(ร่าง) ประกาศธนาคารแห่งประเทศไทย

ที่ สกช. X /2569

เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) สำหรับกลุ่มธุรกิจทางการเงิน

---

1. เหตุผลในการออกประกาศ

ปัจจุบันรูปแบบการดำเนินธุรกิจของสถาบันการเงินมีการเปลี่ยนแปลงเป็นลักษณะกลุ่มธุรกิจทางการเงินมากขึ้น ซึ่งมีการจัดตั้งบริษัทในกลุ่มธุรกิจเพื่อประกอบธุรกิจทางการเงินและธุรกิจสนับสนุนด้านเทคโนโลยีสารสนเทศแก่กลุ่มธุรกิจทางการเงิน รวมถึงบริษัทในกลุ่มธุรกิจทางการเงินมีแนวโน้มในการนำระบบเทคโนโลยีสารสนเทศมาใช้เพื่อรองรับการดำเนินธุรกิจเพิ่มมากขึ้น ในขณะเดียวกันความเสี่ยงการจากการใช้เทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์มีความซับซ้อนและมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยหากเกิดปัญหาขึ้นกับบริษัทใดบริษัทหนึ่งในกลุ่มธุรกิจทางการเงินอาจลุกลามขยายไปยังบริษัทในกลุ่มธุรกิจทางการเงินอื่นและส่งผลกระทบต่อความเชื่อมั่นและชื่อเสียงของสถาบันการเงินและกลุ่มธุรกิจทางการเงินได้ บริษัทแม่ของกลุ่มธุรกิจทางการเงินจึงจำเป็นต้องเข้าใจถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทที่อยู่ในกลุ่มธุรกิจทางการเงิน เพื่อให้สามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสมและทันการณ์

ดังนั้น ธนาคารแห่งประเทศไทย (ธปท.) จึงกำหนดหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศสำหรับกลุ่มธุรกิจทางการเงิน โดยมีหลักการสำคัญที่กำหนดให้บริษัทแม่ของกลุ่มธุรกิจทางการเงินมีหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทในกลุ่มธุรกิจทางการเงินตามระดับความเสี่ยงและความซับซ้อนของธุรกิจ เพื่อให้บริษัทในกลุ่มธุรกิจทางการเงินมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเหมาะสมและไม่ส่งผลกระทบต่อชื่อเสียงของสถาบันการเงินและกลุ่มธุรกิจทางการเงิน

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา X แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยกำหนดหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) สำหรับกลุ่มธุรกิจทางการเงิน ให้บริษัทแม่ของกลุ่มธุรกิจทางการเงิน ถือปฏิบัติตามที่กำหนดในประกาศนี้

3. ประกาศที่ยกเลิก

-

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับบริษัทแม่ของกลุ่มธุรกิจทางการเงิน ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง ยกเว้นสาขาของธนาคารพาณิชย์ต่างประเทศ

5. นิยาม

ในประกาศฉบับนี้

“เทคโนโลยีสารสนเทศ” (Information Technology: IT) หมายความว่า เทคโนโลยีสารสนเทศที่นำมาใช้ในการให้บริการหรือดำเนินธุรกิจ ซึ่งครอบคลุมถึง ข้อมูล ระบบปฏิบัติการ (operating system) ระบบงาน (application system) ระบบฐานข้อมูล (database system) อุปกรณ์คอมพิวเตอร์ (computer hardware) และระบบเครือข่ายสื่อสาร (communication) เป็นต้น

“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (Information Technology Risk: IT risk) หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threats)

“กลุ่มธุรกิจทางการเงิน” หมายความว่า กลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลโครงสร้างและขอบเขตธุรกิจของกลุ่มธุรกิจทางการเงินของธนาคารพาณิชย์

“บริษัทในกลุ่มธุรกิจทางการเงินที่มีนัยสำคัญ” หมายความว่า บริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์เกี่ยวกับการกำกับดูแลโครงสร้างและขอบเขตธุรกิจของกลุ่มธุรกิจทางการเงินที่บริษัทแม่ของกลุ่มธุรกิจทางการเงินพิจารณาแล้วว่ามีความสำคัญต่อกลุ่มธุรกิจทางการเงิน และบริษัทในกลุ่มธุรกิจทางการเงินที่ประกอบธุรกิจเกี่ยวกับสินทรัพย์ดิจิทัล

