ธนาคารแห่งประเทศไทย

8 กุมภาพันธ์ 2564

เรียน ผู้จัดการ

ผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ที่มิใช่สถาบันการเงิน

ที่ ธปท.ฝตท.(01) ว. 150 /2564 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน

ธนาคารแห่งประเทศ (ธปท.) ขอนำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน ลงวันที่ 18 มกราคม 2564 ซึ่งได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไปเล่ม 138 ตอนพิเศษ 22 ง ลงวันที่ 29 มกราคม 2564 และมีผลบังคับใช้ตั้งแต่วันที่ 29 เมษายน 2564 เป็นต้นไป

สาระสำคัญของประกาศฉบับนี้ คือ มุ่งหมายให้ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงินที่ไม่ใช่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจ (ผู้ประกอบธุรกิจ) มีการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อรับมือภัยคุกคามทางไซเบอร์ รวมถึงดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแบ่งหลักเกณฑ์ที่สำคัญออกเป็น 2 ส่วน ดังนี้

1. การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) ซึ่งเป็นมาตรการขั้นต้นที่ผู้ประกอบธุรกิจทุกรายต้องดำเนินการ เพื่อยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่สำคัญ

2. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ซึ่งจะมุ่งเน้นให้ผู้ประกอบธุรกิจที่มีนัยสำคัญ ซึ่งมีคุณสมบัติตามที่ประกาศนี้กำหนดถือปฏิบัติโดยดูแลให้มีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และบริหารความเสี่ยงอย่างเหมาะสม

อนึ่ง ธปท. ขอนำส่งแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management implementation guideline) และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management implementation guideline) ซึ่งมีหลักการที่สอดคล้องกับประกาศฉบับนี้มาพร้อมกัน เพื่อให้ผู้ประกอบธุรกิจใช้เป็นแนวทางในการกำหนดวิธีปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงการบริหารจัดการความเสี่ยงจากบุคคลภายนอก โดยให้ผู้ประกอบธุรกิจพิจารณาปรับใช้อย่างเหมาะสมตามลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีที่นำมาใช้และความเสี่ยงที่เกี่ยวข้อง

ทั้งนี้ ผู้ประกอบธุรกิจต้องประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศตามประกาศฉบับนี้ พร้อมจัดส่งผลการประเมินต่อ ธปท. เป็นประจำทุกปี ตามรูปแบบที่กำหนด โดยขอให้ (1) ผู้บริหารหรือผู้ที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) หรือผู้บริหารหรือผู้ที่ทำหน้าที่กำกับการปฏิบัติตามหลักเกณฑ์ (compliance) และ (2) ผู้บริหารหรือผู้ที่ทำหน้าที่ตรวจสอบภายใน (internal audit) รับรองผลการประเมินตนเองก่อนนำส่งต่อ ธปท.

ตารางสรุปสาระสำคัญของหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

<table>
<tr><td rowspan="2"></td><td colspan="2">หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)</td></tr>
<tr><td>Cyber Hygiene</td><td>IT Risk Management</td></tr>
<tr><td>ขอบเขตการบังคับใช้</td><td>ผู้ประกอบธุรกิจทุกราย</td><td>ผู้ประกอบธุรกิจที่มีนัยสำคัญ ซึ่งมีคุณสมบัติตามข้อ 3.2 ของประกาศ</td></tr>
<tr><td>วันเริ่มต้นบังคับใช้</td><td>90 วันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป</td><td>1 ปี นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป</td></tr>
<tr><td rowspan="2">การแจ้งหรือรายงานต่อ ธปท.</td><td colspan="2">1. การแจ้งการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ
2. การรายงานปัญหาด้านเทคโนโลยีสารสนเทศ
3. การรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ</td></tr>
<tr><td>-</td><td>4. การรายงานบุคคลภายนอกที่มีนัยสำคัญ
5. การรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ</td></tr>
</table>

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวสิริธิดา พนมวัน ณ อยุธยา)
ผู้ช่วยผู้ว่าการ สายนโยบายระบบการชำระเงิน
และเทคโนโลยีทางการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. ภาพรวมโครงสร้างและประกาศธนาคารแห่งประเทศไทย ที่ สนช. 1/2564 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน
2. แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
3. แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6346
E-Mail ITSupervision@bot.or.th

หมายเหตุ [X] ธปท. จัดประชุมชี้แจงในวันที่ 22-23 มิถุนายน 2563 และ 29-30 ตุลาคม 2563 ณ ธปท.
[ ] ไม่มีการประชุมชี้แจง

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ประกาศหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน

บังคับใช้กับทุกราย

1 การรักษาความมั่นคงปลอดภัยของระบบ IT ขั้นต้นที่จำเป็น (Cyber Hygiene)

1. การตั้งค่าระบบ ให้มีความปลอดภัย (Security Baseline and Hardening)
กำหนดและตั้งค่าให้สอดคล้องกับมาตรฐานสากล และสภาพแวดล้อมด้าน IT
ประกาศข้อ 5.1.1

2. การป้องกันระบบจาก Malware (Malware Protection)
ตรวจจับและป้องกัน malware ได้เท่าทันภัยคุกคาม
ประกาศข้อ 5.1.2

3. การบริหารจัดการช่องโหว่ (Security Patch Management)
กำหนดกระบวนการบริหารจัดการ security patch
ประกาศข้อ 5.1.3

4. การจัดการสิทธิสูงของระบบ (Privilege User ID Management)
ควบคุมและจำกัดการใช้บัญชีผู้ใช้สิทธิสูงอย่างเข้มงวด
ประกาศข้อ 5.1.4

5. การพิสูจน์ตัวตนอย่างปลอดภัย (Multi – Factor Authentication)
มีการพิสูจน์ตัวตนแบบ MFA ในบัญชีผู้ใช้สิทธิสูง และบัญชีผู้ใช้งานที่มีความเสี่ยง
ประกาศข้อ 5.1.5

6. การทดสอบหาช่องโหว่ (Vulnerability Management & Pentest)
ประเมินช่องโหว่และทดสอบเจาะระบบอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
ประกาศข้อ 5.1.6

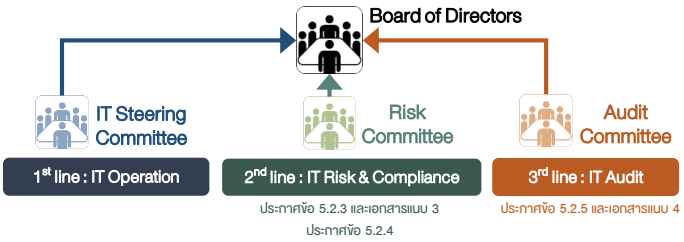
บังคับใช้กับรายนัยสำคัญ

2 การบริหารจัดการความเสี่ยงด้าน IT (IT Risk Management)

IT Governance

ดูแลให้มีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการบริหารความเสี่ยงด้าน IT ที่เหมาะสม ตามระดับความเสี่ยง และจัดโครงสร้างการกำกับดูแลสอดคล้องตามหลัก 3rd line of defence

- บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ
- โครงสร้างการกำกับดูแล
- นโยบายการกำกับดูแลความเสี่ยงด้าน IT
- การบริหารจัดการบุคลากร
- การสร้างความตระหนักถึงความเสี่ยงด้าน IT



ประกาศข้อ 5.2.1 และเอกสารแนบ 1

IT Security

รักษาความมั่นคงปลอดภัยด้าน IT อย่างรัดกุมตามกรอบหลักการ Confidentiality Integrity Availability

- IT asset management
- information security
- access control
- physical and environmental security
- communications security
- IT operations security
- system acquisition and development
- IT incident and problem management
- IT disaster recovery plan
- third party risk management

ประกาศข้อ 5.2.2 และเอกสารแนบ 2

IT Project Management

บริหารจัดการความเสี่ยงของการดำเนินโครงการด้าน IT อย่างมีประสิทธิภาพ

- project management framework
- การเริ่มโครงการ
- การดำเนินการและควบคุมโครงการ
- การปิดโครงการ
- การสอบทานโครงการ

ประกาศข้อ 5.2.6 และเอกสารแนบ 5

ประกาศธนาคารแห่งประเทศไทย

ที่ สนช. 1 /2564

เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน

---

1. เหตุผลในการออกประกาศ

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) มีบทบาทสำคัญต่อการดำเนินธุรกิจและการให้บริการของผู้ประกอบธุรกิจภายใต้กฎหมายว่าด้วยระบบการชำระเงิน โดยนำมาใช้เป็นโครงสร้างพื้นฐานสำคัญที่ช่วยเพิ่มประสิทธิภาพ ลดต้นทุนในการดำเนินงาน รวมถึงอำนวยความสะดวกและรวดเร็วมากยิ่งขึ้น อย่างไรก็ตาม หากขาดการบริหารจัดการที่ดีอาจก่อให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) และภัยคุกคามทางไซเบอร์ (cyber threats) ที่ส่งผลกระทบต่อความเชื่อมั่นของผู้ใช้บริการ รวมทั้งต่อระบบการชำระเงินของประเทศได้

ธนาคารแห่งประเทศไทย (ธปท.) จึงกำหนดหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเพิ่มเติมจากหลักเกณฑ์การกำกับดูแลระบบเทคโนโลยีสารสนเทศที่ใช้บังคับอยู่ในปัจจุบัน เพื่อให้ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน มีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงดังกล่าวอย่างเหมาะสม โดยหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศตามประกาศนี้ ประกอบด้วย 2 ส่วนสำคัญ ได้แก่

1. การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) ซึ่งเป็นมาตรการขั้นต้นที่ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับทุกรายต้องดำเนินการ เพื่อยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่สำคัญ

2. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ซึ่งจะมุ่งเน้นให้ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญ ซึ่งมีคุณสมบัติตามที่ประกาศฉบับนี้กำหนด ต้องปฏิบัติโดยมีหลักเกณฑ์ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม มีโครงสร้างองค์กร องค์ประกอบและการกำหนดบทบาทหน้าที่ของคณะกรรมการเพื่อกำหนดนโยบายในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตลอดจนกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการให้บริการหรือดำเนินธุรกิจ

ฝตทป90-กส65038-256401

กส65038 วันที่ 18 ม.ค. 2564

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 7 มาตรา 24 มาตรา 25 มาตรา และ 26 แห่งพระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 ธนาคารแห่งประเทศไทยกำหนดหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ให้ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับถือปฏิบัติตามที่กำหนดในประกาศนี้

3. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน ที่มิใช่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน โดยแบ่งเป็น 2 ส่วน ได้แก่

3.1 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) บังคับใช้กับผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับทุกรายต้องดำเนินการ

3.2 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) บังคับใช้กับผู้ให้บริการและผู้ประกอบธุรกิจ ดังต่อไปนี้

(1) ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ

(2) ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ

(3) ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีคุณสมบัติ ดังต่อไปนี้

(3.1) เชื่อมต่อโดยตรงกับระบบการชำระเงินภายใต้การกำกับ หรือเชื่อมต่อกับผู้ให้บริการแก่ผู้รับบัตร (acquirer) หรือเชื่อมต่อกับธนาคารที่ให้บริการเชื่อมต่อระบบ (sponsor bank)

(3.2) ให้บริการทางการเงินแก่ลูกค้าผ่านเครือข่ายสื่อสารสาธารณะ (Internet facing)

(3.3) มีบัญชีผู้ใช้งานมากกว่า 5 ล้านบัญชี หรือมีปริมาณธุรกรรมมากกว่า 10 ล้านรายการต่อปี

ทั้งนี้ ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับต้องจัดให้มีการประเมินตนเองเป็นรายปี โดยใช้ข้อมูลประกอบการประเมิน ณ วันสิ้นปีปฏิทิน ว่าเป็นผู้มีคุณสมบัติครบถ้วนตามข้อ (3.1) - (3.3) ข้างต้นหรือไม่ หากผลการประเมินปรากฏว่ามีคุณสมบัติครบถ้วนตามหลักเกณฑ์ดังกล่าว ให้แจ้งผลการประเมินให้ ธปท. ทราบภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน และให้ถือปฏิบัติ ดังนี้

(1) กรณีผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับรายเดิมที่ประเมินตนเองแล้ว ยังคงมีคุณสมบัติครบถ้วนทั้งสามข้อดังกล่าว ให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามข้อ 5.2 ต่อเนื่องต่อไป

(2) สำหรับผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับรายใหม่ที่ประเมินตนเองแล้วปรากฏว่ามีคุณสมบัติครบถ้วนทั้งสามข้อดังกล่าว ให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามข้อ 5.2 ภายใน 1 ปีนับแต่วันสิ้นปีปฏิทินของปีที่มีการประเมิน

สำหรับผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับที่เป็นนิติบุคคลต่างประเทศที่ต้องปฏิบัติตามหลักเกณฑ์หรือกฎหมายการกำกับดูแลของประเทศนั้น ๆ ให้จัดเตรียมข้อมูลที่เกี่ยวข้องตามข้อ 5 ข้อ 6 และข้อ 7.3 - 7.5 ไว้ให้เป็นปัจจุบันเพื่อให้พร้อมสำหรับการตรวจสอบของ ธปท. หรือเมื่อ ธปท. ร้องขอ และยกเว้นการปฏิบัติตามข้อ 7.1

4. 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 ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของผู้ให้บริการและผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threats)

“ระบบการชำระเงินที่มีความสำคัญ” หมายความว่า ระบบการชำระเงินที่ ธปท. จัดตั้งและดำเนินการตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย หรือระบบการชำระเงินอื่นใดที่รัฐมนตรีประกาศกำหนดโดยคำแนะนำของ ธปท. ตามกฎหมายว่าด้วยระบบการชำระเงิน

“ผู้ให้บริการ” หมายความว่า ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญตามกฎหมายว่าด้วยระบบการชำระเงิน

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงินที่มิใช่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“สถาบันการเงิน” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“รัฐวิสาหกิจ” หมายความว่า รัฐวิสาหกิจที่มีกฎหมายเฉพาะจัดตั้งขึ้น

“นิติบุคคลต่างประเทศ” หมายความว่า นิติบุคคลที่จดทะเบียนจัดตั้งขึ้นตามกฎหมายต่างประเทศและประกอบธุรกิจหรือให้บริการระบบการชำระเงินในประเทศไทย

“สมาชิก” หมายความว่า ผู้ใช้บริการที่ยินยอมผูกพันตามหลักเกณฑ์ในการใช้บริการระบบการชำระเงินที่มีความสำคัญ

“ผู้ใช้บริการของระบบ” หมายความว่า ผู้ใช้บริการที่เป็นสมาชิกและยินยอมผูกพันตามหลักเกณฑ์ในการใช้บริการของระบบการชำระเงินภายใต้การกำกับ

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศแทนผู้ให้บริการและผู้ประกอบธุรกิจ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ให้บริการและผู้ประกอบธุรกิจ หรือข้อมูลของสมาชิกหรือลูกค้าที่ควบคุมดูแลโดยผู้ให้บริการและผู้ประกอบธุรกิจได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงสมาชิกหรือลูกค้าที่ใช้ผลิตภัณฑ์และบริการของผู้ให้บริการและผู้ประกอบธุรกิจ

“ธปท.” หมายความว่า ธนาคารแห่งประเทศไทยตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

5. หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

5.1 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene)

ผู้ให้บริการและผู้ประกอบธุรกิจทุกรายต้องปฏิบัติตามหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็นเพื่อยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่สำคัญ ลดความเสี่ยงหรือผลกระทบต่อสมาชิก ผู้ใช้บริการของระบบหรือลูกค้า และต่อระบบชำระเงินโดยรวม ผู้ให้บริการและผู้ประกอบธุรกิจต้องดำเนินการดังนี้

5.1.1 การกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (security baseline and hardening)

กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และตั้งค่าการรักษาความมั่นคงปลอดภัยสอดคล้องกับการให้บริการ (security hardening) ให้ครอบคลุมระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน

(application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้งดำเนินการและสอบทานตามที่ได้กำหนดไว้

หากมีเหตุที่ผู้ให้บริการและผู้ประกอบธุรกิจไม่สามารถปฏิบัติตามมาตรฐานที่กำหนดไว้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

5.1.2 การป้องกันภัยจากโปรแกรมไม่ประสงค์ดี (malware protection)

จัดให้มีเครื่องมือสำหรับป้องกันภัยจาก malware รวมทั้งติดตามให้มีการปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตีโดย malware

5.1.3 การบริหารจัดการ security patch (security patch management)

จัดให้มีกระบวนการบริหารจัดการ security patch สำหรับทุกระบบงานและอุปกรณ์ เพื่อเป็นการลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่และระดับความสำคัญของระบบงาน

หากมีเหตุที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ ผู้ให้บริการและผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

อย่างไรก็ตาม กรณีที่ไม่สามารถติดตั้ง security patch ได้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

5.1.4 การบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิสูง (privilege user management)

กำหนดมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานที่มีสิทธิสูงอย่างเข้มงวด เช่น การมอบหมายสิทธิ การเบิกใช้ กำหนดระยะเวลาการใช้งาน การสอบทานหลังการใช้ การกำหนดรหัสผ่านที่รัดกุมของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย เพื่อป้องกันการนำบัญชีผู้ใช้งานที่มีสิทธิสูงไปใช้โดยไม่ได้รับอนุญาต

5.1.5 การพิสูจน์ตัวตนแบบ multi-factor authentication

จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้

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

(2) บัญชีผู้ใช้งาน (user) ทุกบัญชีที่สามารถเข้าถึงข้อมูลลูกค้าของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายที่เชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing)

หากมีเหตุที่ระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication ผู้ให้บริการและผู้ประกอบธุรกิจสามารถใช้วิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย

อย่างไรก็ตาม กรณีที่ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

5.1.6 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing)

จัดให้มีการประเมินช่องโหว่ (vulnerability assessment) สำหรับทุกระบบงานตามระดับความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระ ครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบ ความเสี่ยง หรือมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ อย่างมีนัยสำคัญ ทั้งนี้ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

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

นอกจากผู้ให้บริการและผู้ประกอบธุรกิจต้องดำเนินการตามข้อ 5.1.1 – 5.1.6 แล้ว ยังต้องปฏิบัติตามข้อ 6 และข้อ 7 ของประกาศฉบับนี้ในเรื่องการจัดทำข้อกำหนดเพื่อพิจารณาความมีนัยสำคัญในเรื่องต่าง ๆ เช่น ระบบงาน การเปลี่ยนแปลงเทคโนโลยีสารสนเทศ หรือเหตุการณ์ปัญหาที่เกิดขึ้น และเรื่องการแจ้งหรือนำส่งรายงานตามที่กำหนดด้วย

