ประกาศธนาคารแห่งประเทศไทย

ที่ สกช. ๕/๒๕๖๖

เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

---

๑. เหตุผลในการออกประกาศ

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

ธนาคารแห่งประเทศไทย (ธปท.) จึงเห็นควรปรับปรุงหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) ให้เท่าทันกับความเสี่ยงและรูปแบบการปฏิบัติงานที่เปลี่ยนแปลงไป เพื่อให้มีความยืดหยุ่น คล่องตัว เพิ่มความชัดเจน ลดภาระในการปฏิบัติตามประกาศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ โดยได้รวมหลักเกณฑ์ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจไว้ในประกาศฉบับเดียวกัน นอกจากนี้กำหนดเพิ่มเติมให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจทำแบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วยตนเอง (IT risk self-assessment) เป็นประจำทุกปี เพื่อส่งเสริมให้เกิดการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วยตนเอง (self-regulated) ที่เข้มแข็งยิ่งขึ้น รวมทั้งกำหนดให้ในรอบ ๑ ปีปฏิทินสถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีการให้บริการทางการเงินผ่าน mobile banking application ต้องดูแลให้ระบบงานหยุดชะงักไม่เกิน ๘ ชั่วโมง

นอกจากนี้ ธปท. ได้ปรับปรุงแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติการบริหารจัดการความเสี่ยงบุคคลภายนอก เพื่อให้สถาบันการเงิน

และสถาบันการเงินเฉพาะกิจ สามารถนำไปประยุกต์ใช้ได้ตามความเหมาะสม สอดคล้องตามขอบเขตและระดับความเสี่ยงที่เผชิญ ทั้งนี้ สำหรับความเสี่ยงจากภัยคุกคามไซเบอร์ สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถนำกรอบการประเมินความพร้อมด้าน Cyber Resilience (Cyber Resilience Assessment Framework : CRAF) มาใช้เพื่อประเมินความเสี่ยงที่เกิดจากภัยไซเบอร์และการควบคุมขั้นต่ำที่ควรมี เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดจากภัยดังกล่าวได้

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๔๑ มาตรา ๔๗ และมาตรา ๗๑ แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) ให้สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศนี้

อาศัยอำนาจตามความในมาตรา ๑๒๐/๑ แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ และที่แก้ไขเพิ่มเติม ธนาคารแห่งประเทศไทยโดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลัง ออกหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk) ให้สถาบันการเงินเฉพาะกิจถือปฏิบัติตามที่กำหนดในประกาศนี้

๓. ประกาศที่ยกเลิก

ประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๒๑/๒๕๖๒ เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk) ของสถาบันการเงิน ลงวันที่ ๑ ตุลาคม ๒๕๖๒

๔. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับ

๔.๑ สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

๔.๒ สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

๕. นิยาม

ในประกาศฉบับนี้

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

“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (Information Technology risk : IT risk) หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของสถาบันการเงินหรือสถาบันการเงินเฉพาะกิจ รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threats)

“สถาบันการเงิน” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศแทนสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ หรือข้อมูลลูกค้าของสถาบันการเงินและสถาบันการเงินเฉพาะกิจในรูปแบบอิเล็กทรอนิกส์ได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์และบริการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

“ธปท.” หมายความว่า ธนาคารแห่งประเทศไทยตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

๖. หลักการ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีหน้าที่เกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

๖.๑ ดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงโครงการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและรัดกุม ภายใต้กรอบหลักการที่สำคัญ ๓ ประการ คือ (๑) การรักษาความลับของระบบและข้อมูล (confidentiality) (๒) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ (๓) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) โดยอยู่บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า

๖.๒ กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านชื่อเสียง ความเสี่ยงจากภัยทุจริตทางการเงิน และความเสี่ยงด้านกฎหมาย รวมถึงให้ความสำคัญกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (enterprise risk management: ERM)

๖.๓ มีโครงสร้างการกำกับดูแลในภาพรวมที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (three lines of defence)

ทั้งนี้ กรณีที่สถาบันการเงินมีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์สำหรับบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง การพิจารณาโครงสร้างการกำกับดูแลตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (three lines of defence) ให้พิจารณาจากภาพรวมทั้งหมดของกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องกันได้

อย่างไรก็ดี สถาบันการเงินและคณะกรรมการของสถาบันการเงินในประเทศไทยยังคงต้องรับผิดชอบต่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเสมือนสถาบันการเงินดำเนินการเอง

