางส่วนต่อการรักษาความลับ (Confidentiality) ของข้อมูล หรือ สารสนเทศที่สำคัญ ● ผลกระทบเพียงบางส่วนต่อความถูกต้องครบถ้วน (Integrity) ของข้อมูล การประมวลผล หรือ การปฏิบัติการทางด้านสารสนเทศ ● ผลกระทบเพียงบางส่วนต่อสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ
ข้อตรวจพบที่มีความสำคัญระดับต่ำ	ข้อตรวจพบที่เกิดจากการขาดกิจกรรมการควบคุมเพียงเล็กน้อยหรือไม่สามารถตอบสนองต่อวัตถุประสงค์ของการควบคุมเป็นส่วนน้อย โดยมีหรืออาจมี ● ผลกระทบเพียงส่วนน้อยต่อการรักษาความลับ (Confidentiality) ของข้อมูล หรือ สารสนเทศที่สำคัญ ● ผลกระทบเพียงส่วนน้อยต่อความถูกต้องครบถ้วน (Integrity) ของข้อมูล การประมวลผล หรือ การปฏิบัติการทางด้านสารสนเทศ ● ผลกระทบเพียงส่วนน้อยต่อสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ หรือ ระบบงานสำคัญ

ข้อสังเกตเพิ่มเติม	ข้อตรวจพบที่ไม่จัดอยู่ในประเด็นตรวจพบสามประเภทข้างต้น ซึ่งจะเป็นข้อตรวจพบที่ไม่มีผลกระทบโดยตรงต่อการบรรลุถึงวัตถุประสงค์ของการบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ โดยอาจเกิดจากข้อตรวจพบที่อยู่นอกเหนือขอบเขตการตรวจสอบหรือข้อตรวจพบส่งผลกระทบกับประสิทธิภาพของการควบคุมเท่านั้น

ข. พิจารณาปรับระดับความสำคัญเบื้องต้นจากปัจจัยที่เกี่ยวข้องอื่น ๆ ซึ่งรวมถึงลักษณะการใช้และสภาพแวดล้อมของระบบสารสนเทศของผู้ประกอบธุรกิจและปัจจัยที่มีผลกระทบต่อโอกาสเกิด (ถ้ามี) ดังนี้

1. <u>ระบบงานที่ได้รับผลกระทบจากข้อตรวจพบ</u>: โดยระบบงานมีส่วนสำคัญในการประเมินระดับผลกระทบของข้อตรวจพบ อาทิ
   - ข้อตรวจพบที่มีผลต่อทุกระบบงานของผู้ประกอบธุรกิจ จะมีระดับความสำคัญสูงกว่า ข้อตรวจพบที่มีผลเพียงบางระบบงานของผู้ประกอบธุรกิจ
   - ข้อตรวจพบที่ส่งผลต่อระบบงานที่มีการใช้งานโดยผู้ใช้งานจำนวนมาก หรือ ลูกค้าภายนอกที่ทำการซื้อขายหลักทรัพย์ จะมีระดับความสำคัญสูงกว่าระบบงานที่ใช้งานโดยผู้ใช้งานจำกัด หรือ ระบบงานที่มีการใช้งานเป็นการภายในสำหรับพนักงานบางส่วนเท่านั้น
   - ข้อตรวจพบทางด้านความมั่นคงปลอดภัยที่ส่งผลต่อระบบงานที่มีการเชื่อมต่อโดยตรงกับระบบเครือข่ายสาธารณะ หรือระบบอินเทอร์เน็ต จะมีระดับความสำคัญสูงกว่าข้อตรวจพบทางด้านความมั่นคงปลอดภัยของระบบที่มีการใช้งานภายในระบบเครือข่ายของบริษัท
   - ข้อตรวจพบที่ส่งผลต่อระบบงานที่ประมวลผลหรือจัดเก็บข้อมูลของผลิตภัณฑ์ที่มีมูลค่าสูง หรือ รายการทางธุรกิจในปริมาณมากจะมีระดับความสำคัญสูงกว่าข้อตรวจพบในระบบงานที่ประมวลผลหรือจัดเก็บข้อมูลของผลิตภัณฑ์บางกลุ่มบางประเภท หรือ ประมวลผลรายการทางธุรกิจเพียงบางส่วน

