การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)

ขอบเขตการดำเนินการตามภาคผนวกนี้

ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ระดับปานกลาง หรือระดับสูง ให้ดำเนินการตามที่กำหนดในภาคผนวกนี้

การดำเนินการเกี่ยวกับการกำกับดูแลและบริหารจัดการด้าน IT

ส่วนที่ 1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ

ผู้ประกอบธุรกิจต้องดำเนินการให้การควบคุมดูแลการบริหารจัดการความเสี่ยงด้าน IT ผ่านการกำกับดูแลโดยคณะกรรมการของผู้ประกอบธุรกิจ เพื่อให้สอดคล้องกับระดับความเสี่ยง (ระดับความเสี่ยงที่ยอมรับได้ตามส่วนที่ 2 ข้อ 2.2.1(3)) โดยคำนึงถึงการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk) (ถ้ามี) ซึ่งอย่างน้อยต้องครอบคลุมในเรื่องดังนี้

1.1 การกำหนดกรอบการกำกับดูแล (governance framework) และการกำกับดูแลแผนงานด้าน IT ให้สอดคล้องกับแผนทางธุรกิจ และมีความเหมาะสมเพียงพอที่จะรองรับการเปลี่ยนแปลงด้าน IT และการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต

1.2 การจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคล ให้มีความเหมาะสมเพียงพอต่อการดำเนินธุรกิจ

1.3 การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ซึ่งมีการกำหนดเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องครอบคลุมนโยบายตามที่กำหนดในส่วนที่ 2 ข้อ 2.2

1.4 การกำหนดขั้นตอนและวิธีปฏิบัติงานในการบริหารจัดการความเสี่ยงด้าน IT และการรักษาความมั่นคงปลอดภัย IT เพื่อให้เป็นไปตามนโยบายใน 1.3 รวมถึงกำกับดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม

1.5 การสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT แก่กรรมการและบุคลากรอย่างต่อเนื่องและมีประสิทธิผล

1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติเพื่อให้เป็นไปตามนโยบายใน 1.3 ต่อคณะกรรมการของผู้ประกอบธุรกิจ โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจทราบโดยไม่ชักช้าด้วย

ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร

2.1 ผู้ประกอบธุรกิจต้องจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT โดยอย่างน้อยต้องมีลักษณะดังนี้

2.1.1 ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระ

2.1.2 สอดคล้องตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense: 3 LoDs) โดยมีการแบ่งแยกหน้าที่อย่างชัดเจนระหว่างการทำหน้าที่ด้าน IT ดังนี้

ระดับที่ 1 (first line of defense) : การปฏิบัติงาน

ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

ระดับที่ 3 (third line of defense) : การตรวจสอบ

2.2 ผู้ประกอบธุรกิจต้องให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ ดังนี้

นโยบาย	เรื่องที่ต้องครอบคลุม
2.2.1 นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy)	(1) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้าน IT (2) เกณฑ์ความเสี่ยง (risk criteria) โดยครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้นเพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง (3) ระดับความเสี่ยงที่ยอมรับได้ (risk appetite) (4) การประเมินความเสี่ยง (risk assessment) ที่ครอบคลุมความเสี่ยงด้าน IT และการคุ้มครองข้อมูลส่วนบุคคลจากการใช้งาน IT (5) การจัดการความเสี่ยง (risk treatment) ให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (6) การจัดทำทะเบียนความเสี่ยง (risk register) (7) การติดตามและทบทวนความเสี่ยง (risk monitor and review) (8) การรายงานความเสี่ยง (risk reporting) และผลการบริหารจัดการความเสี่ยงด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ อย่างน้อยปีละ 1 ครั้ง
2.2.2 นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy)	(1) โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security) (2) การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT หรือบุคคลภายนอก

นโยบาย	เรื่องที่ต้องครอบคลุม
	(3) การบริหารจัดการทรัพย์สินด้าน IT (IT Asset Management) (4) การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) (5) การควบคุมการเข้าถึงและระบบ IT (access control) (6) การควบคุมการเข้ารหัส (Cryptographic control) (7) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) (8) มาตรการรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security) (9) มาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security) (10) การบริหารจัดการโครงการด้าน IT และการจัดหา พัฒนาและบำรุงรักษาระบบ IT (IT Project Management, and System Acquisition, Development and Maintenance) (11) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT (IT Incident Management) (12) การจัดทำแผนฉุกเฉินด้าน IT (IT Contingency Plan)

2.3 ผู้ประกอบธุรกิจต้องจัดให้มีการดำเนินการตามนโยบายใน 2.2 ดังนี้

2.3.1 เปิดเผยนโยบายตาม 2.2 ในลักษณะที่สามารถเข้าถึงได้ง่าย และสื่อสารให้แก่บุคคลที่เกี่ยวข้อง[1] รับทราบอย่างทั่วถึง เพื่อให้บุคคลดังกล่าวเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง

2.3.2 กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายตาม 2.2

2.3.3 ในกรณีที่มีการเปลี่ยนแปลงนโยบายดังกล่าว ต้องสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องการเปลี่ยนแปลงดังกล่าว

2.4 ผู้ประกอบธุรกิจต้องทบทวนหรือปรับปรุงนโยบายตาม 2.2 อย่างน้อยปีละ 1 ครั้ง หรือโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT อย่างมีนัยสำคัญ

[1] บุคคลที่เกี่ยวข้อง หมายความว่า บุคลากร กรรมการ รวมถึงบุคคลภายนอก