ธนาคารแห่งประเทศไทย

15 สิงหาคม 2562

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง

ที่ ธปท.ฝตท.(01) ว.1182/2562 เรื่อง การประเมินความพร้อมการรับมือภัยคุกคามไซเบอร์

ปัจจุบันสถาบันการเงินใช้เทคโนโลยีและระบบเทคโนโลยีสารสนเทศ เป็นกลไกหลักในการขับเคลื่อนธุรกิจ ทำให้เผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) มากขึ้น สถาบันการเงินจึงควรมีการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ที่เข้มงวด รัดกุม และเพียงพอตามระดับความเสี่ยงที่สถาบันการเงินมี เพื่อให้มีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ ทั้งการวางกรอบการกำกับดูแล การบริหารจัดการความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือหรือเทคโนโลยี เพื่อลดผลกระทบต่อลูกค้า สถาบันการเงิน และต่อระบบการเงินโดยรวม

ธนาคารแห่งประเทศไทย ได้กำหนดกรอบการประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber Resilience Assessment Framework) เพื่อให้สถาบันการเงินใช้สำหรับประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment) และแนวทางการบริหารจัดการความเสี่ยงทางไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level) ด้วยตนเอง เพื่อยกระดับความพร้อมในการรับมือภัยไซเบอร์ดังกล่าวให้สอดคล้องกับความเสี่ยงที่สถาบันการเงินมี (Risk-based) โดยกรอบการประเมินฯ มีสาระสำคัญดังนี้

1. **การประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment)** สถาบันการเงินประเมินโอกาสที่จะเผชิญและผลกระทบจากภัยคุกคามทางไซเบอร์ โดยพิจารณาปัจจัยความเสี่ยงพื้นฐานทางเทคโนโลยีสารสนเทศ 5 ด้าน คือ 1) ประเภท ขอบเขตและปริมาณการใช้เทคโนโลยีสารสนเทศในรูปแบบต่าง ๆ รวมถึงลักษณะการติดต่อสื่อสารหรือการเชื่อมต่อของระบบเทคโนโลยีสารสนเทศทั้งภายในและกับภายนอกองค์กร 2) ความหลากหลายของช่องทางการให้บริการอิเล็กทรอนิกส์ 3) รูปแบบ ปริมาณและความซับซ้อนของผลิตภัณฑ์/บริการ จำนวนลูกค้าและปริมาณการใช้งาน 4) ขนาดและลักษณะเฉพาะขององค์กร เช่น จำนวนสาขาหรือบริษัทในเครือที่อยู่ต่างประเทศ การใช้บริการ IT outsourcing และ 5) ประวัติการถูกภัยคุกคามทางไซเบอร์ ซึ่งเป็นปัจจัยที่บ่งชี้ถึงการตกเป็นเป้าหมายในการถูกโจมตี ผลการประเมินระดับความเสี่ยงไซเบอร์จากปัจจัยทั้ง 5 ด้าน แบ่งออกเป็น 3 ระดับ ได้แก่ **ต่ำ ปานกลาง** หรือ **สูง** เพื่อกำหนดแนวทางการบริหารจัดการความเสี่ยงทางไซเบอร์ให้สอดคล้องกัน

2. **แนวทางการบริหารจัดการความเสี่ยงทางไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level)** เป็นการประเมินการบริหารจัดการและการควบคุมความเสี่ยงภัยทางไซเบอร์ว่าอยู่ในระดับที่สอดรับกับความเสี่ยงที่มีหรือไม่ หรือมี Gap ในเรื่องใดบ้าง โดยประเมินใน 6 ด้าน คือ 1) กรอบการกำกับดูแล (Governance) 2) การระบุความเสี่ยง (Risk Identification) 3) การป้องกัน (Protection) 4) การเฝ้าระวังและตรวจจับ (Detection) 5) การตอบสนองต่อเหตุการณ์และการกู้คืน (Response and Recovery) และ 6) การบริหารความเสี่ยงด้านภัยคุกคามไซเบอร์ที่เกิดจากหน่วยงานภายนอก (Third party risk management) โดยระดับความพร้อมในการบริหารจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ (Maturity) แบ่งเป็น 3 ระดับ ได้แก่ Baseline Intermediate และ Advanced สอดคล้องกับระดับความเสี่ยงไซเบอร์ที่สถาบันการเงินมี ดังนี้

| ระดับความเสี่ยง | การบริหารจัดการความเสี่ยงทางไซเบอร์ |
|---|---|
| ต่ำ | สง. ควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ Baseline Maturity |
| ปานกลาง | สง. ควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ Baseline และ Intermediate Maturity |
| สูง | สง. ควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ Baseline Intermediate และ Advanced Maturity |

ทั้งนี้ ขอให้สถาบันการเงินประเมินความพร้อมในการรับมือภัยไซเบอร์ตามแนวทางดังกล่าวอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงเชิงโครงสร้างด้านระบบเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ ซึ่งกระทบต่อความเสี่ยงจากภัยคุกคามไซเบอร์ที่สถาบันการเงินเผชิญ โดยขอให้หน่วยงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) หน่วยงานกำกับการปฏิบัติตามหลักเกณฑ์ (Compliance) และหน่วยงานตรวจสอบภายใน (Internal Audit) ของสถาบันการเงินมีส่วนร่วมกำกับดูแลให้สถาบันการเงินทำการประเมินตามกรอบการประเมินความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework) พร้อมทั้งส่งผลประเมินดังกล่าวมายัง ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน เป็นประจำทุกปี ภายใน 30 วันนับจากวันที่ 31 ธันวาคมของปีที่ประเมิน และเมื่อธนาคารแห่งประเทศไทยร้องขอ

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายจาตุรงค์ จันทรังษ์)
ผู้ช่วยผู้ว่าการ สายกำกับสถาบันการเงิน
ผู้ว่าการแทน

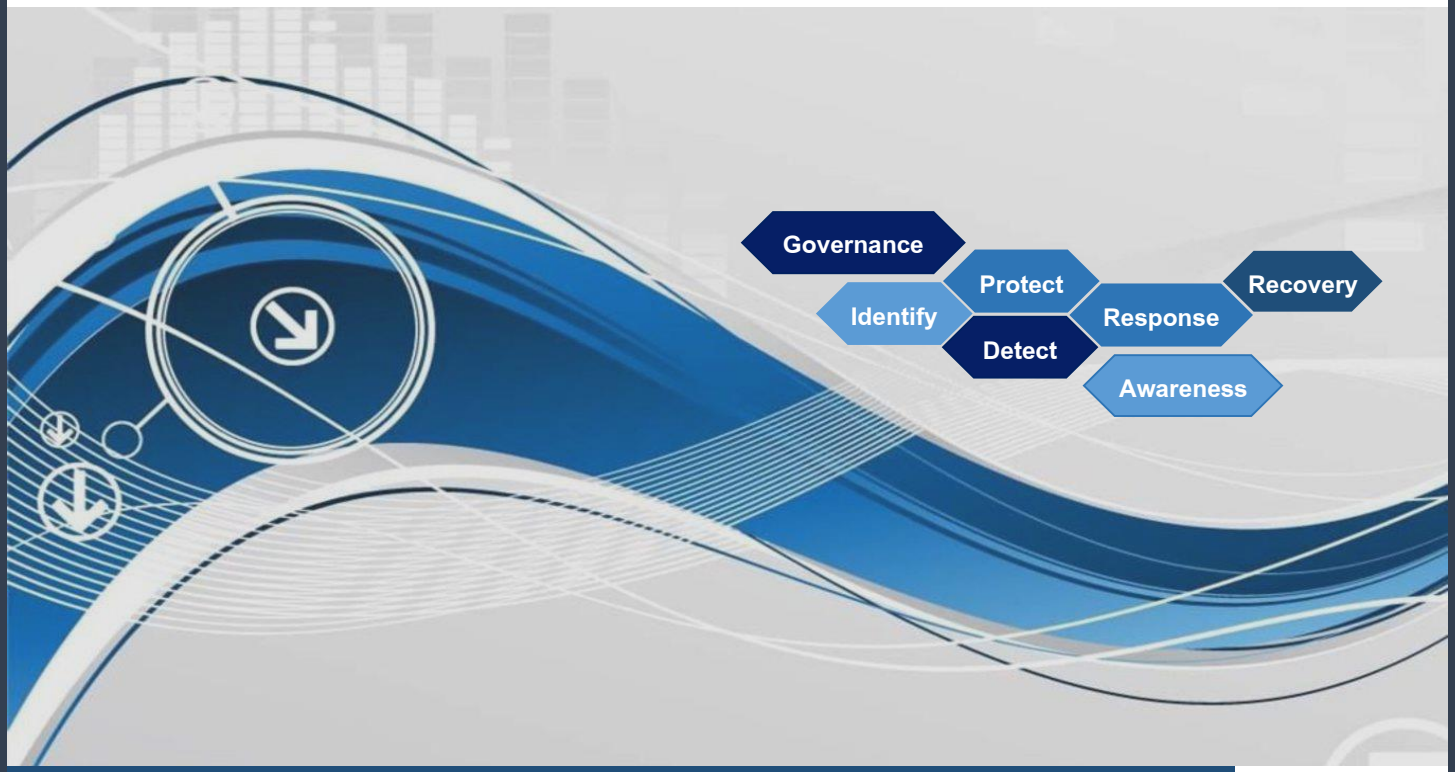
สิ่งที่ส่งมาด้วย กรอบการประเมินความพร้อมด้าน Cyber Resilience

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
โทรศัพท์ 0 2283 5827, 0 2283 6576
E-Mail ITSupervision@bot.or.th

หมายเหตุ [ ] ธนาคารจะจัดให้มีการประชุมชี้แจง ในวันที่ ..... ณ .....

[ X ] ไม่มีการประชุมชี้แจง

ธนาคารแห่งประเทศไทย




# กรอบการประเมินความพร้อมด้าน Cyber Resilience

ภายใต้หลักเกณฑ์การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) ของสถาบันการเงิน

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

## สารบัญ

## กรอบการประเมินความพร้อมด้าน Cyber Resilience

ปัจจุบันสถาบันการเงินใช้เทคโนโลยีและระบบเทคโนโลยีสารสนเทศ เป็นกลไกหลักในการขับเคลื่อนธุรกิจ ทำให้เผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) มากขึ้น สถาบันการเงินจึงควรมีการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ที่เข้มงวด รัดกุม และเพียงพอตามระดับความเสี่ยงที่สถาบันการเงินมี เพื่อให้มีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ ทั้งการวางกรอบการกำกับดูแล การบริหารจัดการความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือหรือเทคโนโลยี เพื่อลดผลกระทบต่อลูกค้า สถาบันการเงิน และต่อระบบโดยรวม

ธนาคารแห่งประเทศไทยจึงได้กำหนดกรอบการประเมินความพร้อมด้าน Cyber Resilience โดยอ้างอิงตามประกาศ ธปท. เรื่องหลักเกณฑ์การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) ของสถาบันการเงิน เพื่อให้สถาบันการเงิน (สง.)[1] ใช้เป็นแนวทางอ้างอิงในการประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment) และกำหนดแนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level) ให้สอดคล้องกับระดับความเสี่ยงตั้งต้นของตนเองโดยมีสาระสำคัญสรุปได้ดังนี้

**ส่วนที่ 1: <u>การประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment)</u>**

เพื่อให้ สง. ทราบถึงประเภทและระดับความเสี่ยงของตนเอง (risk profile) โดยพิจารณาจากปัจจัยความเสี่ยงพื้นฐานทางเทคโนโลยีสารสนเทศ 5 ด้านคือ

1. **เทคโนโลยีและการเชื่อมต่อ** เป็นปัจจัยเสี่ยงที่พิจารณาถึงประเภท ขอบเขต ขนาด และปริมาณการใช้เทคโนโลยีสารสนเทศในประเภทต่าง ๆ รวมถึงลักษณะการติดต่อสื่อสารหรือการเชื่อมต่อของระบบเทคโนโลยีสารสนเทศทั้งภายในและภายนอกองค์กรเพื่อสะท้อนถึงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศทั้งหมดของ สง. เช่น จำนวนการเชื่อมต่อแบบ Unsecured Protocol การใช้อุปกรณ์ที่กำลังจะหมดอายุการใช้งาน (End-of-Life) หรือสิ้นสุดการให้บริการ (End-of-Support) การใช้ Open Source Software หรือการใช้เทคโนโลยีใหม่ เป็นต้น ซึ่งอาจก่อให้เกิดความเสี่ยงตั้งต้นด้านไซเบอร์จากช่องโหว่ของเทคโนโลยีใหม่ที่ยังไม่เคยตรวจพบ เทคโนโลยีเก่าที่ล้าสมัย การเชื่อมต่อที่ไม่ปลอดภัย การทุจริตจากบุคคลภายนอก หรือการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และระบบงานไม่ทั่วถึงและรัดกุม
2. **ช่องทางการให้บริการ** เป็นปัจจัยเสี่ยงที่พิจารณาถึงประเภทและลักษณะของช่องทางการให้บริการผลิตภัณฑ์และการทำธุรกรรมทางการเงินของ สง. ที่มีการเชื่อมต่อกับระบบเครือข่ายภายนอก โดยเฉพาะเครือข่าย Internet เช่น Internet Banking, Mobile Banking หรือ Website ของ สง. เป็นต้น ซึ่งอาจก่อให้เกิดความเสี่ยงด้านไซเบอร์ในรูปแบบและระดับความรุนแรงที่แตกต่างกันไปตามช่องทาง อุปกรณ์ และเทคโนโลยีที่ใช้สำหรับช่องทางการให้บริการแต่ละช่องทาง
3. **ลักษณะผลิตภัณฑ์และการให้บริการ** เป็นปัจจัยเสี่ยงที่พิจารณาขอบเขตและปริมาณการให้บริการผลิตภัณฑ์ทางการเงิน ที่ต้องพึ่งพาระบบเครือข่ายทั้งภายในและภายนอก สง. ในการให้บริการ เช่น ผลิตภัณฑ์บัตร ธุรกรรมการโอนเงินแบบ Real Time Online เป็นต้น รวมถึงการให้บริการด้านเทคโนโลยีแก่องค์กรอื่นภายนอก สง.

[1] สถาบันการเงิน (สง.) ในกรอบการบริหารจัดการด้าน Cyber Resilience ฉบับนี้ หมายถึง ธนาคารพาณิชย์ สถาบันการเงินเฉพาะกิจ ซึ่งรวมถึงบริษัทหรือกลุ่มบริษัทด้านเทคโนโลยีสารสนเทศที่ สง. จัดตั้งขึ้นเพื่อทำหน้าที่บริหารจัดการด้านเทคโนโลยีสารสนเทศแทนหน่วยงานด้านเทคโนโลยีสารสนเทศของ สง. เอง และให้รวมถึงผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ โดยอนุโลมด้วย

ซึ่งลักษณะเฉพาะของผลิตภัณฑ์ทางการเงินแต่ละผลิตภัณฑ์ อาจก่อให้เกิดความเสี่ยงด้านไซเบอร์ในรูปแบบที่แตกต่างกันไป ซึ่งรวมถึงการทำ Social Engineering เพื่อขโมยข้อมูลทางการเงินของลูกค้าผู้ใช้บริการด้วย

**4. ลักษณะเฉพาะขององค์กร** เป็นปัจจัยเสี่ยงที่พิจารณาจากประเภท ที่ตั้ง และลักษณะเฉพาะในการดำเนินงานของ สง. ซึ่งก่อให้เกิดความเสี่ยงด้านไซเบอร์จากปัจจัยแวดล้อมที่แตกต่างกัน เช่น สภาพทางภูมิศาสตร์การเมือง การเปลี่ยนแปลงของสภาพแวดล้อมทางด้านเทคโนโลยีสารสนเทศ เป็นต้น ซึ่งรวมถึงการจ้างบริษัทผู้ให้บริการภายนอกรับผิดชอบดำเนินงานทางด้านเทคโนโลยีสารสนเทศแทน สง. ซึ่งอาจทำให้ สง. ตกเป็นเป้าหมายในการถูกโจมตีทางไซเบอร์จากคุณภาพของบุคลากรภายนอก สภาพสังคม ความขัดแย้ง และวัฒนธรรมองค์กรที่แตกต่างกันได้

**5. ประวัติการถูกคุกคามทางไซเบอร์** เป็นปัจจัยเสี่ยงที่พิจารณาจากประเภท และปริมาณที่ สง. ตกเป็นเป้าของการโจมตีทางไซเบอร์ในอดีต เช่น Phishing, Malware, Social Engineering หรือ DDoS เป็นต้น

ทั้งนี้ ระดับความเสี่ยงตั้งต้นของ สง. แต่ละแห่ง จะถูกแบ่งออกเป็น 3 ระดับตามลักษณะของปัจจัยเสี่ยงทั้ง 5 ด้าน ดังกล่าวข้างต้น ดังนี้

| ระดับความเสี่ยงตั้งต้น | ลักษณะของสถาบันการเงิน |
|---|---|
| ต่ำ | สง. มีกลยุทธ์การทำธุรกิจบนพื้นฐานของ Traditional Banking โดยมีผลิตภัณฑ์และการให้บริการธุรกรรมทางการเงินที่ไม่หลากหลาย และส่วนใหญ่ทำผ่านช่องทางเครือข่ายที่เป็นระบบปิด มีผลิตภัณฑ์และการให้บริการผ่านช่องทางอิเล็กทรอนิกส์หรือ Internet ในวงจำกัด และไม่เคยตกเป็นเป้าโจมตีทางไซเบอร์อย่างรุนแรงในอดีต |
| ปานกลาง | สง. มีกลยุทธ์การทำธุรกิจที่เน้น Electronic Banking ควบคู่ไปกับ Traditional Banking โดยมีผลิตภัณฑ์และการให้บริการทางการเงินที่หลากหลาย มีเครือข่ายที่เชื่อมโยงกับบุคคลภายนอกทั้ง สง. ผู้ให้บริการระบบการชำระเงิน คู่ค้า หรือผู้ให้บริการด้านเทคโนโลยีสารสนเทศอื่น ๆ ผ่านเครือข่ายที่เป็นระบบปิดและ Internet มากทั้งภายในและภายนอกประเทศ เริ่มมีการนำเทคโนโลยีใหม่ ๆ เช่น Cloud Computing มาใช้ มีการใช้ระบบเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอกจำนวนมาก และที่ผ่านมาเคยมีเหตุการณ์ผิดปกติทางไซเบอร์เกิดขึ้นอยู่เป็นระยะ ๆ |
| สูง | สง. มีกลยุทธ์การดำเนินธุรกิจทาง Electronic Banking ในเชิงรุก และครบวงจร เริ่มนำเทคโนโลยีใหม่ที่มีความซับซ้อนและหลากหลายมาใช้ในการบริหารจัดการโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ การพัฒนาผลิตภัณฑ์ และการให้บริการทางการเงินมากขึ้น มีการดำเนินธุรกิจที่ครอบคลุมในหลายประเทศ มีการใช้และให้บริการระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก สง. จำนวนมาก และมีแนวโน้มที่จะตกเป็นเป้าหมายของการถูกคุกคามทางไซเบอร์เพิ่มและรุนแรงขึ้นอย่างต่อเนื่อง |

## ส่วนที่ 2: แนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level)

การกำหนดแนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมีของ สง. ควรอ้างอิงตามระดับความเสี่ยงตั้งต้นของตนเอง เช่น สง. ที่มีความเสี่ยงตั้งต้นอยู่ในระดับสูง ควรมีแนวทางการบริหารจัดการความเสี่ยงที่เข้มงวด มีหน่วยงานหรือผู้รับผิดชอบในการบริหารจัดการความเสี่ยงโดยตรง และมีเครื่องมือที่ใช้ในการระบุ ประเมิน ติดตาม ลด ควบคุม และรายงานงานความเสี่ยงได้อย่างรวดเร็ว ทันกาล และเป็นอัตโนมัติ เป็นต้น ส่วน สง. ที่มีระดับความเสี่ยงปานกลางหรือต่ำ อาจมีแนวทางบริหารจัดการความเสี่ยงที่มีความเข้มงวดลดหลั่นกันไปตามความเหมาะสม ดังนี้

| ระดับความเสี่ยงตั้งต้น | มาตรการควบคุมที่พึงมี (Maturity Level) |
|---|---|
| ต่ำ | สง. ควรปฏิบัติได้ตามมาตรการที่กำหนดไว้สำหรับ Maturity Level ระดับ Baseline ที่ ธปท. กำหนดทุกข้อ |
| ปานกลาง | สง. ควรปฏิบัติได้ตามมาตรการที่กำหนดไว้สำหรับ Maturity Level ระดับ Baseline และระดับ Intermediate ที่ ธปท. กำหนดทุกข้อ |

| ระดับความเสี่ยงตั้งต้น | มาตรการควบคุมที่พึงมี (Maturity Level) |
|---|---|
| สูง | สง. ควรปฏิบัติได้ตามมาตรการที่กำหนดไว้สำหรับ Maturity Level ระดับ Baseline ระดับ Intermediate และระดับ Advanced ที่ ธปท. กำหนดทุกข้อ |

ทั้งนี้ แนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมีของแต่ละ Maturity Level คือ Baseline, Intermediate และ Advanced จะครอบคลุมการบริหารจัดการความเสี่ยงด้านไซเบอร์ของ สง. ใน 6 ด้านหลัก เพื่อให้มั่นใจได้ว่า สง. ทุกแห่งมีกระบวนการหรือมาตรการควบคุมดูแลความเสี่ยงด้านไซเบอร์ได้เหมาะสมกับขนาดและความซับซ้อนของธุรกิจ โครงสร้างพื้นฐาน ลักษณะการดำเนินงาน และปัจจัยเสี่ยงของตนเอง ดังนี้

**1. ธรรมาภิบาล (Governance)** เป็นแนวทางการกำกับดูแลด้าน Cyber Resilience ของคณะกรรมการ สง. คณะกรรมการชุดที่เกี่ยวข้อง และผู้บริหารระดับสูงของ สง. การกำหนดกลยุทธ์และนโยบายด้าน Cyber Resilience การบริหารจัดการความเสี่ยง การตรวจสอบภายใน และการจัดสรรและพัฒนาบุคลากร เพื่อให้ สง. มีกรอบและแนวทางที่ใช้ในการกำกับดูแล และบริหารจัดการความเสี่ยงในภาพรวมขององค์กรที่สอดคล้องและมีมาตรฐานเดียวกันสำหรับทุกๆ หน่วยธุรกิจ

**2. การระบุความเสี่ยง (Identification)** เป็นแนวทางที่ใช้ในการกำหนดขอบเขตและวิธีการในการประเมินความเสี่ยงด้านไซเบอร์ การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการเพิ่ม ลด โยกย้าย และการตั้งค่าอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และระบบงานที่เกี่ยวข้อง เพื่อให้ สง. ทราบ และสามารถระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศที่อาจก่อให้เกิดความเสี่ยง และสามารถบริหารจัดการเพื่อควบคุมและลดความเสี่ยงได้อย่างเหมาะสมและทันการณ์

**3. การป้องกันความเสี่ยง (Protection)** เป็นแนวทางการควบคุมและป้องกันความเสี่ยงของโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ โดยครอบคลุมระบบเครือข่าย อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และระบบงาน เช่น การตั้งค่าระบบงาน การเข้าถึงระบบงานและการจัดการสิทธิ์ การรักษาความมั่นคงปลอดภัยของข้อมูล การพัฒนาระบบงานที่มีความมั่นคงปลอดภัย การบริหารจัดการ Patch เพื่อให้ สง. มีกระบวนการ เครื่องมือ และวิธีการควบคุมหรือลดผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้อยู่ในระดับที่เหมาะสมกับความซับซ้อนในการดำเนินงานของตนเอง

**4. การตรวจจับความเสี่ยง (Detection)** เป็นแนวทางในการค้นหา ทดสอบ และบริหารจัดการช่องโหว่ทางด้านเทคโนโลยีสารสนเทศ เพื่อให้ สง. สามารถตรวจจับ วิเคราะห์ ติดตาม และแจ้งเตือนเหตุการณ์ผิดปกติทางไซเบอร์ให้แก่หน่วยงานหรือผู้รับผิดชอบรับทราบและกำหนดแนวทางในการดำเนินการแก้ไขในเบื้องต้นได้อย่างทันกาล

**5. การรับมือและฟื้นฟูความเสียหาย (Response and Recovery)** เป็นแนวทางในการบริหารจัดการการรับมือเหตุการณ์ผิดปกติทางไซเบอร์ เช่น การจัดทำและทดสอบแผนฉุกเฉิน การสืบสวนและวิเคราะห์สาเหตุการแก้ปัญหา และจัดทำรายงานเพื่อเสนอต่อคณะกรรมการ สง. และผู้บริหารระดับสูง เป็นต้น เพื่อให้ สง. สามารถตอบสนองและรับมือกับความเสี่ยงได้อย่างทันการณ์ รวมถึงมีมาตรการในการฟื้นฟูความเสียหายและป้องกันไม่ให้มีผลกระทบต่อการดำเนินงานและการให้บริการของ สง. อย่างมีนัยสำคัญ

**6. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management)** เป็นแนวทางในการบริหารจัดการบุคคลภายนอก การทำสัญญาจ้าง การประเมินความเหมาะสม การติดตามและประเมินผลการปฏิบัติงาน และการสอบทานผลการปฏิบัติงาน เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถปฏิบัติงานให้ สง. ได้ตามเป้าหมายและเงื่อนไขที่กำหนด โดยไม่ก่อให้เกิดความเสี่ยงด้านไซเบอร์จนส่งผลกระทบต่อการดำเนินงานและการให้บริการของ สง. อย่างมีนัยสำคัญ

**ส่วนที่ 1: การประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment)**

ความเสี่ยงตั้งต้นด้านไซเบอร์เป็นความเสี่ยงด้านไซเบอร์ที่ สง. เผชิญจากการดำเนินงานของ สง. โดยประเมินระดับความเสี่ยงจากปัจจัย 5 ด้าน คือ เทคโนโลยีและการเชื่อมต่อ ช่องทางการให้บริการ ลักษณะผลิตภัณฑ์และการให้บริการ ลักษณะเฉพาะขององค์กร และประวัติการถูกคุกคามจากภัยไซเบอร์ในอดีต และแบ่งผลการประเมินเป็น 3 ระดับ คือ ต่ำ ปานกลาง และสูง มีรายละเอียดการประเมิน ดังนี้