5.2 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

ผู้ให้บริการและผู้ประกอบธุรกิจที่เข้าเงื่อนไขตามที่กำหนดในข้อ 3 ให้ดำเนินการยกระดับการดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการให้บริการ

ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพและรัดกุม ประกอบด้วย 6 เรื่อง คือ ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit) และ การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management) ดังนี้

5.2.1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)

จัดให้มีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ตั้งแต่คณะกรรมการและผู้บริหารระดับสูงที่ให้ความสำคัญในการผลักดันและยกระดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำหนดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ สื่อสารและกำกับดูแลให้มีการปฏิบัติตามนโยบายที่กำหนด นอกจากนี้ต้องจัดให้มีผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งสร้างวัฒนธรรมและพฤติกรรมร่วมของทุกคนในองค์กรให้ตระหนักถึงความเสี่ยงอย่างต่อเนื่อง (รายละเอียดในเอกสารแนบ 1)

5.2.2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

จัดให้มีการบริหารจัดการและควบคุมระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีความปลอดภัย ถูกต้องเชื่อถือได้ และพร้อมใช้งาน โดยนำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ (รายละเอียดในเอกสารแนบ 2)

5.2.3 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

จัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างครอบคลุมทั่วทั้งองค์กรและเหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ โดยกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมโครงสร้างองค์กร บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (รายละเอียดในเอกสารแนบ 3)

5.2.4 การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

กำกับดูแลให้ปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (IT compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วย

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

5.2.5 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบที่มีความเป็นอิสระ รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยงและการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศที่เพียงพอ (รายละเอียดในเอกสารแนบ 4)

5.2.6 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

กำหนดกรอบการบริหารจัดการโครงการ (project management framework) และโครงสร้างการกำกับดูแลโครงการ เพื่อให้โครงการที่มีนัยสำคัญมีการบริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดให้มีประสิทธิภาพสูงสุด สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงาน และบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้ (รายละเอียดในเอกสารแนบ 5)

6. ข้อกำหนดในการพิจารณาความมีนัยสำคัญเพื่อดำเนินการตามประกาศนี้

ผู้ให้บริการและผู้ประกอบธุรกิจต้องมีข้อกำหนดถึงความมีนัยสำคัญที่ชัดเจนเพื่อใช้พิจารณาดำเนินการในเรื่องต่าง ๆ ที่กำหนดไว้ตามประกาศฉบับนี้ โดยดำเนินการดังนี้

6.1 ข้อกำหนดต้องผ่านการพิจารณาความมีนัยสำคัญร่วมกันของหน่วยงานที่เกี่ยวข้อง โดยเฉพาะหน่วยงานซึ่งทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (first line of defence) และหน่วยงานซึ่งทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (second line of defence) รวมทั้งต้องได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย

6.2 ข้อกำหนดในการพิจารณาความมีนัยสำคัญ ต้องพิจารณาภายใต้กรอบหลักการที่คำนึงถึงความเสี่ยงและผลกระทบต่อการให้บริการหรือดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจในวงกว้าง (enterprise wide impact) และผลกระทบต่อระบบการชำระเงินในวงกว้าง (payment system wide impact)

6.3 ต้องสื่อสารและเผยแพร่หลักเกณฑ์ให้หน่วยงานที่เกี่ยวข้องทราบโดยทั่วกันและนำไปปฏิบัติ

6.4 ต้องสอบทานการดำเนินการตามข้อกำหนดอย่างน้อยปีละ 1 ครั้ง

6.5 ต้องทบทวนข้อกำหนดอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจ และระบบการชำระเงิน

7. การแจ้งหรือรายงานต่อ ธปท.

เพื่อให้ ธปท. สามารถกำกับดูแลและติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ และความเสี่ยงของระบบการชำระเงินในภาพรวมได้เท่าทันกับการเปลี่ยนแปลง ปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศหรือภัยคุกคามทางไซเบอร์ ผู้ให้บริการและผู้ประกอบธุรกิจต้องแจ้งหรือรายงานต่อ ธปท. ดังต่อไปนี้

7.1 การแจ้งการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

ผู้ให้บริการต้องแจ้งการนำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ ทั้งกรณีที่ดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต่อ ธปท. ล่วงหน้า 15 วันก่อนดำเนินการตามช่องทางที่ ธปท. กำหนด

ในกรณีที่เป็นผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับหรือผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ให้แจ้งการนำเทคโนโลยีมาใช้หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ ทั้งกรณีที่ดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ตามข้อ 4.2.3 (4.3.2) ของประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และข้อ 4.2.3 (7.2.2) ของประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับด้วย แล้วแต่กรณี

7.2 การรายงานปัญหาด้านเทคโนโลยีสารสนเทศ

ผู้ให้บริการต้องรายงานต่อ ธปท. ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียง รวมถึงกรณีเทคโนโลยีสารสนเทศที่มีนัยสำคัญถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุด โดยผู้ให้บริการต้องรายงานปัญหาหรือเหตุการณ์ดังกล่าวมายัง ธปท. ทันทีเมื่อเกิดเหตุหรือรับรู้ปัญหาหรือเหตุการณ์นั้นตามช่องทางที่ ธปท. กำหนด และแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

ในกรณีที่ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับหรือผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศตามวรรคหนึ่ง ให้รายงานปัญหาด้านเทคโนโลยีสารสนเทศตามข้อ 4.2.3 (5.2.1) ของประกาศว่าด้วย

หลักเกณฑ์การกำกับดูแลการประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และข้อ 4.2.3 (8.3) ของประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับด้วย แล้วแต่กรณี

7.3 การรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญต้องจัดส่งผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งในส่วนของ หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) และหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) สำหรับผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่ไม่เข้าเงื่อนไขตามข้อ 3.2 (3.1) – (3.3) ต้องจัดส่งผลการประเมินเฉพาะหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) โดยจัดส่งผลการประเมินให้ ธปท. ทราบภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน โดยมีรูปแบบและช่องทางตามที่ ธปท. กำหนด

7.4 การรายงานบุคคลภายนอกที่มีนัยสำคัญ

ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญต้องจัดส่งรายงานการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของบุคคลภายนอกที่มีนัยสำคัญเป็น รายไตรมาสตามรูปแบบและช่องทางที่ ธปท. กำหนด

7.5 การรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญต้องจัดส่งรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญเป็นรายไตรมาสตามรูปแบบและช่องทางที่ ธปท. กำหนด ทั้งกรณีที่ดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

8. การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

8.1 กรณีที่ผู้ให้บริการและผู้ประกอบธุรกิจมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ได้ ให้ยื่นขออนุญาตผ่อนผันเป็นรายกรณีต่อ ธปท. ก่อนครบกำหนดระยะเวลาตามที่ประกาศนี้กำหนด พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธปท. จะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ

นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดย ธปท. อาจจะพิจารณาอนุญาตหรือไม่ก็ได้ หรือกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

ทั้งนี้ ในการพิจารณาคำขอผ่อนผัน ธปท. จะพิจารณาตามหลักการเสริมสร้างความมั่นคงของผู้ให้บริการและผู้ประกอบธุรกิจ ซึ่งรวมถึงการกำกับดูแลการบริหารจัดการ การบริหารความเสี่ยง การบริหารความมั่นคงปลอดภัยของผู้ให้บริการและผู้ประกอบธุรกิจให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่องเมื่อเกิดปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อระบบการชำระเงิน ส่งเสริมประสิทธิภาพ สนับสนุนให้มีธรรมาภิบาลที่ดี และคุ้มครองลูกค้าและผู้ใช้บริการ รวมถึงเสถียรภาพของระบบการชำระเงินและระบบเศรษฐกิจ

8.2 ในกรณีที่ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับไม่สามารถปฏิบัติตามข้อ 5.2.1 ได้ ให้ยื่นขอผ่อนผันต่อ ธปท. เป็นรายกรณี พร้อมแสดงเหตุผลและความจำเป็น โดยต้องปฏิบัติดังนี้

(1) กรณีไม่สามารถจัดให้มีกรรมการที่มีความรู้หรือประสบการณ์ด้าน IT ให้จัดหาผู้เชี่ยวชาญด้าน IT เป็นที่ปรึกษาให้คณะกรรมการแทนได้

(2) กรณีไม่สามารถจัดให้มีบุคลากรภายในทำหน้าที่บริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง ให้จัดผู้เชี่ยวชาญภายนอกมาทำหน้าที่ดังกล่าวแทนได้

9. การกำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ สั่งให้แก้ไข เพิกถอน หรือเข้าตรวจสอบ การนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ

ธปท. อาจพิจารณากำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ สั่งให้แก้ไข เพิกถอน หรือเข้าตรวจสอบ การนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ ทั้งกรณีผู้ให้บริการและผู้ประกอบธุรกิจดำเนินการเองและกรณีมีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ตามความจำเป็นเป็นรายกรณี รวมทั้ง ธปท. มีสิทธิเข้าตรวจสอบบุคคลภายนอกดังกล่าวที่มีนัยสำคัญต่อระบบการชำระเงิน หากพบว่าเป็นการดำเนินการที่ส่งผลกระทบต่อประชาชนในวงกว้างหรือความเชื่อมั่นในระบบการชำระเงิน

10. บทเฉพาะกาล

บรรดาประกาศอื่นใดที่ออกภายใต้กฎหมายว่าด้วยระบบการชำระเงินในส่วนที่กำหนดไว้แล้วในประกาศฉบับนี้ หรือซึ่งขัดหรือแย้งกับเนื้อหาในประกาศฉบับนี้ให้ใช้ประกาศฉบับนี้แทน

11. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่ในเรื่องหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ตามข้อ 5.2 เรื่องการรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศตามข้อ 7.3 เรื่องการรายงานบุคคลภายนอกที่มีนัยสำคัญตามข้อ 7.4 และเรื่องการรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญตามข้อ 7.5 ให้ใช้บังคับเมื่อพ้นกำหนด 1 ปี นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 18 มกราคม 2564

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6346

เอกสารแนบ 1

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ
(IT governance)

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ

คณะกรรมการต้องเข้าใจและตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อผู้ให้บริการ ผู้ประกอบธุรกิจ และผู้ที่เกี่ยวข้อง รวมทั้งมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมการดำเนินการและการดูแล ดังต่อไปนี้

1.1 ใช้เทคโนโลยีสารสนเทศที่สอดรับกับกลยุทธ์การให้บริการหรือดำเนินธุรกิจ และยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงต่าง ๆ ในอนาคต

1.2 จัดให้มีนโยบายและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นหนึ่งในความเสี่ยงสำคัญขององค์กร (enterprise wide risk) ทั้งด้านความปลอดภัย ความถูกต้อง และความพร้อมใช้ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ทั้งในภาวะปกติและภาวะวิกฤต รวมทั้งดูแลความเสี่ยงโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญด้วย

1.3 สร้างความรู้และความตระหนักรู้เรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่กรรมการ ผู้บริหาร และพนักงานในองค์กรอย่างต่อเนื่องและมีประสิทธิผล

ทั้งนี้ คณะกรรมการอาจมอบหมายให้คณะกรรมการชุดอื่นหรือผู้บริหารระดับสูงกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ โดยคณะกรรมการยังคงต้องรับผิดชอบในเรื่องดังกล่าว

นอกจากนี้ คณะกรรมการต้องมีกรรมการอย่างน้อย 1 คนที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศเพื่อทำหน้าที่กำกับดูแลเทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจ อย่างไรก็ดี สำหรับผู้ให้บริการและผู้ประกอบธุรกิจซึ่งเป็นนิติบุคคลที่เป็นหน่วยงานของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้นนั้น คณะกรรมการอาจมอบหมายให้คณะกรรมการชุดอื่น ซึ่งต้องมีกรรมการอย่างน้อย 1 คน ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศทำหน้าที่แทนได้

2. โครงสร้างการกำกับดูแล

2.1 โครงสร้างองค์กรในการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

ผู้ให้บริการและผู้ประกอบธุรกิจต้องจัดให้มีโครงสร้างองค์กรต้องเอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ

3 ระดับ (three lines of defence) โดยแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่างการทำหน้าที่ (1) ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (2) บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และ (3) ตรวจสอบด้านเทคโนโลยีสารสนเทศ นอกจากนี้ต้องมีการถ่วงดุลอำนาจกันอย่างอิสระ โดยเฉพาะการทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องมีความเป็นอิสระจากการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

2.2 คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ผู้ให้บริการและผู้ประกอบธุรกิจต้องมีคณะกรรมการ ดังต่อไปนี้

2.2.1 คณะกรรมการที่ทำหน้าที่บริหารจัดการ และกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee

2.2.2 คณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

2.2.3 คณะกรรมการที่ทำหน้าที่กำกับดูแลให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการตรวจสอบการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

2.3 การกำหนดผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.3.1 ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ผู้ให้บริการและผู้ประกอบธุรกิจควรมีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์ และมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งกำหนดบทบาทหน้าที่และความรับผิดชอบ อย่างน้อยดังนี้

- มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

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

- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงขององค์กร และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการเป็นวาระประจำ

- ดูแลและดำเนินการให้มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้ และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และภัยคุกคาม ทางไซเบอร์

2.3.2 ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer : CISO)

นอกเหนือจากการจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามข้อ 2.3.1 แล้ว ผู้ให้บริการและผู้ประกอบธุรกิจอาจพิจารณาจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer : CISO) เพิ่มเติม โดยผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวควรมีความเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ และมีอำนาจหน้าที่เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยต้องดำเนินการอย่างน้อย ดังนี้

- รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด หรือคณะกรรมการที่เกี่ยวข้อง หรือคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ

- ให้ความคิดเห็นในเรื่องภัยคุกคามทางไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการ คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ

3. นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

3.1 ผู้ให้บริการและผู้ประกอบธุรกิจต้องมี (1) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และ (2) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ที่เป็นลายลักษณ์อักษร และอยู่ภายใต้กรอบหลักการการรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity)

และ ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) หรือ CIA โดยนโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการหรือคณะกรรมการที่ได้รับมอบหมายแล้วแต่กรณี และต้องสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีสารสนเทศมาใช้สำหรับให้บริการหรือดำเนินธุรกิจ และนโยบายการบริหารความเสี่ยง รวมทั้งสอดคล้องกับแนวทางการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

นอกจากนี้ การกำหนดนโยบายดังกล่าวต้องคำนึงถึงลักษณะการให้บริการหรือดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศภายในองค์กรและความเสี่ยงจากกรณีมีการใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอกด้วย

3.2 ผู้ให้บริการและผู้ประกอบธุรกิจต้องทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4. การบริหารจัดการบุคลากร

ผู้ให้บริการและผู้ประกอบธุรกิจต้องบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวันอย่างเหมาะสม โดยต้องคำนึงถึงความรู้ความสามารถของบุคลากร ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

4.1 การบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงาน บริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศต้องครอบคลุมในเรื่องกระบวนการคัดเลือกบุคลากรที่มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ ความเพียงพอของบุคลากรที่สอดคล้องกับปริมาณการใช้เทคโนโลยีสารสนเทศ และมาตรการในการสร้างและส่งเสริมความตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ

4.2 ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานหรือระเบียบข้อบังคับภายในองค์กรของบุคลากรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศ

4.3 การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยต้องปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว

5. การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness)

ผู้ให้บริการและผู้ประกอบธุรกิจต้องสื่อสารและให้ความรู้แก่บุคลากรที่ทำหน้าที่ปฏิบัติงานบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ตที่ถูกต้อง และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์

เอกสารแนบ 2

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
(IT security)

ผู้ให้บริการและผู้ประกอบธุรกิจต้องกำหนดให้มีการบริหารจัดการและควบคุมดูแลระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีความปลอดภัย ถูกต้องเชื่อถือได้ และพร้อมใช้งาน ดังต่อไปนี้

1. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

บริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

2. การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

รักษาความมั่นคงปลอดภัยของข้อมูล ทั้งการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ มีการจัดชั้นความลับของข้อมูล (information classification) เก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ รวมทั้งบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากล เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

3. การควบคุมการเข้าถึง (access control)

ควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

4. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

รักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่อง

5. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

รักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของผู้ให้บริการและผู้ประกอบธุรกิจ เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านเครือข่ายสื่อสารมีความมั่นคงปลอดภัย และสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

6. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

รักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

6.1 บริหารจัดการขีดความสามารถของระบบและระบบสาธารณูปโภค (capacity management) เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการให้บริการ หรือดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

6.2 รักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัสหรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่ประสงค์ดี (malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต

6.3 สำรองข้อมูล (data backup) ด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

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

6.5 ติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เช่น เครื่องมือติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้สามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

6.6 บริหารจัดการช่องโหว่ (vulnerability management) โดยจัดให้มีการประเมินช่องโหว่ (vulnerability assessment) สำหรับทุกระบบงานตามระดับความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

6.7 ทดสอบเจาะระบบ (penetration test) โดยจัดให้มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระ ครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบ ความเสี่ยง หรือมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ อย่างมีนัยสำคัญ ทั้งนี้ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

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

6.9 บริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการควบคุมการตั้งค่าของระบบที่ใช้งานจริง และมีการสอบทานการตั้งค่าอย่างสม่ำเสมอ เพื่อป้องกันข้อผิดพลาดในการปฏิบัติงาน

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

7. การจัดหาและการพัฒนาระบบ (system acquisition and development)

7.1 การจัดหาระบบ (system acquisition)

กำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและบุคคลภายนอกที่ให้บริการ เช่น ความน่าเชื่อถือของระบบและบุคคลภายนอกที่ให้บริการที่ได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate) ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ เพื่อให้มั่นใจว่าระบบและบุคคลภายนอกที่ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินการได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการที่เป็นบุคคลภายนอก การเปลี่ยนแปลงเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจในอนาคต

7.2 การพัฒนาระบบ (system development)

ออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยต้องดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- มีเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

- มีกระบวนการหรือเครื่องมือควบคุมเวอร์ชั่นของคำสั่งเขียนโปรแกรม (source code version control)

- แบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบและผู้นำระบบขึ้นใช้งานจริง

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

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

- พัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยต้องมีการทดสอบประสิทธิภาพ (performance test) เมื่อมีการพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์

- มีแนวทางควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

- จัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

8. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)

บริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติ ปัญหา และการแก้ไขให้คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมายในระยะเวลาที่เหมาะสม นอกจากนี้ต้องวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

9. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT disaster recovery plan)

9.1 มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan : IT DRP) อย่างเป็นลายลักษณ์อักษร โดยแผนดังกล่าวต้องเป็นไปตามนโยบายที่กำหนด และได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย

9.2 จัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงลักษณะการให้บริการหรือดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากบุคคลภายนอก (third party risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และความเสี่ยงที่มีผลกระทบต่อระบบการชำระเงิน (systemic risk) เป็นต้น

9.3 แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องมีความเป็นไปได้ในทางปฏิบัติ สามารถนำมาใช้รองรับความเสียหายที่เกิดขึ้นได้จริง โดยการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรครอบคลุมถึงการกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้การให้บริการหรือธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD) เพื่อรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่องของผู้ให้บริการและผู้ประกอบธุรกิจ

9.4 มีคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์และฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้

9.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

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

10. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

ในกรณีที่ผู้ให้บริการและผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้ (1) ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) (2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือ (3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลผู้ใช้บริการของระบบ

ข้อมูลสมาชิก ข้อมูลลูกค้าที่ถูกควบคุมดูแล ผู้ให้บริการและผู้ประกอบธุรกิจต้องกำกับดูแลความเสี่ยง กระบวนการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ ให้สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญบนพื้นฐานที่ต้องรับผิดชอบต่อการให้บริการหรือดำเนินธุรกิจแก่สมาชิก ผู้ใช้บริการระบบ หรือลูกค้า และคงไว้ซึ่งความน่าเชื่อถือชื่อเสียง ประสิทธิภาพในการให้บริการ ตามหลักการดังนี้

10.1 กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างผู้ให้บริการและผู้ประกอบธุรกิจกับบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร และพร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดย ธปท. รวมทั้งต้องระบุให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และ ธปท.มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่มีนัยสำคัญ เป็นเงื่อนไขสัญญาหรือข้อตกลงกับบุคคลภายนอก

ทั้งนี้ ธปท. อาจสั่งให้มีการระบุผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และ ธปท. มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกรายอื่น ๆ เป็นเงื่อนไขในสัญญาหรือข้อตกลงตามความเหมาะสม

10.2 กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ และความเสี่ยงจากการกระจุกตัว (concentration risk) เนื่องจากใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการที่เป็นบุคคลภายนอกเพียงรายเดียว (single provider)

10.3 รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ และอ้างอิงมาตรฐานสากลที่ยอมรับโดยทั่วไป รวมถึงมีการรักษาความปลอดภัยจากภัยไซเบอร์ตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

10.4 เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการให้บริการหรือดำเนินธุรกิจแก่สมาชิก ผู้ใช้บริการของระบบ หรือลูกค้า แล้วแต่กรณี

ทั้งนี้ แนวทางการบริหารจัดการความเสี่ยงบุคคลภายนอกเป็นไปตามแนวปฏิบัติของธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management implementation guideline) โดยให้ผู้ให้บริการและผู้ประกอบธุรกิจสามารถพิจารณาประยุกต์ใช้ให้เหมาะสมและสอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

เอกสารแนบ 3

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(IT risk management)

ผู้ให้บริการและผู้ประกอบธุรกิจต้องกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

1. การประเมินความเสี่ยง

1.1 การระบุความเสี่ยง

ระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

1.2 การวิเคราะห์ความเสี่ยง

เข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

1.3 การประเมินค่าความเสี่ยง

ประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงานและการให้บริการหรือดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

2. การจัดการความเสี่ยง

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) ที่เกี่ยวข้องกับการให้บริการหรือดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

3. การติดตามและทบทวนความเสี่ยง

มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

4. การรายงานความเสี่ยง

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ

ทั้งนี้ ผู้ให้บริการและผู้ประกอบธุรกิจต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

เอกสารแนบ 4

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง การตรวจสอบด้านเทคโนโลยีสารสนเทศ
(IT audit)

ผู้ให้บริการและผู้ประกอบธุรกิจต้องถือปฏิบัติตามหลักเกณฑ์ ดังต่อไปนี้

1. ต้องมีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

2. ต้องมีแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงของการใช้เทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการใช้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก โดยแผนงานและขอบเขตการตรวจสอบดังกล่าวต้องได้รับการอนุมัติจากคณะกรรมการตรวจสอบ และต้องครอบคลุมถึงเทคโนโลยีสารสนเทศที่มีนัยสำคัญ รวมถึงต้องทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าวโดยคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

3. ต้องตรวจสอบด้านเทคโนโลยีสารสนเทศตามแผนงานและขอบเขตที่กำหนดตามข้อ 2 โดยผู้ตรวจสอบภายนอกที่เป็นอิสระ มีความรู้ และประสบการณ์ในการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำหรับงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญควรตรวจสอบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุการณ์ผิดปกติในเทคโนโลยีสารสนเทศที่มีนัยสำคัญ เว้นแต่ กรณีเป็นผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ สามารถดำเนินการตรวจสอบดังกล่าวโดยผู้ตรวจสอบภายในหรือภายนอกที่เป็นอิสระ

ทั้งนี้ ในกรณีที่ ธปท. เห็นว่าผลการตรวจสอบของผู้ประกอบธุรกิจบริการการชำระเงินมีข้อมูลไม่ครบถ้วนหรือมีข้อความคลุมเครือไม่ชัดเจน หรือในกรณีที่ ธปท. เห็นว่าจำเป็นหรือสมควร ธปท. อาจสั่งให้ผู้ประกอบธุรกิจบริการการชำระเงินแต่งตั้งผู้ตรวจสอบภายนอกดำเนินการตรวจสอบและรายงานผลการตรวจสอบให้ ธปท. ทราบ

4. ต้องมีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งผู้ให้บริการและผู้ประกอบธุรกิจเห็นว่ามีความจำเป็นต้องประเมิน แต่มีข้อจำกัด หรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจตามข้อ 1. ไม่สามารถประเมินได้ เช่น การประเมิน

ระบบที่มีความซับซ้อนหรือใช้เทคโนโลยีใหม่ หรือการประเมินความสามารถของระบบในการปรับเปลี่ยนเพื่อรองรับการให้บริการหรือดำเนินธุรกิจในอนาคตภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศที่รวดเร็ว

5. ต้องจัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและเสนอผลการตรวจสอบดังกล่าวต่อคณะกรรมการตรวจสอบ ตลอดจนจัดส่งสำเนาผลการตรวจสอบให้ ธปท. เป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ตามที่กำหนด ภายใน 45 วันนับแต่วันที่ทำการตรวจสอบแล้วเสร็จ

6. ต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานประเด็นสำคัญพร้อมทั้งแผนการปรับปรุงให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้อง

เอกสารแนบ 5

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ
(IT project management)

เมื่อผู้ให้บริการและผู้ประกอบธุรกิจจะจัดทำโครงการด้านเทคโนโลยีสารสนเทศ (IT project management) ที่มีนัยสำคัญ ที่นำมาใช้ในการให้บริการหรือดำเนินธุรกิจ ต้องปฏิบัติตามหลักเกณฑ์ดังต่อไปนี้

1. ศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับสำหรับโครงการที่นำเทคโนโลยีสารสนเทศมาใช้ในการให้บริการหรือดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องพิจารณาเลือกใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม และประเมินความเสี่ยงตลอดจนผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งต้องจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตอำนาจอนุมัติที่กำหนดไว้

2. กำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางบริหารจัดการโครงการ (project management) โดยครอบคลุมขั้นตอนตั้งแต่การเริ่มโครงการ การดำเนินการและการควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ รวมทั้งต้องกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (project governance) โดยอย่างน้อยต้องกำหนดโครงสร้าง ดังต่อไปนี้

2.1 คณะกรรมการที่กำกับดูแลโครงการ เพื่อทำหน้าที่กำกับดูแลความคืบหน้า ให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้การดำเนินงานของโครงการเป็นไปตามแผนงานที่กำหนด ทั้งนี้ คณะกรรมการกำกับดูแลโครงการควรประกอบด้วยผู้บริหารหรือผู้แทนจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้อง

2.2. หน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการ (Project Management Office : PMO) เพื่อทำหน้าที่กำหนดรูปแบบ กระบวนการ และเครื่องมือที่เป็นมาตรฐานในการบริหารจัดการและติดตามความคืบหน้าของโครงการ รวมทั้งรายงานความคืบหน้าและภาพรวมของโครงการที่สำคัญต่อคณะกรรมการที่กำกับดูแลโครงการ เพื่อให้โครงการบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้

2.3 ผู้จัดการโครงการ (project manager) เพื่อทำหน้าที่ในการบริหารจัดการโครงการแต่ละโครงการตามขั้นตอนการบริหารจัดการโครงการ และส่งมอบงานในแต่ละขั้นตอนตามรูปแบบกระบวนการและเครื่องมือ ตามที่หน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการกำหนด เพื่อให้สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานที่กำหนด

คำถาม – คำตอบแนบท้ายประกาศ
เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน
ลงวันที่ 18 มกราคม 2564

ข้อ	ประเด็นคำถาม	คำตอบ
หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene)		
1.	ในกรณีที่ไม่สามารถปฏิบัติตามการบริหารจัดการ security patch ได้ จะต้องดำเนินการอย่างไรเพื่อเข้ากระบวนการยกเว้นภายในบริษัทเองได้	กรณีที่ผู้ให้บริการและผู้ประกอบธุรกิจสามารถปฏิบัติตามการควบคุมนั้น ๆ ได้แล้ว แต่มีเหตุจำเป็นสุดวิสัย เช่น ข้อจำกัดของอุปกรณ์หรือระบบงาน ทำให้ไม่สามารถปฏิบัติตามการควบคุมที่กำหนดไว้ได้ สามารถขออนุมัติยกเว้น (exception) โดยใช้เกณฑ์ภายในเพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ สำหรับในกรณีที่ไม่สามารถปฏิบัติตามการควบคุมนั้น ๆ ได้ เช่น ไม่สามารถจัดให้มีกระบวนการ มาตรฐาน ระเบียบวิธีปฏิบัติ จะต้องขอผ่อนผันเป็นรายกรณีมายัง ธปท.
2.	ผู้เชี่ยวชาญในการทดสอบเจาะระบบ (penetration test) ควรมีคุณสมบัติอย่างไร	ผู้เชี่ยวชาญควรมีความเป็นอิสระและเป็นบุคคลที่มีความรู้ความสามารถในการทดสอบเจาะระบบและทำการเจาะระบบในขอบเขต ขั้นตอน และเครื่องมือที่เป็นมาตรฐานสากล โดยความรู้ความสามารถของผู้เชี่ยวชาญสามารถพิจารณาได้จากประวัติการทดสอบเจาะระบบที่ผ่านมา และการรับรองมาตรฐานในระดับปฏิบัติการ เช่น OSCP OSWP OSCE OSEE OSWE เป็นต้น และขอบเขต ขั้นตอน หรือเครื่องมือในการทดสอบเจาะระบบที่เป็นมาตรฐานสากล เช่น OWASP เป็นต้น
3.	ผู้ให้บริการและผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบเจาะระบบ (penetration test) ภายใน 90 วันตั้งแต่วันถัดจากวันประกาศใน	ในกรณีนี้ สามารถใช้ผลการทดสอบก่อนหน้าที่ประกาศจะมีผลบังคับใช้มาอ้างอิงได้ แต่เมื่อถึงรอบการดำเนินการหรือเมื่อมีการเปลี่ยนแปลง

ข้อ	ประเด็นคำถาม	คำตอบ
	ราชกิจจานุเบกษาเป็นต้นไป ในกรณีที่เคยทำ penetration test ในรอบปีที่ผ่านมา และยังไม่ถึงรอบการจัดทำภายใน 90 วันตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป ถือว่าเป็นการไม่ปฏิบัติตาม Cyber Hygiene ใช่หรือไม่	ที่มีนัยสำคัญขอให้ดำเนินการตามที่ประกาศกำหนดไว้
หลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)		
4.	ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับทุกรายต้องประเมินตนเองรายปีตามคุณสมบัติในข้อ 3.2 (3.1) – (3.3) ใช่หรือไม่ และหากมีคุณสมบัติครบถ้วนตามหลักเกณฑ์ดังกล่าว ต้องดำเนินการอย่างไรต่อไป	ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับทุกรายต้องประเมินตนเองเป็นประจำทุกปี ว่าเป็นผู้ที่มีคุณสมบัติครบถ้วนตามข้อ 3.2 (3.1) – (3.3) หรือไม่ โดยใช้ข้อมูลประกอบการประเมิน ณ วันสิ้นปีปฏิทิน หากผลการประเมินปรากฏว่า มีคุณสมบัติครบถ้วนตามหลักเกณฑ์ดังกล่าว ให้แจ้งผลการประเมินต่อ ธปท. ทราบภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน ตามรูปแบบที่กำหนดในคู่มือประชาชน โดยมีเวลาในการที่ต้องปฏิบัติตามหลักเกณฑ์ IT risk management ภายใน 1 ปีนับแต่วันสิ้นปีปฏิทินของปีที่มีการประเมิน หากกรณีที่มีคุณสมบัติไม่ครบถ้วนตามหลักเกณฑ์ ไม่ต้องแจ้งผลการประเมินต่อ ธปท. แต่ให้จัดเก็บผลการประเมินไว้เพื่อให้พร้อมสำหรับการตรวจสอบของ ธปท. หรือเมื่อ ธปท. ร้องขอ
5.	ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับต้องเริ่มประเมินตนเองตามคุณสมบัติตามข้อ 3.2 (3.1) – (3.3) ครั้งแรกเมื่อใด	ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับทุกรายต้องเริ่มประเมินตนเองครั้งแรกในปี 2565 ตามรูปแบบที่กำหนดในคู่มือประชาชน โดยใช้ข้อมูล ณ วันสิ้นปีปฏิทิน 2564 ประกอบการประเมินตนเอง และหากเข้าเงื่อนไขให้แจ้งผลต่อ ธปท. ภายในวันที่ 30 มกราคม 2565 สำหรับในปี 2564 ธปท. จะมีหนังสือแจ้งผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่เข้า

ข้อ	ประเด็นคำถาม	คำตอบ
		เงื่อนไขข้อ 3.2 (3.1) – (3.3) เพื่อให้ทราบว่าต้องปฏิบัติตามหลักเกณฑ์ IT risk management
คณะกรรมการและโครงสร้างการกำกับดูแล		
6.	ในกรณีที่งานด้าน IT compliance และ IT risk รวมอยู่ด้วยกันภายใต้ทีม IT Security ซึ่งเป็น 1st line ดังนั้น ผู้ให้บริการและผู้ประกอบธุรกิจจะต้องแยกหน่วยงาน ด้าน IT compliance และ IT risk ออกมาเป็นโครงสร้าง 2nd line ที่ชัดเจนหรือไม่	ในหลักเกณฑ์ประกาศฉบับนี้เน้นในเรื่องการแยกฟังก์ชันการปฏิบัติงานอย่างชัดเจน และเป็นอิสระมากกว่าการแบ่งแยกตามโครงสร้าง ดังนั้นหากงานด้าน IT risk หรือ IT compliance มีการแบ่งแยกหน้าที่อย่างชัดเจน ตามหลัก segregation of duties และมีความเป็นอิสระเพียงพอ ผู้ให้บริการและผู้ประกอบธุรกิจสามารถพิจารณาจัดโครงสร้างหน่วยงานได้ตามความเหมาะสม
7.	การแต่งตั้ง CIO เพียงอย่างเดียวสามารถทดแทนการแต่งตั้ง CISO ได้หรือไม่	ไม่สามารถทดแทนกันได้เนื่องจากบทบาทหน้าที่ของ CIO จะเน้นการบริหารจัดการด้าน IT เพื่อสนับสนุนทางธุรกิจ แต่บทบาทหน้าที่ของ CISO จะเน้นการบริหารจัดการความมั่นคงปลอดภัยด้าน IT โดยเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) อย่างไรก็ตาม การแต่งตั้ง CISO นั้น ผู้ให้บริการและผู้ประกอบธุรกิจสามารถพิจารณาแต่งตั้งให้มีเพิ่มเติมได้จากการที่ต้องจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้าน IT (IT security)
8.	ธปท. มีการกำหนดคุณสมบัติของ IT compliance อย่างไร และผู้ให้บริการและผู้ประกอบธุรกิจจำเป็นต้องจัดโครงสร้างองค์กรให้มี IT compliance หรือไม่	ในหลักเกณฑ์ประกาศฉบับนี้เน้นการแยกฟังก์ชันการปฏิบัติงานของ IT compliance อย่างชัดเจนและเป็นอิสระ มากกว่าการแบ่งแยกตามโครงสร้าง โดยคุณสมบัติของ IT compliance จะต้องสามารถกำกับดูแลให้มีการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศได้

ข้อ	ประเด็นคำถาม	คำตอบ
การบริหารจัดการความเสี่ยงจากบุคคลภายนอก		
9.	การใช้บริการจากบุคคลภายนอกในเรื่องต่อไปนี้ เข้าข่ายเป็นการใช้บริการ IT outsourcing หรือไม่ และจะมีแนวทางในการพิจารณาว่าเข้าข่ายเป็นการใช้บริการ IT outsourcing อย่างไร • การจัดซื้อและติดตั้งโปรแกรม (software) สำเร็จรูป เช่น Microsoft Windows, Microsoft Office เป็นต้น • การจัดซื้อและติดตั้งอุปกรณ์คอมพิวเตอร์ • การจ้างที่ปรึกษาด้านเทคโนโลยีสารสนเทศหรือการจ้างเพื่อพัฒนา software หรือ application • การบำรุงรักษาต่อเนื่องตามโปรแกรมดูแลของผู้ให้บริการภายนอกสำหรับ hardware และ software เช่น การทำ preventive maintenance และเป็นบริการที่มาพร้อมกับการจัดซื้อและติดตั้งโดยผู้ให้บริการและผู้ประกอบไม่เสียค่าใช้จ่ายเพิ่มเติม • การใช้บริการ IT outsourcing เพื่อเป็นแผนฉุกเฉิน • การตรวจสอบเพื่อรับรองมาตรฐานหรือเอกสารการรับรองที่เกี่ยวข้องกับด้าน IT (certificate)	การพิจารณาว่า การใช้บริการงาน IT ใดเข้าข่ายเป็น IT outsourcing ให้พิจารณาว่า งาน IT ที่ใช้บริการจากบุคคลภายนอกนั้น เป็นงาน IT ที่โดยปกติแล้วผู้ให้บริการและผู้ประกอบธุรกิจต้องดำเนินการเอง หรือเป็นขอบเขตงานด้าน IT ที่มีการกล่าวถึงการควบคุมในประกาศฉบับนี้ ซึ่งรวมถึงการพัฒนา software หรือ application และการเตรียมการด้าน IT ตามแผนฉุกเฉิน <u>แต่ไม่รวมถึง</u> • การจัดซื้อ ติดตั้ง และบำรุงรักษา ด้าน hardware เช่น เครื่อง server เครื่อง endpoint อุปกรณ์เครือข่าย อุปกรณ์รักษาความปลอดภัยเครือข่าย เป็นต้น <u>ยกเว้น</u> การบำรุงรักษาด้าน hardware ที่สามารถดำเนินการเองได้และจัดซื้อจัดหาบริการดังกล่าวเพิ่มเติม • การจัดซื้อ ติดตั้ง และบำรุงรักษาโปรแกรมสำเร็จรูป เช่น Microsoft Windows Server Microsoft Office หรือ โปรแกรม antivirus เป็นต้น <u>ยกเว้น</u> การบำรุงรักษาด้าน software หรือ application ที่สามารถดำเนินการเองได้และจัดซื้อจัดหาบริการดังกล่าวเพิ่มเติม • การตรวจสอบเพื่อรับรองมาตรฐานหรือเอกสารการรับรองที่เกี่ยวข้องกับด้าน IT (certificate) เช่น ISO 27001 เป็นต้น • การจ้างบุคคลภายนอกเพื่อแก้ไขปัญหาด้าน IT ที่เกิดขึ้นแบบฉุกเฉินได้อย่างทันท่วงที ซึ่งไม่สามารถแก้ไขปัญหาดังกล่าวเองได้
10.	ผู้ให้บริการและผู้ประกอบธุรกิจมีการเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ (data center) โดยผู้ให้เช่าทำหน้าที่ในการบริหารจัดการ	การเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ โดยผู้ให้เช่าทำหน้าที่บริหารจัดการระบบสาธารณูปโภคด้วย เข้าข่ายเป็นการใช้บริการ IT outsourcing