๗. หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีหน้าที่ต้องปฏิบัติตามหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

๗.๑ ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)

จัดให้มีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ตั้งแต่คณะกรรมการของสถาบันการเงินหรือคณะกรรมการของสถาบันการเงินเฉพาะกิจและผู้บริหารระดับสูงที่ให้ความสำคัญในการผลักดันและยกระดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำหนดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ สื่อสารและกำกับดูแลให้มีการปฏิบัติตามนโยบายที่กำหนด นอกจากนี้ต้องจัดให้มีผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งสร้างวัฒนธรรมและพฤติกรรมร่วมของทุกคนในองค์กรให้ตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง (รายละเอียดในเอกสารแนบ ๑)

๗.๒ การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security management)

จัดให้มีการบริหารจัดการและควบคุมระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีการรักษาความลับของระบบและข้อมูล ถูกต้องเชื่อถือได้ และพร้อมใช้งาน โดยนำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (รายละเอียดในเอกสารแนบ ๒)

๗.๓ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

จัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างครอบคลุมทั่วทั้งองค์กร โดยประสานงานร่วมกับหน่วยงานธุรกิจและหน่วยงานด้านเทคโนโลยีสารสนเทศ ในการระบุและประเมินความเสี่ยง การกำหนดมาตรการในการลดความเสี่ยงและระบบการควบคุมภายใน เพื่อให้มั่นใจว่ามีการบริหารความเสี่ยงอย่างเหมาะสมสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (รายละเอียดในเอกสารแนบ ๓)

๗.๔ การปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

จัดให้มีการติดตามดูแล และสอบทานการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายว่าด้วยระบบการชำระเงิน เป็นต้น

เพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและกฎเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง (รายละเอียดในเอกสารแนบ ๔)

๗.๕ การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบที่มีความเป็นอิสระ รวมทั้งต้องติดตามให้มีการปรับปรุงแก้ไขประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยงและการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศอย่างเพียงพอเหมาะสม (รายละเอียดในเอกสารแนบ ๕)

๗.๖ การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

กำหนดกรอบการบริหารจัดการโครงการ (project management framework) และโครงสร้างการกำกับดูแลโครงการ เพื่อให้โครงการที่มีนัยสำคัญมีการบริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดให้มีประสิทธิภาพสูงสุด เลือกใช้เทคโนโลยีอย่างเหมาะสม สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้ (รายละเอียดในเอกสารแนบ ๖)

ทั้งนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถพิจารณาประยุกต์ใช้แนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก เพื่อเป็นแนวทางการบริหารจัดการความเสี่ยงให้เหมาะสมและสอดคล้องตามขอบเขตและระดับความเสี่ยงได้

๘. การดูแลระบบงานที่รองรับช่องทางการให้บริการทางอุปกรณ์เคลื่อนที่ (mobile banking) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

ในรอบ ๑ ปีปฏิทิน สถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีการให้บริการทางการเงินผ่านช่องทาง mobile banking application ต้องดูแลให้ระบบเทคโนโลยีสารสนเทศให้บริการได้อย่างต่อเนื่อง โดยต้องหยุดชะงักไม่เกิน ๘ ชั่วโมง รวมทั้งต้องดูแลให้มีการกู้คืนระบบให้กลับมาให้บริการได้โดยเร็ว

๙. ข้อกำหนดในการพิจารณาความมีนัยสำคัญเพื่อดำเนินการตามประกาศนี้

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีข้อกำหนดในการพิจารณาความมีนัยสำคัญที่ชัดเจนเพื่อใช้พิจารณาดำเนินการในเรื่องต่าง ๆ ที่กำหนดไว้ตามประกาศฉบับนี้ โดยดำเนินการ ดังนี้

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

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

๙.๓ ต้องสื่อสารและเผยแพร่ข้อกำหนดดังกล่าวให้หน่วยงานที่เกี่ยวข้องทราบโดยทั่วกันและนำไปปฏิบัติ

๙.๔ ต้องสอบทานการดำเนินการตามข้อกำหนดอย่างน้อยปีละ ๑ ครั้ง

๙.๕ ต้องทบทวนข้อกำหนดอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบต่อสถาบันการเงินหรือสถาบันการเงินเฉพาะกิจและระบบสถาบันการเงิน

๑๐. การแจ้ง การรายงาน หรือการขออนุญาต ต่อ ธปท.

