Consultation Paper

หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

ธนาคารแห่งประเทศไทย จัดทำ Consultation Paper ฉบับนี้ เพื่อรับฟังความเห็นต่อหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน โดยมีวัตถุประสงค์เพื่อให้สถาบันการเงินมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ สามารถนำเสนอผลิตภัณฑ์และให้บริการได้ตามความต้องการของตลาดหรือลูกค้าได้เร็วขึ้น (time to market) รองรับรูปแบบทางธุรกิจและสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

จึงขอเชิญชวนร่วมแสดงความคิดเห็นต่อหลักเกณฑ์ดังกล่าว โดยสามารถดาวน์โหลดและส่งแบบแสดงความคิดเห็นมายังทีมนโยบายการปฏิบัติการสถาบันการเงิน ฝ่ายนโยบายการกำกับสถาบันการเงิน สายนโยบายสถาบันการเงิน ธนาคารแห่งประเทศไทย ทางอีเมล : BOPTeam@bot.or.th ภายในวันศุกร์ที่ 17 พฤษภาคม 2562

คณะผู้จัดทำ
พฤษภาคม 2562

สารบัญ

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

---

1. เหตุผลในการออกประกาศ

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) มีความสำคัญต่อการดำเนินธุรกิจเพื่อรองรับการให้บริการทางการเงินและเพื่อสนับสนุนการดำเนินธุรกิจของสถาบันการเงิน ซึ่งการนำเทคโนโลยีมาใช้มากขึ้นก็อาจก่อให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk : IT risk) ที่เพิ่มมากขึ้นด้วย โดยที่ผ่านมาธนาคารแห่งประเทศไทยได้มีการออกหลักเกณฑ์เพื่อกำกับดูแลความเสี่ยงจากการที่สถาบันการเงินนำเทคโนโลยีมาใช้ และกรณีที่สถาบันการเงินใช้บริการจากผู้ให้บริการภายนอก ได้แก่ ประกาศธนาคารแห่งประเทศไทยว่าด้วยการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) และประกาศธนาคารแห่งประเทศไทยว่าด้วยการใช้บริการจากผู้ใช้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน โดยหลักเกณฑ์ข้างต้นอยู่ภายใต้กรอบหลักการด้านเทคโนโลยีที่สำคัญ 3 ประการ คือ (1) การรักษาความลับของระบบและข้อมูล (confidentiality) (2) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ (3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) อีกทั้ง สถาบันการเงินต้องให้ความสำคัญกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงิน (Enterprise Risk Management : ERM)

จากการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีซึ่งมีผลต่อการปรับตัวของสถาบันการเงิน ทั้งรูปแบบการประกอบธุรกิจและการควบคุมดูแลการนำเทคโนโลยีมาใช้ รวมถึงการใช้บริการเทคโนโลยีจากบุคคลภายนอกที่นอกเหนือจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT service provider) เช่น การให้บริการของสถาบันการเงินที่มีการเชื่อมต่อระบบงานกับพันธมิตรทางธุรกิจ ดังนั้น ธนาคารแห่งประเทศไทยจึงเห็นความจำเป็นในการปรับปรุงหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้รองรับรูปแบบทางธุรกิจและสอดคล้องกับนวัตกรรมทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว ซึ่งรวมถึงการให้สถาบันการเงินมีข้อกำหนด (criteria) ที่ชัดเจนในการพิจารณาความมีนัยสำคัญของการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ทั้งกรณีสถาบันการเงินดำเนินการเองหรือใช้บริการจากบุคคลภายนอก ภายใต้กรอบหลักการที่คำนึงถึงความเสี่ยงและผลกระทบต่อการดำเนินธุรกิจของสถาบันการเงินในวงกว้าง (bank wide impact) และผลกระทบต่อระบบสถาบันการเงินในวงกว้าง (banking system wide impact) เพื่อให้สถาบันการเงินมีการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ และสามารถนำเสนอผลิตภัณฑ์และให้บริการได้ตามความต้องการของตลาดหรือลูกค้าได้เร็วขึ้น (time to market) โดยหลักเกณฑ์ดังกล่าวมีสาระสำคัญที่ปรับปรุง ดังนี้