ข้อ	ประเด็นคำถาม	คำตอบ
	ระบบสาธารณูปโภคต่าง ๆ ภายในศูนย์คอมพิวเตอร์ (facility) ด้วย เช่น ระบบไฟฟ้า ระบบทำความเย็นและควบคุมความชื้น ระบบป้องกันและระงับอัคคีภัย เพื่อให้อยู่ในสภาพที่พร้อมใช้งานอย่างต่อเนื่อง เข้าข่ายเป็นการใช้บริการ IT outsourcing หรือไม่	เนื่องจากการบริหารจัดการระบบสาธารณูปโภคซึ่งเป็นโครงสร้างพื้นฐานที่มีความสำคัญภายในศูนย์คอมพิวเตอร์ถือเป็นปัจจัยหลักที่มีผลต่อการดำเนินการอย่างต่อเนื่องของศูนย์คอมพิวเตอร์นั้น
11.	กรณีที่การใช้บริการจากบุคคลภายนอกแล้วบุคคลภายนอกนั้นมีการว่าจ้างผู้รับเหมาช่วง (subcontract) ทางผู้ให้บริการและผู้ประกอบธุรกิจจะต้องรายงานผู้รับเหมาช่วงที่มีนัยสำคัญให้แก่ ธปท. ด้วยหรือไม่	ผู้ให้บริการและผู้ประกอบธุรกิจไม่ต้องรายงานผู้รับเหมาช่วงที่มีนัยสำคัญให้แก่ ธปท. แต่ยังคงต้องกำกับดูแลบุคคลภายนอกและทราบถึงการไปใช้และความเสี่ยงที่อาจจะเกิดขึ้นเพิ่มเติมเมื่อบุคคลภายนอกไปใช้บริการผู้รับเหมาช่วง
12.	โปรดยกตัวอย่างการเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือการให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญตามนิยามของบุคคลภายนอก	ตัวอย่างการเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก เช่น การเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับพันธมิตรทางธุรกิจเพื่อให้บริการร่วมกัน การเชื่อมต่อกับผู้ให้บริการเครือข่ายสาธารณะ ผู้ให้บริการระบบชำระเงินกลาง หรือการเชื่อมต่อผ่าน Application Programming Interface (API) สำหรับการเข้าถึงข้อมูลสำคัญของบุคคลภายนอกตามนิยามของ ธปท. นั้น มุ่งเน้นการเข้าถึงข้อมูลประเภทอิเล็กทรอนิกส์ เช่น การเข้าถึงข้อมูลลูกค้าของผู้ประกอบธุรกิจและนำไปพิมพ์เข้าสู่ระบบงาน หรือนำไปผลิตบัตรเครดิตหรือจัดพิมพ์ใบแจ้งยอดรายการ เป็นต้น
ข้อกำหนด (criteria) ในการพิจารณาความมีนัยสำคัญ		
13.	ขอทราบตัวอย่างของการจัดทำหลักเกณฑ์ในการพิจารณาความมีนัยสำคัญ	การพิจารณาความมีนัยสำคัญให้คำนึงถึงกรอบหลักการความเสี่ยงและผลกระทบต่อการให้บริการหรือดำเนินธุรกิจในวงกว้าง (enterprise wide impact) และผลกระทบต่อระบบการชำระเงินในวงกว้าง (payment system wide impact)

ข้อ	ประเด็นคำถาม	คำตอบ
		โดยตัวอย่างเบื้องต้นในการกำหนดความมีนัยสำคัญในบางเรื่อง • ความมีนัยสำคัญของบุคคลภายนอก เช่น ระดับความสำคัญของระบบงานหรือข้อมูลที่ไปใช้บริการเชื่อมต่อหรือเข้าถึงข้อมูล หรือจำนวนลูกค้าที่จะได้รับผลกระทบกรณีบุคคลภายนอกไม่สามารถให้บริการได้ • การนำเทคโนโลยีมาใช้อาจพิจารณาจากระดับความเสี่ยงหรือภัยที่อาจจะเกิดจากเทคโนโลยีนั้น ๆ หรือจำนวนระบบงานสำคัญที่ไปใช้เทคโนโลยีดังกล่าว เป็นต้น • การเปลี่ยนแปลงระบบหรือเทคโนโลยีอาจพิจารณาจากระยะเวลาหยุดชะงักหรือจำนวนลูกค้าที่จะได้รับผลกระทบกรณีการเปลี่ยนแปลงระบบเกิดปัญหา หรือจำนวนระบบที่มีการเชื่อมต่อกับระบบที่มีการเปลี่ยนแปลง เป็นต้น
การแจ้ง หรือรายงานต่อธนาคารแห่งประเทศไทย		
14.	ผู้ให้บริการและผู้ประกอบธุรกิจทุกรายต้องแจ้งการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญตามข้อ 7.1 และรายงานปัญหาด้านเทคโนโลยีสารสนเทศตามข้อ 7.2 ใช่หรือไม่ มีรูปแบบและรายงานผ่านช่องทางใด รวมถึงในปีแรกที่ประกาศฉบับนี้มีผลบังคับใช้ ให้เริ่มดำเนินการเมื่อใด	ผู้ให้บริการและผู้ประกอบธุรกิจทุกราย ต้องดำเนินการตามข้อ 7.1 และ 7.2 เมื่อพ้นกำหนด 90 วันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป โดยมีรูปแบบและช่องทางการรายงานตามที่กำหนดในคู่มือประชาชน อย่างไรก็ดี ในระหว่างที่ประกาศฉบับนี้ยังไม่มีผลบังคับใช้ ให้ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับแจ้งและรายงานเรื่องดังกล่าวต่อเนื่อง ตามประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และประกาศว่าด้วยหลักเกณฑ์

ข้อ	ประเด็นคำถาม	คำตอบ
		การกำกับดูแลการประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ที่มีผลบังคับใช้อยู่ในปัจจุบัน แล้วแต่กรณี สำหรับผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับที่เป็นนิติบุคคลต่างประเทศ ให้ปฏิบัติตามขอบเขตที่ประกาศมีผลบังคับใช้อยู่ในปัจจุบัน
15.	ผู้ให้บริการและผู้ประกอบธุรกิจต้องประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศตามประกาศฉบับนี้อย่างไร และรายงานต่อ ธปท. ผ่านช่องทางใด	สำหรับผู้ให้บริการ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญ ให้ประเมินตนเอง 2 ส่วน ได้แก่ หลักเกณฑ์ Cyber Hygiene และ IT risk management โดยมีรูปแบบและช่องทางการรายงานตามที่กำหนดในคู่มือประชาชน สำหรับผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่ไม่เข้าเงื่อนไขตามข้อ 3.2 (3.1) – (3.3) ให้ประเมินตนเองเฉพาะหลักเกณฑ์ Cyber Hygiene โดยมีรูปแบบและช่องทางการรายงานตามที่กำหนดในคู่มือประชาชน ทั้งนี้ ขอให้ (1) ผู้บริหารหรือผู้ที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) หรือผู้บริหารหรือผู้ที่ทำหน้าที่กำกับการปฏิบัติตามหลักเกณฑ์ (compliance) และ (2) ผู้บริหารหรือผู้ที่ทำหน้าที่ตรวจสอบภายใน (internal audit) รับรองผลการประเมินตนเองก่อนส่งให้ ธปท.
16.	ผู้ให้บริการและผู้ประกอบธุรกิจทุกรายต้องรายงานบุคคลภายนอกที่มีนัยสำคัญตามข้อ 7.4 และรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญตามข้อ 7.5 ใช่หรือไม่ มีรูปแบบและรายงานผ่านช่องทางใด รวมถึงในปีแรก	การรายงานตามข้อ 7.4 และ 7.5 กำหนดให้เฉพาะผู้ให้บริการและผู้ประกอบธุรกิจที่เข้าเงื่อนไขที่ต้องปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ตามข้อ 3.2 ซึ่งได้แก่

ข้อ	ประเด็นคำถาม	คำตอบ
	ที่ประกาศฉบับนี้มีผลบังคับใช้ ให้เริ่มดำเนินการเมื่อใด	1. ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ 2. ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ 3. ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีคุณสมบัติครบถ้วนตามข้อ 3.2 (3.1) – (3.3) โดยกำหนดให้เริ่มรายงาน เมื่อพ้นกำหนด 1 ปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป โดยมีรูปแบบและช่องทางการรายงานตามที่กำหนดในคู่มือประชาชน
หลักเกณฑ์การกำกับดูแลความเสี่ยงเทคโนโลยีสารสนเทศของนิติบุคคลต่างประเทศ		
17.	ตัวอย่างข้อมูลที่ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับที่เป็นนิติบุคคลต่างประเทศต้องจัดเตรียมไว้ให้เป็นปัจจุบันเพื่อให้พร้อมสำหรับการตรวจสอบของ ธปท. หรือเมื่อ ธปท. ร้องขอ คือข้อมูลอะไรบ้าง	ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับที่เป็นนิติบุคคลต่างประเทศ จะต้องจัดเตรียมข้อมูลที่แสดงถึงการปฏิบัติตามหลักเกณฑ์หรือกฎหมายการกำกับดูแลของประเทศอื่นและมีการควบคุมความเสี่ยงด้าน IT ที่เทียบเท่าหลักเกณฑ์ในประกาศฉบับนี้ หรือเทียบเท่ามาตรฐานสากล เช่น PCI-DSS, ISO27001 และ COBIT 5 เป็นต้น
18.	ในกรณีที่เป็นผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับที่เป็นนิติบุคคลต่างประเทศต้องรายงานปัญหาด้านเทคโนโลยีสารสนเทศต่อ ธปท. หรือไม่	ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับที่เป็นนิติบุคคลต่างประเทศต้องรายงานปัญหาด้านเทคโนโลยีสารสนเทศตามประกาศฉบับนี้ อย่างไรก็ดี ในระหว่างที่ประกาศฉบับนี้ยังไม่มีผลบังคับใช้ ให้รายงานในเรื่องดังกล่าวต่อเนื่อง ตามประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับที่มีผลบังคับใช้อยู่ในปัจจุบัน

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6346

ธนาคารแห่งประเทศไทย

IT Risk Management Implementation Guideline

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
ธนาคารแห่งประเทศไทย

สารบัญ

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT governance)

1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ

วัตถุประสงค์ เพื่อให้คณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจกำกับดูแลและสนับสนุนให้องค์กรบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเพียงพอเหมาะสมและสอดคล้องกับการให้บริการหรือดำเนินธุรกิจ

1.1.1 คณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจประกอบด้วยกรรมการที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างน้อย 1 ท่าน เพื่อให้คณะกรรมการสามารถกำหนดทิศทางและกำกับดูแลให้การใช้เทคโนโลยีสารสนเทศสอดรับกับกลยุทธ์การให้บริการหรือดำเนินธุรกิจ มีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีที่เปลี่ยนแปลงไป

1.1.2 ดูแลให้การใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจ และดูแลให้การใช้เทคโนโลยีมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการเปลี่ยนแปลงการให้บริการหรือดำเนินธุรกิจในอนาคต

1.1.3 ดูแลให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมขององค์กร (enterprise risk management : ERM) ในฐานะที่เป็นความเสี่ยงที่สำคัญ

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

1.1.5 ดูแลให้มีมาตรฐาน ระเบียบวิธีปฏิบัติ กระบวนการ เครื่องมือ และบุคลากรในการรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายข้อ 1.1.4 รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม ทบทวนและประเมินประสิทธิภาพนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้ง และทุกครั้งเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.1.6 ดูแลให้มีการติดตาม ตรวจสอบและรายงานต่อคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูง อย่างเหมาะสม ในเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น ผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของผู้ให้บริการและผู้ประกอบธุรกิจ ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ทางด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการและผู้ประกอบธุรกิจ

1.1.7 ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรของผู้ให้บริการและผู้ประกอบธุรกิจ เพื่อให้ตระหนักถึงความสำคัญของความเสี่ยงและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งเข้าใจการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เพื่อช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.1.8 คณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ ต้องได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศอย่างเพียงพอตามระยะเวลาที่เหมาะสม เพื่อให้มีความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศที่เพียงพอต่อการกำกับดูแลและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้ทันกับภัยคุกคามใหม่ รวมถึงการพิจารณาเชิงกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการขับเคลื่อนธุรกิจ

1.2 โครงสร้างการกำกับดูแล

วัตถุประสงค์ เพื่อให้มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเหมาะสมสอดคล้องตามหลัก 3 lines of defence

คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.2.1 ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดตั้งคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงการถ่วงดุลอำนาจอย่างเป็นอิสระ อย่างน้อยครอบคลุม

- คณะกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (เช่น IT steering committee หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดกลยุทธ์ นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์ของผู้ให้บริการและผู้ประกอบธุรกิจ รวมทั้งกำกับดูแลและติดตามการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้ อาจพิจารณาให้มีคณะกรรมการที่ดูแลงานเฉพาะด้านเพิ่มเติม หากเห็นว่างานดังกล่าวมีนัยสำคัญหรือมีผลกระทบสูงต่อผู้ให้บริการและผู้ประกอบธุรกิจ เช่น คณะกรรมการหรืออนุกรรมการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น
- คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (เช่น คณะกรรมการบริหารความเสี่ยง คณะกรรมการบริหารความเสี่ยงด้านปฏิบัติการ คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ รวมทั้งกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในภาพรวม (enterprise risk management) ของผู้ให้บริการและผู้ประกอบธุรกิจ
- คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ (เช่น คณะกรรมการตรวจสอบ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจ มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้ง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

โครงสร้างองค์กร

1.2.2 ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีโครงสร้างองค์กรและหน้าที่ความรับผิดชอบเป็นลายลักษณ์อักษร โดยสอดคล้องตามหลักการถ่วงดุล (check and balance) และการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน (segregation of duties) ระหว่างการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ

1.2.3 ผู้ให้บริการและผู้ประกอบธุรกิจควรดูแลให้มีทรัพยากรเพียงพอที่จะสนับสนุนการปฏิบัติงาน การบริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และการตรวจสอบด้านเทคโนโลยีสารสนเทศสอดคล้องตามปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น จัดให้มีบุคลากรที่มีความรู้ความเชี่ยวชาญและมีเครื่องมือหรือระบบที่ช่วยสนับสนุนการปฏิบัติงาน เป็นต้น

1.2.4 ผู้ให้บริการและผู้ประกอบธุรกิจควรมีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์ และ

มีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) โดยมีบทบาทหน้าที่และความรับผิดชอบ อย่างน้อยดังนี้

- มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด
- มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)
- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจเป็นวาระประจำ
- ดูแลและดำเนินการให้ผู้ให้บริการและผู้ประกอบธุรกิจมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์
- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้านภัยคุกคามทางไซเบอร์

1.2.5 นอกจากนี้ ผู้ให้บริการและผู้ประกอบธุรกิจอาจพิจารณาให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer : CISO) โดยควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (authority) เพียงพอสำหรับการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้

- รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจและคณะกรรมการที่เกี่ยวข้องโดยตรง
- ให้ความเห็นด้านภัยคุกคามไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ที่กระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญ

1.2.6 หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 1st 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 รวมทั้งแนวโน้มความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้นและส่งผลกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจ
- รายงานผลการประเมินความเสี่ยง การติดตามความเสี่ยง และแนวทางการควบคุมที่เกี่ยวข้อง
- รายงานความคืบหน้าการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
- รายงานผลการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก

1.2.6.2 ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ มีหน้าที่ปฏิบัติตามนโยบายและระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องจากการใช้งานระบบ

1.2.7 หน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 2nd line of defence) เช่น หน่วยงานบริหารความเสี่ยง และหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์

1.2.7.1 หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง มีหน้าที่กำหนดกรอบและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สนับสนุนให้มีการประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยงและทบทวนการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ของหน่วยงานที่ทำหน้าที่เป็น 1st line of defence โดยรวบรวมและเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกับความเสี่ยงด้านอื่นของผู้ให้บริการและผู้ประกอบธุรกิจ และนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยง

1.2.7.2 หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ มีหน้าที่กำหนดกระบวนการติดตามดูแล ให้คำปรึกษา สอบทานและรายงานการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง และนำเสนอต่อคณะกรรมการที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยระบบการชำระเงิน เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

1.2.8 หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 3rd line of defence) ซึ่งอาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น หน่วยงานตรวจสอบภายใน

- หน่วยงานที่ทำหน้าที่ตรวจสอบ มีหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงของหน่วยงานที่ทำหน้าที่ 1st line และ 2nd line of defence รวมถึงงานอื่น ๆ ที่เกี่ยวข้อง เช่น การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ เป็นต้น เพื่อสอบทานให้มั่นใจว่ามีการปฏิบัติที่เป็นไปตามนโยบาย มาตรฐาน และระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ
- มีกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมอย่างน้อย ดังนี้

