ธนาคารแห่งประเทศไทย

18 พฤศจิกายน 2562

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง

ที่ ฝนส.(01)ว. 125 /2562 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ธนาคารแห่งประเทศไทยขอนำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ลงวันที่ 1 ตุลาคม 2562 ซึ่งได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 136 ตอนพิเศษ 280 ง ลงวันที่ 14 พฤศจิกายน 2562 แล้ว และมีผลบังคับใช้ตั้งแต่วันที่ 15 พฤศจิกายน 2562 เป็นต้นไป

สาระสำคัญของประกาศฉบับนี้ คือ สถาบันการเงินสามารถพิจารณาการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีด้วยตนเอง เพื่อรองรับรูปแบบทางธุรกิจและสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว โดย

1. ธนาคารพาณิชย์ที่มีนัยต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks: D-SIBs) และสถาบันการเงินที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ต้องมีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO)

2. ธนาคารพาณิชย์ต้องรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญประจำปีให้ธนาคารแห่งประเทศไทยทราบ โดยยกเลิกการขออนุญาตธนาคารแห่งประเทศไทยก่อนการนำเทคโนโลยีมาใช้ หรือก่อนการเปลี่ยนแปลงเทคโนโลยีที่มีนัยสำคัญ ทั้งนี้ สำหรับบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ยังคงให้ขออนุญาตการใช้หรือเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ เว้นแต่ธนาคารแห่งประเทศไทยจะสั่งการเป็นอย่างอื่น

3. สถาบันการเงินที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์สำหรับบริษัทในกลุ่มธุรกิจหรือบริษัทที่มีความเกี่ยวข้องกัน โดยให้บริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องกันนั้นเป็นผู้ดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแทน ซึ่งบริษัทดังกล่าวอาจอยู่ในประเทศหรือต่างประเทศก็ได้ สถาบันการเงินต้องแจ้งธนาคารแห่งประเทศไทยก่อนการใช้โครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศดังกล่าว เช่น กรณีธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศมีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์อยู่ที่บริษัทแม่ในต่างประเทศ

ฝนสว00-คส50001 -2562118

คส500	วันที่ 18 พ.ย. 2562

นอกจากนี้ ธนาคารแห่งประเทศไทยได้รวมการกำกับดูแลผู้ใช้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศในการประกอบธุรกิจ (IT Outsourcing) ให้อยู่ภายใต้หลักเกณฑ์ฉบับนี้ และขอนำส่งแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Implementation Guideline) ซึ่งเป็นแนวทางการบริหารจัดการความเสี่ยงบุคคลภายนอกมาพร้อมกัน เพื่อให้สถาบันการเงินใช้เป็นแนวทางปฏิบัติในกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยให้สถาบันการเงินพิจารณาปรับใช้อย่างเหมาะสมตามลักษณะการดำเนินธุรกิจ และสอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

ปรียานุช จึงประเสริฐ

(นางสาวปรียานุช จึงประเสริฐ)
ผู้อำนวยการอาวุโส ฝ่ายนโยบายการกำกับสถาบันการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ลงวันที่ 1 ตุลาคม 2562
2. แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6876
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 5827

หมายเหตุ [ ] ธนาคารจะจัดให้มีการประชุมชี้แจงในวันที่ ..... ณ .....
[x] ไม่มีการประชุมชี้แจง

ประกาศธนาคารแห่งประเทศไทย
ที่ สนส.๒๑ /2562
เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk) ของสถาบันการเงิน

---

1. เหตุผลในการออกประกาศ

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) มีความสำคัญต่อการดำเนินธุรกิจของสถาบันการเงิน โดยเฉพาะการนำมาใช้เพิ่มประสิทธิภาพการให้บริการทางการเงินแก่ลูกค้า เพื่อให้ลูกค้าได้รับบริการที่ตรงความต้องการด้วยต้นทุนที่ต่ำลง ธนาคารแห่งประเทศไทยจึงเห็นควรปรับปรุงกระบวนการกำกับดูแลให้มีความคล่องตัวขึ้น โดยให้สถาบันการเงินสามารถพิจารณาการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ด้วยตนเอง เพื่อรองรับรูปแบบทางธุรกิจและสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

อย่างไรก็ดี การใช้เทคโนโลยีสารสนเทศอาจก่อให้เกิดความเสี่ยงต่อความปลอดภัยของการใช้บริการ ข้อมูลลูกค้า ความต่อเนื่องของการให้บริการของสถาบันการเงิน และส่งผลกระทบต่อการดำเนินธุรกิจของสถาบันการเงิน รวมถึงต่อระบบสถาบันการเงินโดยรวม ธนาคารแห่งประเทศไทยจึงยกระดับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและระดับความมีนัยต่อความเสี่ยงเชิงระบบในประเทศ ดังนี้

(1) ธนาคารพาณิชย์ที่มีนัยต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks: D-SIBs) และสถาบันการเงินที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ต้องมีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO)

(2) ธนาคารพาณิชย์ต้องรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญประจำปีให้ธนาคารแห่งประเทศไทยทราบ โดยยกเลิกการขออนุญาตธนาคารแห่งประเทศไทยก่อนการนำเทคโนโลยีมาใช้ หรือก่อนการเปลี่ยนแปลงเทคโนโลยีที่มีนัยสำคัญ ทั้งนี้ สำหรับบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ยังคงให้ขออนุญาตการใช้หรือเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ เว้นแต่ธนาคารแห่งประเทศไทยจะสั่งการเป็นอย่างอื่น

(3) สถาบันการเงินที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์สำหรับบริษัทในกลุ่มธุรกิจหรือบริษัทที่มีความเกี่ยวข้องกัน โดยให้บริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องกันนั้นเป็นผู้ดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแทน ซึ่งบริษัทดังกล่าวอาจอยู่ในประเทศหรือต่างประเทศก็ได้ สถาบันการเงินต้องแจ้งธนาคารแห่งประเทศไทยก่อนการใช้โครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศดังกล่าว เช่น กรณีธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศมีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์อยู่ที่บริษัทแม่ในต่างประเทศ

ฝนสป00-คส50001-2562100๑

คส 500	วันที่ ๑ ต.ค. 2562

นอกจากนี้ ธนาคารแห่งประเทศไทยได้รวมการกำกับดูแลผู้ใช้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศในการประกอบธุรกิจ (IT Outsourcing) ให้อยู่ภายใต้หลักเกณฑ์ฉบับนี้ โดยมี Guideline ให้สถาบันการเงินใช้เป็นแนวทางในการปฏิบัติในกรณีที่มีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น พันธมิตรทางธุรกิจ ด้วย

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 41 **มาตรา 47 มาตรา 71** แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ให้สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศนี้

3. ประกาศที่ยกเลิก

3.1 ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2560 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ลงวันที่ 20 ธันวาคม 2560

3.2 ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2559 เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ลงวันที่ 28 ธันวาคม 2559

4. ขอบเขตการบังคับใช้

ประกาศนี้ให้ใช้บังคับกับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

5. เนื้อหา

5.1 คำจำกัดความ

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

“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (Information Technology Risk : IT risk) หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยี ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของสถาบันการเงิน รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threat)

“คณะกรรมการของสถาบันการเงิน” หมายความว่า คณะกรรมการของสถาบันการเงินที่จดทะเบียนในประเทศไทย หรือคณะผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบที่เกี่ยวข้องของสาขาของธนาคารพาณิชย์ต่างประเทศ

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยสถาบันการเงินได้ โดยกรณีของสาขาของธนาคารพาณิชย์ต่างประเทศให้รวมถึงสำนักงานใหญ่หรือสาขาอื่นในต่างประเทศที่เป็นนิติบุคคลเดียวกันด้วย ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์และบริการของสถาบันการเงิน

“บริษัทในกลุ่มธุรกิจเดียวกัน” หมายความว่า บริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลโครงสร้างและขอบเขตธุรกิจของกลุ่มธุรกิจทางการเงิน

“บริษัทที่มีความเกี่ยวข้อง” หมายความว่า บริษัทแม่ บริษัทลูก และบริษัทร่วมของสถาบันการเงิน

5.2 หลักการ

สถาบันการเงินมีหน้าที่เกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) ดังนี้

5.2.1 ดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงโครงการด้านเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพและรัดกุม ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ (1) การรักษาความลับของระบบและข้อมูล (confidentiality) (2) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ (3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) โดยอยู่บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า

5.2.2 กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านชื่อเสียง และความเสี่ยงด้านกฎหมาย รวมถึงให้ความสำคัญกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงิน (Enterprise Risk Management : ERM)

5.2.3 มีโครงสร้างการกำกับดูแลในภาพรวมที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence)

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

5.3 หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.3.1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)

(1) บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของสถาบันการเงิน

คณะกรรมการของสถาบันการเงินต้องเข้าใจและตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อสถาบันการเงินและผู้ที่เกี่ยวข้อง รวมทั้งมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมการดำเนินการและการดูแลด้านต่าง ๆ ดังต่อไปนี้

(1.1) มีการใช้เทคโนโลยีของสถาบันการเงินที่สอดรับกับกลยุทธ์การดำเนินธุรกิจ และมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงต่าง ๆ ในอนาคต

(1.2) มีนโยบายและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นหนึ่งในความเสี่ยงสำคัญขององค์กร (enterprise wide risk) ทั้งด้านความปลอดภัย ด้านความถูกต้อง และด้านความพร้อมใช้ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ทั้งในภาวะปกติและภาวะวิกฤต รวมทั้งดูแลความเสี่ยงโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญด้วย

(1.3) มีการสร้างความรู้และความตระหนักรู้เรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่กรรมการ ผู้บริหาร และพนักงานในองค์กรอย่างต่อเนื่องและมีประสิทธิผล

คณะกรรมการของสถาบันการเงินอาจมอบหมายให้คณะกรรมการชุดอื่นหรือผู้บริหารระดับสูงกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ แต่คณะกรรมการของสถาบันการเงินยังคงต้องรับผิดชอบในเรื่องดังกล่าว

นอกจากนี้ คณะกรรมการสถาบันการเงินต้องมีกรรมการอย่างน้อย 1 คน ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ (ตามประกาศธนาคารแห่งประเทศไทยว่าด้วยธรรมาภิบาลของสถาบันการเงิน) ทั้งนี้ เพื่อทำหน้าที่ด้านการกำกับดูแลเทคโนโลยีสารสนเทศ (IT governance)

(2) โครงสร้างการกำกับดูแล

(2.1) โครงสร้างองค์กร

สถาบันการเงินต้องมีโครงสร้างองค์กรที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence) โดยแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่างการทำหน้าที่ (1) ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (2) บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ **และกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์**ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และ (3) ตรวจสอบด้านเทคโนโลยีสารสนเทศ นอกจากนี้ สถาบันการเงินต้องมีการถ่วงดุลอำนาจกันอย่างอิสระ โดยเฉพาะการทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องมีความเป็นอิสระจากการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**และกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ**

(2.2) คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินต้องมีคณะกรรมการ ดังต่อไปนี้

(2.2.1) คณะกรรมการที่ทำหน้าที่บริหารจัดการ และกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee

(2.2.2) คณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

(2.2.3) คณะกรรมการที่ทำหน้าที่กำกับดูแลให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการตรวจสอบการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

(2.3) การกำหนดผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

(2.3.1) ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินควรมีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์

ทั้งนี้ ผู้บริหารที่ทำหน้าที่ดังกล่าวควรมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งควรมีบทบาทหน้าที่และความรับผิดชอบให้สถาบันการเงินดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยดังนี้

- มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

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

- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการสถาบันการเงินเป็นวาระประจำ

- ดูแลและดำเนินการให้สถาบันการเงินมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านภัยคุกคามทางไซเบอร์

(2.3.2) ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ธนาคารพาณิชย์ที่มีนัยต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks: D-SIBs) หรือสถาบันการเงินที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ตามกรอบการประเมินความพร้อมด้าน cyber resilience ภายใต้หลักเกณฑ์ธนาคารแห่งประเทศไทยว่าด้วยการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน นอกจากต้องจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามข้อ 5.3.1 (2.3.1) แล้ว ต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) ภายใน 1 ปีนับจากวันที่เข้าเงื่อนไขดังกล่าวด้วย

ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (authority) เพียงพอ ในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อยดังนี้

- รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของสถาบันการเงินและคณะกรรมการที่เกี่ยวข้องโดยตรง

- ให้ความเห็นด้านภัยคุกคามไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของสถาบันการเงิน คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ที่กระทบต่อสถาบันการเงินอย่างมีนัยสำคัญ

(3) การบริหารจัดการบุคลากร

สถาบันการเงินต้องบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**และกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ** และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีในการปฏิบัติงานประจำวัน (user) อย่างเหมาะสม โดยต้องคำนึงถึงความรู้ความสามารถของบุคลากร ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยสถาบันการเงินต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(3.1) การบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**และกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ** และตรวจสอบด้านเทคโนโลยีสารสนเทศ ต้องครอบคลุมในเรื่องกระบวนการคัดเลือกบุคลากรที่มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ ความเพียงพอของบุคลากรที่สอดคล้องกับปริมาณการใช้เทคโนโลยี และมาตรการในการสร้างและส่งเสริมความตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(3.2) ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของบุคลากรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินอย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

(3.3) การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยต้องปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว

(4) การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness)

สถาบันการเงินต้องสื่อสารและให้ความรู้แก่บุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**และกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ** และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีในการปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีอย่างปลอดภัย เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ตที่ถูกต้อง และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์

(5) นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(5.1) สถาบันการเงินต้องมี (1) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และ (2) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ที่เป็นลายลักษณ์อักษร และอยู่ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ (1) การรักษาความลับของระบบและข้อมูล (confidentiality) (2) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ (3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) หรือ CIA โดยนโยบายดังกล่าวต้องสอดคล้องกับกลยุทธ์ของสถาบันการเงินในการนำเทคโนโลยีสารสนเทศมาใช้ดำเนินธุรกิจและนโยบายการบริหารความเสี่ยงของสถาบันการเงิน รวมทั้งสอดคล้องกับแนวทางการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

นอกจากนี้ การกำหนดนโยบายดังกล่าวต้องคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้ง

ความเสี่ยงจากการใช้เทคโนโลยีภายในองค์กรและความเสี่ยงจาก**กรณีมีการใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอก** ด้วย

(5.2) สถาบันการเงินต้องทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบเทคโนโลยีสารสนเทศ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ

5.3.2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

เพื่อให้สถาบันการเงินมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ สถาบันการเงินต้องนำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

สถาบันการเงินต้องบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

(2) การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

สถาบันการเงินต้องรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งการรับส่งข้อมูลผ่านเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ จัดชั้นความลับของข้อมูล (information classification) เก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ รวมทั้งบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากล เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

(3) การควบคุมการเข้าถึง (access control)

สถาบันการเงินต้องควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

(4) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

สถาบันการเงินต้องรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค

(facilities) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

(5) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

สถาบันการเงินต้องรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของสถาบันการเงิน เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านเครือข่ายสื่อสารมีความมั่นคงปลอดภัย และสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

(6) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

สถาบันการเงินต้องรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(6.1) การบริหารจัดการขีดความสามารถ (capacity management) ของระบบ และระบบสาธารณูปโภค เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

(6.2) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยี (endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัสหรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่ประสงค์ดี (malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต

(6.3) การสำรองข้อมูล (data backup) ด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

(6.4) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ เช่น การจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (access log) และบันทึกการดำเนินงาน (activity log) เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูลและใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ให้แก่ผู้ใช้บริการ

(6.5) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เช่น เครื่องมือติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

(6.6) การบริหารจัดการช่องโหว่ (vulnerability management) ของระบบที่เหมาะสมตามระดับความเสี่ยง เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ โดยสถาบันการเงินต้องประเมินช่องโหว่ของระบบงานสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบเทคโนโลยีสารสนเทศ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ

(6.7) การทดสอบเจาะระบบ (penetration test) โดยจัดให้มีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงาน (application) และระบบเครือข่าย (network) ที่เชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบเทคโนโลยีสารสนเทศ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ ทั้งนี้ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

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

(6.9) การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการควบคุมการตั้งค่าของระบบที่ใช้งานจริง และมีการสอบทานการตั้งค่าอย่างสม่ำเสมอ เพื่อป้องกันข้อผิดพลาดในการปฏิบัติงาน

(6.10) การบริหารจัดการ patch (patch management) โดยมีกระบวนการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง patch ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์

(7) การจัดหาและการพัฒนาระบบ (system acquisition and development)

(7.1) การจัดหาระบบ (system acquisition)

สถาบันการเงินต้องกำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและบุคคลภายนอกที่เป็นผู้ให้บริการ เช่น ความน่าเชื่อถือของระบบและผู้ให้บริการที่ได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate) ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ เพื่อให้มั่นใจว่าระบบและผู้ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินธุรกิจของสถาบันการเงินได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี หรือการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจในอนาคต

(7.2) การพัฒนาระบบ (system development)

สถาบันการเงินต้องออกแบบ พัฒนา และทดสอบระบบเพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยสถาบันการเงินต้องดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- มีเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

- มีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของคำสั่งเขียนโปรแกรม (source code version control)

- แบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบและผู้นำระบบขึ้นใช้งานจริง

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

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

- พัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยสถาบันการเงินต้องทดสอบประสิทธิภาพ (performance test) เมื่อมีการพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์

- มีแนวทางควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

- จัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

(8) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)

สถาบันการเงินต้องบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีอย่างเหมาะสมและทันท่วงที โดยบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติ ปัญหา และการแก้ไข ให้คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมายในระยะเวลาที่เหมาะสม นอกจากนี้ สถาบันการเงินต้องวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหาเพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

(9) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

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

(9.2) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ สถาบันการเงินต้องคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ **ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ** และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ (operational

risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ (interdependency risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และ**ความเสี่ยงที่มีผลกระทบต่อระบบสถาบันการเงิน** (systemic risk) เป็นต้น

(9.3) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องมีความเป็นไปได้ในทางปฏิบัติ สามารถนำมาใช้รองรับความเสียหายที่เกิดขึ้นได้จริง และสอดคล้องกับแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) โดยการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรครอบคลุมถึงการกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงิน

(9.4) สถาบันการเงินต้องมีคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์และฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้

(9.5) สถาบันการเงินต้องทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

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

(10) การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

ในกรณีที่สถาบันการเงินใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT Outsourcing) หรือเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือกรณีที่บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยสถาบันการเงินได้ เช่น การใช้บริการศูนย์คอมพิวเตอร์และงานด้านดูแลระบบประมวลผล การใช้บริการ cloud computing จากผู้ให้บริการภายนอก การเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับพันธมิตรทางธุรกิจเพื่อให้บริการร่วมกัน การเชื่อมต่อกับผู้ให้บริการเครือข่ายสาธารณะ หรือผู้ให้บริการระบบชำระเงินกลาง สถาบันการเงินต้องมีการกำกับดูแลความเสี่ยง กระบวนการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ บนพื้นฐานที่สถาบันการเงินต้องรับผิดชอบต่อการดำเนินธุรกิจและการให้บริการแก่ลูกค้าและคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิภาพในการให้บริการ ตามหลักการดังนี้

