ธนาคารแห่งประเทศไทย

9 พฤศจิกายน 2566

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง
สถาบันการเงินเฉพาะกิจทุกแห่ง

ที่ ฝตท.(01) ว. 20/2566 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

เทคโนโลยีสารสนเทศเป็นโครงสร้างพื้นฐานสำคัญสำหรับการดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจทั้งในด้านการเพิ่มประสิทธิภาพการดำเนินงาน ส่งเสริมให้ประชาชนสามารถเข้าถึงบริการทางการเงินได้ดียิ่งขึ้น รวมทั้งมีการนำเทคโนโลยีสารสนเทศต่าง ๆ มาประยุกต์ใช้เพิ่มมากขึ้น อาทิ การใช้เทคโนโลยี cloud computing เพื่อให้การจัดการระบบมีความยืดหยุ่น การปรับปรุงระบบให้รองรับการปฏิบัติงานในลักษณะใหม่ ๆ เช่น การทำงานจากภายนอกองค์กร (work from anywhere) อย่างไรก็ตาม ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภัยคุกคามไซเบอร์ รวมทั้งภัยทุจริตทางการเงินยังคงเกิดขึ้นอย่างต่อเนื่อง โดยมีรูปแบบหลากหลายและซับซ้อนขึ้น

ธนาคารแห่งประเทศไทย (ธปท.) จึงได้ปรับปรุงหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจ มีการกำกับดูแลและบริหารจัดการเท่าทันความเสี่ยงจากการใช้เทคโนโลยีที่เปลี่ยนแปลงไป โดยสามารถสรุปสาระสำคัญของการปรับปรุงหลักเกณฑ์ได้ดังนี้

1. สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องดูแลระบบงานที่รองรับช่องทางการให้บริการผ่านอุปกรณ์เคลื่อนที่ (mobile banking) ให้สามารถให้บริการได้อย่างต่อเนื่องโดยต้องหยุดชะงักไม่เกิน 8 ชั่วโมง ในรอบ 1 ปีปฏิทิน

2. สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk self-assessment) ให้ ธปท. ภายใน 30 วัน นับแต่วันสิ้นปีปฏิทิน ตามรูปแบบและช่องทางที่ ธปท. กำหนด

นอกจากนี้ ธปท. ขอนำส่งแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management implementation guideline) และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management implementation guideline) ซึ่งมีหลักการที่สอดคล้องกับประกาศฉบับนี้มาพร้อมกัน เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้เป็นแนวทางสำหรับการกำหนดวิธีปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการความเสี่ยงจากบุคคลภายนอก โดยเหมาะสมตามลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีที่นำมาใช้ และความเสี่ยงที่เกี่ยวข้อง

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวอโรรา อุนนะนันทน์)
ผู้อำนวยการอาวุโส ฝ่ายกำกับและตรวจสอบความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. ประกาศธนาคารแห่งประเทศไทย ที่ สกช. 5/2566 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
2. แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
3. แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6445
E-Mail ITSupervision@bot.or.th

หมายเหตุ [X] ธปท. จัดประชุมชี้แจงในวันที่ 10 พฤศจิกายน 2564 ณ. ธปท. และ เดือนตุลาคม 2565 ผ่าน ระบบ BOT Survey
[ ] ไม่มีการประชุมชี้แจง

ประกาศธนาคารแห่งประเทศไทย
ที่ สกช. 5 /2566
เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

---

1. เหตุผลในการออกประกาศ

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) มีบทบาทสำคัญสำหรับการดำเนินธุรกิจของสถาบันการเงิน และสถาบันการเงินเฉพาะกิจ โดยนำมาใช้เป็นโครงสร้างพื้นฐานสำคัญที่ช่วยเพิ่มประสิทธิภาพ ลดต้นทุนในการดำเนินงาน รวมถึงอำนวยความสะดวกและช่วยให้เข้าถึงบริการทางการเงินได้มากยิ่งขึ้น รวมทั้งมีการประยุกต์ใช้เทคโนโลยีสารสนเทศต่าง ๆ เพิ่มมากขึ้น อาทิ การใช้ cloud computing กับระบบงานสำคัญ (critical system) เพื่อช่วยให้การจัดการระบบมีความยืดหยุ่น เพิ่มประสิทธิภาพ หรือการปรับระบบให้สามารถรองรับการทำงานลักษณะใหม่ ๆ เช่น การทำงานจากภายนอกสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (work from anywhere) อย่างไรก็ดี ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk หรือ IT risk) ภัยคุกคามทางไซเบอร์ (cyber threat) รวมทั้งภัยทุจริตทางการเงินมีความหลากหลายและยังคงเกิดขึ้นอย่างต่อเนื่อง ส่งผลกระทบรุนแรงเป็นวงกว้างมากขึ้น ดังนั้น หากสถาบันการเงินและสถาบันการเงินเฉพาะกิจมีการบริหารจัดการความเสี่ยงภายใน และการบริหารจัดการความเสี่ยงจากบุคคลภายนอกที่ไม่รัดกุมเพียงพอ หรือขาดความพร้อมการรับมือการโจมตีทางไซเบอร์ อาจก่อให้เกิดความเสี่ยงและส่งผลกระทบต่อการให้บริการ ความเชื่อมั่นของลูกค้า รวมถึงต่อระบบสถาบันการเงินโดยรวม

ธนาคารแห่งประเทศไทย (ธปท.) จึงเห็นควรปรับปรุงหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) ให้เท่าทันกับความเสี่ยงและรูปแบบการปฏิบัติงานที่เปลี่ยนแปลงไป เพื่อให้มีความยืดหยุ่น คล่องตัว เพิ่มความชัดเจน ลดภาระในการปฏิบัติตามประกาศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ โดยได้รวมหลักเกณฑ์ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจไว้ในประกาศฉบับเดียวกัน นอกจากนี้กำหนดเพิ่มเติมให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจทำแบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วยตนเอง (IT risk self-assessment) เป็นประจำทุกปี เพื่อส่งเสริมให้เกิดการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วยตนเอง (self-regulated) ที่เข้มแข็งยิ่งขึ้น รวมทั้งกำหนดให้ในรอบ 1 ปีปฏิทินสถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีการให้บริการทางการเงินผ่าน mobile banking application ต้องดูแลให้ระบบงานหยุดชะงักไม่เกิน 8 ชั่วโมง

นอกจากนี้ ธปท. ได้ปรับปรุงแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติการบริหารจัดการความเสี่ยงบุคคลภายนอก เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจ สามารถนำไปประยุกต์ใช้ได้ตามความเหมาะสม สอดคล้องตามขอบเขตและระดับความเสี่ยงที่เผชิญ ทั้งนี้ สำหรับความเสี่ยงจากภัยคุกคามไซเบอร์ สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถนำกรอบการประเมินความพร้อมด้าน Cyber Resilience (Cyber Resilience Assessment Framework : CRAF) มาใช้เพื่อประเมินความเสี่ยงที่เกิดจากภัยไซเบอร์และการควบคุมขั้นต่ำที่ควรมีเพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดจากภัยดังกล่าวได้

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 41 มาตรา 47 และมาตรา 71 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) ให้สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศนี้

อาศัยอำนาจตามความในมาตรา 120/1 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่แก้ไขเพิ่มเติม ธนาคารแห่งประเทศไทยโดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลังออกหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) ให้สถาบันการเงินเฉพาะกิจถือปฏิบัติตามที่กำหนดในประกาศนี้

3. ประกาศที่ยกเลิก

ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk) ของสถาบันการเงิน ลงวันที่ 1 ตุลาคม 2562

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับ

4.1 สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

4.2 สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

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 ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของสถาบันการเงินหรือสถาบันการเงินเฉพาะกิจ รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threats)

“สถาบันการเงิน” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศแทนสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบ

เทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือข้อมูลลูกค้าของสถาบันการเงินและสถาบันการเงินเฉพาะกิจในรูปแบบอิเล็กทรอนิกส์ได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์และบริการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

"ธปท." หมายความว่า ธนาคารแห่งประเทศไทยตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

6. หลักการ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีหน้าที่เกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

6.1 ดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงโครงการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและรัดกุม ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ (1) การรักษาความลับของระบบและข้อมูล (confidentiality) (2) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ (3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) โดยอยู่บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า

6.2 กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านชื่อเสียง ความเสี่ยงจากภัยทุจริตทางการเงินและความเสี่ยงด้านกฎหมาย รวมถึงให้ความสำคัญกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (enterprise risk management: ERM)

6.3 มีโครงสร้างการกำกับดูแลในภาพรวมที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence)

ทั้งนี้ กรณีที่สถาบันการเงินมีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์สำหรับบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง การพิจารณาโครงสร้างการกำกับดูแลตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence) ให้พิจารณาจากภาพรวมทั้งหมดของกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องกันได้ อย่างไรก็ดี สถาบันการเงินและคณะกรรมการของสถาบันการเงินในประเทศไทยยังคงต้องรับผิดชอบต่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเสมือนสถาบันการเงินดำเนินการเอง

7. หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีหน้าที่ต้องปฏิบัติตามหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

7.1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)

จัดให้มีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ตั้งแต่คณะกรรมการของสถาบันการเงินหรือคณะกรรมการของสถาบันการเงินเฉพาะกิจและผู้บริหารระดับสูงที่ให้ความสำคัญในการผลักดันและยกระดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำหนดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ สื่อสารและกำกับดูแลให้มีการปฏิบัติตามนโยบายที่กำหนด นอกจากนี้ต้องจัดให้มีผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งสร้างวัฒนธรรมและพฤติกรรมร่วมของทุกคนในองค์กรให้ตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง (รายละเอียดในเอกสารแนบ 1)

7.2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security management)

จัดให้มีการบริหารจัดการและควบคุมระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีการรักษาความลับของระบบและข้อมูล ถูกต้องเชื่อถือได้ และพร้อมใช้งาน โดยนำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (รายละเอียดในเอกสารแนบ 2)

7.3 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

จัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างครอบคลุมทั่วทั้งองค์กร โดยประสานงานร่วมกับหน่วยงานธุรกิจและหน่วยงานด้านเทคโนโลยีสารสนเทศ ในการระบุและประเมินความเสี่ยง การกำหนดมาตรการในการลดความเสี่ยงและระบบการควบคุมภายใน เพื่อให้มั่นใจว่ามีการบริหารความเสี่ยงอย่างเหมาะสมสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (รายละเอียดในเอกสารแนบ 3)

7.4 การปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

จัดให้มีการติดตามดูแล และสอบทานการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายว่าด้วยระบบการชำระเงิน เป็นต้น เพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและกฎเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง (รายละเอียดในเอกสารแนบ 4)

7.5 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบที่มีความเป็นอิสระ รวมทั้งต้องติดตามให้มีการปรับปรุงแก้ไขประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยงและการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศอย่างเพียงพอเหมาะสม (รายละเอียดในเอกสารแนบ 5)

7.6 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

กำหนดกรอบการบริหารจัดการโครงการ (project management framework) และโครงสร้างการกำกับดูแลโครงการ เพื่อให้โครงการที่มีนัยสำคัญมีการบริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดให้มีประสิทธิภาพสูงสุด เลือกใช้เทคโนโลยีอย่างเหมาะสม สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้ (รายละเอียดในเอกสารแนบ 6)

ทั้งนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถพิจารณาประยุกต์ใช้แนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก เพื่อเป็นแนวทางการบริหารจัดการความเสี่ยงให้เหมาะสมและสอดคล้องตามขอบเขตและระดับความเสี่ยงได้

8. การดูแลระบบงานที่รองรับช่องทางการให้บริการทางอุปกรณ์เคลื่อนที่ (mobile banking) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

ในรอบ 1 ปีปฏิทิน สถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีการให้บริการทางการเงินผ่านช่องทาง mobile banking application ต้องดูแลให้ระบบเทคโนโลยีสารสนเทศให้บริการได้อย่างต่อเนื่อง โดยต้องหยุดชะงักไม่เกิน 8 ชั่วโมง รวมทั้งต้องดูแลให้มีการกู้คืนระบบให้กลับมาให้บริการได้โดยเร็ว

9. ข้อกำหนดในการพิจารณาความมีนัยสำคัญเพื่อดำเนินการตามประกาศนี้

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีข้อกำหนดในการพิจารณาความมีนัยสำคัญที่ชัดเจนเพื่อใช้พิจารณาดำเนินการในเรื่องต่าง ๆ ที่กำหนดไว้ตามประกาศฉบับนี้ โดยดำเนินการดังนี้

9.1 ข้อกำหนดดังกล่าวต้องผ่านการพิจารณาความมีนัยสำคัญร่วมกันของหน่วยงานที่เกี่ยวข้อง โดยเฉพาะหน่วยงานซึ่งทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (first line of defence) และหน่วยงานซึ่งทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (second line of defence) รวมทั้งต้องได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย

9.2 ข้อกำหนดในการพิจารณาความมีนัยสำคัญ ต้องพิจารณาภายใต้กรอบหลักการที่คำนึงถึงความเสี่ยงและผลกระทบต่อการให้บริการหรือดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจในวงกว้าง (bank wide impact) และผลกระทบต่อระบบสถาบันการเงินในวงกว้าง (banking system wide impact)

9.3 ต้องสื่อสารและเผยแพร่ข้อกำหนดดังกล่าวให้หน่วยงานที่เกี่ยวข้องทราบโดยทั่วกันและนำไปปฏิบัติ

9.4 ต้องสอบทานการดำเนินการตามข้อกำหนดอย่างน้อยปีละ 1 ครั้ง

9.5 ต้องทบทวนข้อกำหนดอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญเพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบต่อสถาบันการเงินหรือสถาบันการเงินเฉพาะกิจและระบบสถาบันการเงิน

10. การแจ้ง การรายงาน หรือการขออนุญาต ต่อ ธปท.

เพื่อให้ ธปท. สามารถกำกับดูแลและติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ รวมถึงความเสี่ยงของระบบสถาบันการเงินในภาพรวมได้เท่าทันกับการเปลี่ยนแปลง และสามารถติดตามปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศหรือภัยคุกคามทางไซเบอร์ได้ทันต่อสถานการณ์ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องแจ้งการรายงานหรือขออนุญาตต่อ ธปท. ดังต่อไปนี้

10.1 การแจ้งหรือการขออนุญาตนำเทคโนโลยีสารสนเทศมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

10.1.1 ธนาคารพาณิชย์ที่นำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนดที่ธนาคารพาณิชย์ได้กำหนดขึ้นตามข้อ 9 ทั้งกรณีที่ธนาคารพาณิชย์ดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้องแจ้งการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวต่อ ธปท. ตามที่กำหนดในคู่มือสำหรับประชาชนล่วงหน้าไม่น้อยกว่า 15 วัน ก่อนดำเนินการ เว้นแต่ ธปท. มีคำสั่งให้ธนาคารพาณิชย์ ไม่ต้องแจ้งการนำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

10.1.2 สถาบันการเงินเฉพาะกิจ บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ที่นำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนดตามข้อ 9 ทั้งกรณีที่ดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้องยื่นขออนุญาตก่อนนำมาใช้หรือก่อนการเปลี่ยนแปลงดังกล่าวต่อ ธปท. ตามที่กำหนดในคู่มือสำหรับประชาชน พร้อมเอกสารที่เกี่ยวข้อง ทั้งนี้ ธปท. อาจร้องขอให้ยื่นเอกสารที่เกี่ยวข้องอื่นเพิ่มเติมได้ โดย ธปท. จะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน เว้นแต่ ธปท. มีคำสั่งให้สถาบันการเงินเฉพาะกิจ บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ ไม่ต้องยื่นขออนุญาตการนำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

ทั้งนี้ ในการพิจารณาคำขออนุญาต ธปท. จะพิจารณาตามหลักการเสริมสร้างความมั่นคงของสถาบันการเงิน (micro-prudential) ซึ่งรวมถึงการกำกับดูแล การบริหารจัดการ การบริหารความเสี่ยง การบริหารความมั่นคงปลอดภัยของสถาบันการเงินเฉพาะกิจ บริษัทเงินทุน และบริษัทเครดิตฟองซิเอร์ ให้สามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่อาจส่งผลกระทบต่อระบบสถาบันการเงิน รวมถึงการส่งเสริมประสิทธิภาพของสถาบันการเงิน (efficiency) การสนับสนุนให้สถาบันการเงินมีธรรมาภิบาลที่ดี (good governance) และการคุ้มครองลูกค้าและผู้ใช้บริการทางการเงิน (fairness & consumer protection) รวมถึงเสถียรภาพของระบบสถาบันการเงินและระบบเศรษฐกิจ (macro-prudential)

10.2 การแจ้งการใช้บริการจากบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์สำหรับบริษัทในกลุ่มธุรกิจหรือบริษัทที่มีความเกี่ยวข้องกัน โดยให้บริษัทในกลุ่มธุรกิจ

เดียวกันหรือบริษัทที่มีความเกี่ยวข้องกันนั้นเป็นผู้ดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแทน ซึ่งบริษัทดังกล่าวอาจอยู่ในประเทศไทยหรือนอกประเทศไทยก็ได้ สถาบันการเงินต้องแจ้ง ธปท. ตามที่กำหนดในคู่มือประชาชนล่วงหน้าไม่น้อยกว่า 15 วันก่อนการใช้โครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศดังกล่าว เช่น กรณีธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศมีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์อยู่ที่บริษัทแม่ในต่างประเทศ

10.3 การรายงานปัญหาหรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องรายงานปัญหาหรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศต่อ ธปท. ตามรูปแบบและช่องทางที่กำหนดโดยเร็วเมื่อทราบถึง (1) เหตุการณ์ด้านเทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียงที่มีนัยสำคัญและเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุด หรือ (2) กรณีเทคโนโลยีสารสนเทศที่มีนัยสำคัญถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และ (3) กรณีปัญหาหรือเหตุขัดข้องของระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบ ต่อการให้บริการผ่านช่องทางให้บริการสำคัญที่ประชาชนใช้บริการจำนวนมากตามที่ ธปท. กำหนด ทั้งนี้ สามารถแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมในภายหลังได้

10.4 การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดทำและจัดส่งแบบรายงานในรูปแบบและตามระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด รวมถึงจัดทำและจัดส่งรายงานและข้อมูลอื่นเพิ่มเติมเป็นรายกรณีตามที่ธนาคารแห่งประเทศไทยร้องขอ

10.5 การรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk self-assessment)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดส่งผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ ธปท. ทราบภายใน 30 วัน นับแต่วันสิ้นปีปฏิทิน โดยมีรูปแบบและช่องทางตามที่ ธปท. กำหนด

11. การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ได้ ให้ยื่นขอผ่อนผันเป็นรายกรณีต่อ ธปท. พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธปท. จะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดย ธปท. อาจจะพิจารณาอนุญาตหรือไม่ก็ได้ หรือกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

ทั้งนี้ ในการพิจารณาคำขอผ่อนผัน ธปท. จะพิจารณาตามหลักการเสริมสร้างความมั่นคงของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ซึ่งรวมถึงการกำกับดูแลการบริหารจัดการ การบริหารความเสี่ยง การบริหารความมั่นคงปลอดภัยของสถาบันการเงินและสถาบันการเงินเฉพาะกิจให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่องเมื่อเกิดปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบ

ต่อระบบสถาบันการเงิน รวมถึงการส่งเสริมประสิทธิภาพ การสนับสนุนให้มีธรรมาภิบาลที่ดี และการคุ้มครองลูกค้าและผู้ใช้บริการ รวมถึงเสถียรภาพของระบบสถาบันการเงินและระบบเศรษฐกิจ

12. การกำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ สั่งให้แก้ไข เพิกถอน หรือเข้าตรวจสอบ การนำเทคโนโลยีสารสนเทศมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ

ธปท. อาจพิจารณากำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ สั่งให้แก้ไข เพิกถอน หรือเข้าตรวจสอบ การนำเทคโนโลยีสารสนเทศมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ ทั้งกรณีสถาบันการเงินและสถาบันการเงินเฉพาะกิจดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ตามความจำเป็นเป็นรายกรณี หากพบว่าเป็นการดำเนินการที่ส่งผลกระทบต่อประชาชนในวงกว้างหรือความเชื่อมั่นต่อระบบสถาบันการเงิน

13. บทเฉพาะกาล

สถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีการให้บริการผ่านช่องทาง mobile banking application ก่อนวันที่ประกาศฉบับนี้มีผลใช้บังคับ ให้ดำเนินการจัดให้มีการดูแลระบบงานที่รองรับ mobile banking application ให้เป็นไปตามข้อ 8. วรรคหนึ่ง ภายในวันที่ 1 มกราคม 2567

14. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 16 ตุลาคม 2566

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6346

เอกสารแนบ 1

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT governance)

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจ

คณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจต้องเข้าใจและตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อลูกค้าและผู้ใช้บริการ รวมทั้งมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมการดำเนินการและการดูแล ดังต่อไปนี้

1.1 ดูแลให้การใช้เทคโนโลยีสารสนเทศสอดรับกับกลยุทธ์ในการให้บริการหรือการดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงในอนาคต รวมทั้งดูแลให้ระบบเทคโนโลยีสารสนเทศที่รองรับบริการสำคัญสามารถให้บริการได้อย่างต่อเนื่อง

1.2 ดูแลให้มีนโยบายและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามด้านไซเบอร์ ซึ่งเป็นหนึ่งในความเสี่ยงสำคัญขององค์กร (enterprise wide risk) ทั้งด้านความปลอดภัย ความถูกต้อง และความพร้อมใช้ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ทั้งในภาวะปกติและภาวะวิกฤต ดูแลความเสี่ยงโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ รวมทั้งดูแลให้มีการบริหารจัดการความเสี่ยงจากภัยทุจริตทางการเงินให้รัดกุมเพียงพอ

1.3 ดูแลให้เกิดการสร้างความรู้และความตระหนักรู้เรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่กรรมการ ผู้บริหาร และพนักงานในองค์กร รวมทั้งลูกค้าและผู้ใช้บริการอย่างต่อเนื่องและมีประสิทธิผล

ทั้งนี้ คณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจอาจมอบหมายให้คณะกรรมการชุดอื่นหรือผู้บริหารระดับสูงกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ โดยคณะกรรมการยังคงต้องรับผิดชอบในเรื่องดังกล่าว

นอกจากนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องปฏิบัติเพิ่มเติมในส่วนที่เกี่ยวข้องกับบทบาทหน้าที่ของคณะกรรมการตามที่ ธปท. กำหนดในประกาศธนาคารแห่งประเทศไทยว่าด้วยธรรมาภิบาลของสถาบันการเงิน และประกาศธนาคารแห่งประเทศไทยว่าด้วยธรรมาภิบาลของสถาบันการเงินเฉพาะกิจ เช่น คณะกรรมการต้องมีกรรมการอย่างน้อย 1 คนที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ เป็นต้น

2. โครงสร้างการกำกับดูแล

2.1 โครงสร้างองค์กรในการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีโครงสร้างองค์กรที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence) โดยแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่าง

การทำหน้าที่ (1) ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (2) บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และ (3) ตรวจสอบด้านเทคโนโลยีสารสนเทศ

นอกจากนี้ ต้องมีการถ่วงดุลอำนาจกันอย่างอิสระ โดยเฉพาะการทำหน้าที่ตรวจสอบต้องมีความเป็นอิสระจากการทำหน้าที่ปฏิบัติงานและการทำหน้าที่บริหารความเสี่ยงและกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

2.2 คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมีคณะกรรมการ ดังต่อไปนี้

2.2.1 คณะกรรมการที่ทำหน้าที่บริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee เป็นต้น

2.2.2 คณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้ เช่น IT risk committee เป็นต้น

2.2.3 คณะกรรมการที่ทำหน้าที่กำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการตรวจสอบการปฏิบัติงาน การบริหารความเสี่ยงและการกำกับการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น คณะกรรมการตรวจสอบ เป็นต้น

2.3 การกำหนดผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.3.1 ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (head of IT security) โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์ รวมทั้งมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งกำหนดบทบาทหน้าที่และความรับผิดชอบ อย่างน้อยดังนี้

- กำหนดให้มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

- กำหนดให้มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)

- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงขององค์กร และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจ หรือคณะกรรมการที่ได้รับมอบหมายเป็นวาระประจำ

- ดูแลและดำเนินการให้มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้ และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์

2.3.2 ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer : CISO)

ธนาคารพาณิชย์ที่มีนัยสำคัญต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks : D-SIBs) หรือสถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ตามกรอบการประเมินความพร้อมการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework : CRAF) นอกจากต้องจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามข้อ 2.3.1 แล้ว ต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) ด้วย

ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวต้องเป็นอิสระจากงานด้านปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (authority) ที่เหมาะสมในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยอย่างน้อยต้องมีอำนาจหน้าที่ ดังนี้

- รายงานปัญหาหรือเหตุการณ์ผิดปกติที่มีนัยสำคัญด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด หรือคณะกรรมการที่เกี่ยวข้อง หรือคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจโดยตรง

- ให้ความคิดเห็นในเรื่องการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจ หรือคณะกรรมการที่เกี่ยวข้องกับกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee รวมทั้ง ร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ

3. นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

3.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มี (1) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และ (2) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ที่เป็นลายลักษณ์อักษร และอยู่ภายใต้กรอบหลักการ การรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) หรือ CIA โดยนโยบายดังกล่าวต้องได้รับการอนุมัติจากคณะกรรมการของสถาบันการเงินหรือคณะกรรมการของสถาบันการเงินเฉพาะกิจ และต้องสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีสารสนเทศมาใช้สำหรับให้บริการหรือดำเนินธุรกิจ รวมทั้งสอดคล้องกับแนวทางการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

นอกจากนี้ การกำหนดนโยบายดังกล่าวต้องคำนึงถึงลักษณะการให้บริการหรือดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศภายในองค์กรและความเสี่ยงจากการใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอกด้วย

3.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4. การบริหารจัดการบุคลากร

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวันอย่างเหมาะสม โดยต้องคำนึงถึงความรู้ความสามารถของบุคลากร ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

4.1 การบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงาน บริหารความเสี่ยงและกำกับการปฏิบัติตามกฎเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ ต้องครอบคลุมในเรื่องกระบวนการคัดเลือกบุคลากรที่มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ ความเพียงพอของบุคลากรที่สอดคล้องกับปริมาณการใช้เทคโนโลยีสารสนเทศ และมาตรการในการสร้างและส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ

4.2 ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของบุคลากรหรือระเบียบข้อบังคับภายในองค์กรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้น

4.3 การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศต้องปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว

5. การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องสื่อสารและให้ความรู้แก่บุคลากรที่ทำหน้าที่ปฏิบัติงาน บริหารความเสี่ยงและการปฏิบัติตามกฎเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายสาธารณะที่ถูกต้อง การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น

นอกจากนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรเสริมสร้างความตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามไซเบอร์ให้กับลูกค้าและผู้ใช้บริการอย่างสม่ำเสมอและต่อเนื่องให้เท่าทันกับความเสี่ยงและภัยคุกคามใหม่ ๆ

เอกสารแนบ 2

การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
(IT security management)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำหนดให้มีการบริหารจัดการและควบคุมดูแลระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีการรักษาความลับของระบบและข้อมูล ถูกต้องเชื่อถือได้และพร้อมใช้งาน ดังต่อไปนี้

1. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

บริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม นอกจากนี้ ต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมถึงบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้หมดอายุการใช้งานหรือสิ้นสุดการให้บริการอย่างเหมาะสมและเท่าทันกับความเสี่ยง เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย พร้อมใช้งานและสามารถรองรับการให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

2. การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

รักษาความมั่นคงปลอดภัยของข้อมูล ทั้งการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ มีการจัดชั้นความลับของข้อมูล (information classification) เก็บรักษาและทำลายข้อมูลให้เหมาะสมตามระดับชั้นความลับ รวมทั้งบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากลที่ยอมรับโดยทั่วไป เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

3. การควบคุมการเข้าถึง (access control)

ต้องควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิ โดยต้องครอบคลุมอย่างน้อย ดังนี้

3.1 บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ต้องมีการกำหนดมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานที่มีสิทธิสูงอย่างเข้มงวด เช่น การมอบหมายสิทธิ การเบิกใช้ กำหนดระยะเวลาการใช้งาน การสอบทานหลังการใช้ เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

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)

รักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่อง

5. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

รักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น รวมทั้งพร้อมรองรับการให้บริการได้อย่างต่อเนื่อง

6. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

รักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

6.1 บริหารจัดการขีดความสามารถของระบบเทคโนโลยีสารสนเทศและระบบสาธารณูปโภค (capacity management) เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับการให้บริการหรือดำเนินธุรกิจและสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต สำหรับระบบที่มีการให้บริการผ่านช่องทางดิจิทัลควรมีการติดตามและประเมินขีดความสามารถของระบบอย่างใกล้ชิดรองรับบริการและปริมาณธุรกรรมที่เพิ่มขึ้นอย่างรวดเร็ว

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

6.3 สำรองข้อมูล (data backup) ด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

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

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

6.6 บริหารจัดการช่องโหว่ (vulnerability management) โดยจัดให้มีการประเมินช่องโหว่สำหรับทุกระบบงานตามระดับความเสี่ยง สำหรับระบบงานสำคัญต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

6.7 ทดสอบเจาะระบบ (penetration test) โดยจัดให้มีการทดสอบเจาะระบบโดยผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระ อย่างน้อยครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบ ความเสี่ยง หรือมาตรฐานสากลด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ เป็นต้น เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ นอกจากนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถนำแนวปฏิบัติเรื่อง การทดสอบเจาะระบบ แบบ Intelligence-led (iPentest)[1] มาประยุกต์ใช้ เพื่อให้การทดสอบเจาะระบบมีความสมจริงมากยิ่งขึ้น

