[แนบท้ายประกาศที่ สธ. /25]

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

ให้ผู้ประกอบธุรกิจดำเนินการตามที่กำหนดในภาคผนวกนี้

การดำเนินการ	รายละเอียดในการดำเนินการ
1. การจัดให้มีผู้ตรวจสอบ	ผู้ตรวจสอบตาม 1. ต้องมีลักษณะดังนี้ 1.1 ผ่านการรับรองและมีวุฒิบัตรอย่างหนึ่งอย่างใดดังนี้ 1.1.1 Certified Information Systems Auditor (CISA) 1.1.2 Certified Information Security Manager (CISM) 1.1.3 Certified Information Systems Security Professional (CISSP) 1.1.4 ISO/IEC 27001 Lead Auditor 1.1.5 ใบรับรองอื่นตามที่กำหนดเพิ่มเติมบนเว็บไซต์ของสำนักงาน 1.2 มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ ดังนี้ 1.2.1 ระดับที่ 1 (first line of defense) : การปฏิบัติงาน 1.2.2 ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
2. การวางแผนและกำหนดขอบเขตการตรวจสอบ	ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้าน IT และประกาศที่ สธ..... โดยต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนดังกล่าว
3. การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด	จัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยมีรายละเอียดดังนี้ 3.1 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบแบบเต็มรูปแบบ (full scope) ที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุมอย่างน้อยทุก 2 ปี 3.2 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลางหรือหรือระดับสูง ต้องจัดให้มีการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุม อย่างน้อยปีละ 1 ครั้ง 3.3 กรณีเป็นผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบตามการรักษาความมั่นคงปลอดภัยของระบบ IT ขั้นต้นที่จำเป็น ที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุมอย่างน้อยทุก 2 ปี

การดำเนินการ	รายละเอียดในการดำเนินการ
4. จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบ และการติดตามความคืบหน้า	จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องที่พบจากการตรวจสอบด้าน IT ตาม 3. และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าว โดยไม่ชักช้า
5. การจัดทำและรายงานผลการตรวจสอบ	5.1 เสนอรายงานผลการตรวจสอบตาม 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจโดยไม่ชักช้า 5.2 รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่อง ที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจตาม 5.1 พร้อมทั้งเอกสารรับรองผลการพิจารณาดังกล่าว ต่อสำนักงานตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายใน 30 วันนับแต่วันที่เสนอรายงานและแผนดังกล่าวต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ แต่ต้องไม่เกินกว่าระยะเวลาดังนี้ แล้วแต่ระยะเวลาใดจะครบกำหนดก่อน 5.2.1 90 วันนับแต่วันที่สิ้นสุดการตรวจสอบตาม 3. 5.2.2 3 เดือนนับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบตาม 3. กรณีที่ไม่สามารถจัดทำรายงานผลการตรวจสอบให้เสร็จสิ้นภายในปีที่เริ่มการตรวจสอบ 5.3 จัดเก็บรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า