(1) ให้สถาบันการเงินกำกับดูแลความเสี่ยงด้วยตนเอง (self-regulated) โดยให้พิจารณาความมีนัยสำคัญของการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงเทคโนโลยี ภายใต้กรอบหลักการที่คำนึงถึงผลกระทบต่อการดำเนินธุรกิจของสถาบันการเงินในวงกว้าง (bank wide impact) และผลกระทบต่อระบบสถาบันการเงินในวงกว้าง (banking system wide impact) พร้อมทั้งยกเลิกการขออนุญาตต่อธนาคารแห่งประเทศไทยสำหรับกรณีของธนาคารพาณิชย์ที่มีการนำเทคโนโลยีมาใช้หรือมีการเปลี่ยนแปลงเทคโนโลยีที่มีนัยสำคัญ โดยให้มีการรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญประจำปีให้ธนาคารแห่งประเทศไทยทราบแทน และแจ้งธนาคารแห่งประเทศไทยก่อนการใช้หรือการเปลี่ยนแปลงเทคโนโลยีที่มีนัยสำคัญ เพื่อให้ธนาคารแห่งประเทศไทยติดตามภาพรวมของการใช้เทคโนโลยีสารสนเทศและติดตามตรวจสอบสถาบันการเงินได้อย่างต่อเนื่อง

(2) ยกระดับการดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยกำหนดให้ธนาคารพาณิชย์ที่มีนัยต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks: D-SIBs) หรือสถาบันการเงินที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ต้องมีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO)

(3) รวมการกำกับดูแลผู้ใช้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศในการประกอบธุรกิจ (IT outsourcing) ให้อยู่ภายใต้หลักเกณฑ์ฉบับนี้ โดยธนาคารแห่งประเทศไทยจะกำหนดแนวปฏิบัติเรื่องการบริหารจัดการบุคคลภายนอก (Third Party Management Implementation Guideline) ให้สถาบันการเงินใช้เป็นแนวทางในการปฏิบัติ เพื่อเพิ่มความชัดเจน และครอบคลุมการดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เชื่อมโยงกับบุคคลภายนอกที่มีความหลากหลายด้วย เช่น พันธมิตรทางธุรกิจ

(4) เพิ่มความยืดหยุ่นในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินที่มีข้อจำกัดด้านโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สามารถปรับใช้หลักเกณฑ์ในส่วนที่เกี่ยวข้องให้สอดคล้องกับระดับความเสี่ยงได้

2. อำนาจตามกฎหมาย

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

3. ประกาศที่ยกเลิก

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

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

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

5. เนื้อหา

5.1 คำจำกัดความ

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

“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (Information Technology risk- IT risk) หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของสถาบันการเงิน รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threat)

“คณะกรรมการสถาบันการเงิน” หมายความว่า คณะกรรมการสถาบันการเงินที่จดทะเบียนในประเทศไทย หรือคณะผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบที่เกี่ยวข้องของสาขาของธนาคารพาณิชย์ต่างประเทศ

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอกที่ให้บริการด้านเทคโนโลยีสารสนเทศ หรือที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หรือที่สามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยสถาบันการเงินได้

“บริษัทในกลุ่มธุรกิจเดียวกัน” หมายความว่า บริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับแบบรวมกลุ่ม

“บริษัทที่มีความเกี่ยวข้อง” หมายความว่า บริษัทแม่ บริษัทลูก และบริษัทร่วมของสถาบันการเงิน

5.2 หลักการ

สถาบันการเงินมีหน้าที่เกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) ดังนี้

5.2.1 ดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) รวมถึงโครงการด้านเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพและรัดกุม ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ (1) การรักษาความลับของระบบและข้อมูล (confidentiality) (2) ความ

ถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ (3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) โดยอยู่บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า

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

5.2.3 ควรมีโครงสร้างการกำกับดูแลในภาพรวมที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence) โดยในกรณีที่สถาบันการเงินมีการใช้การบริหารจัดการ หรือการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศจากบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง โดยเฉพาะกรณีสาขาของธนาคารพาณิชย์ต่างประเทศ และธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ ซึ่งช่วยให้สถาบันการเงินสามารถดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศได้มีประสิทธิภาพมากขึ้น อย่างไรก็ดี สถาบันการเงินและคณะกรรมการสถาบันการเงินหรือผู้บริหารระดับสูงของสถาบันการเงินในประเทศไทยยังคงต้องรับผิดชอบต่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเสมือนสถาบันการเงินดำเนินการเอง