(10.1) กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างสถาบันการเงินและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร รวมทั้งควรระบุเงื่อนไขให้ธนาคารแห่งประเทศไทยมีสิทธิเข้าตรวจสอบการดำเนินงานของบุคคลภายนอกด้วย

(10.2) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ และความเสี่ยงจากการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายเดียวกัน

(10.3) รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและอ้างอิงมาตรฐานสากลที่ยอมรับโดยทั่วไป รวมถึงมีการรักษาความปลอดภัยจากภัยไซเบอร์ตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

(10.4) เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อสถาบันการเงินอย่างมีนัยสำคัญ เพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้า

ทั้งนี้ แนวทางการบริหารจัดการความเสี่ยงบุคคลภายนอกเป็นไปตามแนวปฏิบัติของธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Implementation Guideline)

5.3.3 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

เพื่อให้สถาบันการเงินสามารถบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ**และต่อเนื่อง** สถาบันการเงินต้องกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(1) การประเมินความเสี่ยง (risk assessment)

(1.1) การระบุความเสี่ยง (risk identification)

สถาบันการเงินต้องระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งรวมถึง**ความเสี่ยงจาก**ภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(1.2) การวิเคราะห์ความเสี่ยง (risk analysis)

สถาบันการเงินต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(1.3) การประเมินค่าความเสี่ยง (risk evaluation)

สถาบันการเงินต้องประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

(2) การจัดการความเสี่ยง (risk treatment)

สถาบันการเงินต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ สถาบันการเงินต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ**ที่สำคัญ** (IT key risk indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

(3) การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

สถาบันการเงินต้องมีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

(4) การรายงานความเสี่ยง (risk reporting)

สถาบันการเงินต้อง**รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ**

ทั้งนี้ สถาบันการเงินต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ **เช่น กรณีที่มีการเปลี่ยนแปลงของระบบเทคโนโลยีสารสนเทศ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ**

5.3.4 การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

สถาบันการเงินต้องกำกับดูแลให้ปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (IT compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยระบบการชำระเงิน เพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

5.3.5 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

(1) สถาบันการเงินต้องมีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**และกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ**

(2) สถาบันการเงินต้องมีแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงของการใช้เทคโนโลยีของสถาบันการเงิน และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบดังกล่าวต้องได้รับ**การอนุมัติ**จากคณะกรรมการตรวจสอบ และต้องครอบคลุมถึงเทคโนโลยีสารสนเทศที่มีนัยสำคัญของสถาบันการเงิน รวมถึงต้องทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าว**โดยคณะกรรมการตรวจสอบ**อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบเทคโนโลยีสารสนเทศ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ

(3) สถาบันการเงินต้องตรวจสอบด้านเทคโนโลยีสารสนเทศตามแผนงานและขอบเขตที่กำหนดตามข้อ 5.3.5 (2) โดยสำหรับงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญควรตรวจสอบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุการณ์ผิดปกติในเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

(4) สถาบันการเงินต้องมีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่สำคัญ ซึ่งสถาบันการเงินเห็นว่ามีความจำเป็นต้องประเมิน แต่สถาบันการเงินมีข้อจำกัด หรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการเงินตามข้อ (1) ไม่สามารถประเมินได้ เช่น การประเมินระบบที่มีความซับซ้อนหรือใช้เทคโนโลยีใหม่ หรือการประเมินความสามารถของระบบในการปรับเปลี่ยนเพื่อรองรับการทำธุรกิจของสถาบันการเงินในอนาคตภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว

(5) สถาบันการเงินต้องจัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและเสนอ**ผลการตรวจสอบดังกล่าว**ต่อคณะกรรมการตรวจสอบ ตลอดจนจัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่สถาบันการเงิน พร้อมไว้สำหรับการตรวจสอบหรือเมื่อร้องขอโดยธนาคารแห่งประเทศไทย

(6) สถาบันการเงินต้องติดตาม**ให้มีการปรับปรุง**ประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานประเด็นสำคัญ**พร้อมทั้งแผนการปรับปรุง**ให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้อง

5.3.6 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

(1) สถาบันการเงินต้องศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับสำหรับโครงการที่นำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องพิจารณาเลือกใช้เทคโนโลยีอย่างเหมาะสม และประเมินความเสี่ยงตลอดจนผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งต้องจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตอำนาจอนุมัติที่กำหนดไว้

(2) สถาบันการเงินต้องกำหนดกรอบการบริหารจัดการโครงการ (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 รวมทั้งรายงานความคืบหน้าและภาพรวมของโครงการที่สำคัญของสถาบันการเงินต่อคณะกรรมการที่กำกับดูแลโครงการ เพื่อให้โครงการบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้

(2.3) ผู้จัดการโครงการ (project manager) เพื่อทำหน้าที่ในการบริหารจัดการโครงการแต่ละโครงการตามขั้นตอนการบริหารจัดการโครงการ และส่งมอบงานในแต่ละขั้นตอนตามรูปแบบ กระบวนการ และเครื่องมือ ตามที่หน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการกำหนด เพื่อให้สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานที่กำหนด

5.4 การนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี

ในกรณีที่มีการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ทั้งกรณีที่สถาบันการเงินดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก สถาบันการเงินต้องพิจารณาความมีนัยสำคัญก่อนดำเนินการ โดยสถาบันการเงินต้องมีข้อกำหนด (criteria) ในการพิจารณาความมีนัยสำคัญที่ชัดเจน ดังต่อไปนี้

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

5.4.2 ข้อกำหนดในการพิจารณาความมีนัยสำคัญ ต้องพิจารณาภายใต้กรอบหลักการที่คำนึงถึงความเสี่ยงและผลกระทบต่อการดำเนินธุรกิจของสถาบันการเงินในวงกว้าง (bank wide impact) เช่น กระทบลูกค้าส่วนใหญ่ของสถาบันการเงิน และผลกระทบต่อระบบสถาบันการเงินในวงกว้าง (banking system wide impact) เช่น กระทบต่อระบบงานกลางที่มีนัยสำคัญเชิงโครงสร้างต่อการให้บริการของระบบสถาบันการเงิน

5.4.3 ต้องสื่อสารและเผยแพร่ข้อกำหนดให้หน่วยงานที่เกี่ยวข้องทราบโดยทั่วกัน

5.4.4 ต้องสอบทานการดำเนินการตามข้อกำหนดอย่างน้อยปีละ 1 ครั้ง

5.4.5 ต้องทบทวนข้อกำหนดอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบเทคโนโลยีสารสนเทศ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ ทั้งนี้ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบต่อสถาบันการเงิน และระบบสถาบันการเงิน

ทั้งนี้ สถาบันการเงินต้องบริหารความเสี่ยงให้เหมาะสมตามระดับความมีนัยสำคัญของการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ทั้งกรณีที่สถาบันการเงินดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

5.5 การรายงาน แจ้ง หรือขออนุญาตต่อธนาคารแห่งประเทศไทย

5.5.1 การแจ้งการใช้บริการจากบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์สำหรับบริษัทในกลุ่มธุรกิจหรือบริษัทที่มีความเกี่ยวข้องกัน โดยให้บริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องกันนั้นเป็นผู้ดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแทน ซึ่งบริษัทดังกล่าวอาจอยู่ในประเทศไทยหรือนอกประเทศไทยก็ได้ สถาบันการเงินต้องแจ้งธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชนล่วงหน้า 15 วันก่อนการใช้โครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศดังกล่าว เช่น กรณีธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศมีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์อยู่ที่บริษัทแม่ในต่างประเทศ

ทั้งนี้ สถาบันการเงินและคณะกรรมการของสถาบันการเงินในประเทศไทยยังคงต้องรับผิดชอบต่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเสมือนว่าสถาบันการเงินดำเนินการเอง

5.5.2 การรายงาน หรือการแจ้งต่อธนาคารแห่งประเทศไทย สำหรับธนาคารพาณิชย์

(1) การรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

ธนาคารพาณิชย์ต้องจัดส่งรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญประจำปี ทั้งกรณีที่ธนาคารพาณิชย์ดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต่อธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชนดังนี้

(1.1) การรายงานประจำปี ให้รายงานภายในวันที่ 31 มกราคมของทุกปี เพื่อให้ธนาคารแห่งประเทศไทยทราบถึงโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญของธนาคารพาณิชย์ในปีดังกล่าวล่วงหน้า

(1.2) การรายงานประจำไตรมาส ให้รายงานภายใน 15 วันหลังสิ้นไตรมาส ทั้งนี้ หากข้อมูลไม่มีการเปลี่ยนแปลงจากที่ได้รายงานประจำปี ให้แจ้งว่าไม่มีการเปลี่ยนแปลงของข้อมูล

(2) การแจ้งการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ที่มีนัยสำคัญ

ธนาคารพาณิชย์ที่นำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยี โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนด (criteria) ที่ธนาคารพาณิชย์ได้กำหนดขึ้นตาม ข้อ 5.4 ทั้งกรณีที่ธนาคารพาณิชย์ดำเนินการเองและกรณีที่มี

การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้องรายงานการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าว ต่อธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชนล่วงหน้า 15 วันก่อนดำเนินการ

5.5.3 การขออนุญาตการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี สำหรับบริษัทเงินทุน บริษัทเครดิตฟองซิเอร์

บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ที่นำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยี โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนด (criteria) ที่ได้กำหนดขึ้นตาม ข้อ 5.4 ทั้งกรณีที่บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้องยื่นขออนุญาตก่อนนำมาใช้หรือก่อนเปลี่ยนแปลงดังกล่าวต่อธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชน พร้อมเอกสารที่เกี่ยวข้องอื่นใดที่ธนาคารแห่งประเทศไทยอาจร้องขอเพิ่มเติม เว้นแต่ธนาคารแห่งประเทศไทยมีคำสั่งการให้บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ ไม่ต้องยื่นขออนุญาตการนำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยี ที่มีนัยสำคัญ โดยธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน

ทั้งนี้ ในการพิจารณาคำขออนุญาต ธนาคารแห่งประเทศไทยจะพิจารณาตามหลักการเสริมสร้างความมั่นคงของสถาบันการเงิน (micro-prudential) ซึ่งรวมถึงการกำกับดูแลการบริหารจัดการ การบริหารความเสี่ยง การบริหารความมั่นคงปลอดภัยของสถาบันการเงิน ให้สามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อระบบสถาบันการเงิน ส่งเสริมประสิทธิภาพของสถาบันการเงิน (efficiency) สนับสนุนให้สถาบันการเงินมีธรรมาภิบาลที่ดี (good governance) และคุ้มครองลูกค้าและผู้ใช้บริการทางการเงิน (fairness & consumer protection) รวมถึงเสถียรภาพของระบบสถาบันการเงินและระบบเศรษฐกิจ (macro-prudential)

5.5.4 การรายงานปัญหาด้านเทคโนโลยีสารสนเทศต่อธนาคารแห่งประเทศไทย

สถาบันการเงินต้องรายงานต่อธนาคารแห่งประเทศไทยในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียงของสถาบันการเงิน รวมถึงกรณีเทคโนโลยีสารสนเทศที่มีนัยสำคัญของสถาบันการเงินถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่สถาบันการเงินต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงิน โดยสถาบันการเงินต้องรายงานปัญหาหรือเหตุการณ์ดังกล่าวมายังธนาคารแห่งประเทศไทย ทันทีเมื่อเกิดหรือรับรู้ปัญหาหรือเหตุการณ์นั้น และให้สถาบันการเงินแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

5.6 การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่สถาบันการเงินใดไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ได้ ให้สถาบันการเงินยื่นขออนุญาตผ่อนผันการปฏิบัติตามหลักเกณฑ์ดังกล่าวต่อธนาคารแห่งประเทศไทยเป็นรายกรณี พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนในการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน

ทั้งนี้ ในการพิจารณาคำขอผ่อนผัน ธนาคารแห่งประเทศไทยจะพิจารณาตามหลักการเสริมสร้างความมั่นคงของสถาบันการเงิน (micro-prudential) ซึ่งรวมถึงการกำกับดูแลการบริหารจัดการ การบริหารความเสี่ยง การบริหารความมั่นคงปลอดภัยของสถาบันการเงิน ให้สามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อระบบสถาบันการเงิน ส่งเสริมประสิทธิภาพของสถาบันการเงิน (efficiency) สนับสนุนให้สถาบันการเงินมีธรรมาภิบาลที่ดี (good governance) และคุ้มครองลูกค้าและผู้ใช้บริการทางการเงิน (fairness & consumer protection) รวมถึงเสถียรภาพของระบบสถาบันการเงินและระบบเศรษฐกิจ (macro-prudential)

5.7 การกำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ สั่งให้แก้ไข เพิกถอน หรือเข้าตรวจสอบการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี

ธนาคารแห่งประเทศไทยอาจพิจารณากำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ สั่งให้แก้ไข เพิกถอน หรือเข้าตรวจสอบ การนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ทั้งกรณีที่สถาบันการเงินดำเนินการเองและกรณีที่มีบริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ตามความจำเป็นเป็นรายกรณี รวมทั้งธนาคารแห่งประเทศไทยมีสิทธิเข้าตรวจสอบบุคคลภายนอกดังกล่าวที่มีนัยสำคัญต่อระบบสถาบันการเงิน หากพบว่าเป็นการดำเนินการที่ส่งผลกระทบต่อประชาชนในวงกว้างหรือความเชื่อมั่นในระบบสถาบันการเงิน

6. บทเฉพาะกาล

6.1 สถาบันการเงินที่เข้าเงื่อนไขเป็นธนาคารพาณิชย์ที่มีนัยต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks: D-SIBs) หรือสถาบันการเงินที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ก่อนวันที่ประกาศฉบับนี้มีผลบังคับใช้ ต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) ตามที่กำหนดในข้อ 5.3.1 (2.3) ภายใน 1 ปี นับจากวันที่ประกาศนี้มีผลบังคับใช้

6.2 การกำหนดให้สถาบันการเงินจัดทำข้อกำหนด (criteria) ในการพิจารณาความมีนัยสำคัญของการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ตามที่กำหนดในข้อ 5.4 นั้น ให้มีผลใช้บังคับตั้งแต่วันที่ 1 มกราคม 2563 โดยในระหว่างที่สถาบันการเงินยังไม่มีข้อกำหนดดังกล่าว สถาบันการเงินต้องพิจารณาความมีนัยสำคัญของการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ภายใต้กรอบหลักการที่คำนึงถึงความเสี่ยงและผลกระทบต่อการดำเนินธุรกิจของสถาบันการเงินในวงกว้าง (bank wide impact) และความเสี่ยงและผลกระทบต่อระบบสถาบันการเงินในวงกว้าง (banking system wide impact) ตามกรอบหลักการที่กำหนดในข้อ 5.4

7. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 1 ตุลาคม 2562

(นายวิรไท สันติประภพ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6876
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 5827

คำถาม – คำตอบแนบท้ายประกาศ

เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

ลงวันที่ 1 ตุลาคม 2562

ข้อ	ประเด็นคำถาม	คำตอบ
ขอบเขตการบังคับใช้		
1.	บริษัทลูกของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยจะต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ด้วยหรือไม่	บริษัทลูกของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยที่อยู่ในกลุ่ม Solo Consolidation ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ เฉพาะหัวข้อการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management) ทั้งนี้ ธนาคารพาณิชย์ควรกำกับดูแลบริษัทลูกที่จดทะเบียนในประเทศไทยที่อยู่ในกลุ่ม Solo Consolidation ให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมอย่างรัดกุมเพียงพอ โดยสามารถอ้างอิงตามแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของธนาคารแห่งประเทศไทยเป็นแนวทางดำเนินการ
การนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี		
2.	ในช่วงเริ่มต้นของการบังคับใช้หลักเกณฑ์ที่กำหนดให้สถาบันการเงินต้องมีข้อกำหนดในการพิจารณาความมีนัยสำคัญที่ชัดเจน และต้องได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย ซึ่งอาจต้องใช้ระยะเวลาในการดำเนินการ และไม่สามารถปฏิบัติตามหลักเกณฑ์ได้ทันตามกำหนดเวลา สถาบันการเงินสามารถขอขยายเวลาการปฏิบัติตามหลักเกณฑ์ได้หรือไม่	ให้สถาบันการเงินแจ้งมายังฝ่ายกำกับธุรกิจสถาบันการเงิน ธนาคารแห่งประเทศไทย ตามช่องทางการให้บริการผ่านระบบ e-Application โดยชี้แจงเหตุผลและความจำเป็นที่ไม่สามารถปฏิบัติตาม หลักเกณฑ์ดังกล่าว รวมถึงแผนดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ ทั้งนี้ สถาบันการเงินสามารถปฏิบัติตามหลักเกณฑ์นี้ให้ครบถ้วนภายในสิ้นไตรมาส 1 ปี 2563 ได้
การรายงาน แจ้ง หรือขออนุญาตต่อธนาคารแห่งประเทศไทย		
3.	ในกรณีที่สถาบันการเงินไม่มีข้อกำหนดในการพิจารณาความนัยสำคัญ ตามที่กำหนดในประกาศฉบับนี้ สถาบันการเงินใช้หลักเกณฑ์การพิจารณาความมีนัยสำคัญใด ในการรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ สำหรับการรายงานภายในวันที่ 31 มกราคม 2563	การรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ รอบการรายงานภายในวันที่ 31 มกราคม 2563 ให้สถาบันการเงินใช้หลักเกณฑ์การพิจารณาความมีนัยสำคัญที่สถาบันการเงินมีในปัจจุบัน

ข้อ	ประเด็นคำถาม	คำตอบ
การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ		
4.	กรณีสถาบันการเงินได้ปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan: IT DRP) ระหว่างปีแล้ว เช่น ในช่วงสถานการณ์ COVID-19 สถาบันการเงินยังต้องทดสอบแผน BCP และ IT DRP ประจำปี ตามที่หลักเกณฑ์กำหนดหรือไม่	หากสถาบันการเงินได้ปฏิบัติตามแผน BCP และ IT DRP ระหว่างปีแล้ว สถาบันการเงินอาจไม่ต้องทำการทดสอบแผน BCP และ IT DRP ประจำปี โดยการปฏิบัติตามแผนดังกล่าวครอบคลุมประเด็นสำคัญในการดำเนินธุรกิจ เช่น ความพร้อมในการให้บริการธุรกรรมงานที่สำคัญ การบริหารจัดการความเสี่ยงด้าน IT ที่ทำให้สถาบันการเงินสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ทั้งนี้ ให้สถาบันการเงินนำผลการปฏิบัติตามแผนมาทบทวนแผน BCP และ IT DRP ให้มีประสิทธิภาพและเหมาะสมกับการปฏิบัติมากยิ่งขึ้น ทั้งนี้ หากสถาบันการเงินเห็นว่าการดำเนินการยังไม่ครอบคลุมประเด็นสำคัญในการดำเนินธุรกิจ เช่น ความพร้อมในการให้บริการธุรกรรมงานที่สำคัญ ให้สถาบันการเงินนำเสนอถึงเหตุผลและความจำเป็นในส่วนที่ไม่ได้ปฏิบัติแก่คณะกรรมการที่รับผิดชอบ และแจ้งใน ธปท. ทราบภายใน 15 วันนับจากวันที่คณะกรรมการชุดดังกล่าวอนุมัติให้ยกเว้นการดำเนินการ