ทั้งนี้ ในกรณีที่ ธปท. เห็นว่าผลการทดสอบเจาะระบบ มีข้อมูลรายงานไม่ครบถ้วน ขอบเขตหรือวิธีการทดสอบการเจาะระบบไม่ครอบคลุมช่องโหว่สำคัญที่เป็นความเสี่ยงที่ได้รับการยอมรับโดยทั่วไป หรือในกรณีที่ ธปท. เห็นว่าจำเป็นหรือสมควร ธปท. อาจสั่งให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจแต่งตั้งผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระดำเนินการทดสอบเจาะระบบเพิ่มเติมได้

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) ครอบคลุมระบบปฏิบัติการระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้งดำเนินการตั้งค่าและสอบทานการตั้งค่าอย่างสม่ำเสมอตามที่ได้กำหนดไว้ เพื่อให้มั่นใจว่าระบบงานที่รองรับการให้บริการมีการรักษาความมั่นคงปลอดภัยขั้นต่ำตามมาตรฐานที่กำหนดไว้

[1] หนังสือเวียน ธปท.ฝตท.(1) ว. 1252/2562 แนวปฏิบัติเรื่อง การทดสอบเจาะระบบ แบบ Intelligence-led (iPentest) และที่แก้ไขเพิ่มเติม

ในกรณีที่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจไม่สามารถปฏิบัติตามมาตรฐานที่ตนได้กำหนดไว้ข้างต้น 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)

กำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและบุคคลภายนอกที่ให้บริการ 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) ทดสอบความต้องการของ

ผู้ใช้งาน (user acceptance test) และทดสอบความปลอดภัยของระบบ (security test) ตามกระบวนการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) ทดสอบความพร้อมใช้งานของระบบสำรอง

- ทดสอบประสิทธิภาพ (performance test) และความสามารถในการให้บริการเมื่อมีการใช้บริการจำนวนมาก เมื่อมีการพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์

- มีแนวทางควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

- จัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

8. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)

บริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติ ปัญหา และการแก้ไขให้คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมายกรณีเป็นสาขาธนาคารพาณิชย์ต่างประเทศ ในระยะเวลาที่เหมาะสม นอกจากนี้ ต้องวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหาเพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

9. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT disaster recovery plan)

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

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 โดยการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรสอดคล้องกับระยะเวลาในการกู้คืนระบบ (recover time objective : RTO) ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point object : RPO) และระยะเวลาสูงสุดที่ยอมให้การให้บริการหรือธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD) เพื่อรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

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)

ในกรณีที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจดำเนินการดังต่อไปนี้ (1) ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) (2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือ (3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลลูกค้าในรูปแบบอิเล็กทรอนิกส์ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำกับดูแลความเสี่ยงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ให้สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญบนพื้นฐานที่ต้องรับผิดชอบต่อการให้บริการหรือดำเนินธุรกิจแก่ลูกค้า และคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิภาพในการให้บริการ ตามหลักการดังนี้

10.1 กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างสถาบันการเงินและสถาบันการเงินเฉพาะกิจกับบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร และพร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดย ธปท. สำหรับบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ที่มีนัยสำคัญ ต้องระบุให้ ธปท. ผู้ตรวจสอบภายใน และผู้ตรวจสอบภายนอก มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกรายดังกล่าว เป็นเงื่อนไขในสัญญาหรือข้อตกลงระหว่างสถาบันการเงินหรือสถาบันการเงินเฉพาะกิจกับบุคคลภายนอกดังกล่าวด้วย

สำหรับกรณีที่ไม่สามารถระบุสิทธิให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอกมีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ในเงื่อนไขสัญญาหรือข้อตกลงกับบุคคลภายนอก สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมั่นใจว่าบุคคลภายนอกรายดังกล่าวมีผลการตรวจสอบจากผู้ตรวจสอบภายนอกที่เป็นอิสระทดแทน

10.2 กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญและความเสี่ยงจากการกระจุกตัว (concentration risk) เนื่องจากใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการที่เป็นบุคคลภายนอกรายใดรายหนึ่ง (third party/vendor locked-in)

10.3 รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป

10.4 เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการให้บริการหรือดำเนินธุรกิจแก่ลูกค้า

10.5 สำหรับสถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีการนำระบบงานที่มีนัยสำคัญไปใช้บริการ public cloud computing จากบุคคลภายนอก เช่น ระบบ core banking เป็นต้น สถาบันการเงินและสถาบันการเฉพาะกิจต้องปฏิบัติเพิ่มเติมอย่างน้อย ดังนี้

10.5.1 ประเมินระดับความเสี่ยงที่จะเกิดขึ้นจากการใช้บริการ public cloud computing จากบุคคลภายนอกด้านงานเทคโนโลยีสารสนเทศที่มีนัยสำคัญ โดยอย่างน้อยต้องครอบคลุมความเสี่ยงสำคัญ ดังนี้

- ความเสี่ยงด้านกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง
- ความเสี่ยงด้านการรักษาความปลอดภัยของบุคคลภายนอก
- ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง
- ความเสี่ยงข้อมูลที่ไม่ถูกทำลายอย่างสมบูรณ์จากระบบของบุคคลภายนอกเมื่อมีการเปลี่ยนแปลงบุคคลภายนอกหรือนำกลับมาทำเองไม่สมบูรณ์หรือไม่ครบถ้วน
- ความเสี่ยงจากการใช้บริการจากผู้ให้บริการในต่างประเทศ
- ความเสี่ยงจากการที่ผู้ให้บริการ public cloud computing หยุดชะงัก
- ความเสี่ยงจากการกระจุกตัว

10.5.2 กำหนดปัจจัยในการคัดเลือกบุคคลภายนอกก่อนใช้บริการ โดยอย่างน้อยต้องครอบคลุมปัจจัย ดังนี้

- ปัจจัยด้านความเสี่ยงของประเทศที่บุคคลภายนอกที่จัดเก็บหรือประมวลผลข้อมูลบนระบบ public cloud computing
- ปัจจัยด้านการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง
- ปัจจัยด้านความยืดหยุ่นในการเปลี่ยนแปลงระบบงานไปยังบุคคลภายนอกรายอื่นหรือการเชื่อมโยงกับระบบอื่นได้

10.5.3 ระบุสถานที่ที่บุคคลภายนอกประมวลผล จัดเก็บข้อมูล หรือดำเนินการอื่นใดที่เกี่ยวข้องกับข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

10.5.4 กรณีใช้บริการ public cloud computing จากบุคคลภายนอกในต่างประเทศ สถาบันการเงินและสถาบันการเงินเฉพาะกิจ ต้องจัดให้มีกระบวนการสำรองข้อมูล พร้อมทั้งข้อมูลสำรองไว้ในประเทศหรือในประเทศอื่นที่มิใช่ประเทศที่ใช้บริการเป็นหลัก รวมทั้งสอบทานข้อมูลดังกล่าว อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อมูลมีความพร้อมใช้และสามารถนำมาใช้งานได้จริง

10.5.5 จัดให้มีการเข้ารหัสข้อมูลสำคัญด้วยมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป ทั้งข้อมูลที่อยู่ในลักษณะ ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data-in-transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data-at-rest) เมื่อจัดเก็บและประมวลผลบนระบบ public cloud computing ของบุคคลภายนอก

10.5.6 จัดให้มีกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่สอดคล้องกับแนวปฏิบัติการบริหารจัดการความเสี่ยงที่ดีของบุคคลภายนอก หรือมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป รวมทั้งสอบทานการตั้งค่าดังกล่าวอย่างสม่ำเสมอ

10.5.7 มีกระบวนการติดตามเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ที่เกิดกับระบบที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการ public cloud computing อย่างสม่ำเสมอ และมีการกำหนดแนวทางป้องกันภัยคุกคามดังกล่าว เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นก่อนที่บุคคลภายนอกจะสามารถแก้ไขปัญหาหรือดำเนินการปิดช่องโหว่

10.5.8 เมื่อสิ้นสุดหรือยกเลิกการใช้บริการ public cloud computing ในระบบงานที่มีนัยสำคัญจากบุคคลภายนอก สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องนำข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือข้อมูลของลูกค้ากลับมาจากบุคคลภายนอก และดูแลให้มีการทำลายข้อมูลที่เก็บอยู่ที่บุคคลภายนอกโดยบุคคลภายนอกต้องไม่สามารถกู้คืนข้อมูลดังกล่าวได้ หรือดำเนินการใด ๆ เพื่อให้บุคคลอื่นไม่สามารถเข้าถึงข้อมูลดังกล่าวได้

10.5.9 แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ครอบคลุมการใช้บริการ public cloud computing ในระบบงานที่มีนัยสำคัญจากบุคคลภายนอก โดยคำนึงถึงเหตุการณ์ที่อาจส่งผลกระทบรุนแรงหรือเลวร้ายที่สุด (worst case scenario) โดยอย่างน้อยต้องครอบคลุมเหตุการณ์ ดังนี้

(1) ระบบงานของบุคคลภายนอกใน region ที่ใช้บริการอยู่หยุดชะงักจนเป็นเหตุให้บริการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจไม่สามารถให้บริการได้อย่างต่อเนื่อง เช่น hardware และ software ของบุคคลภายนอกที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการจากบุคคลภายนอกได้รับความเสียหายทั้งหมด เป็นต้น

(2) ระบบงานของบุคคลภายนอกทุก region ที่ใช้บริการอยู่หยุดชะงักจนเป็นเหตุให้บริการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจไม่สามารถให้บริการได้อย่างต่อเนื่อง

(3) สายสื่อสารของสถาบันการเงินและสถาบันการเงินเฉพาะกิจขัดข้องทุกช่องทางจนไม่สามารถใช้บริการได้

ทั้งนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถพิจารณาประยุกต์ใช้แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management implementation guideline) เพื่อเป็นแนวทางการบริหารจัดการความเสี่ยงและการควบคุมให้เหมาะสมและสอดคล้องตามขอบเขตระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

เอกสารแนบ 3

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT risk management)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยอย่างน้อยต้องครอบคลุมการดำเนินการ ดังนี้

1. โครงสร้างองค์กร

1.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management function) โดยสามารถจัดตั้งเป็นหน่วยงานที่รับผิดชอบงานการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือเป็นส่วนหนึ่งกับหน่วยงานบริหารความเสี่ยงหรือรูปแบบอื่น ๆ ก็ได้ ทั้งนี้ ต้องมั่นใจว่ายังคงมีความเป็นอิสระเพียงพอที่สามารถปฏิบัติงานได้อย่างครบถ้วนและมีประสิทธิภาพ

1.2 กำหนดสายการรายงานที่ชัดเจนและเป็นอิสระจากหน่วยงานที่ทำหน้าที่เป็น first line of defence โดยรวบรวมและเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกับความเสี่ยงด้านอื่นของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ พร้อมทั้งนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.3 ผู้รับผิดชอบงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องมีความรู้ประสบการณ์ และความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงได้รับการฝึกอบรมด้านการบริหารจัดการความเสี่ยงและเพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง เพื่อให้สามารถบริหารจัดการความเสี่ยงและติดตามความเสี่ยงได้อย่างมีประสิทธิภาพ

2. การปฏิบัติงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กำหนดให้มีระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมายกรณีเป็นสาขาธนาคารพาณิชย์ต่างประเทศรวมทั้งมีการจัดทำกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยประสานงานร่วมกับหน่วยงานที่ทำหน้าที่เป็น first line of defence ในการระบุและประเมินความเสี่ยง การกำหนดมาตรการในลดความเสี่ยงและระบบการควบคุมภายใน โดยมีกระบวนการอย่างน้อยครอบคลุม ดังนี้

2.1 การประเมินความเสี่ยง

2.1.1 การระบุความเสี่ยง ให้ระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร การใช้บริการจากบุคคลภายนอก หรือปัจจัยภายนอก

2.1.2 การวิเคราะห์ความเสี่ยง ควรเข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

2.1.3 การประเมินค่าความเสี่ยง ให้ประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงาน

2.2 การจัดการความเสี่ยง ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

ทั้งนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) ที่เกี่ยวข้องกับการให้บริการหรือดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

2.3 การติดตามและทบทวนความเสี่ยง ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

2.4 การรายงานความเสี่ยง ให้รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อคณะกรรมการของสถาบันการเงินหรือคณะกรรมการของสถาบันการเงินเฉพาะกิจหรือคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมายกรณีเป็นสาขาธนาคารพาณิชย์ต่างประเทศเป็นประจำอย่างสม่ำเสมอ

เอกสารแนบ 4

การกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT compliance)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำหนดกรอบการกำกับการปฏิบัติตามกฎเกณฑ์ให้ครอบคลุมถึงกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และต้องนำมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการกำกับการปฏิบัติตามกฎเกณฑ์ โดยอย่างน้อยต้องครอบคลุม ดังนี้

1. โครงสร้างองค์กร

1.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการดำเนินการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance function) โดยสามารถจัดตั้งเป็นหน่วยงานที่รับผิดชอบงานด้านการกำกับดูแลการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือเป็นส่วนหนึ่งกับหน่วยงานด้านการปฏิบัติตามกฎเกณฑ์ หรือรูปแบบอื่น ๆ ก็ได้ ทั้งนี้ ต้องมั่นใจว่ายังคงมีความเป็นอิสระเพียงพอที่สามารถปฏิบัติงานได้อย่างครบถ้วนและมีประสิทธิภาพ

1.2 กำหนดสายการรายงานที่ชัดเจนและเป็นอิสระจากหน่วยงานที่ทำหน้าที่เป็น first line of defence โดยรายงานถึงหัวหน้าหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ที่มีสายการรายงานตรงถึงคณะกรรมการที่เกี่ยวข้อง เช่น คณะกรรมการที่ทำหน้าที่กำกับดูแลบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎเกณฑ์ เป็นต้น

1.3 ผู้รับผิดชอบงานด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ต้องมีความรู้ ประสบการณ์ และความเข้าใจในกฎหมายและความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศ รวมถึงต้องได้รับการฝึกอบรมด้านกฎเกณฑ์ต่าง ๆ และเพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง

2. การปฏิบัติงานด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

กำหนดกระบวนการในการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยอย่างน้อยครอบคลุม ดังนี้

2.1 การระบุและประเมินความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ ต้องครอบคลุมถึงกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยระบบการชำระเงิน เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและกฎเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

2.2 การกำหนดแผนการบริหารความเสี่ยงด้านการปฏิบัติงานตามกฎเกณฑ์ (compliance program) ประจำปี ต้องครอบคลุมถึงกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ซึ่งต้องสอดคล้องกับระดับความเสี่ยงที่ประเมินจากข้อ 2.1 โดยพิจารณาดำเนินการสอบทานระเบียบข้อบังคับที่ให้พนักงานถือปฏิบัติ สุ่มสอบทานการปฏิบัติตามกฎเกณฑ์ต่าง ๆ (compliance testing) และให้ความรู้แก่พนักงานในเรื่องกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

2.3 การติดตามและรายงานผลการสอบทานด้านการปฏิบัติตามกฎเกณฑ์ สรุปผลเหตุการณ์ไม่ปฏิบัติตามกฎเกณฑ์และมาตรการแก้ไข รวมถึงผลการดำเนินการตามข้อเสนอแนะคำสั่งการของ ธปท. และผู้กำกับดูแลอื่นที่เกี่ยวข้อง ต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย กรณีเป็นสาขาธนาคารพาณิชย์ต่างประเทศ เป็นประจำอย่างสม่ำเสมอ

เอกสารแนบ 5

การตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT audit)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำหนดกรอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมการปฏิบัติงาน กระบวนการทำงานและระบบงานด้านเทคโนโลยีสารสนเทศ และต้องนำมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการตรวจสอบ โดยอย่างน้อยต้องครอบคลุม ดังนี้

1. โครงสร้างองค์กร

1.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการดำเนินการในงานตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit function) โดยสามารถจัดตั้งเป็นหน่วยงานที่รับผิดชอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ หรืออยู่ภายใต้สายงานตรวจสอบภายใน ทั้งนี้ ต้องมั่นใจว่ามีความเป็นอิสระและสามารถปฏิบัติงานได้อย่างครบถ้วนและมีประสิทธิภาพ

1.2 กำหนดสายการรายงานที่เป็นอิสระ โดยต้องรายงานถึงหัวหน้าหน่วยงานตรวจสอบภายในและรายงานตรงต่อคณะกรรมการตรวจสอบ

1.3 ผู้รับผิดชอบงานด้านการตรวจสอบเทคโนโลยีสารสนเทศต้องมีความรู้ ประสบการณ์และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอก ที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

1.4 ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องได้รับการฝึกอบรม เพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง เพื่อให้ผู้ตรวจสอบสามารถนำมาปรับใช้กับวิธีการตรวจสอบได้ทันกับแนวโน้มและการพัฒนาทางด้านเทคโนโลยีสารสนเทศ

ทั้งนี้ ในกรณีที่ ธปท. เห็นว่าผลการตรวจสอบของสถาบันการเงินและสถาบันการเงินเฉพาะกิจมีข้อมูลไม่ครบถ้วนหรือมีข้อความคลุมเครือไม่ชัดเจน หรือในกรณีที่ ธปท. เห็นว่าจำเป็นหรือสมควร ธปท. อาจสั่งให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจแต่งตั้งผู้ตรวจสอบภายนอกดำเนินการตรวจสอบและรายงานผลการตรวจสอบให้ ธปท. ทราบ

2. การปฏิบัติงานด้านการตรวจสอบเทคโนโลยีสารสนเทศ

กำหนดขอบเขตการตรวจสอบต้องครอบคลุมการปฏิบัติงาน กระบวนการทำงานและระบบงานด้านเทคโนโลยีสารสนเทศทั้งหมด รวมทั้งการใช้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก เพื่อให้สามารถระบุและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน โดยมีกระบวนการอย่างน้อยครอบคลุม ดังนี้

2.1 การกำหนดแผนงานตรวจสอบ ต้องสอดคล้องกับความสำคัญและความเสี่ยงของการใช้งานเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ สำหรับงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญต้องตรวจสอบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งเมื่อมีเหตุการณ์ผิดปกติในเทคโนโลยีสารสนเทศที่มีนัยสำคัญ โดยแผนงานและขอบเขตการตรวจสอบต้องได้รับการอนุมัติจากคณะกรรมการ

ตรวจสอบ รวมถึงต้องทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าว โดยคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.2 การตรวจสอบ ต้องตรวจสอบตามแผนงานและขอบเขตที่กำหนดอย่างน้อยปีละ 1 ครั้ง โดยการตรวจสอบควรเป็นไปตามมาตรฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด ซึ่งสอดคล้องกับกฎหมาย กฎเกณฑ์ที่เกี่ยวข้อง และมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป

2.3 การติดตามและรายงานผลการตรวจสอบ ต้องสรุปผลการตรวจสอบและประเด็นที่ต้องแก้ไขกับผู้บริหารของหน่วยงานผู้รับตรวจและจัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการตรวจสอบและแจ้งให้ผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบ รวมถึงติดตามให้มีการปรับปรุงประเด็นการตรวจสอบและรายงานประเด็นสำคัญพร้อมแผนปรับปรุงให้กับคณะกรรมการตรวจสอบเป็นประจำอย่างสม่ำเสมอ ทั้งนี้ ให้จัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจ เพื่อให้พร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดย ธปท.

เอกสารแนบ 6

การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT project management)

เมื่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจจัดทำโครงการด้านเทคโนโลยีสารสนเทศ (IT project management) ที่มีนัยสำคัญ ที่นำมาใช้ในการให้บริการหรือดำเนินธุรกิจ ต้องปฏิบัติตามหลักเกณฑ์ดังต่อไปนี้

1. ศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับสำหรับโครงการที่นำเทคโนโลยีสารสนเทศมาใช้ในการให้บริการหรือดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องพิจารณาเลือกใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม และประเมินความเสี่ยงตลอดจนผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งต้องจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมายกรณีเป็นสาขาธนาคารพาณิชย์ต่างประเทศ ตามขอบเขตอำนาจอนุมัติที่กำหนดไว้

2. กำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางบริหารจัดการโครงการ (project management) โดยครอบคลุมขั้นตอนตั้งแต่การเริ่มโครงการ การดำเนินการและการควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ

3. กำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (project governance) โดยอย่างน้อยต้องกำหนดโครงสร้าง ดังต่อไปนี้

3.1 คณะกรรมการที่ทำหน้าที่กำกับดูแลโครงการ เพื่อทำหน้าที่กำกับดูแลความคืบหน้า ให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้การดำเนินงานของโครงการเป็นไปตามแผนงานที่กำหนด ทั้งนี้ คณะกรรมการกำกับดูแลโครงการควรประกอบด้วยผู้บริหารหรือผู้แทนจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้อง

3.2. หน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการ (project management office : PMO) เพื่อทำหน้าที่กำหนดรูปแบบ กระบวนการ และเครื่องมือที่เป็นมาตรฐานในการบริหารจัดการและติดตามความคืบหน้าของโครงการ รวมทั้งรายงานความคืบหน้าและภาพรวมของโครงการที่สำคัญต่อคณะกรรมการที่กำกับดูแลโครงการ เพื่อให้โครงการบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้

3.3 ผู้จัดการโครงการ (project manager) เพื่อทำหน้าที่ในการบริหารจัดการโครงการแต่ละโครงการตามขั้นตอนการบริหารจัดการโครงการ และส่งมอบงานในแต่ละขั้นตอนตามรูปแบบกระบวนการและเครื่องมือ ตามที่หน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการกำหนด เพื่อให้สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานที่กำหนด

คำถาม – คำตอบแนบท้ายประกาศ
เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk) ของสถาบันการเงิน
ปรับปรุงวันที่ 24 กันยายน 2568

ข้อ	คำถาม	คำตอบ
ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)		
1.	ในกรณีที่สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ (subsidiary) (1) สามารถใช้โครงสร้างการกำกับดูแลความเสี่ยงด้าน IT ทั้ง 3 line of defence รวมทั้งคณะกรรมการชุดต่าง ๆ ของธนาคารพาณิชย์แม่ที่อยู่ที่ต่างประเทศ โดยมีหน่วยงานปฏิบัติงานด้าน IT อยู่ที่ประเทศไทยได้หรือไม่ (2) สามารถใช้นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ที่กำหนดโดยธนาคารพาณิชย์แม่ที่อยู่ที่ต่างประเทศได้หรือไม่	(1) สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ สามารถใช้โครงสร้างการกำกับดูแลของหน่วยงานที่อยู่ต่างประเทศได้ หากโครงสร้าง ดังกล่าวมีการแบ่งแยกหน้าที่ตามหลัก 3 line of defense และมีคณะกรรมการที่ทำหน้าที่กำกับ ดูแล ความเสี่ยงด้าน IT ที่ทำหน้าที่ครอบคลุมมาถึงสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกที่อยู่ในประเทศไทย (2) สามารถนำนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ที่สำนักงานใหญ่หรือธนาคารพาณิชย์แม่ที่อยู่ในต่างประเทศกำหนดมาปรับใช้ได้โดยต้องมั่นใจว่านโยบายดังกล่าวครอบคลุมตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ ทั้งนี้ คณะกรรมการของสาขาของธนาคารพาณิชย์ต่างประเทศนั้นหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศต้องอนุมัตินโยบายดังกล่าวด้วย
การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)		
2.	ในกรณีที่สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ (subsidiary) ซึ่งมีการใช้ระบบ core banking และระบบที่เกี่ยวข้องจากธนาคารพาณิชย์แม่ที่อยู่ที่ต่างประเทศนั้น สามารถใช้ผลการทดสอบเจาะระบบของธนาคารพาณิชย์แม่ที่อยู่ที่ต่างประเทศได้หรือไม่	สามารถใช้ผลการทดสอบของธนาคารพาณิชย์แม่ที่อยู่ที่ต่างประเทศได้โดยผลการทดสอบต้องครอบคลุม ระบบงานสำคัญที่สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศใช้งานอยู่ทั้งหมด

ข้อ	คำถาม	คำตอบ
3.	ระบบงานที่คาดหวังให้มีการทดสอบเจาะระบบ (penetration test) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง คือระบบงานใดบ้าง	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการทดสอบกับระบบงานที่มีการเชื่อมต่อกับระบบเครือข่ายสาธารณะ เช่น หน้าเว็บไซต์ของธนาคาร ระบบ Mobile Banking ระบบ Internet Banking เป็นต้น
การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)		
4.	ขอทราบหลักการในการพิจารณาบุคคลภายนอก (third party)	การพิจารณาบุคคลภายนอกมีหลักในการพิจารณาว่าบุคคลนั้นต้องไม่ใช่ธนาคารเอง (first party) และต้องไม่ใช่ลูกค้าของธนาคาร (second party) ซึ่งหากไม่ใช่ธนาคารเองหรือลูกค้าของธนาคารแล้ว ให้ถือว่าเป็นบุคคลภายนอกทั้งหมด อย่างไรก็ตาม หลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ กำหนดให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องบริหารจัดการความเสี่ยงด้าน IT จาก บุคคลภายนอกตาครอบคลุมเพียง 3 ลักษณะ ดังนี้ (1) บุคคลภายนอกที่ให้บริการงานด้าน IT (IT outsourcing) (2) บุคคลภายนอกที่มีการเชื่อมต่อระบบ IT กับระบบ IT ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (3) บุคคลภายนอกที่สามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลูกค้าในรูปแบบอิเล็กทรอนิกส์
5.	การให้บริการ bill payment กับบริษัท ก. ถือว่าบริษัท ก เป็นบุคคลภายนอกหรือไม่	การพิจารณาบริษัทใดเป็นบุคคลภายนอกต้องพิจารณาแยกเป็นรายบริการ ไม่ใช่การพิจารณาเป็นรายบริษัท สำหรับกรณีการให้บริการ bill payment กับบริษัท ก เป็นการร่วมมือระหว่างกันเพื่อเสนอบริการให้แก่ลูกค้า ซึ่งบริการนั้นจะเกิดขึ้นไม่ได้ถ้าขาดฝั่งใดฝั่งหนึ่ง การให้บริการลักษณะนี้ถือว่าเป็นบุคคลภายนอกตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ ซึ่งอาจเข้าข่ายว่า มีการเชื่อมต่อระบบ IT กับบุคคลภายนอก หรือให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลูกค้าในรูปแบบอิเล็กทรอนิกส์

ข้อ	คำถาม	คำตอบ
6.	ขอทราบหลักการในการพิจารณาการใช้บุคคลภายนอกลักษณะใดที่ถือว่าเป็น IT outsourcing	การพิจารณาว่าการใช้บริการงาน IT ใดเข้าข่ายเป็น IT outsourcing ให้พิจารณาว่างาน IT ที่ใช้บริการจากบุคคลภายนอกนั้น เป็นงาน IT ที่โดยปกติแล้วสถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องดำเนินการเอง โดยพิจารณาขอบเขตงานด้าน IT ตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ ตามเอกสารแนบ 2
7.	ระบบงานที่มีนัยสำคัญ ในกรณีที่เป็น hybrid cloud computing ที่มีทั้งส่วนที่ธนาคารดูแลเองและใช้ public cloud computing จากบุคคลภายนอก จะต้องปฏิบัติตามการบริหารจัดการความเสี่ยงจากบุคคลภายนอก หรือไม่	ระบบงานที่มีนัยสำคัญในส่วนที่ไปใช้บริการ public cloud computing จากบุคคลภายนอก ต้องปฏิบัติตามการบริหารความเสี่ยงจากบุคคลภายนอกตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ ตามเอกสารแนบ 2 ข้อ 10
8.	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องระบุสิทธิ์ให้ ธปท. ผู้ตรวจสอบภายใน และผู้ตรวจสอบภายนอก มีสิทธิ์เข้าตรวจสอบบุคคลภายนอกทุกประเภทหรือไม่	หลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ กำหนดให้เฉพาะบุคคลภายนอกที่ให้บริการงานด้าน IT (IT outsourcing) ที่มีนัยสำคัญต้องระบุให้ ธปท. ผู้ตรวจสอบภายใน และผู้ตรวจสอบภายนอกมีสิทธิ์ในการเข้าตรวจสอบ
9.	กรณีใช้ public cloud computing ต่างประเทศ ต้องสำรองข้อมูลในประเทศไทยหรือไม่	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีกระบวนการสำรองข้อมูล พร้อมทั้งสำรองข้อมูลไว้ในประเทศหรือในประเทศอื่นที่มิใช่ประเทศที่ใช้บริการเป็นหลัก
10.	กรณีใช้ public cloud computing กับระบบงานที่มีนัยสำคัญ มีแนวทางในการรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้าน IT อย่างไรบ้าง	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดทำและทดสอบแผนฉุกเฉินด้าน IT โดยคำนึงถึงเหตุการณ์ที่อาจส่งผลกระทบรุนแรงหรือเลวร้ายที่สุดตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ข้อ 10.5.9 เช่น อาจพิจารณาการใช้งาน multi cloud computing หรือ hybrid cloud computing หรือแนวทางอื่น ๆ ทดแทน เพื่อให้ธุรกิจยังสามารถดำเนินการได้อย่างต่อเนื่อง
การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)		
11.	ในกรณีสถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนดแผนงานตรวจสอบตามความสำคัญและความเสี่ยงของการใช้งาน IT ทำให้ มีงานด้าน IT บางเรื่องที่มีรอบระยะเวลาการตรวจสอบเกินกว่า 1 ปี จึงขอทราบว่าสามารถ	สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถจัดให้มีการตรวจสอบตามแผนดังกล่าวได้ ทั้งนี้สำหรับงานด้าน IT ที่มีความเสี่ยงสูง หรือระบบที่มีนัยสำคัญต้องตรวจสอบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีเหตุการณ์ผิดปกติด้าน IT ที่มีนัยสำคัญ โดยแผนและขอบเขตต้องได้รับอนุมัติจากคณะกรรมการ