5.3 หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.3.1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)

(1) บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการสถาบันการเงิน

คณะกรรมการสถาบันการเงินต้องรู้เท่าทันและเข้าใจถึงความเสี่ยงในการนำเทคโนโลยีสารสนเทศมาใช้ดำเนินธุรกิจ มีบทบาทหน้าที่และความรับผิดชอบกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดรับกับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สถาบันการเงินมีอย่างน้อยครอบคลุมดังนี้

(1.1) ดูแลให้การใช้เทคโนโลยีของสถาบันการเงินสอดรับกับกลยุทธ์การดำเนินธุรกิจ และมีความยืดหยุ่นเพียงพอรองรับการเปลี่ยนแปลงต่าง ๆ ในอนาคต

(1.2) ดูแลให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นหนึ่งในความเสี่ยงสำคัญขององค์กร (enterprise wide risk) และมีนโยบายและการบริหารจัดความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งด้านความปลอดภัย ด้านความถูกต้อง และด้านความพร้อมใช้ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ทั้งในภาวะปกติและภาวะวิกฤต รวมทั้งดูแลความเสี่ยงโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญด้วย

(1.3) ดูแลให้มีการสร้างความรู้และความตระหนักรู้เรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่กรรมการ ผู้บริหาร และพนักงานในองค์กรอย่างต่อเนื่องและมีประสิทธิผล

คณะกรรมการสถาบันการเงินอาจมอบหมายให้คณะกรรมการชุดอื่นหรือผู้บริหารระดับสูงทำหน้าที่ที่เกี่ยวข้องในการกำกับดูแลได้ แต่คณะกรรมการสถาบันการเงินยังคงต้องรับผิดชอบในเรื่องดังกล่าว

นอกจากนี้ องค์ประกอบของคณะกรรมการสถาบันการเงินต้องมีกรรมการที่มีความรู้หรือประสบการณ์ด้านการกำกับดูแลเทคโนโลยีสารสนเทศ (IT governance) อย่างน้อย 1 ท่าน ตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์ด้านธรรมาภิบาลของสถาบันการเงิน

(2) โครงสร้างการกำกับดูแล

(2.1) โครงสร้างองค์กร

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

(2.2) คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2.2.1) สถาบันการเงินต้องจัดให้มีคณะกรรมการที่ทำหน้าที่บริหารจัดการ รวมถึงกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee

(2.2.2) สถาบันการเงินต้องจัดให้มีคณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

(2.2.3) สถาบันการเงินต้องจัดให้มีคณะกรรมการที่ทำหน้าที่กำกับดูแลให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งการตรวจสอบครอบคลุมถึงการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลให้มีการสอบทานการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

(2.3) ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

สถาบันการเงินควรจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) ของสถาบันการเงิน ซึ่งเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือกับภัยคุกคามทางไซเบอร์ โดยการทำหน้าที่ควรมีความเป็นอิสระจากหน้าที่งานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) ซึ่งผู้บริหารดังกล่าวควรมีบทบาทหน้าที่และความรับผิดชอบให้สถาบันการเงินมีการดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อย ดังนี้

– จัดให้มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ และดูแลให้มีการปฏิบัติตามที่กำหนด

– จัดให้มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)

– บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์

– ดำเนินการให้สถาบันการเงินมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ ตามมาตรฐานสากลและแนวทางของ ธนาคารแห่งประเทศไทย

– ดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์

ทั้งนี้ ธนาคารพาณิชย์ที่มีนัยต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks: D-SIBs) หรือสถาบันการเงินที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) ภายใน 1 ปีนับจากวันที่เข้าเงื่อนไขดังกล่าว ซึ่งควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (authority) เพียงพอ ในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยมีอำนาจหน้าที่อย่างน้อย ดังนี้

– รายงานเหตุการณ์และความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญ ต่อผู้บริหารในตำแหน่งสูงสุดและคณะกรรมการสถาบันการเงินได้

– เป็นสมาชิกในคณะกรรมการที่ทำหน้าที่บริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee และคณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

– ร่วมตัดสินใจดำเนินการในเรื่องที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญของสถาบันการเงิน

(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) ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของบุคลากรควรระบุในเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินอย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

(3.3) 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) ความถูกต้องเชื่อถือได้

ของระบบและข้อมูล (integrity) และ (3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) โดยนโยบายดังกล่าวต้องสอดคล้องกับกลยุทธ์ของสถาบันการเงินในการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจและนโยบายการบริหารความเสี่ยงของสถาบันการเงิน รวมทั้งสอดคล้องกับแนวทางการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

นอกจากนี้ การกำหนดนโยบายดังกล่าวต้องคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศภายในองค์กรและความเสี่ยงจากการใช้บริการจาก **บุคคลภายนอก**ด้วย

(5.2) สถาบันการเงินต้องจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.3.2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

เพื่อให้สถาบันการเงินมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ สถาบันการเงินต้องนำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

สถาบันการเงินต้องจัดให้มีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องมีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ**ที่สำคัญ**ได้อย่างครบถ้วน และสามารถนำไปใช้ในการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงต้องจัดให้มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

(2) การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

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

(3) การควบคุมการเข้าถึง (access control)

สถาบันการเงินต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงานและระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้

ตามความจำเป็นในการใช้งานและระดับความเสี่ยง 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 และรายงานเหตุการณ์ผิดปกติ ปัญหา และการแก้ไข ให้คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ในระยะเวลาที่เหมาะสม นอกจากนี้ สถาบันการเงินต้องมีการวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

(9) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

(9.1) สถาบันการเงินต้องจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำ**นโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ**และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรให้เป็นไปตามนโยบายที่กำหนดไว้ และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศดังกล่าวต้องได้รับอนุมัติโดย**คณะกรรมการที่ได้รับมอบหมาย**

(9.2) ในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ สถาบันการเงินต้องคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของสถาบันการเงิน รวมทั้งการบริหารความเสี่ยงที่อาจเกิดจากเหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงทั่วไป เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) และความเสี่ยงอื่นที่เกี่ยวข้อง เช่น ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ (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) การบริหารจัดการบุคคลภายนอก (third party management)

ในกรณีที่สถาบันการเงินมีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) หรือบุคคลภายนอกมีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงินหรือเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือของลูกค้าของสถาบันการเงินได้ เช่น การใช้บริการด้านงานเทคโนโลยีสารสนเทศจาก IT service provider การใช้บริการ cloud computing การเชื่อมต่อระบบเทคโนโลยีสารสนเทศเพื่อร่วมให้บริการกับพันธมิตรทางธุรกิจ การเชื่อมต่อกับผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP) หรือผู้ให้บริการระบบชำระเงินกลาง ให้สถาบันการเงินนำแนวปฏิบัติการบริหารจัดการบุคคลภายนอก (Third Party Management Implementation Guideline) มาปฏิบัติให้เหมาะสมเพียงพอกับระดับความเสี่ยงและระดับความมีนัยสำคัญของการเชื่อมโยงหรือการใช้บริการจากบุคคลภายนอก โดยมีหลักการสำคัญที่สถาบันการเงินต้องบริหารจัดการบุคคลภายนอก ดังนี้

(10.1) ต้องกำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างสถาบันการเงินและบุคคลภายนอกอย่างชัดแจน

(10.2) ต้องกำกับดูแลและบริหารจัดการความเสี่ยงจากการใช้บริการจากบุคคลภายนอกที่สอดคล้องกับระดับความสำคัญของงานที่ใช้บริการและระดับความเสี่ยงจากการใช้บริการจากบุคคลภายนอกให้อยู่ภายใต้ระดับความเสี่ยง

(10.3) ต้องติดตามดูแลประสิทธิภาพของการให้บริการจากบุคคลภายนอกให้เป็นไปตามสัญญาหรือข้อตกลง

(10.4) ต้องดูแลให้มั่นใจว่าการใช้บริการจากบุคคลภายนอกมีการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security) ที่สอดคล้องกับมาตรฐานการการรักษาความมั่นคงปลอดภัยสารสนเทศของสถาบันการเงินและอ้างอิงมาตรฐานสากลที่ยอมรับโดยทั่วไปภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และ ความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (Availability) ซึ่งรวมถึงการคุ้มครองข้อมูลส่วนบุคคล (data privacy)

