ประกาศธนาคารแห่งประเทศไทย

ที่ สนช. ๑/๒๕๖๔

เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน

---

๑. เหตุผลในการออกประกาศ

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

ธนาคารแห่งประเทศไทย (ธปท.) จึงกำหนดหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเพิ่มเติมจากหลักเกณฑ์การกำกับดูแลระบบเทคโนโลยีสารสนเทศที่ใช้บังคับอยู่ในปัจจุบัน เพื่อให้ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน มีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงดังกล่าวอย่างเหมาะสม โดยหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศตามประกาศนี้ ประกอบด้วย ๒ ส่วนสำคัญ ได้แก่

๑. การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) ซึ่งเป็นมาตรการขั้นต้นที่ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับทุกรายต้องดำเนินการ เพื่อยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่สำคัญ

๒. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ซึ่งจะมุ่งเน้นให้ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญ ซึ่งมีคุณสมบัติตามที่ประกาศฉบับนี้กำหนด ต้องปฏิบัติโดยมีหลักเกณฑ์ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม มีโครงสร้างองค์กร องค์ประกอบและการกำหนดบทบาทหน้าที่ของคณะกรรมการ เพื่อกำหนดนโยบายในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตลอดจนกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการให้บริการหรือดำเนินธุรกิจ

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๗ มาตรา ๒๔ มาตรา ๒๕ และมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยระบบการชำระเงิน พ.ศ. ๒๕๖๐ ธนาคารแห่งประเทศไทยกำหนดหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ให้ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ถือปฏิบัติตามที่กำหนดในประกาศนี้

๓. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน ที่มิใช่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน โดยแบ่งเป็น ๒ ส่วน ได้แก่

๓.๑ การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) บังคับใช้กับผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบและบริการการชำระเงินภายใต้การกำกับทุกรายต้องดำเนินการ

๓.๒ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) บังคับใช้กับผู้ให้บริการและผู้ประกอบธุรกิจ ดังต่อไปนี้

(๑) ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ

(๒) ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ

(๓) ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีคุณสมบัติ ดังต่อไปนี้

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

(๓.๒) ให้บริการทางการเงินแก่ลูกค้าผ่านเครือข่ายสื่อสารสาธารณะ (Internet facing)

(๓.๓) มีบัญชีผู้ใช้งานมากกว่า ๕ ล้านบัญชี หรือมีปริมาณธุรกรรมมากกว่า ๑๐ ล้านรายการต่อปี

ทั้งนี้ ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับต้องจัดให้มีการประเมินตนเองเป็นรายปี โดยใช้ข้อมูลประกอบการประเมิน ณ วันสิ้นปีปฏิทิน ว่าเป็นผู้มีคุณสมบัติครบถ้วนตามข้อ (๓.๑) - (๓.๓) ข้างต้นหรือไม่ หากผลการประเมินปรากฏว่ามีคุณสมบัติครบถ้วนตามหลักเกณฑ์ดังกล่าว ให้แจ้งผลการประเมินให้ ธปท. ทราบภายใน ๓๐ วันนับแต่วันสิ้นปีปฏิทิน และให้ถือปฏิบัติดังนี้

(๑) กรณีผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับรายเดิมที่ประเมินตนเองแล้ว ยังคงมีคุณสมบัติครบถ้วนทั้งสามข้อดังกล่าว ให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามข้อ ๕.๒ ต่อเนื่องต่อไป

(๒) สำหรับผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับรายใหม่ที่ประเมินตนเองแล้วปรากฏว่ามีคุณสมบัติครบถ้วนทั้งสามข้อดังกล่าว ให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามข้อ ๕.๒ ภายใน ๑ ปีนับแต่วันสิ้นปีปฏิทินของปีที่มีการประเมิน

สำหรับผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับที่เป็นนิติบุคคลต่างประเทศที่ต้องปฏิบัติตามหลักเกณฑ์หรือกฎหมายการกำกับดูแลของประเทศนั้น ๆ ให้จัดเตรียมข้อมูลที่เกี่ยวข้องตามข้อ ๕ ข้อ ๖ และข้อ ๗.๓ - ๗.๕ ไว้ให้เป็นปัจจุบันเพื่อให้พร้อมสำหรับการตรวจสอบของ ธปท. หรือเมื่อ ธปท. ร้องขอ และยกเว้นการปฏิบัติตามข้อ ๗.๑