ข้อ	คำถาม	คำตอบ
	ตรวจสอบตามแผนและรอบเวลาดังกล่าวได้หรือไม่	ตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยงและการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องด้าน IT อย่างเพียงพอเหมาะสม
การดูแลระบบงานที่รองรับช่องทางการให้บริการทางอุปกรณ์เคลื่อนที่ (mobile banking)		
12.	การนับระยะเวลาของระบบ Mobile Banking ขัดข้อง มีวิธีการอย่างไร (ปรับปรุงวันที่ 24 กันยายน 2568)	ให้นับระยะเวลาของปัญหาหรือเหตุการณ์ขัดข้องที่มีระยะเวลาตั้งแต่ 15 นาทีขึ้นไป และส่งผลกระทบอย่างมีนัยสำคัญต่อการให้บริการลูกค้าในช่องทางการให้บริการ Mobile Banking ตามเงื่อนไข ดังนี้ (1) เหตุการณ์ระบบขัดข้องส่งผลกระทบต่อผู้ใช้บริการมากกว่า 10,000 ราย <u>หรือ</u> (2) เหตุการณ์ระบบขัดข้องส่งผลกระทบต่อธุรกรรมทางการเงินในปริมาณมากกว่า 10% โดยให้นับผลกระทบตั้งแต่เริ่มเกิดปัญหาหรือเหตุการณ์ขัดข้อง จนถึงระบบกลับมาให้บริการได้ปกติ หากเข้าข่ายอย่างใดอย่างหนึ่ง ถือว่าเข้าข่ายนับระยะเวลาขัดข้องตามหลักเกณฑ์ ทั้งนี้ ในกรณีที่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจ มีการให้บริการหลาย Mobile Banking Application ให้นับระยะเวลาขัดข้องตามหลักเกณฑ์เฉพาะผลิตภัณฑ์ Mobile Banking หลักที่ให้บริการแก่ลูกค้ารายย่อย สำหรับวิธีการคำนวณผลกระทบของปัญหาหรือเหตุการณ์ขัดข้องที่เข้าข่ายนับระยะเวลาขัดข้อง ให้ดำเนินการดังนี้ 1) จำนวนผู้ใช้บริการที่ได้รับผลกระทบมากกว่า 10,000 ราย จำนวนผู้ใช้บริการที่ได้รับผลกระทบในช่วงเวลาที่เกิดปัญหาหรือเหตุการณ์ขัดข้อง มากกว่า 10,000 ราย ให้คำนวณดังนี้ 1. จำนวนผู้ใช้บริการที่ได้รับผลกระทบในช่วงเวลาที่เกิดปัญหาหรือเหตุการณ์ขัดข้อง ให้ใช้ค่าเฉลี่ยของบัญชีผู้ใช้บริการ Mobile Banking ที่ทำธุรกรรมทางการเงิน (Financial) ในช่วงเวลาเดียวกันกับช่วงที่

ข้อ	คำถาม	คำตอบ
		เกิดเหตุ ย้อนหลัง 3 เดือนแบบ Rolling Basis โดยอ้างอิงข้อมูลจากวันที่เดียวกันกับวันที่เกิดเหตุในแต่ละเดือน และสิ้นสุดที่สิ้นเดือนก่อนหน้าเดือนที่เกิดเหตุ เช่น หากเกิดเหตุวันที่ 1 ก.ค. เวลา 9.00 - 10.00 น. ให้ใช้ค่าเฉลี่ยของข้อมูลในช่วงเวลา 9.00 – 10.00 น. ของวันที่ 1 เม.ย. 1 พ.ค. และ 1 มิ.ย. <u>กรณีเกิดเหตุวันสิ้นเดือน</u> ให้อ้างอิงข้อมูลวันสิ้นเดือนในแต่ละเดือน เช่น หากเกิดเหตุวันที่ 30 มิ.ย. เวลา 9.00 - 10.00 น. ให้ใช้ค่าเฉลี่ยของข้อมูลในช่วงเวลา 9.00 - 10.00 น. ของวันที่ 31 มี.ค. 30 เม.ย. และ 31 พ.ค. <u>กรณีไม่สามารถหาวันที่เดียวกันในเดือนย้อนหลังได้</u> ให้อ้างอิงข้อมูลวันที่ที่ใกล้เคียงที่สุดในแต่ละเดือน เช่น หากเกิดเหตุวันที่ 30 พ.ค. เวลา 9.00 - 10.00 น. ให้ใช้ค่าเฉลี่ยของข้อมูลในช่วงเวลา 9.00 - 10.00 น. ของวันที่ 28 ก.พ. 30 มี.ค. และ 30 เม.ย. 2) จำนวนธุรกรรมทางการเงินที่ได้รับผลกระทบมากกว่า 10% $\frac{\text{จำนวนธุรกรรมทางการเงินที่ได้รับผลกระทบในช่วงเวลาที่เกิดปัญหาหรือเหตุการณ์ขัดข้อง}}{\text{จำนวนธุรกรรมทางการเงินทั้งหมด}} > 10\%$ ให้คำนวณดังนี้ 1. จำนวนธุรกรรมทางการเงินที่ได้รับผลกระทบในช่วงเวลาที่เกิดปัญหาหรือเหตุการณ์ขัดข้อง ให้ใช้ค่าเฉลี่ยจำนวนธุรกรรมทางการเงินที่สำเร็จในช่วงเวลาเดียวกันกับช่วงที่เกิดเหตุ ย้อนหลัง 3 เดือนแบบ Rolling Basis โดยอ้างอิงข้อมูลจากวันที่เดียวกันกับวันที่เกิดเหตุในแต่ละเดือน และสิ้นสุดที่สิ้นเดือนก่อนหน้าเดือนที่เกิดเหตุ เช่น หากเกิดเหตุวันที่ 1 ก.ค. เวลา 9.00 - 10.00 น. ให้ใช้ค่าเฉลี่ยของข้อมูลในช่วงเวลา 9.00 - 10.00 น. ของวันที่ 1 เม.ย. 1 พ.ค. และ 1 มิ.ย.

ข้อ	คำถาม	คำตอบ
		<u>กรณีเกิดเหตุวันสิ้นเดือน</u> ให้อ้างอิงข้อมูลวันสิ้นเดือนในแต่ละเดือน เช่น หากเกิดเหตุวันที่ 30 มิ.ย. เวลา 9.00 - 10.00 น. ให้ใช้ค่าเฉลี่ยของข้อมูลในช่วงเวลา 9.00 - 10.00 น. ของวันที่ 31 มี.ค. 30 เม.ย. และ 31 พ.ค. <u>กรณีไม่สามารถหาวันที่เดียวกันในเดือนย้อนหลังได้</u> ให้อ้างอิงข้อมูลวันที่ที่ใกล้เคียงที่สุดในแต่ละเดือน เช่น หากเกิดเหตุวันที่ 30 พ.ค. เวลา 9.00 - 10.00 น. ให้ใช้ค่าเฉลี่ยของข้อมูลในช่วงเวลา 9.00 - 10.00 น. ของวันที่ 28 ก.พ. 30 มี.ค. และ 30 เม.ย. 2. จำนวนธุรกรรมทางการเงินทั้งหมด ให้ใช้ประมาณการจากค่าเฉลี่ยของจำนวนธุรกรรมทางการเงินรายวันที่สำเร็จย้อนหลัง 3 เดือนแบบ Rolling Basis โดยอ้างอิงข้อมูลจากทุกวันในแต่ละเดือน และสิ้นสุดที่สิ้นเดือนก่อนหน้าเดือนที่เกิดเหตุ เช่น หากเกิดเหตุวันที่ 1 ก.ค. ให้ใช้ค่าเฉลี่ยของข้อมูลรายวันตั้งแต่วันที่ 1 เม.ย. ถึง 30 มิ.ย. สำหรับลักษณะเหตุการณ์ปัญหา และวิธีการคำนวณผลกระทบของปัญหาหรือเหตุการณ์ขัดข้องที่เข้าข่ายนับระยะเวลาระบบขัดข้อง ให้ดำเนินการตามแนวทางที่กำหนดในหนังสือเวียน เรื่อง การปรับปรุงแนวทางการเปิดเผยข้อมูลสถิติระบบเทคโนโลยีสารสนเทศขัดข้องที่กระทบต่อการให้บริการสำคัญของธนาคารพาณิชย์
การแจ้ง การรายงาน หรือการขออนุญาต ต่อ ธปท.		
13.	การรายงานปัญหาหรือเหตุการณ์ผิดปกติด้าน IT ในข้อ 10.3 (3) กรณีปัญหาหรือเหตุขัดข้องของระบบ IT ที่ส่งผลกระทบต่อการให้บริการผ่านช่องทางให้บริการสำคัญ เป็นเหตุการณ์ใดบ้าง (ปรับปรุงวันที่ 24 กันยายน 2568)	สถาบันการเงินและสถาบันการเงินเฉพาะกิจจะต้องรายงานปัญหาหรือเหตุขัดข้องของระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อการให้บริการผ่านช่องทางให้บริการสำคัญ ได้แก่ สาขา ATM/CDM Internet Banking และ Mobile Banking ที่มีระยะเวลาขัดข้องตั้งแต่ 15 นาทีขึ้นไป (15 นาที 0 วินาที) โดยยังไม่ต้องคำนวณผลกระทบต่อการ

ข้อ	คำถาม	คำตอบ
		ให้บริการ นอกจากนี้ การรายงานปัญหาหรือเหตุการณ์ขัดข้องของช่องทางให้บริการ Internet Banking และ Mobile Banking ให้รายงานครอบคลุมทุกผลิตภัณฑ์ที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจให้บริการ ทั้งนี้ ขอให้รายงานผ่านระบบ event report ธปท. โดยเร็ว โดยสามารถแจ้งสาเหตุ การแก้ไขปัญหา และแนบเอกสารประกอบการคำนวณผลกระทบเพิ่มเติมในภายหลังได้
14.	ขอทราบรายละเอียดการรายงานข้อมูลต่อธนาคารแห่งประเทศไทยที่กำหนดในข้อ 10.4 ของประกาศ	ให้ธนาคารพาณิชย์และสถาบันการเงินเฉพาะกิจทุกแห่งต้องจัดทำและจัดส่งแบบรายงานตามขอบเขตการรายงาน รูปแบบและระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนดตามหนังสือเวียน เรื่อง การรายงานชุดข้อมูล (Data Set) เพื่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารเทศของธนาคารพาณิชย์ โดยให้รายงานผ่านช่องทาง DMS สำหรับบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ให้รายงานเฉพาะชุดข้อมูลบุคคลภายนอกที่มีนัยสำคัญตามขอบเขตการรายงาน รูปแบบและระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนดตามหนังสือเวียน เรื่อง การรายงานชุดข้อมูล (Data Set) เพื่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารเทศของธนาคารพาณิชย์ โดยให้รายงานผ่านช่องทาง e-Application
ขอบเขตการบังคับใช้		
15.	บริษัทลูกในกลุ่ม Solo Consolidation จะต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วยหรือไม่	บริษัทลูกในกลุ่ม Solo Consolidation ตามประกาศ ธปท. ที่ สนส.12/2561 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงของกลุ่มธุรกิจทางการเงิน ให้ปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้เฉพาะหัวข้อการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management) ทั้งนี้ สถาบันการเงินควรกำกับดูแลบริษัทลูกในกลุ่ม Solo Consolidation ให้มีการบริหารจัดการความเสี่ยงด้าน IT ในภาพรวมอย่างรัดกุมเพียงพอ โดย

ข้อ	คำถาม	คำตอบ
		สามารถอ้างอิงตามแนวปฏิบัติในการบริหารความเสี่ยงด้าน IT ของธนาคารแห่งประเทศไทยเป็นแนวทางดำเนินการ

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทร. 0-2283-6445

ธนาคารแห่งประเทศไทย

IT Risk Management Implementation Guideline
แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายกำกับระบบการชำระเงินและคุ้มครองผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย

สารบัญ

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ 3

1. การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT governance) 4

2. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) 16

3. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management) 42

เอกสารอ้างอิง 45

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT governance)

1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

วัตถุประสงค์ เพื่อให้คณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจกำกับดูแลและสนับสนุนให้องค์กรบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามด้านไซเบอร์อย่างเพียงพอเหมาะสมและสอดคล้องกับการให้บริการหรือดำเนินธุรกิจ

1.1.1 คณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจประกอบด้วยกรรมการที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างน้อย 1 ท่าน เพื่อให้คณะกรรมการสามารถกำหนดทิศทางและกำกับดูแลให้การใช้เทคโนโลยีสารสนเทศสอดรับกับกลยุทธ์การให้บริการหรือดำเนินธุรกิจ มีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีที่เปลี่ยนแปลงไป

1.1.2 ดูแลให้การใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจ และดูแลให้การใช้เทคโนโลยีมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการเปลี่ยนแปลงการให้บริการหรือดำเนินธุรกิจในอนาคต

1.1.3 ดูแลให้มีการติดตาม และควบคุมให้บริการทางการเงินผ่านช่องทาง mobile banking application หยุดชะงักได้ไม่เกิน 8 ชั่วโมงในรอบ 1 ปีปฏิทิน รวมทั้งต้องดูแลให้มีการกู้คืนระบบงานที่หยุดชะงักโดยเร็ว

1.1.4 ดูแลให้มีการติดตาม และควบคุมเหตุการณ์ทุจริตทั้งที่เกิดภายในและภายนอกองค์กรให้สอดคล้องตามมาตรฐานสากลและตามระดับความเสี่ยงที่กำหนดไว้

1.1.5 ดูแลให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมขององค์กร (enterprise risk management : ERM) ในฐานะที่เป็นความเสี่ยงที่สำคัญ

1.1.6 ดูแลให้มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยนโยบายดังกล่าวต้องสอดคล้องกับลักษณะการให้บริการหรือดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้อง

1.1.7 ดูแลให้มีมาตรฐาน ระเบียบวิธีปฏิบัติ กระบวนการ เครื่องมือ และบุคลากรในการรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายข้อ 1.1.6 รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม ทบทวนและประเมินประสิทธิภาพนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.1.8 ดูแลให้มีการติดตาม ตรวจสอบและรายงานต่อคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูง อย่างเหมาะสม ในเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น ผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ทางด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

1.1.9 ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เพื่อให้ตระหนักถึงความสำคัญของความเสี่ยงและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งเข้าใจการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เพื่อช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.1.10 คณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ต้องได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศอย่างเพียงพอตามระยะเวลาที่เหมาะสม เพื่อให้มีความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศที่เพียงพอต่อการกำกับดูแลและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้ทันกับภัยคุกคามใหม่ รวมถึงการพิจารณาเชิงกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการขับเคลื่อนธุรกิจ

1.2 โครงสร้างการกำกับดูแล

<u>วัตถุประสงค์</u> เพื่อให้มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเหมาะสมสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence)

<u>คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ</u>

1.2.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดตั้งคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงการถ่วงดุลอำนาจอย่างเป็นอิสระ อย่างน้อยครอบคลุม

- คณะกรรมการที่ทำหน้าที่บริหารจัดการ และกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (เช่น IT steering committee หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดกลยุทธ์ นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ตลอดจนกำกับดูแลการพัฒนา ปรับปรุงระบบและโครงสร้างพื้นฐานด้าน IT ในภาพรวมขององค์กรให้มีความสอดคล้องกัน มีความเสถียรและมีศักยภาพเพียงพอรองรับการให้บริการได้อย่างต่อเนื่อง รวมทั้งกำกับดูแลและติดตามการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้ อาจพิจารณาให้มีคณะกรรมการที่ดูแลงานเฉพาะด้านเพิ่มเติม หากเห็นว่างานดังกล่าวมีนัยสำคัญหรือมีผลกระทบสูงต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เช่น คณะกรรมการหรืออนุกรรมการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้านสถาปัตยกรรมเทคโนโลยีสารสนเทศ เป็นต้น
- คณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (เช่น คณะกรรมการบริหารความเสี่ยง คณะกรรมการบริหารความเสี่ยงด้านปฏิบัติการ คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ รวมทั้งกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในภาพรวม (enterprise risk management) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
- คณะกรรมการที่ทำหน้าที่กำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ (เช่น คณะกรรมการตรวจสอบ เป็นต้น) เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจ มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

<u>โครงสร้างองค์กร</u>

1.2.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีโครงสร้างองค์กรและหน้าที่ความรับผิดชอบเป็นลายลักษณ์อักษร สอดคล้องตามหลักการตรวจสอบและถ่วงดุล (check and balance) และการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน (segregation of duties) ระหว่างการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ

1.2.3 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรดูแลให้มีทรัพยากรเพียงพอที่จะสนับสนุนการปฏิบัติงานการบริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ สอดคล้องตามปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น จัดให้มีบุคลากรที่มีความรู้ความเชี่ยวชาญและมีเครื่องมือหรือระบบที่ช่วยสนับสนุนการปฏิบัติงาน เป็นต้น

1.2.4 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์ และมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) โดยมีบทบาทหน้าที่และความรับผิดชอบอย่างน้อยดังนี้

- กำหนดให้มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด
- กำหนดให้มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)
- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจเป็นวาระประจำ
- ดูแลและดำเนินการให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์
- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้านภัยคุกคามทางไซเบอร์

1.2.5 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer : CISO) โดยควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) งานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (authority) เพียงพอสำหรับการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้

- รายงานปัญหาหรือเหตุการณ์ผิดปกติที่มีนัยสำคัญด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด หรือคณะกรรมการที่เกี่ยวข้อง หรือคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจโดยตรง
- ให้ความคิดเห็นในเรื่องการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจหรือคณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ

1.2.6 หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น first line of defence) เช่น หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานอื่นที่เป็นผู้ใช้งานระบบ

1.2.6.1 หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีหน้าที่ปฏิบัติงานตามที่ได้รับมอบหมาย รวมทั้งประเมินความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ จัดให้มีแนวทางการควบคุม ติดตามและรายงานการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้อง อย่างน้อยครอบคลุม

- รายงานผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations) เช่น สถานะความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ (capacity and system utilization) เหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem) ระดับการให้บริการงานด้านเทคโนโลยีสารสนเทศ (service availability) เป็นต้น
- รายงานความคืบหน้า ปัญหาและอุปสรรคในการดำเนินโครงการด้านเทคโนโลยีสารสนเทศในภาพรวมและรายโครงการที่สำคัญ
- รายงานการติดตามและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งแนวโน้มความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้นและส่งผลกระทบต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
- รายงานผลการประเมินความเสี่ยง การติดตามความเสี่ยง และแนวทางการควบคุมที่เกี่ยวข้อง
- รายงานความคืบหน้าการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง
- รายงานผลการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก

1.2.6.2 ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ มีหน้าที่ปฏิบัติตามนโยบายและระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องจากการใช้งานระบบ

1.2.7 หน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น second line of defence)

1.2.7.1 กำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยอย่างน้อยครอบคลุม ดังนี้

(1) โครงสร้างองค์กร

(1.1) สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management function) โดยสามารถจัดตั้งเป็นหน่วยงานที่รับผิดชอบงานการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือเป็นส่วนหนึ่งกับหน่วยงานบริหารความเสี่ยง หรือรูปแบบอื่น ๆ ก็ได้ ทั้งนี้ ต้องมั่นใจว่ายังคงมีความเป็นอิสระเพียงพอที่สามารถปฏิบัติงานได้อย่างครบถ้วนและมีประสิทธิภาพ

(1.2) กำหนดสายการรายงานที่ชัดเจนและเป็นอิสระจากหน่วยงานที่ทำหน้าที่เป็น first line of defence โดยรวบรวมและเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกับความเสี่ยงด้านอื่นของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ พร้อมทั้งนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยง

(1.3) ผู้รับผิดชอบงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องมีความรู้ประสบการณ์ และความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

รวมถึงได้รับการฝึกอบรมด้านการบริหารจัดการความเสี่ยงและเพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง เพื่อให้สามารถบริหารจัดการความเสี่ยงและติดตามความเสี่ยงได้อย่างมีประสิทธิภาพ

(2) การปฏิบัติงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กำหนดให้มีระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) ที่ได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย รวมทั้งมีการจัดทำกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยประสานงานร่วมกับหน่วยงานที่ทำหน้าที่เป็น first line of defence ในการระบุและประเมินความเสี่ยง การกำหนดมาตรการในลดความเสี่ยงและระบบการควบคุมภายใน โดยมีกระบวนการอย่างน้อยครอบคลุม ดังนี้

(2.1) การประเมินความเสี่ยง

(2.1.1) การระบุความเสี่ยง ควรระบุเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นหรือที่เกิดขึ้นจริง ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการให้บริการหรือดำเนินธุรกิจ โดยครอบคลุมเหตุการณ์ความเสี่ยงอย่างน้อย ดังนี้

- ผู้กระทำให้เกิดความเสี่ยงและเหตุการณ์ความเสี่ยง เช่น ผู้ไม่ประสงค์ดี ภัยคุกคามหรือช่องโหว่ เป็นต้น
- ประเภทของความเสี่ยง เช่น ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ ความเสี่ยงด้านโปรแกรม ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงด้านสถาปัตยกรรมเทคโนโลยีสารสนเทศ ความเสี่ยงด้านการบริหารโครงการ เป็นต้น
- วัน เวลา สถานที่ ช่วงเวลาหรือระยะเวลาที่เกิดเหตุการณ์ผิดปกติหรือความเสี่ยงด้านเทคโนโลยี (ถ้ามี)
- สาเหตุของการเกิดเหตุการณ์ เช่น กระบวนการปฏิบัติงาน ระบบงาน บุคลากร การใช้บริการจากบุคคลภายนอก ปัจจัยภายนอก เป็นต้น
- ผลกระทบต่อทรัพย์สิน ทรัพยากร การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการให้บริการหรือดำเนินธุรกิจ

(2.1.2) การวิเคราะห์ความเสี่ยง ควรเข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยครอบคลุมอย่างน้อย ดังนี้

- กำหนดเจ้าของความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ระบุการควบคุมที่มีอยู่ในปัจจุบัน
- พิจารณาและค้นหาสาเหตุและสถานการณ์ที่เป็นไปได้
- วิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2.1.3) การประเมินค่าความเสี่ยง ควรประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงานและการให้บริการ

หรือดำเนินธุรกิจ เพื่อจัดลำดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อย ดังนี้

- กำหนดเกณฑ์การประเมินความเสี่ยงทั้งโอกาสและผลกระทบ
- ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- จัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแสดงในแผนภาพความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2.2) การจัดการความเสี่ยง ควรมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อย ดังนี้

- กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือกแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมสำหรับสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง การลดหรือบรรเทาโอกาสเกิดความเสี่ยง การลดหรือบรรเทาผลกระทบที่เกิดขึ้น การแบ่งหรือโอนความเสี่ยงให้หน่วยงานอื่น การยอมรับความเสี่ยงไว้โดยแจ้งเหตุผลให้ผู้บริหารทราบเพื่อตัดสินใจในการยอมรับความเสี่ยง เป็นต้น
- ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ
- ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้
- จัดทำแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญในการดำเนินการ
- กำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) ให้สอดคล้องกับความสำคัญของงานเทคโนโลยีสารสนเทศแต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง โดยดัชนีชี้วัดความเสี่ยงควรมีทั้งที่เป็นลักษณะ leading indicator และ lacking indicator
- นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2.3) การติดตามและทบทวนความเสี่ยง ควรจัดให้มีกระบวนการในการติดตามดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ตามที่กำหนดและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบ ซึ่งอาจพิจารณานำเครื่องมือมาใช้เพื่อให้สามารถติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ โดยครอบคลุมอย่างน้อย ดังนี้

- ติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

- ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น
- ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น

(2.4) การรายงานความเสี่ยง ควรกำหนดกระบวนการรายงานระดับความเสี่ยง ผลการประเมินและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร รวมทั้งรายงานแนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ เพื่อให้มั่นใจว่ามีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและต่อเนื่อง โดยครอบคลุมอย่างน้อย ดังนี้

- สถานะและผลลัพธ์การดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี
- ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร
- รายงานดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ และรายงานสรุปเหตุการณ์ผิดปกติ
- แนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
- ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง

1.2.7.2 หน่วยงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สามารถให้คำปรึกษาสำหรับโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ เพื่อลดความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้นต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจได้อย่างทันกาล รวมทั้ง ให้ความเห็นที่เป็นอิสระต่อคณะกรรมการหรือผู้บริหารระดับสูงเกี่ยวกับการประเมินความเสี่ยงจากการใช้บริการจากบุคคลภายนอก เช่น การประเมินความเสี่ยงศูนย์คอมพิวเตอร์ หรือการประเมินความพร้อมด้านระบบเครือข่าย หรือการประเมินความเสี่ยงสำหรับการให้บริการผ่านช่องทางดิจิทัล

1.2.8 หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น second line of defence)

1.2.8.1 กำหนดกรอบการกำกับการปฏิบัติตามกฎเกณฑ์ ให้ครอบคลุมถึงกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการกำกับการปฏิบัติตามกฎเกณฑ์ โดยอย่างน้อยครอบคลุม ดังนี้

(1) โครงสร้างองค์กร

(1.1) สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการดำเนินการในงานกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance function) โดยสามารถจัดตั้งเป็นหน่วยงานที่รับผิดชอบงานด้านการกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือเป็นส่วนหนึ่งกับหน่วยงานด้านการปฏิบัติตามกฎหมายและกฎเกณฑ์ หรือรูปแบบอื่น ๆ ก็ได้ ทั้งนี้ ต้องมั่นใจว่ายังคงมีความเป็นอิสระเพียงพอที่สามารถปฏิบัติงานได้อย่างครบถ้วนและมีประสิทธิภาพ

(1.2) กำหนดสายการรายงานที่ชัดเจนและเป็นอิสระจากหน่วยงานที่ทำหน้าที่เป็น first line of defence โดยรายงานถึงหัวหน้าหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ที่มีสายการรายงานตรงถึงคณะกรรมการที่เกี่ยวข้อง เช่น คณะกรรมการกำกับการปฏิบัติตามกฎเกณฑ์ เป็นต้น

(1.3) ผู้รับผิดชอบงานด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศต้องมีความรู้ ประสบการณ์ และความเข้าใจในกฎหมายและความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศ รวมถึงต้องได้รับการฝึกอบรมด้านกฎเกณฑ์ต่าง ๆ และเพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง

(2) การปฏิบัติงานด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ กำหนดกระบวนการในการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยอย่างน้อยครอบคลุม ดังนี้

(2.1) การระบุและประเมินความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ ต้องครอบคลุมถึงกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยระบบการชำระเงิน กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและกฎเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

(2.2) การกำหนดแผนการบริหารความเสี่ยงด้านการปฏิบัติงานตามกฎเกณฑ์ (compliance program) ประจำปี ต้องครอบคลุมถึงกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ซึ่งต้องสอดคล้องกับระดับความเสี่ยงที่ประเมินจากข้อ (2.1) โดยพิจารณาดำเนินการสอบทานระเบียบข้อบังคับที่ให้พนักงานถือปฏิบัติ สุ่มสอบทานการปฏิบัติตามกฎเกณฑ์ต่างๆ (compliance testing) และให้ความรู้แก่พนักงานในเรื่องกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(2.3) การติดตามและรายงานผลการสอบทานด้านการปฏิบัติตามกฎเกณฑ์ฝ้น ต้องสรุปผลการสอบทานการปฏิบัติตามกฎเกณฑ์และเหตุการณ์ที่ไม่ปฏิบัติตามกฎเกณฑ์พร้อมทั้งมาตรการแก้ไข รวมถึงผลการดำเนินการตามข้อเสนอแนะคำสั่งการของ ธปท. ผู้กำกับดูแลอื่น และรายงานต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำอย่างสม่ำเสมอ โดยอาจพิจารณานำเครื่องมือมาใช้เพื่อให้สามารถติดตามผลการปฏิบัติตามกฎเกณฑ์และมาตรการแก้ไขได้อย่างมีประสิทธิภาพ

1.2.8.2 หน่วยงาน IT compliance ควรเป็นศูนย์กลางด้านการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อให้คำแนะนำ คำปรึกษากับผู้บริหารระดับสูงและพนักงาน รวมถึงจัดอบรมให้ความรู้แก่พนักงานอย่างสม่ำเสมอ

1.2.9 หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น third line of defence)

1.2.9.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดโครงสร้างและสายการรายงาน ดังนี้

(1) สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการดำเนินการในการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit function) โดยสามารถจัดตั้งเป็นหน่วยงานที่รับผิดชอบ

การตรวจสอบด้านเทคโนโลยีสารสนเทศ หรืออยู่ภายใต้สายงานตรวจสอบภายใน ทั้งนี้ ต้องมั่นใจว่ามีความเป็นอิสระและสามารถปฏิบัติงานได้อย่างครบถ้วนและมีประสิทธิภาพ

(2) กำหนดสายการรายงานที่เป็นอิสระ โดยต้องรายงานถึงหัวหน้าหน่วยงานตรวจสอบภายใน และรายงานตรงต่อคณะกรรมการตรวจสอบ

(3) ผู้รับผิดชอบงานด้านการตรวจสอบเทคโนโลยีสารสนเทศต้องมีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก ที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

(4) ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องได้รับการฝึกอบรม เพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง เพื่อให้ผู้ตรวจสอบสามารถนำมาปรับใช้กับวิธีการตรวจสอบได้ทันกับแนวโน้มและการพัฒนาทางด้านเทคโนโลยีสารสนเทศ

1.2.9.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยอย่างน้อยครอบคลุม ดังนี้

(1) การกำหนดแผนงานตรวจสอบ ควรสอดคล้องกับความสำคัญและความเสี่ยงของการใช้งานเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงพิจารณาตรวจสอบงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญควรตรวจสอบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์ผิดปกติในเทคโนโลยีสารสนเทศที่มีนัยสำคัญ โดยแผนงานและขอบเขตการตรวจสอบต้องได้รับการอนุมัติจากคณะกรรมการตรวจสอบ รวมถึงต้องทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าว โดยคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(2) การตรวจสอบ ควรตรวจสอบตามแผนงานและขอบเขตที่กำหนดอย่างน้อยปีละ 1 ครั้ง โดยการตรวจสอบควรเป็นไปตามมาตรฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด สอดคล้องกับกฎหมาย หลักเกณฑ์ที่เกี่ยวข้องและมาตรฐานสากลที่ยอมรับโดยทั่วไป โดยพิจารณานำเครื่องมือมาช่วยในกระบวนการตรวจสอบให้มีประสิทธิภาพยิ่งขึ้น รวมทั้งอาจยกระดับกระบวนการตรวจสอบในรูปแบบของการตรวจสอบและการติดตามการควบคุมแบบต่อเนื่อง เพื่อให้สามารถตรวจจับการทำงานที่ผิดปกติและพบความบกพร่องของการควบคุมภายในได้อย่างทันการณ์ ซึ่งช่วยส่งเสริมให้การตรวจสอบและการควบคุมภายในมีประสิทธิภาพมากยิ่งขึ้น