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ธนาคารแห่งประเทศไทย

IT Risk Management Implementation Guideline

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ

สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

สารบัญ

Executive Summary 1

หลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ 2

ความเชื่อมโยงประกาศและแนวปฏิบัติที่เกี่ยวข้อง 4

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ 5

ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ 6

1. การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ 7

2. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) 16

3. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management) 37

เอกสารอ้างอิง 39

Executive Summary

ปัจจุบัน การดำเนินธุรกิจของสถาบันการเงิน (สง.) กำลังเข้าสู่ยุค digital โดยอาศัยเทคโนโลยีสารสนเทศเป็นตัวขับเคลื่อนและมีบทบาทสำคัญเป็นโครงสร้างพื้นฐานที่ช่วยเสริมสร้างประสิทธิภาพในกระบวนการดำเนินงานให้รองรับกลยุทธ์ทางธุรกิจ อีกทั้งการพัฒนานวัตกรรมทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ยังเป็นกลไกในการพัฒนาประเทศที่สำคัญ ช่วยลดต้นทุนและเพิ่มศักยภาพในการแข่งขัน เพื่อสามารถให้บริการลูกค้าได้อย่างสะดวกรวดเร็ว ตอบสนองความต้องการของลูกค้าที่หลากหลายได้อย่างทั่วถึง

การใช้เทคโนโลยีสารสนเทศของ สง. จึงนับเป็นโจทย์ที่ท้าทาย ภายใต้บริบทของสภาวะแวดล้อมด้านธุรกิจการเงินในปัจจุบันที่มีความผันผวนสูงและยากต่อการคาดเดา ตั้งแต่การกำหนดยุทธศาสตร์ในการพัฒนาเทคโนโลยีสารสนเทศเพื่อเป็นตัวขับเคลื่อนธุรกิจ รวมทั้งการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีที่ สง. ต้องปรับตัวให้เท่าทัน และความเสี่ยงในการเผชิญภัยคุกคามทางไซเบอร์ที่นับวันมีแนวโน้มเพิ่มขึ้น มีวิวัฒนาการที่ซับซ้อนขึ้น ส่งผลกระทบที่มีความรุนแรงและเป็นวงกว้างมากขึ้น ดังเช่น เหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั่วโลก ไม่ว่าจะกรณีการโจมตีด้วย DDoS จนทำให้ระบบใช้งานไม่ได้ หรือโปรแกรม Malware ที่เข้าแทรกแซงระบบให้ส่งคำสั่งโอนเงิน เป็นต้น

จึงเห็นได้ว่าปัจจุบัน สง. กำลังเผชิญกับความเสี่ยงด้านเทคโนโลยีสารสนเทศในหลายมิติมากขึ้น หาก สง. ไม่มีการปรับตัวให้เท่าทันกับการเปลี่ยนแปลง หรือไม่มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เพียงพอ อาจนำไปสู่ความเสี่ยงด้านอื่นที่สำคัญด้วย โดยปัจจุบันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ไม่เป็นเพียงส่วนหนึ่งของความเสี่ยงด้านปฏิบัติการอีกต่อไป แต่กลายเป็นหนึ่งในความเสี่ยงทางธุรกิจที่สำคัญที่สามารถส่งผลกระทบต่อความเชื่อมั่นของลูกค้าที่มีต่อการใช้บริการทางการเงิน รวมทั้ง อาจส่งผลกระทบต่อกลยุทธ์ทางธุรกิจ การปฏิบัติตามกฎระเบียบต่าง ๆ ภาพลักษณ์ชื่อเสียงของ สง.

ดังนั้น สง. จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบและต่อเนื่อง ซึ่งธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญและความจำเป็นในการยกระดับความพร้อมรับมือต่อความเสี่ยงที่ สง. กำลังเผชิญ เพื่อให้ สง. มีการกำกับดูแลและบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศ ทั้งบุคลากร กระบวนการ และการนำเทคโนโลยีสารสนเทศมาใช้ ภายใต้การบริหารความเสี่ยงอย่างเหมาะสมและเพียงพอรองรับตามระดับความเสี่ยงที่ สง. มี โดยเริ่มตั้งแต่คณะกรรมการของ สง. และผู้บริหารระดับสูงที่ให้ความสำคัญในการผลักดันและยกระดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยสร้างวัฒนธรรมและพฤติกรรมร่วมของทุกคนในองค์กรให้ตระหนักถึงความเสี่ยงอย่างรอบด้านและเป็นรูปธรรม การสร้างธรรมาภิบาลที่ดีในองค์กรโดยมีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบอย่างเหมาะสม การกำหนดกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ชัดเจนเพื่อให้มีการประเมิน และติดตามความเสี่ยงอย่างต่อเนื่อง และเท่าทันกับความเสี่ยงรูปแบบใหม่ที่อาจเกิดขึ้น การขับเคลื่อนธุรกิจโดยคำนึงถึงการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและปลอดภัย รวมถึง การดูแลให้มีบุคลากรของ สง. มีความรู้ความเชี่ยวชาญอย่างเพียงพอตลอดจนมีการเสริมสร้างความรู้ความเข้าใจทางด้านเทคโนโลยีทางการเงินให้กับประชาชนอย่างต่อเนื่อง

ธนาคารแห่งประเทศไทยจึงได้จัดทำประกาศ เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ พร้อมทั้งได้จัดทำแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับประกาศดังกล่าว โดยอ้างอิงมาตรฐานสากลที่ยอมรับโดยทั่วไป ดังแสดงในเอกสารอ้างอิง ทั้งนี้ ธนาคารแห่งประเทศไทยมุ่งหวังให้แนวปฏิบัตินี้เกิดประโยชน์ในวงกว้างและ สง. สามารถนำไปใช้เป็นแนวทางปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อสร้างความมั่นคงปลอดภัยและความเชื่อมั่นให้กับองค์กร ระบบการเงิน รวมทั้งลูกค้าประชาชนต่อไป

หลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สรุปหลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีดังนี้

1. **การใช้เทคโนโลยีสารสนเทศสอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจและการเปลี่ยนแปลง**

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจของสถาบันการเงินมากขึ้น โดยเป็นโครงสร้างพื้นฐานที่สำคัญที่รองรับกลยุทธ์ในการดำเนินธุรกิจ ช่วยเพิ่มประสิทธิภาพ ลดต้นทุนในการดำเนินงาน และเพิ่มศักยภาพในการแข่งขัน ตอบสนองต่อความต้องการของลูกค้าที่ต้องการผลิตภัณฑ์และบริการที่หลากหลายได้อย่างสะดวกและรวดเร็ว นอกจากนี้ สง. ยังต้องเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศให้พร้อมรับการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วเพื่อรองรับการดำเนินธุรกิจในอนาคต

2. **คณะกรรมการของ สง. และผู้บริหารระดับสูงมีบทบาทสำคัญในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องมีการกำกับดูแลในระดับองค์กร โดยเป็นความรับผิดชอบของคณะกรรมการของ สง. ที่ต้องสนับสนุนและผลักดันให้องค์กรมีกลยุทธ์และนโยบายด้านเทคโนโลยีสารสนเทศที่เพิ่มประสิทธิภาพให้แก่การดำเนินธุรกิจ ความสามารถในการแข่งขัน มีความมั่นคงปลอดภัยและพร้อมรับมือภัยคุกคามทางเทคโนโลยีและภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งผลักดันให้องค์กรมีการสร้างความตระหนักในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness) อย่างต่อเนื่องและมีประสิทธิภาพ

3. **ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงในระดับองค์กร (enterprise wide risk)**

เนื่องจากเทคโนโลยีสารสนเทศกลายเป็นโครงสร้างพื้นฐานสำคัญรองรับกระบวนการทางธุรกิจและการปฏิบัติงานด้านต่าง ๆ ของ สง. ดังนั้นการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ไม่ได้เป็นความรับผิดชอบอยู่เพียงหน่วยงานด้านเทคโนโลยีสารสนเทศเท่านั้น แต่เป็นเรื่องที่บุคลากรทุกระดับและทุกฝ่ายในองค์กรต้องให้ความตระหนักและมีแนวทางการบริหารความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศครอบคลุมทั้งในเชิงกลยุทธ์และเชิงปฏิบัติการเพื่อให้มีการป้องกันติดตาม และรับมือความเสี่ยงที่อาจเกิดขึ้น ด้วยเหตุนี้ สง. จำเป็นต้องมีกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างครอบคลุมทั่วทั้งองค์กรและเหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ โดยครอบคลุมการกำหนดนโยบายและบทบาทหน้าที่ความรับผิดชอบ การพัฒนากระบวนการและเครื่องมือ รวมถึงการพัฒนาความรู้และความเชี่ยวชาญในด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเพียงพอและทั่วถึง

4. **มีการกำกับดูแลเป็นไปตามหลัก 3 lines of defence**

โครงสร้างการกำกับดูแลการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ จำเป็นต้องสอดคล้องตามหลัก 3 lines of defence เพื่อให้สอดคล้องตามหลักการถ่วงดุล (check and balance) และมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน (segregation of duties) ในการปฏิบัติงาน การบริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ

5. **การรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศสอดคล้องกับความเสี่ยงที่เพิ่มขึ้น**

ความเสี่ยงที่เกิดจากเทคโนโลยีสารสนเทศหากไม่ได้รับการบริหารจัดการและควบคุมอย่างเพียงพอ อาจทำให้เกิดช่องโหว่ด้านการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบในการให้บริการแก่ธุรกิจและการดำเนินงานของ สง. ซึ่งอาจนำไปสู่ความเสี่ยงด้านความน่าเชื่อถือ ชื่อเสียง ภาพลักษณ์ การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

6. **การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศอย่างรัดกุมและมีประสิทธิภาพ**

ความต้องการของลูกค้าที่ต้องการผลิตภัณฑ์และบริการที่หลากหลาย รวมทั้งการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศที่เป็นไปอย่างรวดเร็ว ทำให้ สง. ต้องบริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดให้มีประสิทธิภาพสูงสุด ดังนั้น หาก สง. ไม่สามารถบริหารจัดการโครงการพัฒนาระบบได้อย่างมีประสิทธิภาพ ทำให้ไม่สามารถส่งมอบโครงการได้ตามเป้าหมายที่กำหนด ส่งผลให้เกิดความเสี่ยงที่โครงการด้านเทคโนโลยีสารสนเทศไม่แล้วเสร็จตามกำหนดเวลา โครงการไม่มีคุณภาพ รวมถึงโครงการไม่สอดรับกับกลยุทธ์ทางธุรกิจของ สง. นอกจากนี้ในบางกรณีอาจส่งผลให้ สง. ไม่สามารถปฏิบัติได้ตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องของผู้กำกับดูแลได้

7. **มีการพัฒนาความรู้ความสามารถ (capability) ของบุคลากร**

ด้วยวิวัฒนาการของเทคโนโลยีและความเสี่ยงซึ่งมีความซับซ้อนมากขึ้น สง. จำเป็นต้องมีการพัฒนาความรู้ด้านเทคโนโลยีอย่างต่อเนื่อง เพื่อเพิ่มมุมมองความรู้และความเชี่ยวชาญของบุคลากรในการระบุ ประเมิน ควบคุม ติดตาม และรับมือความเสี่ยงจากภัยที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ นอกจากนี้ การดำเนินธุรกิจในยุคดิจิทัล ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่ได้จำกัดอยู่เพียงระดับปฏิบัติการเท่านั้น แต่ยังส่งผลต่อการดำเนินกลยุทธ์ของธุรกิจ ดังนั้น คณะกรรมการ ผู้บริหารระดับสูง และบุคลากรทุกระดับจึงจำเป็นต้องได้รับการพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศและความเสี่ยงต่อธุรกิจรวมถึงติดตามภัยคุกคามทางไซเบอร์ เพื่อให้มีความรู้เท่าทันภัยคุกคามใหม่ ๆ

ความเชื่อมโยงประกาศและแนวปฏิบัติที่เกี่ยวข้อง

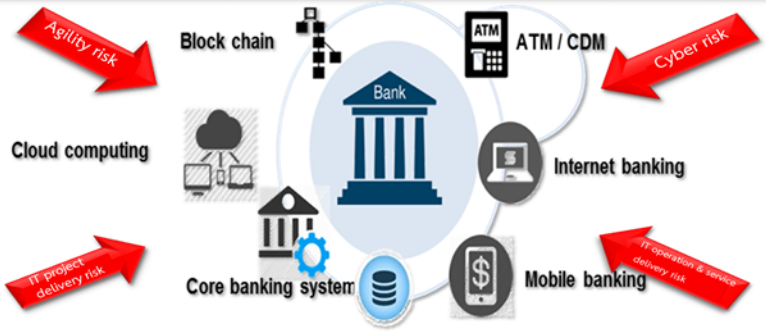
ประกาศ ธปท. ที่ สนส. 19/2559	ประกาศ ธปท. ที่ สนส. 19/2560	แนวปฏิบัติที่เกี่ยวข้อง
เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของ สง.	เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)	➢ แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ➢ แนวปฏิบัติ IT Best Practices I & II ➢ กรอบการประเมินความพร้อมด้าน Cyber Resilience ➢ การบริหารความต่อเนื่องทางธุรกิจ (BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ของ สง. ➢ การป้องกันความเสี่ยงของระบบ ATM จากโปรแกรม Malware

สอบถามเพิ่มเติมติดต่อฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ 02-283-6448

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

สง. กำลังเผชิญความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ



การเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจและเทคโนโลยีอย่างรวดเร็ว (Agility Risk)

สภาพแวดล้อมการเปลี่ยนแปลงทางธุรกิจเป็นไปอย่างรวดเร็ว มีการนำนวัตกรรมและเทคโนโลยีใหม่มาใช้ในการเพิ่มประสิทธิภาพและปรับปรุงผลิตภัณฑ์/ บริการแก่ลูกค้าในหลากหลายรูปแบบ ซึ่ง สง. ต้องมีการเตรียมการให้เท่าทันกับการเปลี่ยนแปลงในมิติต่างๆ เพื่อพร้อมแข่งขันในตลาดธุรกิจการเงิน

ภัยคุกคามทางไซเบอร์ (Cyber Risk) มีแนวโน้มเพิ่มขึ้นและซับซ้อนมากขึ้น

ภัยคุกคามทางไซเบอร์ ปัจจุบันมีแนวโน้มที่เพิ่มขึ้น ซับซ้อนมากขึ้น และแพร่กระจายได้อย่างรวดเร็ว สง. จึงจำเป็นต้องจัดให้มีมาตรการความปลอดภัยที่รัดกุม และเตรียมการให้พร้อมรับมือต่อเหตุการณ์ภัยคุกคามรูปแบบต่างๆ ที่อาจเกิดขึ้นเพื่อความมั่นคงปลอดภัยของ สง. และลูกค้าประชาชน รวมทั้งเพื่อช่วยลดความเสี่ยงและผลกระทบเมื่อเกิดเหตุการณ์

ความเสี่ยงด้านปฏิบัติการ IT (IT Operational Risk) ที่รองรับการดำเนินธุรกิจ

ระบบ IT ถือเป็นโครงสร้างพื้นฐานหลักที่ใช้รองรับการให้บริการของ สง. ซึ่งหากมีการบริหารจัดการและควบคุมทั้งด้านบุคลากร กระบวนการ และระบบที่ไม่เพียงพอ อาจทำให้เกิดช่องโหว่ต่อการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ของระบบและข้อมูล รวมถึงความพร้อมใช้งานของระบบในการให้บริการ

การบริหารจัดการโครงการด้าน IT (IT Project Delivery Risk) มีผลกระทบต่อการดำเนินธุรกิจ

สง. มีการลงทุนโครงการด้าน IT เป็นจำนวนมาก ซึ่งต้องใช้ทรัพยากรทั้งเงินทุน บุคลากร และระยะเวลาในการดำเนินโครงการเพื่อบรรลุตามวัตถุประสงค์ ซึ่งหาก สง. ไม่สามารถบริหารจัดการโครงการได้อย่างมีประสิทธิภาพ รวมถึงไม่มีการกำกับดูแล และควบคุมติดตามการบริหารโครงการอย่างเพียงพอ อาจทำให้โครงการไม่สำเร็จลุล่วงตามแผนและเป้าหมายที่กำหนดจนส่งผลต่อกระทบต่อการดำเนินธุรกิจของ สง.

1. การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของ สง.

<u>วัตถุประสงค์</u> *เพื่อให้คณะกรรมการของ สง. กำกับดูแลและสนับสนุนให้องค์กรมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเพียงพอเหมาะสมและสอดคล้องกับการดำเนินธุรกิจ*

1.1.1 คณะกรรมการของ สง. ประกอบด้วยกรรมการที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างน้อย 1 ท่าน เพื่อให้คณะกรรมการของ สง. สามารถกำหนดทิศทางและกำกับดูแลให้ สง. มีการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์การดำเนินธุรกิจของ สง. มีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีที่เปลี่ยนแปลงไป

1.1.2 ดูแลให้มีการใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการดำเนินธุรกิจของสถาบันการเงิน และดูแลให้การใช้เทคโนโลยีของสถาบันการเงินมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต

1.1.3 ดูแลให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในฐานะที่เป็นความเสี่ยงที่สำคัญ โดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของ สง. (Enterprise Risk Management : ERM)

1.1.4 ดูแลให้มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งรวมถึงนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยนโยบายดังกล่าวต้องสอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้อง รวมทั้งทำหน้าที่ในการอนุมัตินโยบายดังกล่าวด้วย

1.1.5 ดูแลให้มีมาตรฐาน ระเบียบวิธีปฏิบัติ กระบวนการ เครื่องมือ และบุคลากรในการรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายข้อ 1.1.4 รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.1.6 ดูแลให้มีการติดตาม ตรวจสอบและรายงานต่อคณะกรรมการของ สง. คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงของ สง. อย่างเหมาะสม ในเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น ผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของ สง. ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ทางด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของ สง.