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศแทนบริษัทในกลุ่มธุรกิจทางการเงิน หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัทในกลุ่มธุรกิจทางการเงิน หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของบริษัทในกลุ่มธุรกิจทางการเงิน หรือข้อมูลลูกค้าที่ควบคุมดูแลโดยบริษัทในกลุ่มธุรกิจทางการเงินได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงสมาชิกหรือลูกค้าที่ใช้ผลิตภัณฑ์และบริการของบริษัทในกลุ่มธุรกิจทางการเงิน

“ธปท.” หมายความว่า ธนาคารแห่งประเทศไทยตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

6. หลักการ

บริษัทแม่ของกลุ่มธุรกิจทางการเงินมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของกลุ่มธุรกิจทางการเงิน เพื่อให้สามารถบริหารจัดการ ควบคุมดูแลและติดตามความเสี่ยงที่อาจส่งผลกระทบต่อกลุ่มธุรกิจทางการเงินได้อย่างเหมาะสมและทันการณ์ ครอบคลุม (1) การจัดให้มีนโยบายสำคัญด้านเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน สำหรับให้บริษัทในกลุ่มธุรกิจทางการเงินใช้เป็นแนวทางในการบริหารจัดการความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยีสารสนเทศ (2) การมีโครงสร้างการกำกับดูแลความเสี่ยงของบริษัทแม่ที่ครอบคลุมการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (3) กำกับดูแลให้บริษัทในกลุ่มธุรกิจทางการเงินมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความมีนัยสำคัญต่อกลุ่มธุรกิจทางการเงิน รวมถึงติดตามประเด็นความเสี่ยงและเหตุการณ์สำคัญด้านเทคโนโลยีสารสนเทศที่อาจส่งผลกระทบต่อกลุ่มธุรกิจทางการเงินอย่างเท่าทัน

7. บทบาทหน้าที่ของบริษัทแม่ของกลุ่มธุรกิจทางการเงิน

บริษัทแม่ของกลุ่มธุรกิจทางการเงินมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของกลุ่มธุรกิจทางการเงิน อย่างน้อยครอบคลุมดังต่อไปนี้

7.1 กำหนดนโยบายที่สำคัญสำหรับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน ได้แก่ (1) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และ (2) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยนโยบายดังกล่าวต้องได้รับการอนุมัติจากคณะกรรมการของบริษัทแม่ของกลุ่มธุรกิจทางการเงิน รวมถึงทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ทั้งนี้ คณะกรรมการของบริษัทแม่ของกลุ่มธุรกิจทางการเงินสามารถมอบหมายให้คณะกรรมการชุดย่อยในระดับการกำกับดูแล (oversight level) ทำหน้าที่ทบทวนนโยบายที่สำคัญได้ หากเป็นการเปลี่ยนแปลงที่ไม่มีนัยสำคัญ โดยต้องมีการรายงานคณะกรรมการของบริษัทแม่ของกลุ่มธุรกิจทางการเงินเพื่อทราบภายหลังด้วย

7.2 มีโครงสร้างองค์กรของบริษัทแม่ที่เอื้อต่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน โดยมีการกำหนดกระบวนการและบทบาทหน้าที่ของหน่วยงานที่ทำหน้าที่ควบคุม กำกับ และตรวจสอบความเสี่ยงสำคัญด้านเทคโนโลยีสารสนเทศ ตลอดจนติดตามประเด็นปัญหาด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญของกลุ่มธุรกิจทางการเงิน เพื่อกำกับดูแลไม่ให้ส่งผลกระทบต่อชื่อเสียงและความเชื่อมั่นของกลุ่มธุรกิจทางการเงิน

7.3 กำกับดูแลให้บริษัทในกลุ่มธุรกิจทางการเงินมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามความมีนัยสำคัญต่อกลุ่มธุรกิจทางการเงิน ดังนี้