(10.5) ต้องเตรียมความพร้อมรับมือต่อปัญหาหรือการเปลี่ยนแปลงที่อาจเกิดขึ้น และความพร้อมในการดำเนินธุรกิจอย่างต่อเนื่อง

5.3.3 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

เพื่อให้สถาบันการเงินสามารถบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ**และต่อเนื่อง** 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)

สถาบันการเงินต้องมีการ**รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ**

ทั้งนี้ สถาบันการเงินต้องจัดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.3.4 การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

สถาบันการเงินต้องจัดให้มีการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยระบบการชำระเงิน เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง **โดยผู้ที่ทำหน้าที่เกี่ยวกับการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) สามารถอยู่ในฝ่ายกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ (compliance) ได้**

5.3.5 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

(1) สถาบันการเงินต้องจัดให้มีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2) สถาบันการเงินต้องจัดให้มีแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงของการใช้เทคโนโลยีสารสนเทศของสถาบันการเงิน และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบดังกล่าวต้องได้รับ**การอนุมัติ**จากคณะกรรมการตรวจสอบ และต้องครอบคลุมถึงเทคโนโลยีสารสนเทศที่สำคัญของสถาบันการเงิน ทั้งนี้ สถาบันการเงินต้องจัดให้มีการทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าว**โดยคณะกรรมการตรวจสอบ**อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

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

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

(5) สถาบันการเงินต้องจัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและเสนอต่อคณะกรรมการตรวจสอบ ตลอดจนจัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่สถาบันการเงิน พร้อมไว้สำหรับการตรวจสอบหรือเมื่อร้องขอโดยธนาคารแห่งประเทศไทย

(6) สถาบันการเงินต้องจัดให้มีการติดตามประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานประเด็นสำคัญให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้อง

5.3.6 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

(1) สถาบันการเงินต้องจัดให้มีการศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับของโครงการที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องมีการพิจารณาเลือกใช้เทคโนโลยีอย่างเหมาะสม และมีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งต้องมีการจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตอำนาจในการอนุมัติที่กำหนดไว้

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

(2.1) คณะกรรมการ**ที่ทำหน้าที่**กำกับดูแลโครงการ เพื่อทำหน้าที่ในการกำกับดูแลความคืบหน้า ให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้การดำเนินงานของโครงการเป็นไปตามแผนงานที่กำหนด ทั้งนี้ คณะกรรมการกำกับดูแลโครงการควรประกอบด้วยผู้บริหารหรือผู้แทนจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้อง

(2.2) หน่วยงานหรือทีมงานดูแลภาพรวมของโครงการ (Project Management Office : PMO) เพื่อทำหน้าที่ในการกำหนดรูปแบบ กระบวนการ และเครื่องมือที่เป็นมาตรฐานในการบริหารจัดการและติดตามความคืบหน้าของโครงการ รวมทั้งรายงานความคืบหน้าและภาพรวมของโครงการที่สำคัญของสถาบันการเงินต่อคณะกรรมการที่ได้รับมอบหมายในการกำกับดูแลโครงการ หรือผู้บริหารระดับสูง**ที่อนุมัติโครงการดังกล่าว** เพื่อให้โครงการบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้

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

5.4 การนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยี

ในกรณีที่มีการนำเทคโนโลยีมาใช้ หรือมีการเปลี่ยนแปลงระบบหรือเทคโนโลยี ทั้งกรณีสถาบันการเงินดำเนินการเองหรือใช้บริการจากบุคคลภายนอก สถาบันการเงินจะต้องมีการพิจารณาความมีนัยสำคัญก่อนดำเนินการ โดยสถาบันการเงินจะต้องมีข้อกำหนด (criteria) ในการพิจารณาความมีนัยสำคัญที่ชัดเจน ภายใต้กรอบหลักการที่คำนึงถึงความเสี่ยงและผลกระทบ

ต่อการดำเนินธุรกิจของสถาบันการเงินในวงกว้าง (bank wide impact) และผลกระทบต่อระบบสถาบันการเงินในวงกว้าง (banking system wide impact) เช่น กระทบลูกค้าส่วนใหญ่ของสถาบันการเงิน หรือกระทบต่อระบบงานกลาง ทั้งนี้ สถาบันการเงินต้องมีการพิจารณา รวมทั้งการสื่อสาร ติดตาม และทบทวนข้อกำหนด โดยประกอบไปด้วยขั้นตอนอย่างน้อย ดังนี้