เพื่อให้ ธปท. สามารถกำกับดูแลและติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ รวมถึงความเสี่ยงของระบบสถาบันการเงินในภาพรวมได้เท่าทันกับการเปลี่ยนแปลง และสามารถติดตามปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศหรือภัยคุกคามทางไซเบอร์ได้ทันต่อสถานการณ์ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องแจ้งการรายงานหรือขออนุญาตต่อ ธปท. ดังต่อไปนี้

๑๐.๑ การแจ้งหรือการขออนุญาตนำเทคโนโลยีสารสนเทศมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

๑๐.๑.๑ ธนาคารพาณิชย์ที่นำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนดที่ธนาคารพาณิชย์ได้กำหนดขึ้นตามข้อ ๙ ทั้งกรณีที่ธนาคารพาณิชย์ดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้องแจ้งการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าว ต่อ ธปท. ตามที่กำหนดในคู่มือสำหรับประชาชนล่วงหน้าไม่น้อยกว่า ๑๕ วัน ก่อนดำเนินการ เว้นแต่ ธปท. มีคำสั่งให้ธนาคารพาณิชย์ ไม่ต้องแจ้งการนำเทคโนโลยีสารสนเทศมาใช้หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

๑๐.๑.๒ สถาบันการเงินเฉพาะกิจ บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ที่นำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนดตามข้อ ๙ ทั้งกรณีที่ดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต้องยื่นขออนุญาตก่อนนำมาใช้หรือก่อนการเปลี่ยนแปลงดังกล่าวต่อ ธปท. ตามที่กำหนดในคู่มือสำหรับประชาชน พร้อมเอกสารที่เกี่ยวข้อง ทั้งนี้ ธปท. อาจร้องขอให้ยื่นเอกสารที่เกี่ยวข้องอื่นเพิ่มเติมได้ โดย ธปท. จะพิจารณาให้แล้วเสร็จภายใน ๓๐ วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน เว้นแต่ ธปท.

มีคำสั่งให้สถาบันการเงินเฉพาะกิจ บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ ไม่ต้องยื่นขออนุญาตการนำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

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

๑๐.๒ การแจ้งการใช้บริการจากบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์สำหรับบริษัทในกลุ่มธุรกิจหรือบริษัทที่มีความเกี่ยวข้องกัน โดยให้บริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้องกันนั้นเป็นผู้ดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแทน ซึ่งบริษัทดังกล่าวอาจอยู่ในประเทศไทยหรือนอกประเทศไทยก็ได้ สถาบันการเงินต้องแจ้ง ธปท. ตามที่กำหนดในคู่มือประชาชนล่วงหน้าไม่น้อยกว่า ๑๕ วันก่อนการใช้โครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศดังกล่าว เช่น กรณีธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ มีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศแบบรวมศูนย์อยู่ที่บริษัทแม่ในต่างประเทศ

๑๐.๓ การรายงานปัญหาหรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องรายงานปัญหาหรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศต่อ ธปท. ตามรูปแบบและช่องทางที่กำหนดโดยเร็วเมื่อทราบถึง (๑) เหตุการณ์ด้านเทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียงที่มีนัยสำคัญและเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุด หรือ (๒) กรณีเทคโนโลยีสารสนเทศที่มีนัยสำคัญถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และ (๓) กรณีปัญหาหรือเหตุขัดข้องของระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อการให้บริการผ่านช่องทางให้บริการสำคัญที่ประชาชนใช้บริการจำนวนมากตามที่ ธปท. กำหนด ทั้งนี้ สามารถแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมในภายหลังได้

๑๐.๔ การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดทำและจัดส่งแบบรายงานในรูปแบบและตามระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด รวมถึงจัดทำและจัดส่งรายงานและข้อมูลอื่นเพิ่มเติมเป็นรายกรณีตามที่ธนาคารแห่งประเทศไทยร้องขอ

๑๐.๕ การรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk self-assessment)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดส่งผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ ธปท. ทราบภายใน ๓๐ วัน นับแต่วันสิ้นปีปฏิทิน โดยมีรูปแบบและช่องทางตามที่ ธปท. กำหนด

๑๑. การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ได้ ให้ยื่นขอผ่อนผันเป็นรายกรณีต่อ ธปท. พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธปท. จะพิจารณาให้แล้วเสร็จภายใน ๓๐ วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดย ธปท. อาจจะพิจารณาอนุญาตหรือไม่ก็ได้ หรือกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

