การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)

ให้ผู้ประกอบธุรกิจดำเนินการตามที่กำหนดในภาคผนวกนี้

การดำเนินการ	รายละเอียดในการดำเนินการ
๑. การจัดให้มีผู้ตรวจสอบ	ผู้ตรวจสอบตามข้อ ๑. ต้องมีลักษณะดังนี้ ๑.๑ มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ ดังนี้ ๑.๑.๑ ระดับที่ ๑ (first line of defense) : การปฏิบัติงาน ๑.๑.๒ ระดับที่ ๒ (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง ๑.๒ ในกรณีที่เป็นการตรวจสอบด้าน IT ตั้งแต่วันที่ ๑ มกราคม พ.ศ. ๒๕๖๗ เป็นต้นไป ผู้ตรวจสอบต้องผ่านการรับรองและมีวุฒิบัตรอย่างหนึ่งอย่างใดดังนี้ ๑.๒.๑ Certified Information Systems Auditor (CISA) ๑.๒.๒ Certified Information Security Manager (CISM) ๑.๒.๓ Certified Information Systems Security Professional (CISSP) ๑.๒.๔ ISO/IEC ๒๗๐๐๑ Lead Auditor ๑.๒.๕ ใบรับรองอื่นตามที่กำหนดเพิ่มเติมบนเว็บไซต์ของสำนักงาน
๒. การวางแผนและกำหนดขอบเขตการตรวจสอบ	ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้าน IT และประกาศที่ สธ. ๓๘/๒๕๖๕ โดยต้องดำเนินการอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนดังกล่าว
๓. การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด	๓.๑ จัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT โดยมีรายละเอียดดังนี้ ๓.๑.๑ กรณีเป็นผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจขนาดเล็ก แบบเต็มรูปแบบ (full scope) อย่างน้อยทุก ๓ ปี ตามรอบปีที่สำนักงานกำหนด ๓.๑.๒ กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ แบบเต็มรูปแบบ (full scope) อย่างน้อยทุก ๓ ปี ตามรอบปีที่สำนักงานกำหนด ทั้งนี้ กรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจขนาดเล็กและผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ดังกล่าว กรณีที่มีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจขนาดเล็กหรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายใน

การดำเนินการ	รายละเอียดในการดำเนินการ
	ปีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจต้องดำเนินการดังต่อไปนี้ ภายใน ๔ เดือน นับแต่วันที่ทราบเหตุการณ์ดังกล่าว (๑) รายงานเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ได้ภายในปีที่เกิดเหตุการณ์ดังกล่าว และแผนการตรวจสอบด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ รวมทั้งรายงานเหตุจำเป็นดังกล่าวต่อสำนักงาน และ (๒) ดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ๓.๑.๓ กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง แบบเต็มรูปแบบ (full scope) อย่างน้อยปีละ ๑ ครั้ง ๓.๑.๔ กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง แบบเต็มรูปแบบ (full scope) อย่างน้อยปีละ ๑ ครั้ง ๓.๒ จัดให้มีการบันทึกข้อมูลเกี่ยวกับการตรวจสอบ เช่น กระดาษทำการ (working paper) และหลักฐานประกอบการตรวจ เป็นต้น เป็นระยะเวลาไม่น้อยกว่า ๒ ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า
๔. การจัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT และการติดตามความคืบหน้า	จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT ตามข้อ ๓. ที่เหมาะสมกับความเสี่ยงจากข้อบกพร่อง และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าว
๕. การจัดทำและรายงานผลการตรวจสอบ	๕.๑ เสนอรายงานผลการตรวจสอบตามข้อ ๓. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ โดยไม่ชักช้า

การดำเนินการ	รายละเอียดในการดำเนินการ
	๕.๒[๑] รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ ตามข้อ ๕.๑ ต่อสำนักงาน ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายใน ๓ เดือน นับแต่วันสิ้นปีปฏิทินของปีที่ดำเนินการตรวจสอบตามข้อ ๓. เว้นแต่ในกรณีที่เป็นผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่มีหน้าที่ต้องรายงานผลการตรวจสอบตามประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. ๑๙/๒๕๖๑ เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๑ ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลปฏิบัติตามประกาศดังกล่าว ๕.๓ จัดเก็บรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องเป็นระยะเวลาไม่น้อยกว่า ๒ ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

[๑] เว้นแต่กรณีเป็นผู้ประกอบธุรกิจที่เป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ซึ่งได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ดังนี้ โดยไม่ได้มีการประกอบธุรกิจหลักทรัพย์ประเภทอื่น โดยให้ได้รับยกเว้นการดำเนินการตามข้อ ๕.๒

๑. การเป็นนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ และการจัดจำหน่ายขายหลักทรัพย์อันเป็นตราสารแห่งหนี้ หรือ

๒. กิจการการยืมและให้ยืมหลักทรัพย์