**1. เทคโนโลยีและการเชื่อมต่อ**

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 1.1 จำนวน Internet Service Provider (ISP) ที่เชื่อมต่อกับระบบเครือข่ายของธนาคาร | น้อยกว่า 2 ราย | 2 ราย | มากกว่า 2 ราย | | - การพิจารณา นับจำนวนผู้ให้บริการ ISP ในปัจจุบันที่ DC/DR จาก Network Diagram ทั้งนี้ ไม่รวมผู้ให้บริการประเภท Non-Public Network เช่น Leased Line, MPLS และ Dark Fiber เป็นต้น |
| 1.2 จำนวน Public IP Address ของ สง. ที่เชื่อมต่อเครือข่ายอินเทอร์เน็ต (ซึ่งรวมถึง Public IP ที่เชื่อมต่อระหว่างสาขาและระบบเครือข่ายหลักของ สง.) | น้อยกว่า 10 IP Addresses | 10-300 IP Addresses | มากกว่า 300 IP Addresses | | - การพิจารณา นับจำนวน IP Address |
| 1.3 จำนวนเครื่อง Server ที่ให้บริการแบบ Unsecured Protocol เช่น FTP, Telnet, HTTP ผ่านเครือข่ายอินเทอร์เน็ต | น้อยกว่า 2 เครื่อง/VMs | 2-3 เครื่อง/VMs | มากกว่า 3 เครื่อง/VMs | | - การพิจารณา นับจำนวนเครื่องหรือจำนวน VM ของ Internet Facing Server ในปัจจุบันที่ DC/DR ที่เปิด Unsecured Protocol/ Service ได้แก่ FTP, Telnet, HTTP |
| 1.4 จำนวน Public IP Addresses ของ สง. ที่ให้บริการแบบ Unsecured Protocol เช่น FTP, Telnet, HTTP ผ่านเครือข่ายอินเทอร์เน็ต | น้อยกว่า 2 IP Addresses | 2-10 IP Addresses | มากกว่า 10 IP Addresses | | |
| 1.5 ลักษณะระบบเครือข่ายไร้สายของ สง. ในการให้บริการแก่ผู้ใช้ภายใน สง. และบุคคลภายนอก | แยกระบบเครือข่ายออกจากกันทาง | แยกระบบเครือข่ายออกจากกันทาง | ใช้ระบบเครือข่ายร่วมกันทั้งผู้ใช้ภายใน สง. และบุคคลภายนอก | | |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| | Physical (เช่น แยก Access Point, ISP) | Logical (เช่น แยก VLAN) | | | |
| 1.6 จำนวนอุปกรณ์ส่วนตัวของพนักงานหรือของ สง. ที่ลงทะเบียนและสามารถเชื่อมต่อเข้าถึงเครือข่ายภายในหรือระบบงานภายในได้โดยผ่านมาจากเครือข่ายภายนอก | น้อยกว่า 100 เครื่อง | 100-2,000 เครื่อง | มากกว่า 2,000 เครื่อง | | - การพิจารณา นับจำนวนคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่เป็นของส่วนตัวของพนักงาน หรือของ สง. ที่สามารถเชื่อมต่อกับเครือข่ายภายใน สง. โดยเชื่อมต่อเข้ามาจากเครือข่ายภายนอก (ไม่นับการเชื่อมต่อผ่านเครือข่ายไร้สาย WiFi ที่ สง. ให้บริการ ซึ่งจะถูกนับในข้อ 1.8)<br>- เหตุผล การอนุญาตให้นำอุปกรณ์ส่วนตัวมาใช้จะเพิ่มโอกาสที่ข้อมูลจะรั่วไหลหรือมี Malware กระจายเข้าเครือข่ายได้มากขึ้น |
| 1.7 จากข้อ 1.6 ลักษณะการให้บริการที่สามารถเชื่อมต่อเข้าถึงเครือข่ายภายในหรือระบบงานภายในของ สง. ได้ | ไม่มี | เข้าถึงระบบงานทั่วไปหรือเพื่อใช้งาน Internet | เข้าถึงระบบงานสำคัญ | | - การพิจารณา นับจำนวนระบบงานสำคัญ (ตาม BIA หรือหลักเกณฑ์ที่เทียบเท่า ที่สูงสุด 2 ระดับแรก) |
| 1.8 ลักษณะการเข้าถึงเครือข่าย/ระบบงานของ สง. | เฉพาะเครื่องของ สง. สามารถเข้าถึงได้จากเครือข่ายมีสายเท่านั้น | เครื่องของ สง. และเครื่องที่ลงทะเบียนสามารถเข้าถึงได้จากเครือข่ายมีสายและไร้สาย (WiFi) | เครื่องที่ไม่ได้ลงทะเบียนสามารถเข้าถึงได้จาก Internet | | - การพิจารณา เช่น การใช้ Email App โดยใช้User/Password โดยไม่ต้องนำเครื่องมาลงทะเบียน หรือการเข้าถึง Email ผ่าน OWA หรือการเข้าถึง Cloud Email หรือการเข้าถึงระบบงานผ่าน F5 Web Portal และรวมถึงการเชื่อมต่อผ่านเครือข่ายไร้สาย WiFi ที่ สง. ให้บริการ |
| 1.9 จากข้อ 1.8 ลักษณะการให้บริการที่สามารถเชื่อมต่อกับเครือข่าย/ระบบงานของ สง. ได้ | ไม่มี | สามารถเข้าถึงได้เฉพาะระบบงานทั่วไปหรือเพื่อใช้งาน Internet | สามารถเข้าถึงระบบงานสำคัญ | | - การพิจารณา นับจำนวนระบบงานสำคัญ (ตาม BIA หรือหลักเกณฑ์ที่เทียบเท่า ที่สูงสุด 2 ระดับแรก) |
| 1.10 จำนวนองค์กรภายนอกที่มีการเชื่อมต่อกับเครือข่ายของ สง. | น้อยกว่า 10 แห่ง | 10-30 แห่ง | มากกว่า 30 แห่ง | | |
| 1.11 จำนวนบริษัทในเครือในประเทศที่มีการเชื่อมต่อกับเครือข่ายของ สง. | น้อยกว่า 2 แห่ง | 2-7 แห่ง | มากกว่า 7 แห่ง | | |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 1.12 จากข้อ 1.10 และ 1.11 ลักษณะการเชื่อมต่อเครือข่ายกับองค์กรภายนอก และบริษัทในเครือในประเทศ | Private Link เช่น Leased Line MPLS และมี VPN | Private Link เช่น Leased Line MPLS ที่ไม่มีการเข้ารหัส | ใช้ VPN ผ่าน Public Internet | | |
| 1.13 จำนวนองค์กรภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบงานภายในของ สง. | น้อยกว่า 5 แห่ง | 5-10 แห่ง | มากกว่า 10 แห่ง | | การพิจารณา<br>- นับเฉพาะกรณีที่มีองค์กรนั้นมีคนถือครองบัญชีผู้ใช้งานและสามาถเข้าถึงระบบงานภายใน สง. ได้<br>- **ไม่นับ** กรณีที่เป็นการเชื่อมต่อกันของระบบ เช่น แบบ Host-to-Host หรือการเชื่อมต่อผ่าน API<br>- **ไม่นับ** กรณีที่ลูกค้าหรือคู่ค้าเข้าถึงเพื่อรับส่งข้อมูล<br>- **นับ** ที่จำนวนหน่วยงานที่มีการเชื่อมต่อเครือข่ายในข้อ 1.10 |
| 1.14 ลักษณะการเข้าถึงระบบงานภายใน สง. จากองค์กรภายนอก | On-site | VPN over Leased Line | VPN over Internet | | |
| 1.15 จำนวนระบบงานสำคัญที่ สง. พัฒนาขึ้นเองหรือ สง. ปรับแต่ง (Customize) จากระบบงานของ Vendor และเชื่อมต่อกับระบบภายใน สง. | น้อยกว่า 10 ระบบ | 10-50 ระบบ | มากกว่า 50 ระบบ | | - การพิจารณา นับจำนวนระบบงานสำคัญ (ตาม BIA หรือหลักเกณฑ์ที่เทียบเท่า ที่สูงสุด 2 ระดับแรก) ที่ใช้งานในปัจจุบัน ทั้งที่ DC/DR หากระบบงานใดมีการติดตั้งทั้งที่ DC และ DR ให้นับเพียง 1 ระบบ<br>- เหตุผล Application ที่มีการดัดแปลง อาจมีช่องโหว่หรือจุดอ่อนแฝงอยู่ทั้งโดยตั้งใจและไม่ตั้งใจ |
| 1.16 จำนวนระบบงานสำคัญที่ Vendor พัฒนาให้และเชื่อมต่อกับระบบภายใน สง. | น้อยกว่า 3 ระบบ | 3-20 ระบบ | มากกว่า 20 ระบบ | | - การพิจารณา นับจำนวนระบบงานสำคัญ (ตาม BIA หรือหลักเกณฑ์ที่เทียบเท่า ที่สูงสุด 2 ระดับแรก) ที่ใช้งานในปัจจุบัน ทั้งที่ DC/DR หากระบบงานใดมีการติดตั้งทั้งที่ DC และ DR ให้นับเพียง 1 ระบบ |
| 1.17 จำนวนระบบปฏิบัติการ (Operating System : OS) และ Software ของระบบงานสำคัญที่ End-of-Life | น้อยกว่า 2 OS/Software | 2-10 OS/Software | มากกว่า 10 OS/Software | | - การพิจารณา นับ OS เช่น Windows XP, Windows Server 2003, AIX 5.0<br>- นับ Software เช่น Office 2007 |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| | | | | | - นับเฉพาะ Major Version เช่น Windows Server 2008 และ 2008 R2 ให้ถือเป็นตัวเดียวกัน<br>- ระบบงานสำคัญ (ตาม BIA หรือหลักเกณฑ์ที่เทียบเท่าที่สูงสุด 2 ระดับแรก) ที่ใช้งานในปัจจุบัน ทั้งที่ DC และ/หรือ DR (ดูตามการประมวลผลที่ Active อยู่)<br>- เช่น กรณีที่ 1 ระบบงานสำคัญ A มีการประมวลผลเฉพาะที่ DC แบบ Active/Standby ให้นับจำนวน OS และ Software ของเครื่องหรือ VM ที่ประมวลผลระบบงานดังกล่าวเฉพาะที่ DC<br>- กรณีที่ 2 ระบบงานสำคัญ B มีการประมวลผลทั้ง DC และ DR แบบ Active/Active ให้นับจำนวน OS และ Software ของเครื่องหรือ VM ที่ประมวลผลระบบงานดังกล่าวทั้งที่ DC และ DR |
| 1.18 จากข้อ 1.17 จำนวนเครื่อง Server ที่ใช้ระบบปฏิบัติการ (Operation System : OS) และ Software ของระบบงานสำคัญที่ End-of-Life | น้อยกว่า 20 เครื่อง/VMs | 20-200 เครื่อง/VMs | มากกว่า 200 เครื่อง/VMs | | - การพิจารณา นับเครื่อง Server ทั้งที่ DC และ DR โดย<br>- กรณีที่1 เป็น Physical Server 1 เครื่องและมี 1 OS ให้นับเป็น 1 เครื่อง<br>- กรณีที่2 เป็น Physical Server 1 เครื่องและทำ Virtualize เช่น VM หรือ LPAR ออกมาเป็น 10 VMs ให้นับเป็น 10 เครื่อง<br>- และโดยกรณีที่ 1 เครื่อง หรือ 1 VM มี OS และ Software ของระบบงานสำคัญที่ End-of-Life มากกว่า 1 ขึ้นไป ให้นับเป็น 1 เครื่อง หรือ 1 VM |
| 1.19 จำนวน Software ประเภท Open Source รองรับระบบงานสำคัญที่ไม่มีการสนับสนุนจาก Vendor (End-of-Support) | น้อยกว่า 5 Software | 5-10 Software | มากกว่า 10 Software | | - การพิจารณา นับจำนวน Software ที่ใช้งานในปัจจุบันที่ใช้ Open Source เช่น นับ Ubuntu Linux, นับ NginX เป็นต้น โดยแยกตาม version เช่น สง. มีการใช้ Ubuntu |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| | | | | | 14.10 และ Ubuntu 15.04 ที่ไม่มีการ support จาก vendor ให้นับเป็น 2 Software<br>- เหตุผล โดยทั่วไป Open Source Software มีจุดอ่อนที่ไม่ได้เปิดเผยมากกว่า และมีการออก Patch เพื่อแก้ไขช้ากว่า Commercial Software |
| 1.20 จำนวนเครื่อง Server ที่ใช้ Software ประเภท Open Source รองรับระบบงานสำคัญที่ไม่มีการสนับสนุนจาก Vendor | น้อยกว่า 5 เครื่อง | 5-40 เครื่อง | มากกว่า 40 เครื่อง | | - การพิจารณา นับจำนวนเครื่องที่ใช้ Open Source Software ที่รองรับหรือทำงานร่วมกับระบบงานสำคัญ (ตาม BIA หรือหลักเกณฑ์ที่เทียบเท่า ที่สูงสุด 2 ระดับแรก) |
| 1.21 จำนวนอุปกรณ์เครือข่าย ได้แก่ Router, Switch, Firewall, IPS/IDS หรืออุปกรณ์ที่เทียบเท่า | น้อยกว่า 400 เครื่อง | 400-4,000 เครื่อง | มากกว่า 4,000 เครื่อง | | - การพิจารณา นับจำนวนเครื่องที่ใช้งานในปัจจุบัน (รวมอุปกรณ์เช่าซื้อ) รวมถึงอุปกรณ์ที่สาขาทั้งในและต่างประเทศ ตู้ ATM และ Booth Exchange ด้วย ยกเว้นอุปกรณ์ประเภท Unmanageable Device (ไม่มี OS หรือไม่มี Configuration Menu) เช่น Hub, Modem บางประเภท เป็นต้น<br>- เหตุผล อุปกรณ์เครือข่ายที่มีการตั้งค่าไม่ถูกต้องหรือใช้ Software ที่มีจุดอ่อน จะเป็นช่องทางให้ถูกโจมตีได้ง่าย และหากมีจำนวนมาก จะยากในการควบคุมการตั้งค่าหรือปรับปรุงให้มีมาตรฐานเดียวกัน |
| 1.22 จำนวนเครื่องคอมพิวเตอร์ (End-Points) ที่ใช้ OS Windows | น้อยกว่า 3,000 เครื่อง | 3,000-23,000 เครื่อง | มากกว่า 23,000 เครื่อง | | - การพิจารณา นับจำนวนเครื่อง เช่น PC, Notebook, Tablet เป็นต้น<br>- เหตุผล Windows OS มีโอกาสติด Malware และอาจใช้เป็นตัวกระจาย Malware ไปยังระบบอื่นๆ มากกว่า OS อื่น |
| 1.23 การใช้เทคโนโลยี Cloud Computing | ไม่มีการใช้ | ใช้เฉพาะ Private Cloud | ใช้ Public หรือ Hybrid Cloud | | |

## 2. ช่องทางการให้บริการ

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 2.1 รูปแบบการให้บริการผ่าน Website ของ สง. | ไม่มีการให้บริการผ่าน Website | ให้บริการข้อมูลเพียงอย่างเดียว | ให้บริการทำธุรกรรมทางการเงินทั้งลูกค้าบุคคลและ/หรือลูกค้าองค์กร | | - เหตุผล การให้บริการ Online ผ่าน Website ที่หลากหลายจะมีความเสี่ยงมากกว่า |
| 2.2 จำนวน Domain และ Subdomain Website ของ สง. ที่สามารถเข้าถึงได้ผ่านเครือข่าย Internet | 7 Domains | 7-45 Domains | มากกว่า 45 Domains | | - การพิจารณา นับจาก Domain หรือ Web Address ที่ สง. มีทั้งหมด (รวม subdomain ย่อย) เช่น นับ https://www.abcbank.com และ https://online.abcbank.com รวมเป็น 2 domain |
| 2.3 รูปแบบการให้บริการผ่าน Mobile Application | ไม่มีการให้บริการผ่าน Mobile Application | ให้บริการข้อมูลที่ไม่ใช่ข้อมูลทางบัญชีของลูกค้า | ให้บริการข้อมูลทางบัญชี หรือทำธุรกรรมทางการเงินทั้งลูกค้าบุคคลและ/หรือลูกค้าองค์กร | | |
| 2.4 รูปแบบการให้บริการผ่าน Social Media หรือ Instant Messaging | ไม่มีการให้บริการ | ให้บริการประชาสัมพันธ์และ/หรือสื่อสารกับลูกค้า | ให้บริการทำธุรกรรมโอนเงินหรืออื่นๆ ได้ | | - การสื่อสารกับลูกค้า เช่น LINE Official Account<br>- การทำธุรกรรมอื่นๆ เช่น สอบถามยอดเงินบัตรเครดิต |
| 2.5 จำนวนเครื่องที่ให้บริการอัตโนมัติ เช่น ATM / CDM / VTM / Passbook Update | น้อยกว่า 50 เครื่อง | 50-8,000 เครื่อง | มากกว่า 8,000 เครื่อง | | - การพิจารณา นับเฉพาะตู้ ATM / CDM / VTM / Passbook Update ของ สง. ที่ใช้งานในปัจจุบัน |
| 2.6 จำนวนผู้ให้บริการโครงข่ายสื่อสารของตู้ ATM / CDM / VTM / Passbook Update | น้อยกว่า 3 ราย | 3-5 ราย | มากกว่า 5 ราย | | - การพิจารณา ให้นับจำนวน Vendor ที่ให้บริการโครงข่ายสื่อสารทั้งมีสาย (เช่น True, TOT, UIH) และไร้สาย (AIS, DTAC) สำหรับตู้ ATM / CDM / VTM / Passbook Update |
| 2.7 ลักษณะการเชื่อมต่อเครือข่ายของเครื่องที่ให้บริการอัตโนมัติ เช่น | | ใช้เฉพาะเครือข่ายของสาขา | ใช้เครือข่าย Internet | | |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| ATM / CDM / VTM / Passbook Update | | | | | |
| 2.8 การบำรุงรักษาตู้ ATM/CDM (เช่น Patch, OS, Whitelisting, Hardening, Key Management เป็นต้น) | ใช้บริการ Vendor น้อยกว่า 2 ราย | ใช้บริการ Vendor 2-3 ราย | ใช้บริการ Vendor มากกว่า 3 ราย | | - การพิจารณา ให้นับจำนวนราย Vendor หรือ Subcontractors ที่รับผิดชอบบำรุงรักษาตู้ ATM/CDM (มีสิทธิ์ในการเข้าถึงระบบ) เช่น Patch, OS, Whitelisting, Hardening, Key Management เป็นต้น แต่ไม่นับรวมการเติมเงินและทำความสะอาดตู้ |
| 2.9 จำนวนเครื่อง EDC (รวม Mobile EDC) ของ สง. และอุปกรณ์ EDC สำหรับเชื่อมต่อกับ Smartphone | น้อยกว่า 800 เครื่อง | 800-40,000 เครื่อง | มากกว่า 40,000 เครื่อง | | - การพิจารณา นับเฉพาะเครื่อง EDC (รวม Mobile EDC) ของ สง. และอุปกรณ์ EDC สำหรับเชื่อมต่อกับ Smartphone |
| 2.10 จำนวนคู่ค้าที่ สง. ให้บริการ Payment Gateway (เช่น ร้านค้าออนไลน์ เป็นต้น) | น้อยกว่า 50 ราย | 50-500 ราย | มากกว่า 500 ราย | | - การพิจารณา ให้นับร้านค้าที่ สง. ให้บริการ Payment Gateway (จุดชำระเงินของร้านค้าออนไลน์ เช่น Agoda หรือ Lazada เป็นต้น) ในปัจจุบัน<br>- เหตุผล จำนวนคู่ค้ามีผลต่อความเสี่ยงที่ สง. อาจดูแลได้ไม่ทั่วถึง เช่น คู่ค้าบางรายอาจใช้ระบบ Payment Gateway ของ สง.เป็นช่องทางทำทุจริตที่เกี่ยวข้องกับบัตร Credit/Debit ได้ |

## 3. ลักษณะผลิตภัณฑ์และการให้บริการ

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 3.1 จำนวนการให้บริการบัตร ได้แก่ บัตร ATM บัตรเดบิต บัตรเครดิต บัตร Virtual Debit/Credit Card และบัตรกดเงินสดอื่นๆ | น้อยกว่า 500,000 ใบ | 500,000-13,000,000 ใบ | มากกว่า 13,000,000 ใบ | | - การพิจารณา นับจำนวนบัตรทั้งหมด (รวม Fleet Card, Virtual Debit/Credit Card) ที่มีในปัจจุบัน เฉพาะที่ สง. เป็นผู้ออกบัตรเอง ไม่รวมบัตรที่ออกโดยบริษัทในเครือและไม่รวมบัตรเติมเงิน |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| | | | | | - เหตุผล จำนวนบัตรมากจะเพิ่มความเสี่ยงจากการถูก Skimming และ MITMA ผ่านธุรกรรม e-Commerce มากขึ้น |
| 3.2 จำนวนบัญชี E-Wallet | น้อยกว่า 10,000 บัญชี | 10,000-20,000 บัญชี | มากกว่า 20,000 บัญชี | | - การพิจารณา ให้นับจำนวนบัญชี E-Wallet ของ สง. หรือที่ผูกกับบัญชีของ สง.<br>- เหตุผล จำนวนบัญชี e-Wallet มากขึ้นยิ่งเพิ่มความเสี่ยงด้านไซเบอร์ จากการโดน Hack มากขึ้น |
| 3.3 จำนวนบัญชีเงินฝากที่มีการเชื่อมต่อร่วมกับบริการ E-Wallet ของ 3rd Party | ไม่มี | 1-10,000 บัญชี | มากกว่า 10,000 บัญชี | | - เช่น Beats Banking, LINE Pay (ผูกถาวร), mPay Wallet แต่ไม่นับกรณีที่ลูกค้านำไปผูกกับ E-Wallet เอง |
| 3.4 จำนวนผู้ใช้บริการ Internet Banking | น้อยกว่า 10,000 ราย | 10,000-2,000,000 ราย | มากกว่า 2,000,000 ราย | | - การพิจารณา ให้นับจำนวน Users ที่มีในปัจจุบัน ทั้ง Retail และ Corporate<br>- เหตุผล จำนวนผู้ใช้บริการมากจะเพิ่มความเสี่ยงที่เกิดกับ Web และ Mobile เช่น Phishing Web, Phishing Mobile Application, Web Defacing, Malware เป็นต้น |
| 3.5 จำนวนธุรกรรมการโอนเงินรายย่อยและ Corporate เฉลี่ยต่อเดือนผ่าน Internet Banking ในรอบ 12 เดือนที่ผ่านมา | ต่ำกว่า 20,000 รายการ | 20,000-2,000,000 รายการ | มากกว่า 2,000,000 รายการ | | - การพิจารณา ให้นับจำนวนธุรกรรมสะสมในรอบ 12 เดือนแล้วหารด้วย 12<br>- เหตุผล จำนวนธุรกรรมยิ่งมาก ยิ่งมีความเสี่ยงจาก MITMA มากขึ้น |
| 3.6 จำนวนผู้ใช้บริการ Mobile Banking | น้อยกว่า 20,000 ราย | 20,000-3,000,000 ราย | มากกว่า 3,000,000 ราย | | - การพิจารณา ให้นับจำนวน Users ที่มีในปัจจุบัน ทั้ง Retail และ Corporate |
| 3.7 จำนวนธุรกรรมการโอนเงินรายย่อยและ Corporate เฉลี่ยต่อเดือนผ่าน Mobile Banking ในรอบ 12 เดือนที่ผ่านมา | ต่ำกว่า 10,000 รายการ | 10,000-2,000,000 รายการ | มากกว่า 2,000,000 รายการ | | - การพิจารณา ให้นับจำนวนธุรกรรมสะสมในรอบ 12 เดือนแล้วหารด้วย 12<br>- เหตุผล จำนวนธุรกรรมยิ่งมาก ยิ่งมีความเสี่ยงจาก MITMA มากขึ้น |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 3.8 การให้บริการผลิตภัณฑ์การเงินอื่นๆ ผ่าน Website/Mobile Application (นอกเหนือผลิตภัณฑ์หลักของ สง.) | มีเฉพาะผลิตภัณฑ์ของ สง. เท่านั้น | มีผลิตภัณฑ์อื่นๆ ของบริษัทในเครือของ สง. | มีผลิตภัณฑ์อื่นๆ นอกกลุ่มของ สง. | | - นับผลิตภัณฑ์ในเครือ เช่น การลงทุน การประกันภัย เป็นต้น<br>- ยกเว้นผลิตภัณฑ์ที่ธนาคารได้ License และดำเนินการเอง |
| 3.9 จำนวนเทคโนโลยีที่ สง. นำมาใช้เป็นครั้งแรกของ สง. ในรอบ 12 เดือน | ไม่มี | 1-2 เทคโนโลยี | มากกว่า 2 เทคโนโลยี | | - การพิจารณา ตัวอย่างของเทคโนโลยี เช่น Blockchain, AI/ML, Biometric, Cloud Computing เป็นต้น<br>- ให้นับทั้งกรณีที่ สง. ทำ/ใช้เอง และกรณีที่บริษัทในเครือที่เป็น FinTech นำมาทำ/ใช้<br>- เหตุผล เทคโนโลยีใหม่อาจมีช่องโหว่หรือจุดบกพร่องที่ยังไม่ค้นพบและอาจถูกใช้เป็นช่องทางโจมตีทางไซเบอร์ได้ รวมทั้งการนำเทคโนโลยีมาใช้เป็นครั้งแรกอาจทำให้ สง. ตระหนักถึงความเสี่ยงทางไซเบอร์ได้ไม่ครอบคลุมเพียงพอ |

## 4. ลักษณะเฉพาะขององค์กร

* กรณี สง. แยกงานด้าน IT โดย Outsource ให้บริษัทในเครือที่ สง. ถือหุ้น 100% ให้ประเมินด้วยเสมือนเป็นฝ่ายงาน IT ของ สง.