ทั้งนี้ ในการพิจารณาคำขอผ่อนผัน ธปท. จะพิจารณาตามหลักการเสริมสร้างความมั่นคงของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ซึ่งรวมถึงการกำกับดูแลการบริหารจัดการ การบริหารความเสี่ยง การบริหารความมั่นคงปลอดภัยของสถาบันการเงินและสถาบันการเงินเฉพาะกิจให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่องเมื่อเกิดปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อระบบสถาบันการเงิน รวมถึงการส่งเสริมประสิทธิภาพ การสนับสนุนให้มีธรรมาภิบาลที่ดีและการคุ้มครองลูกค้าและผู้ใช้บริการ รวมถึงเสถียรภาพของระบบสถาบันการเงินและระบบเศรษฐกิจ

๑๒. การกำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ สั่งให้แก้ไข เพิกถอน หรือเข้าตรวจสอบการนำเทคโนโลยีสารสนเทศมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ

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

๑๓. บทเฉพาะกาล

สถาบันการเงินและสถาบันการเงินเฉพาะกิจที่มีการให้บริการผ่านช่องทาง mobile banking application ก่อนวันที่ประกาศฉบับนี้มีผลใช้บังคับ ให้ดำเนินการจัดให้มีการดูแลระบบงานที่รองรับ mobile banking application ให้เป็นไปตามข้อ ๘ วรรคหนึ่ง ภายในวันที่ ๑ มกราคม ๒๕๖๗

๑๔. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๖ ตุลาคม พ.ศ. ๒๕๖๖
เศรษฐพุฒิ สุทธิวาทนฤพุฒิ
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

เอกสารแนบ 1

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT governance)

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจ

คณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจต้องเข้าใจและตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อลูกค้าและผู้ใช้บริการ รวมทั้งมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมการดำเนินการและการดูแล ดังต่อไปนี้

1.1 ดูแลให้การใช้เทคโนโลยีสารสนเทศสอดรับกับกลยุทธ์ในการให้บริการหรือการดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงในอนาคต รวมทั้งดูแลให้ระบบเทคโนโลยีสารสนเทศที่รองรับบริการสำคัญสามารถให้บริการได้อย่างต่อเนื่อง

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

1.3 ดูแลให้เกิดการสร้างความรู้และความตระหนักรู้เรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่กรรมการ ผู้บริหาร และพนักงานในองค์กร รวมทั้งลูกค้าและผู้ใช้บริการอย่างต่อเนื่องและมีประสิทธิผล

ทั้งนี้ คณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจอาจมอบหมายให้คณะกรรมการชุดอื่นหรือผู้บริหารระดับสูงกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ โดยคณะกรรมการยังคงต้องรับผิดชอบในเรื่องดังกล่าว

นอกจากนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องปฏิบัติเพิ่มเติมในส่วนที่เกี่ยวข้องกับบทบาทหน้าที่ของคณะกรรมการตามที่ ธปท. กำหนดในประกาศธนาคารแห่งประเทศไทยว่าด้วยธรรมาภิบาลของสถาบันการเงิน และประกาศธนาคารแห่งประเทศไทยว่าด้วยธรรมาภิบาลของสถาบันการเงินเฉพาะกิจ เช่น คณะกรรมการต้องมีกรรมการอย่างน้อย 1 คนที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ เป็นต้น

2. โครงสร้างการกำกับดูแล

2.1 โครงสร้างองค์กรในการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีโครงสร้างองค์กรที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defence) โดยแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่าง

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

นอกจากนี้ ต้องมีการถ่วงดุลอำนาจกันอย่างอิสระ โดยเฉพาะการทำหน้าที่ตรวจสอบต้องมีความเป็นอิสระจากการทำหน้าที่ปฏิบัติงานและการทำหน้าที่บริหารความเสี่ยงและกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

2.2 คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมีคณะกรรมการ ดังต่อไปนี้

2.2.1 คณะกรรมการที่ทำหน้าที่บริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee เป็นต้น

2.2.2 คณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้ เช่น IT risk committee เป็นต้น

2.2.3 คณะกรรมการที่ทำหน้าที่กำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการตรวจสอบการปฏิบัติงาน การบริหารความเสี่ยงและการกำกับการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น คณะกรรมการตรวจสอบ เป็นต้น

2.3 การกำหนดผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.3.1 ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

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

- กำหนดให้มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

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

- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงขององค์กร และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจ หรือคณะกรรมการที่ได้รับมอบหมายเป็นวาระประจำ

- ดูแลและดำเนินการให้มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้ และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์

