ธนาคารแห่งประเทศไทย

19 มกราคม 2561

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง

ที่ ฝนส.(01)ว. 3 /2561 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ธนาคารแห่งประเทศไทยขอนำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ลงวันที่ 20 ธันวาคม 2560 ซึ่งได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 135 ตอนพิเศษ 11 ง ลงวันที่ 18 มกราคม 2561 แล้ว และมีผลบังคับใช้ตั้งแต่วันที่ 1 เมษายน 2561 เป็นต้นไป

สาระสำคัญของประกาศฉบับนี้ คือ

1. ให้สถาบันการเงินให้ความสำคัญในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน โดยสถาบันการเงินต้องมีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงอย่างเหมาะสม มีการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมทั้งการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพและรัดกุม

2. ในกรณีที่สถาบันการเงินเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบ หรือชื่อเสียงของสถาบันการเงิน โดยรวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของสถาบันการเงินถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่สถาบันการเงินต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงินทราบ สถาบันการเงินต้องรายงานมายังธนาคารแห่งประเทศไทยทันทีเมื่อเกิดหรือรับรู้เหตุการณ์นั้น โดยสามารถแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมได้ในภายหลัง

3. เมื่อสถาบันการเงินมีการนำเทคโนโลยีใด ๆ มาใช้เป็นครั้งแรก หรือมีการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจ สถาบันการเงินต้องยื่นแผนการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยี ซึ่งได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมายแล้วต่อธนาคารแห่งประเทศไทย เพื่อขออนุญาตก่อนดำเนินการดังกล่าว

ทั้งนี้ ในกรณีที่ธนาคารแห่งประเทศไทยมีการกำหนดมาตรฐานการกำกับดูแลหรือแนวทางบริหารความเสี่ยงสำหรับการใช้เทคโนโลยีใดแล้ว เช่น มาตรฐานการกำกับดูแลการนำเทคโนโลยี ซึ่งได้ผ่านการทดสอบใน Regulatory Sandbox มาใช้ในการดำเนินธุรกิจ (guideline) ซึ่งครอบคลุมถึงมาตรฐานของเทคโนโลยี

ฝนสว00-คส50001-2561019

คส500	วันที่ 19 ม.ค. 2561

และแนวทางการกำกับดูแลเกี่ยวกับการบริหารความเสี่ยงและการดูแลผู้ใช้บริการ สถาบันการเงินสามารถนำเทคโนโลยีซึ่งมีมาตรฐานการกำกับดูแลดังกล่าวนั้นมาใช้ในการดำเนินธุรกิจได้ โดยไม่ต้องยื่นขออนุญาตต่อธนาคารแห่งประเทศไทยก่อนดำเนินการแม้จะเป็นการนำเทคโนโลยีนั้นมาใช้เป็นครั้งแรก ทั้งนี้ สถาบันการเงินต้องปฏิบัติตามมาตรฐานการกำกับดูแลหรือแนวทางบริหารความเสี่ยงสำหรับการใช้เทคโนโลยีนั้นตามที่ธนาคารแห่งประเทศไทยกำหนดอย่างเคร่งครัด

อนึ่ง ธนาคารแห่งประเทศไทยขอนำส่งแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (implementation guideline) ซึ่งมีหลักการที่สอดคล้องกับประกาศฉบับนี้มาพร้อมกัน เพื่อให้สถาบันการเงินใช้เป็นแนวทางในกำหนดวิธีปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้สถาบันการเงินพิจารณาปรับใช้อย่างเหมาะสมตามลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีที่นำมาใช้ และความเสี่ยงที่เกี่ยวข้อง

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวเมทินี ศุภสวัสดิ์กุล)
ผู้อำนวยการอาวุโส ฝ่ายนโยบายการกำกับสถาบันการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2560 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ลงวันที่ 20 ธันวาคม 2560
2. แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6938, 0 2283 5869

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

ประกาศธนาคารแห่งประเทศไทย
ที่ สนส. 19 /2560
เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk) ของสถาบันการเงิน

---

1. เหตุผลในการออกประกาศ

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) ได้เข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจของสถาบันการเงินมากขึ้น โดยสถาบันการเงินได้นำเทคโนโลยีสารสนเทศมาใช้เป็นโครงสร้างพื้นฐานที่สำคัญที่ช่วยเพิ่มประสิทธิภาพในการดำเนินธุรกิจ ลดต้นทุนในการดำเนินงาน และเพิ่มศักยภาพในการแข่งขัน นอกจากนี้ เทคโนโลยีสารสนเทศยังเป็นส่วนสำคัญที่ช่วยให้สถาบันการเงินสามารถพัฒนาผลิตภัณฑ์และบริการทางการเงินที่ทำให้เข้าถึงลูกค้าได้อย่างทั่วถึง และตอบสนองต่อความต้องการของลูกค้าที่ต้องการผลิตภัณฑ์และบริการที่หลากหลายได้อย่างสะดวกและรวดเร็วมากยิ่งขึ้น โดยเฉพาะการนำเสนอบริการทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ รวมถึงการประกอบธุรกิจเทคโนโลยีทางการเงิน (Financial Technology : FinTech) อย่างไรก็ดี แม้ว่าการใช้เทคโนโลยีสารสนเทศจะช่วยให้การดำเนินธุรกิจของสถาบันการเงินมีประสิทธิภาพมากขึ้นและช่วยให้สถาบันการเงินสามารถตอบสนองต่อความต้องการของลูกค้าได้ดีขึ้น แต่หากสถาบันการเงินขาดการบริหารความเสี่ยงที่ดี การใช้เทคโนโลยีสารสนเทศดังกล่าวก็อาจก่อให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) และภัยคุกคามทางไซเบอร์ (cyber threat) ที่ส่งผลกระทบต่อสถาบันการเงินทั้งในด้านความเสียหายที่เป็นจำนวนเงินและความเสียหายด้านชื่อเสียง รวมทั้ง อาจส่งผลกระทบต่อระบบการชำระเงินและระบบการเงินของประเทศ ซึ่งจะส่งผลต่อความเชื่อมั่นของลูกค้าที่มีต่อการใช้บริการทางการเงินได้