๔. นิยาม

ในประกาศฉบับนี้

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

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

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

“ผู้ให้บริการ” หมายความว่า ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญตามกฎหมายว่าด้วยระบบการชำระเงิน

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงินที่มิใช่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“สถาบันการเงิน” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“รัฐวิสาหกิจ” หมายความว่า รัฐวิสาหกิจที่มีกฎหมายเฉพาะจัดตั้งขึ้น

“นิติบุคคลต่างประเทศ” หมายความว่า นิติบุคคลที่จดทะเบียนจัดตั้งขึ้นตามกฎหมายต่างประเทศและประกอบธุรกิจหรือให้บริการระบบการชำระเงินในประเทศไทย

“สมาชิก” หมายความว่า ผู้ใช้บริการที่ยินยอมผูกพันตามหลักเกณฑ์ในการใช้บริการระบบการชำระเงินที่มีความสำคัญ

“ผู้ใช้บริการของระบบ” หมายความว่า ผู้ใช้บริการที่เป็นสมาชิกและยินยอมผูกพันตามหลักเกณฑ์ในการใช้บริการของระบบการชำระเงินภายใต้การกำกับ

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศแทนผู้ให้บริการและผู้ประกอบธุรกิจ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ให้บริการและผู้ประกอบธุรกิจ หรือข้อมูลของสมาชิกหรือลูกค้าที่ควบคุมดูแลโดยผู้ให้บริการและผู้ประกอบธุรกิจได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงสมาชิกหรือลูกค้าที่ใช้ผลิตภัณฑ์และบริการของผู้ให้บริการและผู้ประกอบธุรกิจ

“ธปท.” หมายความว่า ธนาคารแห่งประเทศไทยตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

๕. หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

๕.๑ การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene)

ผู้ให้บริการและผู้ประกอบธุรกิจทุกรายต้องปฏิบัติตามหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็นเพื่อยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่สำคัญ ลดความเสี่ยงหรือผลกระทบต่อสมาชิก ผู้ใช้บริการของระบบหรือลูกค้า และต่อระบบชำระเงินโดยรวม ผู้ให้บริการและผู้ประกอบธุรกิจต้องดำเนินการ ดังนี้

๕.๑.๑ การกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (security baseline and hardening)

กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และตั้งค่าการรักษาความมั่นคงปลอดภัยสอดคล้องกับการให้บริการ (security hardening) ให้ครอบคลุมระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้งดำเนินการและสอบทานตามที่ได้กำหนดไว้

หากมีเหตุที่ผู้ให้บริการและผู้ประกอบธุรกิจไม่สามารถปฏิบัติตามมาตรฐานที่กำหนดไว้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

๕.๑.๒ การป้องกันภัยจากโปรแกรมไม่ประสงค์ดี (malware protection)

จัดให้มีเครื่องมือสำหรับป้องกันภัยจาก malware รวมทั้งติดตามให้มีการปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตีโดย malware

๕.๑.๓ การบริหารจัดการ security patch (security patch management)

จัดให้มีกระบวนการบริหารจัดการ security patch สำหรับทุกระบบงานและอุปกรณ์ เพื่อเป็นการลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่และระดับความสำคัญของระบบงาน

หากมีเหตุที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ ผู้ให้บริการและผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

อย่างไรก็ตาม กรณีที่ไม่สามารถติดตั้ง security patch ได้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

๕.๑.๔ การบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิสูง (privilege user management)

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

๕.๑.๕ การพิสูจน์ตัวตนแบบ multi-factor authentication

จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณี ดังต่อไปนี้

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

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

หากมีเหตุที่ระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication ผู้ให้บริการและผู้ประกอบธุรกิจสามารถใช้วิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย

อย่างไรก็ตาม กรณีที่ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

๕.๑.๖ การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing)