2.3.2 ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer : CISO)

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

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

- รายงานปัญหาหรือเหตุการณ์ผิดปกติที่มีนัยสำคัญด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด หรือคณะกรรมการที่เกี่ยวข้อง หรือคณะกรรมการของสถาบันการเงินและคณะกรรมการของสถาบันการเงินเฉพาะกิจโดยตรง

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

3. นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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

นอกจากนี้ การกำหนดนโยบายดังกล่าวต้องคำนึงถึงลักษณะการให้บริการหรือดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศภายในองค์กรและความเสี่ยงจากการใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอกด้วย

3.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4. การบริหารจัดการบุคลากร

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวันอย่างเหมาะสม โดยต้องคำนึงถึงความรู้ความสามารถของบุคลากร ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

4.1 การบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงาน บริหารความเสี่ยงและกำกับการปฏิบัติตามกฎเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ ต้องครอบคลุมในเรื่องกระบวนการคัดเลือกบุคลากรที่มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ ความเพียงพอของบุคลากรที่สอดคล้องกับปริมาณการใช้เทคโนโลยีสารสนเทศ และมาตรการในการสร้างและส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ

4.2 ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของบุคลากรหรือระเบียบข้อบังคับภายในองค์กรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้น

4.3 การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศต้องปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว

5. การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องสื่อสารและให้ความรู้แก่บุคลากรที่ทำหน้าที่ปฏิบัติงาน บริหารความเสี่ยงและการปฏิบัติตามกฎเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายสาธารณะที่ถูกต้อง การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น

นอกจากนี้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรเสริมสร้างความตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามไซเบอร์ให้กับลูกค้าและผู้ใช้บริการอย่างสม่ำเสมอและต่อเนื่องให้เท่าทันกับความเสี่ยงและภัยคุกคามใหม่ ๆ

เอกสารแนบ 2

การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
(IT security management)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำหนดให้มีการบริหารจัดการและควบคุมดูแลระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีการรักษาความลับของระบบและข้อมูล ถูกต้องเชื่อถือได้และพร้อมใช้งาน ดังต่อไปนี้

1. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

บริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม นอกจากนี้ ต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมถึงบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้หมดอายุการใช้งานหรือสิ้นสุดการให้บริการอย่างเหมาะสมและเท่าทันกับความเสี่ยง เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย พร้อมใช้งานและสามารถรองรับการให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

2. การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

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

3. การควบคุมการเข้าถึง (access control)

ต้องควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิ โดยต้องครอบคลุมอย่างน้อย ดังนี้

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

3.2 จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้

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

(2) บัญชีผู้ใช้งาน (user) ทุกบัญชีที่สามารถเข้าถึงข้อมูลลูกค้าและเชื่อมต่อมาจากระบบเครือข่ายสื่อสารสาธารณะ

ในกรณีที่ระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีวิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย

อย่างไรก็ตาม กรณีที่ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

4. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

รักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่อง

5. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

รักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น รวมทั้งพร้อมรองรับการให้บริการได้อย่างต่อเนื่อง

6. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

รักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

6.1 บริหารจัดการขีดความสามารถของระบบเทคโนโลยีสารสนเทศและระบบสาธารณูปโภค (capacity management) เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับการให้บริการหรือดำเนินธุรกิจและสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต สำหรับระบบที่มีการให้บริการผ่านช่องทางดิจิทัลควรมีการติดตามและประเมินขีดความสามารถของระบบอย่างใกล้ชิดรองรับบริการและปริมาณธุรกรรมที่เพิ่มขึ้นอย่างรวดเร็ว

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

6.3 สำรองข้อมูล (data backup) ด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

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

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

6.6 บริหารจัดการช่องโหว่ (vulnerability management) โดยจัดให้มีการประเมินช่องโหว่สำหรับทุกระบบงานตามระดับความเสี่ยง สำหรับระบบงานสำคัญต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

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

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

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

6.9 บริหารจัดการการตั้งค่าระบบ (system configuration management) โดยจัดให้มีการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยสอดคล้องกับมาตรฐานดังกล่าว (security hardening) ครอบคลุมระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้งดำเนินการตั้งค่าและสอบทานการตั้งค่าอย่างสม่ำเสมอตามที่ได้กำหนดไว้ เพื่อให้มั่นใจว่าระบบงานที่รองรับการให้บริการมีการรักษาความมั่นคงปลอดภัยขั้นต่ำตามมาตรฐานที่กำหนดไว้