ดังนั้น ธนาคารแห่งประเทศไทยจึงกำหนดหลักเกณฑ์กำกับดูแลให้สถาบันการเงินมีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและมีการบริหารความเสี่ยงดังกล่าวอย่างเหมาะสม โดยเน้นที่องค์ประกอบและบทบาทหน้าที่ของคณะกรรมการของสถาบันการเงิน โครงสร้างองค์กร และการบริหารจัดการบุคลากร โดยคณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินต้องมีความรู้ความเข้าใจอย่างเพียงพอในการกำหนดทิศทางการใช้เทคโนโลยีให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจของสถาบันการเงิน มีความเท่าทันความเสี่ยงที่มีมากขึ้นอันเนื่องมาจากการนำเทคโนโลยีมาใช้อย่างแพร่หลาย ให้ความสำคัญกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงิน (Enterprise Risk Management : ERM) และมีการกำหนดและสื่อสารนโยบายที่เกี่ยวข้องไปยังบุคลากรทุกระดับในองค์กรเพื่อให้เกิดความตระหนักและความเข้าใจ ตลอดจนมีการนำนโยบายไปปฏิบัติด้วยกระบวนการที่เหมาะสม รวมถึงต้องดูแลให้มีการวางแผนและบริหารจัดการด้านบุคลากร โดยเฉพาะที่ทำหน้าที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศให้มีคุณสมบัติและความรู้ที่เหมาะสมกับหน้าที่ที่ได้รับมอบหมาย และมีปริมาณที่เพียงพอที่จะรองรับการดำเนินธุรกิจของสถาบันการเงินทั้งในปัจจุบันและในอนาคต

ฝนสป00-คส50001-2560120

คส 500	วันที่ 20 ธ.ค. 2560

นอกจากนี้ ธนาคารแห่งประเทศไทยยังเน้นให้สถาบันการเงินมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การตรวจสอบด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพและรัดกุม โดยอยู่ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ (1) การรักษาความลับของระบบและข้อมูล (confidentiality) (2) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ (3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) รวมถึงอยู่บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า ซึ่งสถาบันการเงินต้องมีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านชื่อเสียง และความเสี่ยงด้านกฎหมาย

ทั้งนี้ ในกรณีที่สถาบันการเงินเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศ ซึ่งส่งผลกระทบต่อการให้บริการ ระบบ หรือชื่อเสียงของสถาบันการเงิน โดยรวมถึงกรณีที่เทคโนโลยีสารสนเทศที่สำคัญของสถาบันการเงินถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่สถาบันการเงินต้องรายงานให้ผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงินทราบ ให้สถาบันการเงินต้องรายงานมายังธนาคารแห่งประเทศไทยทันทีเมื่อเกิดหรือรับรู้เหตุการณ์นั้น และเมื่อสถาบันการเงินมีการนำเทคโนโลยีใด ๆ มาใช้เป็นครั้งแรก หรือมีการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจ สถาบันการเงินจะต้องได้รับอนุญาตจากธนาคารแห่งประเทศไทยก่อนดำเนินการดังกล่าว

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 41 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ให้สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศนี้

3. ประกาศที่ยกเลิก

ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 26/2551 เรื่อง การอนุญาตให้ธนาคารพาณิชย์ให้บริการการเงินทางอิเล็กทรอนิกส์ ลงวันที่ 3 สิงหาคม 2551

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

5. เนื้อหา

5.1 ให้ยกเลิกความในข้อ 5.2 การรักษาความปลอดภัย และข้อ 5.3 การควบคุมภายในของประกาศธนาคารแห่งประเทศไทยที่ สนส. 27/2551 เรื่อง การอนุญาตให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ให้บริการการเงินทางอิเล็กทรอนิกส์ ลงวันที่ 3 สิงหาคม 2551 และให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้แทน

5.2 คำจำกัดความ

“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของสถาบันการเงิน รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threat)

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

“คณะกรรมการของสถาบันการเงิน” หมายความว่า คณะกรรมการของสถาบันการเงินที่จดทะเบียนในประเทศไทย หรือคณะผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบที่เกี่ยวข้องของสาขาของธนาคารพาณิชย์ต่างประเทศ

5.3 หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.3.1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)

(1) บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของสถาบันการเงิน

คณะกรรมการของสถาบันการเงินต้องมีองค์ประกอบตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์ด้านธรรมาภิบาลของสถาบันการเงิน โดยมีกรรมการที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างน้อย 1 ท่าน เพื่อให้คณะกรรมการของสถาบันการเงินสามารถกำหนดทิศทางและกำกับดูแลให้สถาบันการเงินมีการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจของสถาบันการเงิน มีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีที่เปลี่ยนแปลงไป ซึ่งจะช่วยให้คณะกรรมการของสถาบันการเงินสามารถกำกับดูแลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

นอกจากนี้ กรรมการของสถาบันการเงินต้องได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้องอย่างเพียงพอตามระยะเวลาที่เหมาะสม เพื่อให้คณะกรรมการของสถาบันการเงินมีความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้องเพื่อประโยชน์ในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน คณะกรรมการของสถาบันการเงินมีบทบาทหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยดังต่อไปนี้

(1.1) ดูแลให้มีการใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการดำเนินธุรกิจของสถาบันการเงิน และดูแลให้การใช้เทคโนโลยีของสถาบันการเงินมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต

(1.2) ดูแลให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นความเสี่ยงที่สำคัญ โดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงิน (Enterprise Risk Management : ERM)

(1.3) ดูแลให้มีการกำหนด (1) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งรวมถึงนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และ (2) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยนโยบายดังกล่าวต้องสอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งทำหน้าที่ในการอนุมัตินโยบายดังกล่าว

(1.4) ดูแลให้มีการนำ (1) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และ (2) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ที่ได้อนุมัติ มาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพของนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(1.5) ดูแลให้มีการติดตาม ตรวจสอบ และรายงานต่อคณะกรรมการของสถาบันการเงิน คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงของสถาบันการเงินอย่างเหมาะสม ในเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น ผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของสถาบันการเงิน ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ทางด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของสถาบันการเงิน

(1.6) ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรของสถาบันการเงิน เพื่อให้ตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ และให้เข้าใจถึงการใช้เทคโนโลยีสารสนเทศที่ถูกต้อง เพื่อช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2) โครงสร้างการกำกับดูแล

(2.1) โครงสร้างองค์กร

สถาบันการเงินต้องจัดให้มีโครงสร้างองค์กรที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence) โดยมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่างการทำหน้าที่ (1) ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (2) บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และ (3) ตรวจสอบด้านเทคโนโลยีสารสนเทศ นอกจากนี้ สถาบันการเงินต้องจัดให้มีการถ่วงดุลอำนาจกันอย่างอิสระ โดยเฉพาะการทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องมีความเป็นอิสระจากการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ทั้งนี้ สถาบันการเงินอาจจัดให้มีผู้บริหารระดับสูงหรือหัวหน้าสายงานที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (IT security) โดยควรมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และควรเป็นผู้ที่มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศและด้านการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ เช่น ได้รับการรับรองความรู้ความสามารถตามมาตรฐานสากล

(2.2) คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2.2.1) สถาบันการเงินต้องจัดให้มีคณะกรรมการที่ทำหน้าที่บริหารจัดการ รวมถึงกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee

(2.2.2) สถาบันการเงินต้องจัดให้มีคณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

(2.2.3) สถาบันการเงินต้องจัดให้มีคณะกรรมการที่ทำหน้าที่กำกับดูแลให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งการตรวจสอบครอบคลุมถึงการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลให้มีการสอบทานการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

(3) การบริหารจัดการบุคลากร

สถาบันการเงินต้องมีการบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวัน (user) อย่างเหมาะสม โดยต้องคำนึงถึงความรู้ความสามารถของบุคลากร ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยสถาบันการเงินต้องจัดให้มีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(3.1) การบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ จะต้องครอบคลุมในเรื่องดังต่อไปนี้

(3.1.1) กระบวนการคัดเลือกบุคลากร เพื่อให้ได้บุคลากรที่มีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย โดยอาจพิจารณาการได้รับการรับรองความรู้ความสามารถตามมาตรฐานที่รับรองทั่วไป (certificate) เฉพาะด้านที่เกี่ยวข้องกับงานด้านเทคโนโลยีสนเทศที่ได้รับมอบหมายนั้น

(3.1.2) ความเพียงพอของบุคลากร เพื่อให้มีปริมาณบุคลากรที่เพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศของสถาบันการเงิน

(3.1.3) มาตรการในการสร้างและส่งเสริมความตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้บุคลากรมีการตระหนักถึงบทบาทหน้าที่และความรับผิดชอบของตน และมาตรการดูแลให้บุคลากรปฏิบัติตามหน้าที่และรับผิดชอบตามที่กำหนดไว้

(3.2) การอบรมให้ความรู้แก่คณะกรรมการของสถาบันการเงิน ผู้บริหารระดับสูง และบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ อย่างเพียงพอตามระยะเวลาที่เหมาะสม โดยครอบคลุมเนื้อหาต่าง ๆ ที่เกี่ยวข้อง เช่น พัฒนาการด้านเทคโนโลยี ภัยคุกคามทางไซเบอร์ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อให้คณะกรรมการ

ของสถาบันการเงิน ผู้บริหารระดับสูง และบุคลากรมีความรู้และทักษะที่เพียงพอต่อการกำกับดูแลหรือปฏิบัติงานในส่วนที่เกี่ยวข้อง

(3.3) ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของบุคลากรควรระบุในเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินอย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

(3.4) การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยต้องมีการปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน เช่น ทบทวนสิทธิในการเข้าถึงข้อมูล รวมทั้งต้องมีการสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบดังกล่าว

(4) การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness)

สถาบันการเงินต้องจัดให้มีการสื่อสารและให้ความรู้แก่บุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรมีความเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ที่มีการเชื่อมต่อกับอินเทอร์เน็ตที่ถูกต้อง และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์

(5) นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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

นอกจากนี้ การกำหนดนโยบายดังกล่าวต้องคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศภายในองค์กรและความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกด้วย

(5.2) สถาบันการเงินต้องจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.3.2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

เพื่อให้สถาบันการเงินมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ สถาบันการเงินต้องนำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

สถาบันการเงินต้องจัดให้มีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องมีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้ในการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงต้องจัดให้มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

(2) การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

สถาบันการเงินต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ มีการจัดชั้นความลับของข้อมูล (information classification) มีการเก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากล เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

(3) การควบคุมการเข้าถึง (access control)

สถาบันการเงินต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงานและระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

(4) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

สถาบันการเงินต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค (facility) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

(5) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

สถาบันการเงินต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของสถาบันการเงิน เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่มีการรับส่งผ่านเครือข่ายสื่อสารมีความมั่นคงปลอดภัย และสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

(6) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

สถาบันการเงินต้องจัดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(6.1) การบริหารจัดการขีดความสามารถของระบบ และระบบสาธารณูปโภค (capacity management) เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการดำเนินธุรกิจและสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

(6.2) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (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) โดยมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เช่น เครื่องมือในการติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

(6.6) การบริหารจัดการช่องโหว่ (vulnerability management) ของระบบที่เหมาะสมตามระดับความเสี่ยง เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ โดยสถาบันการเงินต้องมีการประเมินช่องโหว่ของระบบงานสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(6.7) การทดสอบเจาะระบบ (penetration test) โดยจัดให้มีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงาน (application) และระบบเครือข่าย (network) ที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

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

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

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

(7) การจัดหาและการพัฒนาระบบ (system acquisition and development)

(7.1) การจัดหาระบบ (system acquisition)

สถาบันการเงินต้องกำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและผู้ให้บริการ เช่น ความน่าเชื่อถือของระบบและผู้ให้บริการ การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate) ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ เพื่อให้มั่นใจว่าระบบและผู้ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินธุรกิจของสถาบันการเงินได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี หรือการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจในอนาคต

(7.2) การพัฒนาระบบ (system development)

สถาบันการเงินต้องจัดให้มีการออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยสถาบันการเงินต้องจัดให้มีอย่างน้อยในเรื่องดังต่อไปนี้

– เอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการในการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

– กระบวนการหรือเครื่องมือในการควบคุมเวอร์ชันของคำสั่งในการเขียนโปรแกรม (source code version control)

– การแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบและผู้นำระบบขึ้นใช้งานจริง

– การแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)

– การทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (unit test) ทดสอบการทำงานร่วมกันของระบบต่าง ๆ (system integration test) ทดสอบความพร้อมใช้งานตามกระบวนการและความต้องการของผู้ใช้งาน (user acceptance test) และทดสอบความปลอดภัยของระบบ (security test) ตามกระบวนการในการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification)

– การพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ สถาบันการเงินต้องจัดให้มีการทดสอบประสิทธิภาพ (performance test)

– แนวทางในการควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ

– การจัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

(8) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)

สถาบันการเงินต้องจัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยมีการบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติและปัญหา และการแก้ไข ให้คณะกรรมการของสถาบันการเงิน คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ทราบในระยะเวลาที่เหมาะสม นอกจากนี้ สถาบันการเงินต้องมีการวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริงและป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

(9) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

(9.1) สถาบันการเงินต้องจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรให้เป็นไปตามนโยบายที่กำหนดไว้ และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศดังกล่าวต้องได้รับอนุมัติโดยคณะกรรมการของสถาบันการเงิน

(9.2) ในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ สถาบันการเงินต้องคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของสถาบันการเงิน รวมทั้งการบริหารความเสี่ยงที่อาจเกิดจากเหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงทั่วไป เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) และความเสี่ยงอื่นที่เกี่ยวข้อง เช่น ความเสี่ยงจากการพึ่งพาองค์กรอื่น