จัดให้มีการประเมินช่องโหว่ (vulnerability assessment) สำหรับทุกระบบงานตามระดับความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระ ครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) สม่ำเสมออย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความเสี่ยง หรือมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ อย่างมีนัยสำคัญ ทั้งนี้ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

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

นอกจากผู้ให้บริการและผู้ประกอบธุรกิจต้องดำเนินการตามข้อ ๕.๑.๑ - ๕.๑.๖ แล้ว ยังต้องปฏิบัติตามข้อ ๖ และข้อ ๗ ของประกาศฉบับนี้ในเรื่องการจัดทำข้อกำหนดเพื่อพิจารณาความมีนัยสำคัญในเรื่องต่าง ๆ เช่น ระบบงาน การเปลี่ยนแปลงเทคโนโลยีสารสนเทศ หรือเหตุการณ์ปัญหาที่เกิดขึ้น และเรื่องการแจ้งหรือนำส่งรายงานตามที่กำหนดด้วย

๕.๒ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

ผู้ให้บริการและผู้ประกอบธุรกิจที่เข้าเงื่อนไขตามที่กำหนดในข้อ ๓ ให้ดำเนินการยกระดับการดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการให้บริการ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพและรัดกุม ประกอบด้วย ๖ เรื่อง คือ ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit) และการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management) ดังนี้

๕.๒.๑ ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)

จัดให้มีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ตั้งแต่คณะกรรมการและผู้บริหารระดับสูงที่ให้ความสำคัญในการผลักดันและยกระดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำหนดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ สื่อสารและกำกับดูแลให้มีการปฏิบัติตามนโยบายที่กำหนด นอกจากนี้ต้องจัดให้มีผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งสร้างวัฒนธรรมและพฤติกรรมร่วมของทุกคนในองค์กรให้ตระหนักถึงความเสี่ยงอย่างต่อเนื่อง (รายละเอียดในเอกสารแนบ ๑)

๕.๒.๒ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

จัดให้มีการบริหารจัดการและควบคุมระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีความปลอดภัย ถูกต้องเชื่อถือได้ และพร้อมใช้งาน โดยนำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ (รายละเอียดในเอกสารแนบ ๒)

๕.๒.๓ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

จัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างครอบคลุมทั่วทั้งองค์กรและเหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ โดยกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมโครงสร้างองค์กร บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (รายละเอียดในเอกสารแนบ ๓)

๕.๒.๔ การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

กำกับดูแลให้ปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (IT compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

๕.๒.๕ การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบที่มีความเป็นอิสระ รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยการบริหารความเสี่ยงและการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศที่เพียงพอ (รายละเอียดในเอกสารแนบ ๔)

๕.๒.๖ การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management) กำหนดกรอบการบริหารจัดการโครงการ (project management framework) และโครงสร้างการกำกับดูแลโครงการ เพื่อให้โครงการที่มีนัยสำคัญมีการบริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดให้มีประสิทธิภาพสูงสุด สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงาน และบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้ (รายละเอียดในเอกสารแนบ ๕)

๖. ข้อกำหนดในการพิจารณาความมีนัยสำคัญเพื่อดำเนินการตามประกาศนี้

ผู้ให้บริการและผู้ประกอบธุรกิจต้องมีข้อกำหนดถึงความมีนัยสำคัญที่ชัดเจนเพื่อใช้พิจารณาดำเนินการในเรื่องต่าง ๆ ที่กำหนดไว้ตามประกาศฉบับนี้ โดยดำเนินการ ดังนี้

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

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

๖.๓ ต้องสื่อสารและเผยแพร่หลักเกณฑ์ให้หน่วยงานที่เกี่ยวข้องทราบโดยทั่วกันและนำไปปฏิบัติ

๖.๔ ต้องสอบทานการดำเนินการตามข้อกำหนดอย่างน้อยปีละ ๑ ครั้ง

๖.๕ ต้องทบทวนข้อกำหนดอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับระดับความเสี่ยงและผลกระทบต่อผู้ให้บริการและผู้ประกอบธุรกิจ และระบบการชำระเงิน

๗. การแจ้งหรือรายงานต่อ ธปท.