---

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

ในกรณีที่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจไม่สามารถปฏิบัติตามมาตรฐานที่ตนได้กำหนดไว้ข้างต้น ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

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

ในกรณีที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

นอกจากนี้ กรณีที่ไม่สามารถติดตั้ง security patch ได้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

7. การจัดหาและการพัฒนาระบบ (system acquisition and development)

7.1 การจัดหาระบบ (system acquisition)

กำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและบุคคลภายนอกที่ให้บริการ เช่น ความน่าเชื่อถือของระบบ บุคคลภายนอกที่ให้บริการที่รับการรับรองตามมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป (certificate) ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ เป็นต้น เพื่อให้มั่นใจว่าระบบและบุคคลภายนอกที่ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินการได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการที่เป็นบุคคลภายนอก การเปลี่ยนแปลงเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจในอนาคต

7.2 การพัฒนาระบบ (system development)

ออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีการรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยต้องดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- มีรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

- มีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของคำสั่งเขียนโปรแกรม (source code version control)

- แบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบและผู้นำระบบขึ้นใช้งานจริง

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

- ทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (unit test) ทดสอบการทำงานร่วมกันของระบบต่าง ๆ (system integration test) ทดสอบความต้องการของ

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

- ทดสอบประสิทธิภาพ (performance test) และความสามารถในการให้บริการเมื่อมีการใช้บริการจำนวนมาก เมื่อมีการพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์

- มีแนวทางควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

- จัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

8. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)

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

9. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT disaster recovery plan)

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

9.2 จัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยคำนึงถึงลักษณะการให้บริการ การดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากบุคคลภายนอก (third party risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และความเสี่ยงที่มีผลกระทบต่อระบบสถาบันการเงิน (systemic risk) เป็นต้น

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

9.4 มีคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์และฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้

9.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

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

10. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

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

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

สำหรับกรณีที่ไม่สามารถระบุสิทธิให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอกมีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ในเงื่อนไขสัญญาหรือข้อตกลงกับบุคคลภายนอก สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมั่นใจว่าบุคคลภายนอกรายดังกล่าวมีผลการตรวจสอบจากผู้ตรวจสอบภายนอกที่เป็นอิสระทดแทน

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

10.3 รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป

10.4 เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการให้บริการหรือดำเนินธุรกิจแก่ลูกค้า

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

10.5.1 ประเมินระดับความเสี่ยงที่จะเกิดขึ้นจากการใช้บริการ public cloud computing จากบุคคลภายนอกด้านงานเทคโนโลยีสารสนเทศที่มีนัยสำคัญ โดยอย่างน้อยต้องครอบคลุมความเสี่ยงสำคัญ ดังนี้

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

10.5.2 กำหนดปัจจัยในการคัดเลือกบุคคลภายนอกก่อนใช้บริการ โดยอย่างน้อยต้องครอบคลุมปัจจัย ดังนี้

- ปัจจัยด้านความเสี่ยงของประเทศที่บุคคลภายนอกที่จัดเก็บหรือประมวลผลข้อมูลบนระบบ public cloud computing
- ปัจจัยด้านการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง
- ปัจจัยด้านความยืดหยุ่นในการเปลี่ยนแปลงระบบงานไปยังบุคคลภายนอกรายอื่นหรือการเชื่อมโยงกับระบบอื่นได้

10.5.3 ระบุสถานที่ที่บุคคลภายนอกประมวลผล จัดเก็บข้อมูล หรือดำเนินการอื่นใดที่เกี่ยวข้องกับข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

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

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

10.5.6 จัดให้มีกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่สอดคล้องกับแนวปฏิบัติการบริหารจัดการความเสี่ยงที่ดีของบุคคลภายนอก หรือมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป รวมทั้งสอบทานการตั้งค่าดังกล่าวอย่างสม่ำเสมอ

10.5.7 มีกระบวนการติดตามเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ที่เกิดกับระบบที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการ public cloud computing อย่างสม่ำเสมอ และมีการกำหนดแนวทางป้องกันภัยคุกคามดังกล่าว เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นก่อนที่บุคคลภายนอกจะสามารถแก้ไขปัญหาหรือดำเนินการปิดช่องโหว่

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

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

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

(2) ระบบงานของบุคคลภายนอกทุก region ที่ใช้บริการอยู่หยุดชะงักจนเป็นเหตุให้บริการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจไม่สามารถให้บริการได้อย่างต่อเนื่อง