* Privileged ID หมายถึงสิทธิ์สูงสุดของการเข้าระบบงาน เช่น ระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล อุปกรณ์เครือข่าย เป็นต้น ปกติการเบิกใช้สิทธิ์ดังกล่าวเฉพาะเมื่อมีความจำเป็น

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 4.1 จำนวนสาขาหรือบริษัทในเครือที่อยู่ในต่างประเทศและมีการเชื่อมต่อโดยตรงกับระบบเครือข่ายของสำนักงานใหญ่ | น้อยกว่า 4 แห่ง | 4-12 แห่ง | มากกว่า 12 แห่ง | | - การพิจารณา นับจำนวนสาขาหรือบริษัทในเครือที่อยู่ในต่างประเทศและมีการเชื่อมต่อโดยตรงกับระบบเครือข่ายของสำนักงานใหญ่<br>- เหตุผล แต่ละประเทศอาจมีกฎเกณฑ์จากผู้กำกับดูแลและสภาพแวดล้อมที่มีความเสี่ยงด้านไซเบอร์ต่างกัน เช่น รัสเซีย จีน ประเทศโซนยุโรป เป็นต้น ส่งผลให้ความเสี่ยงแตกต่างกัน |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 4.2 จำนวนองค์กรภายนอก (รวมบริษัทในเครือในประเทศ) ที่ สง. รับให้บริการด้านระบบ IT (IT Insourcing) | น้อยกว่า 2 ราย | 2-8 ราย | มากกว่า 8 ราย | | - การพิจารณา ให้นับจำนวนบุคคลภายนอก (รวมบริษัทในเครือ) ที่ สง. มีการดูแลระบบ IT ให้ หรือที่ สง. มีการเชื่อมโยงระบบงานดังกล่าว<br>- เหตุผล การเชื่อมโยงระบบงานสำคัญกัน จะเพิ่มความเสี่ยงกรณีที่บริษัทในเครือโดนโจมตีสำเร็จไปแล้ว |
| 4.3 จำนวนบริการด้านเทคโนโลยีสารสนเทศที่ สง. ใช้บริการจากผู้ให้บริการภายนอก | น้อยกว่า 8 ราย | 8-40 ราย | มากกว่า 40 ราย | | - การพิจารณา ให้นับทุกรายที่ใช้บริการตามรายงาน IT Outsource ของ สง. |
| 4.4 จำนวนผู้ให้บริการ Web Hosting ที่ สง. ใช้บริการในปัจจุบัน | น้อยกว่า 2 ราย | 2 ราย | มากกว่า 2 ราย | | |
| 4.5 อัตรากำลังตามโครงสร้างของ สง. (ไม่รวมพนักงาน Outsource/ IT Outsource) | ต่ำกว่า 1,000 คน | 1,000-10,000 คน | มากกว่า 10,000 คน | | - การพิจารณา นับตามจำนวนอัตรากำลังที่มีอยู่ในปัจจุบันทั้งหมด ถึงแม้ในบางอัตราจะยังไม่มีการจ้างพนักงานก็ตาม |
| 4.6 สัดส่วนจำนวนพนักงานในสายงานด้าน IT ของ สง. ที่ลาออกในระยะ 12 เดือนที่ผ่านมา | น้อยกว่า 2 % | 2-8 % | มากกว่า 8 % | | - การพิจารณา นับเป็นจำนวนพนักงาน IT ที่ลาออกในรอบ 12 เดือนที่ผ่านมา หารด้วยจำนวนอัตรากำลังพนักงานด้าน IT (ไม่รวมพนักงาน Outsource/IT Outsource)<br>- เหตุผล การ Turnover สูง อาจทำให้การจัดการสิทธิ์ การรักษาความลับข้อมูล และการสร้าง Awareness ทำได้ไม่ครบถ้วน |
| 4.7 สัดส่วนจำนวนพนักงานด้าน IT ที่มีสิทธิ์ Privileged ID ที่ลาออกในระยะ 12 เดือนที่ผ่านมา | น้อยกว่า 1 % | 1-2 % | มากกว่า 2 % | | - การพิจารณา นับเป็นจำนวนพนักงานที่มีสิทธิ์ Priviledge เช่น System Administrator ที่ลาออกในรอบ 12 เดือนที่ผ่านมา หารด้วยจำนวนอัตรากำลังพนักงานด้าน IT ที่มีสิทธิ์ Privileged ID |
| 4.8 จำนวนพนักงาน Outsource/ IT Outsource และ Banking Agent ที่มีสิทธิ์เข้าถึงระบบงานของ สง. | ต่ำกว่า 100 คน | 100-2,000 คน | มากกว่า 2,000 คน | | - การพิจารณา นับพนักงานทั้งที่ทำงานที่ สง. และที่ทำงานแบบ Remote |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 4.9 สัดส่วนจำนวน User PID ที่ให้แก่พนักงาน Outsource หรือบุคคลภายนอกใช้งานต่อ User PID ทั้งหมดของธนาคารในรอบระยะ 12 เดือน | น้อยกว่า 1 % | 1-10 % | มากกว่า 10 % | | - การพิจารณา นับ User PID ที่มอบให้แก่พนักงาน Outsource หรือบุคคลภายนอกใช้งานในระยะ 12 เดือนที่ผ่านมา เช่น ธนาคารให้สิทธิ User PID "root-A" ให้แก่พนักงาน Outsource หรือบุคคลภายนอกใช้งานช่วงเดือนมกราคม และสิงหาคม และมอบ User PID "root-B" ให้แก่พนักงาน Outsource หรือบุคคลภายนอกใช้งานทั้ง 12 เดือน ให้นับเป็น 2 User PID และหารด้วยจำนวน User PID ทั้งหมดของธนาคาร |

## 5. ประวัติการถูกคุกคามทางไซเบอร์

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| 5.1 จำนวนเหตุการณ์ Social Engineering | น้อยกว่า 10 ครั้ง | 10-50 ครั้ง | มากกว่า 50 ครั้ง | | - การพิจารณา ให้นับจำนวนครั้งที่เกิด โดยนับทั้งที่มีความเสียหายและไม่มีความเสียหายที่เกิดกับพนักงานภายในและลูกค้าของธนาคารที่พบในรอบ 12 เดือนที่ผ่านมา โดยนับจาก IT / Security Incident Report |
| 5.2 จำนวนเหตุการณ์ Phishing Website / Mobile Application | น้อยกว่า 10 ครั้ง | 10-30 ครั้ง | มากกว่า 30 ครั้ง | | - การพิจารณา ให้นับตามจำนวนครั้งที่เกิด โดยนับทั้งทั้งที่มีความเสียหายและไม่มีความเสียหาย เช่น กรณีที่มีการพบ 1 Website และทำการปิดไปแล้ว และมีการเกิดขึ้นใหม่อีกครั้ง ให้นับเป็น 2 ครั้ง หรือกรณีที่มีการเจอ 2 Websites ในคราวเดียวกัน และทำการปิดไปแล้ว และมีการเกิดขึ้นใหม่อีก 2 Websites ให้นับเป็น 4 ครั้ง โดยนับจากโปรแกรมตรวจจับ |
| 5.3 จำนวนเหตุการณ์ SQL Injection, XSS, CSRF | น้อยกว่า 1,000,000 ครั้ง | 1,000,000-2,000,000 ครั้ง | มากกว่า 2,000,000 ครั้ง | | - การพิจารณา ให้นับจำนวนครั้งที่เกิดกับระบบ Internet / Mobile Banking ที่พบในรอบ 12 เดือนที่ผ่านมา โดยนับทั้งที่มีความเสียหายและไม่มีความเสียหาย โดยนับจาก |

| ปัจจัย | ระดับความเสี่ยง | | | ผลการประเมิน | การพิจารณา / เหตุผลประกอบ |
|---|---|---|---|---|---|
| | ต่ำ | ปานกลาง | สูง | | |
| | | | | | Log ของอุปกรณ์ เช่น WAF, NGFW และ Firewall ที่ทำงานในระดับ Application Layer |
| 5.4 จำนวนเหตุการณ์ DDoS | น้อยกว่า 10,000 ครั้ง | 10,000-50,000 ครั้ง | มากกว่า 50,000 ครั้ง | | - การพิจารณา ให้นับจำนวนครั้งที่มี Bandwidth เกิน Threshold ที่ สง. กำหนดไว้ หากเกินติดต่อกันเป็นระยะเวลานาน ให้นับเป็น 1 ครั้ง ดูจากข้อมูลในรอบ 12 เดือนที่ผ่านมา โดยนับทั้งที่มีความเสียหายและไม่มีความเสียหาย โดยนับจากข้อมูลของ DDoS Protection Service Provider |
| 5.5 จำนวนเหตุการณ์ Malware | น้อยกว่า 5,000 ครั้ง | 5,000-50,000 ครั้ง | มากกว่า 50,000 ครั้ง | | - การพิจารณา ให้นับจำนวนครั้งที่ตรวจพบ Malware ในรอบ 12 เดือนที่ผ่านมา โดยนับทั้งที่มีความเสียหายและไม่มีความเสียหาย โดยนับจากข้อมูลระบบ Anti-Malware |
| 5.6 จำนวนเหตุการณ์ Data Breach | ไม่มี | 1-2 | มากกว่า 2 ครั้ง | | - การพิจารณา นับตามจำนวนครั้งที่เกิดภายใน 12 เดือน ทั้งในกรณีที่ข้อมูลรั่วไหลจาก Cyber attack หรือจากการทุจริตหรือความผิดพลาดของระบบ กระบวนการหรือพนักงานภายในขององค์กร โดยอาจนับจาก IT / Security Incident Report |

## สรุปผลการประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment)

* **ระดับความเสี่ยงของแต่ละปัจจัยเสี่ยง** คิดจากผลที่ได้จากการประเมินระดับความเสี่ยงที่มีจำนวนมากที่สุด (จำนวนผลการประเมิน (ในระดับ ต่ำ ปานกลาง สูง) ของข้อย่อยในแต่ละปัจจัยเสี่ยง เช่น ในปัจจัยเสี่ยงข้อ 1. เทคโนโลยีและการเชื่อมต่อมีผลการประเมินในระดับต่ำ 8 ข้อ / ปานกลาง 10 ข้อ / สูง 5 ข้อ จะได้ระดับความเสี่ยงของปัจจัยเสี่ยงดังกล่าวในระดับปานกลาง

* **ความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment)** คิดจากผลที่ได้จากประเมินปัจจัยเสี่ยงทั้ง 5 ปัจจัยเสี่ยงที่มีจำนวนมากที่สุด (จำนวนผลการประเมิน (ต่ำ ปานกลาง สูง) ของแต่ละปัจจัยเสี่ยงข้อ 1-5 เช่น ปัจจัยเสี่ยงข้อ 1 มีระดับความเสี่ยงสูง ปัจจัยเสี่ยงข้อ 2 มีระดับความเสี่ยงปานกลาง ปัจจัยเสี่ยงข้อ 3 มีระดับความเสี่ยงสูง ปัจจัยเสี่ยงข้อ 4 มีระดับความเสี่ยงสูง ปัจจัยเสี่ยงข้อ 5 มีระดับความเสี่ยงต่ำ ดังนั้นความเสี่ยง **Cyber Inherent Risk Assessment อยู่ในระดับสูง**

ในกรณีที่จำนวนผลประเมินระดับความเสี่ยงมีจำนวนเท่ากัน ให้กำหนดความเสี่ยงตั้งต้นด้านไซเบอร์ตามระดับความเสี่ยงที่สูงกว่า เช่น จำนวนผลการประเมินปัจจัยเสี่ยงมีระดับความเสี่ยงสูง 1 ปัจจัย ระดับความเสี่ยงปานกลาง 2 ปัจจัย ระดับความเสี่ยงต่ำ 2 ปัจจัย ดังนั้น ความเสี่ยง **Cyber Inherent Risk Assessment อยู่ในระดับปานกลาง**

| ปัจจัยเสี่ยง | ระดับความเสี่ยง | เหตุผลประกอบ | ความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment) |
|---|---|---|---|
| **1. เทคโนโลยีและการเชื่อมต่อ** | *(ต่ำ ปานกลาง สูง)* | | |
| **2. ช่องทางการให้บริการ** | *(ต่ำ ปานกลาง สูง)* | | |
| **3. ลักษณะผลิตภัณฑ์และการให้บริการ** | *(ต่ำ ปานกลาง สูง)* | | *(ต่ำ ปานกลาง สูง)* |
| **4. ลักษณะเฉพาะขององค์กร** | *(ต่ำ ปานกลาง สูง)* | | |
| **5. ประวัติการถูกคุกคามทางไซเบอร์** | *(ต่ำ ปานกลาง สูง)* | | |

**ส่วนที่ 2: แนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level)**

แนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมีของ สง. ควรอ้างอิงตามระดับความเสี่ยงตั้งต้นของตนเองที่ สง. ได้ประเมินระดับความเสี่ยงตั้งต้นตามที่กำหนดไว้ในส่วนที่ 1 เรื่อง การประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment) โดยแนวทางการบริการจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมีของแต่ละ Maturity Level คือ Baseline Intermediate และ Advanced จะครอบคลุมการบริหารจัดการความเสี่ยงด้านไซเบอร์ของ สง. ใน 6 ด้านหลัก เพื่อให้มั่นใจได้ว่า สง. ทุกแห่งมีกระบวนการหรือมาตรการควบคุมดูแลความเสี่ยงด้านไซเบอร์ได้เหมาะสมกับขนาดและความซับซ้อนของธุรกิจ โครงสร้างพื้นฐาน ลักษณะการดำเนินงาน และปัจจัยเสี่ยงของตนเอง ดังนี้

## 1. การกำกับดูแล (Governance)

**วัตถุประสงค์ :** เพื่อให้สถาบันการเงินมีการกำกับดูแลและสนับสนุนให้องค์กรมีการบริหารความเสี่ยงด้านไซเบอร์อย่างเพียงพอเหมาะสม มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านไซเบอร์สอดคล้องตามหลัก 3 lines of defence อย่างมีประสิทธิภาพ เป็นส่วนหนึ่งของการบริหารตามกรอบการบริหารจัดการความเสี่ยงในภาพรวมขององค์กร (enterprise wide risk) รวมถึงมีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอในการปฏิบัติงานและบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยไซเบอร์

## 1.1 คณะกรรมการสถาบันการเงิน และผู้บริหารระดับสูง

### 1.1.1 การกำหนดและบทบาทหน้าที่ของคณะกรรมการสถาบันการเงิน และผู้บริหารระดับสูง

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.1.1.1 คณะกรรมการสถาบันการเงินมีบทบาทและหน้าที่ความรับผิดชอบในการดูแลให้มีกลยุทธ์และนโยบาย รวมทั้งดูแลให้มีกลไกในการกำกับดูแลและติดตามให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ ในส่วนของการกำกับดูแลและติดตาม คณะกรรมการสถาบันการเงินอาจมอบหมายให้คณะกรรมการชุดอื่นทำหน้าที่แทนได้ โดยกำหนดบทบาทหน้าที่อย่างชัดเจนและเป็นลายลักษณ์อักษร<br>1.1.1.2 คณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายในการกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีบทบาทหน้าที่ในการกำหนดกลยุทธ์ นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมเรื่องความมั่นคงปลอดภัยไซเบอร์และสอดคล้องกับกลยุทธ์ทางธุรกิจของสถาบันการเงิน รวมทั้งดูแลและติดตามการปฏิบัติงานและความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ของสถาบันการเงิน<br>1.1.1.3 คณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายในการีกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอและเพียงพอ และเมื่อความเสี่ยงมีการเปลี่ยนแปลงหรือเมื่อมีเหตุการณ์ภัยคุกคามทางไซเบอร์ที่สำคัญ<br>1.1.1.4 คณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายในการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศจัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอและเพียงพอ และเมื่อความเสี่ยงมีการเปลี่ยนแปลงหรือมีเหตุการณ์ภัยคุกคามทางไซเบอร์ที่สำคัญ<br>1.1.1.5 คณะกรรมการสถาบันการเงินอย่างน้อย 1 ท่าน ต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศหรือด้านการกำกับดูแลเทคโนโลยีสารสนเทศ (IT Governance)<br>1.1.1.6 คณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายกำหนดให้หน่วยงานธุรกิจและหน่วยงานที่เกี่ยวข้องอื่นมีส่วนร่วมดูแลความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้อง |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Advanced | 1.1.1.7 คณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายกำหนดและอนุมัติข้อความที่แสดงถึงระดับความเสี่ยงด้านไซเบอร์ที่ยอมรับได้ (Cyber Risk Appetite Statement) เพื่อใช้ในการบริหารความเสี่ยงขององค์กร<br>1.1.1.8 คณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายกำหนดให้หน่วยงานธุรกิจรับผิดชอบดูแลความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้อง<br>1.1.1.9 สถาบันการเงินกำหนดให้มีคณะกรรมการหรือผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) ที่ทำหน้าที่ดูแลความมั่นคงปลอดภัยไซเบอร์เป็นการเฉพาะ และอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (authority) เพียงพอ ในการปฏิบัติงานในหน้าที่ CISO เพื่อให้สามารถกำกับดูแลได้อย่างเพียงพอและสอดคล้องกับระดับความเสี่ยงด้านไซเบอร์ที่มี โดยบทบาท หน้าที่ และความรับผิดชอบของ CISO สถาบันการเงินสามารถอ้างอิงตามประกาศของ ธปท. เรื่องหลักเกณฑ์การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) |

**1.1.2 การจัดสรรทรัพยากร**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.1.2.1 สถาบันการเงินจัดสรรงบประมาณในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุม ระบบงาน (application) ข้อมูล (information) โครงสร้างพื้นฐาน (infrastructure) บุคลากร เครื่องมือ และบริการ สอดคล้องและเพียงพอตามระดับความเสี่ยงที่สถาบันการเงินมี |
| Intermediate | 1.1.2.2 สถาบันการเงินจัดสรรงบประมาณให้สามารถรองรับความเสี่ยงด้านไซเบอร์ ที่เพิ่มขึ้นจากกลยุทธ์ทางธุรกิจ และ/หรือ การเปลี่ยนแปลงของรูปแบบและความซับซ้อนภัยคุกคามทางไซเบอร์ |
| Advanced | 1.1.2.3 กระบวนการจัดสรรงบประมาณของสถาบันการเงินในการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของกระบวนการจัดสรรงบประมาณของหน่วยงานธุรกิจ |

**1.1.3 การจัดให้มีการรายงาน**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.1.3.1 สถาบันการเงินจัดให้มีการรายงานสถานะความคืบหน้าตามแผนงาน และ/หรือ โครงการการรักษามั่นคงปลอดภัยไซเบอร์ให้คณะกรรมการสถาบันการเงินและคณะกรรมการที่เกี่ยวข้องรับทราบเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ<br>1.1.3.2 สถาบันการเงินจัดให้มีการรายงานสถานการณ์ภัยคุกคามทางไซเบอร์ที่สถาบันการเงินเผชิญและการรักษาความมั่นคงปลอดภัยไซเบอร์ (Dashboard) ให้คณะกรรมการสถาบันการเงินและคณะกรรมการที่เกี่ยวข้องรับทราบเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง และในกรณีที่ |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | มีเหตุการณ์หรือความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อสถาบันการเงินในวงกว้าง หรือส่งผลกระทบต่อชื่อเสียงของสถาบันการเงินให้รายงานอย่างทันท่วงทีเพื่อการตัดสินใจแก้ไขปัญหา |
| Advanced | 1.1.3.3 รายงานสถานการณ์ภัยคุกคามทางไซเบอร์ที่สถาบันการเงินมีแนวโน้มจะเผชิญจากผลการวิเคราะห์ข้อมูลการรักษาความมั่นคงปลอดภัยไซเบอร์ มีผลการวิเคราะห์แนวโน้มความเสี่ยงของภัยคุกคามทางไซเบอร์เพิ่มเติม รวมทั้งแนวทางการรับมือเรื่องดังกล่าว |

## 1.2 การกำหนดกลยุทธ์และนโยบายด้าน Cyber Resilience

### 1.2.1 กลยุทธ์ด้าน Cyber Resilience

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.2.1.1 สถาบันการเงินกำหนดกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Strategy) โดยคำนึงถึงนโยบาย ระเบียบวิธีปฏิบัติ และเทคโนโลยี<br>1.2.1.2 สถาบันการเงินดูแลให้มีการทบทวนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยเสนอต่อคณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมาย |
| Intermediate | 1.2.1.3 สถาบันการเงินกำหนดโครงการที่สนับสนุนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งสอดคล้องกับทิศทางของเทคโนโลยีและมาตรฐานการรักษาความมั่นคงปลอดภัยที่ยอมรับโดยทั่วไป |
| Advanced | 1.2.1.4 สถาบันการเงินกำหนดให้กลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของกลยุทธ์การบริหารจัดการความเสี่ยงขององค์กร |

### 1.2.2 นโยบายด้าน Cyber Resilience

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.2.2.1 สถาบันการเงินมีนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) ที่ครอบคลุมการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป และได้รับอนุมัติจากคณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมาย<br>1.2.2.2 นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) หรือนโยบายอื่นมีความครอบคลุมการบริหารจัดการเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์<br>1.2.2.3 นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) หรือนโยบายอื่นมีความครอบคลุมการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์กับองค์กรภายนอก (Cyber Threat Intelligence Sharing) |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 1.2.2.4 สถาบันการเงินทบทวนนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) เป็นประจำอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยได้รับความเห็นชอบจากคณะกรรมการสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมาย |
| Advanced | 1.2.2.5 การกำหนดนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) ได้คำนึงถึงผลวิเคราะห์หรือข้อมูลจากองค์ความรู้ด้านภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence) ที่มีผลกระทบอย่างมีนัยสำคัญต่อสถาบันการเงิน<br>1.2.2.6 สถาบันการเงินมีกระบวนการในการทบทวนและปรับปรุงนโยบายที่เกี่ยวข้องกับความเสี่ยงด้านไซเบอร์ทั้งหมดของสถาบันการเงินให้มีความเชื่อมโยงและสอดคล้องกันอย่างทันกาล |

## 1.3 การบริหารจัดการความเสี่ยงด้านไซเบอร์

### 1.3.1 โครงสร้างการบริหารความเสี่ยง

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.3.1.1 หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 1st line of defence) เช่น<br>● หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานอื่นที่เป็นผู้ใช้งานระบบ เป็นต้น มีหน้าที่ ประเมินความเสี่ยงและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมความเสี่ยงด้านไซเบอร์<br>● หน่วยงานด้านการรักษาความมั่นคงปลอดภัย ต้องจัดให้มีแนวทางการควบคุม ติดตาม และรายงานการปฏิบัติงาน รวมทั้งติดตาม จัดทำรายงาน เฝ้าระวังภัยคุกคาม และศึกษาแนวโน้มภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นและส่งผลกระทบต่อสถาบันการเงิน โดยนำเสนอรายงานต่อคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้อง<br>1.3.1.2 หน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงความเสี่ยงด้านไซเบอร์ด้วย (หน่วยงานที่ทำหน้าที่เป็น 2nd line of defence) เช่น หน่วยงานบริหารความเสี่ยง และหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ เป็นต้น มีหน้าที่ดังนี้<br>● หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง มีหน้าที่กำหนดกรอบและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ จัดให้มีการประเมินความเสี่ยงตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยงและทบทวนการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานที่ทำหน้าที่เป็น 1st line of defence และขององค์กรในภาพรวมให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ มีการรวบรวมและเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกับความเสี่ยงด้านอื่นของสถาบันการเงิน และนำเสนอผลการประเมินและการบริหารความเสี่ยงองค์กรต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยง |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | ● หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ มีหน้าที่กำหนดกระบวนการติดตามดูแล ให้คำปรึกษา สอบทาน และรายงานการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง และนำเสนอต่อคณะกรรมการที่รับผิดชอบกำกับดูแล เพื่อป้องกันการละเมิดหรือการปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง<br>1.3.1.3 หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมการตรวจสอบด้านการรับมือกับภัยคุกคามทางไซเบอร์ (หน่วยงานที่ทำหน้าที่เป็น 3rd line of defence) มีหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงของหน่วยงานที่ทำหน้าที่ 1st line และ 2nd line of defence รวมถึงงานอื่น ๆ ที่เกี่ยวข้อง เช่น การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ เป็นต้น เพื่อสอบทานให้มั่นใจว่ามีการปฏิบัติที่เป็นไปตามนโยบาย มาตรฐาน และระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ |

**1.3.2 กระบวนการบริหารจัดการความเสี่ยง**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.3.2.1 สถาบันการเงินมีกระบวนการบริหารจัดการความเสี่ยงด้านไซเบอร์ที่ครอบคลุม ดังนี้<br>● การประเมินความเสี่ยง (Risk Assessment) โดยครอบคลุม การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินค่าความเสี่ยง (Risk Evaluation)<br>● การปิดและการจัดการความเสี่ยง (Risk Treatment)<br>● การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)<br>● การรายงานความเสี่ยง (Risk Reporting)<br>โดยให้อ้างอิงตามประกาศและแนวปฏิบัติของ ธปท. เกี่ยวกับหลักเกณฑ์การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) ของสถาบันการเงิน<br>1.3.2.2 การประเมินความเสี่ยงด้านไซเบอร์ครอบคลุมผลกระทบที่อาจเกิดขึ้นในด้านอื่น ๆ ด้วย เช่น ผลกระทบต่อกลยุทธ์ การดำเนินธุรกิจ หรือต่อชื่อเสียง เป็นต้น |
| Intermediate | 1.3.2.3 สถาบันการเงินมีการกำหนดตัวชี้วัด (Benchmarks or target performance metrics) ที่สะท้อนถึงการเพิ่มขึ้นหรือลดลงของประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง |
| Advanced | 1.3.2.4 สถาบันการเงินมีศักยภาพในการรวบรวมและรายงานข้อมูลความเสี่ยงด้านไซเบอร์ได้อย่างรวดเร็วทันกาล ในการสนับสนุนการติดตามและรายงานความเสี่ยงจากภัยไซเบอร์ได้อย่างมีประสิทธิภาพ โดยเฉพาะขณะเกิดเหตุการณ์ผิดปกติ |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 1.3.2.5 สถาบันการเงินมีการประเมินความจำเป็นในการทำประกันภัยไซเบอร์ (Cyber Insurance) เพื่อบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ |

## 1.4 การตรวจสอบ

### 1.4.1 ขอบเขตการตรวจสอบ

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.4.1.1 ขอบเขตการตรวจสอบครอบคลุมนโยบาย มาตรฐาน ระเบียบวิธีปฏิบัติ และการควบคุมการปฏิบัติงานสำคัญที่เกี่ยวข้องกับความเสี่ยงด้านไซเบอร์ ซึ่งรวมถึงความเสี่ยงด้านไซเบอร์จากการออกผลิตภัณฑ์ทางการเงินใหม่ การใช้ระบบและเทคโนโลยีใหม่<br>1.4.1.2 สถาบันการเงินมีการตรวจสอบการประเมินการรักษาความมั่นคงปลอดภัยการจัดเก็บและรับส่งข้อมูลที่มีความสำคัญของสถาบันการเงิน<br>1.4.1.3 สถาบันการเงินมีการตรวจสอบการประเมินความเพียงพอของการบริหารจัดการและการควบคุมความเสี่ยงด้านไซเบอร์กับระดับความเสี่ยงด้านไซเบอร์ที่สถาบันการเงินมี<br>1.4.1.4 สถาบันการเงินมีการตรวจสอบการประเมินการรับมือและความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่องต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cybersecurity Incident) เพื่อให้มั่นใจว่ามีการเตรียมการที่สอดคล้องกับระดับความเสี่ยงด้านไซเบอร์ที่สถาบันการเงินมี<br>1.4.1.5 ผลการตรวจสอบหรือผลการสอบทานสามารถระบุจุดอ่อนหรือช่องโหว่ในการควบคุมความมั่นคงปลอดภัยไซเบอร์ รวมถึงสาเหตุที่แท้จริงและผลกระทบต่อธุรกิจ |
| Intermediate | 1.4.1.6 สถาบันการเงินมีการตรวจสอบการรวบรวมและแลกเปลี่ยนข้อมูล Cyber Threat Intelligence สอดคล้องกับระดับความเสี่ยงด้านไซเบอร์ที่สถาบันการเงินมี |
| Advanced | 1.4.1.7 สถาบันการเงินมีการตรวจสอบกระบวนการจัดทำ Cyber Risk Appetite Statement เพื่อให้มั่นใจว่าการกำหนด Cyber Risk Appetite Statement สอดคล้องกับขนาดและความซับซ้อนของธุรกิจ รวมถึงเปรียบเทียบความพร้อมในการรับมือภัยไซเบอร์ของสถาบันการเงิน (Cyber Resilience Readiness) กับ Cyber Risk Appetite Statement ที่สถาบันการเงินกำหนด |