1.1.7 ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรของ สง. เพื่อให้ตระหนักถึงความสำคัญของความเสี่ยงและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งเข้าใจการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เพื่อช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.1.8 คณะกรรมการของ สง. ต้องได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศอย่างเพียงพอตามระยะเวลาที่เหมาะสม เพื่อให้มีความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศที่เพียงพอต่อการกำกับดูแลและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สง. ให้ทันกับภัยคุกคามใหม่ รวมถึงการพิจารณาเชิงกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการขับเคลื่อนธุรกิจ

1.2 โครงสร้างการกำกับดูแล

<u>วัตถุประสงค์</u> *เพื่อให้มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่เหมาะสมสอดคล้องตามหลัก 3 lines of defence*

<u>คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ</u>

1.2.1 สง. ควรจัดตั้งคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงการถ่วงดุลอำนาจอย่างเป็นอิสระ อย่างน้อยครอบคลุม

- **คณะกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ** (เช่น IT Steering Committee หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดกลยุทธ์ นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์ของ สง. รวมทั้งกำกับดูแลและติดตามการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้ สง. อาจพิจารณาให้มีคณะกรรมการที่ดูแลงานเฉพาะด้านเพิ่มเติม หากเห็นว่างานดังกล่าวมีนัยสำคัญหรือมีผลกระทบสูงต่อ สง. เช่น คณะกรรมการหรืออนุกรรมการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น
- **คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ** (เช่น คณะกรรมการบริหารความเสี่ยง คณะกรรมการบริหารความเสี่ยงด้านปฏิบัติการ คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ โดยมีการเชื่อมโยงกับความเสี่ยงในภาพรวมของ สง. (enterprise risk management)
- **คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ** (เช่น คณะกรรมการตรวจสอบ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อให้ สง. มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้ง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

<u>โครงสร้างองค์กร</u>

1.2.2 สง. ควรจัดให้มีโครงสร้างองค์กรและหน้าที่ความรับผิดชอบเป็นลายลักษณ์อักษร โดยสอดคล้องตามหลักการถ่วงดุล (check and balance) และการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน (segregation of duties) ระหว่างการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ

1.2.3 สง. ควรดูแลให้มีทรัพยากรเพียงพอที่จะสนับสนุนการปฏิบัติงาน การบริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ สอดคล้องตามปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น จัดให้มีบุคลากรที่มีความรู้ความเชี่ยวชาญและมีเครื่องมือหรือระบบที่ช่วยสนับสนุนการปฏิบัติงาน เป็นต้น

1.2.4 สง. อาจพิจารณาจัดให้มีผู้บริหารระดับสูงหรือหัวหน้าสายงานที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (IT security) โดยควรมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และควรเป็นผู้ที่มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศและ

ด้านการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ เช่น ได้รับการรับรองความรู้ความสามารถตามมาตรฐานสากล เป็นต้น

1.2.5 **หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 1st line of defence)** เช่น หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานอื่นที่เป็นผู้ใช้งานระบบ เป็นต้น

- **หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ** มีหน้าที่ปฏิบัติงานตามที่ได้รับมอบหมาย รวมทั้งประเมินความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ จัดให้มีแนวทางการควบคุม ติดตาม และรายงานการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยนำเสนอต่อคณะกรรมการที่ได้รับมอบหมาย และผู้บริหารระดับสูงที่เกี่ยวข้อง อย่างน้อยครอบคลุม
  - รายงานผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations) เช่น สถานะความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ (capacity and system utilization) เหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem) ระดับการให้บริการงานด้านเทคโนโลยีสารสนเทศ (service availability) เป็นต้น
  - รายงานความคืบหน้า ปัญหาและอุปสรรคในการดำเนินโครงการด้านเทคโนโลยีสารสนเทศในภาพรวมและรายโครงการที่สำคัญ
  - รายงานการติดตามและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งแนวโน้มความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้นและส่งผลกระทบต่อ สง.
  - รายงานผลการประเมินความเสี่ยง การติดตามความเสี่ยง และแนวทางการควบคุมที่เกี่ยวข้อง
  - รายงานความคืบหน้าการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
  - รายงานผลการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก
- **ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ** มีหน้าที่ปฏิบัติตามนโยบายและระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องจากการใช้งานระบบ

1.2.6 **หน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 2nd line of defence)** เช่น หน่วยงานบริหารความเสี่ยง และหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ เป็นต้น

- **หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง** มีหน้าที่กำหนดกรอบและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สนับสนุนให้มีการประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยงและทบทวนการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ของหน่วยงานที่ทำหน้าที่เป็น 1st line of defence โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกับความเสี่ยงด้านอื่นของ สง. และนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยง
- **หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ** มีหน้าที่กำหนดกระบวนการติดตามดูแล ให้คำปรึกษา สอบทานและรายงานการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง และนำเสนอต่อคณะกรรมการที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยระบบการชำระเงิน เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

1.2.7 **หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 3rd line of defence)** ซึ่งอาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น หน่วยงานตรวจสอบภายใน เป็นต้น

- **หน่วยงานที่ทำหน้าที่ตรวจสอบ** มีหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงของหน่วยงานที่ทำหน้าที่ 1st line และ 2nd line of defence รวมถึงงานอื่น ๆ ที่เกี่ยวข้อง เช่น การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ เป็นต้น เพื่อสอบทานให้มั่นใจว่ามีการปฏิบัติที่เป็นไปตามนโยบาย มาตรฐาน และระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ
- กรณี สง. มีข้อจำกัดด้านบุคลากรที่ไม่เพียงพอหรือมีความรู้ความเชี่ยวชาญด้านการตรวจสอบเทคโนโลยีสารสนเทศที่ไม่เพียงพอ อาจพิจารณาว่าจ้างผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้รับมาตรฐานสากลที่ยอมรับโดยทั่วไปในการตรวจสอบเทคโนโลยีสารสนเทศ ดำเนินการแทนได้
- มีกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมอย่างน้อย ดังนี้
  - **การวางแผนงานและกำหนดขอบเขตการตรวจสอบ** (planning and scoping) ครอบคลุมและสอดคล้องกับความสำคัญและความเสี่ยงของการใช้งานเทคโนโลยีสารสนเทศของ สง. และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบต้องได้รับความเห็นชอบจากคณะกรรมการตรวจสอบ และมีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
  - **การตรวจสอบ** (execution) อย่างน้อยปีละ 1 ครั้งตามแผนงานและขอบเขตที่กำหนด และพิจารณาให้มีการตรวจสอบเมื่อมีเหตุการณ์ผิดปกติในงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ นอกจากนี้ แนวทางการตรวจสอบควรเป็นไปตามมาตรฐานที่ สง. กำหนด ซึ่งสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง รวมถึงมาตรฐานสากลที่ยอมรับโดยทั่วไป
  - **การวิเคราะห์** (analysis) นำข้อมูลที่ได้จากการตรวจสอบมาวิเคราะห์ เพื่อสรุปผลการตรวจสอบ และอาจพิจารณาการขยายขอบเขตการตรวจสอบเพิ่มเติม หากมีความจำเป็น เช่น พบข้อบ่งชี้ถึงความเสี่ยงที่อาจกระทบต่อ สง. อย่างมีนัยสำคัญ
  - **การรายงานและติดตามผลการตรวจสอบ** (reporting and follow up) มีการสรุปผลการตรวจสอบและประเด็นที่ต้องแก้ไขกับผู้บริหารของหน่วยงานผู้รับตรวจและจัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการตรวจสอบและแจ้งให้ผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบ ตลอดจนจัดเก็บรายงานผลการตรวจสอบไว้ที่ สง. พร้อมไว้ สำหรับการตรวจสอบหรือเมื่อร้องขอโดยธนาคารแห่งประเทศไทย นอกจากนี้ สง. ต้องจัดให้มีการติดตามการแก้ไขประเด็นที่ตรวจพบภายในระยะเวลาที่กำหนดและรายงานต่อคณะกรรมการตรวจสอบ
- สง. ควรจัดให้มีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่มีความสำคัญซึ่ง สง. เห็นว่ามีความจำเป็นต้องประเมิน แต่มีข้อจำกัดหรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของ สง. ไม่สามารถประเมินได้ เช่น การประเมินระบบที่มีความซับซ้อนหรือมีการใช้เทคโนโลยีใหม่ หรือการประเมินความสามารถของระบบในการปรับเปลี่ยนเพื่อรองรับการทำธุรกิจของ สง. ในอนาคตภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว

1.3 การบริหารจัดการบุคลากร

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอในการปฏิบัติงานที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศ โดยบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สง.*

1.3.1 มีกระบวนการบริหารจัดการบุคลากรอย่างเหมาะสม ครอบคลุม การคัดเลือกบุคลากรที่มีความรู้ความสามารถเพียงพอ การว่าจ้างบุคลากรที่เป็นไปตามข้อกำหนดหรือเงื่อนไขด้านความปลอดภัยเทคโนโลยีสารสนเทศ การพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงหรือสิ้นสุดการว่าจ้างบุคลากร รวมทั้งการดูแลบุคลากรให้เพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศ

1.3.2 สง. อาจพิจารณาการได้รับการรับรองความรู้ความสามารถตามมาตรฐานที่รับรองทั่วไป (certificate) เฉพาะด้านที่เกี่ยวข้องกับงานด้านเทคโนโลยีสนเทศ เพื่อให้ได้บุคลากรที่มีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

1.3.3 หน่วยงานทรัพยากรบุคคล ควรตรวจสอบประวัติของบุคลากรก่อนการว่าจ้างตามความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ เช่น ประวัติการศึกษา ประวัติการทำงาน ประวัติอาชญากรรม ข้อมูลเครดิตบูโร เป็นต้น

1.3.4 มีข้อกำหนดหรือเงื่อนไขการว่าจ้างงาน โดยกล่าวถึงบทบาทหน้าที่ความรับผิดชอบ การปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สง. เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของ สง.

1.3.5 ให้บุคลากรและผู้ให้บริการภายนอกที่ได้รับการว่าจ้างทำความเข้าใจ รับทราบและลงนามยอมรับเงื่อนไขการว่าจ้างงาน นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สง. และข้อตกลงการไม่เปิดเผยข้อมูล (non disclosure agreement) ก่อนเริ่มปฏิบัติงาน

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

- หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (1st line of defence) ให้มีความรู้และความเชี่ยวชาญที่เพียงพอต่อการปฏิบัติงานและการใช้งาน
- หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องกับงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (2nd line of defence) และการตรวจสอบด้านเทคโนโลยีสารสนเทศ (3rd line of defence) ให้มีความรู้และความเชี่ยวชาญเพียงพอที่จะระบุ ประเมิน และให้ข้อเสนอแนะในการปรับปรุงประสิทธิภาพของการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่หน่วยงานที่ทำหน้าที่ 1st line of defence

1.3.7 กำหนดโปรแกรมในการเสริมสร้างความตระหนัก (awareness program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย เช่น การทดสอบเรื่อง social engineering และ phishing การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น โดยโปรแกรมดังกล่าวควรครอบคลุมตั้งแต่ระดับคณะกรรมการ ผู้บริหารระดับสูง และบุคลากรทุกระดับ รวมถึงบุคคลภายนอกที่เกี่ยวข้อง รวมทั้งมีการจัดกิจกรรมเสริมสร้างความตระหนักอย่างต่อเนื่อง นอกจากนี้ สง. ควรจัดให้มีการประชาสัมพันธ์เพื่อสร้างความรู้หรือสร้างความตระหนักในการใช้งานบริการทางอิเล็กทรอนิกส์อย่างปลอดภัย ให้แก่ลูกค้าของ สง. ทราบอย่างสม่ำเสมอด้วย

1.3.8 มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน เช่น การคืนสินทรัพย์ของ สง. การบริหารจัดการสิทธิ์ต้องมีการปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องมีการสื่อสารให้ผู้เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ์ หน้าที่และความรับผิดชอบ เป็นต้น

1.4 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและสอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สง.*

1.4.1 สง. ควรกำหนดให้มีนโยบายเป็นลายลักษณ์อักษรและอยู่ใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ อย่างน้อยครอบคลุมนโยบายดังต่อไปนี้

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

1.4.2 นโยบายดังกล่าวควรสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจ นโยบายการบริหารความเสี่ยงของ สง. รวมทั้งสอดคล้องกับแนวทางบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

1.4.3 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการของ สง. และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรจัดให้มีการชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและมีการควบคุมดูแลให้มีการปฏิบัติตามนโยบายได้อย่างถูกต้องครบถ้วน

1.4.4 **นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy)** ควรรวมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมอย่างน้อย

- 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
- การบริหารจัดการผู้ให้บริการภายนอก (third party management)

1.4.5 **นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy)** โดยครอบคลุมอย่างน้อย

- โครงสร้างองค์กร บทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- จัดทำหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

(1) การประเมินความเสี่ยง (risk assessment)

(1.1) การระบุความเสี่ยง (risk identification)

สง. ควรจัดให้มีการระบุเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นหรือที่เกิดขึ้นจริง รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการดำเนินธุรกิจของ สง. 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 การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการดำเนินธุรกิจของ สง.

ทั้งนี้ ผู้ที่มีส่วนร่วมในการระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศควรมีความรู้และความเข้าใจถึงเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ได้ระบุไว้เป็นอย่างดี

(1.2) การวิเคราะห์ความเสี่ยง (risk analysis)

สง. ควรจัดให้มีการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยควรดำเนินการ ดังนี้

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

(1.3) การประเมินค่าความเสี่ยง (risk evaluation)

สง. ควรประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อจัดลำดับในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยควรดำเนินการ ดังนี้

- กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ เช่น ด้านการเงิน ด้านปฏิบัติการ เป็นต้น
- กำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

- ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- จัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแสดงในแผนภาพความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2) การจัดการความเสี่ยง (risk treatment)

สง. ควรจัดให้มีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรครอบคลุมอย่างน้อย ดังนี้

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

นอกจากนี้ สง. ควรจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ให้สอดคล้องกับความสำคัญของงานเทคโนโลยีสารสนเทศแต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

(3) การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

สง. ควรกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ตามที่กำหนดและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบ เพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ ครอบคลุมอย่างน้อย

- การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง
- ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น
- ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับ สง. และองค์กรอื่น
- รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามรอบที่กำหนด

(4) การรายงานความเสี่ยง (risk reporting)

สง. ควรจัดให้มีกระบวนการนำเสนอผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พร้อมทั้งรายงานผลการประเมินและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร รวมทั้งรายงานแนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น ต่อคณะกรรมการของ สง. หรือคณะกรรมการที่ได้รับมอบหมาย อย่างน้อยไตรมาสละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่า สง. มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและต่อเนื่อง โดยการรายงานควรครอบคลุมอย่างน้อย

- สถานะและผลลัพธ์การดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี
- ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร
- รายงานดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ และรายงานสรุปเหตุการณ์ผิดปกติ
- แนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นกับ สง.
- ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง

ทั้งนี้ สง. ควรจัดให้มีการทบทวนหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.4.6 **นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT outsourcing policy)** โดยครอบคลุมอย่างน้อย

- หลักเกณฑ์การแบ่งประเภทของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
- แนวทางการบริหารจัดการความเสี่ยง แนวทางการคัดเลือกผู้ให้บริการ และแนวทางการประเมินประสิทธิภาพของผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
- แนวทางการรักษาความมั่นคงปลอดภัยของระบบงานและข้อมูล
- การรายงานผลการประเมินความเสี่ยงและประสิทธิภาพการดำเนินงานของผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
- การตรวจสอบผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
- การคุ้มครองผู้ใช้บริการของ สง. จากการใช้บริการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

2. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

2.1 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วนและควบคุมดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง*

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) ที่รองรับระบบเทคโนโลยีสารสนเทศของ สง. อย่างครบถ้วนและเป็นลายลักษณ์อักษร โดยครอบคลุมอย่างน้อย ดังนี้

- ชื่อเครื่องแม่ข่าย
- ชื่อระบบปฏิบัติการ (operating system) และเวอร์ชัน
- ชื่อระบบงาน (application) และเวอร์ชัน
- 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) เมื่อสิ้นสุดการใช้งานครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายใน สง. และกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินของ สง. ทันทีที่มีการยกเลิกสัญญาจ้างด้วย

2.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีการรักษาความมั่นคงปลอดภัยและความลับของข้อมูล ครอบคลุมการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บหรือใช้งานบนระบบและสื่อบันทึกข้อมูลต่างๆ*

<u>การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)</u>

2.2.1 กำหนดให้มีเจ้าของข้อมูล (information owner) รับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึงและการใช้งานข้อมูลอย่างปลอดภัย

2.2.2 กำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูล (information classification) โดยควรระบุชั้นความลับของข้อมูล (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

<u>การบริหารจัดการการเข้ารหัสข้อมูล (cryptography)</u>

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 (เช่น public key cryptography) เป็นต้น โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

2.2.9 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management) ควรกำหนดกระบวนการที่มีความรัดกุมปลอดภัยครอบคลุมตั้งแต่ การสร้างและติดตั้ง การจัดเก็บ และการยกเลิกกุญแจเข้ารหัสข้อมูล

<u>การสร้างและติดตั้งกุญแจเข้ารหัสข้อมูล</u>

- 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 กรณีกุญแจหมดอายุล้าสมัยหรือไม่ปลอดภัย เป็นต้น
- กำหนดกระบวนการทำลายกุญแจ โดยต้องมั่นใจว่าไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก

2.3 การควบคุมการเข้าถึง (Access Control)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีการบริหารจัดการบัญชีสิทธิ์สูงและสิทธิ์ของผู้ใช้งานมีประสิทธิภาพเป็นไปตามหลักความจำเป็นของการใช้งานและสอดคล้องกับหลักการแบ่งแยกงานด้านเทคโนโลยีสารสนเทศที่ดี โดยสามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต*

2.3.1 แนวทางการควบคุมการเข้าถึง ให้ สง. ปฏิบัติตามแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) Phase 1: ธุรกรรมฝาก ถอน โอน

2.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีการรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของศูนย์คอมพิวเตอร์และพื้นที่สำคัญที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเพียงพอรองรับธุรกิจอย่างต่อเนื่อง*

2.4.1 สง. ควรจัดให้ศูนย์คอมพิวเตอร์สำรองแยกออกจากศูนย์คอมพิวเตอร์หลัก ซึ่งควรมีระยะห่างที่เพียงพอและไม่ใช้ระบบสาธารณูปโภคจากแหล่งเดียวกัน เพื่อกระจายความเสี่ยงและป้องกันไม่ให้ได้รับผลกระทบเดียวกัน เช่น ระบบไฟฟ้าหรือระบบโทรคมนาคมขัดข้อง การประท้วงหรือจลาจล ภัยพิบัติทางธรรมชาติ เป็นต้น

2.4.2 สง. ควรมีการรักษาสภาพแวดล้อมและการรักษาความปลอดภัยของศูนย์คอมพิวเตอร์สำรองอย่างเพียงพอตามนโยบายหรือมาตรฐานการรักษาความปลอดภัยของ สง. เพื่อไม่ให้ระบบเทคโนโลยีสารสนเทศที่สำคัญมีความเสี่ยงต่อความพร้อมใช้งาน

2.4.3 แนวทางการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม ให้ สง. ปฏิบัติตามแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) Phase 1: ธุรกรรมฝาก ถอน โอน

2.5 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีโครงสร้างของระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย มีการออกแบบระบบเครือข่ายสื่อสารที่เหมาะสมตามมาตรฐานสากล และมีการป้องกันหรือเฝ้าระวังการบุกรุกหรือภัยคุกคามในรูปแบบต่าง ๆ*

2.5.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารในองค์กร และระหว่างเครือข่ายสื่อสารภายในองค์กรกับระบบเครือข่ายสื่อสารภายนอกองค์กรให้มีความมั่นคงปลอดภัย โดยควรจัดให้มีแนวทางป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหายหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวด

2.5.2 แนวทางการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร ให้ สง. ปฏิบัติตามแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) Phase 1: ธุรกรรมฝาก ถอน โอน

2.6 การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

2.6.1 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีการบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศสอดคล้องตามมาตรฐานสากล 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 ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง โดยครอบคลุมอย่างน้อย ดังนี้

- ผลการประเมินความเสี่ยงและผลกระทบของการเปลี่ยนแปลง โดยมีหน่วยงานเจ้าของระบบและผู้มีหน้าที่เกี่ยวข้องทำการประเมินองค์ประกอบที่เกี่ยวข้อง ได้แก่ ระบบโครงสร้างพื้นฐาน เครือข่ายสื่อสาร และการเชื่อมต่อกับระบบอื่น เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้น ไม่กระทบต่อการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ ความพร้อมใช้ของระบบ
- ผลการทดสอบ เพื่อให้มั่นใจว่าระบบได้ผ่านการทดสอบอย่างครบถ้วนเหมาะสมตามมาตรฐานและระเบียบวิธีปฏิบัติของ สง.
- 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 ผู้มีสิทธิ์ร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น

2.6.1.4 มีหลักเกณฑ์ในการจัดประเภทการเปลี่ยนแปลงระบบตามความเสี่ยงและความสำคัญที่ชัดเจน เช่น การเปลี่ยนแปลงมาตรฐานที่ได้รับอนุมัติเป็นการทั่วไป (standard change) การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการปกติ (normal change) และการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) โดย สง. ควรกำหนดกระบวนการและขั้นตอนในการจัดการการเปลี่ยนแปลงตามแต่ละประเภทอย่างเหมาะสม

2.6.1.5 กรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน ควรมีกระบวนการในการพิจารณาความเสี่ยงและผลกระทบ รวมถึงขออนุมัติจากผู้บริหารที่ได้รับมอบหมายให้สามารถตัดสินใจได้กรณีเร่งด่วน 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> *เพื่อให้ สง. มีกระบวนการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบที่มีความรัดกุมปลอดภัยและเป็นไปตามมาตรฐาน*

2.6.2.1 จัดทำเอกสาร minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษร โดยมีการทบทวนปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ

2.6.2.2 การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ สง. กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.6.2.3 มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์ ระบบและระบบงาน (system configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.6.2.4 มีการสอบทานการตั้งค่าจากหน่วยงานที่มีหน้าที่ควบคุมดูแลความปลอดภัยหรือความเสี่ยงด้านเทคโนโลยีอย่างสม่ำเสมอ เพื่อให้สอดคล้องตามมาตรฐานของ สง.