7.3.1 กำกับดูแลให้บริษัทในกลุ่มธุรกิจทางการเงินที่มีนัยสำคัญ มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีระเบียบวิธีปฏิบัติและกระบวนการควบคุมดูแลให้มีการรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้ และความพร้อมใช้งาน สอดคล้องตามแนวทางการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามรายละเอียดแนบ 1

7.3.2 กำกับดูแลให้บริษัทในกลุ่มธุรกิจทางการเงินที่ไม่เข้าข่ายเป็นบริษัทในกลุ่มธุรกิจทางการเงินที่มีนัยสำคัญ มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีระเบียบวิธีปฏิบัติและกระบวนการควบคุมดูแลให้มีการรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้ และความพร้อมใช้งาน ตามรายละเอียดแนบ 2

ทั้งนี้ การกำหนดบริษัทในกลุ่มธุรกิจทางการเงินที่มีนัยสำคัญข้างต้น ธปท.อาจจะสั่งการเป็นอย่างอื่นก็ได้

8. การรายงานต่อ ธปท.

เพื่อให้ ธปท. สามารถกำกับดูแลและติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงินได้เท่าทัน และสามารถติดตามปัญหาหรือเหตุการณ์ภัยคุกคามทางไซเบอร์ได้ทันต่อสถานการณ์ ให้บริษัทแม่ของกลุ่มธุรกิจทางการเงินรายงานเหตุการณ์ถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ด้านไซเบอร์ที่ถูกโจมตีสำเร็จที่มีผลกระทบกับกลุ่มธุรกิจทางการเงินอย่างมีนัยสำคัญต่อ ธปท. ทันทีเมื่อเกิดเหตุหรือรับรู้ปัญหาหรือเหตุการณ์นั้นตามรูปแบบและช่องทางที่ ธปท. กำหนดและแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมในภายหลัง

ทั้งนี้ ในกรณีที่มีหลักเกณฑ์การรายงานปัญหาหรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งกำหนดให้บริษัทในกลุ่มธุรกิจทางการเงินต้องรายงานต่อ ธปท. ไว้เป็นการเฉพาะแล้ว บริษัทแม่ของกลุ่มธุรกิจไม่ต้องดำเนินการตามวรรคแรก แต่ให้บริษัทในกลุ่มธุรกิจทางการเงินนั้นรายงานเหตุการณ์ดังกล่าวต่อบริษัทแม่ของกลุ่มธุรกิจทางการเงินทราบ เพื่อให้บริษัทแม่ของกลุ่มธุรกิจทางการเงินสามารถติดตามเหตุการณ์ความเสี่ยงในภาพรวมได้อย่างมีประสิทธิภาพ

9. การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่บริษัทแม่ของกลุ่มธุรกิจทางการเงิน มีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ได้ ให้ยื่นขออนุญาตผ่อนผันเป็นรายกรณีต่อ ธปท. ก่อนครบกำหนดระยะเวลาตามที่ประกาศนี้กำหนด พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธปท. จะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ

นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดย ธปท. อาจจะพิจารณาอนุญาตหรือไม่ก็ได้ หรือกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

10. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่ X วันถัดจากวันประกาศในราชกิจจานุเบกษาต่อไป

ประกาศ ณ วันที่ มีนาคม 2569

(นายวิทัย รัตนากร)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์

เอกสารแนบ 1

การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัทแม่ของกลุ่มธุรกิจทางการเงินมีหน้าที่ต้องกำกับดูแลให้บริษัทในกลุ่มธุรกิจทางการเงินที่มีนัยสำคัญให้ถือปฏิบัติ ดังนี้

1. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

จัดให้มีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม นอกจากนี้ ต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมถึงบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้หมดอายุการใช้งานหรือสิ้นสุดการให้บริการอย่างเหมาะสมและเท่าทันกับความเสี่ยง เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย พร้อมใช้งานและสามารถรองรับการให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

2. การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสอดคล้องตามระดับชั้นความลับของข้อมูล (information classification) ครอบคลุมข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่ายสื่อสาร (data-in-transit) และข้อมูลที่อยู่บนระบบงานหรือสื่อบันทึกข้อมูล (data-at-rest) รวมทั้งจัดให้มีกระบวนการบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากลที่ยอมรับโดยทั่วไป โดยอย่างน้อยต้องเข้ารหัสข้อมูลสำคัญที่อยู่ระหว่างการรับผ่านส่งเครือข่ายสื่อสารและข้อมูลสำคัญที่จัดเก็บบนระบบงาน สื่อบันทึกข้อมูลและอุปกรณ์ที่ใช้ปฏิบัติงาน เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

3. การควบคุมการเข้าถึง (access control)

จัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิ โดยต้องครอบคลุมอย่างน้อย ดังนี้

3.1 บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ต้องมีการกำหนดมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานที่มีสิทธิสูงอย่างเข้มงวด สอดคล้องกับหลักการให้สิทธิตามความจำเป็น (least privilege) เช่น การมอบหมายสิทธิ การเบิกใช้ กำหนดระยะเวลา

3.2 จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้

(1) บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ทุกบัญชีของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย

(2) บัญชีผู้ใช้งาน (user) ทุกบัญชีที่สามารถเข้าถึงข้อมูลลูกค้าและเชื่อมต่อมาจากระบบเครือข่ายสื่อสารสาธารณะ

ในกรณีที่ระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีวิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย

อย่างไรก็ตาม กรณีที่ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

4. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่อง

5. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น รวมทั้งพร้อมรองรับการให้บริการได้อย่างต่อเนื่อง

6. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

รักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

6.1 บริหารจัดการขีดความสามารถของระบบเทคโนโลยีสารสนเทศและระบบสาธารณูปโภค (capacity management) เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับการให้บริการหรือดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต สำหรับระบบที่มีการให้บริการผ่าน

ช่องทางดิจิทัลควรมีการติดตามและประเมินขีดความสามารถของระบบอย่างใกล้ชิด รองรับบริการและปริมาณธุรกรรมที่เพิ่มขึ้นอย่างรวดเร็ว

6.2 รักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) ให้สามารถป้องกันการโจมตีด้วยรูปแบบต่าง ๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) รวมทั้งติดตามให้มีการปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตี และป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต

6.3 สำรองข้อมูล (data backup) ด้วยวิธีการและระยะเวลาที่เหมาะสมกับความเสี่ยงและความสำคัญของข้อมูล เช่น การสำรองข้อมูลประจำวัน และกำหนดให้มีการทดสอบความพร้อมใช้ของข้อมูลสำรองเป็นประจำสม่ำเสมอ เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

6.4 จัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญอย่างครบถ้วนและปลอดภัย เช่น การจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (access log) และบันทึกการดำเนินงาน (activity log) เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูลและใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ได้ตามที่กฎหมายกำหนด

6.5 ติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือสำหรับติดตามภัยคุกคามใหม่ ๆ และตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

6.6 บริหารจัดการช่องโหว่ (vulnerability management) โดยระบบงานสำคัญต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งกำหนดแนวทางการดำเนินการและระยะเวลาในการแก้ไขช่องโหว่ให้สอดคล้องตามระดับความเสี่ยงและความสำคัญของระบบงาน

6.7 จัดให้มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระ อย่างน้อยครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบ ความเสี่ยง หรือมาตรฐานสากลด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ เป็นต้น เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

6.8 บริหารจัดการการเปลี่ยนแปลง (change management) โดยจัดให้มีกระบวนการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง (system deployment) การตั้งค่าระบบ (system configuration) การติดตั้ง patch เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

6.9 บริหารจัดการการตั้งค่าระบบ (system configuration management) โดยจัดให้มีการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยสอดคล้องกับมาตรฐานดังกล่าว (security hardening) ครอบคลุมระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้งดำเนินการตั้งค่าและสอบทานการตั้งค่าอย่างสม่ำเสมอตามที่ได้กำหนดไว้ เพื่อให้มั่นใจว่าระบบงานที่รองรับการให้บริการมีการรักษาความมั่นคงปลอดภัยขั้นต่ำตามมาตรฐานที่กำหนดไว้

ในกรณีที่ไม่สามารถปฏิบัติตามมาตรฐานที่ตนได้กำหนดไว้ข้างต้น ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