**1.4.2 กระบวนการตรวจสอบ**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.4.2.1 สถาบันการเงินทบทวนและปรับปรุงกระบวนการตรวจสอบ โดยคำนึงถึงการเปลี่ยนแปลงระดับความเสี่ยงด้านไซเบอร์ของสถาบันการเงิน |
| Intermediate | 1.4.2.2 สถาบันการเงินทบทวนและปรับปรุงกระบวนการตรวจสอบ โดยคำนึงถึงการเปลี่ยนแปลงรูปแบบภัยคุกคามทางไซเบอร์ในภาคธุรกิจการเงินที่กระทบ |
| Advanced | 1.4.2.3 สถาบันการเงินทบทวนและปรับปรุงกระบวนการตรวจสอบ โดยคำนึงถึงการเปลี่ยนแปลงรูปแบบภัยคุกคามทางไซเบอร์ในภาคธุรกิจอื่น ๆ ที่เกี่ยวข้องที่กระทบ เช่น ธุรกิจโทรคมนาคม เป็นต้น |

## 1.5 การบริหารจัดการบุคลากรและการฝึกอบรม

**1.5.1 การบริหารจัดการบุคลากรที่เกี่ยวข้องกับงานความมั่นคงปลอดภัยไซเบอร์**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.5.1.1 สถาบันการเงินกำหนดบทบาทหน้าที่และความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ชัดเจน<br>1.5.1.2 สถาบันการเงินกำหนดคุณสมบัติ ความรู้ และความเชี่ยวชาญของบุคลากรที่รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ชัดเจน<br>1.5.1.3 สถาบันการเงินมีกระบวนการตรวจสอบประวัติของบุคลากรก่อนการว่าจ้างตามความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ เช่น ประวัติการศึกษา ประวัติการทำงาน ประวัติอาชญากรรม ข้อมูลเครดิตบูโร ข้อมูลการทุจริต (ถ้ามี) เป็นต้น<br>1.5.1.4 ผู้บริหารและพนักงานที่ทำหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์มีคุณสมบัติ ความรู้ และความเชี่ยวชาญเป็นไปตามที่สถาบันการเงินกำหนดหรือสามารถปฏิบัติงานได้ตามหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย<br>1.5.1.5 สถาบันการเงินมีกระบวนการจัดการหรือเฝ้าระวังพนักงานที่กำลังจะพ้นสภาพการเป็นพนักงานหรือบริษัทที่กำลังจะสิ้นสุดสัญญากับสถาบันการเงิน ในการเข้าถึงระบบงานและทรัพยากรที่สำคัญของสถาบันการเงิน |
| Intermediate | 1.5.1.6 ผู้บริหารระดับสูงที่รับผิดชอบงานในการผลักดันและสนับสนุนงานด้านไซเบอร์ควรมีความรู้หรือประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์<br>1.5.1.7 สถาบันการเงินมีกระบวนการในการประเมินความเหมาะสมของคุณสมบัติและศักยภาพของบุคลากรกับหน้าที่ที่รับผิดชอบในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง<br>1.5.1.8 สถาบันการเงินมีแนวทางและแผนในการสรรหา การดูแลรักษา และการจัดหาทดแทนพนักงานกลุ่มศักยภาพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Talent Management) |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 1.5.1.9 สถาบันการเงินมีกระบวนการหรือเครื่องมือในการตรวจสอบพฤติกรรมของบุคลากรที่รับผิดชอบในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบอย่างต่อเนื่อง |

**1.5.2 การฝึกอบรมและการสร้างความตระหนัก (Awareness)**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 1.5.2.1 สถาบันการเงินมีการอบรมเพื่อสร้างความรู้และความตระหนักด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่คณะกรรมการสถาบันการเงินและคณะกรรมการที่เกี่ยวข้อง<br>1.5.2.2 สถาบันการเงินมีการอบรมเพื่อสร้างความรู้และความตระหนักด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้แก่บุคลากรในองค์กรและลูกค้าอย่างสม่ำเสมอและต่อเนื่อง สำหรับการอบรมให้บุคลากรในองค์กรควรวัดผลได้<br>1.5.2.3 สถาบันการเงินมีการอบรมและพัฒนาทักษะ ความรู้ ความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเสริมสร้างศักยภาพให้บุคลากรที่รับผิดชอบงานด้านนี้อย่างเพียงพอและต่อเนื่อง<br>1.5.2.4 สถาบันการเงินมีการอบรมและพัฒนาทักษะ ความรู้ ความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มเติมให้กับบุคลากรที่มีการใช้งานสิทธิ์สูง (Privileged Account)<br>1.5.2.5 สถาบันการเงินมีการสร้างความตระหนักและความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับผู้บริหารและพนักงานในเชิงรุกให้มีสถานการณ์เสมือนจริง เช่น การทดสอบ Phishing Email เป็นต้น<br>1.5.2.6 สถาบันการเงินจัดให้มีการนำสิ่งที่ได้เรียนรู้ (Lessons Learned) จากการทดสอบและซักซ้อมการรับมือภัยคุกคามทางไซเบอร์ไปใช้ในการสร้างเสริมความตระหนักด้านการรักษาความมั่นคงปลอดภัยไซเบอร์<br>1.5.2.7 แผนการจัดอบรมประจำปีทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ควรครอบคลุมทั้งเหตุการณ์ที่เกิดขึ้นกับสถาบันการเงินและการรับมือต่อเหตุการณ์ดังกล่าว ภัยไซเบอร์ที่สถาบันการเงินเผชิญในปัจจุบันและภัยใหม่ ๆ ที่อาจเกิดขึ้นในอนาคต |

## 2. การระบุความเสี่ยง (Identification)

**วัตถุประสงค์ :** เพื่อให้สถาบันการเงินมีการบริหารจัดการทรัพย์สินทางด้านเทคโนโลยีที่สามารถเชื่อมโยง นำไปใช้ในการบริหารจัดการ และสามารถระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

### 2.1 ทรัพย์สินด้านเทคโนโลยีสารสนเทศ

#### 2.1.1 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 2.1.1.1 สถาบันการเงินมีทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ครอบคลุมอุปกรณ์คอมพิวเตอร์ ระบบปฏิบัติการ ระบบงาน และข้อมูลที่สามารถเชื่อมโยง นำมาใช้บริหารจัดการ และระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ ดังตัวอย่างหัวข้อในรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศแนบท้ายกรอบการประเมินนี้<br>2.1.1.2 สถาบันการเงินจัดระดับความสำคัญของทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยอาจพิจารณาจากการจัดชั้นความลับของข้อมูล (Information Classification) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) และการวิเคราะห์ความเสี่ยงเพื่อใช้ในการควบคุมการรักษาความมั่นคงปลอดภัยไซเบอร์<br>2.1.1.3 สถาบันการเงินกำหนดหน้าที่ความรับผิดชอบของหน่วยงาน/ผู้รับผิดชอบในการจัดทำ ดูแล และสอบทานทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศไว้อย่างชัดเจน เพื่อให้ทะเบียนทรัพย์สินมีความถูกต้อง ครบถ้วนและเป็นปัจจุบันอยู่เสมอ<br>2.1.1.4 สถาบันการเงินมีกระบวนการปรับปรุงทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่สะท้อนทรัพย์สินที่มีอยู่จริง ทั้งในเชิงปริมาณ ตำแหน่งที่ตั้ง สถานะ รวมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (End-of-Life) หรือสิ้นสุดการให้บริการ (End-of-Support) และมีการตรวจสอบทรัพย์สินที่มีอยู่จริงกับทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง<br>2.1.1.5 สถาบันการเงินมีกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (End-of-Life) หรือสิ้นสุดการให้บริการ (End-of-Support) เพื่อบริหารจัดการความเสี่ยงด้านไซเบอร์ให้สอดคล้องกัน<br>2.1.1.6 สถาบันการเงินมีกระบวนการอนุมัติกระบวนการบริหารจัดการการเปลี่ยนแปลงทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Change management) โดยผู้บริหารที่ได้รับมอบหมาย และ/หรือคณะกรรมการบริหารจัดการการเปลี่ยนแปลง (Change Advisory Board: CAB) ที่จัดตั้งตามหลักการแบ่งแยกหน้าที่ที่ดีจากผู้ปฏิบัติงาน |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Intermediate | 2.1.1.7 สถาบันการเงินประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในกระบวนการการบริหารจัดการการเปลี่ยนแปลงทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Change management) ก่อนนำขึ้นใช้งานจริง (Production) |
| Advanced | 2.1.1.8 ในการจัดซื้อจัดจ้างทรัพย์สินด้านเทคโนโลยีสารสนเทศที่สำคัญมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ของผู้ผลิต ผู้ให้บริการ ผู้พัฒนา ผู้สนับสนุนการให้บริการ และผู้บำรุงรักษา อย่างเพียงพอ<br>2.1.1.9 สถาบันการเงินมีเครื่องมือและกระบวนการที่ใช้ติดตาม (Tracking) ปรับปรุง (Updating) จัดลำดับความสำคัญ (Prioritizing) ในทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ และสามารถปรับเปลี่ยนรูปแบบรายงานทรัพย์สินด้านเทคโนโลยีสารสนเทศได้ตามความต้องการใช้งาน<br>2.1.1.10 สถาบันการเงินมีเครื่องมือและกระบวนการที่ใช้ตรวจจับการเปลี่ยนแปลงแก้ไขของทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ครอบคลุมอุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงาน และข้อมูล โดยไม่ได้รับอนุญาตได้ทันการณ์<br>2.1.1.11 สถาบันการเงินมีเครื่องมือหรือระบบในการบริหารจัดการการเปลี่ยนแปลง (Change Management System) ที่สามารถระบุได้ว่าต้องประเมินความเสี่ยงและผลกระทบของอุปกรณ์หรือระบบงานที่เกี่ยวข้องใดบ้างจากการเปลี่ยนแปลงที่เกิดขึ้น (Pre-defined Thresholds) |

### 2.1.2 การบริการจัดการด้าน IT Configuration

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 2.1.2.1 สถาบันการเงินมีการกำหนดให้การเปลี่ยนแปลงแก้ไข Baseline ของการตั้งค่า (IT Configuration Baseline) ของอุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงาน เครื่องมือด้านการรักษาความมั่นคงปลอดภัยและเครื่องมืออื่น ๆ ต้องผ่านการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยอย่างเพียงพอและได้รับการอนุมัติก่อนดำเนินการด้วย |
| Advanced | 2.1.2.2 สถาบันการเงินมีเครื่องมือที่ใช้ตรวจจับการเปลี่ยนแปลงการตั้งค่าและแก้ไข อุปกรณ์คอมพิวเตอร์ โปรแกรม และระบบงาน โดยไม่ได้รับอนุญาตเพื่อให้สามารถป้องกันหรือระงับการดำเนินการได้ทันกาล |

## 2.2 การระบุและประเมินความเสี่ยงด้านไซเบอร์

### 2.2.1 การระบุและประเมินความเสี่ยงด้านไซเบอร์

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 2.2.1.1 สถาบันการเงินมีกระบวนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สามารถระบุระบบงานด้าน IT ที่สำคัญ (Critical System) หรือธุรกรรมที่มีความเสี่ยงสูง (High-risk Transaction) ที่จำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านไซเบอร์อย่างเข้มงวด |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 2.2.1.2 สถาบันการเงินกำหนดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อข้อมูลลูกค้า เพื่อให้สามารถระบุภัยคุกคามทางไซเบอร์ที่มีโอกาสและความเสียหายที่อาจเกิดขึ้น ตลอดจนความเพียงพอของนโยบาย ขั้นตอนปฏิบัติ และระบบการจัดเก็บข้อมูลลูกค้า<br>2.2.1.3 สถาบันการเงินกำหนดให้มีการประเมินความเสี่ยงด้านไซเบอร์ของข้อมูลลูกค้า เมื่อมีการติดตั้ง การเชื่อมต่อ การเปลี่ยนแปลง และการนำเทคโนโลยีใหม่มาใช้ รวมถึงการออกผลิตภัณฑ์และบริการใหม่<br>2.2.1.4 สถาบันการเงินมีการประเมินความเสี่ยงด้านไซเบอร์ ครอบคลุมการใช้งานอุปกรณ์คอมพิวเตอร์ ระบบปฏิบัติการ ระบบงาน ที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (End-of-Life) หรือสิ้นสุดการให้บริการ (End-of-Support)<br>2.2.1.5 สถาบันการเงินมีการประเมินความเสี่ยงด้านไซเบอร์ที่สามารถระบุความเสี่ยงจากการจัดหาผลิตภัณฑ์หรือบริการ รวมถึงพันธมิตรรายใหม่<br>2.2.1.6 สถาบันการเงินมีการปรับปรุงขอบเขตการประเมินความเสี่ยงด้านไซเบอร์อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญซึ่งกระทบต่อ Cyber Risk Appetite ของสถาบันการเงิน เพื่อให้มีวิธีการบริหารจัดการรองรับอย่างเพียงพอ |

## 3. การป้องกันความเสี่ยง (Protection)

**วัตถุประสงค์ :** เพื่อให้สถาบันการเงินมีกระบวนการบริหารจัดการและเครื่องมือหรืออุปกรณ์ที่พร้อมสำหรับการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดการหยุดชะงักในการให้บริการของระบบงานที่สำคัญ

## 3.1 การควบคุมเพื่อป้องกันโครงสร้างพื้นฐาน

### 3.1.1 การป้องกันระบบเครือข่าย

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.1.1.1 สถาบันการเงินมีอุปกรณ์ป้องกันเครือข่าย เช่น Firewall เป็นต้น ติดตั้งไว้ทุกจุดที่มีการเชื่อมต่อระหว่างเครือข่ายภายใน เครือข่าย DMZ และเครือข่ายภายนอก<br>3.1.1.2 สถาบันการเงินกำหนดกระบวนการบริหารจัดการการตั้งค่าหรือเปลี่ยนแปลงค่าของอุปกรณ์ป้องกันเครือข่าย เช่น Firewall<br>3.1.1.3 สถาบันการเงินตรวจสอบความถูกต้องของการตั้งค่าอุปกรณ์ป้องกันเครือข่าย เช่น Firewall Rules อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ<br>3.1.1.4 สถาบันการเงินติดตั้งอุปกรณ์ในการตรวจจับและปิดกั้นการโจมตีหรือการบุกรุกโดยไม่ได้รับอนุญาต เช่น Intrusion Detection หรือ Prevention System (IDS/IPS)<br>3.1.1.5 สถาบันการเงินมีมาตรการเชิงเทคนิคหรือเครื่องมือเพื่อใช้ป้องกันการเชื่อมต่อและ/หรือการเข้าถึงระบบเครือข่ายภายในของสถาบันการเงินโดยอุปกรณ์ที่ไม่ได้รับอนุญาต<br>3.1.1.6 สถาบันการเงินแยกเครือข่ายไร้สายสำหรับบุคคลภายนอกออกจากระบบเครือข่ายภายในสถาบันการเงินอย่างชัดเจน<br>3.1.1.7 สถาบันการเงินใช้วิธีการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากลในการพิสูจน์ตัวตนและการรับส่งข้อมูลผ่านระบบเครือข่ายไร้สาย<br>3.1.1.8 สถาบันการเงินมีอุปกรณ์ป้องกันเครือข่ายติดตั้งไว้ในระบบเครือข่ายไร้สายเพื่อป้องกันการเข้าถึงเครือข่ายภายใน และจำกัดการติดต่อสื่อสารที่ไม่ได้รับอนุญาต (Unauthorised Traffic)<br>3.1.1.9 สถาบันการเงินแบ่งระบบเครือข่ายภายในเป็นโซน (Network Segmentation) และวางมาตรการการป้องกันตามระดับความเสี่ยงจากการถูกโจมตีทางไซเบอร์ |
| Intermediate | 3.1.1.10 สถาบันการเงินออกแบบระบบเครือข่ายและมีการตั้งค่าอุปกรณ์ให้สามารถจำกัดและติดตามการรับส่งข้อมูลระหว่าง Trusted และ Untrusted Zone ได้ |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 3.1.1.11 สถาบันการเงินมีมาตรการควบคุมการรักษาความมั่นคงปลอดภัยในการเข้าถึงระบบงานจากระยะไกล (Remote Access) สำหรับผู้ใช้งานสิทธิ์สูง<br>3.1.1.12 สถาบันการเงินมีมาตรการเพื่อป้องกันและลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ ที่ก่อให้เกิดการหยุดชะงักในการให้บริการของระบบงานที่สำคัญ เช่น DDoS เป็นต้น โดยอาจดำเนินการเองหรือใช้บริการจากผู้ให้บริการภายนอก เช่น CDN หรือ ISP เป็นต้น<br>3.1.1.13 สถาบันการเงินมีการเปลี่ยนกุญแจเข้ารหัสข้อมูล สำหรับเข้ารหัสการรับส่งข้อมูลผ่านระบบเครือข่ายไร้สายอย่างสม่ำเสมอ |
| Advanced | 3.1.1.14 สถาบันการเงินมีกระบวนการและเครื่องมือเพื่อป้องการเข้าถึงจากอุปกรณ์คอมพิวเตอร์ที่ไม่ได้ Patch ของพนักงานและของบุคคลภายนอกที่ได้รับอนุญาต |

**3.1.2 การตั้งค่าระบบ (System Configuration)**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.1.2.1 สถาบันการเงินจัดทำ Security Configuration สอดคล้องกับมาตรฐานอุตสาหกรรม (Industry Standards) รวมทั้งจัดให้มีการสอบทานการตั้งค่าดังกล่าวอย่างสม่ำเสมอ<br>3.1.2.2 สถาบันการเงินปิดหรือยกเลิกการใช้งาน Ports, Functions, Protocols หรือ Services ต่าง ๆ เมื่อไม่มีความจำเป็น<br>3.1.2.3 สถาบันการเงินมีกระบวนการควบคุมและติดตามการเปลี่ยนแปลงการตั้งค่าอุปกรณ์คอมพิวเตอร์<br>3.1.2.4 สถาบันการเงินมีมาตรการควบคุมเพื่อป้องกันไม่ให้มีการติดตั้งโปรแกรมโดยผู้ใช้ที่ไม่ได้รับอนุญาต<br>3.1.2.5 สถาบันการเงินมีกระบวนการสอบทานระบบงานสำคัญที่ใช้เทคโนโลยีที่ล้าสมัย (Legacy Technologies) หรือสิ้นสุดการสนับสนุนอย่างสม่ำเสมอ เพื่อให้สามารถระบุช่องโหว่ โอกาสในการหาเทคโนโลยี หรือวิธีการป้องกันภัยคุกคามในลักษณะอื่นทดแทน โดยเลือกวิธีการควบคุมที่ปลอดภัยและมีการทดสอบก่อนนำไปใช้จริง<br>3.1.2.6 สถาบันการเงินมีการควบคุมโปรแกรมสำหรับใช้ในการเปลี่ยนแปลง แก้ไข การตั้งค่าระบบปฏิบัติการ (Operation System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication) โดยให้สิทธิ์ตามความจำเป็น (Least Privilege)<br>3.1.2.7 สถาบันการเงินกำหนดระยะเวลาและเงื่อนไขในการยกเลิกการใช้งาน Session ของระบบไว้อย่างชัดเจน |
| Advanced | 3.1.2.8 สถาบันการเงินทำ File Integrity Check กับ Server ที่เชื่อมต่อกับเครือข่ายสาธารณะเป็นประจำเพื่อลดความเสี่ยงต่อภัยคุกคาม |

## 3.2 การควบคุมการเข้าใช้งาน

### 3.2.1 การบริหารจัดการบัญชีผู้ใช้งาน

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.2.1.1 สถาบันการเงินมีการพิสูจน์ตัวตนทั้งระดับ Physical และ Logical เพื่อใช้ควบคุมการเข้าถึงระบบปฏิบัติการ (Operation System) ระบบงาน (Application) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication)<br>3.2.1.2 สถาบันการเงินกำหนดนโยบายรหัสผ่าน (Password Policy) ที่ครอบคลุมการกำหนดระดับความซับซ้อนของรหัสผ่าน จำนวนครั้งสูงสุดของการใส่รหัสผ่านผิด และเงื่อนไขการตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม<br>3.2.1.3 สถาบันการเงินกำหนดสิทธิ์การเข้าถึงระบบงานและข้อมูลลับให้พนักงานตามขอบเขตหน้าที่ความรับผิดชอบของแต่ละคนให้เป็นไปตามความจำเป็น (Least Privilege) และเป็นไปตามหลักการแบ่งแยกหน้าที่ที่ดี (Segregration of Duty)<br>3.2.1.4 สถาบันการเงินกำหนดให้มีกระบวนการเปลี่ยนแปลง และยกเลิกสิทธิ์การเข้าถึงระบบ ทั้งทาง Physical และ Logical ของพนักงานเมื่อมีการโยกย้ายหรือสิ้นสภาพการเป็นพนักงาน โดยกระบวนการดังกล่าวต้องคำนึงถึงความเสี่ยงและผลในทางปฏิบัติ<br>3.2.1.5 สถาบันการเงินสอบทานสิทธิ์การเข้าถึงระบบปฏิบัติการ (Operation System) ระบบงาน (Application) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication) อย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยสอดคล้องกับระดับความเสี่ยงตามที่สถาบันการเงินกำหนด<br>3.2.1.6 สถาบันการเงินเปลี่ยน Default Password และระงับการใช้งาน Default Account ที่ไม่จำเป็นก่อนเริ่มใช้งานครั้งแรก<br>3.2.1.7 สถาบันการเงินมีการเข้ารหัสข้อมูลรหัสผ่าน (Password Encryption) ที่ปลอดภัย ทั้งในการจัดเก็บ (at Rest) และระหว่างการรับส่ง (In Transit)<br>3.2.1.8 สถาบันการเงินแยกบัญชีผู้ใช้งานของระบบที่ไม่ได้ใช้งานจริง (Non-Production) ออกจากบัญชีผู้ใช้งานของระบบที่ใช้งานจริง (Production) อย่างชัดเจน เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงระบบงานโดยไม่ได้รับอนุญาต |
| Intermediate | 3.2.1.9 ระบบงานที่สถาบันการเงินพิจารณาว่ามีความเสี่ยงอย่างมีนัยสำคัญควรมีระบบแจ้งเตือนแบบอัตโนมัติเมื่อมีการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งานให้ผู้ที่เกี่ยวข้องทราบ เช่นการแจ้งเตือนผ่าน Email หรือ SMS เป็นต้น |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Advanced | 3.2.1.10 สถาบันการเงินมีมาตรการป้องกันไม่ให้มีการเข้าถึงระบบงานหรืออุปกรณ์ที่ใช้ในการติดต่อสื่อสารภายในองค์กรของสถาบันการเงิน โดยไม่ได้รับอนุญาตตามระดับความเสี่ยงของการเข้าถึงข้อมูล เช่น ระบบ Instant Messaging, Document Sharing, Networked White Board ระบบประชุมทางไกล และอุปกรณ์ IoT ที่เกี่ยวข้อง |

**3.2.2 การบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิ์สูง**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.2.2.1 สถาบันการเงินมีมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานสิทธิ์สูงอย่างเข้มงวด เช่น การมอบหมายสิทธิ์ การห้ามใช้สิทธิ์ร่วมกับผู้อื่น ระยะเวลาการใช้งาน และการกำหนดรหัสผ่านที่รัดกุม เป็นต้น<br>3.2.2.2 สถาบันการเงินแยกบัญชีผู้ใช้งานของผู้ดูแลระบบ เป็น 2 บัญชีผู้ใช้งาน คือ สำหรับการใช้งานทั่วไป และสำหรับการบริหารจัดการระบบที่จำเป็นต้องใช้สิทธิ์สูง หรือมีการอนุญาตให้ใช้งานสิทธิ์สูงตามความจำเป็น |
| Intermediate | 3.2.2.3 สถาบันการเงินมีมาตรการควบคุมผู้ดูแลระบบฐานข้อมูลที่สามารถเข้าถึงระบบฐานข้อมูล (Database System) เพื่อป้องกันการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต |
| Advanced | 3.2.2.4 สถาบันการเงินใช้วิธีการพิสูจน์ตัวตนแบบ Multifactor เช่น การใช้ Tokens, Digital Certificates เป็นต้น ในการพิสูจน์ตัวตนของบัญชีผู้ใช้งานที่มีสิทธิ์สูงสำหรับระบบงานสำคัญตามที่สถาบันการเงินกำหนด (ตาม BIA หรือหลักเกณฑ์ที่เทียบเท่า ที่สูงสุด 2 ระดับแรก) |

**3.2.3 การบริหารจัดการการเข้าใช้งานของลูกค้า**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.2.3.1 สถาบันการเงินกำหนดมาตรการควบคุมในการพิสูจน์ตัวตนลูกค้าผู้ใช้งานผลิตภัณฑ์และบริการทางการเงินผ่านระบบ Internet ที่สอดคล้องตามระดับความเสี่ยง<br>3.2.3.2 สถาบันการเงินกำหนดให้หน่วยงานด้านการบริการลูกค้า เช่น Call Center มีขั้นตอนพิสูจน์ตัวตนลูกค้าในการใช้บริการหรือทำธุรกรรมตามระดับความเสี่ยง |
| Advanced | 3.2.3.3 สถาบันการเงินมีมาตรการควบคุมการป้องกัน Malware และ Man-in-the-middle ในขั้นตอนการพิสูจน์ตัวตนของลูกค้าในการทำธุรกรรมที่มีความเสี่ยงสูงตามที่สถาบันการเงินกำหนดว่าเป็นธุรกรรมที่มีความเสี่ยงสูงผ่านเครือข่าย Internet<br>3.2.3.4 สถาบันการเงินพิจารณาการนำเทคโนโลยี Tokenization มาใช้ทดแทนค่าเฉพาะ (Unique Value) ของข้อมูลที่เป็นความลับ เช่น ใช้ทดแทนหมายเลขบัตรเครดิต เป็นต้น |

**3.2.4 การบริหารจัดการการเข้าถึงทางกายภาพ (Physical Access Management)**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.2.4.1 สถาบันการเงินมีมาตรการควบคุมการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันการเข้าถึงอุปกรณ์เทคโนโลยีสารสนเทศและระบบเครือข่ายสื่อสารของสถาบันการเงินโดยไม่ได้รับอนุญาต<br>3.2.4.2 สถาบันการเงินมีมาตรการบริหารจัดการการเข้าถึงด้านกายภาพของระบบงาน IT ที่สำคัญ โดยครอบคลุมการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการบันทึกการเข้าถึงพื้นที่ |

**3.2.5 การบริหารจัดการการเข้าถึงจากระยะไกล (Remote Access Management)**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.2.5.1 สถาบันการเงินกำหนดให้มีการเข้ารหัสช่องทางการเชื่อมต่อและใช้วิธีการพิสูจน์ตัวตนแบบ Multifactor ในการอนุญาตให้พนักงานหรือบุคคลภายนอกที่ได้รับอนุญาต เข้าใช้ระบบงาน IT ที่สำคัญ (Critical System) ของสถาบันการเงินจากระยะไกลผ่านเครือข่ายภายนอกตามความเสี่ยง |