5.4.1 ข้อกำหนดต้องผ่านการพิจารณาร่วมกันของหน่วยงานที่เกี่ยวข้อง โดยเฉพาะหน่วยงานปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (first line of defense) หน่วยงานบริหารความเสี่ยงและกำกับภายในด้านเทคโนโลยีสารสนเทศ (second line of defense)

5.4.2 ข้อกำหนดต้องได้รับการอนุมัติโดยคณะกรรมการที่ได้รับมอบหมาย

5.4.3 ข้อกำหนดต้องได้รับการสื่อสารและเผยแพร่ให้หน่วยงานที่เกี่ยวข้องทราบโดยทั่วกัน

5.4.4 ต้องมีการสอบทานการดำเนินการตามข้อกำหนดอย่างน้อยปีละ 1 ครั้ง

5.4.5 ข้อกำหนดต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบของสถาบันการเงิน

ทั้งนี้ สถาบันการเงินต้องมีการบริหารความเสี่ยงให้เหมาะสมตามระดับความมีนัยสำคัญของการนำเทคโนโลยีมาใช้ หรือมีการเปลี่ยนแปลงระบบหรือเทคโนโลยี ทั้งกรณีสถาบันการเงินดำเนินการเองหรือใช้บริการจากบุคคลภายนอก

5.5 การรายงาน แจ้ง หรือขออนุญาตต่อธนาคารแห่งประเทศไทย

5.5.1 กรณีธนาคารพาณิชย์

(1) การรายงานโครงการด้านเทคโนโลยีที่มีนัยสำคัญประจำปี

ธนาคารพาณิชย์จะต้องจัดส่งรายงานโครงการด้านเทคโนโลยีที่มีนัยสำคัญประจำปี ทั้งกรณีธนาคารพาณิชย์ดำเนินการเองหรือใช้บริการจากบุคคลภายนอก ต่อธนาคารแห่งประเทศไทยตามแบบรายงานที่สามารถดาวน์โหลดได้จากเว็บไซต์ของธนาคารแห่งประเทศไทย ภายในวันที่ 31 มกราคมของทุกปี โดยให้ธนาคารพาณิชย์ปรับปรุงข้อมูลรายงานโครงการด้านเทคโนโลยีที่มีนัยสำคัญประจำปีให้ธนาคารแห่งประเทศไทยทราบเป็นรายไตรมาส และจัดส่งภายใน 15 วันหลังสิ้นไตรมาส

(2) การแจ้งการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่มีความเสี่ยงหรือผลกระทบอย่างมีนัยสำคัญ

ธนาคารพาณิชย์ที่มีการนำเทคโนโลยีมาใช้ หรือมีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่มีนัยสำคัญ ทั้งกรณีธนาคารพาณิชย์ดำเนินการเองหรือใช้บริการจากบุคคลภายนอก ให้รายงานการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีนัยสำคัญ ต่อธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชนให้ทราบล่วงหน้า 15 วันก่อนดำเนินการ

5.5.2 กรณีบริษัทเงินทุน บริษัทเครดิตฟองซิเอร์

บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ที่มีการนำเทคโนโลยีมาใช้ หรือมีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่มีนัยสำคัญ ทั้งกรณีบริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ดำเนินการเองหรือใช้บริการจากบุคคลภายนอก ให้ยื่นขออนุญาตการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยีที่มีนัยสำคัญ ต่อธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชน รวมถึงเอกสารที่เกี่ยวข้องอื่นใดที่ธนาคารแห่งประเทศไทยอาจร้องขอเพิ่มเติม เพื่อขออนุญาตก่อนดำเนินการ โดยธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการนับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน

5.6 การรายงานปัญหาด้านเทคโนโลยีสารสนเทศต่อธนาคารแห่งประเทศไทย

สถาบันการเงินต้องรายงานต่อธนาคารแห่งประเทศไทยในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียงของสถาบันการเงิน รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของสถาบันการเงินถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่สถาบันการเงินต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงิน โดยให้สถาบันการเงินรายงานปัญหาหรือเหตุการณ์ดังกล่าวมายังธนาคารแห่งประเทศไทย ทันทีเมื่อเกิดหรือรับรู้ปัญหาหรือเหตุการณ์นั้น และให้สถาบันการเงินแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