(3) สายสื่อสารของสถาบันการเงินและสถาบันการเงินเฉพาะกิจขัดข้องทุกช่องทางจนไม่สามารถใช้บริการได้

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

เอกสารแนบ 3

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT risk management)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยอย่างน้อยต้องครอบคลุมการดำเนินการ ดังนี้

1. โครงสร้างองค์กร

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

1.2 กำหนดสายการรายงานที่ชัดเจนและเป็นอิสระจากหน่วยงานที่ทำหน้าที่เป็น first line of defence โดยรวบรวมและเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกับความเสี่ยงด้านอื่นของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ พร้อมทั้งนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.3 ผู้รับผิดชอบงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องมีความรู้ประสบการณ์ และความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงได้รับการฝึกอบรมด้านการบริหารจัดการความเสี่ยงและเพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง เพื่อให้สามารถบริหารจัดการความเสี่ยงและติดตามความเสี่ยงได้อย่างมีประสิทธิภาพ

2. การปฏิบัติงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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

2.1 การประเมินความเสี่ยง

2.1.1 การระบุความเสี่ยง ให้ระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร การใช้บริการจากบุคคลภายนอก หรือปัจจัยภายนอก

2.1.2 การวิเคราะห์ความเสี่ยง ควรเข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

2.1.3 การประเมินค่าความเสี่ยง ให้ประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงาน

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

ทั้งนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) ที่เกี่ยวข้องกับการให้บริการหรือดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

2.3 การติดตามและทบทวนความเสี่ยง ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

2.4 การรายงานความเสี่ยง ให้รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อคณะกรรมการของสถาบันการเงินหรือคณะกรรมการของสถาบันการเงินเฉพาะกิจหรือคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมายกรณีเป็นสาขาธนาคารพาณิชย์ต่างประเทศเป็นประจำอย่างสม่ำเสมอ

เอกสารแนบ 4

การกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT compliance)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำหนดกรอบการกำกับการปฏิบัติตามกฎเกณฑ์ให้ครอบคลุมถึงกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และต้องนำมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการกำกับการปฏิบัติตามกฎเกณฑ์ โดยอย่างน้อยต้องครอบคลุม ดังนี้

1. โครงสร้างองค์กร

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

1.2 กำหนดสายการรายงานที่ชัดเจนและเป็นอิสระจากหน่วยงานที่ทำหน้าที่เป็น first line of defence โดยรายงานถึงหัวหน้าหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ที่มีสายการรายงานตรงถึงคณะกรรมการที่เกี่ยวข้อง เช่น คณะกรรมการที่ทำหน้าที่กำกับดูแลบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎเกณฑ์ เป็นต้น

1.3 ผู้รับผิดชอบงานด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ต้องมีความรู้ ประสบการณ์ และความเข้าใจในกฎหมายและความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศ รวมถึงต้องได้รับการฝึกอบรมด้านกฎเกณฑ์ต่าง ๆ และเพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง

2. การปฏิบัติงานด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

กำหนดกระบวนการในการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยอย่างน้อยครอบคลุม ดังนี้

2.1 การระบุและประเมินความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ ต้องครอบคลุมถึงกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยระบบการชำระเงิน เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและกฎเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

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

2.3 การติดตามและรายงานผลการสอบทานด้านการปฏิบัติตามกฎเกณฑ์ สรุปผลเหตุการณ์ไม่ปฏิบัติตามกฎเกณฑ์และมาตรการแก้ไข รวมถึงผลการดำเนินการตามข้อเสนอแนะคำสั่งการของ ธปท. และผู้กำกับดูแลอื่นที่เกี่ยวข้อง ต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย กรณีเป็นสาขาธนาคารพาณิชย์ต่างประเทศ เป็นประจำอย่างสม่ำเสมอ

เอกสารแนบ 5

การตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
(IT audit)

สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำหนดกรอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมการปฏิบัติงาน กระบวนการทำงานและระบบงานด้านเทคโนโลยีสารสนเทศ และต้องนำมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการตรวจสอบ โดยอย่างน้อยต้องครอบคลุม ดังนี้

1. โครงสร้างองค์กร

1.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มีการดำเนินการในงานตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit function) โดยสามารถจัดตั้งเป็นหน่วยงานที่รับผิดชอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ หรืออยู่ภายใต้สายงานตรวจสอบภายใน ทั้งนี้ ต้องมั่นใจว่ามีความเป็นอิสระและสามารถปฏิบัติงานได้อย่างครบถ้วนและมีประสิทธิภาพ