**3.2.6 การบริหารจัดการการเข้าถึงกุญแจเข้าและถอดรหัสข้อมูล (Cryptographic Keys Access Management)**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.2.6.1 สถาบันการเงินมีมาตรการควบคุมป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงการจัดเก็บกุญแจเข้ารหัส ข้อมูลที่สถาบันการเงินใช้งาน<br>3.2.6.2 สถาบันการเงินมีมาตรการรักษาความปลอดภัยของกุญแจเข้ารหัสที่ใช้สำหรับระบบงาน IT ที่สำคัญ (Critical System) ทั้งด้าน Physical และ Logical โดยใช้อุปกรณ์รักษาความปลอดภัย HSM (Hardware Security Module) หรืออุปกรณ์อื่นที่ทำหน้าที่ในลักษณะเดียวกัน |

**3.2.7 การบริหารจัดการสิทธิ์การเข้าใช้งานของบุคคลภายนอก**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.2.7.1 สถาบันการเงินใช้วิธีการพิสูจน์ตัวตนอย่างเข้มงวด (Strong Authentication) ตามมาตรฐานสากล ในการอนุญาตให้บุคคลภายนอกเข้าใช้งานระบบงานและระบบเครือข่ายของสถาบันการเงินตามความเสี่ยง |

## 3.3 การรักษาความมั่นคงปลอดภัยของข้อมูล

### 3.3.1 การรักษาความปลอดภัยของข้อมูลในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Data Security)

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.3.1.1 สถาบันการเงินมีมาตรการควบคุมการใช้งานสื่อบันทึกข้อมูลแบบพกพาให้ใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น<br>3.3.1.2 สถาบันการเงินมีมาตรการควบคุมเพื่อป้องกันข้อมูลรั่วไหลจากการส่งข้อมูลออกภายนอกโดยไม่ได้รับอนุญาตผ่านช่องทางต่าง ๆ เช่น สื่อบันทึกข้อมูลแบบพกพา อีเมล และช่องทาง Social Network เป็นต้น<br>3.3.1.3 สถาบันการเงินติดตั้งโปรแกรมป้องกัน Malware บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Devices) ของ สถาบันการเงิน เช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์ปฏิบัติงาน (Workstation) เครื่องคอมพิวเตอร์พกพา (Laptops) และอุปกรณ์พกพา (Mobile Devices) เป็นต้น<br>3.3.1.4 สถาบันการเงินมีมาตรการป้องกันการรั่วไหลของข้อมูลจากอุปกรณ์พกพาที่สูญหายหรือถูกโจรกรรม<br>3.3.1.5 สถาบันการเงินมีกระบวนการควบคุมเพื่อล้างหรือทำลายข้อมูลออกจากสื่อบันทึกข้อมูลใดๆ ที่ไม่ได้ใช้งานแล้ว |
| Intermediate | 3.3.1.6 สถาบันการเงินมีเครื่องมือป้องกันข้อมูลสำคัญรั่วไหลจากการส่งข้อมูลออกโดยไม่ได้รับอนุญาตผ่านช่องทางต่างๆ เช่น สื่อบันทึกข้อมูลแบบพกพา อีเมล และช่องทาง Social Network เป็นต้น<br>3.3.1.7 สถาบันการเงินมีมาตรการควบคุมจากส่วนกลาง เพื่อป้องกันภัยคุกคามจาก Malware สำหรับอุปกรณ์พกพาทุกเครื่องที่สามารถเข้าถึงข้อมูลของสถาบันการเงินได้<br>3.3.1.8 สถาบันการเงินมีเครื่องมือบริหารจัดการอุปกรณ์พกพาเพื่อตรวจจับการเปลี่ยนแปลงแก้ไขอุปกรณ์ที่อาจก่อให้เกิดความเสี่ยง เช่น การทำ Jailbreak หรือ Rooted เป็นต้น<br>3.3.1.9 สถาบันการเงินมีมาตรการในการตรวจสอบและปรับปรุง Patch ของระบบปฏิบัติการ (Operation System) และระบบงาน (Application) บนอุปกรณ์พกพาที่เชื่อมต่อกับระบบเครือข่ายภายในให้เป็นปัจจุบันอยู่เสมอ |
| Advanced | 3.3.1.10 สถาบันการเงินมีการควบคุมการเข้าถึงข้อมูลลับหรือระบบงาน IT ที่สำคัญ (Critical System) ของสถาบันการเงิน ผ่านอุปกรณ์พกพาของพนักงานที่ได้รับอนุญาต (BYOD) ภายใต้สภาวะแวดล้อมที่ปลอดภัย เช่น Isolated Sandbox หรือ Secure Container เป็นต้น |

**3.3.2 การป้องกันข้อมูล**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.3.2.1 สถาบันการเงินกำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูลสารสนเทศ (Information Classification) ที่ระบุชั้นความลับของข้อมูลสารสนเทศ (Labeling) อย่างชัดเจน และกำหนดแนวทางการรักษาความปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับโดยครอบคลุม<br>● อุปกรณ์ที่ใช้ปฏิบัติงาน (in Use/ at Endpoint)<br>● การส่งผ่านเครือข่าย (in Transit)<br>● ระบบและสื่อบันทึกข้อมูล (at Rest) ได้แก่ ข้อมูลบนระบบอุปกรณ์ และสื่อบันทึกข้อมูล เป็นต้น<br>3.3.2.2 สถาบันการเงินเข้ารหัสข้อมูลลับทุกครั้ง ในขณะรับส่งผ่านเครือข่ายสาธารณะหรือเครือข่ายที่ไม่น่าเชื่อถือ เช่น Internet เป็นต้น<br>3.3.2.3 สถาบันการเงินเข้ารหัสสื่อบันทึกข้อมูลของอุปกรณ์คอมพิวเตอร์ (Endpoint Devices) ตามระดับความเสี่ยง เช่น เครื่องคอมพิวเตอร์ปฏิบัติงาน (Workstation) เครื่องคอมพิวเตอร์พกพา (Laptops) และอุปกรณ์พกพา (Mobile Devices) หรือสื่อบันทึกข้อมูลอื่นที่ใช้บันทึกข้อมูลที่เป็นความลับ<br>3.3.2.4 สถาบันการเงินทำการปกปิดหรือลบข้อมูลในส่วนสำคัญของลูกค้า (Sensitive Data) ก่อนนำไปใช้งานใน Non-production Environment เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญของลูกค้าและเป็นไปตามที่กฎหมาย หลักเกณฑ์ของทางการ และนโยบายที่สถาบันการเงินกำหนดไว้ |
| Intermediate | 3.3.2.5 สถาบันการเงินมีเครื่องมือป้องกันการเข้าถึง หรือนำข้อมูลลับออกจากสถาบันการเงินโดยไม่ได้รับอนุญาต |
| Advanced | 3.3.2.6 สถาบันการเงินเข้ารหัสข้อมูลลับในระหว่างการรับส่งข้อมูลผ่านเครือข่ายภายในสถาบันการเงิน |

**3.3.3 การทำลายข้อมูล (Data Disposal)**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.3.3.1 สถาบันการเงินกำหนดระเบียบวิธีปฏิบัติการทำลายข้อมูลสารสนเทศ (Information Disposal) ครอบคลุมขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการทำลายข้อมูลที่สอดคล้องกับระดับความสำคัญของข้อมูล โดยมีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูลก่อนดำเนินการ การควบคุมการทำลายในลักษณะ Dual Control การสอบทานการปฏิบัติงานโดยหัวหน้างาน รวมทั้งจัดทำทะเบียนการทำลายข้อมูลสำคัญ โดยระบุผู้รับผิดชอบในการทำลายข้อมูล วันที่ เวลา ชนิดของสื่อบันทึกข้อมูล Serial Number และวิธีการที่ใช้ทำลายข้อมูล |

## 3.4 กระบวนการพัฒนาโปรแกรมให้มั่นคงปลอดภัย

### 3.4.1 กระบวนการพัฒนาโปรแกรมให้มั่นคงปลอดภัย (Secure Development)

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.4.1.1 สถาบันการเงินกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (Secure Coding) และสอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติดังกล่าว<br>3.4.1.2 สถาบันการเงินจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) ให้ครอบคลุมการควบคุมการรักษาความปลอดภัย (Security Control) ตามนโยบาย/มาตรฐานที่สถาบันการเงินกำหนด<br>3.4.1.3 สถาบันการเงินทบทวนและทดสอบการควบคุมด้านการรักษาความปลอดภัย (Security Control) ตามระดับความเสี่ยงของโปรแกรมที่พัฒนาก่อนนำไปใช้งานจริง<br>3.4.1.4 สถาบันการเงินจัดทำ Vulnerabilities Assessment เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริงและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ<br>3.4.1.5 สถาบันการเงินจัดทำ Penetration Testing โดยเฉพาะระบบงานที่เชื่อมต่อกับภายนอกทุกครั้งก่อนนำไปใช้งานจริงและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ<br>3.4.1.6 สถาบันการเงินมีการจัดทำ Source Code Review ทุกครั้งที่มีการพัฒนา/เปลี่ยนแปลงระบบที่สำคัญ รวมถึงระบบ Internet Banking และ Mobile Banking เพื่อระบุช่องโหว่ด้านความมั่นคงปลอดภัย และปิดช่องโหว่ที่พบทุกครั้งก่อนนำไปใช้งานจริง<br>3.4.1.7 สถาบันการเงินควรจัดให้มีการทดสอบประสิทธิภาพ (Performance Test) ของระบบที่เกี่ยวข้องกับการให้บริการ/ทำธุรกรรมทางอิเล็กทรอนิกส์หรือระบบที่มีการเชื่อมโยงกับระบบอื่นจำนวนมาก เพื่อให้มั่นใจว่าระบบมีเสถียรภาพในการรองรับการใช้งานจำนวนมาก<br>3.4.1.8 สถาบันการเงินมีกระบวนการประเมินความจำเป็นในการจัดทำสัญญาและข้อตกลงการรับฝากทรัพย์สิน (Escrow Agreement) ในระบบงานสำคัญ |

## 3.5 การบริหารจัดการ Patch (Patch Management)

### 3.5.1 กระบวนการและเครื่องมือในการบริหารจัดการ Patch

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.5.1.1 สถาบันการเงินมีการบริหารจัดการเพื่อปรับปรุง Patch ของระบบปฏิบัติการ (Operation System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication) ในระยะเวลาที่เหมาะสมตามระดับความเสี่ยง<br>3.5.1.2 สถาบันการเงินมีวิธีการรับ Patch ใหม่ ๆ จากแหล่งที่เชื่อถือได้ เพื่อใช้เตรียมการปรับปรุงการตั้งค่า ของระบบปฏิบัติการ (Operation System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication)<br>3.5.1.3 สถาบันการเงินมีกระบวนการหรือเครื่องมือเพื่อใช้ในการระบุ จัดลำดับความสำคัญ และติดตาม Patch ด้านการรักษาความปลอดภัยที่ยังไม่มีการติดตั้ง รวมถึงมีมาตรการควบคุมความเสี่ยงอย่างรัดกุมในส่วนที่ยังไม่ได้ติดตั้ง Patch |
| Advanced | 3.5.1.4 สถาบันการเงินติดตั้ง Patch Monitoring Software ที่ใช้ติดตาม Patch ด้านการรักษาความปลอดภัยที่ยังไม่มีการติดตั้งของระบบปฏิบัติการ (Operation System) ระบบงาน (Application System) และระบบฐานข้อมูล (Database System) ที่สำคัญ<br>3.5.1.5 สถาบันการเงินทบทวนและปรับปรุงกระบวนการบริหารจัดการ Patch เพื่อให้มั่นใจได้ว่าสถาบันการเงินสามารถทดสอบและติดตั้ง Patch ด้านการรักษาความปลอดภัย ได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว |

### 3.5.2 การประเมินและทดสอบ Patch

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.5.2.1 สถาบันการเงินมีกระบวนการในการจัดหา ทดสอบ และติดตั้ง Patch ตามระดับความสำคัญ<br>3.5.2.2 สถาบันการเงินกำหนดให้ทดสอบ Patch ที่ออกใหม่ทุกครั้ง ก่อนนำไปติดตั้งบนระบบงานจริง |
| Intermediate | 3.5.2.3 สถาบันการเงินทดสอบและติดตั้ง Patch สำหรับช่องโหว่ที่มีความเสี่ยงสูงทันทีที่ Patch ได้ถูกเผยแพร่ออกมาหรือภายในกรอบเวลาตามที่สถาบันการเงินสามารถยอมรับความเสี่ยงได้ |

## 3.6 การบริหารจัดการประเด็นที่ตรวจพบ (Remediation Management)

### 3.6.1 การบริหารจัดการประเด็น (Issues Management)

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 3.6.1.1 สถาบันการเงินจัดลำดับความสำคัญของประเด็นที่พบจากการประเมินช่องโหว่ด้านไซเบอร์จากการประเมินช่องโหว่ (Vulnerabilites Assessment) และการทดสอบเจาะระบบ (Penetration Test) และปรับปรุงแก้ไขตามกรอบเวลาที่กำหนด<br>3.6.1.2 สถาบันการเงินทำการทดสอบซ้ำอีกครั้ง (Re-test) เพื่อตรวจสอบว่าผลจากการประเมินช่องโหว่ (Vulnerabilites Assessment) และการทดสอบเจาะระบบ (Penetration Test) ที่เคยพบ ได้รับการแก้ไขแล้ว<br>3.6.1.3 สถาบันการเงินบันทึกและสอบทานรายละเอียดการบำรุงรักษาหรือซ่อมแซมอุปกรณ์คอมพิวเตอร์ของ สถาบันการเงิน ในเวลาที่เหมาะสม |
| Advanced | 3.6.1.4 สถาบันการเงินกำหนดให้การบำรุงรักษาหรือซ่อมแซมอุปกรณ์คอมพิวเตอร์ของสถาบันการเงินต้องดำเนินการโดยบุคลากรและเครื่องมือที่ได้รับอนุญาตซึ่งอยู่ภายใต้การควบคุมของ สถาบันการเงิน |

## 4. การตรวจจับ (Detection)

**วัตถุประสงค์ :** เพื่อให้สถาบันการเงินมีกระบวนการบริหารจัดการและมาตรการในการตรวจหาช่องโหว่หรือจุดอ่อนของระบบงาน เพื่อให้ทราบถึงช่องโหว่ด้านการรักษาความมั่นคงปลอดภัยของระบบ และสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันการณ์ มีการบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management) เพื่อติดตามและรายงานพฤติกรรมที่ผิดปกติได้อย่างทันกาล และมีการแลกเปลี่ยนองค์ความรู้ภัยคุกคามทางไซเบอร์ภายในองค์กรและการสร้างความร่วมมือกับหน่วยงานภายนอกเพื่อประโยชน์ในการสร้างความร่วมมือกับการรับมือภัยไซเบอร์และสามารถระงับเหตุการณ์ที่อาจเกิดขึ้นได้

### 4.1 การตรวจช่องโหว่

#### 4.1.1 การตรวจหาและกำจัดไวรัสและมัลแวร์

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.1.1.1 สถาบันการเงินติดตั้ง Anti-Malware บนอุปกรณ์คอมพิวเตอร์ และมีการปรับปรุงโปรแกรม Anti-Malware ให้เป็นปัจจุบันโดยอัตโนมัติ<br>4.1.1.2 สถาบันการเงินมีกระบวนการบริหารจัดการหรือมาตรการคัดกรอง (Filter) ภัยคุกคามทางไซเบอร์ที่ปะปนมากับ Email เช่น โปรแกรม Malware หรือ Email ที่ส่งมาจากผู้ส่งที่น่าสงสัย เป็นต้น |
| Intermediate | 4.1.1.3 สถาบันการเงินมีเครื่องมือตรวจหา (Scan) และปิดกั้น (Block) โปรแกรม Malware ที่แฝงมากับ Email และ เอกสารแนบโดยอัตโนมัติ |

#### 4.1.2 การประเมินช่องโหว่ และการทดสอบเจาะระบบ

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.1.2.1 สถาบันการเงินจัดทำ Vulnerabilities Assessment ครอบคลุมระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบงานสำคัญ (Critical System) ควรจัดทำอย่างน้อยปีละ 1 ครั้ง และรายงานไปยังผู้ที่รับผิดชอบ เพื่อดำเนินการแก้ไขหรือปิดช่องโหว่อย่างเหมาะสม<br>4.1.2.2 สถาบันการเงินจัดทำ Penetration Testing ครอบคลุมระบบงานที่เชื่อมต่อกับภายนอกอย่างน้อยปีละ 1 ครั้ง โดยผู้เชี่ยวชาญ และมีการรายงานไปยังผู้ที่รับผิดชอบ เพื่อดำเนินการแก้ไขหรือปิดช่องโหว่อย่างเหมาะสม<br>4.1.2.3 สถาบันการเงินมีกระบวนการปรับปรุงแก้ไขช่องโหว่หรือจุดอ่อนที่ตรวจพบจากการทำ Vulnerabilites Assessment, Penetration Testing และ Source Code Review อย่างชัดเจน |
| Intermediate | 4.1.2.4 หน่วยงานอิสระ เช่น หน่วยงานตรวจสอบภายใน หรือหน่วยงานบริหารความเสี่ยง ประเมินขอบเขต กระบวนการ คุณภาพผู้ทดสอบ และผลของการทดสอบเจาะระบบเพื่อประเมินคุณภาพการจัดทำ และติดตามควบคุมดูแลให้มีการแก้ไขช่องโหว่ให้อยู่ในกรอบเวลาที่กำหนด |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Advanced | 4.1.2.5 สถาบันการเงินมีกระบวนการทดสอบเจาะระบบในลักษณะ Red Team ที่ครอบคลุมการบริหารจัดการ กระบวนการป้องกัน ตรวจจับ รับมือ กู้คืน รวมถึงรวมข้อมูลการรายงานเหตุการณ์จากการถูกโจมตีหรือภัยคุกคามทางไซเบอร์ จาก Cyber Threat Intelligence มาออกแบบสถานการณ์จำลองให้อยู่ในรูปแบบเสมือนจริง (Simulation Cyber Attack) และมีการทดสอบเจาะระบบโดยไม่มีการแจ้งเตือนหน่วยงานเฝ้าระวังการรักษาความมั่นคงปลอดภัยล่วงหน้า (Silent Mode) เพื่อให้มั่นใจได้ว่าสถาบันการเงินสามารถรับมือเมื่อมีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้นจริง ซึ่งสถาบันการเงินสามารถอ้างอิงตามแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่อง การทดสอบเจาะระบบแบบ Intelligence-led Penetration Testing (iPentest) |

## 4.2 การตรวจจับกิจกรรมที่ผิดปกติ (Anomalies Activity Detection)

### 4.2.1 การติดตามและวิเคราะห์บันทึกเหตุการณ์ (Log Monitoring and Analysis)

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.2.1.1 สถาบันการเงินจัดให้มีการจัดเก็บบันทึกเหตุการณ์ (Log)<br>● บันทึกการเข้าถึง (Access Log)<br>● บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ<br>● บันทึกร่องรอยกิจกรรมการทำธุรกรรม (Transaction Log)<br>● บันทึกด้านการรักษาความปลอดภัย (Security Event Log)<br>โดยบันทึกดังกล่าวต้องถูกจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด ด้วยวิธีการที่ปลอดภัย<br>4.2.1.2 ข้อมูลการบันทึกเหตุการณ์ ถูกจัดเก็บไว้ที่เครื่องแม่ข่ายที่แยกเฉพาะ และมีการควบคุมการเข้าถึง เพื่อป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ<br>4.2.1.3 สถาบันการเงินมีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสาร ให้ตรงกับเครื่องเซิร์ฟเวอร์ Network Time Protocol:NTP (Clock Synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์ (Log) มีความถูกต้องในลักษณะ Real-Time ซึ่งเครื่องเซิร์ฟเวอร์ NTP ต้องรับสัญญาณนาฬิกาจากสถาบันที่มีความน่าเชื่อถือ ยกตัวอย่างเช่น กรมอุทกศาสตร์ (กองทัพเรือ) หรือ สถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี) เป็นต้น |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 4.2.1.4 สถาบันการเงินมีการสอบทาน Access Log และ Activity Log ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูงอย่างสม่ำเสมอ เช่น System Administrator, System Operator เป็นต้น เพื่อให้มั่นใจได้ว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย<br>4.2.1.5 สถาบันการเงินมีกระบวนการหรือระบบ ที่สามารถเฝ้าระวังหรือติดตามพฤติกรรมการเข้าใช้งานระบบของพนักงานและบุคคลภายนอก (3rd Party) รวมถึงแจ้งเตือนผู้ที่รับมอบอำนาจทันทีเมื่อมีพฤติกรรมที่น่าสงสัย เพื่อดำเนินการแก้ไขอย่างทันการณ์ |

**4.2.2 การบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management)**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.2.2.1 สถาบันการเงินมีกระบวนการในการตรวจจับการเข้าถึงระบบงานสำคัญ (Critical System) เพื่อตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาต หรือการพยายามเข้าถึงอย่างผิดปกติ<br>4.2.2.2 สถาบันการเงินมีการกำหนดความเหมาะสมและประเมินการตั้งค่าที่แสดงความผิดปกติ (Thresholds) สำหรับข้อมูลการบันทึกเหตุการณ์ (Log) อย่างสม่ำเสมอ เพื่อติดตามและรายงานพฤติกรรมที่ผิดปกติได้อย่างทันกาล<br>4.2.2.3 สถาบันการเงินมีมาตรการควบคุมเชิงเทคนิคที่ใช้ Defense-in-Depth ตรวจจับและรับมือการโจมตีระบบเครือข่ายที่อาจมีรูปแบบของการรับส่งข้อมูลเข้าออกที่ผิดปกติ และ/หรือการโจมตีแบบ DDoS ได้อย่างทันกาล |
| Intermediate | 4.2.2.4 สถาบันการเงินมีเครื่องมือสำหรับตรวจจับเหตุการณ์ผิดปกติที่เกิดขึ้นกับระบบ และแจ้งเตือนไปยังผู้ที่รับผิดชอบโดยอัตโนมัติเมื่อถึง Thresholds ที่กำหนดไว้ เพื่อดำเนินการแก้ไขอย่างทันท่วงที<br>4.2.2.5 สถาบันการเงินมีระบบหรือเครื่องมือติดตามกิจกรรมที่ผิดปกติหรืออาจเข้าข่ายที่ผิดปกติ (Potential and unusual insider activities) ที่อาจนำไปสู่การขโมยข้อมูลหรือทำลายข้อมูล |
| Advanced | 4.2.2.6 สถาบันการเงินมีเครื่องมือเพื่อนำข้อมูลกิจกรรมที่ผิดปกติและการแจ้งเตือนจากระบบและเครือข่ายต่าง ๆ มาใช้เชื่อมโยงเพื่อตรวจจับและป้องกันการโจมตีในลักษณะ Multi-Faceted เช่น Simultaneous Account Takeover และ DDoS attack เป็นต้น<br>4.2.2.7 สถาบันการเงินมีระบบการติดตามและวิเคราะห์เพื่อใช้แจ้งเตือนพฤติกรรมที่ผิดปกติของผู้ใช้งานตามระดับความเสี่ยง เช่น การใช้งานระบบเครือข่าย การทำงานนอกเวลาทำการ หรือการใช้อุปกรณ์ที่ไม่ได้รับอนุญาต เป็นต้น |

### 4.2.3 การติดตามธุรกรรมของลูกค้า

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.2.3.1 สถาบันการเงินมีการเฝ้าระวังและติดตามพฤติกรรมการดำเนินการใด ๆ ที่น่าสงสัยและ/หรือเข้าข่ายเป็นการทุจริตของลูกค้า เช่น การทุจริตในขั้นตอนการพิสูจน์ตัวตน การเปลี่ยนแปลงข้อมูลส่วนตัวหรือวงเงินการทำรายการ และการทำธุรกรรมทางอิเล็กทรอนิกส์<br>4.2.3.2 สถาบันการเงินมีระบบในการติดตามและแจ้งเตือน เมื่อพบรายการการนำเงินออกจากบัญชีลูกค้าที่ผิดปกติ โดยมีการแจ้งเตือนให้ลูกค้ารับทราบก่อนหรือหลังการทำธุรกรรมดังกล่าวทันที |
| Intermediate | 4.2.3.3 สถาบันการเงินมีเครื่องมือแจ้งเตือนโดยอัตโนมัติ เมื่อพบพฤติกรรมของลูกค้าที่ผิดปกติ เช่น ลูกค้า Log in เข้าใช้ระบบงาน จาก IP Address ในสถานที่ที่แตกต่างกันในช่วงเวลาใกล้เคียงกัน เป็นต้น |

## 4.3 การตรวจจับเหตุการณ์ผิดปกติทางไซเบอร์

### 4.3.1 การเฝ้าระวังเหตุการณ์

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.3.1.1 สถาบันการเงินมีกระบวนการเฝ้าระวัง การเข้าใช้งานโดยผู้ที่ไม่ได้รับอนุญาต การเชื่อมต่อกับระบบของสถาบันการเงินด้วยอุปกรณ์ที่ไม่ได้รับอนุญาต และการติดตั้ง Software ที่ไม่ได้รับอนุญาต<br>4.3.1.2 สถาบันการเงินกำหนดบทบาทและหน้าที่ความรับผิดชอบในการติดตาม ดูแล และรายงานการถูกคุกคามทางไซเบอร์ รวมทั้งกิจกรรมต้องสงสัย<br>4.3.1.3 สถาบันการเงินเฝ้าระวังตรวจหาการบุกรุกพื้นที่โดยไม่ได้รับอนุญาต เช่น การเฝ้าระวังผ่านระบบกล้องวงจรปิด (CCTV) ตลอดเวลา เป็นต้น<br>4.3.1.4 สถาบันการเงินมีกระบวนการเฝ้าระวังเหตุการณ์ต่างๆ โดยเชื่อมโยงข้อมูลจากหลายแหล่ง เช่น จากระบบเครือข่าย ระบบงาน และ Firewall เป็นต้น<br>4.3.1.5 สถาบันการเงินมีมาตรการเฝ้าระวังการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่สำคัญ (Critical System) และทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง |
| Intermediate | 4.3.1.6 สถาบันการเงินมี Security Operations Center (SOC) หรือหน่วยงานที่เทียบเท่า รับผิดชอบในการเฝ้าระวัง ติดตาม วิเคราะห์ ประสานงาน และเป็นศูนย์กลางในการจัดการเหตุการณ์ผิดปกติทางไซเบอร์<br>4.3.1.7 สถาบันการเงินมีเครื่องมือตรวจจับการรับส่งข้อมูลสำคัญผ่านช่องทางต่าง ๆ ซึ่งอาจมีความเสี่ยงต่อการรั่วไหลข้อมูลสำคัญ เช่น ระบบ Data Loss Prevention หรือ Data Leak Prevention เป็นต้น |