(3) การติดตามและรายงานผลการตรวจสอบ ต้องสรุปผลการตรวจสอบและประเด็นที่ต้องแก้ไขกับผู้บริหารของหน่วยงานผู้รับตรวจและจัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการตรวจสอบและแจ้งให้ผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบ รวมถึงติดตามให้มีการปรับปรุงประเด็นการตรวจสอบและรายงานประเด็นสำคัญพร้อมแผนปรับปรุงให้กับคณะกรรมการตรวจสอบเป็นประจำอย่างสม่ำเสมอ

1.2.9.3 ผู้ตรวจสอบภายในอาจถูกร้องขอให้มีส่วนร่วมในการให้คำปรึกษาเกี่ยวกับระบบการควบคุมภายในต่างๆ ในเรื่อง การออกผลิตภัณฑ์ใหม่ ระบบใหม่ หรือโครงการที่มีนัยสำคัญต่างๆ อย่างไรก็ตาม

การทำหน้าที่ให้คำปรึกษา ผู้ตรวจสอบควรคำนึงถึงความเป็นอิสระของผู้ตรวจสอบในการทำหน้าที่ตรวจสอบด้วย

1.2.9.4 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีการรับรองคุณภาพงานตรวจสอบให้ครอบคลุมถึงงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ โดยอาจใช้การตรวจสอบคุณภาพงานภายในกันเองระหว่างผู้ตรวจสอบ นอกจากนี้ ควรมีการสอบทานคุณภาพงานตรวจสอบภายในโดยบุคคลภายนอกที่เป็นอิสระ อย่างน้อยทุก 3-5 ปี เพื่อให้มั่นใจว่าการปฏิบัติงานตรวจสอบเป็นไปตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

<u>วัตถุประสงค์</u> เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและสอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.3.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีนโยบายเป็นลายลักษณ์อักษรและอยู่ใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) อย่างน้อยครอบคลุมนโยบายดังต่อไปนี้

- นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy)
- นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy)

1.3.2 นโยบายดังกล่าวควรสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการให้บริการหรือดำเนินธุรกิจ ความเสี่ยงที่เกี่ยวข้องทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศและความเสี่ยงจากบุคคลภายนอก รวมทั้งสอดคล้องกับแนวทางบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

1.3.3 นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ควรรวมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมอย่างน้อย ดังนี้

- การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)
- การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)
- การควบคุมการเข้าถึง (access control)
- การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)
- การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)
- การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)
- การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (system acquisition and development)
- การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem management)
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

1.3.4 นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ครอบคลุมโครงสร้างองค์กร บทบาทหน้าที่ของผู้เกี่ยวข้อง และกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.3.5 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรจัดให้มีการ

ชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและมีการควบคุมดูแลให้มีการปฏิบัติตามนโยบายได้อย่างถูกต้องครบถ้วน

1.4 การบริหารจัดการบุคลากร

วัตถุประสงค์ เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอสำหรับปฏิบัติงานที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศ โดยบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

1.4.1 มีกระบวนการบริหารจัดการบุคลากรอย่างเหมาะสม ครอบคลุม การคัดเลือกบุคลากรที่มีความรู้ความสามารถเพียงพอ การว่าจ้างบุคลากรที่เป็นไปตามข้อกำหนดหรือเงื่อนไขด้านความปลอดภัยเทคโนโลยีสารสนเทศ การพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงหรือสิ้นสุดการว่าจ้างบุคลากร รวมทั้งการดูแลบุคลากรให้เพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศ

1.4.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจอาจพิจารณาการได้รับการรับรองความรู้ความสามารถตามมาตรฐานที่รับรองทั่วไป (certificate) เฉพาะด้านที่เกี่ยวข้องกับงานด้านเทคโนโลยีสนเทศ เพื่อให้ได้บุคลากรที่มีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

1.4.3 หน่วยงานทรัพยากรบุคคล ควรตรวจสอบประวัติของบุคลากรก่อนการว่าจ้างตามความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ เช่น ประวัติการศึกษา ประวัติการทำงาน ประวัติอาชญากรรม ข้อมูลเครดิตบูโร เป็นต้น

1.4.4 มีข้อกำหนดหรือเงื่อนไขในสัญญาจ้างหรือระเบียบข้อบังคับภายในองค์กร โดยกล่าวถึงบทบาทหน้าที่ความรับผิดชอบ การปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

1.4.5 ให้บุคลากรและบุคคลภายนอกที่ได้รับการว่าจ้างทำความเข้าใจ รับทราบและลงนามยอมรับเงื่อนไขการว่าจ้างงานหรือระเบียบข้อบังคับภายในองค์กร นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และข้อตกลงการไม่เปิดเผยข้อมูล (non disclosure agreement) ก่อนเริ่มปฏิบัติงาน

1.4.6 มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน เช่น การคืนทรัพย์สินของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ การบริหารจัดการสิทธิต้องมีการปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องมีการสื่อสารให้ผู้เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่และความรับผิดชอบ เป็นต้น

1.5 การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness)

วัตถุประสงค์ เพื่อให้บุคลากรทุกระดับของสถาบันการเงินและสถาบันการเงินเฉพาะกิจมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1.5.1 กำหนดโปรแกรมการอบรมและพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ (training program) ที่ครอบคลุม การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ให้แก่บุคลากรทุกระดับ โดยมีการวัดประสิทธิผลของหลักสูตรฝึกอบรมที่จัดขึ้น เช่น

- หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (first line of defence) ให้มีความรู้และความเชี่ยวชาญที่เพียงพอต่อการปฏิบัติงานและการใช้งาน
- หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องกับงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (second line of defence) และการตรวจสอบด้านเทคโนโลยีสารสนเทศ (third line of defence) ให้มีความรู้และความเชี่ยวชาญเพียงพอที่จะระบุ ประเมิน และให้ข้อเสนอแนะในการปรับปรุงประสิทธิภาพของการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่หน่วยงานที่ทำหน้าที่ first line of defence

1.5.2 กำหนดโปรแกรมในการเสริมสร้างความตระหนัก (awareness program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย เช่น การทดสอบเรื่อง social engineering และ phishing การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น โดยโปรแกรมดังกล่าวควรครอบคลุมตั้งแต่ระดับคณะกรรมการ ผู้บริหารระดับสูง และบุคลากรทุกระดับ รวมถึงบุคคลภายนอกที่เกี่ยวข้อง รวมทั้งมีการจัดกิจกรรมเสริมสร้างความตระหนักอย่างต่อเนื่อง นอกจากนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรจัดให้มีการประชาสัมพันธ์เพื่อสร้างความรู้หรือสร้างความตระหนักในการใช้งานบริการทางอิเล็กทรอนิกส์อย่างปลอดภัย ให้แก่ลูกค้า หรือผู้ใช้บริการทราบอย่างสม่ำเสมอด้วย

1.5.3 เสริมสร้างความตระหนัก เรื่องการรักษาความมั่นคงปลอดภัย ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภัยคุกคามทางไซเบอร์ให้กับลูกค้าและผู้ใช้บริการอย่างสม่ำเสมอ เท่าทันกับความเสี่ยงและภัยคุกคามใหม่ ๆ

2. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

2.1 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

วัตถุประสงค์ เพื่อให้มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วนและควบคุมดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งานและสามารถรองรับการให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

2.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน

2.1.2 จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำ ปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ และบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

2.1.3 วางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) จากผู้ผลิตได้อย่างเหมาะสมทันการณ์

2.1.4 กรณีมีการใช้ทรัพย์สินด้านเทคโนโลยีสารสนเทศที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการให้บริการ ควรมีการประเมินความเสี่ยงจากการใช้งาน จัดหาการควบคุมแทน รวมทั้งได้รับอนุมัติจากผู้บริหารที่ทำหน้าที่บริหารความเสี่ยง นอกจากนี้ ควรใช้ทรัพย์สินด้านเทคโนโลยีสารสนเทศที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการให้บริการเพียงระยะสั้นตามระดับความเสี่ยงเท่านั้น

2.1.5 มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT inventory list) ของฮาร์ดแวร์ (hardware) และซอฟต์แวร์ (software) ที่รองรับระบบเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างครบถ้วนและเป็นลายลักษณ์อักษร โดยครอบคลุมอย่างน้อย ดังนี้

- ชื่อเครื่องแม่ข่าย
- ชื่อระบบปฏิบัติการ (operating system) และเวอร์ชั่น
- ชื่อระบบงาน (application) และเวอร์ชั่น
- เจ้าของทรัพย์สิน (owner)
- ประเภทของอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (specification)
- หมายเลขอ้างอิงของฮาร์ดแวร์ (serial number) และหมายเลขอ้างอิงของซอฟต์แวร์ (software license)
- สถานที่ตั้ง
- วันที่เริ่มติดตั้ง
- ประเภทการครอบครอง (ซื้อหรือเช่า)
- รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา
- วันที่บำรุงรักษาล่าสุด
- วันสิ้นสุดการใช้งานตามสัญญา (warranty) และวันสิ้นสุดการรับประกันการใช้งาน (support contract)
- วันสิ้นสุดการให้บริการจากผู้ผลิต (end of support)

2.1.6 มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการทรัพย์สินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

2.1.7 มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน (return asset) เมื่อสิ้นสุดการใช้งานครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในองค์กรของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และกรณี

บุคคลภายนอกมีการใช้งานทรัพย์สินของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ทันทีที่มีการยกเลิกสัญญาจ้างด้วย

2.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

วัตถุประสงค์ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลในรูปแบบอิเล็กทรอนิกส์ ครอบคลุมการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสาร การจัดเก็บหรือใช้ข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ การเก็บรักษาและการทำลายข้อมูล

การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

2.2.1 กำหนดให้มีเจ้าของข้อมูล (information owner) รับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึงและการใช้งานข้อมูลอย่างปลอดภัย

2.2.2 กำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูล (information classification) และวิธีการจัดการข้อมูล (data handling) ตามชั้นความลับให้ครอบคลุมตลอดวงจรชีวิตของข้อมูล (data life cycle) ตั้งแต่ การสร้างหรือการได้มาซึ่งข้อมูล การประมวลผล การจัดเก็บ การใช้งาน ตลอดจนการทำลายข้อมูล รวมทั้งควรระบุชั้นความลับของข้อมูล (labeling) อย่างชัดเจน

2.2.3 กำหนดแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับ ครอบคลุม

- ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint)
- ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit)
- ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest)

2.2.4 กำหนดแนวทางการควบคุมดูแลรักษาความปลอดภัยสื่อบันทึกข้อมูลระหว่างขนส่ง (physical media transfer) เพื่อให้มีการควบคุมการเข้าถึงสื่อที่มีข้อมูลสำคัญในระหว่างการขนส่ง

2.2.5 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการทำลายข้อมูล (information disposal) ครอบคลุม ขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการทำลายข้อมูลให้สอดคล้องกับระดับความสำคัญของข้อมูล โดยมีกระบวนการควบคุมการทำลายข้อมูล ที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูลก่อนดำเนินการ การควบคุมการทำลายในลักษณะ dual control การสอบทานการปฏิบัติงานโดยหัวหน้างาน รวมทั้งจัดให้มีการจัดทำทะเบียนการทำลายข้อมูลสำคัญ โดยระบุผู้รับผิดชอบในการทำลายข้อมูล วันที่ เวลา ชนิดของสื่อบันทึกข้อมูล serial number และวิธีการที่ใช้ทำลายข้อมูล

การบริหารจัดการการเข้ารหัสข้อมูล (cryptography)

2.2.6 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูล ครอบคลุม ขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการเข้ารหัสข้อมูล (cryptographic algorithm) ที่สอดคล้องตามระดับความสำคัญของข้อมูล และการบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management)

2.2.7 วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล เช่น การเข้ารหัสข้อมูลแบบสมมาตร (เช่น AES) การเข้ารหัสข้อมูลแบบอสมมาตร (เช่น public key cryptography) การรับรองเอกสาร (message authentication) การเข้ารหัสด้วยฟังก์ชันแฮช (hash function) และ ลายเซ็นอิเล็กทรอนิกส์ (digital signature) เป็นต้น โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

2.2.8 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management) ควรกำหนดกระบวนการที่มีความรัดกุมปลอดภัยครอบคลุมตั้งแต่ การสร้างและติดตั้ง การจัดเก็บ และการยกเลิกกุญแจเข้ารหัส

การสร้างและติดตั้งกุญแจเข้ารหัสข้อมูล

- มีการควบคุมสภาพแวดล้อมในการสร้างรหัสที่มีความรัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (certification authority) ที่น่าเชื่อถือ มีขั้นตอนการทำลายหลักฐานที่ใช้หลังจากสร้างกุญแจแล้วเสร็จ
- กุญแจเข้ารหัสข้อมูล จะต้องไม่มีพนักงานหรือบุคคลใดบุคคลหนึ่งรู้รหัสทั้งหมด
- กำหนดขนาดของกุญแจเข้ารหัสข้อมูลที่มีความยาวเพียงพอในการป้องกันการถูกถอดรหัส เช่น การถูกโจมตีแบบ brute force เป็นต้น
- การแลกเปลี่ยนกุญแจต้องผ่านกระบวนการและช่องทางที่ปลอดภัย
- กำหนดไม่ให้ใช้กุญแจเข้ารหัสข้อมูลเดียวกันกับหลายระบบงาน

<u>การจัดเก็บกุญแจเข้ารหัสข้อมูล</u>

- มีการรักษาความปลอดภัยของกุญแจเข้ารหัสข้อมูลทั้งด้าน physical และ logical โดยใช้อุปกรณ์รักษาความปลอดภัย HSM หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน
- มีการสำรองข้อมูลกุญแจเข้ารหัสข้อมูล โดยวิธีการเก็บรักษากุญแจเข้ารหัสข้อมูลชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสข้อมูลชุดหลัก

<u>การเปลี่ยนและเพิกถอนกุญแจเข้ารหัสข้อมูล</u>

- กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัสข้อมูล เช่น กรณีกุญแจหมดอายุล้าสมัย กรณีกุญแจเข้ารหัสเกิดการรั่วไหลหรือไม่ปลอดภัย เป็นต้น
- กำหนดกระบวนการทำลายกุญแจ โดยต้องมั่นใจว่าไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก

2.2.9 กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัสข้อมูล เช่น การติดต่อหน่วยงานหรือผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัสชุดดังกล่าว การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจการเข้ารหัสข้อมูล เป็นต้น

2.3 การควบคุมการเข้าถึง (access control)

<u>วัตถุประสงค์</u> เพื่อให้มีการบริหารจัดการบัญชีสิทธิสูงและสิทธิของผู้ใช้งานมีประสิทธิภาพเป็นไปตามหลักความจำเป็นของการใช้งานและสอดคล้องกับหลักการแบ่งแยกงานด้านเทคโนโลยีสารสนเทศที่ดี โดยสามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.3.1 กำหนดมาตรฐานและระเบียบปฏิบัติการบริหารจัดการบัญชีสิทธิสูงและบัญชีผู้ใช้งานภายในองค์กร ครอบคลุมหน่วยงานที่รับผิดชอบ การกำหนดสิทธิการเข้าถึง การเบิกใช้งาน การสอบทานและการยกเลิกสิทธิ

2.3.2 กำหนดบทบาท หน้าที่และความรับผิดชอบของผู้ใช้งานที่มีสิทธิสูงและผู้ใช้งานให้ชัดเจน

2.3.3 บัญชีผู้ใช้งานที่มีสิทธิสูงที่ครอบคลุมระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ควรมีการควบคุมอย่างน้อย ดังนี้

- ควบคุมดูแลการให้สิทธิ โดยจำกัดตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน
- จำกัดจำนวนบัญชีผู้ใช้งานที่มีสิทธิสูงเท่าที่จำเป็น
- มีเครื่องมือหรือกระบวนการสร้าง จัดเก็บ เบิกใช้ อนุมัติ การติดตามระหว่างการใช้งานหรือการเข้าถึงระบบ ข้อมูล รวมทั้งสอบทานหลังการใช้งานของบัญชีผู้ใช้งานที่มีสิทธิสูง ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยงอย่างเป็นประจำ เพื่อให้มั่นใจว่าการใช้งานสิทธิเป็นไปตามขอบเขต และความจำเป็นในการใช้งาน

- กำหนดวิธีการระบุตัวตนและพิสูจน์ตัวตนผู้ใช้งานที่รัดกุม สอดคล้องกับนโยบาย มาตรฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนดและมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป โดยอย่างน้อยต้องใช้วิธีการพิสูจน์ตัวตนแบบ multi-factor authentication
- จัดเก็บข้อมูลประวัติการพิสูจน์ตัวตนและการเข้าถึง (access log) และประวัติการดำเนินงาน (activities log)
- กรณีบัญชีผู้ใช้งานที่มีสิทธิสูงสามารถเข้าถึงระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย จากช่องทางการเข้าถึงระยะไกล (remote access) สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีการควรคุมที่เข้มงวด อย่างน้อย ดังนี้
  (1) ขออนุมัติก่อนเข้าถึงจากระยะไกล (remote access) อย่างเคร่งครัด โดยให้ใช้เฉพาะกรณีที่มีความจำเป็นเท่านั้น และจำกัดระยะเวลาในการเข้าถึงระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย
  (2) ใช้การพิสูจน์ตัวตนผู้ใช้งานแบบ multi-factor authentication และการเชื่อมต่อผ่าน virtual private network (VPN)
  (3) ควบคุมการเข้าใช้งาน โดยจำกัดการเข้าใช้งานได้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้น หรือใช้เทคโนโลยีบริหารจัดการเครื่องคอมพิวเตอร์แบบเสมือน (virtual destops infrastructure) เพื่อลดความเสี่ยงจากการติด malware หรือการเข้าถึงระบบงานที่ไม่เหมาะสม
  (4) สามารถระบุและสอบทานแหล่งที่มาของอุปกรณ์หรือระบบปลายทางที่เข้าเชื่อมต่อกับระบบเครือข่ายของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ แบบระยะไกล
  (5) สอบทานการเข้าถึงระบบงานระยะไกลจากบัญชีผู้ใช้งานที่มีสิทธิสูงด้วยบุคคลหรือหน่วยงานที่มีความเป็นอิสระและมีความรู้ความเชี่ยวชาญเพียงพอ

2.3.4 บัญชีของผู้ใช้งานทุกบัญชีของระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย

- กำหนดสิทธิผู้ใช้งานตามบทบาทหน้าที่ ความรับผิดชอบและความจำเป็นในการใช้งาน
- กำหนดวิธีการระบุตัวตนและพิสูจน์ตัวที่เหมาะสม สอดคล้องตามความเสี่ยง สอดคล้องกับนโยบาย มาตรฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด
- กำหนดการตั้งรหัสผ่านสำหรับบัญชีผู้ใช้งานให้เข้มแข็ง โดยอย่างน้อยควรครอบคลุม ดังนี้
  (1) การบังคับให้เปลี่ยนรหัสผ่านครั้งแรกที่เข้าใช้งาน
  (2) ความยาวรหัสผ่านขั้นต่ำและรอบการใช้รหัสผ่านเดิมซ้ำ
  (3) กำหนดให้ตั้งรหัสผ่านแบบซับซ้อน (password complexity)
  (4) จำนวนครั้งการใส่รหัสผ่านผิด
- ไม่ควรใช้บัญชีผู้ใช้งานร่วมกับผู้ใช้งานอื่น
- กรณีที่บัญชีผู้ใช้งานที่สามารถเข้าถึงข้อมูลลูกค้าและเชื่อมต่อมาจากระบบเครือข่ายสื่อสารสาธารณะ (Internet) สถาบันการเงินและสถาบันการเงินเฉพาะกิจ ต้องกำหนดให้การพิสูจน์ตัวตนเป็นแบบ multi-factor authentication อย่างไรก็ตาม หากระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication สถาบันการเงินและสถาบันการเงินเฉพาะกิจ สามารถใช้วิธีการอื่นที่มีประสิทธิภาพเทียบเท่าทดแทนได้ เพื่อลดความเสี่ยงจากการถูกปลอมแปลงตัวตนได้โดยง่าย

2.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

<u>วัตถุประสงค์</u> เพื่อให้มีการรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของศูนย์คอมพิวเตอร์และพื้นที่สำคัญที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเพียงพอรองรับธุรกิจอย่างต่อเนื่อง

2.4.1 การควบคุมการเข้าถึงศูนย์คอมพิวเตอร์และพื้นที่สำคัญต่าง ๆ ภายในศูนย์คอมพิวเตอร์ทางกายภาพควรครอบคลุมอย่างน้อย ดังนี้

- กำหนดมาตรฐานและระเบียบปฏิบัติควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ (ศูนย์ฯ) และพื้นที่สำคัญต่าง ๆ ภายในศูนย์คอมพิวเตอร์
- กำหนดกระบวนการจัดการสิทธิและหน่วยงานที่รับผิดชอบชัดเจน ในการเข้าถึงศูนย์คอมพิวเตอร์และพื้นที่สำคัญ ให้เป็นไปตามหลักความจำเป็น ถูกต้อง และเป็นปัจจุบัน โดยอย่างน้อยครอบคลุมเรื่อง ดังนี้
  (1) จัดทำตารางการควบคุมการให้สิทธิที่สอดคล้องกับตำแหน่งหน้าที่งานเพื่อใช้เป็นแนวทางการกำหนดสิทธิอย่างเป็นระบบและเป็นปัจจุบัน (authorization matrix) และมีการทบทวนตารางควบคุมการให้สิทธิ (authorization matrix) ทุกครั้งที่มีการเปลี่ยนแปลงหรือเป็นประจำอย่างน้อยทุก 6 เดือน
  (2) การอนุมัติการเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่สำคัญภายในศูนย์คอมพิวเตอร์ ต้องดำเนินการโดยผู้ที่มีอำนาจอนุมัติและสอดคล้องตามตารางการควบคุมการให้สิทธิ
  (3) ปรับปรุง/ ยกเลิกสิทธิการเข้า–ออกศูนย์ฯ ทันทีที่พนักงานลาออก โยกย้าย หรือเปลี่ยนหน้าที่ความรับผิดชอบ
  (4) มีการทบทวนสิทธิการเข้า-ออกศูนย์ฯ โดยผู้ที่มีอำนาจอนุมัติอย่างสม่ำเสมอ อย่างน้อยทุก 6 เดือน
- การเข้าถึงโดยพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำภายในศูนย์ฯ หรือบุคคลภายนอกมีกระบวนการในการควบคุมการเข้าถึงแบบชั่วคราว โดยอย่างน้อยควรครอบคลุมเรื่อง ดังนี้
  (1) อนุมัติโดยผู้มีอำนาจอนุมัติก่อนทุกครั้ง
  (2) เจ้าหน้าที่ศูนย์คอมพิวเตอร์ติดตาม (escort) ผู้เข้าถึงแบบชั่วคราวตลอดระยะเวลาที่เข้ามาปฏิบัติงานภายในศูนย์คอมพิวเตอร์
- มีเจ้าหน้าที่ควบคุมการลงบันทึกเข้า-ออกศูนย์ฯ โดยมีขั้นตอนและเครื่องมือที่สามารถระบุตัวตนของผู้ที่ได้รับอนุญาตให้เข้าถึงศูนย์ฯ แบบชั่วคราว พร้อมทั้งจัดทำทะเบียนคุมสำหรับลงบันทึกการเข้า-ออกศูนย์ฯ ที่มีรายละเอียดเพียงพอสำหรับใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลได้
- กำหนดการควบคุมทางกายภาพและมีระบบควบคุมการเข้าถึงตัวอาคารศูนย์คอมพิวเตอร์ และพื้นที่สำคัญต่างๆ ภายในศูนย์คอมพิวเตอร์ ให้เข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตตามสิทธิที่ได้รับมอบหมายเท่านั้น โดยระบบควบคุมควรมีความสามารถอย่างน้อย ดังต่อไปนี้
  (1) รองรับการพิสูจน์ตัวตนของผู้เข้าออกพื้นที่สำคัญภายในศูนย์คอมพิวเตอร์แบบ multi-factor authentication เช่น ใช้ access card door ร่วมกับรหัสผ่านส่วนตัว (PIN) รวมถึงระบบควบคุมการเข้าออกสามารถป้องกันการหมุนเวียนบัตร (pass back) และการแอบลักลอบเข้ามาพร้อมผู้มีสิทธิ (piggy back)
  (2) สามารถบันทึกและจัดเก็บ log files ของการเข้าถึงศูนย์ฯ และพื้นที่สำคัญภายในศูนย์ฯ ได้อย่างถูกต้องแม่นยำ และมีรายละเอียดเพียงพอสำหรับใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ โดยเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(3) มีกระบวนการสอบทาน log files ตลอดจนทะเบียนคุมการเข้า-ออกศูนย์ฯ โดยผู้ที่มีอำนาจอนุมัติอย่างสม่ำเสมอ อย่างน้อยทุก 30 วัน เพื่อติดตามการเข้าถึงศูนย์ฯ ที่ผิดปกติ เช่น ช่วงเวลาหรือความถี่ที่ผิดปกติ หรือการพยายามเข้าถึงโดยบุคคลไม่เหมาะสม

(4) สามารถแจ้งเตือนผู้เกี่ยวข้องเมื่อเกิดเหตุผิดปกติได้อย่างทันการณ์ตลอด 24x7 ชม. เช่น เมื่อพบการพยายามเข้าถึงพื้นที่สำคัญภายในศูนย์ฯ โดยผู้ไม่ได้รับอนุญาต การผ่านเข้า-ออกศูนย์ฯ ทางประตูหนีไฟ การเปิดประตูค้างไว้ เป็นต้น

- ควบคุมการเข้าถึงทางกายภาพพื้นที่รอบนอกศูนย์ฯ ที่เหมาะสม เช่น มีกำแพงหรือรั้วที่มั่นคง มีเจ้าหน้าที่ตรวจสอบการผ่านเข้า-ออกและมีการตรวจสอบยานพาหนะ เป็นต้น อีกทั้งมีการแบ่งแยกพื้นที่ลานจอดรถบุคคลภายนอก (visitor parking area) รวมถึงพื้นที่/ อุปกรณ์ที่ใช้ในการขนส่งสินค้า (loading docks) ออกจากบริเวณศูนย์ ฯ
- ติดตั้งกล้องวงจรปิดบริเวณรอบนอกอาคารศูนย์ฯ ประตูทางเข้าศูนย์ฯ และภายในศูนย์ฯ อย่างทั่วถึง เพื่อใช้เป็นเครื่องมือสำคัญในการติดตามการเข้า-ออก และการกระทำต่างๆ ภายในศูนย์ โดยเก็บบันทึกภาพจากกล้องวงจรปิดไว้เป็นระยะเวลาอย่างน้อย 90 วัน และให้ภาพที่จัดเก็บมีความชัดเจนเพียงพอที่จะใช้ในการพิสูจน์หลักฐาน
- มีเจ้าหน้าที่ดูแลรักษาความปลอดภัยศูนย์ฯ เฝ้าระวังผ่านระบบกล้องวงจรปิด (CCTV) ตลอดเวลา (24x7)
- ห้ามนำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถบันทึกภาพ/เสียงได้เข้ามาภายในพื้นที่สำคัญภายในศูนย์ ฯ เว้นแต่จะได้รับอนุญาตโดยผู้ที่มีอำนาจอนุมัติ
- เครื่องประมวลผลและอุปกรณ์เครือข่ายควรถูกจัดเก็บอยู่ในตู้ rack ที่มีการปิดล็อกอยู่ตลอดเวลา และการเข้าถึงต้องเป็นแบบ dual control

2.4.2 การบริหารจัดการศูนย์คอมพิวเตอร์ (facility management) ควรครอบคลุมอย่างน้อย ดังนี้

- จัดให้ศูนย์คอมพิวเตอร์สำรองแยกออกจากศูนย์คอมพิวเตอร์หลัก ซึ่งควรมีระยะห่างที่เพียงพอและไม่ใช้ระบบสาธารณูปโภคจากแหล่งเดียวกัน เพื่อกระจายความเสี่ยงและป้องกันไม่ให้ได้รับผลกระทบเดียวกัน เช่น ระบบไฟฟ้าหรือระบบโทรคมนาคมขัดข้อง การประท้วงหรือจลาจล ภัยพิบัติทางธรรมชาติ เป็นต้น
- สถานที่ตั้งศูนย์คอมพิวเตอร์ไม่อยู่ในพื้นที่เสี่ยงภัย เช่น ตั้งอยู่ใกล้ปั๊มน้ำมัน ปั๊มแก๊ส ควรกำหนดเป็นปัจจัยหนึ่งของการพิจารณาที่ตั้งของศูนย์ฯ สำหรับกรณีศูนย์คอมพิวเตอร์ในปัจจุบันควรจัดให้มีมาตรการรองรับเหตุฉุกเฉินจากภัยพิบัติต่างๆ
- สถานที่ตั้งศูนย์คอมพิวเตอร์ควรแยกจากอาคารสำนักงาน (stand alone) โดยออกแบบโครงสร้างอาคาร สถานที่และการติดตั้งระบบสาธารณูปโภคที่เหมาะสม
- โครงสร้างตัวอาคารศูนย์คอมพิวเตอร์ ถูกออกแบบให้สามารถรองรับภัยต่าง ๆ ในระดับที่เหมาะสม ปลอดภัยและยากต่อการทำลาย ดังนี้