เพื่อให้ ธปท. สามารถกำกับดูแลและติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ และความเสี่ยงของระบบการชำระเงินในภาพรวมได้เท่าทันกับการเปลี่ยนแปลง ปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศหรือภัยคุกคามทางไซเบอร์ ผู้ให้บริการและผู้ประกอบธุรกิจต้องแจ้งหรือรายงานต่อ ธปท. ดังต่อไปนี้

๗.๑ การแจ้งการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

ผู้ให้บริการต้องแจ้งการนำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ ทั้งกรณีที่ดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือ

การเข้าถึงข้อมูลจากบุคคลภายนอก ต่อ ธปท. ล่วงหน้า ๑๕ วันก่อนดำเนินการตามช่องทางที่ ธปท. กำหนด

ในกรณีที่เป็นผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับหรือผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ให้แจ้งการนำเทคโนโลยีมาใช้หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ ทั้งกรณีที่ดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ตามข้อ ๔.๒.๓ (๔.๓.๒) ของประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และข้อ ๔.๒.๓ (๗.๒.๒) ของประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับด้วย แล้วแต่กรณี

๗.๒ การรายงานปัญหาด้านเทคโนโลยีสารสนเทศ

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

ในกรณีที่ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับหรือผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศตามวรรคหนึ่ง ให้รายงานปัญหาด้านเทคโนโลยีสารสนเทศตามข้อ ๔.๒.๓ (๕.๒.๑) ของประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และข้อ ๔.๒.๓ (๘.๓) ของประกาศว่าด้วยหลักเกณฑ์การกำกับดูแลการประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับด้วย แล้วแต่กรณี

๗.๓ การรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญต้องจัดส่งผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งในส่วนของหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) และหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) สำหรับผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่ไม่เข้าเงื่อนไขตามข้อ ๓.๒ (๓.๑) - (๓.๓) ต้องจัดส่งผลการประเมินเฉพาะหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ขั้นต้นที่จำเป็น (Cyber Hygiene) โดยจัดส่งผลการประเมินให้ ธปท. ทราบภายใน ๓๐ วันนับแต่วันสิ้นปีปฏิทิน โดยมีรูปแบบและช่องทางตามที่ ธปท. กำหนด

๗.๔ การรายงานบุคคลภายนอกที่มีนัยสำคัญ

ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญต้องจัดส่งรายงานการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของบุคคลภายนอกที่มีนัยสำคัญเป็นรายไตรมาสตามรูปแบบและช่องทางที่ ธปท. กำหนด

๗.๕ การรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญต้องจัดส่งรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญเป็นรายไตรมาสตามรูปแบบและช่องทางที่ ธปท. กำหนด ทั้งกรณีที่ดำเนินการเองและกรณีที่มีการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก

๘. การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

๘.๑ กรณีที่ผู้ให้บริการและผู้ประกอบธุรกิจมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ได้ ให้ยื่นขออนุญาตผ่อนผันเป็นรายกรณีต่อ ธปท. ก่อนครบกำหนดระยะเวลาตามที่ประกาศนี้กำหนด พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธปท. จะพิจารณาให้แล้วเสร็จภายใน ๓๐ วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดย ธปท. อาจจะพิจารณาอนุญาตหรือไม่ก็ได้ หรือกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

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

๘.๒ ในกรณีที่ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับไม่สามารถปฏิบัติตามข้อ ๕.๒.๑ ได้ ให้ยื่นขอผ่อนผันต่อ ธปท. เป็นรายกรณี พร้อมแสดงเหตุผลและความจำเป็น โดยต้องปฏิบัติ ดังนี้

(๑) กรณีไม่สามารถจัดให้มีกรรมการที่มีความรู้หรือประสบการณ์ด้าน IT ให้จัดหาผู้เชี่ยวชาญด้าน IT เป็นที่ปรึกษาให้คณะกรรมการแทนได้

(๒) กรณีไม่สามารถจัดให้มีบุคลากรภายในทำหน้าที่บริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง ให้จัดผู้เชี่ยวชาญภายนอกมาทำหน้าที่ดังกล่าวแทนได้