**4.3.2 การตรวจจับและแจ้งเตือน (Detect and Alert)**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.3.2.1 สถาบันการเงินมีกระบวนการหรือมาตรการแจ้งเตือนเมื่อพบเหตุการณ์ที่มีโอกาสเป็นการโจมตีทางไซเบอร์ เช่น Antivirus Alert, Log Event Alerts เป็นต้น เพื่อให้หน่วยงานหรือผู้รับผิดชอบในการเฝ้าระวังด้านการรักษาความมั่นคงปลอดภัยทราบอย่างทันกาล<br>4.3.2.2 สถาบันการเงินกำหนดค่าพารามิเตอร์ที่ใช้ในการตรวจจับเหตุการณ์ผิดปกติทางไซเบอร์เพื่อสามารถแก้ไขเหตุการณ์ได้อย่างทันกาล<br>4.3.2.3 รายงาน System Performance รวมถึง Network Utilization มีข้อมูลที่สะท้อนความเสี่ยงในการตรวจจับเหตุการณ์ผิดปกติทางไซเบอร์<br>4.3.2.4 สถาบันการเงินมีเครื่องมือและกระบวนการในการตรวจจับและแจ้งเตือน เมื่อตรวจพบพฤติกรรมหรือเหตุการณ์ที่ผิดปกติ เพื่อรายงานให้หน่วยงานหรือผู้มีหน้าที่รับผิดชอบในการรับมือเหตุการณ์ผิดปกติทางไซเบอร์ทราบและดำเนินการแก้ไข |
| Intermediate | 4.3.2.5 สถาบันการเงินมีเครื่องมือหรือกระบวนการที่สามารถตรวจจับการพยายามบุกรุกเครือข่ายที่อาจจะสร้างความเสียหายต่อสถาบันการเงิน<br>4.3.2.6 สถาบันการเงินมีเครื่องมือตรวจจับเหตุการณ์ผิดปกติ (incident) และสามารถแจ้งเตือนไปยังหน่วยงานหรือผู้ที่เกี่ยวข้องให้รับมือได้ทันกาล |
| Advanced | 4.3.2.7 สถาบันการเงินมีเครื่องมือที่สามารถตรวจจับโดยอัตโนมัติ เมื่อมีการเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบโดยไม่ได้รับอนุญาต เช่น การแก้ไขค่าความปลอดภัยของ System file ที่สำคัญ อุปกรณ์เครือข่าย หรืออุปกรณ์รักษาความปลอดภัยเครือข่าย เป็นต้น<br>4.3.2.8 สถาบันการเงินมีเครื่องมือที่สามารถติดตามภัยคุกคามที่ซับซ้อนแบบอัตโนมัติ สามารถตรวจจับและแจ้งเตือนเหตุการณ์ตามความเสี่ยงไปยังผู้รับผิดชอบที่เกี่ยวข้องได้ทันที<br>4.3.2.9 สถาบันการเงินมีเครื่องมือวิเคราะห์เชื่อมโยงข้อมูลเหตุการณ์จากแหล่งต่าง ๆ ของสถาบันการเงิน แบบ Real Time จากอุปกรณ์เครือข่ายหรืออุปกรณ์รักษาความปลอดภัยเครือข่ายของระบบที่สำคัญ เช่น Firewall, IPS, IDS เป็นต้น และสามารถแจ้งเตือนได้ตามเงื่อนไขที่สถาบันการเงินกำหนด<br>4.3.2.10 สถาบันการเงินมีเครื่องมือที่สามารถตรวจจับภัยคุกคามจากภายในและภายนอกที่เชื่อมโยงในระดับองค์กร รวมถึงแจ้งเตือนหน่วยงานที่รับผิดชอบและหน่วยงานที่เกี่ยวข้อง เพื่อให้ดำเนินการแก้ไขตามแนวทางการรับมือที่เครื่องมือแจ้งมาในเบื้องต้น |

## 4.4 การตระหนักถึงสถานการณ์ความเสี่ยง

### 4.4.1 การรวบรวมองค์ความรู้ภัยคุกคามทางไซเบอร์

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.4.1.1 สถาบันการเงินมอบหมายให้มีหน่วยงานหรือผู้รับผิดชอบในการรวบรวมและวิเคราะห์ Cyber Threat Intelligence เพื่อให้มีข้อมูลภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่และแนวทางดำเนินการ เพื่อเป็นประโยชน์ในการป้องกัน ติดตาม และรับมือกับเหตุการณ์ทางไซเบอร์อย่างมีประสิทธิภาพ<br>4.4.1.2 สถาบันการเงินเป็นสมาชิกหรือใช้บริการหน่วยงานที่ให้บริการ Cyber Threat Intelligence ซึ่งให้ข้อมูลข่าวสาร ผลการวิเคราะห์ วิธีการรูปแบบ และข้อเสนอแนะในการลดและควบคุมความเสี่ยงจากภัยคุกคามทางไซเบอร์ |
| Intermediate | 4.4.1.3 สถาบันการเงินจัดให้มีกระบวนการรวบรวมข้อมูลภัยคุกคาม (Threat Feed) ทั้งจากแหล่งข้อมูลภายในและจากภายนอก<br>4.4.1.4 สถาบันการเงินมีหลักเกณฑ์ในการรวบรวมข้อมูล Cyber Threat Intelligence เช่น ความถี่ ประเภทช่องทางในการรับ และการจัดลำดับความสำคัญของข้อมูล (Data Classification) เป็นต้น<br>4.4.1.5 สถาบันการเงินมีการจัดเก็บ Cyber Threat Intelligence แบบศูนย์กลาง (Central Repository) เพื่อประโยชน์ในการใช้งาน และสามารถควบคุมไม่ให้มีการแก้ไขข้อมูล |
| Advanced | 4.4.1.6 สถาบันการเงินมีระบบที่สามารถรวบรวม Cyber Threat Intelligence จากแหล่งต่างๆ แบบ Real-time ได้โดยอัตโนมัติ<br>4.4.1.7 สถาบันการเงินจัดลำดับความสำคัญของแหล่งข้อมูล Threat Intelligence เพื่อใช้ในการติดตาม<br>4.4.1.8 Threat Intelligence ควรครอบคลุมถึงข้อมูลเหตุการณ์ทางการเมืองระหว่างประเทศที่อาจกระทบกับความเสี่ยงด้านไซเบอร์ |

### 4.4.2 การติดตามและวิเคราะห์ภัยคุกคาม

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.4.2.1 สถาบันการเงินมีกระบวนการติดตาม Cyber Threat Intelligence เพื่อตรวจพบภัยคุกคามทางไซเบอร์รูปแบบใหม่ |
| Advanced | 4.4.2.2 สถาบันการเงินมีระบบวิเคราะห์ภัยคุกคาม (Threat analysis system) ที่สามารถเชื่อมโยงข้อมูลภัยคุกคามต่างๆ และแจ้งเตือนไปยังผู้รับผิดชอบที่เกี่ยวข้อง ตามระดับความเสี่ยงที่เกิดขึ้นได้<br>4.4.2.3 สถาบันการเงินนำผลการวิเคราะห์ Threat Intelligence จัดทำรายงานสรุปภัยคุกคามทางไซเบอร์ ความเสี่ยงด้านไซเบอร์และแนวทางการรับมือภัยคุกคามดังกล่าว |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 4.4.2.4 สถาบันการเงินนำผลการวิเคราะห์ Threat Intelligence ปรับปรุงข้อมูล Risk Profile ขององค์กรและระดับความเสี่ยงที่ยอมรับได้ เพื่อจัดลำดับความสำคัญของมาตรการลดความเสี่ยงของภัยคุกคามทางไซเบอร์<br>4.4.2.5 สถาบันการเงินนำผลการวิเคราะห์ Threat Intelligence ปรับปรุงสถาปัตยกรรมการรักษาความมั่นคงปลอดภัย (IT Security Architecture) และการกำหนดมาตรฐานการตั้งค่าระบบเทคโนโลยีสารสนเทศ<br>4.4.2.6 สถาบันการเงินนำผลการวิเคราะห์ Threat Intelligence มาคาดการณ์แนวโน้มและรูปแบบของภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต |

**4.4.3 การแลกเปลี่ยนองค์ความรู้ภัยคุกคามทางไซเบอร์ภายในองค์กร**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.4.3.1 สถาบันการเงินมีแนวทางการสื่อสารข้อมูลด้าน Cyber Threat Intelligence และเหตุการณ์ผิดปกติทางไซเบอร์ ให้แก่พนักงานที่เกี่ยวข้อง |
| Intermediate | 4.4.3.2 ผู้บริหารระดับสูงของสถาบันการเงินมีการสื่อสารข้อมูลด้าน Cyber Threat Intelligence ที่อาจส่งผลกระทบต่อความเสี่ยงด้านธุรกิจ และให้ข้อแนะนำเพื่อการบริหารจัดการความเสี่ยงเหล่านั้นให้หน่วยงานธุรกิจที่เกี่ยวข้องรับทราบ |

**4.4.4 การสร้างความร่วมมือกับหน่วยงานภายนอก**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 4.4.4.1 สถาบันการเงินจัดทำทะเบียนข้อมูลผู้ประสานงานของหน่วยงานต่าง ๆ เช่น หน่วยงานกำกับดูแล หรือหน่วยงานภาครัฐอื่น ๆ เป็นต้น พร้อมทั้งทบทวนให้เป็นปัจจุบันอยู่เสมอ<br>4.4.4.2 สถาบันการเงินแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับหน่วยงานกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องตามความจำเป็น เพื่อประโยชน์ในการสร้างความร่วมมือกับการรับมือภัยไซเบอร์<br>4.4.4.3 สถาบันการเงินมีกระบวนการที่มั่นคงปลอดภัย ในการแลกเปลี่ยนข้อมูลภัยคุกคามและช่องโหว่กับหน่วยงานภายนอก<br>4.4.4.4 สถาบันการเงินมีตัวแทนเข้ามีส่วนร่วมเพื่อแลกเปลี่ยนข้อมูล Cyber Threat Intelligence อย่างสม่ำเสมอ โดยอย่างน้อยต้องมีส่วนร่วมการแลกเปลี่ยนข้อมูลด้าน Cyber Threat Intelligence ที่จัดตั้งโดยสมาคมธนาคารไทย |
| Advanced | 4.4.4.5 สถาบันการเงินมีการจัดทำข้อตกลงอย่างเป็นลายลักษณ์อักษรในการแลกเปลี่ยน Cyber Threat Intelligence กับสถาบันการเงินหรือหน่วยงานภายนอกอื่น<br>4.4.4.6 สถาบันการเงินแลกเปลี่ยนข้อมูล Cyber Threat Intelligence ในเชิงรุกให้แก่สถาบันการเงินอื่น หน่วยงานกำกับดูแลหรือหน่วยงานที่บังคับใช้กฎหมาย โดยทันทีเมื่อพบข้อมูลภัยคุกคามทางไซเบอร์ที่อาจจะกระทบต่อระบบสถาบันการเงิน |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 4.4.4.7 สถาบันการเงินมีกระบวนการในการสื่อสารและร่วมมือเกี่ยวกับภัยคุกคามทางไซเบอร์กับหน่วยงานภายนอก รวมถึงมีการสื่อสารต่อสาธารณะตามความเหมาะสมเมื่อมีความจำเป็น |

## 5. การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ (Response and Recovery)

**วัตุประสงค์ :** เพื่อให้สถาบันการเงินมีแผน มาตรฐาน และระเบียบวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่อาจส่งผลกระทบให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ และสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายใต้ระยะเวลาที่ยอมรับได้

### 5.1 การเตรียมการเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Response Planning)

#### 5.1.1 การวางแผนการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 5.1.1.1 สถาบันการเงินมีแผน มาตรฐาน และระเบียบวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ซึ่งรวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital (Digital Forensics) ไว้อย่างชัดเจน<br>5.1.1.2 สถาบันการเงินมีการจัดทำแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) สำหรับภัยไซเบอร์สำคัญที่สถาบันการเงินมีโอกาสเผชิญ โดยการจัดทำแผนมีการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบเพื่อให้สามารถใช้อ้างอิงในการรับมือภัยคุกคาม ตอบสนองต่อเหตุการณ์ และกู้คืนระบบและข้อมูลได้อย่างรวดเร็วและทันการณ์<br>5.1.1.3 สถาบันการเงินมีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์และเชื่อมโยงกับแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยการจัดทำอย่างน้อยครอบคลุมกระบวนการ ดังนี้<br>● การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)<br>● การประเมินความเสี่ยง (Risk Analysis)<br>● การวางกลยุทธ์สำหรับแผนฉุกเฉิน<br>● การจัดทำแผนฉุกเฉิน<br>● การสื่อสารและฝึกอบรมให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอก<br>● การทดสอบ ปรับปรุง และสอบทานแผนฉุกเฉิน<br>5.1.1.4 การจัดทำแผนฉุกเฉินดังกล่าวให้อ้างอิงตามแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Implementation Guideline) |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| | 5.1.1.5 แผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) สอดคล้องและเชื่อมโยงกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) และแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP)<br>5.1.1.6 สถาบันการเงินนำสิ่งที่ได้เรียนรู้ (Lessons learned) จากการถูกโจมตีหรือจากที่มีเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้นทั้งภายในและภายนอกสถาบันการเงินมาปรับปรุงแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ แผน IT DRP และ แผน BCP<br>5.1.1.7 สถาบันการเงินมีการทบทวนแผนฉุกเฉินที่รองรับภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยคำนึงถึงเหตุการณ์ความเสียหายครอบคลุมสถานการณ์จำลองต่าง ๆ ที่อาจเกิดขึ้น รวมถึงเหตุการณ์จากภัยไซเบอร์ที่อาจส่งผลกระทบรุนแรง อย่างน้อยครอบคลุมเหตุการณ์ ดังนี้<br>● ระบบงานสำคัญที่ศูนย์คอมพิวเตอร์หลัก และศูนย์สำรองไม่สามารถใช้งานได้พร้อมกัน<br>● ข้อมูลจริงและข้อมูลชุดสำรองไม่สามารถใช้งานได้<br>5.1.1.8 การเปลี่ยนแปลงกระบวนการทำงาน ระบบงาน หรือสิทธิ์ผู้ใช้งาน ที่เกี่ยวข้องกับการจัดการเหตุการณ์ผิดปกติทางไซเบอร์ต้องได้รับการอนุมัติจากผู้บริหารก่อนนำไปใช้ปฏิบัติงานจริง |
| Intermediate | 5.1.1.9 สถาบันการเงินมีการประเมินประสิทธิภาพ ความพร้อมและศักยภาพของเครื่องมือ บุคลากรและบริการของบุคคลภายนอก ผู้เชี่ยวชาญ หรือที่ปรึกษา (Due Diligence) อย่างสม่ำเสมอ เพื่อให้มั่นใจในความพร้อมของการให้บริการเมื่อมีเหตุการณ์ผิดปกติทางไซเบอร์เกิดขึ้น |

**5.1.2 การทดสอบความพร้อมรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์**

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 5.1.2.1 สถาบันการเงินทดสอบความสามารถในการกู้คืนข้อมูลจากชุดข้อมูลสำรอง และความถูกต้องของการประมวลผลระบบงานและข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลสำรองมีความครบถ้วนถูกต้องสามารถนำมาใช้งานได้เมื่อมีเหตุการณ์ผิดปกติทางไซเบอร์เกิดขึ้นจริง<br>5.1.2.2 สถาบันการเงินจัดให้มีการทดสอบแผนในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) ที่ครอบคลุมระบบงานด้านเทคโนโลยีสารสนเทศที่สำคัญของสถาบันการเงิน<br>5.1.2.3 สถาบันการเงินจัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ( IT DRP) ที่ครอบคลุมภัยคุกคามทางไซเบอร์ และระบบงานสำคัญระบบที่เชื่อมต่อกับบุคคลภายนอกที่เกี่ยวข้อง โดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการลูกค้าหรือต่อสถาบันการเงินทั้งระบบ เช่น ระบบเงินฝาก ระบบการโอนและชำระเงินระหว่างธนาคาร เป็นต้น นอกจากนี้ มีการทดสอบระบบสำรองในลักษณะเสมือนจริง (DR live test) เพื่อให้มั่นใจว่าระบบสำรองสามารถรองรับธุรกิจให้สามารถดำเนินได้อย่างต่อเนื่อง |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Intermediate | 5.1.2.4 สถาบันการเงินทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีโอกาสเกิดขึ้น โดยให้ครอบคลุมตามสถานการณ์จำลอง (Scenario) ที่สะท้อนภัยคุกคามทางไซเบอร์รูปแบบใหม่ ๆ ที่มีโอกาสเกิดขึ้นกับสถาบันการเงิน โดยมีการทดสอบในรูปแบบต่าง ๆ เช่น ลักษณะ table top หรือการจำลองการโจมตีทางไซเบอร์ (Cyber War Game/Cyber Simulation) เป็นต้น<br>5.1.2.5 สถาบันการเงินนำผลการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ IT (DRP) และแผนในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) มาทบทวนและปรับปรุงกระบวนการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่เกี่ยวข้องทั้งหมดให้มีประสิทธิภาพยิ่งขึ้น |
| Advanced | 5.1.2.6 สถาบันการเงินทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ ครอบคลุมธุรกรรมสำคัญและเชื่อมโยงไปยังธุรกิจหรือองค์กรที่เกี่ยวข้อง<br>5.1.2.7 สถาบันการเงินมีการทดสอบการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident response) ที่ซับซ้อน ซึ่งเคยเกิดขึ้นกับองค์กรอื่น เพื่อให้มั่นใจในความพร้อมของสถาบันการเงินในการรองรับสถานการณ์ในลักษณะเดียวกัน<br>5.1.2.8 สถาบันการเงินจัดให้มีกระบวนการหาสาเหตุที่แท้จริง (Root Cause) ของปัญหาที่พบในระหว่างการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) การทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ เพื่อใช้ประโยชน์ในการแก้ไขปัญหาในภายหลัง<br>5.1.2.9 สถาบันการเงินมีการทดสอบศักยภาพ (Stress Test) ในการบริหารจัดการความเสี่ยงด้านไซเบอร์ โดยใช้สถานการณ์จำลองเหตุการณ์ผิดปกติทางไซเบอร์ที่ส่งผลกระทบต่อการให้บริการของระบบ หรือก่อให้เกิดความเสียหายทางการเงินอย่างมีนัยสำคัญ<br>5.1.2.10 การทดสอบแผนฉุกเฉินของสถาบันการเงิน ครอบคลุมการย้ายศูนย์ประมวลผล การเปลี่ยนแปลงกระบวนการทำงาน การเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ อันเนื่องมาจากเหตุการณ์ที่สถาบันการเงินได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ โดยไม่ก่อให้เกิดการหยุดชะงักหรือกระทบต่อความสามารถในการให้บริการ และไม่ก่อให้เกิดความเสียหายต่อข้อมูลของสถาบันการเงิน |

### 5.1.3 บทบาทหน้าที่การรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Incident Response Function)

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 5.1.3.1 สถาบันการเงินมีการกำหนดบทบาทหน้าที่ความรับผิดชอบในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์<br>5.1.3.2 สถาบันการเงินมีบุคลากรที่ทำหน้าที่รับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่มีความรู้ความเชี่ยวชาญอย่างเพียงพอ รวมทั้งประเมินบุคลากรทางด้านเทคนิค ที่ปรึกษาหรือผู้เชี่ยวชาญที่เกี่ยวข้องกับการรับมือเหตุการณ์ผิดปกติทางไซเบอร์ เพื่อให้มีความพร้อมสำหรับการใช้บริการในระหว่างหรือหลังเกิดเหตุการณ์ |
| Intermediate | 5.1.3.3 สถาบันการเงินมีบุคลากรที่ทำหน้าที่ในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ของสถาบันการเงิน รวมถึงการประสานงานและติดต่อสื่อสารกับหน่วยงานและผู้มีส่วนได้เสียทั้งภายในและภายนอก ทั้งระหว่างและหลังการเกิดเหตุการณ์การโจมตีทางไซเบอร์ |
| Advanced | 5.1.3.4 เมื่อมีเหตุการณ์ผิดปกติทางไซเบอร์เกิดขึ้น ผู้ทำหน้าที่บริหารจัดการเหตุการณ์ผิดปกติและผู้ทำหน้าที่ติดตามและวิเคราะห์ Cyber Threat Intelligence ต้องมีการทำงานอย่างใกล้ชิดมีบูรณาการ<br>5.1.3.5 สถาบันการเงินเชื่อมโยงและวิเคราะห์ Threat Intelligence ข้อมูลการบริหารจัดการระบบเครือข่าย และข้อมูลการรับมือเหตุการณ์ผิดปกติเพื่อเตรียมรับมือภัยคุกคามและตอบสนองในเชิงรุกต่อเหตุการณ์ผิดปกติที่อาจเกิดขึ้น |

## 5.2 การบริหารจัดการเหตุการณ์ผิดปกติ

### 5.2.1 กระบวนการบริหารจัดการเหตุการณ์ผิดปกติ

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 5.2.1.1 สถาบันการเงินจัดให้มีรายชื่อหน่วยงานภายนอกพร้อมช่องทางการติดต่อที่เป็นปัจจุบัน เพื่อใช้ติดต่อกรณีเกิดเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์หรือเมื่อมีความจำเป็น เพื่อทำให้สามารถแก้ไขสถานการณ์ได้อย่างทันกาล<br>5.2.1.2 สถาบันการเงินจัดให้มีกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ได้รับผลกระทบจากเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์ ซึ่งครอบคลุมการจำกัดการเข้าถึง การยกเลิกใช้งาน การทำลายหรือทดแทน รวมถึงการตั้งค่าใหม่และการทดสอบก่อนนำกลับมาใช้งาน<br>5.2.1.3 สถาบันการเงินมีกระบวนการในการตัดสินใจใช้แผนรับมือภัยคุกคามและตอบสนอง ต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดกับหน่วยงานภายนอกที่เกี่ยวข้อง |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Intermediate | 5.2.1.4 สถาบันการเงินวิเคราะห์เหตุการณ์ผิดปกติทางด้านความมั่นคงปลอดภัยตั้งแต่ช่วงแรกเมื่อตรวจพบเหตุการณ์บุกรุก เพื่อตอบสนองและลดผลกระทบต่อเหตุการณ์ดังกล่าวที่อาจเกิดขึ้นได้อย่างทันกาล |

## 5.3 การส่งต่อและการรายงานข้อมูลเหตุการณ์ (Escalation and Reporting)

### 5.3.1 การส่งต่อและการสื่อสารข้อมูลเหตุการณ์

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 5.3.1.1 สถาบันการเงินกำหนดช่องทางและวิธีการการสื่อสารและการส่งต่อข้อมูลเหตุการณ์ทางไซเบอร์ไปยังผู้ที่เกี่ยวข้อง เพื่อให้พนักงานสามารถรายงานข้อมูลเหตุการณ์ทางไซเบอร์ได้อย่างทันกาล<br>5.3.1.2 สถาบันการเงินมีระเบียบวิธีปฏิบัติในการแจ้งลูกค้า หน่วยงานผู้กำกับดูแล และหน่วยงานที่บังคับใช้กฎหมายทราบ เมื่อเกิดเหตุการณ์ผิดปกติทางไซเบอร์ เช่น มีการเข้าถึงหรือใช้ข้อมูลลูกค้าจากผู้ไม่ประสงค์ดี<br>5.3.1.3 สถาบันการเงินกำหนดเงื่อนไขการรายงานเหตุการณ์ผิดปกติทางไซเบอร์หรือช่องโหว่ของระบบที่ตรวจพบเสนอผู้บริหารระดับสูงตามระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น<br>5.3.1.4 สถาบันการเงินมีแผนสื่อสารเหตุการณ์ผิดปกติทางไซเบอร์ไปยังองค์กรหรือหน่วยงานภายนอกที่เกี่ยวข้องหรือที่ได้รับผลกระทบ<br>5.3.1.5 สถาบันการเงินมีแผนสื่อสารเหตุการณ์ผิดปกติทางไซเบอร์ไปยังสื่อมวลชนตามความจำเป็นและเหมาะสม |

### 5.3.2 การรายงานเหตุการณ์ผิดปกติ

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 5.3.2.1 สถาบันการเงินจัดประเภทของเหตุการณ์ บันทึก ติดตามและรายงานเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้น<br>5.3.2.2 สถาบันการเงินมีกระบวนการส่งข้อมูลเหตุการณ์ต่อผู้รับผิดชอบในการวิเคราะห์ รับมือภัยคุกคาม และตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Escalation process)<br>5.3.2.3 สถาบันการเงินจัดทำรายงานสรุปเหตุการณ์ผิดปกติ ภัยคุกคาม หรือเหตุละเมิด (Violations) ทางไซเบอร์ที่เกิดขึ้นกับสถาบันการเงินเสนอคณะกรรมการสถาบันการเงิน หรือคณะกรรมการที่เกี่ยวข้องรับทราบ |

## 6. การบริหารความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management)

**วัตถุประสงค์ :** เพื่อให้สถาบันการเงินมีแนวทางในการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างมีประสิทธิภาพ รวมถึงมีการติดตามความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างสม่ำเสมอ ซึ่งสถาบันการเงินสามารถอ้างอิงตามประกาศและแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และแนวปฏิบัติ เรื่อง การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Guideline)

### 6.1 การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก (Third Party)

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 6.1.1.1 สถาบันการเงินมีนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) ซึ่งครอบคลุมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก<br>6.1.1.2 สถาบันการเงินสามารถระบุกระบวนการทางธุรกิจที่สำคัญที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกได้<br>6.1.1.3 สถาบันการเงินมี Network and System's Data Flow Diagram ที่แสดงถึงรายละเอียด Data Flow และการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างชัดเจน โดยได้รับอนุมัติจากผู้มีอำนาจ<br>6.1.1.4 สถาบันการเงินทบทวนและปรับปรุง Network and System's Data Flow Diagram การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้เป็นปัจจุบันอย่างน้อยปีละครั้ง และเมื่อมีการเปลี่ยนแปลง<br>6.1.1.5 สถาบันการเงินจัดเก็บ Network and System's Data Flow Diagram การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกไว้เป็นความลับและมีการควบคุมการเข้าถึงอย่างเข้มงวด<br>6.1.1.6 สถาบันการเงินมีกระบวนการติดตามและทดสอบความพร้อมใช้ (Availability) ของการเชื่อมต่อหลักและการเชื่อมต่อสำรองกับบุคคลภายนอกทุกรายเป็นประจำ<br>6.1.1.7 สถาบันการเงินกำหนด Security Control เพื่อตรวจจับและป้องกันการบุกรุกผ่านการเชื่อมต่อระบบเครือข่ายของบุคคลภายนอกอย่างรัดกุมเพียงพอและมีการสอบทาน Security Control อย่างสม่ำเสมอ<br>6.1.1.8 การเปลี่ยนแปลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่สถาบันการเงินกำหนด |

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Intermediate | 6.1.1.9 สถาบันการเงินนำข้อมูลจากทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศมาจัดทำ Diagrams ที่แสดงถึงการจัดเก็บข้อมูล (Data Repositories) การไหลผ่านของข้อมูล (Data Flow) และโครงสร้างระบบเครือข่าย (Network Infrastructure) ของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก |
| Advanced | 6.1.1.10 สถาบันการเงินมีหน่วยงานหรือผู้รับผิดชอบในการประสานงานกับบุคคลภายนอกที่ให้บริการ สถาบันการเงิน เพื่อร่วมกันพัฒนาปรับปรุงการรักษาความมั่นคงปลอดภัยของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างต่อเนื่อง |