ในการดำเนินธุรกิจ (interdependency risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และความเสี่ยงที่มีผลกระทบต่อสถาบันการเงิน ผู้ใช้บริการ ผู้มีส่วนได้เสีย และระบบสถาบันการเงิน (systemic risk)

(9.3) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องมีความเป็นไปได้ในทางปฏิบัติ สามารถนำมาใช้รองรับความเสียหายที่เกิดขึ้นได้จริง และสอดคล้องกับแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) โดยแผนฉุกเฉินดังกล่าวควรครอบคลุมถึงการกำหนดระยะเวลาในการกู้คืนระบบ (recovery time objective : RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point objective : RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงิน และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามทางไซเบอร์ ภัยธรรมชาติ เพื่อให้สถาบันการเงินดำเนินการกู้ระบบและกลับสู่การทำงานได้ตามปกติให้เร็วที่สุด

(9.4) สถาบันการเงินต้องจัดทำคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์แผนและฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนได้

(9.5) สถาบันการเงินต้องจัดให้มีการทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(9.6) สถาบันการเงินต้องจัดให้มีศูนย์คอมพิวเตอร์สำรอง (disaster recovery site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก (primary site) หยุดชะงัก โดยสถาบันการเงินควรพิจารณาให้ศูนย์คอมพิวเตอร์สำรองอยู่ห่างจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะมิให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง และภัยธรรมชาติ

(10) การบริหารจัดการผู้ให้บริการภายนอก (third party management)

ในกรณีที่สถาบันการเงินมีการจัดจ้างผู้ให้บริการภายนอก หรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หรือสามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือของลูกค้าของสถาบันการเงินได้ สถาบันการเงินต้องมีการจัดทำสัญญาหรือข้อตกลงการให้บริการโดยระบุหน้าที่ ความรับผิดชอบ และเงื่อนไขในการให้บริการอย่างชัดเจน เช่น การทำลายข้อมูลของสถาบันการเงินหรือของลูกค้าทั้งหมดเมื่อสิ้นสุดสัญญาหรือเลิกใช้บริการ ความรับผิดชอบต่อการรั่วไหลของข้อมูลอันเนื่องมาจากการนำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ

นอกจากนี้ ในการจัดจ้างผู้ให้บริการภายนอกหรือมีพันธมิตรทางธุรกิจในการร่วมพัฒนาหรือให้บริการทางการเงิน สถาบันการเงินต้องคำนึงถึงความต่อเนื่องในการดำเนินธุรกิจของสถาบันการเงิน ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ

และการยกเลิกหรือสิ้นสุดสัญญา (exit strategy) เพื่อให้สถาบันการเงินสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และพร้อมรับการเปลี่ยนแปลงด้านเทคโนโลยีที่อาจเกิดขึ้นในอนาคต

ทั้งนี้ ในกรณีที่สถาบันการเงินใช้บริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) ให้สถาบันการเงินปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยเรื่องการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงินด้วย

5.3.3 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

เพื่อให้สถาบันการเงินสามารถบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ สถาบันการเงินต้องกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(1) การประเมินความเสี่ยง (risk assessment)

(1.1) การระบุความเสี่ยง (risk identification)

สถาบันการเงินต้องระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงภัยคุกคามทางไซเบอร์ 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)

สถาบันการเงินต้องมีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ สถาบันการเงินต้องจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ในการติดตามและทบทวนความเสี่ยง

(3) การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

สถาบันการเงินต้องจัดให้มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

(4) การรายงานความเสี่ยง (risk reporting)

สถาบันการเงินต้องมีการรายงานผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและแนวโน้มของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น ต่อคณะกรรมการของสถาบันการเงิน หรือคณะกรรมการที่ได้รับมอบหมายในระยะเวลาที่เหมาะสม

ทั้งนี้ สถาบันการเงินต้องจัดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.3.4 การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

สถาบันการเงินต้องจัดให้มีการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยระบบการชำระเงิน เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

5.3.5 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

(1) สถาบันการเงินต้องจัดให้มีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2) สถาบันการเงินต้องจัดให้มีแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงของการใช้เทคโนโลยีสารสนเทศของสถาบันการเงิน และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการตรวจสอบ และต้องครอบคลุมถึงเทคโนโลยีสารสนเทศที่สำคัญของสถาบันการเงิน ทั้งนี้ สถาบันการเงินต้องจัดให้มีการทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าวอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(3) สถาบันการเงินต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง ตามแผนงานและขอบเขตที่กำหนดตามข้อ (2) และเมื่อมีเหตุการณ์ผิดปกติในเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

(4) สถาบันการเงินต้องจัดให้มีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่มีความสำคัญ ซึ่งสถาบันการเงินเห็นว่ามีความจำเป็นต้องประเมิน แต่สถาบันการเงินมีข้อจำกัด หรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการเงินตามข้อ (1) ไม่สามารถประเมินได้ เช่น การประเมินระบบที่มีความซับซ้อนหรือมีการใช้เทคโนโลยีใหม่ หรือการประเมินความสามารถของระบบในการปรับเปลี่ยนเพื่อรองรับการทำธุรกิจของสถาบันการเงินในอนาคตภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว

(5) สถาบันการเงินต้องจัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและเสนอต่อคณะกรรมการตรวจสอบ ตลอดจนจัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่สถาบันการเงิน พร้อมไว้สำหรับการตรวจสอบหรือเมื่อร้องขอโดยธนาคารแห่งประเทศไทย

(6) สถาบันการเงินต้องจัดให้มีการติดตามประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานประเด็นสำคัญให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้องทราบ

5.3.6 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

(1) สถาบันการเงินต้องจัดให้มีการศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับของโครงการที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องมีการพิจารณาเลือกใช้เทคโนโลยีอย่างเหมาะสม และมีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งต้องมีการจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการของสถาบันการเงิน คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงตามขอบเขตอำนาจในการอนุมัติที่กำหนดไว้

(2) สถาบันการเงินต้องมีการกำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางในการบริหารจัดการโครงการ (project management) โดยครอบคลุมขั้นตอนตั้งแต่การเริ่มโครงการ การดำเนินการและการควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ รวมทั้งต้องมีการกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (project governance) โดยสถาบันการเงินต้องจัดให้มีอย่างน้อยในเรื่องต่อไปนี้

(2.1) คณะกรรมการกำกับดูแลโครงการ เพื่อทำหน้าที่ในการกำกับดูแลความคืบหน้า ให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้การดำเนินงานของโครงการเป็นไปตามแผนงานที่กำหนด ทั้งนี้ คณะกรรมการกำกับดูแลโครงการควรประกอบด้วยผู้บริหารหรือผู้แทนจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้อง