2. <u>ลักษณะการดำเนินธุรกิจ และ ประเภทธุรกรรมของผู้ประกอบธุรกิจ</u>: ลักษณะการดำเนินธุรกิจ หรือ ประเภทธุรกรรมมีส่วนในการประเมินระดับความสำคัญของข้อตรวจพบ อาทิ กรณีที่ผู้ประกอบธุรกิจมีปริมาณการทำรายการผ่านระบบเครือข่ายสาธารณะ หรือระบบอินเทอร์เน็ตในปริมาณมาก อาจทำให้ข้อตรวจพบที่เกี่ยวเนื่องกับความมั่นคงปลอดภัยในระบบมีการเชื่อมต่อระบบสารสนเทศกับระบบเครือข่ายสาธารณะ มีระดับความสำคัญสูงกว่าผู้ประกอบธุรกิจที่ยังมีปริมาณการทำรายการผ่านตัวแทนเป็นหลัก หรือ ข้อตรวจพบเกี่ยวกับความพร้อมใช้งานของระบบงานผู้ของประกอบธุรกิจประเภทตัวกลาง (Intermediaries) อาจมีความสำคัญมากกว่าข้อตรวจพบลักษณะเดียวกันของผู้ประกอบธุรกิจประเภทตัวแทน(Selling Agent) เนื่องจากลักษณะการดำเนินธุรกิจของประกอบธุรกิจประเภทตัวกลางที่อาจมีความต้องการการใช้งานระบบสารสนเทศตลอดระยะเวลาที่เปิดให้มีการซื้อขาย ในขณะที่ผู้ประกอบธุรกิจประเภทตัวแทนอาจมีระยะเวลาในการรวบรวมรายการทั้งหมดเพื่อสรุปยอดคำสั่ง ณ สิ้นวัน

3. <u>จำนวนข้อผิดพลาดที่ตรวจพบ:</u> โดยจากการตรวจสอบการควบคุม ซึ่งตรวจสอบจากรายการทั้งหมด หรือ สุ่มตรวจสอบทานตามความถี่ที่เกิดขึ้น จำนวนข้อผิดพลาดที่ตรวจพบเมื่อเปรียบเทียบกับจำนวนตัวอย่าง ส่งผลในการประเมินระดับความสำคัญของข้อตรวจพบ อาทิ ข้อผิดพลาดที่พบในปริมาณมาก มีแนวโน้มที่ทำให้ระดับความสำคัญของข้อตรวจพบสูงกว่าข้อผิดพลาดที่ตรวจพบเพียงส่วนน้อย ทั้งนี้ อาจพิจารณาร่วมกับสาเหตุที่มาของข้อผิดพลาดนั้น โดยในกรณีที่ข้อผิดพลาดเกิดขึ้นเพียง 1-2 รายการและเกิดจากเหตุสุดวิสัย (one-off error) อาจพิจารณาลดระดับหรือยกเลิกข้อตรวจพบนั้นได้

4. <u>การควบคุมเพิ่มเติม และ การควบคุมทดแทนอื่น ๆ</u>: นอกจากการควบคุมตามข้อกำหนดฯ และ นโยบายขององค์กรแล้ว ในกรณีที่ผู้ประกอบธุรกิจมีการควบคุมเพิ่มเติม หรือ การควบคุมทดแทนอื่น ๆ ที่สามารถลดผลกระทบ จำกัดโอกาสการเกิด หรือ ทำให้ข้อผิดพลาดหรือความเสี่ยงที่เกิดขึ้นถูกตรวจพบและได้รับการแก้ไขอย่างทันท่วงที การควบคุมเหล่านั้นสามารถนำมาพิจารณาเพิ่มเติมเพื่อลดระดับความสำคัญของข้อตรวจพบ รวมทั้ง สามารถพิจารณายกเลิกประเด็นข้อตรวจพบได้ ในกรณีที่การควบคุมเพิ่มเติม และ การควบคุมทดแทนเหล่านั้น สามารถลดระดับของผลกระทบ จำกัดโอกาสการเกิด หรือ ทำให้ข้อผิดพล าดหรือความเสี่ยงถูกตรวจพบและได้รับการแก้ไขอย่างทันท่วงทีเทียบเท่ากับการมีการควบคุมที่กำหนด

หมายเหตุ: ปัจจัยที่ใช้ในการประเมินระดับความสำคัญของข้อตรวจพบข้างต้นเป็นเพียงหลักการในภาพรวม อาจพิจารณาถึงปัจจัยอื่น ๆ อาทิ สิ่งที่สำนัก งานฯหรือผู้บริหารให้ความสำคัญ ข้อตรวจพบในการตรวจสอบครั้งที่ผ่านมา หรือ ปัจจัยอื่น ๆเพิ่มเติมตามความเหมาะสม