๙. การกำหนดเงื่อนไขเพิ่มเติม ชะลอ ระงับ สั่งให้แก้ไข เพิกถอน หรือเข้าตรวจสอบ การนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศ

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

๑๐. บทเฉพาะกาล

บรรดาประกาศอื่นใดที่ออกภายใต้กฎหมายว่าด้วยระบบการชำระเงินในส่วนที่กำหนดไว้แล้วในประกาศฉบับนี้ หรือซึ่งขัดหรือแย้งกับเนื้อหาในประกาศฉบับนี้ให้ใช้ประกาศฉบับนี้แทน

๑๑. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนด ๙๐ วันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่ในเรื่องหลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ตามข้อ ๕.๒ เรื่อง การรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศตามข้อ ๗.๓ เรื่องการรายงานบุคคลภายนอกที่มีนัยสำคัญตามข้อ ๗.๔ และเรื่องการรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญตามข้อ ๗.๕ ให้ใช้บังคับเมื่อพ้นกำหนด ๑ ปี นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๘ มกราคม พ.ศ. ๒๕๖๔
เศรษฐพุฒิ สุทธิวาทนฤพุฒิ
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

เอกสารแนบ 1

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ
(IT governance)

1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ

คณะกรรมการต้องเข้าใจและตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อผู้ให้บริการ ผู้ประกอบธุรกิจ และผู้ที่เกี่ยวข้อง รวมทั้งมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมการดำเนินการและการดูแล ดังต่อไปนี้

1.1 ใช้เทคโนโลยีสารสนเทศที่สอดรับกับกลยุทธ์การให้บริการหรือดำเนินธุรกิจ และยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงต่าง ๆ ในอนาคต

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

1.3 สร้างความรู้และความตระหนักรู้เรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่กรรมการ ผู้บริหาร และพนักงานในองค์กรอย่างต่อเนื่องและมีประสิทธิผล

ทั้งนี้ คณะกรรมการอาจมอบหมายให้คณะกรรมการชุดอื่นหรือผู้บริหารระดับสูงกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ โดยคณะกรรมการยังคงต้องรับผิดชอบในเรื่องดังกล่าว

นอกจากนี้ คณะกรรมการต้องมีกรรมการอย่างน้อย 1 คนที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศเพื่อทำหน้าที่กำกับดูแลเทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจ อย่างไรก็ดี สำหรับผู้ให้บริการและผู้ประกอบธุรกิจซึ่งเป็นนิติบุคคลที่เป็นหน่วยงานของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้นนั้น คณะกรรมการอาจมอบหมายให้คณะกรรมการชุดอื่น ซึ่งต้องมีกรรมการอย่างน้อย 1 คน ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศทำหน้าที่แทนได้

2. โครงสร้างการกำกับดูแล

2.1 โครงสร้างองค์กรในการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

ผู้ให้บริการและผู้ประกอบธุรกิจต้องจัดให้มีโครงสร้างองค์กรต้องเอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ

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

2.2 คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ผู้ให้บริการและผู้ประกอบธุรกิจต้องมีคณะกรรมการ ดังต่อไปนี้

2.2.1 คณะกรรมการที่ทำหน้าที่บริหารจัดการ และกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee

2.2.2 คณะกรรมการที่ทำหน้าที่กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

2.2.3 คณะกรรมการที่ทำหน้าที่กำกับดูแลให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการตรวจสอบการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

2.3 การกำหนดผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.3.1 ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

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

- มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

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

- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงขององค์กร และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการเป็นวาระประจำ

- ดูแลและดำเนินการให้มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้ และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์

2.3.2 ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer : CISO)

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

- รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด หรือคณะกรรมการที่เกี่ยวข้อง หรือคณะกรรมการของผู้ให้บริการและผู้ประกอบธุรกิจ

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

3. นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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

และ ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) หรือ CIA โดยนโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการหรือคณะกรรมการที่ได้รับมอบหมายแล้วแต่กรณี และต้องสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีสารสนเทศมาใช้สำหรับให้บริการหรือดำเนินธุรกิจ และนโยบายการบริหารความเสี่ยง รวมทั้งสอดคล้องกับแนวทางการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