1.2 กำหนดสายการรายงานที่เป็นอิสระ โดยต้องรายงานถึงหัวหน้าหน่วยงานตรวจสอบภายในและรายงานตรงต่อคณะกรรมการตรวจสอบ

1.3 ผู้รับผิดชอบงานด้านการตรวจสอบเทคโนโลยีสารสนเทศต้องมีความรู้ ประสบการณ์และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก ที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

1.4 ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องได้รับการฝึกอบรม เพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง เพื่อให้ผู้ตรวจสอบสามารถนำมาปรับใช้กับวิธีการตรวจสอบได้ทันกับแนวโน้มและการพัฒนาทางด้านเทคโนโลยีสารสนเทศ

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

2. การปฏิบัติงานด้านการตรวจสอบเทคโนโลยีสารสนเทศ

กำหนดขอบเขตการตรวจสอบต้องครอบคลุมการปฏิบัติงาน กระบวนการทำงานและระบบงานด้านเทคโนโลยีสารสนเทศทั้งหมด รวมทั้งการใช้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก เพื่อให้สามารถระบุและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน โดยมีกระบวนการอย่างน้อยครอบคลุม ดังนี้

2.1 การกำหนดแผนงานตรวจสอบ ต้องสอดคล้องกับความสำคัญและความเสี่ยงของการใช้งานเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ สำหรับงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญต้องตรวจสอบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งเมื่อมีเหตุการณ์ผิดปกติในเทคโนโลยีสารสนเทศที่มีนัยสำคัญ โดยแผนงานและขอบเขตการตรวจสอบต้องได้รับการอนุมัติจากคณะกรรมการ

ตรวจสอบ รวมถึงต้องทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าว โดยคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.2 การตรวจสอบ ต้องตรวจสอบตามแผนงานและขอบเขตที่กำหนดอย่างน้อยปีละ 1 ครั้ง โดยการตรวจสอบควรเป็นไปตามมาตรฐานที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด ซึ่งสอดคล้องกับกฎหมาย กฎเกณฑ์ที่เกี่ยวข้อง และมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป

2.3 การติดตามและรายงานผลการตรวจสอบ ต้องสรุปผลการตรวจสอบและประเด็นที่ต้องแก้ไขกับผู้บริหารของหน่วยงานผู้รับตรวจและจัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการตรวจสอบและแจ้งให้ผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบ รวมถึงติดตามให้มีการปรับปรุงประเด็นการตรวจสอบและรายงานประเด็นสำคัญพร้อมแผนปรับปรุงให้กับคณะกรรมการตรวจสอบเป็นประจำอย่างสม่ำเสมอ ทั้งนี้ ให้จัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจ เพื่อให้พร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดย ธปท.

เอกสารแนบ 6

การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (IT project management)

เมื่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจจัดทำโครงการด้านเทคโนโลยีสารสนเทศ (IT project management) ที่มีนัยสำคัญ ที่นำมาใช้ในการให้บริการหรือดำเนินธุรกิจ ต้องปฏิบัติตามหลักเกณฑ์ดังต่อไปนี้

1. ศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับสำหรับโครงการที่นำเทคโนโลยีสารสนเทศมาใช้ในการให้บริการหรือดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องพิจารณาเลือกใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม และประเมินความเสี่ยงตลอดจนผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งต้องจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมายกรณีเป็นสาขาธนาคารพาณิชย์ต่างประเทศ ตามขอบเขตอำนาจอนุมัติที่กำหนดไว้

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

3. กำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (project governance) โดยอย่างน้อยต้องกำหนดโครงสร้าง ดังต่อไปนี้

3.1 คณะกรรมการที่ทำหน้าที่กำกับดูแลโครงการ เพื่อทำหน้าที่กำกับดูแลความคืบหน้า ให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้การดำเนินงานของโครงการเป็นไปตามแผนงานที่กำหนด ทั้งนี้ คณะกรรมการกำกับดูแลโครงการควรประกอบด้วยผู้บริหารหรือผู้แทนจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้อง

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

3.3 ผู้จัดการโครงการ (project manager) เพื่อทำหน้าที่ในการบริหารจัดการโครงการแต่ละโครงการตามขั้นตอนการบริหารจัดการโครงการ และส่งมอบงานในแต่ละขั้นตอนตามรูปแบบกระบวนการและเครื่องมือ ตามที่หน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการกำหนด เพื่อให้สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานที่กำหนด