5.7 การใช้บริการจากบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินควรมีโครงสร้างการกำกับดูแลในภาพรวมที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence) ตามหลักเกณฑ์ที่กำหนดในข้อ 5.3.1 โดยในกรณีที่สถาบันการเงินมีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศจากบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง โดยเฉพาะกรณีสาขาของธนาคารพาณิชย์ต่างประเทศและธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ ซึ่งช่วยให้สถาบันการเงินสามารถดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศได้มีประสิทธิภาพมากขึ้น โดยให้สถาบันการเงินแจ้งการใช้บริการจากบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชน

ทั้งนี้ สถาบันการเงินและคณะกรรมการสถาบันการเงินหรือผู้บริหารระดับสูงของสถาบันการเงินในประเทศไทยยังคงต้องรับผิดชอบต่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเสมือนว่าสถาบันการเงินดำเนินการเอง

5.8 การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

ในกรณีที่สถาบันการเงินใดไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดตามประกาศฉบับนี้ได้ ให้สถาบันการเงินยื่นขออนุญาตผ่อนผันการปฏิบัติตามหลักเกณฑ์ดังกล่าวต่อธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชน เป็นรายกรณี พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนในการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการนับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน

5.9 การกำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ เพิกถอน หรือเข้าตรวจสอบ การนำเทคโนโลยีมาใช้ หรือมีการเปลี่ยนแปลงระบบหรือเทคโนโลยี

ธนาคารแห่งประเทศไทยอาจพิจารณากำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ เพิกถอน หรือเข้าตรวจสอบ การนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ทั้งกรณีสถาบันการเงินดำเนินการเองหรือใช้บริการจากบุคคลภายนอก ตามความจำเป็นเป็นรายกรณี รวมทั้งธนาคารแห่งประเทศไทยมีสิทธิ์ในการเข้าตรวจสอบบุคคลภายนอกที่มีนัยสำคัญต่อระบบสถาบันการเงิน หากพบว่าเป็นการดำเนินการที่ส่งผลกระทบต่อประชาชนในวงกว้างหรือความเชื่อมั่นในระบบสถาบันการเงิน

5.10 บทเฉพาะกาล

5.10.1 ให้สถาบันการเงินที่ต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) ตามที่กำหนดในข้อ 5.3.1 (2.3) ดำเนินการให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) ภายใน 1 ปี นับจากวันที่ประกาศฉบับนี้มีผลบังคับใช้

5.10.2 ให้สถาบันการเงินจัดทำข้อกำหนด (criteria) ในการพิจารณาความมีนัยสำคัญที่ชัดเจนตามที่กำหนดในข้อ 5.4 ให้แล้วเสร็จภายในวันที่ 1 มกราคม 2563 โดยในระหว่างที่สถาบันการเงินยังดำเนินการไม่แล้วเสร็จ สถาบันการเงินยังคงต้องพิจารณาความมีนัยสำคัญของการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยีภายใต้กรอบหลักการที่คำนึงถึงผลกระทบต่อการดำเนินธุรกิจของสถาบันการเงินในวงกว้าง (bank wide impact) และผลกระทบต่อระบบสถาบันการเงินในวงกว้าง (banking system wide impact) ตามกรอบหลักการที่กำหนดในข้อ 5.4

5.10.3 ให้ธนาคารพาณิชย์จัดส่งรายงานโครงการด้านเทคโนโลยีที่มีนัยสำคัญประจำปีตามหลักเกณฑ์ที่กำหนดในข้อ 5.5.1 (1) สำหรับปี 2562 ภายใน 30 วันนับจากวันที่ประกาศฉบับนี้มีผลบังคับใช้

6. วันเริ่มต้นบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

หากมีความเห็นหรือข้อเสนอแนะเพิ่มเติมประการใด โปรดส่งความเห็นมายังทีมนโยบายการปฏิบัติการสถาบันการเงิน ฝ่ายนโยบายการกำกับสถาบันการเงิน สายนโยบายสถาบันการเงิน ธนาคารแห่งประเทศไทย ทางอีเมล : BOPTeam@bot.or.th ภายในวันที่ 17 พฤษภาคม 2562