(1) การวางแผนงานและกำหนดขอบเขตการตรวจสอบ (planning and scoping) ครอบคลุมและสอดคล้องกับความสำคัญและความเสี่ยงของการใช้งานเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจและนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบต้องได้รับความเห็นชอบจากคณะกรรมการตรวจสอบ และมีการทบทวนอย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(2) การตรวจสอบ (execution) อย่างน้อยปีละ 1 ครั้งตามแผนงานและขอบเขตที่กำหนด และพิจารณาให้มีการตรวจสอบเมื่อมีเหตุการณ์ผิดปกติในงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ นอกจากนี้ แนวทางการตรวจสอบควรเป็นไปตามมาตรฐานที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด สอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง รวมถึงมาตรฐานสากลที่ยอมรับโดยทั่วไป

(3) การวิเคราะห์ (analysis) นำข้อมูลที่ได้จากการตรวจสอบมาวิเคราะห์ เพื่อสรุปผลการตรวจสอบและอาจพิจารณาขยายขอบเขตการตรวจสอบเพิ่มเติม หากมีความจำเป็น เช่น พบข้อบ่งชี้ถึงความเสี่ยงที่อาจกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญ

(4) การรายงานและติดตามผลการตรวจสอบ (reporting and follow up) มีการสรุปผลการตรวจสอบและประเด็นที่ต้องแก้ไขกับผู้บริหารของหน่วยงานผู้รับตรวจและจัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการตรวจสอบและแจ้งให้ผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบ รวมถึงติดตามให้มีการปรับปรุงประเด็นการตรวจสอบและรายงานประเด็นสำคัญพร้อมแผนปรับปรุงให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้อง

- ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่มีความสำคัญ ซึ่งผู้ให้บริการและผู้ประกอบธุรกิจ เห็นว่ามีความจำเป็นต้องประเมิน แต่มีข้อจำกัดหรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ ไม่สามารถประเมินได้ เช่น การประเมินระบบที่มีความซับซ้อนหรือมีการใช้เทคโนโลยีใหม่ หรือการประเมินความสามารถของระบบในการปรับเปลี่ยนเพื่อรองรับการทำธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจในอนาคตภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว

1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

<u>วัตถุประสงค์</u> เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและสอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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

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

1.3.2 นโยบายดังกล่าวควรสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการให้บริการหรือดำเนินธุรกิจ ความเสี่ยงที่เกี่ยวข้องทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศและความเสี่ยงกรณีมีการใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอก รวมทั้งสอดคล้องกับแนวทางบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

1.3.3 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรจัดให้มีการชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและมีการควบคุมดูแลให้มีการปฏิบัติตามนโยบายได้อย่างถูกต้องครบถ้วน

1.3.4 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)

1.3.5 นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยครอบคลุมอย่างน้อย

- โครงสร้างองค์กร บทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- การกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)
- จัดทำหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

(1) การประเมินความเสี่ยง (risk assessment)

(1.1) การระบุความเสี่ยง (risk identification)

ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีการระบุเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นหรือที่เกิดขึ้นจริง รวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการให้บริการหรือดำเนินธุรกิจ โดยเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรระบุอย่างน้อยครอบคลุม

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

ทั้งนี้ ผู้ที่มีส่วนร่วมในการระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศควรมีความรู้และความเข้าใจถึงเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ได้ระบุไว้เป็นอย่างดี

(1.2) การวิเคราะห์ความเสี่ยง (risk analysis)

ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยควรดำเนินการ ดังนี้

- กำหนดเจ้าของความเสี่ยงด้านเทคโนโลยีสารสนเทศ (risk owner)
- ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing control)
- พิจารณาและค้นหาสาเหตุและสถานการณ์ที่เป็นไปได้
- วิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(1.3) การประเมินค่าความเสี่ยง (risk evaluation)

ผู้ให้บริการและผู้ประกอบธุรกิจควรประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงานและการให้บริการหรือดำเนินธุรกิจ เพื่อจัดลำดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยควรดำเนินการ ดังนี้

- กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ เช่น ด้านการเงิน ด้านปฏิบัติการ เป็นต้น
- ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- จัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแสดงในแผนภาพความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2) การจัดการความเสี่ยง (risk treatment)

ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรครอบคลุมอย่างน้อย ดังนี้

- กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือกแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมสำหรับผู้ให้บริการและผู้ประกอบธุรกิจ เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง การลดหรือบรรเทาโอกาสเกิดความเสี่ยง การลดหรือบรรเทาผลกระทบที่เกิดขึ้น การแบ่งหรือโอนความเสี่ยงให้หน่วยงานอื่น การยอมรับความเสี่ยงไว้โดยแจ้งเหตุผลให้ผู้บริหารทราบเพื่อตัดสินใจในการยอมรับความเสี่ยง เป็นต้น
- ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ
- ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้
- จัดทำแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญในการดำเนินการ
- นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

นอกจากนี้ผู้ให้บริการและผู้ประกอบธุรกิจ ควรจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) ให้สอดคล้องกับความสำคัญของงานเทคโนโลยีสารสนเทศแต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

(3) การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ตามที่กำหนดและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบ เพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ ครอบคลุมอย่างน้อย

- การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง
- ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น
- ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับผู้ให้บริการและผู้ประกอบธุรกิจ และองค์กรอื่น
- รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามรอบที่กำหนด

(4) การรายงานความเสี่ยง (risk reporting)

ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีกระบวนการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พร้อมทั้งรายงานผลการประเมินและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร รวมทั้งรายงานแนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น ต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ เพื่อให้มั่นใจว่าผู้ให้บริการและผู้ประกอบธุรกิจมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและต่อเนื่อง โดยการรายงานควรครอบคลุมอย่างน้อย

- สถานะและผลลัพธ์การดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี
- ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร
- รายงานดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ และรายงานสรุปเหตุการณ์ผิดปกติ
- แนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นกับผู้ให้บริการและผู้ประกอบธุรกิจ
- ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง

1.3.6 ทั้งนี้ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีการทบทวนหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.4 การบริหารจัดการบุคลากร

<u>วัตถุประสงค์</u> เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจมีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอสำหรับปฏิบัติงานที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศ โดยบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ

1.4.1 มีกระบวนการบริหารจัดการบุคลากรอย่างเหมาะสม ครอบคลุม การคัดเลือกบุคลากรที่มีความรู้ความสามารถเพียงพอ การว่าจ้างบุคลากรที่เป็นไปตามข้อกำหนดหรือเงื่อนไขด้านความปลอดภัยเทคโนโลยีสารสนเทศ การพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยง

ด้านเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงหรือสิ้นสุดการว่าจ้างบุคลากร รวมทั้งการดูแลบุคลากรให้เพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศ

1.4.2 ผู้ให้บริการและผู้ประกอบธุรกิจอาจพิจารณาการได้รับการรับรองความรู้ความสามารถตามมาตรฐานที่รับรองทั่วไป (certificate) เฉพาะด้านที่เกี่ยวข้องกับงานด้านเทคโนโลยีสนเทศ เพื่อให้ได้บุคลากรที่มีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

1.4.3 หน่วยงานทรัพยากรบุคคล ควรตรวจสอบประวัติของบุคลากรก่อนการว่าจ้างตามความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ เช่น ประวัติการศึกษา ประวัติการทำงาน ประวัติอาชญากรรม ข้อมูลเครดิตบูโร เป็นต้น

1.4.4 มีข้อกำหนดหรือเงื่อนไขในสัญญาจ้างหรือระเบียบข้อบังคับภายในองค์กร โดยกล่าวถึงบทบาทหน้าที่ความรับผิดชอบ การปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ

1.4.5 ให้บุคลากรและบุคคลภายนอกที่ได้รับการว่าจ้างทำความเข้าใจ รับทราบและลงนามยอมรับเงื่อนไขการว่าจ้างงานหรือระเบียบข้อบังคับภายในองค์กร นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ และข้อตกลงการไม่เปิดเผยข้อมูล (non disclosure agreement) ก่อนเริ่มปฏิบัติงาน

1.4.6 มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน เช่น การคืนสินทรัพย์ของผู้ให้บริการและผู้ประกอบธุรกิจ การบริหารจัดการสิทธิต้องมีการปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องมีการสื่อสารให้ผู้เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิหน้าที่และความรับผิดชอบ เป็นต้น

1.5 การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness)

<u>วัตถุประสงค์</u> เพื่อให้บุคลากรทุกระดับของผู้ให้บริการและผู้ประกอบธุรกิจมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

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

- หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (1st line of defence) ให้มีความรู้และความเชี่ยวชาญที่เพียงพอต่อการปฏิบัติงานและการใช้งาน
- หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องกับงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (2nd line of defence) และการตรวจสอบด้านเทคโนโลยีสารสนเทศ (3rd line of defence) ให้มีความรู้และความเชี่ยวชาญเพียงพอที่จะระบุ ประเมิน และให้ข้อเสนอแนะในการปรับปรุงประสิทธิภาพของการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่หน่วยงานที่ทำหน้าที่ 1st 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 ผู้ให้บริการและผู้ประกอบธุรกิจ ควรจัดให้มีการประชาสัมพันธ์เพื่อสร้างความรู้หรือสร้างความตระหนักในการใช้งานบริการทางอิเล็กทรอนิกส์อย่างปลอดภัย ให้แก่สมาชิก ผู้ใช้บริการของระบบหรือลูกค้า หรือผู้ใช้บริการทราบอย่างสม่ำเสมอด้วย

1.5.3 มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน เช่น การคืนสินทรัพย์ของผู้ให้บริการและผู้ประกอบธุรกิจ การบริหารจัดการสิทธิต้องมีการปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องมีการสื่อสารให้ผู้เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิหน้าที่และความรับผิดชอบ เป็นต้น

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 รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) จากผู้ผลิตได้อย่างเหมาะสมทันการณ์

2.1.3 มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT inventory list) ของฮาร์ดแวร์ (hardware) และซอฟต์แวร์ (software) ที่รองรับระบบเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ อย่างครบถ้วนและเป็นลายลักษณ์อักษร 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)

2.1.4 มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

2.1.5 มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน (return asset) เมื่อสิ้นสุดการใช้งานครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในองค์กรของผู้ให้บริการและผู้ประกอบธุรกิจ และกรณีที่บุคคลภายนอกมีการใช้งานทรัพย์สินของผู้ให้บริการและผู้ประกอบธุรกิจ ทันทีที่มีการยกเลิกสัญญาจ้างด้วย

2.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

วัตถุประสงค์ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งรูปแบบกระดาษและอิเล็กทรอนิกส์ 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 กำหนดให้มีการเข้ารหัสข้อมูลสำคัญและช่องทางการสื่อสารที่ใช้รับส่งข้อมูลสำคัญกับภายนอก

2.2.8 วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล เช่น การเข้ารหัสข้อมูลแบบสมมาตร (เช่น AES) การเข้ารหัสข้อมูลแบบอสมมาตร (public key cryptography) เป็นต้น โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

2.2.9 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management) ควรกำหนดกระบวนการที่มีความรัดกุมปลอดภัยครอบคลุมตั้งแต่ การสร้างและติดตั้ง การจัดเก็บ และการยกเลิกกุญแจเข้ารหัสข้อมูล

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 กรณีกุญแจหมดอายุ ล้าสมัย หรือไม่ปลอดภัย เป็นต้น
- กำหนดกระบวนการทำลายกุญแจ โดยต้องมั่นใจว่าไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก

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 บัญชีผู้ใช้งานที่มีสิทธิสูง ครอบคลุมระบบปฏิบัติการ (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 มาตรฐานที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนดและมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป โดยอย่างน้อยควรใช้วิธีการพิสูจน์ตัวตนแบบ multi-factor authentication
- จัดเก็บข้อมูลประวัติการพิสูจน์ตัวตนและการเข้าถึง (access log) และประวัติการดำเนินงาน (activities log)
- กรณีบัญชีผู้ใช้งานที่มีสิทธิสูงสามารถเข้าถึงระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัย

เครือข่าย จากช่องทางการเข้าถึงระยะไกล (remote access) ผู้ให้บริการและผู้ประกอบธุรกิจ ควรมีการควรคุมที่เข้มงวด 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) สามารถระบุและสอบทานแหล่งที่มาของอุปกรณ์หรือระบบปลายทางที่เข้าเชื่อมต่อกับระบบเครือข่ายของผู้ให้บริการและผู้ประกอบธุรกิจ แบบระยะไกล

(5) สอบทานการเข้าถึงระบบงานระยะไกลจากบัญชีผู้ใช้งานที่มีสิทธิสูงด้วยบุคคลหรือหน่วยงานที่มีความเป็นอิสระและมีความรู้ความเชี่ยวชาญเพียงพอ

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

- กำหนดสิทธิผู้ใช้งานตามบทบาทหน้าที่ ความรับผิดชอบและความจำเป็นในการใช้งาน
- กำหนดวิธีการระบุตัวตนและพิสูจน์ตัวที่เหมาะสม สอดคล้องตามความเสี่ยง สอดคล้องกับนโยบายมาตรฐานที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด
- กำหนดการตั้งรหัสผ่านสำหรับบัญชีผู้ใช้งานให้เข้มแข็ง โดยอย่างน้อยควรครอบคลุม ดังนี้
  (1) การบังคับให้เปลี่ยนรหัสผ่านครั้งแรกที่เข้าใช้งาน
  (2) ความยาวรหัสผ่านขั้นต่ำและรอบการใช้รหัสผ่านเดิมซ้ำ
  (3) กำหนดให้ตั้งรหัสผ่านแบบซับซ้อน (password complexity)
  (4) จำนวนครั้งการใส่รหัสผ่านผิด
- ไม่ควรใช้บัญชีผู้ใช้งานร่วมกับผู้ใช้งานอื่น
- กรณีที่บัญชีผู้ใช้งานที่สามารถเข้าถึงข้อมูลสมาชิก ผู้ใช้บริการของระบบและลูกค้าที่เชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (Internet facing) ผู้ให้บริการและผู้ประกอบธุรกิจ ควรกำหนดให้การพิสูจน์ตัวตนเป็นแบบ multi-factor authentication อย่างไรก็ตาม หากระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication ผู้ให้บริการและผู้ประกอบธุรกิจ สามารถใช้วิธีการอื่นที่มีประสิทธิภาพเทียบเท่าทดแทนได้ เพื่อลดความเสี่ยงจากการถูกปลอมแปลงตัวตนได้โดยง่าย

2.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

<u>วัตถุประสงค์</u> เพื่อให้มีการรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของศูนย์คอมพิวเตอร์และพื้นที่สำคัญที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเพียงพอรองรับธุรกิจอย่างต่อเนื่อง

2.4.1 การควบคุมการเข้าถึงศูนย์คอมพิวเตอร์และพื้นที่สำคัญต่าง ๆ ภายในศูนย์คอมพิวเตอร์ทางกายภาพ ควรครอบคลุมอย่างน้อย 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 หรือทางด่วน 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 และฝนังกั้นพื้นที่อื่น 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 ควรควบคุมอุณหภูมิให้อยู่ระหว่าง 20-25 C^{o} 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 โดยในการทดสอบควรพึงระวังไม่ให้การทดสอบนั้นกระทบต่อการดำเนินงานปกติของผู้ให้บริการและผู้ประกอบธุรกิจ

(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)

วัตถุประสงค์ เพื่อให้มีโครงสร้างของระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย มีการออกแบบระบบเครือข่ายสื่อสารที่เหมาะสมตามมาตรฐานสากล และมีการป้องกันหรือเฝ้าระวังการบุกรุกหรือภัยคุกคามในรูปแบบต่าง ๆ

2.5.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารในองค์กร และระหว่างระบบเครือข่ายสื่อสารภายในองค์กรกับระบบเครือข่ายสื่อสารภายนอกองค์กรให้มีความมั่นคงปลอดภัย โดยควรจัดให้มีแนวทางป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหายหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวด

2.5.2 แบ่งแยกเครือข่ายส่วนที่เป็น private network และ public network ออกจากกัน กรณีแบ่งแยกเครือข่ายเป็นหลายชั้น ควรใช้อุปกรณ์รักษาความปลอดภัยเครือข่ายที่ต่างยี่ห้อกันในแต่ละจุดเพื่อลดความเสี่ยงที่อุปกรณ์เครือข่ายอาจมีช่องโหว่เดียวกัน

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

2.5.4 จัดแบ่งเครือข่ายอย่างเหมาะสม โดยคำนึงถึง ระดับความสำคัญของระบบงาน ระดับความสำคัญของข้อมูลที่ถูกประมวลผล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่น ๆ หรือจากภายนอกองค์กร และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่างๆ มายังระบบงานที่มีความสำคัญอย่างเข้มงวด

2.5.5 จุดที่มีการแบ่งแยกเครือข่ายที่มีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรอง traffic ที่ส่งผ่านระบบเครือข่าย การเฝ้าระวังการบุกรุก การป้องกันการบุกรุก และการตรวจจับไวรัส หรือมัลแวร์ต่างๆ ที่อาจบุกรุกเข้าสู่เครือข่าย

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

2.5.7 ควบคุม และจำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบเครือข่ายได้ รวมถึงมีการระบุตัวตนของอุปกรณ์ที่มาเชื่อมต่อกับระบบเครือข่ายอย่างเหมาะสม

2.5.8 จำกัดให้เฉพาะบุคคลที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงระบบเครือข่าย โดยจำกัดสิทธิในการเข้าถึงระบบเครือข่ายให้อยู่ในส่วนที่มีความจำเป็น และเหมาะสมตามหน้าที่การทำงานเท่านั้น

2.5.9 การเข้าถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเพื่อบริหารจัดการค่าต่างๆ ควรทำผ่านเครือข่ายเฉพาะที่แยกออกจากเครือข่ายปกติ เพื่อลดความเสี่ยงในการเปลี่ยนแปลงอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายโดยบุคคลที่ไม่ได้รับอนุญาต

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

2.5.11 เปลี่ยน default password ของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย รวมทั้งปรับตั้งค่าการรักษาความปลอดภัยให้เป็นไปตามมาตรฐานการตั้งค่าความปลอดภัย (security baseline) ที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด

2.5.12 มีกระบวนการหรือเครื่องมือในการตรวจสอบการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่พิจารณาว่ามีความสำคัญหรือมีความเสี่ยง เช่น การเปลี่ยนแปลง service การเปลี่ยนแปลง port และมีการแจ้งเตือนไปยังผู้ที่ได้รับมอบอำนาจ

2.5.13 จำกัดสิทธิในการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย และการเข้าถึงหน้าจอการบริหารจัดการระบบเครือข่าย (configuration page) เฉพาะผู้ที่รับมอบอำนาจเท่านั้น