## 6.2 การบริหารจัดการบุคคลภายนอก (Third Party Management)

### 6.2.1 การบริหารจัดการสัญญา

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 6.2.1.1 สถาบันการเงินจัดทำสัญญากับบุคคลภายนอกของสถาบันการเงิน โดยมีการระบุข้อกำหนดในการรักษาความมั่นคงปลอดภัยที่บุคคลภายนอกต้องปฏิบัติไว้ในสัญญาอย่างชัดเจน ทั้งนี้ข้อกำหนดดังกล่าวต้องสอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยที่สถาบันการเงินกำหนด<br>6.2.1.2 สัญญาที่จัดทำกับบุคคลภายนอกต้องระบุถึงความรับผิดชอบในการรักษาความมั่นคงปลอดภัยข้อมูลของสถาบันการเงินที่บุคคลภายนอกเป็นผู้ดูแล รับส่ง จัดเก็บ และประมวลผล<br>6.2.1.3 สัญญาที่จัดทำกับบุคคลภายนอกต้องระบุถึงความรับผิดชอบในการรับมือต่อเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยไว้อย่างชัดเจน<br>6.2.1.4 สัญญาที่จัดทำกับบุคคลภายนอกต้องระบุถึงแนวทางการรักษาความมั่งคงปลอดภัยสำหรับการส่งคืนข้อมูลสำคัญหรือการทำลายข้อมูลสำคัญในกรณีที่มีการยกเลิกสัญญา<br>6.2.1.5 สัญญาที่จัดทำกับบุคคลภายนอกของสถาบันการเงินมีการระบุสิทธิเรียกร้องค่าเสียหายในกรณีที่บุคคลภายนอกไม่สามารถปฏิบัติตามข้อกำหนดที่สถาบันการเงินกำหนดไว้<br>6.2.1.6 สถาบันการเงินมีแนวทางรองรับกรณียกเลิกหรือยุติการใช้บริการ (Termination/Exit strategy) จากบุคคลภายนอกเพื่อลดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของสถาบันการเงิน |
| Intermediate | 6.2.1.7 สัญญาที่จัดทำกับบุคคลภายนอกมีการระบุบทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอกในการรายงานช่องโหว่และเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยแก่สถาบันการเงิน |

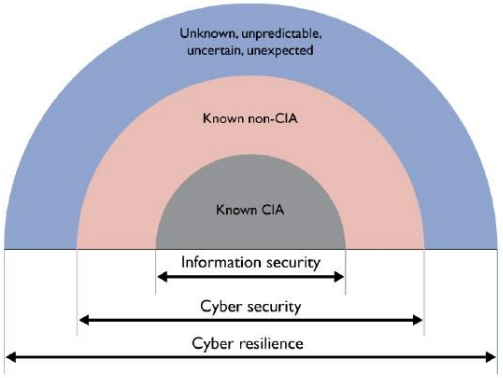
### 6.2.2 การทำ Due Diligence

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 6.2.2.1 สถาบันการเงินกำหนดให้มีการประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ก่อนทำสัญญาว่าจ้างบุคคลภายนอก<br>6.2.2.2 สถาบันการเงินจัดเก็บและปรับปรุงรายชื่อบุคคลภายนอกให้เป็นปัจจุบันอยู่เสมอ |

## 6.3 การติดตามความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกจากบุคคลภายนอก (Ongoing Monitor on Third Party Risk)

| Maturity Level | ระบบการควบคุมที่พึงมี |
|---|---|
| Baseline | 6.3.1.1 สถาบันการเงินประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคคลภายนอกที่สำคัญอย่างสม่ำเสมอ<br>6.3.1.2 สถาบันการเงินสอบทานแผนรับมือจากเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Resilience Plan) ของบุคคลภายนอกที่สำคัญอย่างสม่ำเสมอ<br>6.3.1.3 สถาบันการเงินมีหน่วยงานหรือผู้รับผิดชอบในการติดตามดูแลการเข้าถึงทาง Physical และ Logical จากบุคคลภายนอก<br>6.3.1.4 สถาบันการเงินจัดให้มีการตรวจสอบการบริหารจัดการบุคคลภายนอก เพื่อให้มั่นใจว่า สถาบันการเงินมีกระบวนการติดตาม รายงาน และแก้ไขปัญหาอย่างมีประสิทธิภาพ |
| Intermediate | 6.3.1.5 สถาบันการเงินกำหนดขอบเขตและความถี่ในการติดตามการปฏิบัติงานตามระดับความเสี่ยงของบุคคลภายนอก<br>6.3.1.6 สถาบันการเงินระบุการควบคุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เมื่อมีความจำเป็นต้องรวบรวมและจัดเก็บข้อมูลที่ได้มาจากบุคคลภายนอก |
| Advanced | 6.3.1.7 สถาบันการเงินมีการตรวจสอบ หรือสอบทานรายงานตรวจสอบจากผู้ตรวจสอบหรือผู้เชี่ยวชาญภายนอก ที่มีมาตรฐานเป็นที่ยอมรับ (เช่น SSAE 18 Type II SOC 2) เพื่อประเมินความเพียงพอของการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคคลภายนอกที่สำคัญ เช่น ที่ให้บริการประมวลผล จัดเก็บ รับส่งข้อมูล<br>6.3.1.8 สถาบันการเงินมีการติดตามการเข้าถึงข้อมูลสำคัญ (Sensitive Data) จากบุคคลภายนอก ทั้งข้อมูลที่อยู่ในระบบของสถาบันการเงิน และระบบที่ใช้บริการจากบุคคลภายนอกให้เป็นไปตามหลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege) |

## อภิธานศัพท์

| คำศัทพ์ | คำอธิบาย |
|---|---|
| Cyber Resilience | หน่วยงาน Information Security Forum (ISF) แบ่งวิธีรับมือกับภัยคุกคามทางไซเบอร์ออกเป็น 3 ส่วน ได้แก่<br>1. **Information Security** หมายถึง การรับมือกับภัยคุกคามที่ส่งผลกระทบต่อ Confidentiality, Integrity และ Availability โดยการรับมือกับภัยคุกคามนี้เรียกว่า **Known CIA**<br>2. **Cyber Security** คือ การรับมือกับภัยคุกคามที่ส่งผลกระทบต่อความเสี่ยงอื่น ที่นอกเหนือจาก CIA เช่น Authentication, Authorization การรับมือกับภัยคุกคามนี้เรียกว่า **Known non-CIA**<br>3. **Cyber Resillience** คือ การรับมือกับภัยคุกคามที่ไม่เคยพบมาก่อน ไม่สามารถทำนายได้ ไม่ชัดเจน หรือไม่คาดคิดมาก่อน เช่น การโจมตีแบบ Zero-day การรับมือกับภัยคุกคามนี้เรียกว่า **Unknown**<br>  <br><br>ดังนั้น **Cyber Resilience Management คือ แนวทางในการเตรียมความพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์ทั้งปัจจุบันและภัยในอนาคต ที่ไม่เคยพบมาก่อน ไม่สามารถทำนายได้ ไม่ชัดเจน หรือไม่คาดคิดมา โดยครอบคลุมตั้งแต่การกำกับดูแล การระบุความเสี่ยง การป้องกัน ตรวจจับ รับมือ และการบริหารจัดการความเสี่ยงจากบุคคลภายนอก** |
| การโจมตีในลักษณะ Multi-Faceted | ประเภทการโจมตีจากหลายช่องทางพร้อมๆกันโดยผู้ไม่ประสงค์ดีเช่น การโจมตีด้วย DDoS และ Account Takeover พร้อมกัน เป็นต้น |

| คำศัพท์ | คำอธิบาย |
|---|---|
| การพิสูจน์ตัวตนแบบ Multi Factor Authentication | วิธีการพิสูจน์ตัวตนของผู้ทำรายการโดยใช้ปัจจัยมากกว่าหนึ่งอย่างประกอบกัน ซึ่งข้อมูลมี 3 ปัจจัย ได้แก่<br>1) Something You Know เช่น User ID และ Password เป็นต้น<br>2) Something You Have เช่น บัตรอนุมัติรายการ เป็นต้น<br>3) Something You Are เช่น ลายนิ้วมือ เป็นต้น |
| Cyber Drill | การจำลองสถานการณ์การโจมตีด้วยรูปแบบภัยคุกคามและเทคนิควิธีการต่าง ๆ เพื่อให้ผู้ใช้งานคุ้นเคยและรู้วิธีการป้องกันรับมือภัยคุกคามทางไซเบอร์ รวมถึงทดสอบการตอบสนองต่อเหตุการณ์ภัยคุกคามของฝ่ายเทคโนโลยีสารสนเทศขององค์กร นอกจากนี้การจำลองสถานการณ์การโจมตีจะสามารถวัดผลความตระหนักด้านความมั่นคงปลอดภัยของผู้ใช้งานและช่วยลดจำนวนปัญหาด้านความมั่นคงขององค์กรได้อย่างมีประสิทธิภาพ |
| Cyber Resilience Testing | การทดสอบความสามารถในการเตรียมการ ต้านทาน ควบคุมสถานการณ์ และฟื้นฟูระบบให้คืนสู่สภาวะปกติโดยเร็ว หลังจากถูกโจมตีทางไซเบอร์ โดยครอบคลุมตั้งแต่การตรวจจับ การรายงานผู้บริหาร และการรับมือภัยคุกคามทางไซเบอร์ ครอบคลุมการทดสอบอย่างน้อย<br>- Vulnerability Assessment (VA) และ Penetration Testing<br>- Scenario-based Testing การทดสอบแผนการรับมือและกู้คืนจากภัยคุกคามทางไซเบอร์<br>- Red team test เป็นทีมที่สร้างขึ้นมาจากบุคคลภายใน และ/หรือ ภายนอก ทำหน้าที่วางแผนการทดสอบ การดำเนินการทดสอบ และการควบคุมการทดสอบ |
| Cyber Resilience Plan | การวางแผนด้านความสามารถในการเตรียมการ ต้านทาน ควบคุมสถานการณ์ และฟื้นฟูให้คืนสู่สภาวะปกติโดยเร็ว หลังจากถูกโจมตีทางไซเบอร์ |
| Defense in depth | เป็นยุทธศาสตร์ป้องกันภัยคุกคามรูปแบบหนึ่ง โดยมีการแบ่งการป้องกันเป็นหลายๆชั้น (Multi Layers) เพื่อใช้ป้องกันและบรรเทาการโจมตี หลักการดังกล่าวแบ่งออกเป็น 3 เรื่อง ได้แก่<br>1. การควบคุมทางกายภาพ เช่น ระบบ CCTV รปภ. รักษาความปลอดภัย และการแบ่งเขตพื้นที่หวงห้าม เป็นต้น<br>2. การควบคุมทางเทคนิค เช่น การเข้ารหัสข้อมูล การแบ่งแยกระบบเครือข่าย (Network Segmentation) และการใช้ระบบควมคุม Active Directory<br>3. การควบคุมการบริหารจัดการ เช่น การกำหนดนโยบายและขั้นตอนการทำงาน เป็นต้น |

| คำศัทพ์ | คำอธิบาย |
|---|---|
| Demilitarized Zone (DMZ) | ระบบเครือข่ายสื่อสารที่เป็นส่วนที่เชื่อมต่อกับเครือข่ายสาธารณะภายนอก เช่น Internet โดยจะมีการติดตั้งระบบรักษาความปลอดภัยเอาไว้เพื่อป้องกันการบุกรุกจากภายนอกเข้ามาสู่ระบบเครือข่ายภายใน |
| Due Diligence | การประเมินและวิเคราะห์ศักยภาพของผู้ให้บริการทั้งภายในและภายนอกก่อนที่สถาบันการเงินจะดำเนินการคัดเลือกเพื่อใช้บริการ ซึ่งครอบคลุมถึง ศักยภาพทางด้านการเงิน ศักยภาพด้านประสบการณ์ เป็นต้น |
| Information Assurance | ทำหน้าที่ยืนยันความปลอดภัยของข้อมูล (CIA) ให้สอดคล้องตามนโยบายชั้นความลับของข้อมูลที่สถาบันการเงินกำหนด |
| Threat Intelligence | องค์ความรู้ที่ได้มาจากการวิเคราะห์และจัดการข้อมูลภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กร ครอบคลุมถึงลักษณะการโจมตี แนวโน้มที่จะเกิด และการวิธีการรับมือต่อภัยคุกคามนั้น |
| Tokenization | เป็นเทคโนโลยีที่ใช้ทดแทนข้อมูลเฉพาะที่เป็นความลับ เช่น การใช้ชุดตัวเลขสมมติแทนข้อมูลจริงบนเลขบัตรเครดิต เป็นต้น |
| Transaction Signing OTP | เป็นการสร้าง One time password (OTP) โดยใช้ข้อมูลจากการทำรายการ (Transaction) มาใช้เป็นส่วนหนึ่งของการกำหนดค่า OTP |
| Simulation Testing | การทดสอบหาช่องโหว่และเจาะระบบเสมือนจริง โดยจัดให้มีหน่วยงานทางธุรกิจและหน่วยงานเทคโนโลยีสารสนเทศเข้ามามีส่วนร่วมในการทดสอบ ซึ่งครอบคลุมตั้งแต่การทดสอบกระบวนการในการติดตาม การตรวจพบรายงานเมื่อเกิดเหตุการณ์ผิดปกติทางไซเบอร์ การแก้ไขปัญหาตามมาตรการที่กำหนดไว้ และการรายงานให้ผู้บริหารรวมถึงผู้เกี่ยวข้องที่ได้รับมอบหมายรับทราบ ทั้งนี้ ในการกำหนดขอบเขตการทดสอบ สถาบันการเงินมีการนำข้อมูลจากการทำ Threat Intelligence มาใช้ประกอบการกำหนดสถานการณ์จำลอง (Scenario) และขอบเขตการทดสอบ เพื่อให้สะท้อนถึงความเสี่ยงภัยคุกคามที่อาจเกิดขึ้นกับสถาบันการเงิน |
| Social Engineering | วิธีการหลอกลวงโดยใช้หลักการทางจิตวิทยาหลายรูปแบบ เพื่อให้เหยื่อเปิดเผยข้อมูล ซึ่งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้อง เช่น การโทรศัพท์เข้ามาหลอกลวงเหยื่อเพื่อให้เปิดเผยข้อมูลสำคัญหรือหลอกล่อให้เหยื่อกระทำการตามที่ผู้ไม่หวังดีต้องการ การล่อลวงผ่านการเข้าใช้งานเว็บบอร์ด อีเมล หรือการแชท เป็นต้น |
| บุคคลภายนอก (Third Party) | บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือข้อมูลของลูกค้าที่ควบคุมโดยสถาบันการเงินได้ โดยกรณีสาขาของธนาคารพาณิชย์ต่างประเทศให้รวมถึงสำนักงานใหญ่หรือสาขาอื่นในต่างประเทศที่เป็นนิติบุคคลเดียวกันด้วย ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าของสถาบันการเงิน |

**ตัวอย่างหัวข้อในรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ**

| ทรัพย์สินสารสนเทศประเภทฮาร์ดแวร์ (Hardware) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| เลขทะเบียนทรัพย์สินสารสนเทศ | ประเภทฮาร์ดแวร์ | ลักษณะการใช้งาน | ระดับความมั่นคงปลอดภัย (สูงสุด/สูง/ปานกลาง/ต่ำ) | ผู้เป็นเจ้าของฮาร์ดแวร์ | ผู้ใช้งาน | ที่ตั้ง | วันที่เริ่มสัญญาบำรุงรักษา (ววว/ดด/ปปปป) | หมายเหตุ |
| | | | | | | | | |
| | | | | | | | | |

| ทรัพย์สินสารสนเทศประเภทซอฟต์แวร์ (Software) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| เลขทะเบียนทรัพย์สินสารสนเทศ | ชื่อซอฟต์แวร์ | ผู้พัฒนา | จำนวนลิขสิทธิ์ | ประเภทซอฟต์แวร์ | รายละเอียดซอฟต์แวร์ | ระดับความมั่นคงปลอดภัย (สูงสุด/สูง/ปานกลาง/ต่ำ) | ผู้เป็นเจ้าของซอฟต์แวร์ | ที่เก็บซอฟต์แวร์ | วันที่ลงทะเบียนซอฟต์แวร์ | เลขทะเบียนทรัพย์สินฮาร์ดแวร์ (ใช้อ้างอิง) |
| | | | | | | | | | | |
| | | | | | | | | | | |

| ทรัพย์สินสารสนเทศประเภทข้อมูล (INF) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| เลขทะเบียนทรัพย์สินสารสนเทศ | ประเภทของข้อมูล | รายละเอียดของสารสนเทศ | ระดับความลับ | ระดับความมั่นคงปลอดภัย (สูงสุด/สูง/ปานกลาง/ต่ำ) | ผู้เป็นเจ้าของสารสนเทศ | ที่เก็บสารสนเทศ (ชื่อสถานที่) | เลขทะเบียนทรัพย์สินซอฟต์แวร์ (ใช้อ้างอิง) | หมายเหตุ |
| | | | | | | | | |
| | | | | | | | | |

## เอกสารอ้างอิง


- Framework for Improving Critical Infrastructure Cybersecurity ของ National Institute of Standards and Technology ซึ่งเป็นองค์กรที่กำหนดมาตรฐานด้านเทคโนโลยีในสหรัฐอเมริกา
- The Cyber Resilience Assessment Framwork ของ Hong Kong Monetary Authority ซึ่งเป็นหน่วยงานกำกับดูแลสถาบันการเงินในฮ่องกง
- ISO27001:2013 Information technology - Security techniques – Information Security Management Systems – Requirement มาตรฐานด้านการจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
- FFIEC Cybersecurity Assessment Tool

ธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

# กรอบการประเมินความพร้อมการรับมือภัยคุกคามไซเบอร์

(Cyber Resilience Assessment Framework)

ภายใต้หลักเกณฑ์การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk Management) ของสถาบันการเงิน

สถาบันการเงินสามารถดาวน์โหลด Template ในรูปแบบ excel สำหรับประเมินความพร้อมการรับมือภัยคุกคามไซเบอร์ (Cyber Resilience Assessment Framework) ตาม link ดังต่อไปนี้

Template สำหรับการประเมินความพร้อมการรับมือภัยคุกคามไซเบอร์ (Cyber Resilience Assessment Framework)

ฝ่ายกำกับและตรวจสอบด้านเทคโนโลยีสารสนเทศ
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

| | | |
|---|---|---|
| เทอดพงษ์ เปล่งศิริวัฒน์ | 0-2283-5827 | Email : TerdponP@bot.or.th |
| ปฐมพงศ์ สว่างวงศ์ธรรม | 0-2283-6576 | Email : Pathomps@bot.or.th |
| สุรัติ ทังสุภูติ | 0-2283-6597 | Email : SuratTu@bot.or.th |

**คำถาม – คำตอบแนบท้าย**
**กรอบการประเมินความพร้อมด้าน Cyber Resilience**
**(Cyber Resilience Assessment Framework, CRAF)**
**ลงวันที่ 15 สิงหาคม 2562**