  (1) การบุกรุก การทุบทำลาย และการรองรับแรงระเบิด

  (2) การป้องกันอัคคีภัย ผนังภายนอกศูนย์คอมพิวเตอร์ สามารถกันไฟได้อย่างน้อย 4 ชั่วโมง ผนังภายในที่กั้นพื้นที่สำคัญสามารถกันไฟได้อย่างน้อย 2 ชั่วโมง และผนังกั้นพื้นที่อื่น ๆ สามารถกันไฟได้อย่างน้อย 1 ชั่วโมง

- ระบบไฟฟ้าสำหรับศูนย์คอมพิวเตอร์ ควรคำนึงถึงเรื่องอย่างน้อย ดังนี้

(1) เส้นทางจ่ายไฟจากภายนอกมายังศูนย์คอมพิวเตอร์ มีจำนวนเส้นทางจ่ายไฟ (feeders) จากสถานีจ่ายไฟของการไฟฟ้า (substation) มายังศูนย์คอมพิวเตอร์ อย่างน้อย 2 เส้นทาง โดยมีการจ่ายไฟพร้อมกันทั้ง 2 เส้นทาง (active/active)

(2) เส้นทางจ่ายไฟภายในศูนย์คอมพิวเตอร์ มีจำนวนเส้นทางจ่ายไฟ ตั้งแต่อุปกรณ์รับไฟฟ้าแรงสูง (high voltage) หม้อแปลงไฟฟ้า (transformer) อุปกรณ์สลับการรับกระแสไฟฟ้า (automatic transfer switch (ATS)) และอุปกรณ์ปรับแรงดันและสำรองไฟฟ้า (uninterrupted power supply (UPS)) ไปจนถึงอุปกรณ์ภายในศูนย์คอมพิวเตอร์ อย่างน้อย 2 เส้นทาง โดยมีการจ่ายไฟพร้อมกันทั้ง 2 เส้นทาง (active/active)

(3) อุปกรณ์คอมพิวเตอร์และอุปกรณ์สาธารณูปโภคภายในศูนย์คอมพิวเตอร์ ควรรองรับกระแสไฟฟ้าจากสองเส้นทาง (dual sources) แต่หากอุปกรณ์ใดไม่สามารถรับไฟจาก 2 เส้นทางได้ ต้องมีการติดตั้งอุปกรณ์ Static Transfer Switch (STS)

(4) ติดตั้งอุปกรณ์ระบบไฟฟ้า เช่น high voltage, transformer, ATS เพื่อรองรับการทำงานของอุปกรณ์สำคัญในศูนย์คอมพิวเตอร์ แบบ 2 ชุด โดยแต่ละชุดมีเส้นทางการเดินกระแสไฟแยกจากกันและตั้งอยู่คนละห้อง (compartmentalization) หากอุปกรณ์ชุดใดชุดหนึ่งหยุดชะงักหรืออยู่ระหว่างการบำรุงรักษา อีกชุดต้องสามารถจ่ายไฟแทนได้อย่างต่อเนื่อง ทั้งนี้แต่ละชุดควรติดตั้งให้ครอบคลุมความเสี่ยงจากกรณีที่เครื่องใดเครื่องหนึ่งในชุดหยุดชะงักหรืออยู่ระหว่างการบำรุงรักษา เครื่องที่เหลือต้องสามารถรองรับการให้บริการได้อย่างต่อเนื่อง (เป็นโครงสร้างแบบ 2(n+1))

(5) ติดตั้งอุปกรณ์ UPS และ generator เพื่อรองรับการทำงานของอุปกรณ์สำคัญในศูนย์คอมพิวเตอร์ แบบ 2 ชุด โดยแต่ละชุดมีเส้นทางการเดินกระแสไฟแยกจากกันและตั้งอยู่คนละห้อง (compartmentalization) หากอุปกรณ์ UPS/generator ชุดใดชุดหนึ่งหยุดชะงักหรืออยู่ระหว่างการบำรุงรักษา อีกชุดต้องสามารถจ่ายไฟแทนได้อย่างต่อเนื่อง ทั้งนี้แต่ละชุดควรติดตั้งให้ครอบคลุมความเสี่ยงจากกรณีที่เครื่องใดเครื่องหนึ่งในชุดหยุดชะงักหรืออยู่ระหว่างการบำรุงรักษา เครื่องที่เหลือต้องสามารถรองรับการให้บริการได้อย่างต่อเนื่อง ทั้งนี้ควรมีการจัดการค่า utilization ที่เหมาะสมเพื่อให้ระบบทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

(6) เมื่อเกิดเหตุการณ์ไฟฟ้าขัดข้อง UPS ควรรองรับการให้บริการอย่างน้อย 15 นาที และเพียงพอรองรับการให้บริการระหว่างที่รอการทำงานของเครื่องปั่นไฟ (generator) (โครงสร้าง UPS และ generator เป็นแบบ 2(n+1))

(7) สำรองน้ำมันไว้ในระดับที่เพียงพอให้อุปกรณ์ generator สามารถจ่ายไฟให้ศูนย์คอมพิวเตอร์ได้อย่างต่อเนื่องเป็นระยะเวลาอย่างน้อย 4 วัน และมีมาตรการในการดำเนินการเพื่อขนส่งน้ำมันมายังศูนย์ฯ เพิ่มเติมเพื่อการให้บริการอย่างต่อเนื่อง

(8) อุปกรณ์ระบบไฟฟ้า เช่น high voltage, transformer, ATS, UPS และ generator ติดตั้งในห้องที่แยกจากห้องจัดเก็บอุปกรณ์อื่น ๆ โดยมีการควบคุมอุณหภูมิ ความชื้น และมีการระบายอากาศที่เหมาะสม

- ระบบทำความเย็นและควบคุมความชื้น ควรคำนึงถึงเรื่องอย่างน้อย ดังนี้

(1) ติดตั้งระบบทำความเย็นและควบคุมความชื้น (ระบบทำความเย็น ฯ) เช่น precision air conditioner, computer room air conditioner (CRAC) เพื่อรองรับพื้นที่สำคัญฯ โดยมีเครื่องสำรองเพื่อรองรับการทำงานในกรณีที่เครื่องหลักชำรุดหรือหยุดชะงักหรือบำรุงรักษา เครื่องที่เหลือต้องสามารถรองรับการให้บริการได้อย่างต่อเนื่อง

(2) ระบบไฟฟ้าและระบบท่อน้ำเย็น (chiller system) ที่รองรับระบบทำความเย็นฯ ควรมีระบบสำรองสามารถรองรับการให้บริการได้อย่างต่อเนื่อง โดยระบบทำความเย็นฯ ควรควบคุมอุณหภูมิให้อยู่

ระหว่าง 20-25 C° และความชื้นที่ 40-55% สำหรับห้องที่ต้องการควบคุมความเย็นและความชื้นให้เหมาะสม เช่น ห้องจัดเก็บเครื่องประมวลผล ห้องจัดเก็บอุปกรณ์เครือข่าย ห้องจัดเก็บสื่อบันทึกข้อมูล เป็นต้น

(3) ติดตั้งระบบตรวจวัดอุณหภูมิและความชื้น โดยติดตั้งให้ครอบคลุมพื้นที่สำคัญฯ และมีการเฝ้าระวังรักษาระดับอุณหภูมิและความชื้นให้อยู่ในระดับที่เหมาะสม

- ระบบป้องกัน/ ระงับอัคคีภัย และระบบตรวจจับน้ำรั่วซึม ควรครอบคลุมอย่างน้อย ดังนี้
  (1) ติดตั้งระบบป้องกัน/ ระงับอัคคีภัย (fire protection and suppression system) ได้แก่ อุปกรณ์ตรวจจับควันและความร้อน (smoke & heat detector) และระบบระงับอัคคีภัย โดยติดตั้งให้ครอบคลุมทุกพื้นที่
  (2) ถังดับเพลิงแบบมือถือ (hand-held fire extinguisher) จะต้องติดตั้งให้ครอบคลุมพื้นที่ภายในศูนย์คอมพิวเตอร์
  (3) ติดตั้งระบบตรวจจับน้ำรั่วซึม (water leak detection system) โดยติดตั้งให้ครอบคลุมพื้นที่สำคัญ
- การบำรุงรักษา ควรครอบคลุมอย่างน้อย ดังนี้
  (1) กำหนดกระบวนการ และเจ้าหน้าที่รับผิดชอบในการตรวจเช็คประจำวัน (Daily Checklist) ของระบบสาธารณูปโภคที่สำคัญในศูนย์คอมพิวเตอร์ ได้แก่ สภาพแวดล้อมของสถานที่จัดเก็บอุปกรณ์และการทำงานของอุปกรณ์ต่างๆ ได้แก่ high voltage, transformer, UPS, generator, ATS, precision air conditioner, chiller และอุปกรณ์สำคัญอื่น ๆ
  (2) จัดให้ผู้ผลิตหรือผู้เชี่ยวชาญทำการตรวจเช็ค บำรุงรักษา (preventive maintenance) และแก้ไขเมื่อเกิดปัญหา (corrective maintenance) ระบบสาธารณูปโภคที่สำคัญ เช่น อุปกรณ์ UPS แบตเตอรี่ของอุปกรณ์ UPS อุปกรณ์ generator chiller system ระบบป้องกัน/ ระงับอัคคีภัย และระบบตรวจจับน้ำรั่วซึม ตามรอบระยะเวลาที่ผู้ผลิตแนะนำ
  (3) ทดสอบการใช้งานระบบสาธารณูปโภคอย่างสม่ำเสมอ โดยในการทดสอบควรพึงระวังไม่ให้การทดสอบนั้นกระทบต่อการดำเนินงานปกติของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
  (4) มีระบบศูนย์กลางในการติดตามสถานะของระบบสาธารณูปโภคที่สำคัญภายในศูนย์ฯ เช่น อุปกรณ์ UPS, แบตเตอรี่ของอุปกรณ์ UPS, อุปกรณ์ generator, chiller system, ระบบป้องกัน/ ระงับอัคคีภัย และระบบตรวจจับน้ำรั่วซึม โดยมีเจ้าหน้าที่เฝ้าระวังระบบตลอด 24 ชม. และมีระบบแจ้งเตือนอัตโนมัติให้ผู้เกี่ยวข้องทราบทันทีเมื่อมีเหตุผิดปกติ

2.4.3 จัดให้มีการประเมินความเสี่ยงของศูนย์คอมพิวเตอร์ ครอบคลุมปัจจัยเสี่ยงอย่างน้อยในเรื่องความปลอดภัยของพื้นที่รอบนอกศูนย์คอมพิวเตอร์ ตัวอาคาร และภายในศูนย์คอมพิวเตอร์ ความพร้อมใช้ของระบบสาธารณูปโภค ประสิทธิภาพระบบป้องกันภัยต่าง ๆ และความเพียงพอของการปฏิบัติงานภายในศูนย์คอมพิวเตอร์ การประเมินความเสี่ยงควรดำเนินการอย่างน้อยเป็นประจำทุกปี และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยมีการบันทึกไว้เป็นลายลักษณ์อักษรและนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายเพื่อพิจารณา

2.5 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

<u>วัตถุประสงค์</u> เพื่อให้มีโครงสร้างของระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย มีการออกแบบระบบเครือข่ายสื่อสารที่เหมาะสมตามมาตรฐานสากล และมีการป้องกันหรือเฝ้าระวังการบุกรุกหรือภัยคุกคามในรูปแบบต่าง ๆ

2.5.1 การออกแบบเครือข่ายสื่อสารโดยคำนึงถึงความมั่นคงปลอดภัย (Security) ความน่าเชื่อถือ (Reliability) และความสามารถในการรองรับการขยายตัว (Scalability) เพื่อให้ระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย และสามารถรองรับการใช้งานเครือข่ายสื่อสารที่เพิ่มสูงขึ้นได้

2.5.2 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารในองค์กร และระหว่างระบบเครือข่ายสื่อสารภายในองค์กรกับระบบเครือข่ายสื่อสารภายนอกองค์กรให้มีความมั่นคงปลอดภัย โดยควรจัดให้มีแนวทางป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหายหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวด

2.5.3 แบ่งแยกเครือข่ายส่วนที่เป็น private network และ public network ออกจากกัน กรณีแบ่งแยกเครือข่ายเป็นหลายชั้น ควรใช้อุปกรณ์รักษาความปลอดภัยเครือข่ายที่ต่างยี่ห้อกันในแต่ละจุดเพื่อลดความเสี่ยงที่อุปกรณ์เครือข่ายอาจมีช่องโหว่เดียวกัน

2.5.4 จัดตั้งโซนเครือข่าย demilitarized zone (DMZ) เพื่อรองรับระบบงานที่ต้องให้บริการ ติดต่อสื่อสารหรือแลกเปลี่ยนข้อมูลกับภายนอก เช่น ระบบงาน Internet/mobile banking ระบบงาน e-mail เป็นต้น โดยไม่จัดวาง Server ที่เป็นระบบฐานข้อมูลสำคัญไว้ในโซนดังกล่าว

2.5.5 จัดแบ่งเครือข่ายอย่างเหมาะสม โดยคำนึงถึง ระดับความสำคัญของระบบงาน ระดับความสำคัญของข้อมูลที่ถูกประมวลผล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่น ๆ หรือจากภายนอกองค์กร และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่างๆ มายังระบบงานที่มีความสำคัญอย่างเข้มงวด

2.5.6 จุดที่มีการแบ่งแยกเครือข่ายที่มีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรอง traffic ที่ส่งผ่านระบบเครือข่าย การเฝ้าระวังการบุกรุก การป้องกันการบุกรุก และการตรวจจับไวรัส หรือมัลแวร์ต่างๆ ที่อาจบุกรุกเข้าสู่เครือข่าย

2.5.7 ใช้อุปกรณ์รักษาความปลอดภัยเครือข่ายเพื่อคัดกรอง traffic ในระดับ application ในจุดที่มีการเชื่อมต่อกับ Internet เช่น การใช้ web application firewall เป็นต้น

2.5.8 ควบคุม และจำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบเครือข่ายได้ รวมถึงมีการระบุตัวตนของอุปกรณ์ที่มาเชื่อมต่อกับระบบเครือข่ายอย่างเหมาะสม

2.5.9 จำกัดให้เฉพาะบุคคลที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงระบบเครือข่าย โดยจำกัดสิทธิในการเข้าถึงระบบเครือข่ายให้อยู่ในส่วนที่มีความจำเป็น และเหมาะสมตามหน้าที่การทำงานเท่านั้น

2.5.10 การเข้าถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเพื่อบริหารจัดการค่าต่างๆ ควรทำผ่านเครือข่ายเฉพาะที่แยกออกจากเครือข่ายปกติ เพื่อลดความเสี่ยงในการเปลี่ยนแปลงอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายโดยบุคคลที่ไม่ได้รับอนุญาต

2.5.11 กรณีมีการเชื่อมต่อมาจากเครือข่ายจากระยะไกล (remote access) เพื่อทำการแก้ไขและ/หรือตั้งค่าพารามิเตอร์ของเครื่องแม่ข่าย อุปกรณ์เครือข่าย หรือโปรแกรมระบบงาน ควรมีการระบุตัวตนและพิสูจน์ตัวตนของบุคคลในลักษณะ multi-factors authentication และกระทำผ่านช่องทางที่มีความปลอดภัย เช่น SSH, VPN หรือ SSL/TLS เป็นต้น

2.5.12 เปลี่ยน default password ของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย รวมทั้งปรับตั้งค่าการรักษาความปลอดภัยให้เป็นไปตามมาตรฐานการตั้งค่าความปลอดภัย (security baseline) ที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด

2.5.13 มีกระบวนการหรือเครื่องมือในการตรวจสอบการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่พิจารณาว่ามีความสำคัญหรือมีความเสี่ยง เช่น การเปลี่ยนแปลง service การเปลี่ยนแปลง port และมีการแจ้งเตือนไปยังผู้ที่ได้รับมอบอำนาจ

2.5.14 จำกัดสิทธิในการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย และการเข้าถึงหน้าจอการบริหารจัดการระบบเครือข่าย (configuration page) เฉพาะผู้ที่รับมอบอำนาจเท่านั้น

2.5.15 ติดตามสถานะความพร้อมใช้งานของระบบเครือข่ายว่ายังอยู่ในระดับ service level agreement (SLA) ที่กำหนด และจัดให้มีกระบวนการจัดการปัญหา และวิธีแก้ปัญหาเมื่อระบบเครือข่ายขัดข้อง

2.5.16 เครือข่ายสื่อสารสำรองควรเป็นผู้ให้บริการคนละรายกับเครือข่ายสื่อสารหลัก

2.5.17 ทดสอบระบบเครือข่ายสื่อสาร และอุปกรณ์เครือข่ายชุดสำรองอย่างสม่ำเสมอ สำหรับเครือข่ายสื่อสารที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจออกแบบในลักษณะพร้อมสำหรับให้บริการอย่างต่อเนื่อง (High Availability – HA) ควรพิจารณาทดสอบในลักษณะเสมือนจริงอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าระบบเครือข่ายสื่อสารสามารถให้บริการได้อย่างต่อเนื่อง รวมทั้งสามารถมั่นใจได้ว่าระบบเครือข่ายสื่อสารสามารถทำงานได้ตามที่ออกแบบไว้ พร้อมรองรับกรณีเกิดเหตุการณ์ไม่ปกติ

2.6 การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

2.6.1 การบริหารจัดการการเปลี่ยนแปลง (change management)

วัตถุประสงค์ เพื่อให้มีการบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศสอดคล้องตามมาตรฐานสากล โดยมีการควบคุมที่รัดกุมปลอดภัยเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างครบถ้วนถูกต้อง

2.6.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร เพื่อควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้มีความรัดกุมเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง การตั้งค่าระบบ การติดตั้ง patch บนระบบที่ให้บริการจริง เป็นต้น

2.6.1.2 กำหนดบทบาทหน้าที่และความรับผิดชอบของผู้บริหารที่ได้รับมอบหมายหรือคณะกรรมการบริหารจัดการการเปลี่ยนแปลง (Change Advisory Board: CAB) ซึ่งควรประกอบด้วยผู้บริหารจากหน่วยงานเทคโนโลยีสารสนเทศ หน่วยงานธุรกิจและหน่วยงานผู้ใช้งานเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อทำหน้าที่ประเมินผลกระทบและพิจารณาเหตุผลความจำเป็นก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลงระบบ ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง โดยครอบคลุมอย่างน้อย ดังนี้

- ผลการประเมินความเสี่ยงและผลกระทบของการเปลี่ยนแปลง ครอบคลุมการเชื่อมต่อระบบงานแบบ End-to-end ตั้งแต่ช่องทางการให้บริการจนถึงระบบประมวลผลและระบบที่เกี่ยวข้องทั้งหมด เช่น ระบบโครงสร้างพื้นฐาน ระบบเครือข่ายสื่อสาร การเชื่อมต่อกับระบบอื่น และผู้ให้บริการภายนอกหรือ บุคคลภายนอก (third party) โดยมีหน่วยงานเจ้าของระบบและผู้มีหน้าที่เกี่ยวข้องทำการประเมินองค์ประกอบที่เกี่ยวข้อง เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้น ไม่กระทบต่อการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ ความพร้อมใช้ของระบบงานและระบบที่เกี่ยวข้อง
- ผลการทดสอบ เพื่อให้มั่นใจว่าระบบได้ผ่านการทดสอบอย่างครบถ้วนเหมาะสมตามมาตรฐานและระเบียบวิธีปฏิบัติของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
- ข้อจำกัดหรือปัญหาต่าง ๆ ที่พบในระหว่างการทดสอบได้รับการแก้ไขอย่างเหมาะสม
- แผนย้อนกลับ (roll back plan) กรณีที่ทำการเปลี่ยนแปลงไม่สำเร็จ เพื่อรองรับปัญหาขัดข้องระหว่างการเปลี่ยนแปลง
- ตารางเวลาการเปลี่ยนแปลงในภาพรวม (change calendar) เพื่อบริหารทรัพยากรและลดความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้น

นอกจากนี้ ผู้บริหารที่ได้รับมอบหมายหรือ CAB ควรมีการติดตามผลหลังการเปลี่ยนแปลงระบบ (post implementation review) เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้นเป็นไปตามวัตถุประสงค์ที่กำหนด

2.6.1.3 ผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลงควรมีการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ผู้มีสิทธิร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น

2.6.1.4 มีหลักเกณฑ์ในการจัดประเภทการเปลี่ยนแปลงระบบตามความเสี่ยงและความสำคัญที่ชัดเจน เช่น การเปลี่ยนแปลงมาตรฐานที่ได้รับอนุมัติเป็นการทั่วไป (standard change) การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการปกติ (normal change) และการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) โดยสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรกำหนดกระบวนการและขั้นตอนในการจัดการการเปลี่ยนแปลงตามแต่ละประเภทอย่างเหมาะสม

2.6.1.5 กรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน ควรมีกระบวนการในการพิจารณาความเสี่ยงและผลกระทบรวมถึงขออนุมัติจากผู้บริหารที่ได้รับมอบหมายให้สามารถตัดสินใจได้กรณีเร่งด่วน โดยภายหลังดำเนินการให้มีการรายงานผู้บริหารที่เกี่ยวข้องและ CAB ได้รับทราบโดยเร็ว

2.6.1.6 คำขอการเปลี่ยนแปลง (change request) ควรได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมจากหน่วยงานเจ้าของระบบ

2.6.1.7 มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้องเพื่อใช้ควบคุมการปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และสามารถใช้ในการติดตามและสอบทานการปฏิบัติงานได้

2.6.1.8 มีการจัดเก็บการเปลี่ยนแปลงของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (version control) เช่น การนำระบบขึ้นใช้งานจริง การตั้งค่าระบบ การติดตั้ง patch บนระบบที่ให้บริการจริง เป็นต้น เพื่อควบคุมความเสี่ยงในการเปลี่ยนแปลงและลดข้อผิดพลาดที่อาจเกิดขึ้น

2.6.1.9 มีการประเมินผลกระทบหรือทำการทดสอบบนระบบที่มีสภาพแวดล้อมใกล้เคียงกับระบบที่ให้บริการจริงก่อนนำไปตั้งค่าบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

2.6.1.10 นำ lesson learned จากผลกระทบของการเปลี่ยนแปลงที่ผ่านมา มาทบทวน ปรับปรุงกระบวนการ เครื่องมือที่ใช้ในการควบคุมการเปลี่ยนแปลงระบบงาน เพื่อให้มีความถูกต้องและไม่ก่อให้เกิดข้อผิดพลาดต่อระบบอย่างมีนัยสำคัญและส่งผลกระทบต่อการให้บริการอย่างต่อเนื่อง

2.6.2 การบริหารจัดการการตั้งค่าระบบ (system configuration management)

<u>วัตถุประสงค์</u> เพื่อให้มีกระบวนการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบที่มีความรัดกุมปลอดภัยและเป็นไปตามมาตรฐาน

2.6.2.1 จัดทำเอกสาร minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษร โดยมีการทบทวน ปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ

2.6.2.2 การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.6.2.3 มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์และระบบงาน (system configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.6.2.4 มีการสอบทานการตั้งค่าจากหน่วยงานที่มีหน้าที่ควบคุมดูแลความปลอดภัยหรือความเสี่ยงด้านเทคโนโลยีอย่างสม่ำเสมอ เพื่อให้สอดคล้องตามมาตรฐานของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

2.6.3 การบริหารจัดการ patch (patch management)

<u>วัตถุประสงค์</u> เพื่อให้มีการบริหารจัดการ patch โดยมีการควบคุมที่รัดกุมปลอดภัย และติดตั้งได้อย่างเหมาะสมทันการณ์

2.6.3.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในกระบวนการบริหารจัดการ patch ที่ครอบคลุม การตรวจสอบความถูกต้องของ patch และการประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch ใหม่จากผู้ผลิตอย่างเหมาะสมทันการณ์

2.6.3.2 มีการจัดเก็บการเปลี่ยนแปลงการติดตั้งของทุกอุปกรณ์และระบบงาน (patch version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.6.3.3 มีกระบวนการทดสอบ patch ที่ออกใหม่ทุกครั้งก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

2.6.3.4 การติดตั้ง patch บนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.6.3.5 มีการทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าสถาบันการเงินและสถาบันการเงินเฉพาะกิจ สามารถทดสอบและติดตั้ง patch ด้านการรักษาความปลอดภัย ได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว

2.6.3.6 กรณีมีเหตุที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการควบคุมอื่นทดแทนเพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

2.6.4 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

<u>วัตถุประสงค์</u> เพื่อให้มีข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัย สามารถใช้ติดตาม ตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

2.6.4.1 มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารที่สำคัญด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดที่ครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด

- บันทึกร่องรอยกิจกรรมการทำธุรกรรม (transaction log)
- บันทึกการเข้าถึง (access log)
- บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยต้องครอบคลุม
  - การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูล (update/ insert/ delete) ในตารางที่สำคัญ
  - การเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ
  - การเข้าถึง object ที่สำคัญของระบบ
  - การเปลี่ยนแปลงแก้ไขบัญชีและสิทธิของผู้ใช้งาน

2.6.4.2 มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารให้ตรงกับเครื่องแม่ข่าย Network Time Protocol : NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งเครื่องแม่ข่าย NTP ต้องรับสัญญาณนาฬิกาจากแหล่งที่มีความน่าเชื่อถือ

2.6.4.3 ข้อมูลการบันทึกเหตุการณ์ของอุปกรณ์สำคัญควรจัดเก็บไว้ที่เครื่องแม่ข่ายที่แยกเฉพาะ อย่างน้อยครอบคลุม access log และ activity log โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย

2.6.4.4 มีการสอบทานบันทึกการเข้าถึง (access Log) และบันทึกการดำเนินงาน (activity log) ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิสูงอย่างสม่ำเสมอ เช่น system administrator หรือ system operator เป็นต้น เพื่อให้มั่นใจได้ว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย

2.6.5 การบริหารจัดการขีดความสามารถของระบบ (capacity management)

วัตถุประสงค์ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับต่อการให้บริการหรือดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

2.6.5.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติเรื่องการบริหารจัดการขีดความสามารถของระบบ เพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึง ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ

2.6.5.2 มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศสอดคล้องกับการประมาณการ (Forecasting) ปริมาณธุรกรรมและปริมาณลูกค้าในภาวะปกติและภาวะวิกฤตที่อาจจะเกิดขึ้น ทั้งในปัจจุบันและอนาคต เพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง

2.6.5.3 มีกระบวนการหรือแนวทางในการขยายขีดความสามารถของระบบและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ให้ทันต่อความต้องการใช้งาน เช่น ออกแบบให้สามารถรองรับการขยายอุปกรณ์แบบเร่งด่วน (Capacity on Demand) เป็นต้น

2.6.5.4 มีกระบวนการหรือแนวทางในการรองรับการพร้อมทำงานโดยอัตโนมัติเมื่อเกิดเหตุฉุกเฉิน เช่น การจัดเตรียมเครื่อง อุปกรณ์ ระบบ และข้อมูลสำรอง ในลักษณะ high availability เป็นต้น

2.6.5.5 มีกระบวนการหรือเครื่องมือในการติดตามประสิทธิภาพและความเพียงพอของการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของระบบ เช่น ระบบการชำระเงิน ระบบที่ให้บริการทางการเงินอิเล็กทรอนิกส์ เป็นต้น เพื่อบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงที และสามารถตอบสนองความต้องการในการดำเนินงานทางธุรกิจอย่างต่อเนื่อง

2.6.5.6 มีการกำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (threshold และ trigger) ในระดับต่าง ๆ เช่น ตัวชี้วัดด้านความพร้อมใช้ (Availability) ขีดความสามารถ (Capacity) ประสิทธิภาพการทำงาน (Performance) ของระบบและโครงสร้างพื้นฐาด้านเทคโนโลยีสารสนเทศ เป็นต้น โดยครอบคลุมการเชื่อมต่อตั้งแต่ช่องทางการให้บริการจนถึงระบบประมวลผล รวมถึงผู้ให้บริการภายนอก (End-to-end) เพื่อให้มีการแจ้งเตือนผู้เกี่ยวข้องอย่างทันท่วงที และสามารถวิเคราะห์ปัญหาและแนวทางการรับมือที่เหมาะสม รวมถึงการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง

2.6.5.7 กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศหรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือ ตัดการเชื่อมต่อกับผู้ให้บริการหรือบุคคลภายนอกที่มีผลกระทบต่อระบบ เช่น สถาบันการเงินผู้รับโอนเงิน ผู้ให้บริการ Bill Payment เป็นต้น

2.6.5.8 จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อม

และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

2.6.6 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring)

<u>วัตถุประสงค์</u> เพื่อให้สามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบ รวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง

2.6.6.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

2.6.6.2 มีหน่วยงานที่ทำหน้าที่ในการเฝ้าระวัง ติดตาม วิเคราะห์ ประสานงาน อย่างชัดเจน เพื่อเป็นศูนย์กลางในการจัดการเหตุการณ์ผิดปกติได้อย่างต่อเนื่องและทันท่วงที

2.6.6.3 กำหนดกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของระบบที่สำคัญอย่างทันท่วงที ครอบคลุมระบบงานและระบบเครือข่ายสื่อสารทั้งในเชิง physical และ logical เช่น ศูนย์คอมพิวเตอร์ ระบบการชำระเงิน และระบบที่ให้บริการทางการเงินอิเล็กทรอนิกส์ เป็นต้น เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม

2.6.6.4 มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูลภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์

2.6.6.5 กำหนดให้มีผู้รับผิดชอบในการประสานงานแลกเปลี่ยนข้อมูลภัยคุกคาม ระหว่างสถาบันการเงินและสถาบันการเงินเฉพาะกิจ กับหน่วยงานที่เกี่ยวข้อง รวมทั้งมีกระบวนการและช่องทางในการรายงาน แลกเปลี่ยน ติดตาม เพื่อป้องกันรับมือและแก้ไขภัยคุกคาม

2.6.6.6 ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรจัดให้มีการรายงานผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง รวมทั้งมีการรายงานหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมทั้งจัดให้มีกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) โดยผู้ที่มีความเชี่ยวชาญ เพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