2.5.14 ติดตามสถานะความพร้อมใช้งานของระบบเครือข่ายว่ายังอยู่ในระดับ service level agreement (SLA) ที่กำหนด และจัดให้มีกระบวนการจัดการปัญหา และวิธีแก้ปัญหาเมื่อระบบเครือข่ายขัดข้อง

2.5.15 ผู้ให้บริการและผู้ประกอบธุรกิจเครือข่ายสำรองควรเป็นคนละรายกับผู้ให้บริการและผู้ประกอบธุรกิจหลัก

2.5.16 ทดสอบระบบเครือข่ายสื่อสาร และอุปกรณ์เครือข่ายชุดสำรองอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าระบบเครือข่ายสื่อสารพร้อมใช้งาน

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 และหน่วยงานผู้ใช้งานเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อทำหน้าที่ประเมินผลกระทบและพิจารณาเหตุผลความจำเป็นก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลงระบบ ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง โดยครอบคลุมอย่างน้อย ดังนี้

- ผลการประเมินความเสี่ยงและผลกระทบของการเปลี่ยนแปลง โดยมีหน่วยงานเจ้าของระบบและผู้มีหน้าที่เกี่ยวข้องทำการประเมินองค์ประกอบที่เกี่ยวข้อง ได้แก่ ระบบโครงสร้างพื้นฐาน ระบบเครือข่ายสื่อสาร และการเชื่อมต่อกับระบบอื่น เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้น ไม่กระทบต่อการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ ความพร้อมใช้ของระบบ
- ผลการทดสอบ เพื่อให้มั่นใจว่าระบบได้ผ่านการทดสอบอย่างครบถ้วนเหมาะสมตามมาตรฐานและระเบียบวิธีปฏิบัติของผู้ให้บริการและผู้ประกอบธุรกิจ
- 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) การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการ

ปกติ (normal change) และการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) โดยผู้ให้บริการและผู้ประกอบธุรกิจ 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

2.6.2 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 ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.6.2.3 มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์และระบบงาน (system configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.6.2.4 มีการสอบทานการตั้งค่าจากหน่วยงานที่มีหน้าที่ควบคุมดูแลความปลอดภัยหรือความเสี่ยงด้านเทคโนโลยีอย่างสม่ำเสมอ เพื่อให้สอดคล้องตามมาตรฐานของผู้ให้บริการและผู้ประกอบธุรกิจ

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 ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ผู้ให้บริการและผู้ประกอบธุรกิจ กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.6.3.5 มีการทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าผู้ให้บริการและผู้ประกอบธุรกิจ สามารถทดสอบและติดตั้ง patch ด้านการรักษาความปลอดภัย ได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว

2.6.4 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

วัตถุประสงค์ 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 โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอในการป้องกันการเปลี่ยนแปลงแก้ไข 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 มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศเพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง

2.6.5.3 มีกระบวนการหรือเครื่องมือในการติดตามประสิทธิภาพและความเพียงพอของการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของระบบ เช่น ระบบการชำระเงิน ระบบที่ให้บริการทางการเงินอิเล็กทรอนิกส์ เป็นต้น เพื่อบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงที และสามารถตอบสนองความต้องการในการดำเนินงานทางธุรกิจอย่างต่อเนื่อง

2.6.5.4 มีการกำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (threshold และ trigger) ในระดับต่าง ๆ เพื่อให้มีการแจ้งเตือนผู้เกี่ยวข้องอย่างทันท่วงที และสามารถวิเคราะห์ปัญหาและแนวทางการรับมือที่เหมาะสม รวมถึงการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง

2.6.5.5 จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมและความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

2.6.6 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring)

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

2.6.6.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

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

2.6.6.3 มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูลภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์

2.6.6.4 กำหนดให้มีผู้รับผิดชอบในการประสานงานแลกเปลี่ยนข้อมูลภัยคุกคาม ระหว่างผู้ให้บริการและผู้ประกอบธุรกิจกับหน่วยงานที่เกี่ยวข้อง รวมทั้งมีกระบวนการและช่องทางในการรายงาน แลกเปลี่ยน ติดตาม เพื่อป้องกันรับมือและแก้ไขภัยคุกคาม

2.6.6.5 ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญผู้ให้บริการและผู้ประกอบธุรกิจ ควรจัดให้มีการรายงานผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง รวมทั้งมีการรายงานหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมทั้งจัดให้มีกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) โดยผู้ที่มีความเชี่ยวชาญเพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

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) โดยผู้ให้บริการและผู้ประกอบธุรกิจ ควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบบงานสำคัญควรจัดทำอย่างน้อยปีละ 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 และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.6.7.5 มีการรายงานผลการทดสอบเจาะระบบไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

2.6.7.6 มีกระบวนการรวบรวมและวิเคราะห์ช่องโหว่ทางด้านเทคนิคที่ตรวจพบ เพื่อกำหนดเป็นมาตรการรักษาความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาในอนาคต

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 จัดให้มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งานและปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติของผู้ให้บริการและผู้ประกอบธุรกิจ

2.6.9 การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

<u>วัตถุประสงค์</u> เพื่อให้อุปกรณ์ที่ใช้ปฏิบัติงานมีความปลอดภัยและไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต

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

2.6.9.2 กำหนด Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงาน เพื่อป้องกันความเสี่ยงที่อุปกรณ์เหล่านั้นอาจเป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญตามระดับความเสี่ยงที่เหมาะสม โดยอย่างน้อยครอบคลุม ดังนี้

- ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ (personal computer, notebook) โดยมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้ผู้ใช้งานสามารถติดตั้งโปรแกรมอื่น ๆ นอกเหนือจากผู้ให้บริการและผู้ประกอบธุรกิจกำหนด
- ติดตั้งโปรแกรมรักษาความปลอดภัย เช่น anti-Virus/ anti-malware, Host-based Intrusion Prevention System (HIPS) เป็นต้น โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (malware) ให้เพียงพอและเป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ
- ควบคุมไม่ให้มีการจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แต่หากมีความจำเป็นต้องจัดเก็บ ต้องมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น มีการเข้ารหัส เป็นต้น
- มีกระบวนการหรือเครื่องมือในการตรวจจับ (detect) คัดกรอง (filter) สกัดกั้น (block) เพื่อป้องกันข้อมูลสำคัญรั่วไหล (Data Leakage Prevention : DLP)
- จำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานเท่านั้น
- การควบคุมการใช้งานอินเตอร์เน็ต โดยผู้ให้บริการและผู้ประกอบธุรกิจควรมีเครื่องมือในการควบคุมให้อุปกรณ์ที่สามารถเชื่อมต่ออินเตอร์เน็ตเข้าถึงเฉพาะเว็บไซต์ที่ได้รับอนุญาตเท่านั้น 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 ระบบงานและข้อมูลของผู้ให้บริการและผู้ประกอบธุรกิจ
- มีกระบวนการตรวจสอบ วิเคราะห์ และติดตามความเสี่ยงของอุปกรณ์ที่นำมาใช้งานในผู้ให้บริการและผู้ประกอบธุรกิจ
- กำหนดรหัสผ่านเพื่อใช้ในการล็อคหรือปลดล็อคในการเข้าถึงอุปกรณ์ส่วนตัว
- กรณีเครื่องคอมพิวเตอร์ (personal computer, notebook) ต้องติดตั้ง anti-virus/ anti-malware หรือโปรแกรมตามที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด

- ไม่อนุญาตให้อุปกรณ์โทรศัพท์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jailbroken) ลงทะเบียนใช้งาน BYOD
- ใช้วิธีการพิสูจน์ตัวตนอุปกรณ์ที่เชื่อถือได้ขององค์กร เช่น trusted root certification authorities, digital certificate เป็นต้น

2.7 การจัดหาและการพัฒนาระบบ (system acquisition and development)

<u>วัตถุประสงค์</u> เพื่อให้มั่นใจได้ว่ากระบวนการจัดหาและการพัฒนาระบบ มีการควบคุมการรักษาความปลอดภัยอย่างรัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล

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
  (7) ความน่าเชื่อถือของระบบและผู้ให้บริการ
  (8) ผลการจัดทำ proof of concept ในกรณีที่เป็นระบบสำคัญ
- ผู้ให้บริการและผู้ประกอบธุรกิจควรควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบและพัฒนาระบบ
- ผู้ให้บริการและผู้ประกอบธุรกิจกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการตรวจสอบและส่งมอบระบบเทคโนโลยีสารสนเทศ

2.7.2 การพัฒนาระบบเทคโนโลยีสารสนเทศ (system development) ควรครอบคลุมอย่างน้อย ดังนี้

- กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงการรักษาความมั่นคงปลอดภัย ครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง
- มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอ เพื่อเสริมสร้างทักษะในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย (secure software development)
- กำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงานธุรกิจ (business requirement) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐานที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด (security requirement) และ sign off ก่อนเริ่มออกแบบระบบ <u>การออกแบบระบบ</u>
- จัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมการรักษาความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด (security

specification) รวมทั้งจัดให้มีการสอบทานความถูกต้องครบถ้วนและ sign off จากผู้ที่เกี่ยวข้องก่อนเริ่มพัฒนาระบบ

- จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่าง ๆ ด้านประสิทธิภาพ ตามความต้องการของหน่วยงานธุรกิจ (business requirement) รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด เพื่อเป็นแนวทางการพัฒนาระบบและสอบทานผลการทดสอบก่อนที่จะออกใช้งานจริง (exit criteria)

<u>การพัฒนาระบบ</u>

- มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) การทดสอบ (testing) และระบบที่ให้บริการจริง (production) ออกจากกัน เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง
- มีการควบคุมเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้มีความปลอดภัยเพียงพอตามระดับความเสี่ยงเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- มีกระบวนการหรือเครื่องมือในการควบคุมเวอร์ชั่นของคำสั่งในการเขียนโปรแกรม (source code version control)
- 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) performance test
  (5) security test ตาม security specification

  ทั้งนี้ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีกระบวนการและเอกสารการ sign off ผลการทดสอบระบบจากฝ่ายงานที่เกี่ยวข้อง ที่ผ่านตาม exit criteria อย่างครบถ้วน ก่อนนำระบบขึ้นใช้งานจริง
- มีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอ
- การพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการ การทำธุรกรรมทางอิเล็กทรอนิกส์ หรือระบบที่มีการเชื่อมโยงกับระบบอื่นจำนวนมาก ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีการทดสอบประสิทธิภาพ (performance test) เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการใช้งานจำนวนมาก

- มีการทดสอบระบบรักษาความปลอดภัยควรครอบคลุมการประเมินช่องโหว่ (vulnerability assessment) ของระบบงาน และกรณีเป็นระบบที่เชื่อมต่อกับภายนอก ควรมีการทำทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญภายนอกเพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริง
- มีการสอบทานคำสั่งในการเขียนโปรแกรม (sourcecode review) อย่างเป็นอิสระ ทุกครั้งที่ผู้ให้บริการและผู้ประกอบธุรกิจ มีการพัฒนาหรือเปลี่ยนแปลงระบบในส่วนที่เป็นการทำธุรกรรมสำคัญ เพื่อระบุช่องโหว่ด้านความมั่นคงปลอดภัย
- มีแนวทางการควบคุมการรักษาความปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ เช่น data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูลสำคัญดังกล่าว
- มีกระบวนการในการจัดการข้อผิดพลาดหรือข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ เพื่อพิจารณาแนวทางปรับปรุงหรือลดความเสี่ยงหรือผลกระทบของข้อผิดพลาดหรือข้อบกพร่องที่มีต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ
- มีการจัดทำคู่มือและอบรมผู้ใช้งานระบบ เพื่อให้มีความเข้าใจฟังก์ชันการทำงานและมีการใช้งานระบบอย่างปลอดภัย รวมถึงจัดให้มีคู่มือการดูแลระบบและอบรมผู้ดูแลระบบ เพื่อสามารถตรวจสอบและจัดการแก้ไขปัญหาได้
- หลังจากนำระบบขึ้นใช้งานจริงผู้ให้บริการและผู้ประกอบธุรกิจ ควรพิจารณาจัดให้มีการทดสอบจริงในวงจำกัด (pilot test) สำหรับฟังก์ชันการทำงานที่สำคัญ รวมทั้งจัดให้มีการติดตามการใช้งานระบบหลังจากให้บริการจริงอย่างใกล้ชิดตามระยะเวลาที่เหมาะสม เพื่อให้มั่นใจต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ

  <u>การนำระบบขึ้นใช้งานจริง (system deployment)</u>
- การนำระบบขึ้นใช้งานจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ผู้ให้บริการและผู้ประกอบธุรกิจ กำหนดเพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน
- มีการจัดเก็บการเปลี่ยนแปลง (version control) ของระบบงานขึ้นใช้งานจริงทั้งหมด โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ
- ระบบงานสำรองควรปรับปรุงให้มีความเป็นปัจจุบัน เพื่อให้มีความพร้อมใช้งานเมื่อเกิดเหตุฉุกเฉิน

2.8 การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem management)

2.8.1 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT incident management)

<u>วัตถุประสงค์</u> เพื่อให้มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ให้สามารถจัดการแก้ไขปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจ

2.8.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ครอบคลุมตั้งแต่กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดำเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ

2.8.1.2 กำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ (escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้องหรือคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจได้รับทราบ 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

2.8.1.6 จัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย โดยครอบคลุม วัน เวลา เหตุการณ์ ความเสียหาย การวิเคราะห์สาเหตุที่แท้จริง การวิเคราะห์ผลกระทบ การแก้ไขปัญหาและแนวทางหรือแผนดำเนินการเพื่อป้องกันเหตุการณ์ผิดปกติในอนาคต และในกรณีที่เป็นความเสียหายส่งผลกระทบต่อชื่อเสียงและการให้บริการหรือดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจ อย่างมีนัยสำคัญ ให้รายงานต่อคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ ทราบด้วย

2.8.1.7 ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียงของผู้ให้บริการและผู้ประกอบธุรกิจ รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของผู้ให้บริการและผู้ประกอบธุรกิจ ถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่ผู้ให้บริการและผู้ประกอบธุรกิจต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของผู้ให้บริการและผู้ประกอบธุรกิจทราบ โดยให้ผู้ให้บริการและผู้ประกอบธุรกิจ รายงานปัญหาหรือเหตุการณ์ดังกล่าวมายัง ธปท. ทันทีเมื่อเกิดหรือรับรู้ปัญหาหรือเหตุการณ์นั้น และให้ผู้ให้บริการและผู้ประกอบธุรกิจแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

2.8.1.8 มีกระบวนการบริหารภาวะวิกฤต (crisis management) เพื่อรองรับกรณีเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศเพิ่มระดับความรุนแรงหรือมีความยืดเยื้อ อย่างน้อย ดังนี้

- ผู้ให้บริการและผู้ประกอบธุรกิจ 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 ผู้ใช้บริการของระบบหรือลูกค้าที่ได้รับผลกระทบ

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 โดยคำนึงความสอดคล้องกับนโยบายการบริหารความต่อเนื่องของธุรกิจและนโยบายการบริหารความเสี่ยงของผู้ให้บริการและผู้ประกอบธุรกิจ

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

2.9.3 นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมอย่างน้อย

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

การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

2.9.4 มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยต้องได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย โดยจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.9.5 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น

2.9.6 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงลักษณะการให้บริการหรือดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงที่เกี่ยวข้องในการให้บริการหรือดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจ เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการให้บริการหรือดำเนินธุรกิจ (interdependency risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และความเสี่ยงที่มีผลกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจ ผู้ใช้บริการ ผู้มีส่วนได้เสียและระบบการชำระเงิน (systemic risk)

2.9.7 กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมการดำเนินการ ดังนี้

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

- การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศผู้ให้บริการและผู้ประกอบธุรกิจ ต้องมีการกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและแนวทางจัดเตรียมทรัพยากรระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามการจัดลำดับความสำคัญของระบบงาน โดยพิจารณาอย่างน้อยครอบคลุม
  (1) เป้าหมายระยะเวลาที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ เช่น RTO, RPO เป็นต้น
  (2) ปัจจัยสำคัญที่สนับสนุนให้แผนเป็นไปตามกลยุทธ์ เช่น เทคโนโลยีในการสำรองและกู้คืนข้อมูล ความพร้อมใช้ของสถานที่ปฏิบัติงานสำรอง เป็นต้น เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจ มีทิศทางในการพัฒนาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่บรรลุเป้าหมายที่กำหนดไว้
  (3) ทรัพยากรและงบประมาณ เพื่อจัดเตรียมระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามแผนกลยุทธ์และกิจกรรมที่ต้องดำเนินการทั้งหมด
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรมีการระบุกระบวนการและขั้นตอนสนับสนุนการปฏิบัติที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ 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 ทั้งนี้ผู้ให้บริการและผู้ประกอบธุรกิจ ควรจัดทำเอกสารหรือคู่มือประกอบการกู้คืนในแต่ละระบบ ในกรณีที่มีการปรับปรุงหรือเพิ่มเติมขั้นตอนนอกเหนือจากที่ระบุในแผนขณะปฏิบัติงานจริงผู้ให้บริการและผู้ประกอบธุรกิจควรมีกระบวนการรายงานและขออนุมัติจากผู้บริหารตามที่กำหนดในโครงสร้างการบังคับบัญชา พร้อมทั้งนำขั้นตอนดังกล่าวมาปรับปรุงแผนให้เป็นปัจจุบัน
  (6) ขั้นตอนในการกลับคืนสู่ภาวะปกติ (return to normal) และการประกาศยกเลิกแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
  (7) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง
- การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศผู้ให้บริการและผู้ประกอบธุรกิจ ต้องจัดให้มีการสื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และจัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้อง
  (1) ในการสื่อสารแผนฯ ต้องมีการระบุแนวทางสื่อสารที่ชัดเจนให้บุคลากรทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน
  (2) จัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยควรครอบคลุม วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงาน

และการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน ระบบรักษาความปลอดภัย กระบวนการเฉพาะของแต่ละกลุ่มดำเนินงาน และความรับผิดชอบของแต่ละบุคคล เป็นต้น

- การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

(1) จัดให้มีแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียดอย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้อง ทั้งนี้แผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปีในภาพรวมควรได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย

(2) จัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศทั้งในระดับหน่วยงานและระดับองค์กรอย่างน้อยปีละ 1 ครั้ง โดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการสมาชิก ผู้ใช้บริการของระบบหรือลูกค้าหรือต่อผู้ให้บริการและผู้ประกอบธุรกิจทั้งระบบ เช่น ระบบการโอนและชำระเงินระหว่างผู้ให้บริการและผู้ประกอบธุรกิจ เป็นต้น นอกจากนี้อาจพิจารณาการทดสอบระบบสำรองในลักษณะเสมือนจริง (DR live test) เพื่อให้มั่นใจว่าระบบสำรองสามารถรองรับให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง

(3) กรณีระบบงานมีการเชื่อมโยงระบบเครือข่ายสื่อสารหรือใช้บริการจากหน่วยงานภายนอก ผู้ให้บริการและผู้ประกอบธุรกิจ ควรมีการทดสอบแผนฉุกเฉินร่วมกับหน่วยงานภายนอกที่เกี่ยวข้องด้วย เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ มีความพร้อมใช้งานร่วมกับระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

(4) มีการรายงานผลการทดสอบต่อคณะกรรมการที่ได้รับมอบหมาย โดยมีรายละเอียดอย่างน้อยครอบคลุม วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข

(5) ผู้ให้บริการและผู้ประกอบธุรกิจ ควรจัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงบุคลากรที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน การเปลี่ยนสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศ เป็นต้น เพื่อให้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน

(6) ผู้ให้บริการและผู้ประกอบธุรกิจ อาจจัดให้มีการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยหน่วยงานภายนอกหรือภายในที่มีความเป็นอิสระ เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผนให้สามารถใช้งานได้จริง

2.10 การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

<u>วัตถุประสงค์</u> เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจ มีแนวทางในการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ให้มีความเสี่ยงในระดับที่ผู้ให้บริการและผู้ประกอบธุรกิจยอมรับได้ บนพื้นฐานที่ผู้ให้บริการและผู้ประกอบธุรกิจต้องรับผิดชอบต่อการดำเนินธุรกิจและการให้บริการแก่สมาชิก ผู้ใช้บริการของระบบหรือลูกค้า และคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิภาพและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการให้บริการ

2.10.1 ให้ปฏิบัติตามแนวปฏิบัติของธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management implementation guideline)

3. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

วัตถุประสงค์ 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 รายงานภาพรวมโครงการสำคัญของผู้ให้บริการและผู้ประกอบธุรกิจ ให้กับคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ และผู้บริหารระดับสูงที่เกี่ยวข้องได้รับทราบ เพื่อติดตามและสนับสนุนให้บริหารจัดการโครงการสำเร็จลุล่วงสอดคล้องกับเป้าหมายในระดับกลยุทธ์ของผู้ให้บริการและผู้ประกอบธุรกิจ ตามแผนงานที่กำหนด
- ผู้จัดการโครงการ (project manager) มีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการ ครอบคลุม กำหนดแผนงานโครงการ วิเคราะห์ผลกระทบ และจัดให้มีแนวทางรองรับหรือแผนสำรองกรณีโครงการประสบปัญหาหรือล่าช้า รวมทั้งรายงานให้คณะกรรมการกำกับดูแลโครงการพิจารณาตัดสินใจแก้ไขปัญหาได้ทันการณ์ เพื่อให้โครงการสามารถส่งมอบได้อย่างถูกต้องครบถ้วนสำเร็จตามแผนงานที่กำหนด โดยผู้จัดการโครงการ ต้องมีความรู้ความสามารถและประสบการณ์ในการบริหารโครงการที่เพียงพอ

3.1.2 แนวทางการบริหารจัดการโครงการ ควรกำหนดครอบคลุมอย่างน้อย ดังนี้

- ระเบียบขั้นตอนการบริหารจัดการโครงการ ครอบคลุมตั้งแต่ ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ
- ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ
- รูปแบบของเอกสารหรือผลลัพธ์ที่เป็นมาตรฐาน ที่ต้องส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น

การเริ่มโครงการ

3.2 มีการประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งเลือกใช้เทคโนโลยีที่เหมาะสม ทั้งนี้โครงการต้องมีเป้าหมายที่ชัดเจน (project objective) สอดคล้องกับกลยุทธ์ขององค์กรและคำนึงถึงการรักษาความมั่นคงปลอดภัย

3.3 มีแผนการดำเนินโครงการ ที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการ อย่างน้อยครอบคลุม

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

3.4 มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตในการอนุมัติที่กำหนดไว้

<u>การดำเนินการและควบคุมโครงการ</u>

3.5 มีการบันทึกและจัดเก็บข้อมูลโครงการของแต่ละโครงการอย่างเพียงพอเพื่อใช้ติดตามดูแลและสามารถตรวจสอบย้อนหลังได้

3.6 มีการประเมินและติดตามการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากรที่วางแผนไว้ ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาและหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ

3.7 มีการรายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการ ต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารที่ได้รับมอบหมายอย่างเป็นประจำ เพื่อสามารถให้คำแนะนำและแนวทางในการแก้ไขปัญหาที่จะลดความเสี่ยงที่อาจเกิดขึ้นอย่างทันท่วงที โดยโครงการที่ส่งผลกระทบต่อธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญ ควรนำเสนอแก่คณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ 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 ระเบียบและวิธีปฏิบัติของผู้ให้บริการและผู้ประกอบธุรกิจ รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

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
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
ธนาคารแห่งประเทศไทย

สารบัญ

แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

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

ส่วนที่ 1 : การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (risk governance)

ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยประกอบด้วย การกำหนดบทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงของผู้ให้บริการและผู้ประกอบธุรกิจในการกำกับดูแล การจัดให้มีโครงสร้างองค์กรที่มีการถ่วงดุลในเรื่องการบริหารจัดการความเสี่ยงจากบุคคลภายนอก การบริหารจัดการบุคลากรที่เกี่ยวข้อง การคุ้มครองสมาชิก ผู้ใช้บริการของระบบหรือลูกค้า การจัดให้มีนโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก และการตรวจสอบ ดังนี้

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

    1.1 ดูแลให้การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องกับกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจ มีการบริหารความเสี่ยงให้อยู่ในระดับที่ผู้ให้บริการและผู้ประกอบธุรกิจยอมรับได้ (risk appetite) และไม่ขัดต่อกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

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

    1.3 จัดให้มีการกำกับและควบคุมดูแลการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้เป็นไปตามนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติที่กำหนด และพิจารณาให้ความเห็นชอบต่อการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลที่มีนัยสำคัญ

2. จัดโครงสร้างองค์กรให้มีการถ่วงดุล

    ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดโครงสร้างองค์กร และหน้าที่ความรับผิดชอบที่เกี่ยวกับการบริหารจัดการบุคคลภายนอกให้มีการถ่วงดุลตามหลัก 3 lines of defence โดยมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนและมีการถ่วงดุลในการทำหน้าที่ของหน่วยงานที่ทำหน้าที่ปฏิบัติงาน (1st line) บริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ (2nd line) และการตรวจสอบ (3rd line)

    2.1 หน้าที่ของหน่วยงานที่ทำหน้าที่ปฏิบัติงานกับบุคคลภายนอก (1st line)

    เพื่อให้การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีประสิทธิภาพ มีการบริหารจัดการความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด 1st line ควรมีหน้าที่ครอบคลุม ดังนี้

(1) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และประเมินศักยภาพของบุคคลภายนอก (due diligence) ก่อนเริ่มหรือต่อสัญญาหรือข้อตกลง

(2) จัดให้มีกรอบและแนวทางการประเมิน ควบคุม และติดตามผลอย่างสม่ำเสมอและต่อเนื่อง ทั้งด้านประสิทธิภาพและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (CIA) รวมถึงการดูแลคุ้มครองข้อมูลส่วนบุคคลด้วย

(3) ติดตามการเปลี่ยนแปลง ปัญหาและเหตุการณ์ผิดปกติสำคัญที่เกิดขึ้นอันสืบเนื่องหรือเกี่ยวเนื่องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อดูแลให้การดำเนินการของบุคคลภายนอกเป็นไปตามที่ระบุในสัญญาหรือข้อตกลง

(4) รายงานผลการปฏิบัติงาน ผลการประเมินความเสี่ยง ปัญหาและเหตุการณ์ผิดปกติที่ส่งผลกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย อย่างเพียงพอ ต่อเนื่อง ทันการณ์ และสอดรับกับระดับความเสี่ยง

2.2 หน้าที่ของหน่วยงานที่ทำหน้าที่บริหารความเสี่ยง และการกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ (2nd line)

เพื่อให้การบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีประสิทธิภาพ มีความมั่นคงปลอดภัยตามกรอบการบริหารความเสี่ยงของผู้ให้บริการและผู้ประกอบธุรกิจตลอดจนปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง 2nd line ควรมีหน้าที่ครอบคลุม ดังนี้

(1) จัดให้มีกรอบและกระบวนการบริหารความเสี่ยงตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป ประกอบไปด้วย การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามทบทวนความเสี่ยง และการรายงานความเสี่ยง

(2) ติดตามดูแลให้ 1st line มีการบริหารความเสี่ยง และให้มีการรายงานความเสี่ยงดังกล่าวมายัง 2nd line เพื่อรวบรวมและเชื่อมโยงความเสี่ยงดังกล่าวกับความเสี่ยงด้านอื่นของผู้ให้บริการและผู้ประกอบธุรกิจ ตลอดจนชี้แนะและให้คำปรึกษาในการบริหารจัดการความเสี่ยงของ 1st line

(3) ติดตามความเสี่ยง และทบทวนการควบคุมและการบริหารจัดการความเสี่ยง ซึ่งรวมถึงการทบทวนปัจจัยเสี่ยง ดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) และกระบวนการควบคุมและบริหารจัดการความเสี่ยง เพื่อให้มั่นใจว่าผู้ให้บริการและผู้ประกอบธุรกิจมีความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกในระดับความเสี่ยงที่ผู้ให้บริการและผู้ประกอบธุรกิจยอมรับได้ รวมทั้งนำเสนอผลการบริหารความเสี่ยงดังกล่าวต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

(4) กำกับดูแลการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง รวมถึงดูแลให้เป็นไปตามนโยบาย มาตรฐานระเบียบปฏิบัติของผู้ให้บริการและผู้ประกอบธุรกิจ ตลอดจนมาตรฐานสากลที่ผู้ให้บริการและผู้ประกอบธุรกิจอ้างอิงหรือนำมาบังคับใช้ และนำเสนอรายงานผลการปฏิบัติตามกฎหมายและกฎเกณฑ์ต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

2.3 หน้าที่การตรวจสอบ (3rd line)

เพื่อให้มั่นใจว่าการทำหน้าที่ 1st line และ 2nd line ในการควบคุมดูแล และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกของผู้ให้บริการและผู้ประกอบธุรกิจเป็นไปตามนโยบาย มาตรฐาน ระเบียบปฏิบัติที่เกี่ยวข้อง 3nd line ควรมีหน้าที่ครอบคลุม ดังนี้

(1) จัดให้มีการตรวจสอบการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยผู้ตรวจสอบภายนอกที่เป็นอิสระ เพื่อตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ 1st line 2nd line และบุคคลภายนอก ว่ามีการปฏิบัติตามนโยบาย มาตรฐาน ระเบียบปฏิบัติของผู้ให้บริการและผู้ประกอบธุรกิจ สัญญาหรือข้อตกลง และการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(2) รายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบ

3. การบริหารจัดการบุคลากรที่เกี่ยวข้อง

การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ทำให้บทบาทหน้าที่รวมถึงความรู้ความเชี่ยวชาญในการปฏิบัติงานเปลี่ยนแปลงจากที่ผู้ให้บริการและผู้ประกอบธุรกิจเคยดำเนินการ ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดสรรบุคลากร สร้างความเข้าใจและความตระหนักก่อนการเปลี่ยนแปลง รวมถึงพัฒนาความรู้ความเชี่ยวชาญของบุคลากรที่เกี่ยวข้อง ให้เพียงพอในการปฏิบัติงานอย่างมีประสิทธิภาพ เช่น จัดให้มีการพัฒนาทักษะความรู้ของพนักงานที่เกี่ยวข้องครอบคลุมการบริหารจัดการความเสี่ยงจากบุคคลภายนอก การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรณีการใช้ cloud computing ควรเสริมสร้างทักษะความรู้ให้แก่ผู้บริหารและพนักงานที่เกี่ยวข้องให้สามารถปฏิบัติงานได้ตามมาตรฐานและแนวปฏิบัติที่ดีของผู้ให้บริการ cloud computing เป็นต้น

4. การคุ้มครองสมาชิก ผู้ใช้บริการของระบบหรือลูกค้าของผู้ให้บริการและผู้ประกอบธุรกิจ

กรณีที่ผู้ให้บริการและผู้ประกอบธุรกิจมีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้บริการแก่สมาชิก ผู้ใช้บริการของระบบหรือลูกค้า ผู้ให้บริการและผู้ประกอบธุรกิจควรดำเนินการ ดังนี้

4.1 ดูแลและบริหารจัดการบุคคลภายนอกที่มีการเข้าถึง การใช้ และการดูแลรักษาข้อมูลสมาชิก ผู้ใช้บริการของระบบหรือลูกค้าอย่างรัดกุม เพื่อให้ข้อมูลสมาชิก ผู้ใช้บริการของระบบหรือลูกค้าได้รับการดูแลอย่างปลอดภัย โดยคำนึงถึงความเป็นส่วนตัว และเป็นไปตามกฎหมายอื่นที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

4.2 ดูแลการแก้ไขปัญหาและจัดการเรื่องร้องเรียนให้แก่สมาชิก ผู้ใช้บริการของระบบหรือลูกค้าอย่างรับผิดชอบและเป็นธรรม

5. นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

5.1 ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดนโยบายที่ครอบคลุมถึงการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างชัดเจนเป็นลายลักษณ์อักษร โดยอาจเป็นนโยบายที่จัดทำขึ้นเฉพาะหรือรวมอยู่ในนโยบายที่ผู้ให้บริการและผู้ประกอบธุรกิจมีอยู่แล้ว

5.2 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกควรสอดคล้องกับนโยบายอื่นที่เกี่ยวข้องของผู้ให้บริการและผู้ประกอบธุรกิจ เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

5.3 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกได้รับอนุมัติจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรจัดชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและควบคุมดูแลให้ปฏิบัติตามนโยบาย

5.4 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ควรครอบคลุม

(1) โครงสร้างการกำกับดูแล บทบาทหน้าที่ของผู้เกี่ยวข้องในการกำกับดูแลและบริหารจัดการความเสี่ยงจากบุคคลภายนอก

(2) หลักเกณฑ์การจัดระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

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

(4) หลักเกณฑ์การขออนุมัติความเห็นชอบ และการรายงานต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

(5) การตรวจสอบการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(6) การเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญ เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ซึ่งรวมถึงการมีข้อมูลพร้อมใช้สำหรับการดำเนินธุรกิจและการให้บริการแก่สมาชิก ผู้ใช้บริการของระบบหรือลูกค้า

(7) การคุ้มครองสมาชิก ผู้ใช้บริการของระบบหรือลูกค้าของผู้ให้บริการและผู้ประกอบธุรกิจ

5.5 ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีมาตรฐานและระเบียบวิธีปฏิบัติ เพื่อสนับสนุนการดำเนินการตามนโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ให้สอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญ รวมถึงมาตรฐานสากลที่ยอมรับโดยทั่วไป

6. การตรวจสอบ

ผู้ให้บริการและผู้ประกอบธุรกิจควรดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ให้บริการและผู้ประกอบธุรกิจ สามารถเข้าตรวจสอบบุคคลภายนอกในส่วนที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของผู้ให้บริการและผู้ประกอบธุรกิจได้ เช่น ระบุเงื่อนไขในสัญญาหรือข้อตกลง เป็นต้น และจัดให้มีการตรวจสอบให้สอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญ โดยการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลที่มีนัยสำคัญควรได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง และเมื่อพบเหตุการณ์ผิดปกติที่มีนัยสำคัญ

ทั้งนี้ หากมีเหตุจำเป็นที่ผู้ให้บริการและผู้ประกอบธุรกิจไม่สามารถดำเนินการตรวจสอบ ระบุสิทธิหรือเงื่อนไขการตรวจสอบในสัญญาหรือข้อตกลงได้ ผู้ให้บริการและผู้ประกอบธุรกิจควรมีแนวทางที่จะใช้ประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอก ให้รัดกุมเพียงพอสอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล โดยผู้ให้บริการและผู้ประกอบธุรกิจอาจใช้ผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล 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)

ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างรัดกุมเพียงพอและต่อเนื่อง และดูแลให้สอดคล้องตามกรอบและกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ (IT risk management) เพื่อให้ความเสี่ยงอยู่ในระดับที่ผู้ให้บริการและผู้ประกอบธุรกิจยอมรับได้ โดยกำหนดให้มีระเบียบวิธีปฏิบัติที่ชัดเจนและเป็นลายลักษณ์อักษร ครอบคลุมวัฏจักรการบริหารจัดการบุคคลภายนอก (third party management life cycle) ตั้งแต่การประเมินความเสี่ยง การคัดเลือกบุคคลภายนอก การจัดทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานอย่างต่อเนื่อง และการยกเลิก/สิ้นสุดสัญญาหรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้าน IT

7. การประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

   7.1 ผู้ให้บริการและผู้ประกอบธุรกิจควรประเมินความเสี่ยงและผลกระทบทั้งก่อนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงจากบุคคลภายนอก และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ รวมถึงประเมินเป็นประจำตามรอบระยะเวลาที่สอดคล้องตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญอย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงความเสี่ยงดังต่อไปนี้

   (1) ความเสี่ยงด้านกลยุทธ์ (strategic risk)

   (2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่ครอบคลุมและรัดกุมเพียงพอ

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

   (4) ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยทางไซเบอร์ เช่น ระบบขัดข้องหรือหยุดบริการโดยมีสาเหตุจากบุคคลภายนอก ระบบของบุคคลภายนอกมีช่องโหว่ด้านความปลอดภัยทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล บุคคลภายนอกใช้งานสิทธิสูงเกินกว่าที่ได้รับอนุญาต การจัดเตรียมทรัพยากรระบบไม่เพียงพอ เป็นต้น

   (5) ความเสี่ยงด้านกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น การปฏิบัติไม่ถูกต้องตามพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 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) ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง (third party/vendor locked-in) โดยการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก อาจทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยีของผู้ให้บริการหรือพันธมิตร และข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

(9) ความเสี่ยงจากการกระจุกตัว (concentration risk) เช่น ผู้ให้บริการและผู้ประกอบธุรกิจใช้บริการจากบุคคลภายนอกเพียงรายเดียว (single provider) ในทุกการใช้บริการจากบุคคลภายนอก เป็นต้น

(10) ความเสี่ยงจากบุคคลภายนอกว่าจ้างผู้อื่นดำเนินการแทน (subcontractor) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น

