ภาคผนวก 4

[แนบท้ายประกาศที่ สธ. 38/2565]

<u>การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)</u>

ให้ผู้ประกอบธุรกิจดำเนินการตามที่กำหนดในภาคผนวกนี้

การดำเนินการ	รายละเอียดในการดำเนินการ
1. การจัดให้มีผู้ตรวจสอบ	ผู้ตรวจสอบตามข้อ 1. ต้องมีลักษณะดังนี้ 1.1 มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ ดังนี้ 1.1.1 ระดับที่ 1 (first line of defense) : การปฏิบัติงาน 1.1.2 ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง 1.2 ในกรณีที่เป็นการตรวจสอบด้าน IT ตั้งแต่วันที่ 1 มกราคม พ.ศ. 2567 เป็นต้นไป ผู้ตรวจสอบต้องผ่านการรับรองและมีวุฒิบัตรอย่างหนึ่งอย่างใดดังนี้ 1.2.1 Certified Information Systems Auditor (CISA) 1.2.2 Certified Information Security Manager (CISM) 1.2.3 Certified Information Systems Security Professional (CISSP) 1.2.4 ISO/IEC 27001 Lead Auditor 1.2.5 ใบรับรองอื่นตามที่กำหนดเพิ่มเติมบนเว็บไซต์ของสำนักงาน
2. การวางแผนและกำหนดขอบเขตการตรวจสอบ	ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้าน IT และประกาศที่ สธ. 38/2565 โดยต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนดังกล่าว
3. การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด	3.1 จัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT โดยมีรายละเอียดดังนี้ 3.1.1 กรณีเป็นผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจขนาดเล็ก อย่างน้อยทุก 2 ปี 3.1.2 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบแบบเต็มรูปแบบ (full scope) ที่ครอบคลุมหลักเกณฑ์ทั้งหมด อย่างน้อยทุก 2 ปี 3.1.3 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลางหรือหรือระดับสูง ต้องจัดให้มีการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ที่ครอบคลุมหลักเกณฑ์ทั้งหมด อย่างน้อยปีละ 1 ครั้ง 3.2 จัดให้มีการบันทึกข้อมูลเกี่ยวกับการตรวจสอบ เช่น กระดาษทำการ (working paper) และหลักฐานประกอบการตรวจ เป็นต้น เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่

การดำเนินการ	รายละเอียดในการดำเนินการ
	จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า
4. การจัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT และการติดตามความคืบหน้า	จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT ตามข้อ 3. ที่เหมาะสมกับความเสี่ยงจากข้อบกพร่อง และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าว
5. การจัดทำและรายงานผลการตรวจสอบ	5.1 เสนอรายงานผลการตรวจสอบตามข้อ 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจโดยไม่ชักช้า 5.2[1] รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจตามข้อ 5.1 ต่อสำนักงานตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายในระยะเวลาดังนี้ แล้วแต่ระยะเวลาใดจะครบกำหนดก่อน * 5.2.1 30 วัน นับแต่วันที่เสนอรายงานและแผนดังกล่าวต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ 5.2.2 90 วัน นับแต่วันที่สิ้นสุดการตรวจสอบตามข้อ 3. 5.2.3 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบตามข้อ 3. กรณีที่ไม่สามารถจัดทำรายงานผลการตรวจสอบให้เสร็จสิ้นภายในปีที่เริ่มการตรวจสอบ (* หมายเหตุ สำหรับการรายงานผลการตรวจสอบรอบปี พ.ศ. 2566 ให้ผู้ประกอบธุรกิจรายงานภายใน 3 เดือนนับแต่วันสิ้นปีปฏิทินของปี พ.ศ. 2566) 5.3 จัดเก็บรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

[1] เว้นแต่กรณีเป็นผู้ประกอบธุรกิจที่เป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ซึ่งได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ดังนี้ โดยไม่ได้มีการประกอบธุรกิจหลักทรัพย์ประเภทอื่น โดยให้ได้รับยกเว้นการดำเนินการตามข้อ 5.2

1. การเป็นนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ และการจัดจำหน่ายขายหลักทรัพย์อันเป็นตราสารแห่งหนี้ หรือ
2. กิจการการยืมและให้ยืมหลักทรัพย์