2.6.6.7 จัดให้มีการนำสิ่งที่ได้เรียนรู้ (Lessons learned) จากการถูกโจมตีหรือจากเหตุการณ์ผิดปกติที่เกิดขึ้นทั้งภายในและภายนอกสถาบันการเงินและสถาบันการเงินเฉพาะกิจ มาปรับปรุงแผนรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติ เพื่อเพิ่มประสิทธิภาพการป้องกันและรับมือเหตุการณ์ผิดปกติให้มากขึ้น

2.6.7 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration test)

<u>วัตถุประสงค์</u> เพื่อให้ได้รับทราบถึงช่องโหว่ด้านการรักษาความปลอดภัยของระบบ และสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันการณ์

2.6.7.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ <u>การบริหารจัดการช่องโหว่ (vulnerability management)</u>

2.6.7.2 มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment) โดยสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบบงานสำคัญต้องจัดทำอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.6.7.3 มีการรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

<u>การทดสอบเจาะระบบ (penetration test)</u>

2.6.7.4 มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระ ครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (Internet facing) อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.6.7.5 มีการรายงานผลการทดสอบเจาะระบบไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

2.6.7.6 มีกระบวนการรวบรวมและวิเคราะห์ช่องโหว่ทางด้านเทคนิคที่ตรวจพบ เพื่อกำหนดเป็นมาตรการรักษาความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาในอนาคต

2.6.7.7 นอกจากนี้ อาจพิจารณาค้นหาช่องโหว่ของระบบงานในลักษณะ Bug Bountry program เพื่อให้มั่นใจว่าช่องโหว่ใหม่ ๆ จะสามารถถูกค้นพบและปิดได้อย่างรวดเร็ว

2.6.8 การสำรองข้อมูล (data backup)

<u>วัตถุประสงค์</u> เพื่อให้มั่นใจว่ามีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหายจนไม่สามารถใช้งานได้ตามปกติ

2.6.8.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการสำรองข้อมูล เพื่อให้มีข้อมูลสำรองพร้อมใช้และมีความปลอดภัย โดยควรครอบคลุมอย่างน้อย

- วิธีการ เทคโนโลยีและรอบระยะเวลาที่ใช้ในการสำรองข้อมูล โดยควรสอดคล้องกับเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point objective : RPO) ที่กำหนด
- รอบระยะเวลาและวิธีการทดสอบความพร้อมใช้ของข้อมูลสำรอง

2.6.8.2 มีกระบวนการสำรองทั้งระบบ (full backup) ทุกครั้งภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการและระบบงาน เพื่อให้ระบบสำรองมีความเป็นปัจจุบัน

2.6.8.3 มีระบบหรือทะเบียนควบคุมการจัดเก็บและเรียกใช้งานสื่อบันทึกข้อมูลตามประเภทของสื่อที่จัดเก็บ โดยระบุข้อมูล ชื่อ วันที่ และช่วงเวลาที่จัดเก็บ ที่สามารถติดตามตรวจสอบได้

2.6.8.4 มีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยมีการรักษาสภาพแวดล้อมและการควบคุมความปลอดภัยในการเข้าถึงข้อมูลที่จัดเก็บไว้ เทียบเคียงกับศูนย์คอมพิวเตอร์หลัก

2.6.8.5 จัดให้มีการสอบทานการสำรองข้อมูลและทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งานและปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

2.6.9 การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

<u>วัตถุประสงค์</u> เพื่อให้อุปกรณ์ที่ใช้ปฏิบัติงานมีความปลอดภัยและไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต

2.6.9.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงานเป็นลายลักษณ์อักษร ทั้งอุปกรณ์ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และอุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD) เช่น personal computer, notebook, tablet, smartphone, removable media เป็นต้น เพื่อให้

สถาบันการเงินและสถาบันการเงินเฉพาะกิจ มีแนวทางที่ใช้ในการควบคุมความเสี่ยงจากการใช้งานอุปกรณ์ดังกล่าว

2.6.9.2 กำหนด Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงานทั้งอุปกรณ์ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และอุปกรณ์ส่วนตัว เพื่อป้องกันความเสี่ยงที่อุปกรณ์เหล่านั้นอาจเป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญตามระดับความเสี่ยงที่เหมาะสม โดยอย่างน้อยครอบคลุม ดังนี้

- ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ (personal computer, notebook) โดยมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้ผู้ใช้งานสามารถติดตั้งโปรแกรมอื่น ๆ นอกเหนือจากสถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนดและจัดหาให้
- ติดตั้งโปรแกรมรักษาความปลอดภัย เช่น anti-Virus/ anti-malware, Host-based Intrusion Prevention System (HIPS) เป็นต้น บนเครื่องคอมพิวเตอร์ เครื่องแม่ข่าย (server) รวมถึงเครื่องจำลองเสมือน (virtual machine) โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (malware) ให้เป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ
- ควบคุมไม่ให้มีการจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แต่หากมีความจำเป็นต้องจัดเก็บ ต้องมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น มีการเข้ารหัส เป็นต้น
- มีกระบวนการหรือเครื่องมือในการตรวจจับ (detect) คัดกรอง (filter) สกัดกั้น (block) เพื่อป้องกันข้อมูลสำคัญรั่วไหล (Data Leakage Prevention : DLP)
- มีการจัดการควบคุม ติดตาม การใช้อุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ และบริการด้านเทคโนโลยีสารสนเทศที่ไม่ได้รับอนุญาตและถูกจัดหาให้โดยหน่วยงานด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (shadow IT)
- จำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานเท่านั้น
- มีการควบคุมการใช่ฟงกชัน Print Screen และ มีการกำหนดระยะเวลาที่เหมาะสมในการบังคับระบบให่มีการ Lock หน่าจอการทำงานเมื่อไมมีการเคลื่อนไหว
- การควบคุมการใช้งานอินเตอร์เน็ต โดยควรมีเครื่องมือในการควบคุมให้อุปกรณ์ที่สามารถเชื่อมต่ออินเตอร์เน็ตเข้าถึงเฉพาะเว็บไซต์ที่ได้รับอนุญาตเท่านั้น รวมถึงมีการจำกัดการดาวน์โหลดหรืออัพโหลดข้อมูลจากอินเตอร์เน็ต
- การควบคุมการใช้สื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการอนุญาตให้ใช้งาน Universal Serial Bus (USB) หรือ external harddisk เป็นต้น
- การควบคุมการใช้ Email เช่น กำหนดแนวทางการใช้งาน Email เป็นต้น

2.6.9.3 มีกระบวนการบริหารจัดการอุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD) ตั้งแต่การลงทะเบียน การต่ออายุ และการยกเลิกการใช้งาน BYOD อย่างน้อยครอบคลุมดังนี้

- หลักเกณฑ์การอนุญาตให้ใช้งาน BYOD
- การควบคุมการใช้ BYOD ในการเข้าถึงระบบเครือข่ายสื่อสาร ระบบงานและข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
- มีกระบวนการตรวจสอบ วิเคราะห์ และติดตามความเสี่ยงของอุปกรณ์ที่นำมาใช้งานในสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
- กำหนดรหัสผ่านเพื่อใช้ในการล็อคหรือปลดล็อคในการเข้าถึงอุปกรณ์ส่วนตัว

- กรณีเครื่องคอมพิวเตอร์ (personal computer, notebook) ต้องติดตั้ง anti-virus/ anti-malware หรือโปรแกรมตามที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด
- ไม่อนุญาตให้อุปกรณ์โทรศัพท์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jailbroken) ลงทะเบียนใช้งาน BYOD
- ใช้วิธีการพิสูจน์ตัวตนอุปกรณ์ที่เชื่อถือได้ขององค์กร เช่น trusted root certification authorities, digital certificate เป็นต้น

2.6.9.4 กำหนดมาตรฐานและระเบียบปฏิบัติในการบริหารจัดการระบบเสมือนจริง (Virtualisation) โดยครอบคลุมการควบคุมสิทธิการเข้าถึง และการรักษาความปลอดภัยของระบบ ตลอดจนการควบคุมข้อมูลที่เกิดจากระบบเสมือนจริง เช่น ข้อมูลระบบปฏิบัติการ (VM image) และข้อมูลสำรองระบบ (VM snapshot) เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบโดยผู้ไม่มีสิทธิหรือไม่รับอนุญาต

2.7 การจัดหาและการพัฒนาระบบ (system acquisition and development)

<u>วัตถุประสงค์</u> เพื่อให้มั่นใจได้ว่ากระบวนการจัดหาและการพัฒนาระบบ มีการควบคุมการรักษาความมั่นคงปลอดภัยอย่างรัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล

2.7.1 การจัดหาระบบ (system acquisition) ควรคำนึงถึงเรื่องอย่างน้อย ดังนี้

- มีหลักเกณฑ์การพิจารณาคัดเลือกระบบและผู้ให้บริการ เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ซึ่งควรครอบคลุมอย่างน้อย ดังนี้
  (1) รายละเอียดทั่วไป เช่น หมายเลขอ้างอิงของซอฟต์แวร์ (software license) ฟังก์ชันการทำงาน ประสิทธิภาพของระบบ เป็นต้น
  (2) ความมั่นคงปลอดภัยของระบบ
  (3) ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค
  (4) การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate)
  (5) การสนับสนุนและการบำรุงรักษาระบบ
  (6) สัญญาและข้อตกลงการรับฝากทรัพย์สิน (escrow agreement) ตามระดับความสำคัญของระบบ โดยในสัญญาระบุสิทธิการเข้าถึง source code ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ รวมทั้งการเลือกเปลี่ยนซอฟต์แวร์ ในกรณีที่ผู้ให้บริการไม่สามารถให้บริการได้ตามข้อตกลง
  (7) ความน่าเชื่อถือของระบบและผู้ให้บริการ
  (8) ผลการจัดทำ proof of concept ในกรณีที่เป็นระบบสำคัญ
- สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบและพัฒนาระบบ
- สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการตรวจสอบและส่งมอบระบบเทคโนโลยีสารสนเทศ
- กรณีสถาบันการเงินและสถาบันการเงินเฉพาะกิจ มีการใช้ซอฟต์แวร์สำเร็จรูป (commercial off-the-shelf) ควรประเมินความเสี่ยงและกำหนดการควบคุมความเสี่ยง เพื่อลดหรือบรรเทาผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงก่อนนำไปใช้งาน

2.7.2 การพัฒนาระบบเทคโนโลยีสารสนเทศ (system development) ควรครอบคลุมอย่างน้อย ดังนี้

- กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและ พัฒนาระบบ อย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงการรักษาความมั่นคงปลอดภัย ครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง
- มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอ เพื่อเสริมสร้างทักษะในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย (secure software development)
- กำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงานธุรกิจ (business requirement) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด (security requirement) และ sign off ก่อนเริ่มออกแบบระบบ

<u>การออกแบบระบบ</u>

- จัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) รวมทั้งจัดให้มีการสอบทานความถูกต้องครบถ้วนและ sign off จากผู้ที่เกี่ยวข้องก่อนเริ่มพัฒนาระบบ อย่างน้อยครอบคุลมด้านต่าง ๆ ดังนี้
  (1) ด้านความพร้อมใช้ (availability) เช่น การออกแบบให้มีระบบทดแทน high availability หรือ redundancy รวมถึงมีระบบสำรอง (DR strategy) เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่องและลดความเสี่ยงที่จุดใดจุดหนึ่งทำให้ระบบเกิดปัญหาหรือล้มเหลวทั้งหมด (single point of failure)
  (2) ด้านความยืดหยุ่นและคล่องตัว (flexibility and agility) เช่น ความสามารถในการลดหรือเพิ่มทรัพยากรของระบบได้ง่าย (scalability) รวมถึงให้ระบบมีความเป็นอิสระต่อกัน (Independent) หรือ มีการแบ่งแยกขอบเขตสภาพแวดล้อมการทำงานของระบบออกจากกัน (Fault Isolation) เพื่อลดความเสี่ยงจากการผูกติดหรือพึ่งพาระบบใดระบบหนึ่งอย่างมาก (tightly coupled) และลดความเสี่ยงที่ระบบงานถูกออกแบบมาให้มีความซับซ้อนยากต่อการเปลี่ยนแปลงแก้ไข (complexity) รวมถึงความเสี่ยงจากปัญหาคอขวด (bottle neck) หรือการกระจุกตัวของการใช้ทรัพยากรของระบบงาน(concentration)
  (3) ด้านการรักษาความมั่นคงปลอดภัย ตามนโยบายหรือมาตรฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด (security specification)
- จัดทำแผนภาพสถาปัตยกรรมด้านเทคโนโลยีสารสนเทศของระบบ (IT architecture diagram) ให้ครอบคลุมด้าน application, data, IT infrastructure และ security รวมทั้งความสัมพันธ์ของบริการ ระบบงาน และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้สามารถเชื่อมโยงระหว่างระบบ และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศในภาพรวมขององค์กรกับแผนการดำเนินธุรกิจ และสามารถจัดการความพร้อมใช้ของระบบและอุปกรณ์ที่เกี่ยวข้องได้อย่างเหมาะสม
- จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่าง ๆ ด้านประสิทธิภาพ ตามความต้องการของหน่วยงานธุรกิจ (business requirement) รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด เพื่อเป็นแนวทางการพัฒนาระบบและสอบทานผลการทดสอบก่อนที่จะออกใช้งานจริง (exit criteria)

<u>การพัฒนาระบบ</u>

- มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) การทดสอบ (testing) และระบบที่ให้บริการจริง (production) ออกจากกัน เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง

- มีการควบคุมเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้มีความปลอดภัยเพียงพอตามระดับความเสี่ยงเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- มีกระบวนการหรือเครื่องมือในการควบคุมเวอร์ชั่นของคำสั่งในการเขียนโปรแกรม (source code version control)
- มีการควบคุมการเข้าถึง source code โดยจำกัดสิทธิ์การเข้าถึงเฉพาะผู้ที่ได้รับอนุญาต
- มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปลโปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต

<u>การทดสอบระบบ</u>

- บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบควรเป็นไปตามหลักการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ควรแยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น
- มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงของการเปลี่ยนแปลงบนระบบที่ให้บริการจริง
- การทดสอบระบบที่ได้รับการพัฒนาหรือเปลี่ยนแปลง ควรครอบคลุม อย่างน้อย ดังนี้

  (1) unit test

  (2) system and integration test

  (3) user acceptance test

  (4) security test ตาม security specification

  ทั้งนี้สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีกระบวนการและเอกสารการ sign off ผลการทดสอบระบบจากฝ่ายงานที่เกี่ยวข้อง ที่ผ่านตาม exit criteria อย่างครบถ้วน ก่อนนำระบบขึ้นใช้งานจริง
- มีการกำหนด test scenario ที่มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริงแบบ End-to-end ได้อย่างครอบคลุม และมีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอ รวมถึงการนำ lesson learned จากปัญหาและเหตุการณ์ระบบขัดข้องที่เคยเกิดขึ้นเป็นข้อมูลในการกำหนด test scenario
- การพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการ การทำธุรกรรมทางอิเล็กทรอนิกส์หรือระบบที่มีการเชื่อมโยงกับระบบอื่นจำนวนมาก สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการทดสอบประสิทธิภาพ (performance test) เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการใช้งานจำนวนมาก
- มีการทดสอบระบบรักษาความปลอดภัยควรครอบคลุมการประเมินช่องโหว่ (vulnerability assessment) ของระบบงาน และกรณีเป็นระบบที่เชื่อมต่อกับเครือข่ายภายนอก ควรมีการทำทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญภายนอกเพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริง
- มีการสอบทานคำสั่งในการเขียนโปรแกรม (sourcecode review) อย่างเป็นอิสระ ทุกครั้งที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจ มีการพัฒนาหรือเปลี่ยนแปลงระบบในส่วนที่เป็นการทำธุรกรรมสำคัญเพื่อระบุช่องโหว่ด้านความมั่นคงปลอดภัย

- มีแนวทางการควบคุมการรักษาความปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ เช่น data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูลสำคัญดังกล่าว
- มีกระบวนการในการจัดการข้อผิดพลาดหรือข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ เพื่อพิจารณาแนวทางปรับปรุงหรือลดความเสี่ยงหรือผลกระทบของข้อผิดพลาดหรือข้อบกพร่องที่มีต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ
- มีการจัดทำคู่มือและอบรมผู้ใช้งานระบบ เพื่อให้มีความเข้าใจฟังก์ชันการทำงานและมีการใช้งานระบบอย่างปลอดภัย รวมถึงจัดให้มีคู่มือการดูแลระบบและอบรมผู้ดูแลระบบ เพื่อสามารถตรวจสอบและจัดการแก้ไขปัญหาได้
- หลังจากนำระบบขึ้นใช้งานจริงสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรพิจารณาจัดให้มีการทดสอบจริงในวงจำกัด (pilot test) สำหรับฟังก์ชันการทำงานที่สำคัญ รวมทั้งจัดให้มีการติดตามการใช้งานระบบหลังจากให้บริการจริงอย่างใกล้ชิดตามระยะเวลาที่เหมาะสม เพื่อให้มั่นใจต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ

  <u>การนำระบบขึ้นใช้งานจริง (system deployment)</u>
- การนำระบบขึ้นใช้งานจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่กำหนดเพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน
- มีการจัดเก็บการเปลี่ยนแปลง (version control) ของระบบงานขึ้นใช้งานจริงทั้งหมด โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ
- ระบบงานสำรองควรปรับปรุงให้มีความเป็นปัจจุบัน เพื่อให้มีความพร้อมใช้งานเมื่อเกิดเหตุฉุกเฉิน
- การใช้หรือการให้บริการผ่านช่องทาง API (Application Programming Interface) อาจก่อให้เกิดความเสี่ยงด้าน IT เพิ่มมากขึ้น เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลเกินความจำเป็น บริการหยุดชะงักไม่สามารถให้บริการได้อย่างต่อเนื่อง เป็นต้น ดังนั้น ควรมีการกำหนดแนวทางควบคุมที่เหมาะสมเพียงพอต่อระดับความเสี่ยงของ API นั้น ๆ ซึ่งสถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถใช้แนวปฏิบัติ เรื่อง การใช้เทคโนโลยี Application Programming Interface (API) ในการให้บริการทางการเงิน เป็นแนวทางในการกำกับดูแล API ให้มีการบริหารจัดการความเสี่ยงที่เกี่ยวข้องอย่างรัดกุม และมีการรักษาความมั่นคงปลอดภัยสอดคล้องเป็นไปตามมาตรฐานสากล

2.8 การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem management)

2.8.1 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT incident management)

<u>วัตถุประสงค์</u> เพื่อให้มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ให้สามารถจัดการแก้ไขปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

2.8.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ครอบคลุมตั้งแต่กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดำเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ

2.8.1.2 กำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ (escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้องหรือคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจได้รับทราบ ให้สอดคล้องกับระดับความรุนแรงของเหตุการณ์ผิดปกติ

2.8.1.3 การจัดระดับความรุนแรงของปัญหา ควรพิจารณาอย่างน้อยให้ครอบคลุม ผลกระทบต่อการให้บริการ ผลกระทบต่อผู้ใช้งาน โดยกรอบระยะเวลาในการแก้ไขเหตุการณ์ผิดปกติควรคำนึงถึงเป้าหมายระยะเวลาในการกู้คืนระบบ (recovery time objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD) เพื่อที่จะสามารถตัดสินใจใช้แผนสำรองอย่างเหมาะสมทันการณ์

2.8.1.4 จัดให้มีศูนย์รับแจ้งเหตุการณ์ผิดปกติ โดยทำหน้าที่ในการบันทึกและแก้ไขในเบื้องต้น หรือส่งต่อเหตุการณ์ผิดปกติ ไปยังหน่วยงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

2.8.1.5 จัดทำแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan) ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยอย่างน้อยแผนควรระบุกระบวนการรับมือและช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก และมีแนวทางการตรวจสอบวิเคราะห์หาสาเหตุ และประเมินผลกระทบ รวมถึงจัดให้มีการซักซ้อมและทดสอบแผนรับมือเหตุการณ์ผิดปกติทั้งในระดับหน่วยงานและระดับองค์กรอย่างน้อยปีละ 1 ครั้ง โดยเฉพาะระบบงานสำคัญ

2.8.1.6 จัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย โดยครอบคลุม วัน เวลา เหตุการณ์ ความเสียหาย การวิเคราะห์สาเหตุที่แท้จริง การวิเคราะห์ผลกระทบ การแก้ไขปัญหาและแนวทางหรือแผนดำเนินการเพื่อป้องกันเหตุการณ์ผิดปกติในอนาคต และในกรณีที่เป็นความเสียหายส่งผลกระทบต่อชื่อเสียงและการให้บริการหรือดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ อย่างมีนัยสำคัญ ให้รายงานต่อคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ทราบด้วย

2.8.1.7 ในกรณีที่เกิดปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียง ที่มีนัยสำคัญและเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุด หรือกรณีเทคโนโลยีสารสนเทศที่มีนัยสำคัญถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ รวมทั้งกรณีปัญหาหรือเหตุขัดข้องของระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อการให้บริการผ่านช่องทางให้บริการสำคัญที่ประชาชนใช้บริการจำนวนมากตามที่ ธปท. กำหนด ให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจ รายงานปัญหาหรือเหตุการณ์ดังกล่าวมายัง ธปท. โดยเร็วเมื่อทราบหรือรับรู้ปัญหาหรือเหตุการณ์นั้น ตามรูปแบบและช่องทางที่ ธปท. กำหนด และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

2.8.1.8 นำเหตุการณ์ที่เกิดขึ้นหรือ lesson learned จากเหตุการณ์ผิดปกติที่ผ่านมา เพื่อทบทวนหรือปรับปรุงกระบวนการการจัดการเหตุการณ์ผิดปกติ เพื่อป้องกันการปัญหาเดิมซ้ำ

2.8.1.9 มีกระบวนการบริหารภาวะวิกฤต (crisis management) เพื่อรองรับกรณีเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศเพิ่มระดับความรุนแรงหรือมีความยืดเยื้อ อย่างน้อย ดังนี้

- สถาบันการเงินและสถาบันการเงินเฉพาะกิจ จัดให้มีคณะกรรมการบริหารภาวะวิกฤติ (crisis management committee) โดยประกอบด้วยผู้บริหารระดับสูง (C-level) จากฝ่ายงานต่าง ๆ เพื่อให้สามารถพิจารณาประเมินสถานการณ์ได้อย่างครอบคลุม และตัดสินใจแก้ไขสถานการณ์ได้อย่างรวดเร็วทันการณ์ บรรเทาผลกระทบหรือความเสียหายและสามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง ตลอดจนกำกับดูแลการดำเนินการต่าง ๆ จนสถานการณ์กลับสู่ภาวะปกติ
- จัดตั้งศูนย์บัญชาการ กำหนดขั้นตอนการสั่งการและการตัดสินใจที่ชัดเจน

- กำหนดทีมงานรับผิดชอบดำเนินการด้านต่าง ๆ ได้แก่ ด้านสถานที่ ด้านบุคลากร ด้านเทคโนโลยีสารสนเทศ ด้านความปลอดภัย ด้านสื่อสารองค์กร เป็นต้น ในการประเมินลักษณะและผลกระทบของความเสียหายที่เกิดขึ้น พิจารณาแนวทางบรรเทาผลกระทบและแนวทางรองรับธุรกิจอย่างต่อเนื่อง ซึ่งครอบคลุมการกู้คืนระบบ เพื่อนำเสนอต่อคณะกรรมการบริหารภาวะวิกฤต ในการพิจารณาตัดสินใจดำเนินการใช้แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง
- จัดทำแผนการสื่อสารภาวะวิกฤต (crisis communication plan) ครอบคลุมการสื่อสารไปยังผู้ที่เกี่ยวข้อง (call tree) รวมทั้งสมาชิก ผู้ใช้บริการของระบบหรือลูกค้าที่ได้รับผลกระทบโดยควรกำหนด ประเภท ระยะเวลาของเหตุการณ์ หน่วยงานที่รับผิดชอบ และช่องทางการสื่อสารอย่างชัดเจนทันการณ์ พร้อมทั้งมีแนวทางหรือขั้นตอนในการดูแลลูกค้าที่มีความจำเป็นเร่งด่วน และมีแผนและมาตรการรองรับและเยียวยาแก่ลูกค้าที่ได้รับผลกระทบ

2.8.1.10 กำหนดกระบวนการแจ้ง สื่อสารลูกค้า เมื่อเกิดเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศครอบคลุมการแจ้งผลกระทบการให้บริการ การจัดการสื่อสาธารณะ ช่องทางการสื่อสาร และกำหนดผู้รับผิดชอบการสื่อสารไปยังลูกค้า รวมถึงรายงานความคืบหน้าการแก้ไขเหตุการณ์ผิดปกติให้ลูกค้าทราบ และให้คำแนะนำการใช้บริการในทางช่องทางอื่น ระหว่างที่บริการที่เกิดเหตุยังไม่สามารถกลับมาใช้งานได้ปกติ เพื่อให้ลูกค้าได้มีทางเลือกในการจัดการธุรกรรมตนเอง

2.8.2 การบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ (IT problem management)

<u>วัตถุประสงค์</u> เพื่อให้มีกระบวนการติดตามหาสาเหตุที่แท้จริง ให้มีแนวทางป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

2.8.2.1 มีมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ เพื่อให้มีการนำเหตุการณ์ผิดปกติที่ยังไม่ทราบสาเหตุที่แท้จริง (unknown root cause) เหตุการณ์ผิดปกติที่เกิดขึ้นซ้ำ (repeated incident) มาวิเคราะห์และพิจารณาแนวทางแก้ไขปัญหาจากสาเหตุที่แท้จริง (root cause)

2.8.2.2 มีกระบวนการหรือเครื่องมือในการบันทึกปัญหา หลักเกณฑ์ในการจัดประเภทปัญหา การจัดลำดับความสำคัญ วิเคราะห์ และจัดให้มีการติดตามการแก้ไขปัญหาเพื่อให้ปัญหาได้รับการแก้ไข

2.8.2.3 มีกระบวนการหรือเครื่องมือบันทึกปัญหาที่เคยเกิดขึ้น เพื่อให้เป็นแหล่งข้อมูลความรู้ให้สามารถสืบค้นเหตุการณ์ปัญหาและแนวทางการแก้ไขปัญหาได้ในภายหลังอย่างรวดเร็วและมีประสิทธิภาพ

2.9 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

<u>วัตถุประสงค์</u> เพื่อให้มีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจดำเนินการต่อไปได้อย่างต่อเนื่องและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้

<u>นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ</u>

2.9.1 กำหนดนโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยคำนึงความสอดคล้องกับนโยบายการบริหารความต่อเนื่องของธุรกิจและนโยบายการบริหารความเสี่ยงของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

2.9.2 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนฯ เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการให้บริการหรือดำเนินธุรกิจหรือทรัพยากรหรือโครงสร้างระบบ IT เป็นต้น

2.9.3 นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมอย่างน้อย

- บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ ผู้บริหารระดับสูง และผู้เกี่ยวข้อง
- การประเมินความเสี่ยง
- การวิเคราะห์ผลกระทบทางธุรกิจและกำหนดเป้าหมายในการกู้คืนระบบเทคโนโลยีสารสนเทศ
- การจัดระดับความสำคัญของระบบงาน
- การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

<u>การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ</u>

2.9.4 มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยต้องได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย โดยจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.9.5 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น

2.9.6 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงลักษณะการให้บริการหรือดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงที่เกี่ยวข้องในการให้บริการหรือดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการให้บริการหรือดำเนินธุรกิจ (interdependency risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และความเสี่ยงที่มีผลกระทบต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ผู้ใช้บริการ ผู้มีส่วนได้เสียและระบบสถาบันการเงิน (systemic risk)

2.9.7 กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมการดำเนินการ ดังนี้

- การประเมินความเสี่ยง (risk analysis) เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจ สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการอย่างเหมาะสมเพียงพอดังนี้
  (1) ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบเทคโนโลยีสารสนเทศหยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ เป็นต้น
  (2) ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้น พร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง
  (3) จัดทำแผนในการจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการและจัดเตรียมทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่มีผลต่อการให้บริการหรือดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ รวมถึงผลกระทบจากการหยุดชะงักและความเชื่อมโยงของการให้บริการหรือดำเนินธุรกิจกับระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการดังนี้

(1) ระบุระบบเทคโนโลยีสารสนเทศทั้งหมดของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และทรัพยากรที่มีการเชื่อมโยงพึ่งพาระหว่างกัน (dependency)

(2) วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศ โดยคำนึงถึงเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD)

(3) กำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (recovery time objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point objective : RPO)