6.10 บริหารจัดการ patch (patch management) โดยต้องจัดให้มีกระบวนการบริหารจัดการ security patch ในทุกระบบงานและอุปกรณ์ เพื่อเป็นการลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศจะถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่และระดับความสำคัญของระบบงาน

ในกรณีที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

นอกจากนี้ กรณีที่ไม่สามารถติดตั้ง security patch ได้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

7. การจัดหาและการพัฒนาระบบ (system acquisition and development)

7.1 การจัดหาระบบ (system acquisition)

จัดให้มีหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและบุคคลภายนอกที่ให้บริการ เช่น ความน่าเชื่อถือของระบบ บุคคลภายนอกที่ให้บริการที่รับการรับรองตามมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป (certificate) ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ เป็นต้น เพื่อให้มั่นใจว่าระบบและบุคคลภายนอกที่ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินการได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการที่เป็นบุคคลภายนอก การเปลี่ยนแปลงเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจในอนาคต

7.2 การพัฒนาระบบ (system development)

ออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีการรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยต้องดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- มีรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

- มีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของคำสั่งเขียนโปรแกรม (source code version control)

- แบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบและผู้นำระบบขึ้นใช้งานจริง

- แบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)

- ทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (unit test) ทดสอบการทำงานร่วมกันของระบบต่าง ๆ (system integration test) ทดสอบความต้องการของผู้ใช้งาน (user acceptance test) และทดสอบความปลอดภัยของระบบ (security test) ตามกระบวนการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) ทดสอบความพร้อมใช้งานของระบบสำรอง

- ทดสอบประสิทธิภาพ (performance test) และความสามารถในการให้บริการเมื่อมีการใช้บริการจำนวนมาก เมื่อมีการพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์

- มีแนวทางควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

- จัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

8. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)

จัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติ ปัญหา และการแก้ไข ให้แก่คณะกรรมการที่ได้รับมอบหมาย ในระยะเวลาที่เหมาะสม นอกจากนี้ ต้องวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

9. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT disaster recovery plan)

9.1 มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT disaster recovery plan: IT DRP) โดยแผนดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย

9.2 จัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยคำนึงถึงลักษณะการให้บริการ การดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากบุคคลภายนอก (third party risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และความเสี่ยงที่มีผลกระทบต่อระบบสถาบันการเงิน (systemic risk) เป็นต้น

9.3 แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องมีความเป็นไปได้ในทางปฏิบัติ สามารถนำมาใช้รองรับความเสียหายที่เกิดขึ้นได้จริง และสอดคล้องกับหลักเกณฑ์อื่นที่เกี่ยวข้องของธนาคารแห่งประเทศไทย โดยการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรสอดคล้องกับ ระยะเวลาในการกู้คืนระบบ (recover time objective : RTO) ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point object : RPO) และระยะเวลาสูงสุดที่ยอมให้การให้บริการหรือธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD) เพื่อรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่องของบริษัท

9.4 มีคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์และฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้

9.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

9.6 มีศูนย์คอมพิวเตอร์สำรอง (disaster recovery site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก (primary site) หยุดชะงัก โดยศูนย์คอมพิวเตอร์สำรองควรอยู่ห่างจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะมิให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง และภัยธรรมชาติ เป็นต้น

10. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

ในกรณีที่มีการดำเนินการดังต่อไปนี้ (1) ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) (2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือ (3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของบริษัทในกลุ่มธุรกิจทางการเงิน หรือเข้าถึงข้อมูลลูกค้าในรูปแบบอิเล็กทรอนิกส์ ต้องมีการกำกับดูแลความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์จากการดำเนินการดังกล่าว ให้สอดคล้องตามระดับความเสี่ยงบนพื้นฐานที่ต้องรับผิดชอบต่อการให้บริการหรือดำเนินธุรกิจแก่กลุ่มธุรกิจทางการเงินหรือลูกค้า และคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิภาพในการให้บริการ ตามหลักการดังนี้

10.1 กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างบริษัทกับบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร สำหรับกรณีบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ที่มีนัยสำคัญ ต้องระบุให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบของบริษัทแม่ ผู้ตรวจสอบ