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| **ขอบเขตการประเมินตามกรอบการประเมินความพร้อมด้าน Cyber Resilience** | | |
| 1. | การรายงานผลการประเมิน CRAF กำหนดให้รายงานผลเป็นประจำทุกปี ภายใน 30 วัน นับจากวันที่ 31 ธันวาคมของปีที่ประเมิน ให้แก่ธนาคารแห่งประเทศไทยนั้น ในช่วงปีแรกสถาบันการเงินอาจต้องใช้ระยะเวลาในการดำเนินการ และไม่สามารถปฏิบัติตามหลักเกณฑ์ได้ทันตามกำหนดเวลา สถาบันการเงินสามารถขอขยายเวลาในการรายงานผลการประเมินดังกล่าวได้หรือไม่ | ธปท. รับทราบถึงข้อจำกัดดังกล่าวในการประเมินครั้งแรกปี 2562 ให้สถาบันการเงินรายงานผลการประเมินมายัง ธปท. **ภายใน 31 มีนาคม 2563**<br>ทั้งนี้ในปีต่อ ๆ ไป ธปท. จะให้ สถาบันการเงินรายงานผลการประเมินมายัง ธปท. เป็นประจำทุกปี ภายใน **28 กุมภาพันธ์ของปีถัดไป** |
| 2. | ความคาดหวังของ ธปท. ในเรื่อง<br>2.1) การมีส่วนร่วมของหน่วยงาน 2nd line และ 3rd line ในการประเมิน CRAF<br>2.2) ผู้ที่จะลงนามรับรองผลประเมินควรจะเป็นใคร ระดับใด | 2.1) การประเมิน CRAF ครอบคลุมหน้าที่ของทั้งหน่วยงาน 1st line 2nd line และ 3rd line ตามขอบเขตงานและความรับผิดชอบที่มี ดังนั้น หน่วยงานที่ทำหน้าที่ 2nd line และ 3rd line จึงต้องมีส่วนร่วมประเมินในส่วนที่เกี่ยวข้อง<br>2.2) การรายงานผลให้<br>**(1) Head of IT Security หรือ Chief Information Security Officer (CISO) <u>และ</u>**<br>**(2) ตัวแทนจาก 2nd line ที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือกำกับการปฏิบัติตามหลักเกณฑ์**<br>ลงนามรับรองผลการประเมินร่วมกัน<br>กรณีที่ผู้ลงนามรับรองอยู่ต่างประเทศ สถาบันการเงินสามารถพิจารณาให้ผู้บริหารสูงสุดของสำนักงานในประเทศไทยลงนามรับรองผลได้ |
| 3. | นิยามของเกณฑ์การประเมินผลในส่วนมาตรการการจัดการความเสี่ยงด้านไซเบอร์ | ธปท. แบ่งผลการประเมินเป็น 5 ระดับ โดยมีนิยามดังนี้<br>**1) Pass**ผ่านเกณฑ์ที่กำหนดทั้งหมด<br>**2) Not Pass** ไม่ผ่านเกณฑ์ที่กำหนดทั้งหมด<br>**3) Partially Pass** ผ่านเกณฑ์ที่กำหนดบางส่วน |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| | | **4) Alternative Control** ไม่มีการควบคุมที่พึงมีตามเกณฑ์ที่กำหนด แต่มีการควบคุมอื่นที่เทียบเท่าทดแทน<br>**5) Not Applicable** ไม่ต้องประเมิน เนื่องจากเกณฑ์ที่กำหนดไม่เกี่ยวข้อง |
| 4. | การประเมินผลในส่วนที่ 2 เรื่อง แนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (maturity level)<br>4.1) ต้องประเมินทุกมาตรการหรือไม่ และ<br>4.2) ต้องมีเอกสารหรือข้อมูลประกอบการประเมินด้วยหรือไม่ | 4.1) ให้ประเมินตามระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber inherent risk) ของสถาบันการเงิน เช่น สถาบันการเงินมีความเสี่ยงตั้งต้นอยู่ในระดับปานกลาง การประเมินต้องครอบคลุมในระดับ Baseline และ Intermediate เท่านั้น (สถาบันการเงินอาจพิจารณาประเมินระดับ Advanced เพิ่มเติมได้ตามที่เห็นสมควร)<br>4.2) สถาบันการเงินต้องให้เหตุผลประกอบผลการประเมินทุกข้อ ส่วนเอกสารอ้างอิงให้นำส่งเฉพาะผลการประเมิน Partially Pass และ Alternative Control เท่านั้น หรือตามที่ ธปท. ร้องขอ |
| 5. | ความสอดคล้องของแนวทางการประเมินด้าน Cyber Resilience ของ ธปท. และ ก.ล.ต. | Cyber Resilience ของ ธปท. และ ก.ล.ต. มีกรอบหลักการและแนวทางในการประเมินสอดคล้องกันตามมาตรฐานสากลที่อ้างอิง คือ NIST Cybersecurity Framework<br>เพื่อลดภาระและความซ้ำซ้อนให้กับสถาบันการเงินที่กำกับดูแล ธปท. และ ก.ล.ต. มีข้อตกลงให้มีการแลกเปลี่ยนผลการประเมินในส่วนที่ทดแทนกันได้ |
| **การประเมินระดับความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment)** | | |
| **เทคโนโลยีและการเชื่อมต่อ** | | |
| 6. | ข้อ 1.2 จำนวน Public IP Address ของสถาบันการเงินที่เชื่อมต่อเครือข่ายอินเทอร์เน็ต (ซึ่งรวมถึง Public IP ที่เชื่อมต่อระหว่างสาขาและระบบเครือข่ายหลักของสถาบันการเงิน)<br>กรณีที่ ระบบงานที่ประเทศไทยมีการบริหารจัดการ โดยการแยกระบบระหว่าง Intranet และ Internet ออกจากกัน จะถือว่าความเสี่ยงลดลงจากหลักเกณฑ์ที่ธนาคารแห่งประเทศไทยกำหนด หรือไม่ | การประเมินในส่วนที่ 1 เป็นการประเมินความเสี่ยงตั้งต้นด้านไซเบอร์ของสถาบันการเงิน (Cyber Inherent Risk) โดยยังไม่คำนึงถึงการควบคุมที่มีอยู่ ดังนั้น จำนวน Public IP Address ของสถาบันการเงินที่เชื่อมต่อเครือข่ายอินเทอร์เน็ต สะท้อนให้สถาบันการเงินเห็นถึงความเสี่ยงตั้งต้นที่สถาบันการเงินเผชิญจากการมีช่องทาง Public ที่มากขึ้นโดยยังไม่คำนึงถึงการควบคุมที่มี ซึ่งการบริหารจัดการระบบเครือข่าย โดยการแยกระบบระหว่าง Intranet และ Internet ออกจากกัน นั้นเป็นการควบคุม เพื่อให้ความเสี่ยงสุทธิลดลง ซึ่งจะนำไปประเมินในขั้นตอนการประเมินมาตรการควบคุมที่พึงมี (Maturity Level) |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| 7. | ข้อ 1.7 จากข้อ 1.6 ลักษณะการให้บริการที่สามารถเชื่อมต่อเข้าถึงเครือข่ายภายในหรือระบบงานภายในของสถาบันการเงินได้<br>กรณีที่สถาบันการเงินอนุญาตให้มีการเชื่อมต่อเครือข่ายภายในเฉพาะพนักงานที่ได้รับอนุญาตผ่านการเชื่อมต่อแบบ VPN ให้ถือว่าเป็นการเชื่อมต่อแบบ VPN-based ใช่หรือไม่ | การประเมินในส่วนที่ 1 เป็นการประเมินความเสี่ยงตั้งต้นด้านไซเบอร์ของสถาบันการเงิน (Cyber Inherent Risk) โดยยังไม่คำนึงถึงการควบคุมที่มีอยู่ ดังนั้น ลักษณะการเชื่อมต่อเข้าถึงเครือข่ายภายในหรือระบบงานภายในของสถาบันการเงินจากอุปกรณ์ส่วนตัวของพนักงานหรือของสถาบันการเงินที่ลงทะเบียนสะท้อนให้สถาบันการเงินเห็นถึงความเสี่ยงตั้งต้นที่สถาบันการเงินเผชิญจากการที่สถาบันการเงินอนุญาตให้อุปกรณ์ส่วนตัวของพนักงานหรือของสถาบันการเงินที่ลงทะเบียนสามารถเข้าถึงเครือข่ายภายในหรือระบบงานภายในของสถาบันการเงินได้ โดยยังไม่คำนึงถึงการควบคุมที่มี ซึ่งการที่สถาบันการเงินอนุญาตให้เชื่อมต่อเครือข่ายภายในเฉพาะพนักงานที่ได้รับอนุญาตผ่านการเชื่อมต่อแบบ VPN ถือเป็นการควบคุมเพื่อให้ความเสี่ยงสุทธิลดลง ซึ่งจะนำไปประเมินในขั้นตอนการประเมินมาตรการควบคุมที่พึงมี (Maturity Level) |
| 8. | ข้อ 1.8 ลักษณะการเข้าถึงเครือข่าย/ระบบงานของสถาบันการเงิน<br>ในที่นี้หมายรวมถึงอุปกรณ์ส่วนตัว (bring your own device (BYOD)) ด้วยหรือไม่ | ให้สถาบันการเงินนับรวมอุปกรณ์ทุกประเภทที่สามารถเข้าถึงเครือข่าย/ระบบงานของสถาบันการเงินได้ |
| 9. | ข้อ 1.9 จากข้อ 1.8 ลักษณะการให้บริการที่สามารถเชื่อมต่อกับเครือข่าย/ระบบงานของสถาบันการเงินได้<br>กรณีที่ลักษณะการเข้าถึงเข้าถึงระบบสำคัญที่ไม่ได้เชื่อมต่อโดยตรง แต่เป็นการเข้าถึงผ่าน software ที่มีการควบคุมการเข้าถึงระบบงาน ไม่ควรจัดระดับลักษณะการเข้าถึงในลักษณะดังกล่าวเป็นความเสี่ยงสูง | การประเมินในส่วนที่ 1 เป็นการประเมินความเสี่ยงตั้งต้นด้านไซเบอร์ของสถาบันการเงิน (Cyber Inherent Risk) โดยยังไม่คำนึงถึงการควบคุมที่มีอยู่ ดังนั้น ลักษณะการให้บริการที่สามารถเชื่อมต่อกับระบบงานที่สำคัญของสถาบันการเงินจากอุปกรณ์ทุกประเภท สะท้อนให้สถาบันการเงินเห็นถึงความเสี่ยงตั้งต้นที่สถาบันการเงินอนุญาตให้มีอุปกรณ์เชื่อมต่อเข้าถึงเครือข่ายภายในหรือระบบงานภายในของสถาบันการเงินได้ โดยยังไม่คำนึงถึงการควบคุมที่มี ซึ่งมีควบคุมการเข้าถึงระบบงานผ่าน software อื่น ถือเป็นการควบคุมเพื่อให้ความเสี่ยงสุทธิลดลง ซึ่งจะนำไปประเมินในขั้นตอนการประเมินมาตรการควบคุมที่พึงมี (Maturity Level) |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| 10. | ข้อ 1.10 จำนวนองค์กรภายนอกที่มีการเชื่อมต่อกับเครือข่ายของสถาบันการเงิน<br>การนับจำนวนดังกล่าวรวมถึงการเชื่อมต่อในลักษณะ private link หรือไม่ | ให้สถาบันการเงินนับจำนวนองค์กรภายนอกที่มีการเชื่อมต่อกับเครือข่ายของสถาบันการเงินในทุกช่องทาง ทุกประเภท ทุกรูปแบบของการเชื่อมต่อ |
| 11. | ข้อ 1.15 จำนวนระบบงานสำคัญที่สถาบันการเงินพัฒนาขึ้นเอง หรือสถาบันการเงินปรับแต่ง (customize) จากระบบงานของ vendor และเชื่อมต่อกับระบบงานภายใน โดย คำจำกัดความ “ระบบงานสำคัญ” หมายถึงอะไร | ด้วยความสำคัญของระบบเทคโนโลยีสารสนเทศของแต่ละสถาบันการเงินมีผลกระทบต่อการดำเนินธุรกิจแตกต่างกัน ดังนั้น สถาบันการเงินควรกำหนดหลักเกณฑ์หรือใช้หลักเกณฑ์ที่กำหนดไว้แล้วในการจัดลำดับความสำคัญของระบบงาน |
| 12. | ข้อ 1.16 การนับจำนวนระบบงานสำคัญที่ vendor พัฒนาให้และเชื่อมต่อกับระบบงานภายในของสถาบันการเงิน<br>การนับจำนวนข้างต้น ให้นับรวมถึงจำนวนระบบงานสำคัญที่บริษัทแม่ในต่างประเทศพัฒนาระบบงานให้สถาบันการเงินใช้งานโดยไม่มีการปรับปรุงเพิ่มเติม (customize) หรือไม่ | นับระบบงานสำคัญเฉพาะที่ผู้ให้บริการภายนอกพัฒนาให้และเชื่อมต่อกับระบบงานภายในของสถาบันการเงิน โดยไม่รวมถึงระบบงานที่บริษัทแม่ในต่างประเทศเป็นผู้พัฒนาระบบงานให้ |
| 13. | ข้อ 1.21 จำนวนอุปกรณ์เครือข่าย ได้แก่ router, switch, firewall, IPS/IDS หรืออุปกรณ์ที่เทียบเท่า<br>การนับจำนวนข้างต้นให้นับรวมถึงอุปกรณ์เครือข่ายสำรอง หรือไม่ | นับรวมถึงอุปกรณ์เครือข่ายชุดสำรองเฉพาะที่มีการเปิดใช้งานและเชื่อมต่อกับระบบงานของสถาบันการเงิน |
| 14. | ข้อ 1.23 การใช้เทคโนโลยี Cloud Computing<br>ในการประเมินตามกรอบฉบับนี้ กำหนดให้สถาบันการเงินประเมินระดับความเสี่ยงจากการใช้เทคโนโลยี Cloud Computing อ้างอิงตามลักษณะการ deployment ว่าเป็น private cloud, hybrid cloud หรือ public cloud นั้น อาจทำให้การใช้บริการ Microsoft office 365 เข้าข่ายเป็น public cloud และจัดระดับเป็นความเสี่ยงสูง ซึ่งอาจไม่สะท้อนถึงความเสี่ยงที่แท้จริง | การประเมินความเสี่ยงตั้งต้นจากการใช้เทคโนโลยี Cloud Computing คำนึงถึงลักษณะ deployment เป็นหลัก เนื่องจากการใช้ public cloud จะมีความเสี่ยงตั้งต้นที่กระทบต่อภัยไซเบอร์มากกว่า private cloud ดังนั้น แม้ว่าการใช้บริการ Microsoft office 365 เข้าข่ายเป็นระบบงานสนับสนุน แต่ก็อาจทำให้สถาบันการเงินมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้ |
| **ลักษณะผลิตภัณฑ์และการให้บริการ** | | |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| 15. | ข้อ 3.9 จำนวนเทคโนโลยีสารสนเทศที่สถาบันการเงินนำมาใช้เป็นครั้งแรกในรอบ 12 เดือน<br>การนับจำนวนข้างต้น ให้รวมถึง กรณีที่สถาบันการเงินนำเทคโนโลยี blockchain มาใช้ในการให้บริการ แต่เป็นเพียงการเข้าร่วมเป็นสมาชิกเท่านั้น หรือไม่ | ให้นับรวมการใช้เทคโนโลยีสารสนเทศใหม่ที่สถาบันการเงินนำมาใช้ในการให้บริการทุกรูปแบบ โดยการนับจำนวนให้เริ่มนับตั้งแต่สถาบันการเงินใช้เทคโนโลยีดังกล่าวทั้งในวงจำกัด (sandbox) และในวงกว้าง สำหรับกรณีการเข้าร่วมเป็นสมาชิกแต่ยังไม่มีการเข้าใช้หรือเชื่อมต่อระบบกับวงสมาชิก ไม่ต้องนับรวม |
| **ลักษณะเฉพาะขององค์กร** | | |
| 16. | ข้อ 4.3 จำนวนบริการด้านเทคโนโลยีสารสนเทศที่สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอก<br>การนับจำนวนข้างต้น ให้รวมถึง จำนวนบริการด้านเทคโนโลยีสารสนเทศที่บริษัทในกลุ่มธุรกิจการเงินเดียวกันในต่างประเทศใช้บริการจากผู้ให้บริการภายนอก หรือไม่ | นับรวม เฉพาะการใช้บริการด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอกที่สถาบันการเงินใช้บริการโดยตรงเท่านั้น |
| 17. | ข้อ 4.6 สัดส่วนจำนวนพนักงานในสายงาน IT ของสถาบันการเงิน ที่ลาออกในระยะเวลา 12 เดือนที่ผ่านมา<br>กรณีที่สถาบันการเงินมีจำนวนพนักงาน IT น้อย และเมื่อมีการลาออกเกิดขึ้นเพียงเล็กน้อย จะทำให้สัดส่วนการลาออกสูง ซึ่งอาจไม่สะท้อนถึงระดับความเสี่ยงที่แท้จริง | การที่มีจำนวนพนักงานด้าน IT น้อย ทำให้บทบาทหน้าที่ และความรับผิดชอบในแต่ละบุคคลมีงานที่ต้องรับผิดชอบมาก ดังนั้น หากพนักงานคนใดคนหนึ่งลาออก จะส่งผลกระทบกับงานทั้งหมดที่พนักงานท่านนั้นดูแลอยู่ซึ่งส่งผลให้ความเสี่ยงด้านไซเบอร์ของสถาบันการเงินเพิ่มมากขึ้น |
| 18. | ข้อ 4.9 สัดส่วนจำนวน User PID ที่มอบให้แก่พนักงาน outsource หรือบุคคลภายนอกใช้งานต่อ user PID ทั้งหมดของธนาคาร<br>การนับจำนวนข้างต้นให้นับอย่างไรในกรณีดังต่อไปนี้<br>(1) กรณีที่ outsource ได้รับ privileged ID รายครั้งตาม change<br>(2) กรณีที่พนักงานที่ได้รับ privileged ID อยู่ต่างประเทศทั้งหมด ซึ่งทำให้ไม่สามารถทราบจำนวนที่แน่นอนได้ | (1) ให้นับจำนวนรหัสผู้ใช้งาน privileged ID ที่ให้พนักงาน outsource หรือบุคคลภายนอกใช้งานในทุกกรณีไม่ว่าจะเป็นการมอบหมายเป็นรายครั้งหรือให้จัดเก็บไว้ถาวร<br>(2) เจตนารมณ์ของการนับสัดส่วนจำนวน User PID ที่มอบให้แก่พนักงาน outsource หรือบุคคลภายนอกใช้งานต่อ user PID ทั้งหมดของสถาบันเงิน เพื่อให้สถาบันการเงินทราบว่า สถาบันการเงินมีความเสี่ยงจากการเข้าถึงระบบงานโดยใช้สิทธิ์สูงสุดจากพนักงาน outsource หรือบุคคลภายนอก ดังนั้น สถาบันการเงินควรทราบว่ามีการใช้ privileged ID จากบุคคลภายนอกในทุกกรณี |
| **แนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level)** | | |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| **การกำกับดูแล (Governance)** | | |
| 19. | นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) ครอบคลุมการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์กับองค์กรภายนอก (Cyber Threat Intelligence Sharing) องค์กรภายนอกดังกล่าวหมายถึงผู้ให้บริการ (Vendor) หรือไม่ | องค์กรภายนอก หมายถึง ผู้ให้บริการภายนอก หน่วยงานกลาง หรือผู้ให้บริการ (Vendor) ที่สถาบันการใช้บริการ เพื่อให้สถาบันการเงินกำหนดแนวทางการดำเนินการที่เหมาะสมในการป้องกัน ติดตาม และรับมือกับเหตุการณ์ทางไซเบอร์กับองค์ภายนอก |
| 20. | การแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ (cyber threat intelligence sharing) ต้องกำหนดอยู่ในนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) หรือไม่ | สถาบันการเงินสามารถกำหนดการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ (cyber threat intelligence sharing) อยู่ในนโยบายฉบับอื่นได้ โดยไม่จำเป็นต้องกำหนดอยู่ในนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy) |
| 21. | สถาบันการเงินมีการตรวจสอบการประเมินการรับมือและความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่องต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cybersecurity Incident) หากสถาบันการเงินมีการทำ Cyber Drill ถือว่าสถาบันการเงินปฏิบัติตามหลักเกณฑ์ หรือไม่ | การตรวจสอบการประเมินการรับมือและความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่องต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cybersecurity Incident) เป็นการตรวจสอบกระบวนการการตอบสนองต่อเหตุการณ์และการกู้คืนระบบว่ามีความพร้อมเพียงพอต่อการรับมือและมีความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดเหตุการณ์ผิดปกติทางไซเบอร์ (Cybersecurity Incident)<br>ทั้งนี้ การทำ Cyber Drill เป็นเพียงตัวอย่างการเตรียมความพร้อมแบบหนึ่งเท่านั้น |
| 22. | สถาบันการเงินมีการอบรมเพื่อสร้างความรู้และความตระหนักด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้แก่บุคลากรในองค์กรและลูกค้าอย่างสม่ำเสมอ ต่อเนื่อง และสามารถวัดผลได้ โดยการวัดผลดังกล่าวหมายถึงการวัดผลในด้านใด | การวัดผลดังกล่าว มุ่งเน้นประเมินความเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านไซเบอร์ของบุคลากรในองค์กรเป็นสำคัญ เพื่อให้มั่นใจว่ามีความเข้าใจและความพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์<br>สำหรับการวัดผลของลูกค้านั้น ขึ้นอยู่กับการพิจารณาในการดำเนินการเพิ่มเติมของแต่ละสถาบันการเงิน |
| 23. | สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ สามารถใช้โครงสร้างกรรมการ การกำหนดกลยุทธ์ นโยบายการบริหารความเสี่ยงด้าน IT การใช้ระบบ | สาขาของธนาคารพาณิชย์ต่างประเทศ หรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศสามารถใช้โครงสร้างกรรมการการกำหนดกลยุทธ์ นโยบายการบริหารความเสี่ยง |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| | เทคโนโลยีสารสนเทศ และผลการตรวจสอบจากธนาคารพาณิชย์แม่ในต่างประเทศ ได้หรือไม่ | ด้าน IT การใช้ระบบเทคโนโลยีสารสนเทศ และผลการตรวจสอบจากธนาคารพาณิชย์แม่ในต่างประเทศได้ |
| **การป้องกันความเสี่ยง (Protection)** | | |
| 24. | สถาบันการเงินติดตั้งอุปกรณ์ในการตรวจจับและปิดกั้นการโจมตีหรือการบุกรุกโดยไม่ได้รับอนุญาต เช่น Intrusion Detection หรือ Prevention System (IDS/IPS) ครอบคลุมถึงการเชื่อมต่อกับองค์กรภาครัฐ หรือไม่ | สถาบันการเงินควรติดตั้งอุปกรณ์ในการตรวจจับและปิดกั้นการโจมตีหรือการบุกรุกโดยไม่ได้รับอนุญาต เช่น Intrusion Detection หรือ Prevention System (IDS/IPS) ครอบคลุมถึงการเชื่อมต่อกับบุคคลภายนอกทุกประเภท เพื่อให้สถาบันการเงินพร้อมสำหรับการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดการหยุดชะงักในการให้บริการของสถาบันการเงิน |
| 25. | สถาบันการเงินต้องทำ File Integrity Check ทุก file กับ server ที่เชื่อมต่อกับเครือข่ายสาธารณะเป็นประจำ หรือไม่ | สถาบันการเงินควรทำ File Integrity Check กับ server ที่เชื่อมต่อกับเครือข่ายสาธารณะสำหรับการดำเนินการ จะดำเนินการกับทุก file หรือเฉพาะ file ที่มีนัยสำคัญ ขอให้พิจารณาให้สอดคล้องกับระดับความเสี่ยงของเครื่อง server หรือ file นั้น ๆ |
| 26. | สถาบันการเงินใช้วิธีการพิสูจน์ตัวตนแบบ Multifactor เช่น การใช้ Tokens, Digital Certificates เป็นต้น ในการพิสูจน์ตัวตนของบัญชีผู้ใช้งานที่มีสิทธิ์สูงสำหรับงานที่มีความเสี่ยงตามที่สถาบันการเงินกำหนด (Tier 1,2) ดังนั้น ระบบงานที่เป็น Tier 1,2 ตามที่กำหนดข้างต้นธนาคารแห่งประเทศไทยใช้หลักเกณฑ์ใดในการอ้างอิง | เนื่องจากความสำคัญของระบบเทคโนโลยีสารสนเทศของแต่ละสถาบันการเงินที่มีผลกระทบต่อการดำเนินธุรกิจแตกต่างกัน ดังนั้น สถาบันการเงินควรใช้หลักเกณฑ์การจัดลำดับความสำคัญของระบบงาน Tier 1,2 ตามที่สถาบันการเงินกำหนด |
| 27. | สถาบันการเงินเข้ารหัสข้อมูลลับทุกครั้งในขณะรับส่งผ่านเครือข่ายสาธารณะหรือเครือข่ายที่ไม่น่าเชื่อถือ เช่น Internet เป็นต้น สถาบันการเงินเข้ารหัสข้อมูลลับ เฉพาะข้อมูล Confidential หรือข้อมูลความเสี่ยงสูง ถือว่าสถาบันการเงินปฏิบัติตามหลักเกณฑ์หรือไม่ | การเข้ารหัสข้อมูลลับ สถาบันการเงินสามารถพิจารณาตามระดับชั้นความลับข้อมูล โดยอาจอ้างอิงจากหลักเกณฑ์การจัดชั้นความลับของข้อมูล (information classification) ของสถาบันการเงิน |
| 28. | สถาบันการเงินจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) ให้ครอบคลุมการควบคุมการรักษาความปลอดภัย (Security Control) | สถาบันการเงินควรจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) ให้ครอบคลุมทุกระบบงาน เพื่อให้มั่นใจได้ว่าระบบงานทุกระบบได้มีการพิจารณาถึงมาตรการการควบคุมการรักษาความปลอดภัยอย่างรัดกุม |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| | เฉพาะระบบงานที่มีนัยสำคัญ เพียงพอหรือไม่ | และสอดคล้องตามระดับความเสี่ยงของสถาบันการเงิน |
| **การตรวจจับ (Detection)** | | |
| 29. | สถาบันการเงินจัดทำ Penetration Testing ครอบคลุมระบบงานที่เชื่อมต่อกับภายนอกอย่างน้อยปีละ 1 ครั้ง โดยผู้เชี่ยวชาญ และมีการรายงานไปยังผู้ที่รับผิดชอบ เพื่อดำเนินการแก้ไขหรือปิดช่องโหว่อย่างเหมาะสม หากสถาบันการเงินไม่มีระบบงานที่เชื่อมต่อกับภายนอกจำเป็นต้องทำ Penetration Testing หรือไม่ | หากสถาบันการเงินไม่มีระบบงานที่เชื่อมต่อกับภายนอกไม่จำเป็นต้องจัดทำ Penetration Testing อย่างไรก็ดี การทำ Penetration Testing และการตรวจสอบช่องโหว่อย่างสม่ำเสมอแม้จะไม่ใช่กับระบบที่มีการเชื่อมต่อกับภายนอก เป็นการช่วยลดความเสี่ยงและปิดจุดอ่อนของระบบงานจากภัยคุกคามทางไซเบอร์ได้ |
| 30. | หากสถาบันการเงินมีกระบวนการการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสาร ให้ตรงกับเครื่องเซิร์ฟเวอร์ Network Time Protocol: NTP จากสถาบันที่มีความน่าเชื่อถือ ในรูปแบบ manual เป็นประจำทุกเดือน ถือว่าสถาบันการเงินปฏิบัติตามหลักเกณฑ์ หรือไม่ | สถาบันการเงินต้องมั่นใจได้ว่า เครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารของสถาบันการเงินมีการอ้างอิงเวลาที่ตรงกัน ดังนั้นการกำหนดความถี่หรือวิธีการในการ sync เวลาระหว่างเครื่องเซิร์ฟเวอร์ Network Time Protocol ขึ้นอยู่กับกระบวนการภายในของแต่ละสถาบันการเงิน |
| 31. | สถาบันการเงินมีกระบวนการหรือระบบที่สามารถเฝ้าระวังหรือติดตามพฤติกรรมการเข้าใช้งานระบบของพนักงานและบุคคลภายนอก (3rd Party) รวมถึงแจ้งเตือนผู้ที่รับมอบอำนาจอัตโนมัติ เมื่อมีพฤติกรรมที่น่าสงสัย หากสถาบันการเงินมีกระบวนการการเฝ้าระวังหรือติดตามพฤติกรรมการเข้าใช้งานระบบของพนักงานและบุคคลภายนอก แต่ไม่สามารถแจ้งเตือนแบบอัตโนมัติ (Automatic Notification) ถือว่าสถาบันการเงินปฏิบัติตามหลักเกณฑ์ หรือไม่ | ปัจจุบันภัยคุกคามทางไซเบอร์มีความซับซ้อน มีรูปแบบหลากหลายและมีปริมาณเพิ่มขึ้นอย่างมาก ดังนั้นการมีกระบวนการหรือระบบ ที่สามารถเฝ้าระวังหรือติดตามพฤติกรรมการเข้าใช้งานระบบของพนักงานและบุคคลภายนอก (3rd Party) รวมถึงแจ้งเตือนผู้ที่รับมอบอำนาจอัตโนมัติ เป็นสิ่งที่สถาบันการเงินควรพิจารณาดำเนินการเพื่อให้จะสามารถรับมือต่อภัยคุกคามได้อย่างทันท่วงทีและสอดคล้องตามระดับความเสี่ยง |
| 32. | สถาบันการเงินมีระบบในการติดตามและแจ้งเตือน เมื่อพบรายการการนำเงินออกจากบัญชีลูกค้าที่ผิดปกติ โดยมีการแจ้งเตือนให้ลูกค้ารับทราบก่อนหรือหลังการทำธุรกรรมดังกล่าวทันที จำเป็นต้องทำเฉพาะกับสถาบันการเงินที่มี ATM เท่านั้น หรือไม่ | สถาบันการเงินควรมีระบบในการติดตามและแจ้งเตือนให้ครอบคลุมทุกช่องทางการให้บริการที่สำคัญ โดยเฉพาะเมื่อพบรายการหรือธุรกรรมที่ผิดปกติ |
| 33. | สถาบันการเงินจำเป็นต้องมีส่วนร่วมการแลกเปลี่ยนข้อมูลด้าน Cyber Threat | สถาบันการเงินควรพิจารณาเข้าไปมีส่วนร่วมการแลกเปลี่ยนข้อมูลด้าน Cyber Threat Intelligence |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| | Intelligence ที่จัดตั้งโดยสมาคมธนาคารไทย หรือไม่ | ที่จัดตั้งโดยสมาคมธนาคารไทย เพื่อให้ภาคการเงินของประเทศไทยมีความเข้มแข็ง และการเพื่อให้เกิดแลกเปลี่ยนข้อมูลด้าน Cyber Threat ที่เป็นประโยชน์ โดยการเข้าไปมีส่วนร่วมอาจจะมีหลากหลายรูปแบบ เช่น การเข้าร่วมเป็นสมาชิก หรือเข้าร่วมเสวนาแลกเปลี่ยนในการประชุมหรือการสัมมนาต่างๆ |
| **การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ (Response and Recovery)** | | |
| 34. | สถาบันการเงินจำเป็นต้องมีการทบทวนแผนฉุกเฉินที่รองรับภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยคำนึงถึงเหตุการณ์ความเสียหายครอบคลุมสถานการณ์จำลองต่าง ๆ ที่อาจเกิดขึ้น โดยอย่างน้อยควรครอบคลุมเหตุการณ์ ดังนี้ (1) ระบบงานสำคัญที่ศูนย์คอมพิวเตอร์หลักและศูนย์สำรองไม่สามารถใช้งานได้พร้อมกัน และ (2) ข้อมูลจริงและข้อมูลชุดสำรองไม่สามารถใช้งานได้ หรือไม่ | สถาบันการเงินควรคำนึง กำหนดและทบทวนแผนฉุกเฉิน ให้ครอบคลุมถึงสถานการณ์ต่างๆ โดยเฉพาะกรณี worst case เพื่อให้มีการเตรียมพร้อมทั้งด้านระบบ กระบวนการ การสื่อสาร และการรับมือหากเกิดเหตุการณ์ขึ้นจริง โดยการทดสอบอาจทดสอบในรูปแบบที่เหมาะสมและความพร้อมของแต่ละสถาบันการเงิน เช่น การทดสอบในลักษณะ table top |
| **การบริหารความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management)** | | |
| 35. | คำจำกัดความ “บุคคลภายนอก” ตามกรอบการประเมินความพร้อมการรับมือภัยคุกคามทางไซเบอร์ หมายถึงบุคคลใดบ้าง | คำจำกัดความ “บุคคลภายนอก” ให้อ้างอิงตามประกาศและแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และแนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Guideline) โดยหมายถึง บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือข้อมูลของลูกค้าที่ควบคุมโดยสถาบันการเงินได้<br>โดยกรณีสาขาของธนาคารพาณิชย์ต่างประเทศให้รวมถึงสำนักงานใหญ่หรือสาขาอื่นในต่างประเทศที่เป็นนิติบุคคลเดียวกันด้วย<br>ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์และบริการของสถาบันการเงิน |

| ข้อ | ประเด็นคำถาม | แนวคำตอบ |
|---|---|---|
| 36. | สถาบันการเงินจำเป็นต้องกำหนดให้มีการดำเนินการประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ก่อนทำสัญญาว่าจ้างบุคคลภายนอก รวมถึงการจัดทำสัญญากับบุคคลภายนอก จำเป็นต้องระบุทุกสัญญาหรือไม่ | เจตนารมณ์ของการกำหนดให้มีการบริหารจัดการความเสี่ยงจากบุคคลภายนอก เช่น การประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ก่อนทำสัญญาว่าจ้างบุคคลภายนอก รวมถึงการจัดทำสัญญากับบุคคลภายนอก เพื่อให้สถาบันการเงินมั่นใจว่า ผู้ให้บริการภายนอกควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงความสามารถในการให้บริการทั้งในภาวะปกติและไม่ปกติ อย่างไรก็ดี ในกรณีที่สถาบันการเงินมีการเชื่อมต่อกับบุคคลภายนอกบางประเภท (เช่น หน่วยงานภาครัฐ ระบบชำระเงินกลาง เป็นต้น) อาจไม่สามารถกำหนดการควบคุมได้ตามที่กำหนดในกรอบการประเมินความพร้อมด้าน Cyber Resilience สถาบันการเงินควรพิจารณาการควบคุมอื่นทดแทน โดยให้สอดคล้องตามรูปแบบและความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการแต่ละประเภท |

**ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ**
**โทร. 0-2283-6347**