นอกจากนี้ การกำหนดนโยบายดังกล่าวต้องคำนึงถึงลักษณะการให้บริการหรือดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศภายในองค์กรและความเสี่ยงจากกรณีมีการใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอกด้วย

3.2 ผู้ให้บริการและผู้ประกอบธุรกิจต้องทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4. การบริหารจัดการบุคลากร

ผู้ให้บริการและผู้ประกอบธุรกิจต้องบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวันอย่างเหมาะสม โดยต้องคำนึงถึงความรู้ความสามารถของบุคลากร ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

4.1 การบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงาน บริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศต้องครอบคลุมในเรื่องกระบวนการคัดเลือกบุคลากรที่มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ ความเพียงพอของบุคลากรที่สอดคล้องกับปริมาณการใช้เทคโนโลยีสารสนเทศ และมาตรการในการสร้างและส่งเสริมความตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ

4.2 ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานหรือระเบียบข้อบังคับภายในองค์กรของบุคลากรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศ

4.3 การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยต้องปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว

5. การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness)

ผู้ให้บริการและผู้ประกอบธุรกิจต้องสื่อสารและให้ความรู้แก่บุคลากรที่ทำหน้าที่ปฏิบัติงานบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ตที่ถูกต้อง และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์

เอกสารแนบ 2

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
(IT security)

ผู้ให้บริการและผู้ประกอบธุรกิจต้องกำหนดให้มีการบริหารจัดการและควบคุมดูแลระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีความปลอดภัย ถูกต้องเชื่อถือได้ และพร้อมใช้งาน ดังต่อไปนี้

1. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

บริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

2. การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

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

3. การควบคุมการเข้าถึง (access control)

ควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

4. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

รักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่อง

5. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

รักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของผู้ให้บริการและผู้ประกอบธุรกิจ เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านเครือข่ายสื่อสารมีความมั่นคงปลอดภัย และสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

6. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

รักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

6.1 บริหารจัดการขีดความสามารถของระบบและระบบสาธารณูปโภค (capacity management) เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการให้บริการ หรือดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

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

6.3 สำรองข้อมูล (data backup) ด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

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

6.5 ติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เช่น เครื่องมือติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้สามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

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

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

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

6.9 บริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการควบคุมการตั้งค่าของระบบที่ใช้งานจริง และมีการสอบทานการตั้งค่าอย่างสม่ำเสมอ เพื่อป้องกันข้อผิดพลาดในการปฏิบัติงาน

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

7. การจัดหาและการพัฒนาระบบ (system acquisition and development)

7.1 การจัดหาระบบ (system acquisition)

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

7.2 การพัฒนาระบบ (system development)

ออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยต้องดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- มีเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

- มีกระบวนการหรือเครื่องมือควบคุมเวอร์ชั่นของคำสั่งเขียนโปรแกรม (source code version control)

- แบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบและผู้นำระบบขึ้นใช้งานจริง

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

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

- พัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยต้องมีการทดสอบประสิทธิภาพ (performance test) เมื่อมีการพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์

- มีแนวทางควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

- จัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

8. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)

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

9. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT disaster recovery plan)

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

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

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

9.4 มีคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์และฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้

9.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

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

10. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

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

ข้อมูลสมาชิก ข้อมูลลูกค้าที่ถูกควบคุมดูแล ผู้ให้บริการและผู้ประกอบธุรกิจต้องกำกับดูแลความเสี่ยง กระบวนการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ ให้สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญบนพื้นฐานที่ต้องรับผิดชอบต่อการให้บริการหรือดำเนินธุรกิจแก่สมาชิก ผู้ใช้บริการระบบ หรือลูกค้า และคงไว้ซึ่งความน่าเชื่อถือชื่อเสียง ประสิทธิภาพในการให้บริการ ตามหลักการดังนี้

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

ทั้งนี้ ธปท. อาจสั่งให้มีการระบุผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และ ธปท. มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกรายอื่น ๆ เป็นเงื่อนไขในสัญญาหรือข้อตกลงตามความเหมาะสม