ภายนอก มีสิทธิเข้าตรวจสอบ การดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกรายดังกล่าว เป็นเงื่อนไขในสัญญาหรือข้อตกลง ระหว่างบริษัทกับบุคคลภายนอกดังกล่าวด้วย

สำหรับกรณีที่ไม่สามารถระบุสิทธิให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอกมีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ในเงื่อนไขสัญญาหรือข้อตกลงกับบุคคลภายนอก บริษัทต้องมั่นใจว่าบุคคลภายนอกรายดังกล่าวมีผลการตรวจสอบจากผู้ตรวจสอบภายนอกที่เป็นอิสระทดแทน

10.2 กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ และความเสี่ยงจากการกระจุกตัว (concentration risk) เนื่องจากใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการที่เป็นบุคคลภายนอกรายใดรายหนึ่ง (third party/vendor locked-in)

10.3 รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ของบริษัท และสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป

10.4 เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการให้บริการกับกลุ่มธุรกิจทางการเงิน หรือลูกค้า

เอกสารแนบ 2

การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขั้นต่ำ

บริษัทแม่ของกลุ่มธุรกิจทางการเงินมีหน้าที่ต้องกำกับดูแลให้บริษัทในกลุ่มธุรกิจทางการเงินที่ไม่เข้าข่ายเป็นบริษัทในกลุ่มธุรกิจทางการเงินที่มีนัยสำคัญให้ถือปฏิบัติ ดังนี้

1. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

จัดให้มีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม นอกจากนี้ ต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมถึงบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้หมดอายุการใช้งานหรือสิ้นสุดการให้บริการอย่างเหมาะสมและเท่าทันกับความเสี่ยง เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย พร้อมใช้งานและสามารถรองรับการให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

2. การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสอดคล้องตามระดับชั้นความลับของข้อมูล (information classification) ครอบคลุมข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่ายสื่อสาร (data-in-transit) และข้อมูลที่อยู่บนระบบงานหรือสื่อบันทึกข้อมูล (data-at-rest) รวมทั้งจัดให้มีกระบวนการบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากลที่ยอมรับโดยทั่วไป โดยอย่างน้อยต้องเข้ารหัสข้อมูลสำคัญที่อยู่ระหว่างการรับผ่านส่งเครือข่ายสื่อสารและข้อมูลสำคัญที่จัดเก็บบนระบบงาน สื่อบันทึกข้อมูลและอุปกรณ์ที่ใช้ปฏิบัติงาน เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

3. การควบคุมการเข้าถึง (access control)

จัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิ โดยต้องครอบคลุมอย่างน้อย ดังนี้

3.1 บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ต้องมีการกำหนดมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานที่มีสิทธิสูงอย่างเข้มงวด สอดคล้องกับหลักการให้สิทธิตามความจำเป็น (least privilege) เช่น การมอบหมายสิทธิ การเบิกใช้ กำหนดระยะเวลา

3.2 จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้

(1) บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ทุกบัญชีของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย

(2) บัญชีผู้ใช้งาน (user) ทุกบัญชีที่สามารถเข้าถึงข้อมูลลูกค้าและเชื่อมต่อมาจากระบบเครือข่ายสื่อสารสาธารณะ

ในกรณีที่ระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีวิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย

อย่างไรก็ตาม กรณีที่ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

4. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น รวมทั้งพร้อมรองรับการให้บริการได้อย่างต่อเนื่อง

5. การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint)

จัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) ให้สามารถป้องกันภัยจากโปรแกรมไม่ประสงค์ดี (malware) รวมทั้งติดตามปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตี และป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต

6. การสำรองข้อมูล (data backup)

สำรองข้อมูลด้วยวิธีการและระยะเวลาที่เหมาะสมกับความเสี่ยงและความสำคัญของข้อมูล เช่น การสำรองข้อมูลประจำวัน และกำหนดให้มีการทดสอบความพร้อมใช้ของข้อมูลสำรองเป็นประจำสม่ำเสมอ เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

7. การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

จัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญอย่างครบถ้วนและปลอดภัย เช่น การจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (access log) และ