(2.2) หน่วยงานหรือทีมงานดูแลภาพรวมของโครงการ (Project Management Office : PMO) เพื่อทำหน้าที่ในการกำหนดรูปแบบ กระบวนการ และเครื่องมือที่เป็นมาตรฐานในการบริหารจัดการและติดตามความคืบหน้าของโครงการ รวมทั้งรายงานความคืบหน้าและภาพรวมของโครงการที่สำคัญของสถาบันการเงินต่อคณะกรรมการของสถาบันการเงิน คณะกรรมการที่ได้รับมอบหมายในการกำกับดูแลโครงการ หรือผู้บริหารระดับสูงที่เกี่ยวข้องทราบ เพื่อให้โครงการบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้

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

5.4 การรายงานต่อธนาคารแห่งประเทศไทย

สถาบันการเงินต้องรายงานต่อธนาคารแห่งประเทศไทยในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียงของสถาบันการเงิน รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของสถาบันการเงินถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่สถาบันการเงินต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงินทราบ โดยให้สถาบันการเงินรายงานปัญหาหรือเหตุการณ์ดังกล่าวมายังฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธนาคารแห่งประเทศไทย ทันทีเมื่อเกิดหรือรับรู้ปัญหาหรือเหตุการณ์นั้น และให้สถาบันการเงินแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

5.5 การขออนุญาตการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยี

ในกรณีที่สถาบันการเงินมีการนำเทคโนโลยีใด ๆ มาใช้เป็นครั้งแรก หรือมีการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจ ให้สถาบันการเงินยื่นแผนการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยีที่ได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงินหรือคณะกรรมการที่ได้รับมอบหมาย ต่อฝ่ายกำกับธุรกิจสถาบันการเงิน สายนโยบายสถาบันการเงิน ธนาคารแห่งประเทศไทยเพื่อขออนุญาตก่อนดำเนินการ ซึ่งแผนดังกล่าวอย่างน้อยต้องระบุถึงเหตุผลและความจำเป็น รายละเอียดการใช้เทคโนโลยีสารสนเทศ การคุ้มครองผู้ใช้บริการ แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และผลการประเมินความเสี่ยงและแนวทางการบริหารความเสี่ยงที่ผ่านการพิจารณาและลงนามรับทราบเป็นลายลักษณ์อักษรจากหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงของสถาบันการเงิน รวมถึงเอกสารที่เกี่ยวข้องอื่นใดที่ธนาคารแห่งประเทศไทยอาจร้องขอเพิ่มเติม โดยธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการนับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน

ทั้งนี้ หากสถาบันการเงินมีข้อสงสัยเกี่ยวกับการพิจารณาการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจ ให้สถาบันการเงินหารือมายังฝ่ายกำกับธุรกิจสถาบันการเงิน สายนโยบายสถาบันการเงิน ธนาคารแห่งประเทศไทยก่อนดำเนินการ

5.6 การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

ในกรณีที่สถาบันการเงินใดไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดตามประกาศฉบับนี้ได้ ให้สถาบันการเงินยื่นขออนุญาตผ่อนผันการปฏิบัติตามหลักเกณฑ์ดังกล่าวมายังฝ่ายกำกับธุรกิจสถาบันการเงิน สายนโยบายสถาบันการเงิน ธนาคารแห่งประเทศไทย เป็นรายกรณี พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนในการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการนับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน

5.7 **บทเฉพาะกาล**

เมื่อประกาศฉบับนี้มีผลใช้บังคับแล้ว สถาบันการเงินใดไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในข้อ 5.3.1 ได้ ให้สถาบันการเงินดำเนินการแก้ไขปรับปรุงให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในเรื่องดังกล่าวได้ภายในเวลา 1 ปีนับจากวันที่ประกาศฉบับนี้มีผลบังคับใช้ โดยไม่ต้องยื่นขออนุญาตผ่อนผันในเรื่องดังกล่าวมายังธนาคารแห่งประเทศไทย

6. วันเริ่มต้นบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันที่ 1 เมษายน 2561 เป็นต้นไป

ประกาศ ณ วันที่ 20 ธันวาคม 2560

(นายวิรไท สันติประภพ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายนโยบายการกำกับสถาบันการเงิน
โทรศัพท์ 0 2283 6938

คำถาม – คำตอบแนบท้ายประกาศ
เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk) ของสถาบันการเงิน
ลงวันที่ 20 ธันวาคม 2560