2.6.2.5 กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสาร minimum baseline standard ควรผ่านกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

2.6.3 การบริหารจัดการ patch (patch management)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีการบริหารจัดการ patch โดยมีการควบคุมที่รัดกุมปลอดภัย และติดตั้งได้อย่างเหมาะสมทันการณ์*

2.6.3.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในกระบวนการบริหารจัดการ patch ที่ครอบคลุม การตรวจสอบความถูกต้องของ patch และการประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch ใหม่จากผู้ผลิตอย่างเหมาะสมทันการณ์

2.6.3.2 มีการจัดเก็บการเปลี่ยนแปลงการติดตั้งของทุกอุปกรณ์ ระบบและระบบงาน (patch version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.6.3.3 มีกระบวนการทดสอบ patch ที่ออกใหม่ทุกครั้งก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

2.6.3.4 การติดตั้ง patch บนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ สง. กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.6.3.5 มีการทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่า สง. สามารถทดสอบและติดตั้ง patch ด้านการรักษาความปลอดภัย ได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว

2.6.4 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัย สามารถใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน 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
  - การเปลี่ยนแปลงแก้ไขบัญชีและสิทธิ์ของผู้ใช้งาน

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) ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูงอย่างสม่ำเสมอ เช่น system administrator หรือ system operator เป็นต้น เพื่อให้มั่นใจได้ว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย

2.6.5 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับต่อการดำเนินธุรกิจ 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 ระบบ core banking ระบบการชำระเงิน ระบบที่ให้บริการทางการเงินอิเล็กทรอนิกส์ เป็นต้น เพื่อบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงทีและสามารถตอบสนองความต้องการในการดำเนินงานทางธุรกิจอย่างต่อเนื่อง

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> *เพื่อให้ สง. สามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบ รวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง*

2.6.6.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

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

2.6.6.3 มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูลภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์

2.6.6.4 กำหนดให้มีผู้รับผิดชอบในการประสานงานแลกเปลี่ยนข้อมูลภัยคุกคาม ระหว่าง สง. และหน่วยงานที่เกี่ยวข้อง รวมทั้งมีกระบวนการและช่องทางในการรายงาน แลกเปลี่ยน ติดตาม เพื่อป้องกันรับมือและแก้ไขภัยคุกคาม

2.6.6.5 ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญ สง. ควรจัดให้มีการรายงานผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง รวมทั้งมีการรายงานหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมทั้งจัดให้มีกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) โดยผู้ที่มีความเชี่ยวชาญ เพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

2.6.7 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Test)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. ได้รับทราบถึงช่องโหว่ด้านการรักษาความปลอดภัยของระบบ และสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันการณ์*

2.6.7.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ

<u>การบริหารจัดการช่องโหว่ (Vulnerability Management)</u>

2.6.7.2 มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment) โดย สง. ควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบบงานสำคัญควรจัดทำอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.6.7.3 มีการรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

<u>การทดสอบเจาะระบบ (Penetration Test)</u>

2.6.7.4 มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความอิสระ ครอบคลุมระบบงานและระบบเครือข่ายกับระบบที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.6.7.5 มีการรายงานผลการทดสอบเจาะระบบไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

2.6.7.6 มีกระบวนการรวบรวมและวิเคราะห์ช่องโหว่ทางด้านเทคนิคที่ตรวจพบ เพื่อกำหนดเป็นมาตรการรักษาความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาในอนาคต

2.6.8 การสำรองข้อมูล (Data Backup)

<u>วัตถุประสงค์</u> *เพื่อให้มั่นใจว่า สง. มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหายจนไม่สามารถใช้งานได้ตามปกติ*

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 โดยมีการระบุข้อมูล ชื่อ วันที่ และช่วงเวลาที่จัดเก็บ ที่สามารถติดตามตรวจสอบได้

2.6.8.4 มีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยมีการรักษาสภาพแวดล้อมและการควบคุมความปลอดภัยในการเข้าถึงข้อมูลที่จัดเก็บไว้ เทียบเคียงกับศูนย์คอมพิวเตอร์หลัก

2.6.8.5 จัดให้มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งานและปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติของ สง.

2.6.9 การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

<u>วัตถุประสงค์</u> *เพื่อให้อุปกรณ์ที่ใช้ปฏิบัติงานมีความปลอดภัยและไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญของ สง. รั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต*

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

2.6.9.2 กำหนด Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงานของ สง. เพื่อป้องกันความเสี่ยงที่อุปกรณ์เหล่านั้นอาจเป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญตามระดับความเสี่ยงที่เหมาะสม โดยอย่างน้อยครอบคลุม ดังนี้

- ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ (personal computer, notebook) โดยมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้ผู้ใช้งานสามารถติดตั้งโปรแกรมอื่น ๆ นอกเหนือจาก สง. กำหนด
- 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 โดย สง. ควรมีเครื่องมือในการควบคุมให้อุปกรณ์ที่สามารถเชื่อมต่ออินเตอร์เน็ตเข้าถึงเฉพาะเว็บไซต์ที่ได้รับอนุญาตเท่านั้น 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 ระบบงานและข้อมูล ของ สง.
- มีกระบวนการตรวจสอบ วิเคราะห์ และติดตามความเสี่ยงของอุปกรณ์ที่นำมาใช้งานใน สง.
- กำหนดรหัสผ่านเพื่อใช้ในการล็อคหรือปลดล็อคในการเข้าถึงอุปกรณ์ส่วนตัว
- กรณีเครื่องคอมพิวเตอร์ (personal computer, notebook) ต้องติดตั้ง anti-virus/ anti-malware หรือโปรแกรมตามที่ สง. กำหนด

- 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)

2.7.1.1 มีหลักเกณฑ์การพิจารณาคัดเลือกระบบและผู้ให้บริการ เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ซึ่งควรครอบคลุมอย่างน้อย ดังนี้

- รายละเอียดทั่วไป เช่น หมายเลขอ้างอิงของซอฟต์แวร์ (software license) ฟังก์ชันการทำงาน ประสิทธิภาพของระบบ เป็นต้น
- ความมั่นคงปลอดภัยของระบบ
- ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค
- การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate)
- การสนับสนุนและการบำรุงรักษาระบบ
- สัญญาและข้อตกลงการรับฝากทรัพย์สิน (escrow agreement) ตามระดับความสำคัญของระบบ
- ความน่าเชื่อถือของระบบและผู้ให้บริการ
- ผลการจัดทำ proof of concept ในกรณีที่เป็นระบบสำคัญ

2.7.1.2 สง. ควรควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบและพัฒนาระบบ

2.7.1.3 สง. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการตรวจสอบและส่งมอบระบบเทคโนโลยีสารสนเทศ

2.7.2 การพัฒนาระบบเทคโนโลยีสารสนเทศ (System Development)

2.7.2.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงการรักษาความมั่นคงปลอดภัย ครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง

2.7.2.2 มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอ เพื่อเสริมสร้างทักษะในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย (secure software development)

2.7.2.3 กำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงานธุรกิจ (business requirement) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐานที่ สง. กำหนด (security requirement) และ sign off ก่อนเริ่มออกแบบระบบ

<u>การออกแบบระบบ</u>

2.7.2.4 จัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมการรักษาความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่ สง. กำหนด (security specification) รวมทั้งจัดให้มีการสอบทานความถูกต้องครบถ้วนและ sign off จากผู้ที่เกี่ยวข้องก่อนเริ่มพัฒนาระบบ

2.7.2.5 จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่าง ๆ ด้านประสิทธิภาพ ตามความต้องการของหน่วยงานธุรกิจ (business requirement) รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่ สง. กำหนด เพื่อเป็นแนวทางการพัฒนาระบบและสอบทานผลการทดสอบก่อนที่จะออกใช้งานจริง (exit criteria)

การพัฒนาระบบ

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

2.7.2.7 มีการควบคุมเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้มีความปลอดภัยเพียงพอตามระดับความเสี่ยงเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.7.2.8 มีกระบวนการหรือเครื่องมือในการควบคุมเวอร์ชันของคำสั่งในการเขียนโปรแกรม (source code version control)

2.7.2.9 มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปลโปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต

การทดสอบระบบ

2.7.2.10 บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบควรเป็นไปตามหลักการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ควรแยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น

2.7.2.11 มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงของการเปลี่ยนแปลงบนระบบที่ให้บริการจริง

2.7.2.12 การทดสอบระบบที่ได้รับการพัฒนาหรือเปลี่ยนแปลง ควรครอบคลุม

- unit test
- system and integration test
- user acceptance test
- performance test
- security test ตาม security specification

ทั้งนี้ สง. ควรจัดให้มีกระบวนการและเอกสารการ sign off ผลการทดสอบระบบจากฝ่ายงานที่เกี่ยวข้องที่ผ่านตาม exit criteria อย่างครบถ้วน ก่อนนำระบบขึ้นใช้งานจริง

2.7.2.13 มีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอ

2.7.2.14 การพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการ การทำธุรกรรมทางอิเล็กทรอนิกส์หรือระบบที่มีการเชื่อมโยงกับระบบอื่นจำนวนมาก สง. ควรจัดให้มีการทดสอบประสิทธิภาพ (performance test) เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการใช้งานจำนวนมาก

2.7.2.15 มีการทดสอบระบบรักษาความปลอดภัยควรครอบคลุมการประเมินช่องโหว่ (vulnerability assessment) ของระบบงาน และกรณีเป็นระบบที่เชื่อมต่อกับภายนอก ควรมีการทำทดสอบเจาะระบบ (penetration test) เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริง

2.7.2.16 มีการสอบทานคำสั่งในการเขียนโปรแกรม (source code review) อย่างเป็นอิสระ ทุกครั้งที่ สง. มีการพัฒนาหรือเปลี่ยนแปลงระบบในส่วนที่เป็นการทำธุรกรรมสำคัญ รวมถึงระบบ internet banking และ mobile banking เพื่อระบุช่องโหว่ด้านความมั่นคงปลอดภัย

2.7.2.17 มีแนวทางการควบคุมการรักษาความปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ เช่น data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูลสำคัญดังกล่าว

2.7.2.18 มีกระบวนการในการจัดการข้อผิดพลาดหรือข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ เพื่อพิจารณาแนวทางปรับปรุงหรือลดความเสี่ยงหรือผลกระทบของข้อผิดพลาดหรือข้อบกพร่อง ที่มีต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ

2.7.2.19 มีการจัดทำคู่มือและอบรมผู้ใช้งานระบบ เพื่อให้มีความเข้าใจฟังก์ชันการทำงานและมีการใช้งานระบบอย่างปลอดภัย รวมถึงจัดให้มีคู่มือการดูแลระบบและอบรมผู้ดูแลระบบ เพื่อสามารถตรวจสอบและจัดการแก้ไขปัญหาได้

2.7.2.20 หลังจากนำระบบขึ้นใช้งานจริง สง. ควรพิจารณาจัดให้มีการทดสอบจริงในวงจำกัด (pilot test) สำหรับฟังก์ชันการทำงานที่สำคัญ รวมทั้งจัดให้มีการติดตามการใช้งานระบบหลังจากให้บริการจริงอย่างใกล้ชิดตามระยะเวลาที่เหมาะสม เพื่อให้มั่นใจต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ

<u>การนำระบบขึ้นใช้งานจริง (system deployment)</u>

2.7.2.21 การนำระบบขึ้นใช้งานจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ สง. กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.7.2.22 มีการจัดเก็บการเปลี่ยนแปลง (version control) ของระบบงานขึ้นใช้งานจริงทั้งหมด โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.7.2.23 ระบบงานสำรองควรปรับปรุงให้มีความเป็นปัจจุบัน เพื่อให้มีความพร้อมใช้งานเมื่อเกิดเหตุฉุกเฉิน

2.8 การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)

2.8.1 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ให้สามารถจัดการแก้ไขปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจของ สง.*

2.8.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมตั้งแต่กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดำเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ

2.8.1.2 กำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ (escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้องหรือคณะกรรมการสถาบันการเงินได้รับทราบให้สอดคล้องกับระดับความรุนแรงของเหตุการณ์ผิดปกติ

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 และมีแนวทางการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบ

2.8.1.6 จัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อคณะกรรมการสถาบันการเงิน คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย โดยครอบคลุม วัน เวลา เหตุการณ์ ความเสียหาย การวิเคราะห์สาเหตุที่แท้จริง การวิเคราะห์ผลกระทบ การแก้ไขปัญหาและแนวทางหรือแผนดำเนินการเพื่อป้องกันเหตุการณ์ผิดปกติในอนาคต และในกรณีที่เป็นความเสียหายส่งผลกระทบต่อชื่อเสียงและการดำเนินธุรกิจของ สง. อย่างมีนัยสำคัญ ให้รายงานต่อคณะกรรมการของ สง. ทราบด้วย

2.8.1.7 ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการระบบงาน หรือชื่อเสียงของสถาบันการเงิน รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของ สง. ถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่สถาบันการเงินต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของ สง. ทราบ โดยให้ สง. รายงานปัญหาหรือเหตุการณ์ดังกล่าวมายังฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธนาคารแห่งประเทศไทย ทันทีเมื่อเกิดหรือรับรู้ปัญหาหรือเหตุการณ์นั้น และให้สถาบันการเงินแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

2.8.1.8 มีกระบวนการบริหารภาวะวิกฤต (crisis management) เพื่อรองรับกรณีเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศเพิ่มระดับความรุนแรงหรือมีความยืดเยื้อ

- สง. จัดให้มีคณะกรรมการบริหารภาวะวิกฤติ (crisis management committee) โดยประกอบด้วยผู้บริหารระดับสูง (C-level) จากฝ่ายงานต่าง ๆ เพื่อให้สามารถพิจารณาประเมินสถานการณ์ได้อย่างครอบคลุม และตัดสินใจแก้ไขสถานการณ์ได้อย่างรวดเร็วทันการณ์ บรรเทาผลกระทบหรือความเสียหายและสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ตลอดจนการกำกับดูแลการดำเนินการต่าง 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) รวมทั้งลูกค้าประชาชนที่ได้รับผลกระทบ

2.8.2 การบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ (IT Problem Management)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีกระบวนการติดตามหาสาเหตุที่แท้จริง 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> *เพื่อให้ สง. มีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจดำเนินการต่อไปได้อย่างต่อเนื่องและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้*

<u>นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ</u>

2.9.1 กำหนดนโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยคำนึงความสอดคล้องกับนโยบายการบริหารความต่อเนื่องของธุรกิจและนโยบายการบริหารความเสี่ยงของ สง.