บันทึกการดำเนินงาน (activity log) เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูล และใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

8. การเฝ้าระวังภัยคุกคาม (security monitoring)

จัดให้มีการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม โดยมีกระบวนการหรือเครื่องมือสำหรับติดตามภัยคุกคามใหม่ ๆ และตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

9. การบริหารจัดการช่องโหว่ (vulnerability management)

จัดให้มีการประเมินช่องโหว่ สำหรับทุกระบบงานตามระดับความเสี่ยง โดยระบบงานสำคัญต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งกำหนดแนวทางการดำเนินการและระยะเวลาในการแก้ไขช่องโหว่ให้สอดคล้องตามระดับความเสี่ยงและความสำคัญของระบบงาน

10. การทดสอบเจาะระบบ (penetration testing)

จัดให้มีการทดสอบเจาะระบบ โดยผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระอย่างน้อยครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบ ความเสี่ยง หรือมาตรฐานสากลด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ เป็นต้น เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

11. การบริหารจัดการการเปลี่ยนแปลง (change management)

จัดให้มีกระบวนการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง (system deployment) การตั้งค่าระบบ (system configuration) การติดตั้ง patch เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

12. การกำหนดด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (security baseline and hardening)

จัดให้มีการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยสอดคล้องกับมาตรฐานดังกล่าว (security hardening) ครอบคลุมระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญ ให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้ง

ดำเนินการตั้งค่าและสอบทานการตั้งค่าอย่างสม่ำเสมอตามที่ได้กำหนดไว้ เพื่อให้มั่นใจว่าระบบงานที่รองรับการให้บริการมีการรักษาความมั่นคงปลอดภัยขั้นต่ำตามมาตรฐานที่กำหนดไว้

ในกรณีที่บริษัทไม่สามารถปฏิบัติตามมาตรฐานที่ตนได้กำหนดไว้ข้างต้น ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

13. การบริหารจัดการ security patch (security patch management)

จัดให้มีกระบวนการบริหารจัดการ security patch สำหรับทุกระบบงานและอุปกรณ์ เพื่อเป็นการลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่และระดับความสำคัญของระบบงาน

ในกรณีที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ บริษัทต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

นอกจากนี้ กรณีที่ไม่สามารถติดตั้ง security patch ได้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมเพื่อลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศจะถูกโจมตี

14. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

ในกรณีที่บริษัทดำเนินการดังต่อไปนี้ (1) ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) (2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือ (3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของบริษัทและกลุ่มธุรกิจทางการเงิน หรือเข้าถึงข้อมูลลูกค้าในรูปแบบอิเล็กทรอนิกส์ บริษัทต้องกำกับดูแลความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์จากการดำเนินการดังกล่าว ให้สอดคล้องตามระดับความเสี่ยงบนพื้นฐานที่ต้องรับผิดชอบต่อการให้บริการหรือดำเนินธุรกิจแก่กลุ่มธุรกิจทางการเงินหรือลูกค้า และคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิภาพในการให้บริการตามหลักการดังนี้

14.1 กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างบริษัทกับบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร สำหรับกรณีบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ที่มีนัยสำคัญ ต้องระบุให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบของบริษัทแม่ ผู้ตรวจสอบภายนอก มีสิทธิเข้าตรวจสอบ การดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกรายดังกล่าว เป็นเงื่อนไขในสัญญาหรือข้อตกลง ระหว่างบริษัทกับบุคคลภายนอกดังกล่าวด้วย

สำหรับกรณีที่ไม่สามารถระบุสิทธิให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยี

สารสนเทศ (IT outsourcing) ในเงื่อนไขสัญญาหรือข้อตกลงกับบุคคลภายนอก บริษัทต้องมั่นใจว่าบุคคลภายนอกรายดังกล่าวมีผลการตรวจสอบจากผู้ตรวจสอบภายนอกที่เป็นอิสระทดแทน

14.2 กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ

14.3 รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์บริษัทและสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป

14.4 เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการให้บริการหรือดำเนินธุรกิจแก่กลุ่มธุรกิจทางการเงินหรือลูกค้า