ข้อ	ประเด็นคำถาม	แนวคำตอบ
ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)		
1.	ในกรณีที่สถาบันการเงินไม่มีกรรมการที่มีความรู้ด้านเทคโนโลยีสารสนเทศ (Information Technology : IT) แต่สถาบันการเงินมีการจัดอบรมด้าน IT ให้แก่กรรมการของสถาบันการเงินแทน จะถือว่าสถาบันการเงินปฏิบัติตามหลักเกณฑ์ของประกาศฉบับนี้แล้วหรือไม่	สถาบันการเงินต้องมีกรรมการที่มีความรู้หรือประสบการณ์ด้าน IT อย่างน้อย 1 ท่านในคณะกรรมการของสถาบันการเงิน เพื่อช่วยให้ความเห็นในการกำหนดทิศทางและกำกับดูแลให้สถาบันการเงินมีการใช้ IT ให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ และมีการกำกับดูแลการบริหารจัดการความเสี่ยงด้าน IT ได้อย่างมีประสิทธิภาพ โดยจบการศึกษาในสาขาที่เกี่ยวข้องกับ IT หรือมีประสบการณ์ในการทำงานที่เกี่ยวข้องกับ IT ซึ่งการอบรมด้าน IT นั้นอาจไม่เพียงพอเนื่องจากเป็นการเสริมความรู้และความตระหนักรู้ให้กรรมการเท่าทันต่อสถานการณ์ความเสี่ยงและเทคโนโลยีที่เปลี่ยนแปลงไปมากขึ้นเท่านั้น
2.	กรรมการที่มีความรู้หรือประสบการณ์ด้าน IT อย่างน้อย 1 ท่านที่ธนาคารแห่งประเทศไทยกำหนดนั้น ต้องเป็นกรรมการอิสระ หรือเป็นกรรมการที่ไม่เป็นผู้บริหารด้วยหรือไม่	ธนาคารแห่งประเทศไทยไม่ได้กำหนดว่ากรรมการที่มีความรู้หรือประสบการณ์ด้าน IT ต้องเป็นกรรมการอิสระกรรมการที่ไม่เป็นผู้บริหาร หรือกรรมการที่เป็นผู้บริหาร
3.	ในกรณีที่คณะกรรมการของสถาบันการเงินมอบหมายหน้าที่กำกับดูแลและสนับสนุนการบริหารความเสี่ยงด้าน IT ให้คณะกรรมการชุดย่อย เช่น คณะกรรมการบริหารความเสี่ยงในการทำหน้าที่กำกับดูแล อนุมัติโครงการและนโยบายที่เกี่ยวข้องกับการกำกับดูแลด้าน IT รวมทั้งติดตามการนำนโยบายไปใช้อย่างเหมาะสมแทนแล้ว สถาบันการเงินยังคงต้องสรรหาและคัดเลือกบุคคลที่มีความรู้หรือประสบการณ์ด้าน IT เข้าเป็นหนึ่งในกรรมการในคณะกรรมการของสถาบันการเงินอีกหรือไม่	คณะกรรมการของสถาบันการเงินไม่สามารถมอบหมายให้คณะกรรมการชุดย่อยทำหน้าที่ในการอนุมัตินโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT แต่สามารถมอบหมายให้คณะกรรมการชุดย่อยดำเนินการในส่วนของการดูแลและติดตามการนำนโยบายที่ได้รับอนุมัติไว้แล้วไปใช้อย่างเหมาะสมได้ โดยต้องมีการรายงานให้คณะกรรมการของสถาบันการเงินทราบในการดำเนินการในเรื่องดังกล่าว ดังนั้น สถาบันการเงินยังคงต้องสรรหาและคัดเลือกบุคคลที่มีความรู้หรือประสบการณ์ด้าน IT เข้าเป็นหนึ่งในกรรมการในคณะกรรมการของสถาบันการเงินเพื่อให้คณะกรรมการของสถาบันการเงินทำหน้าที่ได้ตามบทบาทที่ประกาศกำหนดได้อย่างมีประสิทธิภาพ
4.	ในกรณีที่สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ มีคณะกรรมการชุดต่าง ๆ รวมทั้งโครงสร้างการกำกับดูแลความเสี่ยงด้าน IT ทั้งระดับการปฏิบัติงาน (1st line) ระดับการบริหารความเสี่ยง (2nd line) และระดับการตรวจสอบ (3rd line) อยู่ที่ต่างประเทศ โดยมีหน่วยงาน	การพิจารณาโครงสร้างการกำกับดูแลความเสี่ยงด้าน IT ให้พิจารณาที่โครงสร้างการกำกับดูแลโดยรวมของสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศทั้งหน่วยงานที่อยู่ต่างประเทศและในประเทศไทย ดังนั้น หากโครงสร้างดังกล่าวมีการแบ่งแยกหน้าที่ระหว่าง (1) ปฏิบัติงานด้าน IT (2) บริหารความเสี่ยงด้าน IT

ข้อ	ประเด็นคำถาม	แนวคำตอบ
	ปฏิบัติงานด้าน IT ที่อยู่ในประเทศไทยเป็นส่วนหนึ่งของ 1st line ของธนาคารพาณิชย์แม่ที่อยู่ในต่างประเทศนั้น การมีโครงสร้างในลักษณะดังกล่าว ถือว่าสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ มีโครงสร้างตามที่ธนาคารแห่งประเทศไทยกำหนดแล้วหรือไม่	และ (3) ตรวจสอบด้าน IT และมีคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้าน IT ตามหลักเกณฑ์ที่กำหนดในข้อ 5.3.1 (2.1) และ (2.2) ก็ถือว่าสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศนั้นมีการจัดโครงสร้างที่สอดคล้องกับหลักเกณฑ์ของธนาคารแห่งประเทศไทยแล้ว
5.	ในกรณีของสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ (subsidiary) ซึ่งปัจจุบันมีการใช้นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ที่กำหนดโดยธนาคารพาณิชย์แม่ที่อยู่ในต่างประเทศ สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศยังจำเป็นต้องมีนโยบายในเรื่องดังกล่าวที่ได้รับอนุมัติจากคณะผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบที่เกี่ยวข้องกับสาขาของธนาคารพาณิชย์ต่างประเทศนั้นหรือคณะกรรมการของธนาคารพาณิชย์ที่เป็นบริษัทลูกอีกหรือไม่	สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศสามารถนำนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ที่สำนักงานใหญ่หรือธนาคารพาณิชย์แม่ที่อยู่ในต่างประเทศกำหนดมาปรับใช้ได้ โดยต้องมั่นใจว่านโยบายดังกล่าวครอบคลุมตามหลักเกณฑ์ที่ธนาคารแห่งประเทศไทยกำหนด ทั้งนี้ คณะผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบที่เกี่ยวข้องของสาขาของธนาคารพาณิชย์ต่างประเทศนั้นหรือคณะกรรมการของธนาคารพาณิชย์ที่เป็นบริษัทลูกต้องอนุมัตินโยบายดังกล่าวด้วย
การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)		
6.	การกำหนดกระบวนการจัดการการเข้าถึงข้อมูลสามารถทำได้โดยหน่วยงานที่ปฏิบัติงานด้าน IT (IT operation) หรือจำเป็นต้องแยกเป็นหน่วยงานอิสระอีกหน่วยงานหนึ่งออกจากหน่วยงานที่ปฏิบัติงานด้าน IT	สถาบันการเงินสามารถกำหนดโครงสร้างของหน่วยงานที่ทำหน้าที่จัดการการเข้าถึงข้อมูลได้เองโดยธนาคารแห่งประเทศไทยไม่ได้กำหนดให้ต้องอยู่ในความรับผิดชอบของหน่วยงานใดเป็นการเฉพาะ ซึ่งให้ขึ้นอยู่กับการจัดสรรงานของสถาบันการเงินแต่ละแห่งและเป็นไปตามหลักการแบ่งแยกหน้าที่ที่ดี
7.	ในกรณีธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ ซึ่งมีการใช้ระบบ core banking และระบบที่เกี่ยวข้องจากธนาคารพาณิชย์แม่ที่อยู่ในต่างประเทศนั้น ธนาคารพาณิชย์ที่เป็นบริษัทลูกสามารถใช้ผลการทดสอบเจาะระบบของธนาคารพาณิชย์แม่ที่อยู่ในต่างประเทศ ได้หรือไม่	ธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศสามารถใช้ผลการทดสอบของธนาคารพาณิชย์แม่ที่อยู่ในต่างประเทศได้ โดยผลการทดสอบต้องครอบคลุมระบบงานสำคัญที่ธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศใช้งานอยู่ทั้งหมด
8.	ในกรณีที่สถาบันการเงินมีศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองอยู่หนึ่งแห่งแล้ว จำเป็นหรือไม่ที่ต้องมีศูนย์คอมพิวเตอร์สำรองแห่งที่สอง	สถาบันการเงินต้องกำหนดนโยบายในการจัดตั้งศูนย์คอมพิวเตอร์สำรอง โดยควรคำนึงถึงความจำเป็น ความเสี่ยง และความเหมาะสมในการจัดตั้งศูนย์คอมพิวเตอร์สำรองแห่งที่สอง