- การจัดลำดับความสำคัญของระบบงาน โดยคำนึงถึงทรัพยากร ระยะเวลาในการกู้คืนระบบ เป้าหมายของระบบงานและข้อมูลที่ควรกู้ได้ภายหลังเกิดการหยุดชะงัก และทรัพยากรทางเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็นต้องใช้ในการกู้คืนระบบ ทั้งนี้สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรพิจารณาให้ระบบ Core Banking ระบบ ATM ระบบที่รองรับการให้บริการผ่านสาขา ระบบ Internet Banking และ Mobile Banking หรือระบบการชำระเงินหรือระบบที่มีผลกระทบกับระบบการชำระเงินเป็นวงกว้างเป็นระบบที่มีความสำคัญ
- การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศสถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมีการกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและแนวทางจัดเตรียมทรัพยากรระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามการจัดลำดับความสำคัญของระบบงาน โดยพิจารณาอย่างน้อยครอบคลุม
  (1) เป้าหมายระยะเวลาที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ เช่น RTO, RPO เป็นต้น
  (2) ปัจจัยสำคัญที่สนับสนุนให้แผนเป็นไปตามกลยุทธ์ เช่น เทคโนโลยีในการสำรองและกู้คืนข้อมูล ความพร้อมใช้ของสถานที่ปฏิบัติงานสำรอง เป็นต้น เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีทิศทางในการพัฒนาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่บรรลุเป้าหมายที่กำหนดไว้
  (3) ทรัพยากรและงบประมาณ เพื่อจัดเตรียมระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามแผนกลยุทธ์และกิจกรรมที่ต้องดำเนินการทั้งหมด
- แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรมีการระบุกระบวนการและขั้นตอนสนับสนุนการปฏิบัติที่ชัดเจนเพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ รวมทั้งมีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น อย่างน้อยครอบคลุม
  (1) ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่น ๆ ที่เกี่ยวข้อง
  (2) ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบ และผู้ปฏิบัติที่ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกการเปลี่ยนแปลงของแผน
  (3) รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบเครือข่ายสื่อสาร เป็นต้น
  (4) ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ การตอบสนองต่อเหตุการณ์ฉุกเฉินและแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ
  (5) ขั้นตอนในการดำเนินการกู้คืนระบบ โดยควรระบุรายละเอียดอย่างชัดเจนและเพียงพอ เพื่อให้สามารถใช้เป็น checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้ ทั้งนี้สถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรจัดทำเอกสารหรือคู่มือประกอบการกู้คืนในแต่ละระบบ ในกรณีที่มีการปรับปรุงหรือเพิ่มเติมขั้นตอนนอกเหนือจากที่ระบุในแผนขณะปฏิบัติงานจริงสถาบันการเงินและ

สถาบันการเงินเฉพาะกิจ ควรมีกระบวนการรายงานและขออนุมัติจากผู้บริหารตามที่กำหนดในโครงสร้างการบังคับบัญชา พร้อมทั้งนำขั้นตอนดังกล่าวมาปรับปรุงแผนให้เป็นปัจจุบัน

(6) ขั้นตอนในการกลับคืนสู่ภาวะปกติ (return to normal) และการประกาศยกเลิกแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

(7) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง

- แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรครอบคลุมเหตุการณ์ความเสี่ยงที่สำคัญ หรือเหตุการณ์ที่มีโอกาสเกิดขึ้นได้บ่อย เช่น กรณีระบบเทคโนโลยีสารสนเทศที่ศูนย์คอมพิวเตอร์หลักขัดข้องทั้งหมด กรณีระบบงานสำคัญขัดข้องบางส่วน เป็นต้น
- การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ต้องจัดให้มีการสื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และจัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้อง

  (1) ในการสื่อสารแผนฯ ต้องมีการระบุแนวทางสื่อสารที่ชัดเจนให้บุคลากรทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน

  (2) จัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยควรครอบคลุม วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงานและการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน ระบบรักษาความปลอดภัย กระบวนการเฉพาะของแต่ละกลุ่มดำเนินงาน และความรับผิดชอบของแต่ละบุคคล เป็นต้น
- การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

  (1) จัดให้มีแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียดอย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้อง ทั้งนี้แผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปีในภาพรวมควรได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย

  (2) จัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศทั้งในระดับหน่วยงานและระดับองค์กรอย่างน้อยปีละ 1 ครั้ง โดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการลูกค้าหรือต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจทั้งระบบ เช่น ระบบการโอนและชำระเงินระหว่างสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ระบบที่ให้บริการผ่านช่องทางอิเล็กทรอนิกส์ เป็นต้น นอกจากนี้อาจพิจารณาการทดสอบระบบสำรองในลักษณะเสมือนจริง (DR live test) เพื่อให้มั่นใจว่าระบบสำรองสามารถรองรับให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง

  (3) สำหรับระบบที่มีการออกแบบในลักษณะที่พร้อมให้บริการอย่างต่อเนื่อง (high availablity - HA) ควรทดสอบในลักษณะเสมือนจริงอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าระบบงานสามารถให้บริการได้อย่างต่อเนื่องจริง รวมทั้งสามารถมั่นใจได้ว่าระบบงานสามารถทำงานได้ตามที่ออกแบบไว้ พร้อมรองรับกรณีเกิดเหตุการณ์ไม่ปกติ

  (4) กรณีระบบงานมีการเชื่อมโยงระบบเครือข่ายสื่อสารหรือใช้บริการจากหน่วยงานภายนอก ควรมีการทดสอบแผนฉุกเฉินร่วมกับหน่วยงานภายนอกที่เกี่ยวข้องด้วย เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ มีความพร้อมใช้งานร่วมกับระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

(5) มีการรายงานผลการทดสอบต่อคณะกรรมการที่ได้รับมอบหมาย โดยมีรายละเอียดอย่างน้อย ครอบคลุม วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข

(6) สถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรจัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงบุคลากรที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน การเปลี่ยนสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศ เป็นต้น เพื่อให้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน

(7) สถาบันการเงินและสถาบันการเงินเฉพาะกิจ อาจจัดให้มีการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยหน่วยงานภายนอกหรือภายในที่มีความเป็นอิสระ เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผนให้สามารถใช้งานได้จริง

2.10 การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

วัตถุประสงค์ เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจ มีแนวทางในการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ให้มีความเสี่ยงในระดับที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจยอมรับได้ บนพื้นฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องรับผิดชอบต่อการดำเนินธุรกิจและการให้บริการลูกค้า และคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิภาพ และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการให้บริการ

2.10.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถพิจารณาประยุกต์ใช้แนวปฏิบัติของธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management implementation guideline) เพื่อเป็นแนวทางการบริหารจัดการความเสี่ยงบุคคลภายนอกให้เหมาะสมและสอดคล้องตามขอบเขตระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

3. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

<u>วัตถุประสงค์</u> เพื่อให้มีการบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนกลยุทธ์ทางธุรกิจ

3.1 กำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางดำเนินโครงการจัดหาหรือพัฒนาระบบเทคโนโลยีสารสนเทศ โดยควรครอบคลุมดังนี้

3.1.1 โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด อย่างน้อย ดังนี้

- คณะกรรมการกำกับดูแลโครงการ มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลให้โครงการสำเร็จเป็นไปตามเป้าหมายที่กำหนด มีการติดตามความคืบหน้า ปัญหาและอุปสรรคของโครงการ เพื่อให้คำแนะนำและพิจารณาตัดสินใจการดำเนินงานที่สำคัญ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/ project sponsor) มีส่วนร่วมในการตัดสินใจ รวมทั้งคณะกรรมการกำกับดูแลโครงการควรมีการประชุมอย่างสม่ำเสมอ เพื่อควบคุมดูแลโครงการที่สำคัญให้เป็นไปตามแผนงานที่กำหนด
- หน่วยงานหรือทีมงานดูแลภาพรวมโครงการ (project management office) มีบทบาทหน้าที่และความรับผิดชอบในการกำหนดรูปแบบ กระบวนการและเครื่องมือที่เป็นมาตรฐานในการบริหารจัดการและติดตามโครงการ รวมทั้งติดตาม รายงานภาพรวมโครงการสำคัญให้กับคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และผู้บริหารระดับสูงที่เกี่ยวข้องได้รับทราบ เพื่อติดตามและสนับสนุนให้บริหารจัดการโครงการสำเร็จลุล่วงสอดคล้องกับเป้าหมายในระดับกลยุทธ์ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ตามแผนงานที่กำหนด
- ผู้จัดการโครงการ (project manager) มีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการ ครอบคลุม กำหนดแผนงานโครงการ วิเคราะห์ผลกระทบ และจัดให้มีแนวทางรองรับหรือแผนสำรองกรณีโครงการประสบปัญหาหรือล่าช้า รวมทั้งรายงานให้คณะกรรมการกำกับดูแลโครงการพิจารณาตัดสินใจแก้ไขปัญหาได้ทันการณ์ เพื่อให้โครงการสามารถส่งมอบได้อย่างถูกต้องครบถ้วนสำเร็จตามแผนงานที่กำหนด โดยผู้จัดการโครงการ ต้องมีความรู้ความสามารถและประสบการณ์ในการบริหารโครงการที่เพียงพอ
- หน่วยงานหรือผู้รับผิดชอบประเมินคุณภาพโครงการที่มีความเป็นอิสระจากผู้ดำเนินโครงการ เพื่อสอบทานให้มั่นใจว่าการดำเนินโครงการเป็นไปตามมาตรฐานของสถาบันการเงินและสถาบันการเงินเฉพาะกิจและแผนงานที่กำหนด

3.1.2 แนวทางการบริหารจัดการโครงการ ควรกำหนดครอบคลุมอย่างน้อย ดังนี้

- ระเบียบขั้นตอนการบริหารจัดการโครงการ และข้อกำหนดการกำกับดูแลโครงการตามระดับความเสี่ยงที่อาจเกิดจากความซับซ้อนของเทคโนโลยีที่นำมาใช้ ครอบคลุมตั้งแต่ ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ
- ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ
- มาตรฐานการควบคุมคุณภาพโครงการ ครอบคลุมคุณลักษณะโครงการคุณภาพ และการประเมินคุณภาพโครงการ รวมทั้งกำหนดหน่วยงานหรือผู้รับผิดชอบประเมินคุณภาพโครงการที่มีความเป็นอิสระจากผู้ดำเนินโครงการ

- รูปแบบของเอกสารหรือผลลัพธ์ที่เป็นมาตรฐาน ที่ต้องส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น

<u>การเริ่มโครงการ</u>

3.2 มีการประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งเลือกใช้เทคโนโลยีที่เหมาะสม ทั้งนี้โครงการต้องมีเป้าหมายที่ชัดเจน (project objective) สอดคล้องกับกลยุทธ์ขององค์กรและคำนึงถึงการรักษาความมั่นคงปลอดภัย

3.3 มีแผนการดำเนินโครงการ ที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการ อย่างน้อยครอบคลุม

- เป้าหมายโครงการ
- คุณลักษณะโครงการคุณภาพที่คาดหวัง
- ทรัพยากร (resources) ที่ใช้
- บทบาทหน้าที่ ความรับผิดชอบของทีมงานในการดำเนินโครงการ โดยทีมงานจะต้องมีประสิทธิภาพและมีความรู้ความเชี่ยวชาญเพียงพอในการดำเนินโครงการ
- ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน
- ผลงานที่จะส่งมอบในแต่ละขั้นตอน
- ข้อกำหนดเงื่อนไขที่เกี่ยวข้องกับโครงการ เช่น ข้อกำหนดของผู้ว่าจ้าง ภาระผูกพัน ข้อจำกัด เป็นต้น

3.4 มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตในการอนุมัติที่กำหนดไว้

<u>การดำเนินการและควบคุมโครงการ</u>

3.5 มีการบันทึกและจัดเก็บข้อมูลโครงการของแต่ละโครงการอย่างเพียงพอเพื่อใช้ติดตามดูแลและสามารถตรวจสอบย้อนหลังได้

3.6 มีการประเมินและติดตามการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากรที่วางแผนไว้ และคุณภาพโครงการที่คาดหวัง ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาและหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ

3.7 มีการรายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการ ต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารที่ได้รับมอบหมายอย่างเป็นประจำ เพื่อสามารถให้คำแนะนำและแนวทางในการแก้ไขปัญหาที่จะลดความเสี่ยงที่อาจเกิดขึ้นอย่างทันท่วงที โดยโครงการที่ส่งผลกระทบต่อธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างมีนัยสำคัญ ควรนำเสนอแก่คณะกรรมการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือคณะกรรมการที่ได้รับมอบหมายด้วย

<u>การปิดโครงการ</u>

3.8 มีการสรุปประโยชน์ที่ได้รับจากโครงการเทียบกับเป้าหมายที่กำหนด

3.9 มีการรวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์ ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไปให้มีประสิทธิภาพมากขึ้น

<u>การสอบทานโครงการ</u>

3.10 มีการสอบทานโครงการที่สำคัญ โดยหน่วยงานอิสระ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ รวมทั้งกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

เอกสารอ้างอิง

- Control Objectives for Information and related Technology 5 for Risk (COBIT 5 for risk) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ISO27001:2013 Information technology - Security techniques – Information Security Management Systems – Requirement มาตรฐานด้านการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ISO27005:2011 Information technology - Security techniques – Information Security Risk Management หลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ISO31000:2009 Risk Management – Principles and Guideline มาตรฐานการบริหารความเสี่ยง
- ISO21500:2012 Guidance on Project Management การบริหารจัดการโครงการ
- มาตรฐานการตรวจสอบด้านเทคโนโลยีสารสนเทศของ Federal Financial Institution Examination Council (FFIEC) ซึ่งเป็นองค์กรที่กำกับดูแลผู้ให้บริการและผู้ประกอบธุรกิจ ในสหรัฐอเมริกา

ธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทย

Third Party Risk Management Implementation Guideline
แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายกำกับระบบการชำระเงินและคุ้มครองผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย

สารบัญ

แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก 1

ส่วนที่ 1 : การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (risk governance) 2

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย 2
2. จัดโครงสร้างองค์กรให้มีการถ่วงดุล 2
3. การบริหารจัดการบุคลากรที่เกี่ยวข้อง 4
4. การคุ้มครองลูกค้าของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ 4
5. นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก 4
6. การตรวจสอบ 5

ส่วนที่ 2 : การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management) 6

7. การประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก 6
8. การคัดเลือกบุคคลภายนอก 7
9. การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก 8
10. การติดตามผลการปฏิบัติงานของบุคคลภายนอก 9
11. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง 10
12. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก 10

เอกสารอ้างอิง 20

แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ธปท. จัดทำแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management implementation guideline) เพื่อเป็นแนวทางให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถพิจารณาประยุกต์ใช้ให้เหมาะสมและสอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

ทั้งนี้ สำหรับการใช้บริการจากบุคคลภายนอกประเภท cloud computing เพื่อรองรับระบบงานสำคัญ (critical system) เช่น ระบบ core banking ระบบชำระเงิน ระบบที่เกี่ยวกับการให้บริการลูกค้าเป็นวงกว้าง เป็นต้น ให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจปฏิบัติตามแนวปฏิบัติฉบับนี้ในส่วนที่ 3 ทุกข้อ

ส่วนที่ 1 : การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (risk governance)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยประกอบด้วยการกำหนดบทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงในการกำกับดูแล การจัดให้มีโครงสร้างองค์กรที่มีการถ่วงดุลในเรื่องการบริหารจัดการความเสี่ยงจากบุคคลภายนอก การบริหารจัดการบุคลากรที่เกี่ยวข้อง การคุ้มครองลูกค้า การจัดให้มีนโยบายที่ครอบคลุมการบริหารจัดการความเสี่ยงจากบุคคลภายนอก และการตรวจสอบ ดังนี้

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

    1.1 ดูแลให้การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องกับกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจ มีการบริหารความเสี่ยงให้อยู่ในระดับที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจยอมรับได้ (risk appetite) และไม่ขัดต่อกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

    1.2 ดูแลให้นโยบาย ครอบคลุมการบริหารจัดการความเสี่ยงจากบุคคลภายนอก เพียงพอตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร อาจเป็นนโยบายที่จัดทำขึ้นเฉพาะ หรือรวมอยู่ในนโยบายที่มีอยู่แล้ว รวมทั้งจัดทำมาตรฐานและระเบียบวิธีปฏิบัติที่สอดรับกับนโยบายดังกล่าว จัดให้มีการนำไปปฏิบัติอย่างทั่วถึง นอกจากนี้ ดูแลให้มีการทบทวนและประเมินประสิทธิภาพของนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติดังกล่าวอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

    1.3 จัดให้มีการกำกับและควบคุมดูแลการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้เป็นไปตามนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติที่กำหนด และพิจารณาให้ความเห็นชอบต่อการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลที่มีนัยสำคัญ

2. จัดโครงสร้างองค์กรให้มีการถ่วงดุล

    สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดโครงสร้างองค์กร และหน้าที่ความรับผิดชอบที่เกี่ยวกับการบริหารจัดการบุคคลภายนอกให้มีการถ่วงดุลตามหลัก three lines of defence โดยมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนและมีการถ่วงดุลในการทำหน้าที่ของหน่วยงานที่ทำหน้าที่ปฏิบัติงาน (first line) บริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ (second line) และการตรวจสอบ (third line)

2.1 หน้าที่ของหน่วยงานที่ทำหน้าที่ปฏิบัติงานกับบุคคลภายนอก (first line of defence) ควรมีหน้าที่ครอบคลุม ดังนี้

(1) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และประเมินศักยภาพของบุคคลภายนอก (due diligence) ก่อนเริ่มหรือต่อสัญญาหรือข้อตกลง

(2) จัดให้มีกรอบและแนวทางการประเมิน ควบคุม และติดตามผลอย่างสม่ำเสมอและต่อเนื่อง ทั้งด้านประสิทธิภาพและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงการดูแลคุ้มครองข้อมูลส่วนบุคคลด้วย

(3) ติดตามการเปลี่ยนแปลง ปัญหาและเหตุการณ์ผิดปกติสำคัญที่เกิดขึ้นอันสืบเนื่องหรือเกี่ยวเนื่องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อดูแลให้การดำเนินการของบุคคลภายนอกเป็นไปตามที่ระบุในสัญญาหรือข้อตกลง

(4) รายงานผลการปฏิบัติงาน ผลการประเมินความเสี่ยง ปัญหาและเหตุการณ์ผิดปกติที่ส่งผลกระทบต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างมีนัยสำคัญต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย อย่างเพียงพอ ต่อเนื่อง ทันการณ์ และสอดรับกับระดับความเสี่ยง

2.2 หน้าที่ของหน่วยงานที่ทำหน้าที่บริหารความเสี่ยง และการกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ (second line of defense) ควรมีหน้าที่ครอบคลุม ดังนี้

(1) จัดให้มีกรอบและกระบวนการบริหารความเสี่ยงตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป ประกอบไปด้วย การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามทบทวนความเสี่ยง และการรายงานความเสี่ยง ที่ครอบคลุมความเสี่ยงจากบุคคลภายนอก

(2) ติดตามดูแลให้หน่วยงานที่ทำหน้าที่ first line of defense มีการบริหารความเสี่ยง และให้มีการรายงานความเสี่ยงดังกล่าวมายังหน่วยนงานที่ทำหน้าที่ second line of defense เพื่อรวบรวมและเชื่อมโยงความเสี่ยงดังกล่าวกับความเสี่ยงด้านอื่นของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ตลอดจนชี้แนะและให้คำปรึกษาในการบริหารจัดการความเสี่ยงของหน่วยงานที่ทำหน้าที่ first line of defense

(3) ติดตามความเสี่ยง และทบทวนการควบคุมและการบริหารจัดการความเสี่ยง ซึ่งรวมถึงการทบทวนปัจจัยเสี่ยง ดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) และกระบวนการควบคุมและบริหารจัดการความเสี่ยง เพื่อให้มั่นใจว่าสถาบันการเงินและสถาบันการเงินเฉพาะกิจมีความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกในระดับความเสี่ยงที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจยอมรับได้ รวมทั้งนำเสนอผลการบริหารความเสี่ยงดังกล่าวต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

(4) กำกับดูแลการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง รวมถึงดูแลให้เป็นไปตามนโยบาย มาตรฐานระเบียบปฏิบัติของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ตลอดจนมาตรฐานสากลที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจอ้างอิงหรือนำมาบังคับใช้ และนำเสนอรายงานผลการปฏิบัติตามกฎหมายและกฎเกณฑ์ต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

2.3 หน้าที่ของหน่วยงานที่ทำหน้าที่ตรวจสอบ (third line of defense) ควรมีหน้าที่ครอบคลุม ดังนี้

(1) จัดให้มีการตรวจสอบการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกโดยผู้ตรวจสอบที่เป็นอิสระ เพื่อตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ first line of defense second line of defense และบุคคลภายนอก ว่ามีการปฏิบัติตามนโยบาย มาตรฐาน ระเบียบปฏิบัติของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ สัญญาหรือข้อตกลง และการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(2) รายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบ

3. การบริหารจัดการบุคลากรที่เกี่ยวข้อง

สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดสรรบุคลากร สร้างความเข้าใจและความตระหนักรู้ถึงความเสี่ยงของบุคคลภายนอก รวมถึงพัฒนาความรู้ความเชี่ยวชาญของบุคลากรที่เกี่ยวข้อง ให้เพียงพอในการปฏิบัติงานอย่างมีประสิทธิภาพ เช่น จัดให้มีการพัฒนาทักษะความรู้ของพนักงานที่เกี่ยวข้องครอบคลุมการบริหารจัดการความเสี่ยงจากบุคคลภายนอก การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรณีการใช้ cloud computing ควรเสริมสร้างทักษะความรู้ให้แก่ผู้บริหารและพนักงานที่เกี่ยวข้องให้สามารถปฏิบัติงานได้ตามมาตรฐานและแนวปฏิบัติที่ดีของผู้ให้บริการ cloud computing เป็นต้น

4. การคุ้มครองลูกค้าของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

กรณีที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้บริการแก่ลูกค้า สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรดำเนินการ ดังนี้

4.1 ดูแลและบริหารจัดการบุคคลภายนอกที่มีการเข้าถึง การใช้ และการดูแลรักษาข้อมูลลูกค้าอย่างรัดกุม เพื่อให้ได้รับการดูแลอย่างปลอดภัย โดยคำนึงถึงความเป็นส่วนตัว และเป็นไปตามกฎหมายอื่นที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

4.2 ดูแลการแก้ไขปัญหาและจัดการเรื่องร้องเรียนให้แก่ลูกค้าอย่างรับผิดชอบและเป็นธรรม

5. นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

5.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดนโยบายที่ครอบคลุมถึงการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างชัดเจนเป็นลายลักษณ์อักษร โดยอาจเป็นนโยบายที่จัดทำขึ้นเฉพาะหรือรวมอยู่ในนโยบายที่มีอยู่แล้ว

5.2 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกควรสอดคล้องกับนโยบายอื่นที่เกี่ยวข้องของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

5.3 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกได้รับอนุมัติจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรจัดชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและควบคุมดูแลให้ปฏิบัติตามนโยบาย

5.4 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ควรครอบคลุม อย่างน้อย ดังนี้

(1) โครงสร้างการกำกับดูแล บทบาทหน้าที่ของผู้เกี่ยวข้องในการกำกับดูแลและบริหารจัดการความเสี่ยงจากบุคคลภายนอก

(2) การบริหารจัดการความเสี่ยงที่ครอบคลุมวงจรการบริหารจัดการบุคคลภายนอก (third party management life cycle) และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตามหลัก CIA

(3) หลักเกณฑ์การขออนุมัติความเห็นชอบ และการรายงานต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

(4) การตรวจสอบการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(5) การเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างมีนัยสำคัญ เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ซึ่งรวมถึงการมีข้อมูลพร้อมใช้สำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้า

(6) การคุ้มครองลูกค้าของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

5.5 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีมาตรฐานและระเบียบวิธีปฏิบัติเพื่อสนับสนุนการดำเนินการตามนโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ให้สอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญ รวมถึงมาตรฐานสากลที่ยอมรับโดยทั่วไป

6. การตรวจสอบ

6.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากสถาบันการเงินและสถาบันการเงินเฉพาะกิจ สามารถเข้าตรวจสอบบุคคลภายนอกในส่วนที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจได้ เช่น ระบุเงื่อนไขในสัญญาหรือข้อตกลง เป็นต้น สำหรับกรณีที่ไม่สามารถระบุสิทธิ์ให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอก ในเงื่อนไขสัญญาหรือข้อตกลงได้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมั่นใจว่าบุคคลภายนอกรายดังกล่าวมีผลการตรวจสอบจากผู้ตรวจสอบภายนอกที่เป็นอิสระทดแทนได้

6.2 จัดให้มีการตรวจสอบให้สอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญโดยการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่มีนัยสำคัญควรได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง และเมื่อพบเหตุการณ์ผิดปกติที่มีนัยสำคัญ

ทั้งนี้ หากมีเหตุจำเป็นที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจไม่สามารถดำเนินการตรวจสอบได้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีแนวทางที่จะใช้ประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอก ให้รัดกุมเพียงพอสอดคล้องตามขอบเขต ระดับความเสี่ยง และความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล โดยอาจใช้ผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น ผลการตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 type

2 report) หรือ PCI-DSS Attestation of Compliance (AOC) เป็นต้น และรับทราบโดยคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายแล้วได้

ส่วนที่ 2 : การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างรัดกุมเพียงพอและต่อเนื่อง และดูแลให้สอดคล้องตามกรอบและกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT risk management) เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ โดยกำหนดให้มีระเบียบวิธีปฏิบัติที่ชัดเจนและเป็นลายลักษณ์อักษร ครอบคลุมวัฏจักรการบริหารจัดการบุคคลภายนอก (third party management life cycle) ตั้งแต่การประเมินความเสี่ยง การคัดเลือกบุคคลภายนอก การจัดทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานอย่างต่อเนื่อง และการยกเลิก/สิ้นสุดสัญญาหรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้าน IT

7. การประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

7.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรประเมินความเสี่ยงและผลกระทบทั้งก่อนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงจากบุคคลภายนอก และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ รวมถึงประเมินเป็นประจำตามรอบระยะเวลาที่สอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญอย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงความเสี่ยงดังต่อไปนี้

(1) ความเสี่ยงด้านกลยุทธ์ (strategic risk)

(2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่ครอบคลุมและรัดกุมเพียงพอ

(3) ความเสี่ยงด้านชื่อเสียง (reputation risk) เช่น ระบบหรือบริการที่ดำเนินการร่วมกับบุคคลภายนอกเกิดขัดข้อง ส่งผลกระทบต่อการให้บริการ รวมถึงชื่อเสียงและความน่าเชื่อถือของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เป็นต้น

(4) ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยทางไซเบอร์ เช่น ระบบขัดข้องหรือหยุดบริการโดยมีสาเหตุจากบุคคลภายนอก ระบบของบุคคลภายนอกมีช่องโหว่ด้านความปลอดภัยทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล บุคคลภายนอกใช้งานสิทธิสูงเกินกว่าที่ได้รับอนุญาต การจัดเตรียมทรัพยากรระบบไม่เพียงพอ เป็นต้น

(5) ความเสี่ยงด้านกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น การปฏิบัติไม่ถูกต้องตามพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการ

รักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติลิขสิทธิ์ และ The EU General Data Protection Regulation (GDPR) เป็นต้น

(6) ความเสี่ยงของประเทศที่บุคคลภายนอกตั้งอยู่หรือประกอบธุรกิจ (country /cross border risk) ทั้งในด้านการเมือง เศรษฐกิจและสังคม เช่น การไม่สามารถเข้าถึงข้อมูลอันเนื่องมาจากการขัดข้องหรือการปิดกั้นเครือข่ายสื่อสารระหว่างประเทศ เป็นต้น

(7) ความเสี่ยงที่เกี่ยวข้องกับสัญญาหรือข้อตกลง เช่น ความครอบคลุม ชัดเจน และความครบถ้วนสมบูรณ์ของสัญญาหรือข้อตกลง เป็นต้น

(8) ความเสี่ยงจากการผูกติดกับบุคคลภายนอกรายใดรายหนึ่ง (third party/vendor locked-in) โดยการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก อาจทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยี และข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง-หรือใช้บริการจากบุคคลภายนอกรายอื่น

(9) ความเสี่ยงจากการกระจุกตัว (concentration risk) สามารถครอบคลุมได้หลายกรณี เช่น
- การใช้บริการจากบุคคลภายนอกเพียงรายเดียว (single provider) ในทุกการใช้บริการจากบุคคลภายนอก
- การใช้บริการจากบุคคลภายนอกรายใดรายหนึ่งที่ให้บริการกับหลายสถาบันการเงิน
- การใช้บริการจากผู้ให้บริการภายนอกที่มีส่วนแบ่งทางการตลาดสูง
- การใช้บริการจากบุคคลภายนอกที่ไปว่าจ้างผู้อื่นดำเนินการแทนเป็นรายเดียวกัน (Subcontractor Concentration)
- การใช้บริการจากบุคคลภายนอกที่ไปว่าจ้างผู้อื่นดำเนินการแทนซึ่งตั้งอยู่หรือประกอบธุรกิจไปในประเทศหรือต่างประเทศเดียวกันเป็นจำนวนมาก (Geographic Concentration)

(10) ความเสี่ยงจากบุคคลภายนอกว่าจ้างผู้อื่นดำเนินการแทน (subcontractor) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น

7.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดให้มีการควบคุมและบริหารจัดการความเสี่ยงครอบคลุมวัฏจักรการบริหารจัดการบุคคลภายนอก (third party management life cycle) ตั้งแต่การคัดเลือก การจัดทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานอย่างต่อเนื่อง ตลอดจนการยกเลิก/สิ้นสุดสัญญาหรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้าน IT ข้อ 8 – 12

7.3 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดหลักเกณฑ์ที่ชัดเจนสำหรับใช้จัดระดับความเสี่ยงและระดับ
ความมีนัยสำคัญจากการใช้บริการ เชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

7.4 จัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ให้ครอบคลุมครบถ้วนตามหลักเกณฑ์ที่กำหนดในข้อ 7.3 โดยควรมีรายละเอียดครอบคลุมตามข้อ 12.1(2) เพื่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถใช้บริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของบุคคลภายนอกได้ครบถ้วนต่อเนื่อง

8. การคัดเลือกบุคคลภายนอก

8.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดให้มีระเบียบวิธีปฏิบัติและหลักเกณฑ์ในการพิจารณาคัดเลือกบุคคลภายนอก อย่างชัดเจน และเป็นลายลักษณ์อักษร โดยมีข้อมูลที่เพียงพอสำหรับสนับสนุนการพิจารณาตัดสินใจใช้บริการ เชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อ

สามารถคัดเลือกบุคคลภายนอกที่มีความเหมาะสมตามวัตถุประสงค์การดำเนินการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

8.2 การตัดสินใจใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่มีความเสี่ยงหรือมีนัยสำคัญควรได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

8.3 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรทำการประเมินศักยภาพบุคคลภายนอก (due diligence) โดยพิจารณาประเมินให้ครอบคลุมตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญ โดยควรคำนึงถึงเรื่องดังต่อไปนี้