2.9.2 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการของ สง. และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนฯ เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการดำเนินธุรกิจหรือทรัพยากรหรือโครงสร้างระบบ IT เป็นต้น

2.9.3 นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมอย่างน้อย

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

<u>การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ</u>

2.9.4 มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยต้องได้รับการอนุมัติจากคณะกรรมการของ สง. โดยจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.9.5 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น

2.9.6 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของ สง. เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ (interdependency risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และความเสี่ยงที่มีผลกระทบต่อ สง. ผู้ใช้บริการ ผู้มีส่วนได้เสียและระบบสถาบันการเงิน (systemic risk)

2.9.7 กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมการดำเนินการ ดังนี้

(1) การประเมินความเสี่ยง (risk analysis) เพื่อให้ สง. สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการอย่างเหมาะสมเพียงพอดังนี้

- ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบเทคโนโลยีสารสนเทศหยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ เป็นต้น
- ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้น พร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง
- จัดทำแผนในการจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการและจัดเตรียมทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

(2) **การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis)** เพื่อให้ทราบถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่มีผลต่อการดำเนินธุรกิจของ สง. รวมถึงผลกระทบจากการหยุดชะงักและความเชื่อมโยงของการดำเนินธุรกิจกับระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการดังนี้

- ระบุระบบเทคโนโลยีสารสนเทศทั้งหมดของ สง. และทรัพยากรที่มีการเชื่อมโยงพึ่งพาระหว่างกัน (dependency)
- วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศ โดยคำนึงถึงเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD)
- กำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO)

(3) **การจัดลำดับความสำคัญของระบบงาน** โดยคำนึงถึงทรัพยากร ระยะเวลาในการกู้คืนระบบเป้าหมายของระบบงานและข้อมูลที่ควรกู้ได้ภายหลังเกิดการหยุดชะงัก และทรัพยากรทางเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็นต้องใช้ในการกู้คืนระบบ ทั้งนี้ สง. ควรพิจารณาให้ระบบการชำระเงินหรือระบบที่มีผลกระทบกับระบบ สง. เป็นวงกว้างเป็นระบบที่มีความสำคัญสูงสุด

(4) **การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ** สง. ต้องมีการกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและแนวทางจัดเตรียมทรัพยากรระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามการจัดลำดับความสำคัญของระบบงาน โดยพิจารณาอย่างน้อยครอบคลุม

- เป้าหมายระยะเวลาที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ เช่น RTO, RPO เป็นต้น
- ปัจจัยสำคัญที่สนับสนุนให้แผนเป็นไปตามกลยุทธ์ เช่น เทคโนโลยีในการสำรองและกู้คืนข้อมูล ความพร้อมใช้ของสถานที่ปฏิบัติงานสำรอง เป็นต้น เพื่อให้ สง. มีทิศทางในการพัฒนาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่บรรลุเป้าหมายที่กำหนดไว้
- ทรัพยากรและงบประมาณ เพื่อจัดเตรียมระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามแผนกลยุทธ์และกิจกรรมที่ต้องดำเนินการทั้งหมด

(5) **การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ** แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรมีการระบุกระบวนการและขั้นตอนสนับสนุนการปฏิบัติที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ รวมทั้งมีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น อย่างน้อยครอบคลุม

- ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่น ๆ ที่เกี่ยวข้อง
- ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบและผู้ปฏิบัติที่ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกการเปลี่ยนแปลงของแผน

- รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบเครือข่ายสื่อสาร เป็นต้น
- ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ การตอบสนองต่อเหตุการณ์ฉุกเฉินและแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ
- ขั้นตอนในการดำเนินการกู้คืนระบบ โดยควรระบุรายละเอียดอย่างชัดเจนและเพียงพอเพื่อให้สามารถใช้เป็น checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้ ทั้งนี้ สง. ควรจัดทำเอกสารหรือคู่มือประกอบการกู้คืนในแต่ละระบบ ในกรณีที่มีการปรับปรุงหรือเพิ่มเติมขั้นตอนนอกเหนือจากที่ระบุในแผนขณะปฏิบัติงานจริง สง. ควรมีกระบวนการรายงานและขออนุมัติจากผู้บริหารตามที่กำหนดในโครงสร้างการบังคับบัญชา พร้อมทั้งนำขั้นตอนดังกล่าวมาปรับปรุงแผนให้เป็นปัจจุบัน
- ขั้นตอนในการกลับคืนสู่ภาวะปกติ (return to normal) และการประกาศยกเลิกแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง

(6) การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ สง. ต้องจัดให้มีการสื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และจัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้อง

- ในการสื่อสารแผนฯ ต้องมีการระบุแนวทางสื่อสารที่ชัดเจนให้บุคลากรทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน
- จัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยควรครอบคลุม วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงานและการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน ระบบรักษาความปลอดภัย กระบวนการเฉพาะของแต่ละกลุ่มดำเนินงาน และความรับผิดชอบของแต่ละบุคคล เป็นต้น

(7) การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

- จัดให้มีแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียดอย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้อง ทั้งนี้แผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปีในภาพรวมควรได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย
- จัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศทั้งในระดับหน่วยงานและระดับองค์กรอย่างน้อยปีละ 1 ครั้ง โดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการลูกค้าหรือต่อ สง. ทั้งระบบ เช่น ระบบเงินฝาก ระบบการโอนและชำระเงินระหว่าง สง. เป็นต้น นอกจากนี้อาจพิจารณาการทดสอบระบบสำรองในลักษณะเสมือนจริง (DR live test) เพื่อให้มั่นใจว่าระบบสำรองสามารถรองรับให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง
- กรณีระบบงานมีการเชื่อมโยงเครือข่ายสื่อสารหรือใช้บริการจากหน่วยงานภายนอก สง. ควรมีการทดสอบแผนฉุกเฉินร่วมกับหน่วยงานภายนอกที่เกี่ยวข้องด้วย เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศของ สง. มีความพร้อมใช้งานร่วมกับระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

- มีการรายงานผลการทดสอบต่อคณะกรรมการของ สง. โดยมีรายละเอียดอย่างน้อยครอบคลุม วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข
- สง. ควรจัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงบุคลากรที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน การเปลี่ยนสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศ เป็นต้น เพื่อให้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน
- สง. อาจจัดให้มีการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยหน่วยงานภายนอกหรือภายในที่มีความเป็นอิสระ เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผนให้สามารถใช้งานได้จริง

2.10 การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีแนวทางการบริหารจัดการผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของ สง. หรือสามารถเข้าถึงข้อมูลสำคัญหรือลูกค้าของ สง.*

2.10.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการผู้ให้บริการภายนอก เพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยทรัพย์สินของ สง. โดยอย่างน้อยครอบคลุม

- ก่อนใช้บริการ สง. ดำเนินการระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกสามารถเข้าถึง โดยอย่างน้อยควรพิจารณา ขอบเขต เหตุผลและความจำเป็นในการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจและการยกเลิกหรือสิ้นสุดสัญญา (exit strategy)
- ข้อกำหนดในการรักษาความมั่นคงปลอดภัยของหน่วยงานภายนอก รวมถึง sub-contract ต้องปฏิบัติโดยควรสอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยที่ สง. กำหนด
- ข้อตกลงการไม่เปิดเผยข้อมูล (non disclosure agreement)
- สัญญาการให้บริการและเงื่อนไขระหว่าง สง. และผู้ให้บริการภายนอก สอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยที่ สง. กำหนด เช่น การทำลายข้อมูลของ สง. หรือลูกค้าทั้งหมดเมื่อสิ้นสุดการใช้บริการ ความรับผิดชอบต่อการรั่วไหลของข้อมูลอันเนื่องมาจากการนำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงในการให้บริการ เป็นต้น
- มีกระบวนการติดตาม ประเมิน ทบทวน และรายงานผลการปฏิบัติงานของหน่วยงานภายนอก

2.10.2 ในกรณีที่ สง. ใช้บริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) ให้ สง. ปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยเรื่องการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT outsourcing)

3. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management)

<u>วัตถุประสงค์</u> *เพื่อให้ สง. มีการบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนกลยุทธ์ทางธุรกิจ*

3.1 กำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางดำเนินโครงการจัดหาหรือพัฒนาระบบเทคโนโลยีสารสนเทศ โดยควรครอบคลุมดังนี้

3.1.1 โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด

- **คณะกรรมการกำกับดูแลโครงการ** มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลให้โครงการสำเร็จเป็นไปตามเป้าหมายที่กำหนด มีการติดตามความคืบหน้า ปัญหาและอุปสรรคของโครงการ เพื่อให้คำแนะนำและพิจารณาตัดสินใจการดำเนินงานที่สำคัญ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/ project sponsor) มีส่วนร่วมในการตัดสินใจ รวมทั้งคณะกรรมการกำกับดูแลโครงการควรมีการประชุมอย่างสม่ำเสมอ เพื่อควบคุมดูแลโครงการที่สำคัญให้เป็นไปตามแผนงานที่กำหนด
- **หน่วยงานหรือทีมงานดูแลภาพรวมโครงการ (project management office)** มีบทบาทหน้าที่และความรับผิดชอบในการกำหนดรูปแบบ กระบวนการและเครื่องมือที่เป็นมาตรฐานในการบริหารจัดการและติดตามโครงการ รวมทั้งติดตาม รายงานภาพรวมโครงการสำคัญของ สง. ให้กับคณะกรรมการของ สง. และผู้บริหารระดับสูงที่เกี่ยวข้องได้รับทราบเพื่อติดตามและสนับสนุนให้บริหารจัดการโครงการสำเร็จลุล่วงสอดคล้องกับเป้าหมายในระดับกลยุทธ์ของ สง. 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

<u>การเริ่มโครงการ</u>

3.2 มีการประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งเลือกใช้เทคโนโลยีที่เหมาะสม ทั้งนี้โครงการต้องมีเป้าหมายที่ชัดเจน (project objective) สอดคล้องกับกลยุทธ์ขององค์กรและคำนึงถึงการรักษาความมั่นคงปลอดภัย

3.3 มีแผนการดำเนินโครงการ ที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการอย่างน้อยครอบคลุม

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

3.4 มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการของ สง. 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 โดยโครงการที่ส่งผลกระทบต่อธุรกิจของ สง. อย่างมีนัยสำคัญ ควรนำเสนอแก่คณะกรรมการของ สง. ด้วย

<u>การปิดโครงการ</u>

3.8 มีการสรุปประโยชน์ที่ได้รับจากโครงการเทียบกับเป้าหมายที่กำหนด

3.9 มีการรวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์ ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไปให้มีประสิทธิภาพมากขึ้น

<u>การสอบทานโครงการ</u>

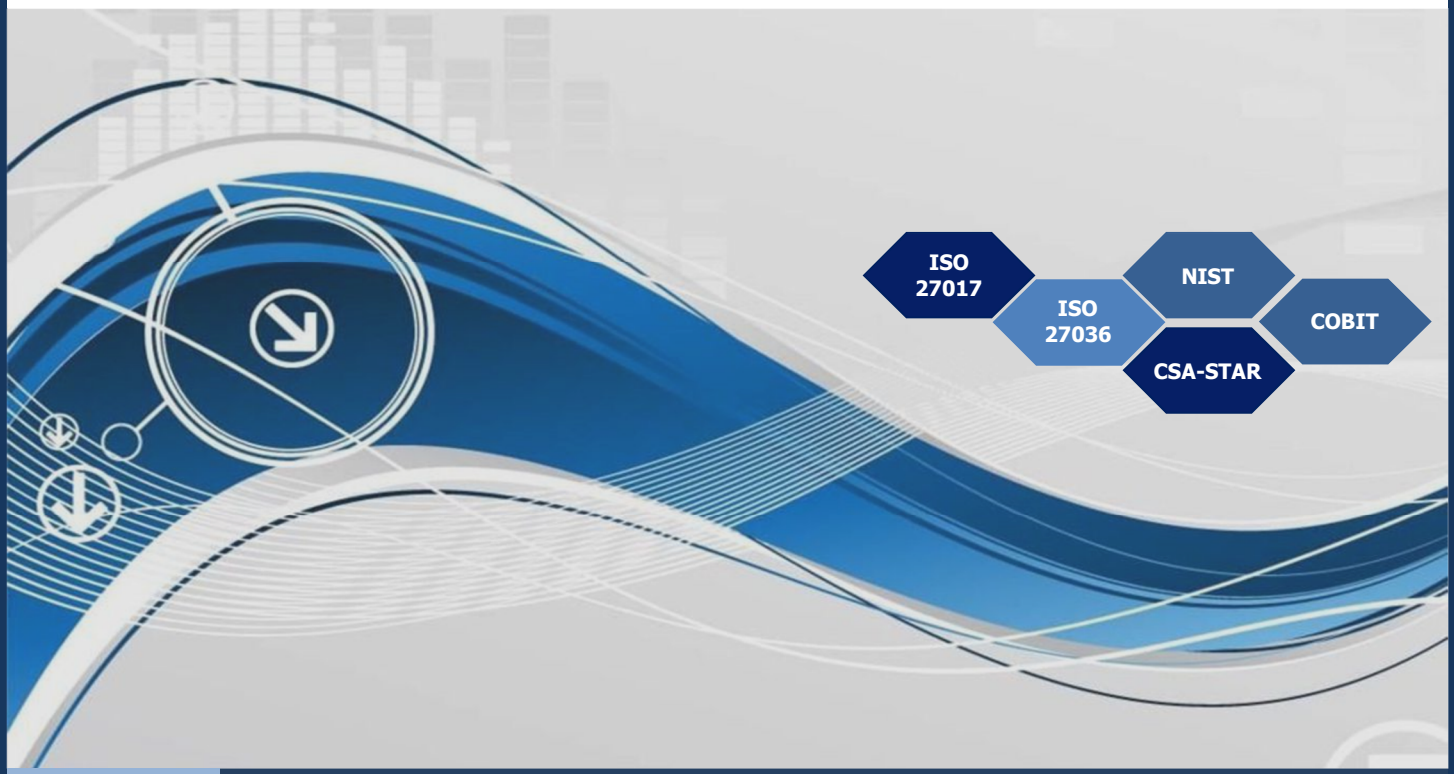
3.10 มีการสอบทานโครงการที่สำคัญ โดยหน่วยงานอิสระ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของ สง. รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

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) ซึ่งเป็นองค์กรที่กำกับดูแล สง. ในสหรัฐอเมริกา

ธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทย



Third Party Risk Management Implementation Guideline

แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

สารบัญ

Executive Summary 1

ขอบเขตและหลักการ 2

แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก 4

ส่วนที่ 1 : การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Risk Governance) 5

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย 5
2. จัดโครงสร้างองค์กรให้มีการถ่วงดุล 5
3. การบริหารจัดการบุคลากรที่เกี่ยวข้อง 7
4. การคุ้มครองลูกค้าของสถาบันการเงิน 7
5. นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก 8
6. การตรวจสอบ 9

ส่วนที่ 2 : การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management) 9

7. การประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก 10
8. การคัดเลือกบุคคลภายนอก 11
.9 การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก 12
10. การติดตามผลการปฏิบัติงานของบุคคลภายนอก 13
11. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง 13
.12 การรักษาความมั่นคงปลอดภัยด้าน IT ในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก 14

ส่วนที่ 3 : การรายงานต่อธนาคารแห่งประเทศไทย 20

เอกสารอ้างอิง 21

Executive Summary

ปัจจุบันสถาบันการเงิน (สง.) มีการนำเทคโนโลยีสารสนเทศมาใช้เป็นกลไกหลักในการดำเนินธุรกิจ และเพื่อให้สามารถปรับตัวได้รวดเร็วและมีความยืดหยุ่นในการนำเทคโนโลยีมาใช้ให้สอดรับกับการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยี สง. จึงมีการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศมากขึ้น ตลอดจนมีการเปิดระบบเทคโนโลยีสารสนเทศให้เชื่อมต่อหรือแลกเปลี่ยนข้อมูลกับบุคคลหรือองค์กรภายนอกมากขึ้นเพื่อเพิ่มโอกาสและศักยภาพในการดำเนินธุรกิจ

ธนาคารแห่งประเทศไทย (ธปท.) เห็นถึงความจำเป็นดังกล่าว และตระหนักถึงความเสี่ยงที่อาจเพิ่มขึ้น ทั้งความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงจากภัยทางไซเบอร์ ความเสี่ยงด้านข้อมูล ตลอดจนความเสี่ยงจากการพึ่งพาผู้ให้บริการหรือจากการเชื่อมต่อกับบุคคลภายนอก ตลอดจนความเสี่ยงด้านกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง อันอาจส่งผลต่อความต่อเนื่องในการดำเนินธุรกิจของ สง. ความปลอดภัยของข้อมูลและระบบ และความเชื่อมั่นของประชาชน

ธปท. กำกับดูแลความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management) ภายใต้ประกาศ ธปท. เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน นอกจากนี้เพื่อยกระดับการดูแลเรื่องดังกล่าวของ สง. ให้ครอบคลุม เข้มแข็ง และรัดกุมตามมาตรฐานสากล ธปท. ได้จัดทำ**แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Implementaion Guideline: แนวปฏิบัติฯ)** เพื่อให้ สง. มีแนวปฏิบัติในการปฏิบัติตามประกาศและสามารถดูแลความเสี่ยงจากบุคคลภายนอกได้อย่างมีประสิทธิผล

แนวปฏิบัติฯ ฉบับนี้ ครอบคลุมบุคคลภายนอก ใน 3 กรณี ได้แก่ 1) กรณีการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT Outsourcing และ Cloud Computing) 2) กรณีการเชื่อมต่อระบบเทคโนโลยีสารสนเทศของ สง. กับบุคคลภายนอก เช่น การเชื่อมต่อระบบเทคโนโลยีสารสนเทศเพื่อร่วมให้บริการกับพันธมิตรทางธุรกิจ การเชื่อมต่อกับบริการเครือข่ายสาธารณะหรือกับผู้ให้บริการระบบชำระเงินกลาง เป็นต้น และ 3**) กรณีการที่สามารถเข้าถึงข้อมูลสำคัญของ สง. หรือข้อมูลลูกค้าของ สง. จากบุคคลภายนอก ทั้งนี้ "บุคคลภายนอก" ไม่ครอบคลุมถึงลูกค้าของสถาบันการเงิน** เนื่องจาก สง. ต้องดูแลความมั่นคงปลอดภัยของระบบในการให้บริการลูกค้าตามหัวข้ออื่นในประกาศและแนวปฏิบัติ ธปท. เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงินแล้ว

แนวปฏิบัติฯ แบ่งเป็น 2 ส่วน ส่วนแรกเป็นการกำกับดูแลการบริหารจัดการความเสี่ยง (Risk Governance) ประกอบด้วย การกำหนดบทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูง การจัดโครงสร้างองค์กรให้ถ่วงดุลตามหลัก 3 Lines of defence และการบริหารจัดการบุคลากร การคุ้มครองลูกค้าของ สง. การจัดให้มีนโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก และการตรวจสอบ

ส่วนที่สองเป็นการบริหารจัดการความเสี่ยง (Third Party Risk Management) ประกอบด้วย การประเมินความเสี่ยง การคัดเลือกบุคคลภายนอก การทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานของบุคคลภายนอก การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลงกับบุคคลภายนอก รวมทั้งการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและจากภัยคุกคามไซเบอร์จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก

ขอบเขตและหลักการ

แนวปฏิบัติฉบับนี้จัดทำขึ้นเพื่อให้สถาบันการเงินใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ให้มีความเสี่ยงในระดับที่สถาบันการเงินยอมรับได้ บนพื้นฐานที่สถาบันการเงินต้องรับผิดชอบต่อการดำเนินธุรกิจและการให้บริการแก่ลูกค้า และคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิภาพและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการให้บริการ โดยมีขอบเขตและหลักการครอบคลุม ดังนี้

1. ขอบเขตและคำจำกัดความ

"บุคคลภายนอก" หมายความว่า บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศหรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือข้อมูลของลูกค้าที่ควบคุมโดยสถาบันการเงินได้ โดยกรณีสาขาของธนาคารพาณิชย์ต่างประเทศให้รวมถึงสำนักงานใหญ่หรือสาขาอื่นในต่างประเทศที่เป็นนิติบุคคลเดียวกันด้วย ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์และบริการของสถาบันการเงิน

"การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก" หมายความว่า การใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT Outsourcing) หรือการเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือการที่บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือข้อมูลของลูกค้าที่ควบคุมโดยสถาบันการเงินได้ เช่น การใช้บริการศูนย์คอมพิวเตอร์และงานด้านดูแลระบบประมวลผล การใช้บริการ Cloud Computing จากผู้ให้บริการภายนอก การเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับพันธมิตรทางธุรกิจเพื่อให้บริการร่วมกัน การเชื่อมต่อกับผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการระบบชำระเงินกลาง การว่าจ้างผลิตบัตรเครดิตหรือการว่าจ้างพิมพ์ใบแจ้งยอดรายการบัตรเครดิต เป็นต้น

2. หลักการในการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

สถาบันการเงินต้องจัดให้มีการกำกับดูแลความเสี่ยง กระบวนการบริหารความเสี่ยง และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ ดังนี้

1) มีการกำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างสถาบันการเงินและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร

2) มีการกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการหรือการเชื่อมต่อ เพื่อให้อยู่ในระดับความเสี่ยงที่สถาบันการเงินยอมรับได้

3) มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ตามมาตรฐานสากลที่ยอมรับโดยทั่วไป และตามมาตรฐานหรือแนวทางที่สถาบันการเงินกำหนดโดยด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ครอบคลุม การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (Availability)

4) มีการเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อสถาบันการเงินอย่างมีนัยสำคัญ ต้องสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง (Business Continuity) และมีข้อมูลพร้อมใช้ในการดำเนินธุรกิจให้บริการแก่ลูกค้า และเมื่อธนาคารแห่งประเทศไทยร้องขอ (Data Availability)

สอบถามเพิ่มเติมติดต่อฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ โทร. 0 2283 5827

แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ส่วนที่ 1 : การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Risk Governance)

สถาบันการเงิน (สง.) ต้องจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยประกอบด้วย การกำหนดบทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงของสถาบันการเงินในการกำกับดูแล การจัดให้มีโครงสร้างองค์กรที่มีการถ่วงดุลในเรื่องการบริหารจัดการความเสี่ยงจากบุคคลภายนอก การบริหารจัดการบุคลากรที่เกี่ยวข้อง การคุ้มครองลูกค้า การจัดให้มีนโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกและการตรวจสอบ ดังนี้

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

1.1 ดูแลให้การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกสอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ มีการบริหารความเสี่ยงให้อยู่ในระดับที่สถาบันการเงินยอมรับได้ (Risk Appetite) และไม่ขัดต่อกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

1.2 ดูแลให้มีนโยบาย ครอบคลุมการบริหารจัดการความเสี่ยงจากบุคคลภายนอก เพียงพอกับระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร อาจเป็นนโยบายที่จัดทำขึ้นเฉพาะหรือรวมอยู่ในนโยบายที่สถาบันการเงินมีอยู่แล้ว รวมทั้งจัดทำมาตรฐานและระเบียบวิธีปฏิบัติที่สอดรับกับนโยบายดังกล่าว จัดให้มีการนำไปปฏิบัติอย่างทั่วถึง นอกจากนี้ ดูแลให้มีการทบทวนและประเมินประสิทธิภาพของนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติดังกล่าวอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.3 จัดให้มีการกำกับและควบคุมดูแลการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้เป็นไปตามนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติที่กำหนด และพิจารณาให้ความเห็นชอบต่อการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลที่มีนัยสำคัญ

2. จัดโครงสร้างองค์กรให้มีการถ่วงดุล

สถาบันการเงินควรจัดโครงสร้างองค์กร และหน้าที่ความรับผิดชอบที่เกี่ยวกับการบริหารจัดการบุคคลภายนอกให้มีการถ่วงดุลตามหลัก 3 Lines of Defence โดยมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนและมีการถ่วงดุลในการทำหน้าที่ของหน่วยงานที่ทำหน้าที่ปฏิบัติงาน (1st line) บริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ (2nd line) และการตรวจสอบ (3rd line)

ทั้งนี้ กรณีที่สถาบันการเงินมีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศรวมกับบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง การพิจารณาโครงสร้างการกำกับดูแลตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบตาม 3 Lines of Defence ให้สามารถพิจารณาโดยดูจากภาพรวมทั้งหมดของกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องได้ อย่างไรก็ดี สถาบันการเงินและคณะกรรมการของสถาบันการเงินในประเทศไทยยังคงต้องรับผิดชอบต่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเสมือนสถาบันการเงินดำเนินการเอง

2.1 **หน้าที่ของหน่วยงานที่ทำหน้าที่ปฏิบัติงานกับบุคคลภายนอก (1st line)**

เพื่อให้การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีประสิทธิภาพ มีการบริหารจัดการความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่สถาบันการเงินกำหนด 1st line ควรมีหน้าที่ครอบคลุม ดังนี้

2.1.1 ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และประเมินศักยภาพของบุคคลภายนอก (Due Diligence) ก่อนเริ่มหรือต่อสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

2.1.2 จัดให้มีกรอบและแนวทางการประเมิน ควบคุม และติดตามผลจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างสม่ำเสมอและต่อเนื่อง ทั้งด้านประสิทธิภาพและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (CIA) รวมถึงการดูแลคุ้มครองข้อมูลส่วนบุคคลด้วย

2.1.3 ติดตามการเปลี่ยนแปลง ปัญหาและเหตุการณ์ผิดปกติสำคัญที่เกิดขึ้นอันสืบเนื่องหรือเกี่ยวเนื่องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อดูแลให้การดำเนินการของบุคคลภายนอกเป็นไปตามที่ระบุในสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

2.1.4 รายงานผลการปฏิบัติงาน ผลการประเมินความเสี่ยง ปัญหาและเหตุการณ์ผิดปกติจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่ส่งผลกระทบต่อสถาบันการเงินอย่างมีนัยสำคัญต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายอย่างเพียงพอต่อเนื่อง ทันการณ์ และสอดรับกับระดับความเสี่ยง

2.2 **หน้าที่ของหน่วยงานที่ทำหน้าที่บริหารความเสี่ยง และการกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ (2nd line)**

เพื่อให้การบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีประสิทธิภาพ มีความมั่นคงปลอดภัยตามกรอบการบริหารความเสี่ยงของสถาบันการเงิน ตลอดจนปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง 2nd line ควรมีหน้าที่ครอบคลุม ดังนี้

2.2.1 จัดให้มีกรอบและกระบวนการบริหารความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป ประกอบไปด้วย การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามทบทวนความเสี่ยง และการรายงานความเสี่ยง

2.2.2 ติดตามดูแลให้ 1st line มีการบริหารความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และให้มีการรายงานความเสี่ยงดังกล่าวมายัง 2nd line เพื่อรวบรวมและเชื่อมโยงความเสี่ยงดังกล่าวกับความเสี่ยงด้านอื่นของสถาบันการเงิน ตลอดจนชี้แนะและให้คำปรึกษาในการบริหารจัดการความเสี่ยงของ 1st line

2.2.3 ติดตามความเสี่ยง และทบทวนการควบคุมและการบริหารจัดการความเสี่ยง ซึ่งรวมถึงการทบทวนปัจจัยเสี่ยง ดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT Key Risk Indicators) และกระบวนการควบคุมและบริหารจัดการความเสี่ยง เพื่อให้มั่นใจว่าสถาบัน

การเงินมีความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกในระดับความเสี่ยงที่สถาบันการเงินยอมรับได้ รวมทั้งนำเสนอผลการบริหารความเสี่ยงดังกล่าวต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

2.2.4 กำกับดูแลการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง รวมถึงดูแลให้เป็นไปตามนโยบาย มาตรฐานระเบียบปฏิบัติของสถาบันการเงิน ตลอดจนมาตรฐานสากลที่สถาบันการเงินอ้างอิงหรือนำมาบังคับใช้ และนำเสนอรายงานผลการปฏิบัติตามกฎหมายและกฎเกณฑ์ในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

2.3 **หน้าที่การตรวจสอบ (3rd line)**

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

2.3.1 จัดให้มีการตรวจสอบการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่เป็นอิสระ เพื่อตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ 1st line และ 2nd line และบุคคลภายนอก ว่ามีการปฏิบัติตามนโยบาย มาตรฐาน ระเบียบปฏิบัติของสถาบันการเงิน สัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

2.3.2 รายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบ และจัดเก็บรายงานดังกล่าวไว้ที่ สง. เพื่อพร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดยธนาคารแห่งประเทศไทย หรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง

3. การบริหารจัดการบุคลากรที่เกี่ยวข้อง

การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ทำให้บทบาทหน้าที่ รวมถึงความรู้ความเชี่ยวชาญในการปฏิบัติงานเปลี่ยนแปลงจากที่ สง. เคยดำเนินการ สง. จึงควรจัดสรรบุคลากร สร้างความเข้าใจและความตระหนักก่อนการเปลี่ยนแปลง รวมถึงพัฒนาความรู้ความเชี่ยวชาญของบุคลากรที่เกี่ยวข้อง ให้เพียงพอในการปฏิบัติงานรองรับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างมีประสิทธิภาพ เช่น จัดให้มีการพัฒนาทักษะความรู้ของพนักงานที่เกี่ยวข้องครอบคลุมการบริหารจัดการความเสี่ยงจากบุคคลภายนอก การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรณีการใช้ Cloud Computing ควรเสริมสร้างทักษะความรู้ให้แก่ผู้บริหารและพนักงานที่เกี่ยวข้องให้สามารถปฏิบัติงานได้ตามมาตรฐานและแนวปฏิบัติที่ดีของผู้ให้บริการ Cloud Computing เป็นต้น

4. การคุ้มครองลูกค้าของสถาบันการเงิน

กรณีที่ สง. มีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้บริการแก่ลูกค้า สง. ต้องดำเนินการ ดังนี้

4.1 ดูแลและบริหารจัดการบุคคลภายนอกในการเข้าถึง การใช้ และการดูแลรักษาข้อมูลลูกค้าอย่างรัดกุม เพื่อให้ข้อมูลลูกค้าได้รับการดูแลอย่างปลอดภัย โดยคำนึงถึงความเป็นส่วนตัว และเป็นไปตาม

กฎหมายอื่นที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นต้น รวมทั้งสอดคล้องกับมาตรฐานขั้นต่ำสำหรับการดูแลข้อมูลของลูกค้า (Data Privacy) ตามประกาศ ธปท. ว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct)

4.2 ดูแลการแก้ไขปัญหาและจัดการเรื่องร้องเรียนให้แก่ลูกค้าอย่างรับผิดชอบและเป็นธรรมให้สอดคล้องกับมาตรฐานขั้นต่ำสำหรับการแก้ไขปัญหาและจัดการเรื่องร้องเรียน (Problem and Complaint Handling) ตามประกาศ ธปท. ว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct)

5. นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

5.1 สง. ต้องกำหนดนโยบายที่ครอบคลุมถึงการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างชัดเจนเป็นลายลักษณ์อักษร โดยอาจเป็นนโยบายที่จัดทำขึ้นเฉพาะหรือรวมอยู่ในนโยบายที่สถาบันการเงินมีอยู่แล้ว

5.2 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกควรสอดคล้องกับนโยบายอื่นที่เกี่ยวข้องของ สง. เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

5.3 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกต้องได้รับอนุมัติจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย 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) การเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อสถาบันการเงินอย่างมีนัยสำคัญ เพื่อให้สถาบันการเงินสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ซึ่งรวมถึงการมีข้อมูลพร้อมใช้สำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้า

(7) การคุ้มครองลูกค้าของสถาบันการเงิน

5.5 สง. ควรจัดให้มีมาตรฐานและระเบียบวิธีปฏิบัติ เพื่อสนับสนุนการดำเนินการตามนโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ให้สอดคล้องกับระดับความเสี่ยงและความมีนัยสำคัญ รวมถึงมาตรฐานสากลที่ยอมรับโดยทั่วไป

6. การตรวจสอบ

สง. ควรดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจาก สง. สามารถเข้าตรวจสอบบุคคลภายนอก ในส่วนที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของ สง. ได้ เช่น ระบุเงื่อนไขในสัญญาหรือข้อตกลง เป็นต้น และจัดให้มีการตรวจสอบการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับระดับความเสี่ยงและความมีนัยสำคัญ โดยการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลที่มีนัยสำคัญควรได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง และเมื่อพบเหตุการณ์ผิดปกติที่มีนัยสำคัญ

ทั้งนี้ หากมีเหตุจำเป็นที่ สง. ไม่สามารถดำเนินการตรวจสอบ ระบุสิทธิหรือเงื่อนไขการตรวจสอบในสัญญาหรือข้อตกลงได้ สง. ควรมีแนวทางที่จะใช้ประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล โดย สง. อาจใช้ผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล 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)

สง. ต้องจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างรัดกุมเพียงพอและต่อเนื่อง และดูแลให้สอดคล้องตามกรอบและกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สง. (IT Risk Management) เพื่อให้ความเสี่ยงอยู่ในระดับที่สถาบันการเงินยอมรับได้ โดยกำหนดให้มีระเบียบวิธีปฏิบัติที่ชัดเจนและเป็นลายลักษณ์อักษร ครอบคลุมวัฏจักรการบริหารจัดการบุคคลภายนอก (Third Party Management Life Cycle) ตั้งแต่การประเมินความเสี่ยง การคัดเลือกบุคคลภายนอก การจัดทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานอย่างต่อเนื่อง และการยกเลิก/สิ้นสุดสัญญาหรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้าน IT

7. การประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

7.1 สง. ต้องประเมินความเสี่ยงและผลกระทบทั้งก่อนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก และเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงประเมินเป็นประจำตามรอบระยะเวลาที่สอดคล้องกับระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล ซึ่งต้องมีผลประเมินเป็นลายลักษณ์อักษร โดยคำนึงถึงความเสี่ยงดังต่อไปนี้

(1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

(2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่ครอบคลุมและรัดกุมเพียงพอ

(3) ความเสี่ยงด้านชื่อเสียง (Reputation Risk) เช่น ระบบหรือบริการที่ดำเนินการร่วมกับบุคคลภายนอกเกิดขัดข้อง ส่งผลกระทบต่อการให้บริการ รวมถึงชื่อเสียงและความน่าเชื่อถือของสถาบันการเงิน เป็นต้น

(4) ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยทางไซเบอร์ เช่น ระบบขัดข้องหรือหยุดบริการโดยมีสาเหตุจากบุคคลภายนอก ระบบของบุคคลภายนอกมีช่องโหว่ด้านความปลอดภัยทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล บุคคลภายนอกใช้งานสิทธิสูงเกินกว่าที่ได้รับอนุญาต การจัดเตรียมทรัพยากรระบบไม่เพียงพอ เป็นต้น

(5) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น การปฏิบัติไม่ถูกต้องตามพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติลิขสิทธิ 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 อาจทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยีผู้ให้บริการหรือพันธมิตร และข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

(9) ความเสี่ยงจากการกระจุกตัว (Concentration Risk) เช่น สง. และบริษัทในกลุ่มธุรกิจเดียวกันใช้บริการจากบุคคลภายนอกเพียงรายเดียว (Single Provider) เป็นต้น

(10) ความเสี่ยงจากบุคคลภายนอกว่าจ้างผู้อื่นดำเนินการแทน (Subcontractor) เช่น Subcontractor ปฏิบัติงานบกพร่อง เป็นต้น

7.2 สง. ต้องจัดให้มีการควบคุมและบริหารจัดการความเสี่ยงครอบคลุมวัฏจักรการบริหารจัดการบุคคลภายนอก (Third Party Management Life Cycle) ตั้งแต่การคัดเลือก การจัดทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานอย่างต่อเนื่อง ตลอดจนการยกเลิก/สิ้นสุดสัญญาหรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้าน IT ตามที่กล่าวต่อไปในข้อ 8 – 12

7.3 การจัดระดับความเสี่ยงและระดับความมีนัยสำคัญ สง. ต้องกำหนดหลักเกณฑ์ที่ชัดเจน และจัดทำทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ให้ครอบคลุมครบถ้วน

ตามหลักเกณฑ์ที่ สง. กำหนด โดยควรมีรายละเอียดครอบคลุมตามที่กล่าวในข้อ 12.1 (2) เพื่อ สง. สามารถใช้บริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของบุคคลภายนอกได้ครบถ้วนต่อเนื่อง

8. การคัดเลือกบุคคลภายนอก

8.1 สง. ต้องกำหนดให้มีระเบียบวิธีปฏิบัติและหลักเกณฑ์ในการพิจารณาคัดเลือกบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยให้มีข้อมูลที่เพียงพอสำหรับสนับสนุนการพิจารณาตัดสินใจใช้บริการ เชื่อมต่อหรือให้เข้าถึงข้อมูลกับบุคคลภายนอก เพื่อสามารถคัดเลือกบุคคลภายนอกที่มีความเหมาะสมตามวัตถุประสงค์การดำเนินการของ สง.

8.2 การตัดสินใจใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่มีความเสี่ยงหรือมีนัยสำคัญต้องได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

8.3 สง. ต้องทำการประเมินศักยภาพบุคคลภายนอก (Due Diligence) โดยพิจารณาประเมินให้ครอบคลุมตามระดับความมีนัยสำคัญและความเสี่ยงที่เกี่ยวข้องของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ในเรื่องดังต่อไปนี้

(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 สง. ต้องจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเป็นลายลักษณ์อักษร และจัดเก็บสัญญาหรือข้อตกลงดังกล่าวไว้ที่ สง. เพื่อสามารถบังคับใช้ได้ตามกฎหมาย และพร้อมสำหรับการตรวจสอบ หรือเมื่อร้องขอโดยธนาคารแห่งประเทศไทย

9.2 สง. ต้องระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญในสัญญาหรือข้อตกลงกับบุคคลภายนอกอย่างชัดเจน โดยพิจารณาให้ครอบคลุมตามระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ดังนี้

(1) ขอบเขตการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(2) บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอก และ สง.

(3) มาตรฐานการปฏิบัติงานขั้นต่ำของบุคคลภายนอก เช่น มาตรฐานการควบคุมภายใน มาตรฐานการรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (Availability) และมาตรฐานการคุ้มครองลูกค้าของ สง. เป็นต้น

(4) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศสำหรับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกควรสอดคล้องกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของ สง.

(5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก (Ongoing Monitoring) ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือเหตุการณ์ที่สำคัญ และรายงานปัญหาผิดปกติที่เกิดจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

(6) การคุ้มครองข้อมูลส่วนบุคคลทั้งข้อมูลของ สง. และข้อมูลของลูกค้า ต้องกำหนดให้เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น การกำหนดให้บุคคลภายนอกต้องออกหนังสือรับรองการทำลายข้อมูลของ สง.

(8) เงื่อนไขหรือสิทธิของ สง. ในการขอเปลี่ยนแปลง ยุติหรือยกเลิกสัญญาหรือข้อตกลง กรณีที่เกิดการเปลี่ยนแปลงหรือเกิดการละเมิดสัญญาหรือข้อตกลง เช่น การเปลี่ยนเจ้าของกิจการ การละเมิดความปลอดภัยหรือการรักษาความลับ และการที่บุคคลภายนอกอยู่ระหว่างกระบวนการพิทักษ์ทรัพย์/การชำระบัญชี/ล้มละลาย เป็นต้น

(9) แนวทางการระงับข้อพิพาท และความรับผิดต่อความเสียหาย

(10) การระบุสิทธิในการเข้าตรวจสอบโดยสถาบันการเงิน ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจาก สง. หรือ ธปท. ให้สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกในส่วนที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกของ สง.