ข้อ	ประเด็นคำถาม	แนวคำตอบ
9.	**ในกรณีที่สถาบันการเงินมีนโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) ที่ครอบคลุมถึงการจัดทำแผนฉุกเฉินด้าน IT และได้รับความเห็นชอบจากคณะกรรมการที่ได้รับมอบหมายแล้ว สถาบันการเงินสามารถใช้นโยบาย BCM ดังกล่าวแทนการจัดทำแผนฉุกเฉินด้าน IT ที่กำหนดอยู่ในประกาศข้อ 5.3.2 (9) ได้หรือไม่** **(เพิ่มเติมเมื่อ 27 กุมภาพันธ์ 2562)**	**สถาบันการเงินสามารถใช้นโยบาย BCM ของสถาบันการเงิน แทนการจัดทำแผนฉุกเฉินด้าน IT ได้ หากนโยบาย BCM ดังกล่าว ครอบคลุมถึงการจัดทำแผนฉุกเฉินด้าน IT ซึ่งมีวัตถุประสงค์เพื่อให้สถาบันการเงินมีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจดำเนินการต่อไปได้อย่างต่อเนื่อง และสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้**
การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)		
10.	งานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับ IT (IT compliance) ต้องแยกออกจากหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์อื่น ๆ (compliance) หรือไม่ และผู้ที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับ IT ต้องมีคุณสมบัติอย่างไร	ผู้ที่ทำหน้าที่ IT compliance อาจอยู่ในหน่วยงานหรือทีมงานที่อยู่ในฝ่ายกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์อื่น ๆ ที่ปัจจุบันมีอยู่แล้วได้ โดยผู้ที่ทำหน้าที่นี้ ต้องเป็นผู้ที่มีความรู้และเข้าใจในกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องกับการใช้เทคโนโลยีของสถาบันการเงิน
11.	สาขาของธนาคารพาณิชย์ต่างประเทศ หรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ สามารถใช้หน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับ IT (IT compliance) ของธนาคารพาณิชย์แม่ในต่างประเทศ ได้หรือไม่ หรือต้องจัดตั้งหน่วยงานหรือทีมงานขึ้นใหม่ในประเทศไทยโดยเฉพาะ	สาขาของธนาคารพาณิชย์ต่างประเทศ หรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ สามารถใช้หน่วยงาน IT compliance ของสำนักงานใหญ่หรือธนาคารพาณิชย์แม่ในต่างประเทศได้ ทั้งนี้ หน่วยงาน IT compliance ของสำนักงานใหญ่หรือธนาคารพาณิชย์แม่ในต่างประเทศ ต้องมีความรู้และเข้าใจในกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องกับการใช้เทคโนโลยีของสถาบันการเงินของประเทศไทย ซึ่งอาจมีความแตกต่างจากกฎหมายหรือหลักเกณฑ์ที่กำกับดูแลสำนักงานใหญ่หรือธนาคารพาณิชย์แม่ที่อยู่ในต่างประเทศ
การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)		
12.	หน่วยงานใดของสถาบันการเงินต้องทำหน้าที่ดำเนินการจ้างผู้เชี่ยวชาญภายนอกที่จะทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่มีความสำคัญตามประกาศกำหนด	ธนาคารแห่งประเทศไทยไม่ได้กำหนดหน่วยงานที่ทำหน้าที่ดำเนินการจ้างผู้เชี่ยวชาญภายนอก ทั้งนี้ สถาบันการเงินต้องกำหนดนโยบายในเรื่องการจัดจ้างผู้เชี่ยวชาญภายนอกดังกล่าว โดยนโยบายนั้นต้องสอดคล้องกับนโยบายอื่นที่เกี่ยวข้องของสถาบันการเงิน

ข้อ	ประเด็นคำถาม	แนวคำตอบ
13.	ตามที่ธนาคารแห่งประเทศไทยได้มีการสื่อสารในการจัดประชุมชี้แจงร่างประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน (ประกาศ IT Risk) เมื่อวันที่ 23 สิงหาคม 2560 ซึ่งเนื้อหาส่วนหนึ่งได้สื่อสารถึงการยกเลิกประกาศธนาคารแห่งประเทศไทย ที่ สนส. 26/2551 เรื่อง การอนุญาตให้ธนาคารพาณิชย์ให้บริการการเงินทางอิเล็กทรอนิกส์ หลังจากประกาศ IT Risk บังคับใช้นั้น หมายความว่าธนาคารพาณิชย์สามารถเตรียมความพร้อมเพื่อปฏิบัติตามประกาศ IT Risk โดยไม่ต้องทำการตรวจสอบระบบการให้บริการโอนเงินทางอิเล็กทรอนิกส์โดยผู้ตรวจสอบบัญชีภายนอกในรอบปี 2560 และในช่วงเดือนมกราคม – มีนาคม 2561 ตามประกาศธนาคารแห่งประเทศไทย ที่ สนส. 26/2551 ได้หรือไม่ (เพิ่มเติมเมื่อ 30 เมษายน 2561)	ธนาคารแห่งประเทศไทยพิจารณาผ่อนผันให้ธนาคารพาณิชย์สามารถดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit) ตามหลักเกณฑ์ที่ระบุในประกาศ IT Risk แทนการตรวจสอบระบบการให้บริการโอนเงินทางอิเล็กทรอนิกส์ตามประกาศธนาคารแห่งประเทศไทย ที่ สนส. 26/2551 ในช่วงปี 2560 – มีนาคม 2561 เนื่องจากธนาคารพาณิชย์ได้รับทราบเกี่ยวกับการยกเลิกประกาศธนาคารแห่งประเทศไทย ที่ สนส. 26/2551 และดำเนินการเตรียมความพร้อมที่จะมีการปฏิบัติตามประกาศ IT Risk ฉบับใหม่แทน (ซึ่งประกาศ IT Risk ไม่ได้มีการกำหนดเป็นการเฉพาะให้ตรวจสอบระบบการให้บริการโอนเงินทางอิเล็กทรอนิกส์โดยผู้ตรวจสอบบัญชีภายนอก แต่กำหนดให้ธนาคารพาณิชย์ต้องจัดให้มีแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงของการใช้เทคโนโลยีสารสนเทศของธนาคารพาณิชย์ โดยใช้ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระ) อีกทั้งเพื่อเป็นการลดภาระและค่าใช้จ่ายของธนาคารพาณิชย์ ในการตรวจสอบระบบการให้บริการโอนเงินดังกล่าว
14.	**ตามที่กำหนดให้สถาบันการเงินต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง (ตามประกาศข้อ 5.3.5 (3)) นั้น หากสถาบันการเงินมีการจัดทำแผนและขอบเขตการตรวจสอบด้าน IT จากการประเมินความเสี่ยงและความสำคัญของการใช้เทคโนโลยี ทำให้มีงานด้าน IT บางเรื่องที่มีรอบระยะเวลาการตรวจสอบเกินกว่า 1 ปี จึงขอทราบว่าสถาบันการเงินสามารถตรวจสอบตามแผนและรอบเวลาดังกล่าวได้หรือไม่** **(เพิ่มเติมเมื่อ 27 กุมภาพันธ์ 2562)**	**สถาบันการเงินสามารถจัดให้มีการตรวจสอบตามแผนดังกล่าวได้ หากสถาบันการเงินมีการประเมินความสำคัญและความเสี่ยงของการใช้เทคโนโลยีสารสนเทศเพื่อกำหนดแผนงานและขอบเขตการตรวจสอบ และแผนงานและขอบเขตการตรวจสอบดังกล่าวได้รับความเห็นชอบจากคณะกรรมการตรวจสอบแล้ว (ตามประกาศข้อ 5.3.5 (2)) โดยขอให้สถาบันการเงินจัดเก็บผลการประเมินและเหตุผลประกอบการประเมินเพื่อให้ธนาคารแห่งประเทศไทยสามารถตรวจสอบได้**