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

7.3 การจัดระดับความเสี่ยงและระดับความมีนัยสำคัญ ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดหลักเกณฑ์ที่ชัดเจน และจัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ให้ครอบคลุมครบถ้วนตามหลักเกณฑ์ที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด โดยควรมีรายละเอียดครอบคลุมตามที่กล่าวในข้อ 12.1 (2) เพื่อผู้ให้บริการและผู้ประกอบธุรกิจสามารถใช้บริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของบุคคลภายนอกได้ครบถ้วนต่อเนื่อง

8. การคัดเลือกบุคคลภายนอก

8.1 ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดให้มีระเบียบวิธีปฏิบัติและหลักเกณฑ์ในการพิจารณาคัดเลือกบุคคลภายนอก อย่างชัดเจน และเป็นลายลักษณ์อักษร โดยมีข้อมูลที่เพียงพอสำหรับสนับสนุนการพิจารณาตัดสินใจใช้บริการ เชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อสามารถคัดเลือกบุคคลภายนอกที่มีความเหมาะสมตามวัตถุประสงค์การดำเนินการของผู้ให้บริการและผู้ประกอบธุรกิจ

8.2 การตัดสินใจใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่มีความเสี่ยงหรือมีนัยสำคัญควรได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

8.3 ผู้ให้บริการและผู้ประกอบธุรกิจควรทำการประเมินศักยภาพบุคคลภายนอก (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 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 ผู้ให้บริการและผู้ประกอบธุรกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเป็นลายลักษณ์อักษร และจัดเก็บสัญญาหรือข้อตกลงดังกล่าวไว้ที่ผู้ให้บริการและผู้ประกอบธุรกิจเพื่อสามารถบังคับใช้ได้ตามกฎหมาย

9.2 ผู้ให้บริการและผู้ประกอบธุรกิจควรระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญในสัญญาหรือข้อตกลงกับบุคคลภายนอกอย่างชัดเจน โดยพิจารณาให้ครอบคลุมตามขอบเขต ระดับความเสี่ยง และความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ดังนี้

(1) ขอบเขตการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(2) บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอก และผู้ให้บริการและผู้ประกอบธุรกิจ

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

(4) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรสอดคล้องกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ

(5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก (ongoing monitoring) ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือเหตุการณ์ที่สำคัญ และรายงานปัญหาผิดปกติ

(6) กำหนดให้การคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการและผู้ประกอบธุรกิจและข้อมูลของสมาชิก ผู้ใช้บริการของระบบหรือลูกค้า เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น การกำหนดให้บุคคลภายนอกออกหนังสือรับรองการทำลายข้อมูลของผู้ให้บริการและผู้ประกอบธุรกิจ

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

(9) แนวทางการระงับข้อพิพาท และความรับผิดต่อความเสียหาย

(10) การระบุสิทธิในการเข้าตรวจสอบโดยผู้ให้บริการและผู้ประกอบธุรกิจ ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ให้บริการและผู้ประกอบธุรกิจหรือ ธปท. ให้สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกที่มีนัยสำคัญ

9.3 ในกรณีเป็นการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) ที่มีนัยสำคัญ ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดสิทธิของผู้ให้บริการและผู้ประกอบธุรกิจในการพิจารณาอนุมัติกรณีบุคคลภายนอกว่าจ้างผู้รับเหมาช่วง (subcontract) และข้อกำหนดที่บุคคลภายนอกต้องรับผิดชอบต่อผลการปฏิบัติงานของผู้รับเหมาช่วง

9.4 กรณีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่ตั้งอยู่ในต่างประเทศ สัญญาหรือข้อตกลงในการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกควรพิจารณาถึงความเสี่ยงและอุปสรรคที่อาจเกิดขึ้นจากประเทศที่บุคคลภายนอกตั้งอยู่หรือประกอบธุรกิจ (country risk) ด้วย

10. การติดตามผลการปฏิบัติงานของบุคคลภายนอก

10.1 ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น กำหนดให้บุคคลภายนอกรายงานผลการปฏิบัติงานอย่างสม่ำเสมอ กำหนดการประชุมติดตามอย่างสม่ำเสมอและต่อเนื่อง การเข้าสังเกตการณ์การดำเนินงานของบุคคลภายนอก เป็นต้น

10.2 ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดให้บุคคลภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องให้ผู้ให้บริการและผู้ประกอบธุรกิจได้รับทราบอย่างทันการณ์ เพื่อประเมินผลกระทบที่มีต่อผู้ให้บริการและผู้ประกอบธุรกิจ ทั้งนี้กรณีประเมินว่าผลกระทบที่เกิดขึ้นมีผลต่อการดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญ ผู้ให้บริการและผู้ประกอบธุรกิจควรมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ

10.3 ผู้ให้บริการและผู้ประกอบธุรกิจควรทบทวนการประเมินศักยภาพ การประเมินผลการปฏิบัติงาน และการประเมินความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ทั้งในด้านประสิทธิภาพการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และการปฏิบัติตามกฎหมาย เมื่อจะต่อสัญญาและเมื่อถึงรอบระยะเวลาที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด ทั้งนี้ การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่มีนัยสำคัญควรกำหนดให้ดำเนินการ

อย่างน้อยปีละครั้ง รวมถึงให้รายงานผลการประเมินดังกล่าวต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

11. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง

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

11.2 การพิจารณายกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง ผู้ให้บริการและผู้ประกอบธุรกิจควรประเมินผลกระทบและความเสี่ยงที่อาจเกิดขึ้นจากการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง และดำเนินการตามมาตรฐานหรือระเบียบปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง และกำหนดกลยุทธ์และแผนงานการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง (exit strategy and exit plan) ที่ชัดเจน เพื่อให้มั่นใจว่าการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลงเป็นไปอย่างมีประสิทธิภาพและได้เตรียมความพร้อมต่อผลกระทบที่อาจเกิดขึ้น เช่น การหยุดให้บริการของระบบที่ส่งผลกระทบกับสมาชิกผู้ใช้บริการของระบบหรือลูกค้า การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

12. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

ผู้ให้บริการและผู้ประกอบธุรกิจควรดูแลให้มั่นใจว่าการใช้บริการ 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 ผู้ให้บริการและผู้ประกอบธุรกิจควรนำแนวปฏิบัติที่ดีของผู้ให้บริการ Cloud Computing มาเป็นแนวทางในการปฏิบัติงานและควบคุมดูแลเพื่อให้ระบบที่ใช้บริการ Cloud Computing มีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และควรดำเนินการตามแนวทางการควบคุมเพิ่มเติม ดังต่อไปนี้

12.1 การจัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกและทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

(1) จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำ และปรับปรุงทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจสามารถนำมาใช้ระบุความเสี่ยงได้อย่างชัดเจน

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 การใช้บริการของผู้ให้บริการและผู้ประกอบธุรกิจชำระเงินกลาง เป็นต้น
- ระดับความเสี่ยง และระดับความมีนัยสำคัญ
- ที่ตั้งศูนย์คอมพิวเตอร์หลักและสำรองของบุคคลภายนอกที่ประมวลผล จัดเก็บข้อมูล หรือดำเนินการใด ๆ เกี่ยวกับข้อมูลหรือระบบงานให้แก่ผู้ให้บริการและผู้ประกอบธุรกิจ
- วันเริ่มต้นและสิ้นสุดสัญญาหรือข้อตกลง
- การรับรองตามมาตรฐานสากลด้าน IT ที่เกี่ยวข้อง (ถ้ามี)
- รายละเอียดทรัพย์สินที่เกี่ยวข้อง เช่น ข้อมูลที่นำไปจัดเก็บหรือประมวลผล ระดับชั้นความลับข้อมูล เป็นต้น

12.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

(1) ทำการเข้ารหัสข้อมูลที่อยู่ภายใต้การดูแลของบุคคลภายนอกให้เป็นไปตามนโยบายและมาตรฐานของผู้ให้บริการและผู้ประกอบธุรกิจสอดคล้องกับมาตรฐานสากลตามระดับชั้นของข้อมูล (information classification) และพิจารณาให้ครอบคลุมทั้งข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest) ซึ่งรวมถึงข้อมูลสำรอง

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

(3) สร้างกุญแจการเข้ารหัสข้อมูลด้วยตนเอง ทั้งนี้ หากผู้ให้บริการและผู้ประกอบธุรกิจไม่สามารถสร้างกุญแจการเข้ารหัสด้วยตนเองได้ ผู้ให้บริการและผู้ประกอบธุรกิจควรมั่นใจได้ว่ากุญแจการเข้ารหัสของบุคคลภายนอกไม่มีการนำมาใช้ร่วมกับผู้ใช้บริการรายอื่น และทราบถึงรายละเอียดเกี่ยวกับระบบการบริหารจัดการกุญแจเข้ารหัสข้อมูลของบุคคลภายนอก ได้แก่

- ประเภทของกุญแจเข้ารหัสข้อมูล

- รายละเอียดของระบบ รวมถึงกระบวนการควบคุมการเข้ารหัสข้อมูลในแต่ละขั้นตอนตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส
- ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล

(4) เก็บกุญแจการเข้ารหัสข้อมูลในอุปกรณ์รักษาความปลอดภัย เช่น Hardware Security Module (HSM) เป็นต้น และดูแลรักษาความปลอดภัยอุปกรณ์ HSM ด้วยการจัดตั้งในโซนเครือข่ายที่ปลอดภัยและจำกัดการเชื่อมต่อกับระบบงานอื่นที่ไม่เกี่ยวข้อง

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

12.3 การควบคุมการเข้าถึง (access control)

(1) กำหนดกระบวนการจัดการและควบคุมดูแลสิทธิในการเบิกใช้และการเข้าถึงระบบและข้อมูลของผู้ให้บริการและผู้ประกอบธุรกิจที่ชัดเจนเป็นลายลักษณ์อักษร เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนดสอดคล้องตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป

(2) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้มีสิทธิเข้าใช้งานระบบและผู้ใช้งานที่ได้รับสิทธิสูงให้ชัดเจน

(3) ควบคุมดูแลการให้สิทธิแก่บุคคลภายนอก โดยจำกัดสิทธิตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน มีการอนุมัติการเบิกใช้งาน เพื่อไม่ให้บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ

(4) มีระบบหรือกระบวนการติดตามระหว่างการใช้งานบัญชีผู้ใช้งานที่มีสิทธิสูงสุด รวมทั้งควรติดตามและสอบทานสถานะสิทธิและการใช้งานหรือการเข้าถึงระบบข้อมูล ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิอย่างเป็นประจำ เพื่อให้มั่นใจว่าการใช้งานสิทธิเป็นไปตามขอบเขต และความจำเป็นในการใช้งาน

(5) กำหนดวิธีการระบุและพิสูจน์ตัวตนผู้ใช้งาน ด้วยวิธีการที่รัดกุมเพียงพอ สอดคล้องกับมาตรฐานนโยบายที่ผู้ให้บริการและผู้ประกอบธุรกิจกำหนด หรือมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป

(6) ในกรณีที่บุคคลภายนอกเชื่อมต่อเพื่อเข้าถึงระบบงานของผู้ให้บริการและผู้ประกอบธุรกิจผ่านช่องทางการเข้าถึงระบบงานระยะไกล (system remote access) ผู้ให้บริการและผู้ประกอบธุรกิจควรมีกระบวนการบริหารจัดการการเข้าถึงระยะไกลด้วยวิธีการที่ปลอดภัย 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
- สามารถระบุและสอบทานแหล่งที่มาของอุปกรณ์หรือระบบปลายทางที่เข้าเชื่อมต่อกับระบบเครือข่ายของผู้ให้บริการและผู้ประกอบธุรกิจแบบระยะไกล
- สอบทานการเข้าถึงระบบงานระยะไกล โดยบัญชีผู้ใช้งานสิทธิสูงด้วยบุคคลหรือหน่วยงานที่มีความเป็นอิสระและมีความรู้ความเชี่ยวชาญเพียงพอ

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

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

(3) กรณีการใช้บริการ cloud computing ผู้ให้บริการ cloud computing ควรแบ่งแยกสภาพแวดล้อมของผู้ให้บริการและผู้ประกอบธุรกิจจากผู้ใช้บริการรายอื่นที่อยู่ในสภาพแวดล้อมบน cloud computing ร่วมกัน

12.5 การบริหารจัดการการเปลี่ยนแปลง (change management)

(1) กำหนดกระบวนการและแนวทางบริหารจัดการการเปลี่ยนแปลงร่วมกับบุคคลภายนอก เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจสามารถประเมินผลกระทบและเตรียมแนวทางรองรับ

เช่น เมื่อมีการเปลี่ยนแปลงระบบของผู้ให้บริการ cloud computing และกระทบกับการให้บริการและดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจ

(2) ให้บุคคลภายนอกแจ้งการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบกับการให้บริการและดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจให้ผู้ให้บริการและผู้ประกอบธุรกิจได้ทราบล่วงหน้าในระยะเวลาที่ตกลงร่วมกัน เพื่อให้ผู้ให้บริการและผู้ประกอบธุรกิจพิจารณาแนวทางลดผลกระทบต่อการให้บริการสมาชิก ผู้ใช้บริการของระบบหรือลูกค้าของผู้ให้บริการและผู้ประกอบธุรกิจ

12.6 การบริหารจัดการการตั้งค่าระบบ (system configuration management)

กรณีบุคคลภายนอกมีหน้าที่เปลี่ยนแปลงการตั้งค่าระบบงาน ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดมาตรฐานการตั้งค่าระบบงานให้ปลอดภัยเพียงพอตามมาตรฐานด้านความปลอดภัยเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ เช่น ค่า System Configuration ของระบบปฏิบัติการและการตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย 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 เพื่อให้ ผู้ให้บริการและผู้ประกอบธุรกิจทราบอย่างทันการณ์

12.8 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

ดูแลให้มั่นใจว่าบุคคลภายนอกมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัยเพื่อผู้ให้บริการและผู้ประกอบธุรกิจใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน 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) ตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป และสอดคล้องกับนโยบายระเบียบวิธีปฏิบัติของผู้ให้บริการและผู้ประกอบธุรกิจ

(2) สอบทานขอบเขตและผลการทดสอบเจาะระบบ (penetration testing) ของบุคคลภายนอก เพื่อให้มั่นใจว่าการทดสอบดังกล่าวครอบคลุมระบบทั้งหมดที่ผู้ให้บริการและผู้ประกอบธุรกิจใช้บริการหรือเชื่อมต่อกับบุคคลภายนอก และครอบคลุมภัยคุกคามที่สำคัญ

12.11 การสำรองข้อมูล (data backup)

กรณีที่ผู้ให้บริการและผู้ประกอบธุรกิจใช้บริการหรือเชื่อมต่อกับบุคคลภายนอก ซึ่งมีการจัดเก็บข้อมูลของผู้ให้บริการและผู้ประกอบธุรกิจ หรือข้อมูลสมาชิก ผู้ใช้บริการของระบบหรือลูกค้า ผู้ให้บริการและผู้ประกอบธุรกิจควรกำหนดมาตรฐานวิธีปฏิบัติในการสำรองข้อมูลให้บุคคลภายนอกปฏิบัติให้สอดคล้องกับมาตรฐานของผู้ให้บริการและผู้ประกอบธุรกิจ โดยครอบคลุม

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

12.12 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT incident management)

(1) ระบุหน้าที่และความรับผิดชอบของผู้ให้บริการและผู้ประกอบธุรกิจและบุคคลภายนอกอย่างชัดเจนในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ รวมถึงกำหนดระดับความรุนแรงของเหตุการณ์ผิดปกติดังกล่าว และกำหนดให้แจ้งผู้ให้บริการและผู้ประกอบธุรกิจทราบเหตุการณ์ผิดปกติที่เกิดขึ้นและเกี่ยวข้องกับผู้ให้บริการและผู้ประกอบธุรกิจอย่างเพียงพอและทันการณ์

(2) หากเหตุการณ์ผิดปกติที่เกิดขึ้นนั้นมีผลกระทบต่อการดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญ ผู้ให้บริการและผู้ประกอบธุรกิจควรมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ

(3) กำหนดให้บุคคลภายนอกจัดให้มีช่องทาง ระบบ หรือเครื่องมือเพื่อรองรับกรณี ผู้ให้บริการและผู้ประกอบธุรกิจตรวจพบและต้องการรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศให้บุคคลภายนอกทราบ และเพื่อช่วยให้ผู้ให้บริการและผู้ประกอบธุรกิจติดตามสถานการณ์และการแก้ไขของบุคคลภายนอกต่อเหตุการณ์ผิดปกติที่เกี่ยวข้องกับผู้ให้บริการและผู้ประกอบธุรกิจได้อย่างทันการณ์

(4) กำหนดให้บุคคลภายนอกมีผู้ประสานงานอย่างเป็นทางการ เพื่อประสานงานกับผู้ให้บริการและผู้ประกอบธุรกิจในการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศได้อย่างทันการณ์

12.13 การบริหารความต่อเนื่องทางธุรกิจ (business continuity management)

(1) มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (disaster recovery plan) ที่ครอบคลุมถึงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้มีแนวทางรองรับต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจอย่างมีนัยสำคัญ เพื่อสามารถให้บริการและดำเนินธุรกิจได้อย่างต่อเนื่อง

(2) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรคำนึงถึงปัจจัยสำคัญหรือความเสี่ยงที่อาจเกิดขึ้นและส่งผลต่อการหยุดชะงักจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ผลกระทบที่มีต่อการให้บริการและดำเนินธุรกิจของผู้ให้บริการและผู้ประกอบธุรกิจ และการติดต่อสื่อสารระหว่างบุคคลภายนอกกับผู้ให้บริการและผู้ประกอบธุรกิจ รวมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติให้คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างทันการณ์ตามความสำคัญและระดับความรุนแรงหรือผลกระทบของเหตุการณ์

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

(4) หากผู้ให้บริการและผู้ประกอบธุรกิจสามารถเข้าร่วมทดสอบกับบุคคลภายนอกได้ ผู้ให้บริการและผู้ประกอบธุรกิจควรเข้าร่วมทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศกับบุคคลภายนอก เพื่อประเมินความพร้อมของบุคคลภายนอกในการกู้คืนระบบงานตามกรอบ MTPD, RTO และ RPO ที่กำหนดไว้

(5) ทีมบริหารจัดการในสภาวะวิกฤติ (crisis management team) ของผู้ให้บริการและผู้ประกอบธุรกิจควรได้รับทราบถึงรายละเอียดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของบุคคลภายนอก เพื่อเตรียมความพร้อมในการบริหารจัดการในส่วนที่เกี่ยวข้อง

(6) รวบรวมปัญหาที่พบระหว่างการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และปรับปรุงแก้ไขร่วมกับบุคคลภายนอก

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