9.3 ในกรณีเป็นการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT Outsourcing) ที่มีนัยสำคัญ สง. ควรกำหนดสิทธิของ สง. ในการพิจารณาอนุมัติกรณีบุคคลภายนอกว่าจ้างผู้รับเหมาช่วง (Subcontract) และข้อกำหนดที่บุคคลภายนอกต้องรับผิดชอบต่อผลการปฏิบัติงานของผู้รับเหมาช่วง

9.4 กรณีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่ตั้งอยู่ในต่างประเทศ สัญญาหรือข้อตกลงในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกควรพิจารณาถึง

ความเสี่ยงและอุปสรรคที่อาจเกิดขึ้นจากประเทศที่บุคคลภายนอกตั้งอยู่หรือประกอบธุรกิจ (Country Risk) ด้วย

10. การติดตามผลการปฏิบัติงานของบุคคลภายนอก

10.1 สง. ต้องกำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น กำหนดให้บุคคลภายนอกรายงานผลการปฏิบัติงานอย่างสม่ำเสมอ กำหนดการประชุมติดตามอย่างสม่ำเสมอและต่อเนื่อง การเข้าสังเกตการณ์การดำเนินงานของบุคคลภายนอก เป็นต้น

10.2 สง. ต้องกำหนดให้บุคคลภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของ สง. ให้ สง. ได้รับทราบอย่างทันการณ์เพื่อประเมินผลกระทบที่มีต่อ สง. ทั้งนี้ กรณีประเมินว่าผลกระทบที่เกิดขึ้นมีผลต่อการดำเนินธุรกิจของ สง. อย่างมีนัยสำคัญ สง. ต้องมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ

10.3 สง. ต้องทบทวนการประเมินศักยภาพ การประเมินผลการปฏิบัติงาน และการประเมินความเสี่ยงของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกทั้งในด้านประสิทธิภาพ การรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และการปฏิบัติตามกฎหมาย เมื่อจะต่อสัญญาและเมื่อถึงรอบระยะเวลาที่ สง. กำหนด ทั้งนี้ การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่มีนัยสำคัญควรกำหนดให้ดำเนินการอย่างน้อยปีละครั้ง รวมถึงให้รายงานผลการประเมินดังกล่าวต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

11. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง

11.1 จัดให้มีมาตรฐานหรือระเบียบปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง เพื่อเป็นกรอบแนวทางการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง โดยคำนึงถึงความต่อเนื่องในการให้บริการ และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้งนี้ มาตรฐานหรือระเบียบปฏิบัติดังกล่าว ควรครอบคลุม บทบาทหน้าที่คณะกรรมการและหน่วยงานที่เกี่ยวข้อง กระบวนการและการควบคุมภายใน เช่น การสำรองข้อมูลก่อนการยกเลิก การลบหรือนำกลับทรัพย์สินสำคัญของ สง. (ตัวอย่างเช่น ข้อมูล กุญแจการเข้ารหัสข้อมูล และบัญชีผู้ใช้งาน) เป็นต้น

11.2 การพิจารณายกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง สง. ควรประเมินผลกระทบและความเสี่ยงที่อาจเกิดขึ้นจากการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง และดำเนินการตามมาตรฐานหรือระเบียบปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง และกำหนดกลยุทธ์และแผนงานการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง (Exit Strategy and Exit Plan) ที่ชัดเจน เพื่อให้มั่นใจว่าการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลงเป็นไปอย่างมีประสิทธิภาพและได้เตรียมความพร้อมต่อผลกระทบที่อาจเกิดขึ้น เช่น การหยุดให้บริการของระบบที่ส่งผลกระทบกับลูกค้าหรือผู้ใช้บริการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

12. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

สง. ควรดูแลให้มั่นใจว่าการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก 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 โดยพิจารณาให้สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ทั้งนี้ ในกรณีที่มีการใช้บริการ Cloud Computing สง. ควรนำแนวปฏิบัติที่ดีของผู้ให้บริการ Cloud Computing มาเป็นแนวทางในการปฏิบัติงานและควบคุมดูแลเพื่อให้ระบบที่ใช้บริการ Cloud Computing มีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และควรดำเนินการตามแนวทางการควบคุมเพิ่มเติม ดังต่อไปนี้

12.1 การจัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกและทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

(1) จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำ และปรับปรุงทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้ สง. สามารถนำมาใช้ระบุความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกได้อย่างชัดเจน และสามารถบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างปลอดภัยและทันการณ์ เช่น ใช้พิจารณาความเสี่ยงที่เกี่ยวข้องเมื่อเกิดเหตุการณ์ภัยไซเบอร์ หรือใช้วางแผนรองรับเมื่อใกล้สิ้นสุดสัญญาหรือข้อตกลง เป็นต้น

(2) ทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ควรครอบคลุม

- ชื่อบุคคลภายนอก
- ประเภทของบุคคลภายนอก เช่น บุคคลภายนอกที่อยู่ในกลุ่มของ สง. บุคคลภายนอกที่อยู่นอกกลุ่มของ สง. และ Regulator เป็นต้น
- ชื่อบริการ/ระบบงาน
- ลักษณะและขอบเขตของงาน
- ประเภทของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น IT Outsourcing Cloud Computing บริการร่วมกับพันธมิตรทางธุรกิจ การใช้บริการเครือข่ายสาธารณะ การใช้บริการของผู้ให้บริการระบบชำระเงินกลาง เป็นต้น
- ระดับความเสี่ยง และระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

- ที่ตั้งศูนย์คอมพิวเตอร์หลักและสำรองของบุคคลภายนอกที่ประมวลผล จัดเก็บข้อมูล หรือดำเนินการใด ๆ เกี่ยวกับข้อมูลหรือระบบงานให้แก่ สง.
- วันเริ่มต้นและสิ้นสุดสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก
- การรับรองตามมาตรฐานสากลด้าน IT ที่เกี่ยวข้อง (ถ้ามี)
- รายละเอียดทรัพย์สินที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น ข้อมูลที่นำไปจัดเก็บหรือประมวลผล ระดับชั้นความลับข้อมูล เป็นต้น

12.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

(1) ทำการเข้ารหัสข้อมูลที่อยู่ภายใต้การดูแลของบุคคลภายนอกให้เป็นไปตามนโยบายและมาตรฐานของ สง. สอดคล้องกับมาตรฐานสากลตามระดับชั้นของข้อมูล (Information Classification) และพิจารณาให้ครอบคลุมทั้งข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at Endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (Data in Transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (Data at Rest) ซึ่งรวมถึงข้อมูลสำรอง

(2) บริหารจัดการกุญแจการเข้ารหัสข้อมูลของ สง. ด้วยตนเอง ซึ่งควรควบคุมในทุกขั้นตอนตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส (Lifecycle of Cryptographic Keys) ตั้งแต่การสร้าง การจัดเก็บ การใช้งาน การสำรอง การเพิกถอน และการต่ออายุของกุญแจเข้ารหัสข้อมูล

(3) สร้างกุญแจการเข้ารหัสด้วยตนเอง ทั้งนี้ หาก สง. ไม่สามารถสร้างกุญแจการเข้ารหัสด้วยตนเองได้ สง. ควรมั่นใจได้ว่ากุญแจการเข้ารหัสของบุคคลภายนอกไม่มีการนำมาใช้ร่วมกับผู้ใช้บริการรายอื่น และทราบถึงรายละเอียดเกี่ยวกับระบบการบริหารจัดการกุญแจเข้ารหัสข้อมูลของบุคคลภายนอก ได้แก่
   - ประเภทของกุญแจเข้ารหัสข้อมูล
   - รายละเอียดของระบบ รวมถึงกระบวนการควบคุมการเข้ารหัสข้อมูลในแต่ละขั้นตอนตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส
   - ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล

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

(5) สอบทานการปฏิบัติงานการบริหารจัดการการเข้ารหัสข้อมูลทั้งที่ดำเนินการโดย สง. และโดยบุคคลภายนอก ให้ครอบคลุมการสอบทานช่องโหว่และความเสี่ยงของการเข้ารหัสข้อมูล โดยพิจารณาให้มีความปลอดภัยสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป เช่น อัลกอริธึมการเข้ารหัส (Encryption Algorithm) และขนาดความยาวของกุญแจเข้ารหัสข้อมูล เป็นต้น

12.3 การควบคุมการเข้าถึง (Access Control)

(1) กำหนดกระบวนการจัดการและควบคุมดูแลสิทธิในการเบิกใช้และการเข้าถึงระบบและข้อมูลของ สง. ที่ชัดเจนเป็นลายลักษณ์อักษร เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่ สง. กำหนด รวมทั้งตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป

(2) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้มีสิทธิเข้าใช้งานระบบและผู้ใช้งานที่ได้รับสิทธิสูงให้ชัดเจน

(3) ควบคุมดูแลการให้สิทธิแก่บุคคลภายนอก โดยจำกัดสิทธิตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน มีการอนุมัติการเบิกใช้งาน เพื่อไม่ให้บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ

(4) มีระบบหรือกระบวนการติดตามระหว่างการใช้งานบัญชีผู้ใช้งานที่มีสิทธิสูงสุด รวมทั้งควรติดตามและสอบทานสถานะสิทธิและการใช้งานหรือการเข้าถึงระบบข้อมูล ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิอย่างเป็นประจำ เพื่อให้มั่นใจว่าการใช้งานสิทธิเป็นไปตามขอบเขต และความจำเป็นในการใช้งาน

(5) กำหนดวิธีการระบุและพิสูจน์ตัวตนผู้ใช้งาน ด้วยวิธีการที่รัดกุมเพียงพอ สอดคล้องกับมาตรฐานนโยบายที่ สง. กำหนด หรือมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป

(6) ในกรณีที่บุคคลภายนอกเชื่อมต่อเพื่อเข้าถึงระบบงานของ สง. ผ่านช่องทางการเข้าถึงระบบงานระยะไกล (System Remote Access) สง. ควรมีกระบวนการบริหารจัดการการเข้าถึงระยะไกลด้วยวิธีการที่ปลอดภัย ดังนี้

- มีการขออนุมัติก่อนการเข้าถึงระบบงานระยะไกล (System Remote Access) ของบัญชีผู้ใช้งานสิทธิสูงอย่างเคร่งครัด โดยให้ใช้เฉพาะกรณีที่มีความจำเป็นเท่านั้น และจำกัดระยะเวลาในการเข้าถึงระบบงาน
- มีการพิสูจน์ตัวตนผู้ใช้งานแบบ Two-Factors Authentication และการเชื่อมต่อผ่าน Virtual Private Network (VPN)
- มีการควบคุมการเข้าใช้งาน โดยจำกัดการเข้าใช้งานได้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้น หรือใช้เทคโนโลยีบริหารจัดการเครื่องคอมพิวเตอร์แบบเสมือน (Virtual Desktops Infrastructure) เพื่อลดความเสี่ยงจากการติด Malware หรือการเข้าถึงระบบงานที่ไม่เหมาะสม
- สามารถระบุและสอบทานแหล่งที่มาของอุปกรณ์หรือระบบปลายทางที่เข้าเชื่อมต่อกับระบบเครือข่ายของ สง. แบบระยะไกล
- มีการสอบทานการเข้าถึงระบบงานระยะไกล โดยบัญชีผู้ใช้งานสิทธิสูงด้วยบุคคลหรือหน่วยงานที่มีความเป็นอิสระและมีความรู้ความเชี่ยวชาญเพียงพอ

(7) ดูแลให้บุคคลภายนอกจัดเก็บบันทึกข้อมูลประวัติของการพิสูจน์ตัวตนและการเข้าถึง (Access Log) บันทึกการดำเนินงาน (Activity Log) ตามระยะเวลาที่กฎหมายกำหนด โดยมีการสอบทานข้อมูลการบันทึกเหตุการณ์ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยง

และความสำคัญอย่างเป็นประจำ เพื่อให้มั่นใจว่าบุคคลภายนอกปฏิบัติงานเป็นไปตามข้อตกลงและมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของ สง.

12.4 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

(1) มีการรักษาความปลอดภัยในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารกับบุคคลภายนอกเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

(2) ดูแลให้บุคคลภายนอก มีระบบหรือกระบวนการสำหรับคัดกรอง Traffic ที่ส่งผ่านระบบเครือข่าย ตรวจจับ แจ้งเตือน และสามารถยับยั้งการบุกรุกหรือตอบโต้การโจมตีได้โดยอัตโนมัติแบบต่อเนื่องบนระบบเครือข่ายให้เพียงพอเหมาะสมตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก 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 หรือมัลแวร์ต่าง ๆ ที่อาจบุกรุกเข้าสู่เครือข่าย เป็นต้น

(3) กรณีการใช้บริการ Cloud Computing ผู้ให้บริการ Cloud Computing ควรแบ่งแยกสภาพแวดล้อมของสถาบันการเงินจากผู้ใช้บริการรายอื่นที่อยู่ในสภาพแวดล้อมบน Cloud Computing ร่วมกัน

12.5 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

(1) กำหนดกระบวนการและแนวทางบริหารจัดการการเปลี่ยนแปลงร่วมกับบุคคลภายนอกเพื่อให้ สง. สามารถประเมินผลกระทบและเตรียมแนวทางรองรับ เช่น เมื่อมีการเปลี่ยนแปลงระบบของผู้ให้บริการ Cloud Computing และกระทบกับการให้บริการของ สง.

(2) ให้บุคคลภายนอกแจ้งการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบกับการให้บริการของ สง. ให้ สง. ได้ทราบล่วงหน้าในระยะเวลาที่ตกลงร่วมกัน เพื่อให้ สง. พิจารณาแนวทางลดผลกระทบต่อการให้บริการลูกค้าของ สง.

12.6 การบริหารจัดการการตั้งค่าระบบ (System Configuration Management)

กรณีบุคคลภายนอกมีหน้าที่เปลี่ยนแปลงการตั้งค่าระบบงาน สง. ควรกำหนดมาตรฐานการตั้งค่าระบบงานให้ปลอดภัยเพียงพอตามมาตรฐานด้านความปลอดภัยเทคโนโลยีสารสนเทศของ สง. เช่น ค่า System Configuration ของระบบปฏิบัติการ และการตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย เป็นต้น

12.7 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

(1) มีกระบวนการติดตาม ประเมินประสิทธิภาพและความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ ของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเพียงพอ

และต่อเนื่อง ตลอดจนรายงานผลการติดตามและประเมินดังกล่าวให้คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมใช้และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

(2) มีการกำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (Threshold และ Trigger) ในระดับต่าง ๆ และกำหนดกระบวนการรายงานและแจ้งเตือน ปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการให้บริการหรือเชื่อมต่อกับบุคคลภายนอก แนวทางการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง ให้เพียงพอเหมาะสมตามระดับความเสี่ยงและระดับความมีนัยสำคัญของบริการ เพื่อให้ สง. ทราบอย่างทันการณ์

12.8 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging)

ดูแลให้มั่นใจว่าบุคคลภายนอกมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัยเพื่อ สง. ใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน 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) ตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไปและสอดคล้องกับนโยบายระเบียบวิธีปฏิบัติของ สง.

(2) สอบทานขอบเขตและผลการทดสอบเจาะระบบของบุคคลภายนอกเพื่อให้มั่นใจว่าการทดสอบดังกล่าวครอบคลุมระบบทั้งหมดที่ สง. ใช้บริการหรือเชื่อมต่อกับบุคคลภายนอก และครอบคลุมภัยคุกคามที่สำคัญ

12.11 การสำรองข้อมูล (Data Backup)

กรณีที่ สง. ใช้บริการหรือเชื่อมต่อกับบุคคลภายนอก ซึ่งมีการจัดเก็บข้อมูลของ สง. หรือข้อมูลลูกค้า สง. ควรกำหนดมาตรฐานวิธีปฏิบัติในการสำรองข้อมูล ให้บุคคลภายนอกปฏิบัติให้สอดคล้องกับมาตรฐานของ สง. ครอบคลุม

- ขอบเขต/รายละเอียดของการสำรองข้อมูลและรอบเวลาสำรองข้อมูล
- วิธีการ/เทคโนโลยีการสำรองข้อมูล และรูปแบบข้อมูล (Data Format)
- ระยะเวลาในการเก็บรักษาข้อมูลสำรอง

- การตรวจสอบความถูกต้องครบถ้วนของข้อมูลสำรอง
- ขั้นตอนและวิธีการกู้ข้อมูล
- การสอบทานการสำรองข้อมูล (Restore)
- สถานที่จัดเก็บข้อมูลสำรอง

12.12 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

(1) มีการระบุหน้าที่และความรับผิดชอบของ สง. และบุคคลภายนอกอย่างชัดเจน ในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ รวมถึงกำหนดระดับความรุนแรงของเหตุการณ์ผิดปกติดังกล่าว และกำหนดให้แจ้ง สง. ทราบเหตุการณ์ผิดปกติที่เกิดขึ้นและเกี่ยวข้องกับ สง. อย่างเพียงพอและทันการณ์

(2) หากเหตุการณ์ผิดปกติที่เกิดขึ้นนั้นมีผลกระทบต่อการดำเนินธุรกิจของ สง. อย่างมีนัยสำคัญ สง. ควรมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ

(3) กำหนดให้บุคคลภายนอกจัดให้มีช่องทาง ระบบ หรือเครื่องมือเพื่อรองรับกรณี สง. ตรวจพบและต้องการรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศให้บุคคลภายนอกทราบ และเพื่อช่วยให้ สง. ติดตามสถานการณ์และการแก้ไขของบุคคลภายนอกต่อเหตุการณ์ผิดปกติที่เกี่ยวข้องกับ สง. ได้อย่างทันการณ์

(4) กำหนดให้บุคคลภายนอกมีผู้ประสานงานอย่างเป็นทางการ เพื่อประสานงานกับ สง. ในการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศได้อย่างทันการณ์

12.13 การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

(1) มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan) ที่ครอบคลุมถึงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้มีแนวทางรองรับต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อ สง. อย่างมีนัยสำคัญ เพื่อสามารถดำเนินธุรกิจอย่างต่อเนื่อง

(2) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรคำนึงถึงปัจจัยสำคัญหรือความเสี่ยงที่อาจเกิดขึ้นและส่งผลต่อการหยุดชะงักจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ผลกระทบที่มีต่อการดำเนินธุรกิจของ สง. และการติดต่อสื่อสารระหว่างบุคคลภายนอกกับ สง. รวมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติให้คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างทันการณ์ตามความสำคัญและระดับความรุนแรงหรือผลกระทบของเหตุการณ์

(3) ประเมินและทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของบุคคลภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของ สง. เช่น ความสอดคล้องกันของขอบเขต คำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

(4) หาก สง. สามารถเข้าร่วมทดสอบกับบุคคลภายนอกได้ สง. ควรเข้าร่วมทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศกับบุคคลภายนอก เพื่อประเมินความพร้อมของบุคคลภายนอกในการกู้คืนระบบงานตามกรอบ MTPD, RTO และ RPO ที่กำหนดไว้

(5) ทีมบริหารจัดการในสภาวะวิกฤติ (Crisis Management Team) ของ สง. ควรได้รับทราบถึงรายละเอียดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของบุคคลภายนอก เพื่อเตรียมความพร้อมในการบริหารจัดการในส่วนที่เกี่ยวข้อง

(6) รวบรวมปัญหาที่พบระหว่างการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และปรับปรุงแก้ไขร่วมกับบุคคลภายนอก

ส่วนที่ 3 : การรายงานต่อธนาคารแห่งประเทศไทย

สถาบันการเงินต้องจัดส่งรายงานบุคคลภายนอกที่สถาบันการเงินใช้บริการงานด้านเทคโนโลยีสารสนเทศ (IT Outsourcing) และพันธมิตรทางธุรกิจที่มีนัยสำคัญ ให้ธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชนเป็นรายไตรมาส

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