(1) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์และความสามารถในการให้บริการของบุคคลภายนอกในช่วงที่ผ่านมา
(2) ธรรมาภิบาลและวัฒนธรรมองค์กรของบุคคลภายนอก
(3) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน
(4) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
(5) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ
(6) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เป็นต้น
(7) การปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ เช่น การขอตรวจสอบการได้รับการรองรับตามมาตรฐาน ISO 27001 เป็นต้น โดยการรับรองการปฏิบัติตามมาตรฐานสากลควรพิจารณาว่าบุคคลภายนอกได้รับการรับรองการให้บริการในส่วนที่สำคัญ หรือส่วนที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจจะใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูล เช่น ศูนย์คอมพิวเตอร์ และ/หรือ ได้รับการรับรองครอบคลุมทั้งองค์กร
(8) ปัจจัยภายนอกที่อาจกระทบต่อการให้บริการของบุคคลภายนอก เช่น สถานการณ์ทางการเมือง สภาวะเศรษฐกิจ ข้อจำกัดด้านกฎหมายของประเทศที่บุคคลภายนอกตั้งอยู่หรือประกอบธุรกิจ
(9) การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยีผู้ให้บริการหรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง เช่น การใช้รูปแบบการรับส่งข้อมูลกับบุคคลภายนอกที่เป็นมาตรฐานแบบเปิด (open standard หรือ open source) เป็นต้น

9. การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

9.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเป็นลายลักษณ์อักษร และจัดเก็บสัญญาหรือข้อตกลงดังกล่าวไว้ที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจเพื่อสามารถบังคับใช้ได้ตามกฎหมาย

9.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญในสัญญาหรือข้อตกลงกับบุคคลภายนอกอย่างชัดเจน โดยพิจารณาให้ครอบคลุมตามขอบเขต ระดับความ

เสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ดังนี้

(1) ขอบเขตการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(2) บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอก และสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

(3) มาตรฐานการปฏิบัติงานขั้นต่ำของบุคคลภายนอก เช่น มาตรฐานการควบคุมภายใน มาตรฐานการรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (availability) เป็นต้น

(4) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรสอดคล้องกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

(5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก (ongoing monitoring) ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือเหตุการณ์ที่สำคัญ และรายงานปัญหาผิดปกติ

(6) กำหนดให้การคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจและข้อมูลของลูกค้า เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น การกำหนดให้บุคคลภายนอกออกหนังสือรับรองการทำลายข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

(8) เงื่อนไขหรือสิทธิของสถาบันการเงินและสถาบันการเงินเฉพาะกิจในการขอเปลี่ยนแปลง ยุติหรือยกเลิกสัญญาหรือข้อตกลง กรณีที่เกิดการเปลี่ยนแปลงหรือเกิดการละเมิดสัญญาหรือข้อตกลง เช่น การเปลี่ยนเจ้าของกิจการ การละเมิดความปลอดภัยหรือการรักษาความลับ และการที่บุคคลภายนอกอยู่ระหว่างกระบวนการพิทักษ์ทรัพย์/การชำระบัญชี/ล้มละลาย เป็นต้น

(9) แนวทางการระงับข้อพิพาท และความรับผิดต่อความเสียหาย

(10) การระบุสิทธิในการเข้าตรวจสอบโดยสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากสถาบันการเงินและสถาบันการเงินเฉพาะกิจหรือ ธปท. ให้สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกที่มีนัยสำคัญ

10. การติดตามผลการปฏิบัติงานของบุคคลภายนอก

10.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดผู้รับผิดชอบและติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น กำหนดให้บุคคลภายนอกรายงานผลการปฏิบัติงานอย่างสม่ำเสมอ กำหนดการประชุมติดตามอย่างสม่ำเสมอและต่อเนื่อง การเข้าสังเกตการณ์การดำเนินงานของบุคคลภายนอก เป็นต้น

10.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดให้บุคคลภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจได้รับทราบอย่างทันการณ์ เพื่อประเมินผลกระทบที่มีต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ทั้งนี้กรณีประเมินว่าผลกระทบที่เกิดขึ้นมีผลต่อการดำเนินธุรกิจของสถาบันการเงินและสถาบัน

การเงินเฉพาะกิจอย่างมีนัยสำคัญ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ

10.3 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรทบทวนการประเมินศักยภาพ การประเมินผลการปฏิบัติงาน และการประเมินความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกทั้งในด้านประสิทธิภาพการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และการปฏิบัติตามกฎหมาย เมื่อจะต่อสัญญาและเมื่อถึงรอบระยะเวลาที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด ทั้งนี้ การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่มีนัยสำคัญควรกำหนดให้ดำเนินการอย่างน้อยปีละครั้ง รวมถึงให้รายงานผลการประเมินดังกล่าวต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

11. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง

11.1 จัดให้มีมาตรฐานหรือระเบียบปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง เพื่อเป็นกรอบแนวทางการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง โดยคำนึงถึงความต่อเนื่องในการให้บริการและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้งนี้ มาตรฐานหรือระเบียบปฏิบัติดังกล่าวควรครอบคลุม บทบาทหน้าที่คณะกรรมการและหน่วยงานที่เกี่ยวข้อง กระบวนการและการควบคุมภายใน เช่น การสำรองข้อมูลก่อนการยกเลิก การลบหรือนำกลับทรัพย์สินสำคัญของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (ตัวอย่างเช่น ข้อมูล กุญแจการเข้ารหัสข้อมูล และบัญชีผู้ใช้งาน) เป็นต้น

11.2 การพิจารณายกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรประเมินผลกระทบและความเสี่ยงที่อาจเกิดขึ้นจากการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง และดำเนินการตามมาตรฐานหรือระเบียบปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง และกำหนดกลยุทธ์และแผนงานการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง (exit strategy and exit plan) ที่ชัดเจน เพื่อให้มั่นใจว่าการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลงเป็นไปอย่างมีประสิทธิภาพและได้เตรียมความพร้อมต่อผลกระทบที่อาจเกิดขึ้น เช่น การหยุดให้บริการของระบบที่ส่งผลกระทบกับลูกค้าหรือผู้ใช้บริการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

12. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรดูแลให้มั่นใจว่าการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นไปตามกรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (availability) หรือ CIA สอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และมาตรฐานสากลด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เช่น ISO/IEC 27001, ISO/IEC 27017 เป็นต้น โดยควรปฏิบัติตามแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่อง การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management implementation guideline) รวมถึงมาตรฐานสากลทางด้านการป้องกันและรับมือภัยไซเบอร์ที่เป็นมาตรฐานสากลที่ยอมรับโดยทั่วไป โดยพิจารณาให้สอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญ ทั้งนี้ ในกรณีที่มีการใช้บริการ cloud computing

สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรนำแนวปฏิบัติที่ดีของผู้ให้บริการ cloud computing มาเป็นแนวทางในการปฏิบัติงานและควบคุมดูแลเพื่อให้ระบบที่ใช้บริการ cloud computing มีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และควรดำเนินการตามแนวทางการควบคุมเพิ่มเติมดังต่อไปนี้

12.1 การจัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกและทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

(1) จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำ และปรับปรุงทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถนำมาใช้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างปลอดภัยและทันการณ์ เช่น ใช้พิจารณาความเสี่ยงที่เกี่ยวข้องเมื่อเกิดเหตุการณ์ภัยไซเบอร์ หรือใช้วางแผนรองรับเมื่อใกล้สิ้นสุดสัญญาหรือข้อตกลง เป็นต้น

(2) ทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ควรครอบคลุม

- ชื่อบุคคลภายนอก
- ประเภทของบุคคลภายนอก เช่น IT outsourcing ISP เป็นต้น
- ชื่อบริการ/ระบบงาน
- ลักษณะและขอบเขตของงาน
- ประเภทของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น IT outsourcing cloud computing บริการร่วมกับพันธมิตรทางธุรกิจ การใช้บริการเครือข่ายสาธารณะ การใช้บริการชำระเงินกลาง เป็นต้น
- ระดับความเสี่ยง และระดับความมีนัยสำคัญ
- ที่ตั้งศูนย์คอมพิวเตอร์หลักและสำรองของบุคคลภายนอกที่ประมวลผล จัดเก็บข้อมูล หรือดำเนินการใด ๆ เกี่ยวกับข้อมูลหรือระบบงานให้แก่สถาบันการเงินและสถาบันการเงินเฉพาะกิจ
- วันเริ่มต้นและสิ้นสุดสัญญาหรือข้อตกลง
- การรับรองตามมาตรฐานสากลด้าน IT ที่เกี่ยวข้อง (ถ้ามี)
- รายละเอียดทรัพย์สินที่เกี่ยวข้อง เช่น ข้อมูลที่นำไปจัดเก็บหรือประมวลผล ระดับชั้นความลับข้อมูล เป็นต้น

12.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

(1) ดูแลข้อมูลที่อยู่ภายใต้การดูแลของบุคคลภายนอกให้เป็นไปตามนโยบายและมาตรฐานของสถาบันการเงินและสถาบันการเงินเฉพาะกิจสอดคล้องกับมาตรฐานสากลตามระดับชั้นของข้อมูล (information classification) ครอบคลุมทั้งข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit) และข้อมูลที่อยู่บน

ระบบงานและสื่อบันทึกข้อมูล (data at rest) ซึ่งรวมถึงข้อมูลที่ถูกจัดเก็บที่สื่อบันทึกข้อมูลสำรอง

(2) บริหารจัดการกุญแจการเข้ารหัสข้อมูลด้วยตนเอง ซึ่งควรควบคุมในทุกขั้นตอน ตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส (lifecycle of cryptographic keys) ตั้งแต่การสร้าง การจัดเก็บ การใช้งาน การสำรอง การเพิกถอน และการต่ออายุของกุญแจเข้ารหัสข้อมูล

(3) สร้างกุญแจการเข้ารหัสข้อมูลด้วยตนเอง ทั้งนี้ หากสถาบันการเงินและสถาบันการเงินเฉพาะกิจไม่สามารถสร้างกุญแจการเข้ารหัสด้วยตนเองได้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมั่นใจได้ว่ากุญแจการเข้ารหัสของบุคคลภายนอกไม่มีการนำมาใช้ร่วมกับผู้ใช้บริการรายอื่น และทราบถึงรายละเอียดเกี่ยวกับระบบการบริหารจัดการกุญแจเข้ารหัสข้อมูลของบุคคลภายนอก ได้แก่

- ประเภทของกุญแจเข้ารหัสข้อมูล
- รายละเอียดของระบบ รวมถึงกระบวนการควบคุมการเข้ารหัสข้อมูลในแต่ละขั้นตอนตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส
- ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล

(4) เก็บกุญแจการเข้ารหัสข้อมูลในอุปกรณ์รักษาความปลอดภัย เช่น hardware security module (HSM) เป็นต้น และดูแลรักษาความปลอดภัยอุปกรณ์ HSM ด้วยการจัดตั้งในโซนเครือข่ายที่ปลอดภัยและจำกัดการเชื่อมต่อกับระบบงานอื่นที่ไม่เกี่ยวข้อง

(5) สอบทานการปฏิบัติงานการบริหารจัดการการเข้ารหัสข้อมูลทั้งที่ดำเนินการเองและดำเนินการโดยบุคคลภายนอก ให้ครอบคลุมการสอบทานช่องโหว่และความเสี่ยงของการเข้ารหัสข้อมูล โดยพิจารณาให้มีความปลอดภัยสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป เช่น อัลกอริธึมการเข้ารหัส (encryption algorithm) และขนาดความยาวของกุญแจเข้ารหัสข้อมูล เป็นต้น

12.3 การควบคุมการเข้าถึง (access control)

(1) กำหนดกระบวนการจัดการและควบคุมดูแลสิทธิในการเบิกใช้และการเข้าถึงระบบและข้อมูลที่ชัดเจนเป็นลายลักษณ์อักษร เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่กำหนด สอดคล้องตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป

(2) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้มีสิทธิเข้าใช้งานระบบและผู้ใช้งานที่ได้รับสิทธิสูงให้ชัดเจน

(3) ควบคุมดูแลการให้สิทธิแก่บุคคลภายนอก โดยจำกัดสิทธิตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน มีการอนุมัติการเบิกใช้งาน เพื่อไม่ให้บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ตั้งแต่ต้น จนจบกระบวนการ

(4) มีระบบหรือกระบวนการติดตามระหว่างการใช้งานบัญชีผู้ใช้งานที่มีสิทธิสูงสุด รวมทั้งควรติดตามและสอบทานสถานะสิทธิและการใช้งานหรือการเข้าถึงระบบข้อมูล ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิอย่างเป็นประจำ เพื่อให้มั่นใจว่าการใช้งานสิทธิเป็นไปตามขอบเขต และความจำเป็นในการใช้งาน

(5) กำหนดวิธีการระบุและพิสูจน์ตัวตนผู้ใช้งาน ด้วยวิธีการที่รัดกุมเพียงพอ สอดคล้องกับมาตรฐานนโยบายที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด หรือมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป

(6) ในกรณีที่บุคคลภายนอกเชื่อมต่อเพื่อเข้าถึงระบบงานของสถาบันการเงินและสถาบันการเงินเฉพาะกิจผ่านช่องทางการเข้าถึงระบบงานระยะไกล (system remote access) สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีกระบวนการบริหารจัดการการเข้าถึงระยะไกลด้วยวิธีการที่ปลอดภัย ดังนี้

- ขออนุมัติก่อนการเข้าถึงระบบงานระยะไกล (system remote access) ของบัญชีผู้ใช้งานสิทธิสูงอย่างเคร่งครัด โดยให้ใช้เฉพาะกรณีที่มีความจำเป็นเท่านั้น และจำกัดระยะเวลาในการเข้าถึงระบบงาน
- พิสูจน์ตัวตนผู้ใช้งานแบบ multi-factors authentication และการเชื่อมต่อผ่าน virtual private network (VPN)
- ควบคุมการเข้าใช้งาน โดยจำกัดการเข้าใช้งานได้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้น หรือใช้เทคโนโลยีบริหารจัดการเครื่องคอมพิวเตอร์แบบเสมือน (virtual desktops infrastructure) เพื่อลดความเสี่ยงจากการติด malware หรือการเข้าถึงระบบงานที่ไม่เหมาะสม
- สามารถระบุและสอบทานแหล่งที่มาของอุปกรณ์หรือระบบปลายทางที่เข้าเชื่อมต่อกับระบบเครือข่ายของสถาบันการเงินและสถาบันการเงินเฉพาะกิจแบบระยะไกล
- สอบทานการเข้าถึงระบบงานระยะไกล โดยบัญชีผู้ใช้งานสิทธิสูงด้วยบุคคลหรือหน่วยงานที่มีความเป็นอิสระและมีความรู้ความเชี่ยวชาญเพียงพอ

(7) ดูแลให้บุคคลภายนอกจัดเก็บบันทึกข้อมูลประวัติของการพิสูจน์ตัวตนและการเข้าถึง (access log) บันทึกการดำเนินงาน (activity log) ตามระยะเวลาที่กฎหมายกำหนด โดยมีการสอบทานข้อมูลการบันทึกเหตุการณ์ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยงและความสำคัญอย่างเป็นประจำ เพื่อให้มั่นใจว่าบุคคลภายนอกปฏิบัติงานเป็นไปตามข้อตกลงและมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

12.4 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

(1) รักษาความปลอดภัยในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารกับบุคคลภายนอกเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

(2) ดูแลให้บุคคลภายนอกมีระบบหรือกระบวนการสำหรับคัดกรอง traffic ที่ส่งผ่านระบบเครือข่าย ตรวจจับ แจ้งเตือน และสามารถยับยั้งการบุกรุกหรือตอบโต้การโจมตีได้โดยอัตโนมัติแบบต่อเนื่องบนระบบเครือข่ายให้เพียงพอเหมาะสมตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น มีเครื่องมือที่ใช้ตรวจหาและแจ้งเตือนที่สามารถยับยั้งการบุกรุก หรือตอบโต้การโจมตีได้โดยอัตโนมัติบนระบบเครือข่าย (network intrusion detection and prevention

systems : NIDPS) เครื่องมือป้องกันการโจมตีเว็บไซต์ (web application firewall : WAF) มาตรการป้องกันการโจมตีแบบ distributed denial of services (DDoS) และระบบป้องกันข้อมูลรั่วไหล (data leakage prevention systems : DLPS) และมีการตรวจจับไวรัส หรือโปรแกรมไม่ประสงค์ดีต่าง ๆ ที่อาจบุกรุกเข้าสู่เครือข่าย เป็นต้น

12.5 การบริหารจัดการการเปลี่ยนแปลง (change management)

(1) กำหนดกระบวนการและแนวทางบริหารจัดการการเปลี่ยนแปลงร่วมกับบุคคลภายนอก เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถประเมินผลกระทบและเตรียมแนวทางรองรับ เช่น เมื่อมีการเปลี่ยนแปลงระบบของผู้ให้บริการ cloud computing และกระทบกับการให้บริการและดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

(2) ให้บุคคลภายนอกแจ้งการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบกับการให้บริการและดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจได้ทราบล่วงหน้าในระยะเวลาที่ตกลงร่วมกัน เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจพิจารณาแนวทางลดผลกระทบต่อการให้บริการลูกค้าของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

12.6 การบริหารจัดการการตั้งค่าระบบ (system configuration management)

กรณีบุคคลภายนอกมีหน้าที่เปลี่ยนแปลงการตั้งค่าระบบงาน สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดมาตรฐานการตั้งค่าระบบงานให้ปลอดภัยเพียงพอตามมาตรฐานด้านความปลอดภัยเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เช่น ค่า system configuration ของระบบปฏิบัติการ และการตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย เป็นต้น

12.7 การบริหารจัดการขีดความสามารถของระบบ (capacity management)

(1) มีกระบวนการติดตาม ประเมินประสิทธิภาพและความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ ของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเพียงพอและต่อเนื่อง ตลอดจนรายงานผลการติดตามและประเมินดังกล่าวให้คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมใช้และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

(2) กำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (threshold และ trigger) ในระดับต่าง ๆ และกำหนดกระบวนการรายงานและแจ้งเตือน ปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการให้บริการหรือเชื่อมต่อกับบุคคลภายนอก แนวทางการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง ให้เพียงพอเหมาะสมตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของบริการ เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจทราบอย่างทันการณ์

12.8 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

ดูแลให้มั่นใจว่าบุคคลภายนอกมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัยเพื่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้

งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

12.9 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring)

(1) ดูแลบุคคลภายนอกให้ติดตามดูแลระบบและเฝ้าระวังภัยคุกคามอย่างรัดกุมเพียงพอและต่อเนื่อง รวมทั้งระบบ/บริการที่มีนัยสำคัญ ควรมีการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยทั้งในระดับ system network และ application เพื่อรับมือภัยคุกคามได้อย่างทันการณ์

(2) จัดให้มีการวิเคราะห์ข้อมูลบันทึกเหตุการณ์ (logging) ของระบบ/บริการที่ใช้หรือเชื่อมต่อกับบุคคลภายนอก เพื่อป้องกันและตรวจจับการบุกรุก

12.10 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing)

(1) ดูแลให้บุคคลภายนอกมีการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing) ตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไปและสอดคล้องกับนโยบายระเบียบวิธีปฏิบัติของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

(2) สอบทานขอบเขตและผลการทดสอบเจาะระบบ (penetration testing) ของบุคคลภายนอก เพื่อให้มั่นใจว่าการทดสอบดังกล่าวครอบคลุมระบบทั้งหมดที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการหรือเชื่อมต่อกับบุคคลภายนอก และครอบคลุมภัยคุกคามที่สำคัญ

12.11 การสำรองข้อมูล (data backup)

กรณีที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการหรือเชื่อมต่อกับบุคคลภายนอก ซึ่งมีการจัดเก็บข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือข้อมูลลูกค้า สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดมาตรฐานวิธีปฏิบัติในการสำรองข้อมูลให้บุคคลภายนอกปฏิบัติให้สอดคล้องกับมาตรฐานของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ โดยครอบคลุม

- ขอบเขต/รายละเอียดของการสำรองข้อมูลและรอบเวลาสำรองข้อมูล
- วิธีการ/เทคโนโลยีการสำรองข้อมูล และรูปแบบข้อมูล (data format)
- ระยะเวลาในการเก็บรักษาข้อมูลสำรอง
- การตรวจสอบความถูกต้องครบถ้วนของข้อมูลสำรอง
- ขั้นตอนและวิธีการกู้ข้อมูล
- การสอบทานการสำรองข้อมูล (restore)
- สถานที่จัดเก็บข้อมูลสำรอง

12.12 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT incident management)

(1) ระบุหน้าที่และความรับผิดชอบของสถาบันการเงินและสถาบันการเงินเฉพาะกิจและบุคคลภายนอกอย่างชัดเจน ในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ รวมถึงกำหนดระดับความรุนแรงของเหตุการณ์ผิดปกติดังกล่าว และกำหนดให้แจ้งสถาบันการเงินและสถาบัน

การเงินเฉพาะกิจทราบเหตุการณ์ผิดปกติที่เกิดขึ้นและเกี่ยวข้องกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างเพียงพอและทันการณ์

(2) หากเหตุการณ์ผิดปกติที่เกิดขึ้นนั้นมีผลกระทบต่อการดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างมีนัยสำคัญ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ

(3) กำหนดให้บุคคลภายนอกจัดให้มีช่องทาง ระบบ หรือเครื่องมือเพื่อรองรับกรณี สถาบันการเงินและสถาบันการเงินเฉพาะกิจตรวจพบและต้องการรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศให้บุคคลภายนอกทราบ และเพื่อช่วยให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจติดตามสถานการณ์และการแก้ไขของบุคคลภายนอกต่อเหตุการณ์ผิดปกติที่เกี่ยวข้องกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจได้อย่างทันการณ์

(4) กำหนดให้บุคคลภายนอกมีผู้ประสานงานอย่างเป็นทางการ เพื่อประสานงานกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจในการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศได้อย่างทันการณ์

12.13 การบริหารความต่อเนื่องทางธุรกิจ (business continuity management)

(1) มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (disaster recovery plan) ที่ครอบคลุมถึงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้มีแนวทางรองรับต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างมีนัยสำคัญ เพื่อสามารถให้บริการและดำเนินธุรกิจได้อย่างต่อเนื่อง

(2) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรคำนึงถึงปัจจัยสำคัญหรือความเสี่ยงที่อาจเกิดขึ้นและส่งผลต่อการหยุดชะงักจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ผลกระทบที่มีต่อการให้บริการและดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และการติดต่อสื่อสารระหว่างบุคคลภายนอกกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจ รวมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติให้คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างทันการณ์ตามความสำคัญและระดับความรุนแรงหรือผลกระทบของเหตุการณ์

(3) ประเมินและทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของบุคคลภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ เช่น ความสอดคล้องกันของขอบเขต คำนิยามและการกำหนดระยะเวลาที่สำคัญ : maximum tolerable period of disruption (MTPD), recovery time objective (RTO) และ recovery point objective (RPO) เป็นต้น

(4) หากสถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถเข้าร่วมทดสอบกับบุคคลภายนอกได้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรเข้าร่วมทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศกับบุคคลภายนอก

เพื่อประเมินความพร้อมของบุคคลภายนอกในการกู้คืนระบบงานตามกรอบ MTPD, RTO และ RPO ที่กำหนดไว้

(5) ทีมบริหารจัดการในสภาวะวิกฤติ (crisis management team) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจควรได้รับทราบถึงรายละเอียดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของบุคคลภายนอก เพื่อเตรียมความพร้อมในการบริหารจัดการในส่วนที่เกี่ยวข้อง

(6) รวบรวมปัญหาที่พบระหว่างการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และปรับปรุงแก้ไขร่วมกับบุคคลภายนอก

ส่วนที่ 3 : การใช้บริการ public cloud computing กับระบบงานสำคัญ

กรณีที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีความประสงค์จะนำระบบงานที่มีนัยสำคัญไปใช้บริการ public cloud computing จากบุคคลภายนอก เช่น ระบบ core banking สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรปฏิบัติเพิ่มเติมจากแนวปฏิบัติการบริหารจัดการบุคคลภายนอกข้างต้น ดังนี้

1. ต้องมีความเข้าใจและสามารถประเมินระดับความเสี่ยงที่จะเกิดขึ้นจากการใช้บริการ public cloud computing จากบุคคลภายนอกด้านงานเทคโนโลยีที่มีนัยสำคัญ โดยอย่างน้อยควรครอบคลุมความเสี่ยงสำคัญ ดังนี้
    - ความเสี่ยงด้านกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง
    - ความเสี่ยงจากการหยุดให้บริการของบุคคลภายนอก
    - ความเสี่ยงด้านการรักษาความปลอดภัยของบุคคลภายนอก
    - ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง (third party/ vendor locked-in)
    - ความเสี่ยงข้อมูลที่ไม่ถูกทำลายอย่างสมบูรณ์จากระบบของบุคคลภายนอกเมื่อมีการเปลี่ยนแปลงบุคคลภายนอกหรือนำกลับมาทำเองไม่สมบูรณ์หรือไม่ครบถ้วน
    - ความเสี่ยงจากการกระจุกตัว
    - ความเสี่ยงจากการใช้บริการจากผู้ให้บริการในต่างประเทศ
    - ความเสี่ยงจากการที่ผู้ให้บริการ cloud computing หยุดชะงัก
2. กำหนดปัจจัยในการคัดเลือกบุคคลภายนอกก่อนใช้บริการ โดยอย่างน้อยควรครอบคลุมปัจจัย ดังนี้
    - ปัจจัยด้านความเสี่ยงของประเทศที่บุคคลภายนอกที่จัดเก็บหรือประมวลผลข้อมูลบนระบบ cloud computing
    - ปัจจัยด้านการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง
    - ปัจจัยด้านความยืดหยุ่นในการเปลี่ยนแปลงระบบงานไปยังบุคคลภายนอกรายอื่นหรือการเชื่อมโยงกับระบบอื่นได้
3. กำหนดให้บุคคลภายนอกระบุสถานที่ในการประมวลผล จัดเก็บข้อมูล หรือดำเนินการอื่นใดที่เกี่ยวข้องกับข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
4. กรณีใช้บริการ public cloud computing จากบุคคลภายนอกในต่างประเทศ สถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรจัดให้มีกระบวนการสำรองข้อมูล พร้อมทั้งข้อมูลสำรองไว้ในประเทศหรือในประเทศอื่นที่มิใช่ประเทศผู้ให้บริการ รวมทั้งสอบทานข้อมูลดังกล่าว อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อมูลมีความพร้อมใช้และสามารถนำมาใช้งานได้

5. จัดให้มีการเข้ารหัสข้อมูลสำคัญด้วยมาตรฐานสากลทั้งข้อมูลที่อยู่ในลักษณะ data-in-transit และ data-at-rest เมื่อจัดเก็บและประมวลผลบนระบบ public cloud computing ของบุคคลภายนอก
6. จัดให้มีกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศโดยอ้างอิงแนวปฏิบัติที่ดีของบุคคลภายนอก หรือมาตรฐานสากล รวมทั้งสอบทานการตั้งค่าดังกล่าวอย่างสม่ำเสมอ
7. มีกระบวนการติดตามเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ที่เกิดกับระบบที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการ cloud computing อย่างสม่ำเสมอ และมีการกำหนดแนวทางป้องกันภัยคุกคามดังกล่าว เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นก่อนที่บุคคลภายนอกจะสามารถแก้ไขปัญหาหรือดำเนินการ patch แล้วเสร็จ
8. เมื่อสิ้นสุดหรือยกเลิกการใช้บริการ cloud computing ในระบบงานที่มีนัยสำคัญจากบุคคลภายนอก สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องนำข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจหรือข้อมูลของลูกค้ากลับมาจากบุคคลภายนอก และลบหรือทำลายข้อมูลทั้งหมดที่อยู่กับบุคคลภายนอกอย่างครบถ้วน โดยบุคคลภายนอกต้องไม่สามารถกู้คืนข้อมูลได้
9. แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ครอบคลุมการใช้บริการ cloud computing ในระบบงานที่มีนัยสำคัญจากบุคคลภายนอก โดยควรคำนึงถึงเหตุการณ์ที่อาจส่งผลกระทบรุนแรงหรือเลวร้ายที่สุด (worst case scenario) อย่างน้อยครอบคลุมเหตุการณ์ ดังนี้
   (1) ระบบงานของบุคคลภายนอกใน region ที่ใช้บริการอยู่หยุดชะงักจนเป็นเหตุให้บริการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ไม่สามารถให้บริการได้อย่างต่อเนื่อง เช่น hardware และ software ที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการจากบุคคลภายนอกได้รับเสียหายทั้งหมด management console ถูกโจมตี เป็นต้น

   (2) ระบบงานของบุคคลภายนอกทุก region หยุดชะงักจนเป็นเหตุให้บริการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจไม่สามารถให้บริการได้อย่างต่อเนื่อง

   (3) สายสื่อสารระหว่างสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และบุคคลภายนอกขัดข้องทุกช่องทางจนไม่สามารถใช้บริการได้

เอกสารอ้างอิง

- ISO/IEC 27017:2016 Information technology - Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for Cloud services ของ the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- ISO/IEC 27036:2014 Information technology - Security techniques – Information Security for Supplier Relationship ของ the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Vendor Management Using COBIT 5 ของ Information Systems Audit and Control Association Inc. (ISACA)
- Special Publication 800-146 Cloud Computing Synopsis and Recommendation ของ National Institute of Standards and Technology (NIST)
- Cloud Controls Matrix Version 3.0.1 ของ Cloud Security Alliance
- Third-Party Relationships ของ Office of the Comptroller of the Currency (OCC) สหรัฐอเมริกา
- FG16/5: Guidance for firms outsourcing to the ‘cloud’ and other third party IT services ของ Financial Conduct Authority (FCA) สหราชอาณาจักร
- Cyber Resilience: Range of Practices ของ Basel Committee on Banking Supervision

ธนาคารแห่งประเทศไทย