ข้อ	ประเด็นคำถาม	แนวคำตอบ
การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)		
15.	หน่วยงานหรือทีมงานดูแลภาพรวมของโครงการ (Project Management Office : PMO) สามารถเป็นหน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการที่ครอบคลุมทั้งด้าน IT และ Non IT ได้หรือไม่ และสาขาธนาคารพาณิชย์ต่างประเทศที่อยู่ในประเทศไทยสามารถใช้หน่วยงานหรือทีมงานดูแลภาพรวมของโครงการของสำนักงานใหญ่ประจำภูมิภาค (regional) แทนการจัดตั้งหน่วยงานหรือทีมงานขึ้นใหม่เพื่อทำหน้าที่นี้ได้หรือไม่	PMO สามารถเป็นหน่วยงานหรือทีมงานที่ดูแลภาพรวมทั้งโครงการด้าน IT และ โครงการที่เป็น Non IT ได้ และสามารถใช้ PMO ของสำนักงานใหญ่ประจำภูมิภาค (regional) ได้ โดยไม่ต้องจัดตั้งหน่วยงานหรือทีมงานขึ้นใหม่เพื่อทำหน้าที่นี้ในประเทศไทย อย่างไรก็ดี PMO ของสำนักงานใหญ่ประจำภูมิภาคต้องติดตามความคืบหน้าและภาพรวมของโครงการด้าน IT ที่สำคัญของสาขาธนาคารพาณิชย์ต่างประเทศที่อยู่ในประเทศไทย และรายงานต่อคณะกรรมการที่ได้รับมอบหมายในการกำกับดูแลโครงการหรือผู้บริการระดับสูงที่เกี่ยวข้องทราบให้ครบถ้วน เพื่อให้โครงการบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้
การขออนุญาตการเปลี่ยนแปลงการใช้เทคโนโลยี		
16.	หากสถาบันการเงินจะนำเทคโนโลยีใหม่มาใช้ซึ่งจะมีผลกระทบอย่างมีนัยสำคัญในการดำเนินธุรกิจ แต่เป็นเทคโนโลยีที่บริษัทในกลุ่มธุรกิจทางการเงินมีการใช้งานอยู่แล้ว สถาบันการเงินจำเป็นต้องขออนุญาตจากธนาคารแห่งประเทศไทยหรือไม่	สถาบันการเงินต้องขออนุญาตจากธนาคารแห่งประเทศไทยตามหลักเกณฑ์กำหนด เนื่องจากธนาคารแห่งประเทศไทยต้องพิจารณาความเสี่ยงและผลกระทบจากการที่สถาบันการเงินนำเทคโนโลยีดังกล่าวมาใช้
17.	การเปลี่ยนแปลงการใช้เทคโนโลยีในลักษณะใดที่ธนาคารแห่งประเทศไทยถือว่ามีนัยสำคัญและต้องยื่นขออนุญาตต่อธนาคารแห่งประเทศไทยตามที่กำหนดในประกาศ	การพิจารณาว่าการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีนัยสำคัญ ให้สถาบันการเงินพิจารณาความเสี่ยงหรือผลกระทบประการใดประการหนึ่งดังต่อไปนี้ (1) ก่อให้เกิดความเสี่ยงและผลกระทบต่อสถาบันการเงินในวงกว้าง (bank wide impact) เช่น การเปลี่ยนแปลงระบบที่ให้บริการแก่ผู้ใช้บริการของสถาบันการเงิน และประชาชนทั่วไปในวงกว้าง (2) ก่อให้เกิดความเสี่ยงและผลกระทบต่อระบบ สถาบันการเงิน หรือธุรกิจอื่นในวงกว้าง (banking system wide impact) เช่น การเปลี่ยนแปลงระบบงานที่เชื่อมต่อกับระบบชำระเงินกลาง ทั้งนี้ หากสถาบันการเงินมีข้อสงสัยเกี่ยวกับการพิจารณาการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจให้สถาบันการเงินหารือมายังฝ่ายกำกับธุรกิจสถาบันการเงิน สายนโยบายสถาบันการเงิน ธนาคารแห่งประเทศไทยก่อนดำเนินการ

ธนาคารแห่งประเทศไทย

IT Risk Management Implementation Guideline

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ

สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

สารบัญ

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

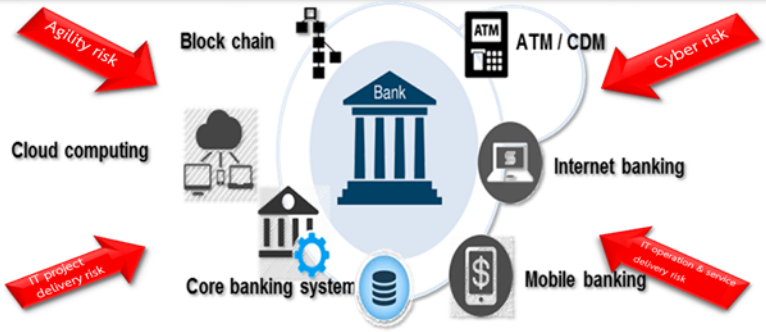
ประกาศ ธปท. ที่ สนส. 19/2559	ประกาศ ธปท. ที่ สนส. 19/2560	แนวปฏิบัติที่เกี่ยวข้อง
เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของ สง.	เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)	➢ แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ➢ 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