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

10.3 รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ และอ้างอิงมาตรฐานสากลที่ยอมรับโดยทั่วไป รวมถึงมีการรักษาความปลอดภัยจากภัยไซเบอร์ตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

10.4 เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการให้บริการหรือดำเนินธุรกิจแก่สมาชิก ผู้ใช้บริการของระบบ หรือลูกค้า แล้วแต่กรณี

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

เอกสารแนบ 3

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(IT risk management)

ผู้ให้บริการและผู้ประกอบธุรกิจต้องกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

1. การประเมินความเสี่ยง

1.1 การระบุความเสี่ยง

ระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

1.2 การวิเคราะห์ความเสี่ยง

เข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

1.3 การประเมินค่าความเสี่ยง

ประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงานและการให้บริการหรือดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

2. การจัดการความเสี่ยง

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) ที่เกี่ยวข้องกับการให้บริการหรือดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

3. การติดตามและทบทวนความเสี่ยง

มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

4. การรายงานความเสี่ยง

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ

ทั้งนี้ ผู้ให้บริการและผู้ประกอบธุรกิจต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

เอกสารแนบ 4

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง การตรวจสอบด้านเทคโนโลยีสารสนเทศ
(IT audit)

ผู้ให้บริการและผู้ประกอบธุรกิจต้องถือปฏิบัติตามหลักเกณฑ์ ดังต่อไปนี้

1. ต้องมีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

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

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

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

4. ต้องมีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งผู้ให้บริการและผู้ประกอบธุรกิจเห็นว่ามีความจำเป็นต้องประเมิน แต่มีข้อจำกัด หรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจตามข้อ 1. ไม่สามารถประเมินได้ เช่น การประเมิน

ระบบที่มีความซับซ้อนหรือใช้เทคโนโลยีใหม่ หรือการประเมินความสามารถของระบบในการปรับเปลี่ยนเพื่อรองรับการให้บริการหรือดำเนินธุรกิจในอนาคตภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศที่รวดเร็ว

5. ต้องจัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและเสนอผลการตรวจสอบดังกล่าวต่อคณะกรรมการตรวจสอบ ตลอดจนจัดส่งสำเนาผลการตรวจสอบให้ ธปท. เป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ตามที่กำหนด ภายใน 45 วันนับแต่วันที่ทำการตรวจสอบแล้วเสร็จ

6. ต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานประเด็นสำคัญพร้อมทั้งแผนการปรับปรุงให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้อง

เอกสารแนบ 5

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ
เรื่อง การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ
(IT project management)

เมื่อผู้ให้บริการและผู้ประกอบธุรกิจจะจัดทำโครงการด้านเทคโนโลยีสารสนเทศ (IT project management) ที่มีนัยสำคัญ ที่นำมาใช้ในการให้บริการหรือดำเนินธุรกิจ ต้องปฏิบัติตามหลักเกณฑ์ดังต่อไปนี้

1. ศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับสำหรับโครงการที่นำเทคโนโลยีสารสนเทศมาใช้ในการให้บริการหรือดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องพิจารณาเลือกใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม และประเมินความเสี่ยงตลอดจนผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งต้องจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตอำนาจอนุมัติที่กำหนดไว้

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

2.1 คณะกรรมการที่กำกับดูแลโครงการ เพื่อทำหน้าที่กำกับดูแลความคืบหน้า ให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้การดำเนินงานของโครงการเป็นไปตามแผนงานที่กำหนด ทั้งนี้ คณะกรรมการกำกับดูแลโครงการควรประกอบด้วยผู้บริหารหรือผู้แทนจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้อง

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

2.3 ผู้จัดการโครงการ (project manager) เพื่อทำหน้าที่ในการบริหารจัดการโครงการแต่ละโครงการตามขั้นตอนการบริหารจัดการโครงการ และส่งมอบงานในแต่ละขั้นตอนตามรูปแบบกระบวนการและเครื่องมือ ตามที่หน่วยงานหรือทีมงานที่ดูแลภาพรวมของโครงการกำหนด เพื่อให้สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานที่กำหนด