ประกาศคณะกรรมการการมาตรฐานแห่งชาติ

ฉบับที่ ๓ (พ.ศ. ๒๕๕๙)

เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการกำหนดสาขาและขอบข่าย และการสุ่มตัวอย่าง เพื่อการรับรองระบบงานหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๒๐ วรรคสาม และมาตรา ๒๘ วรรคสอง แห่งพระราชบัญญัติการมาตรฐานแห่งชาติ พ.ศ. ๒๕๕๑ และมติคณะอนุกรรมการพิจารณาหลักเกณฑ์ วิธีการ และเงื่อนไขในการประชุมครั้งที่ ๑๓-๑/๒๕๕๙ เมื่อวันที่ ๒๐ เมษายน ๒๕๕๙ คณะกรรมการการมาตรฐานแห่งชาติออกประกาศกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขการกำหนดสาขาและขอบข่าย และการสุ่มตัวอย่างเพื่อการรับรองระบบงานหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ ดังมีรายละเอียดต่อท้ายประกาศนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๗ กรกฎาคม พ.ศ. ๒๕๕๙

สมคิด จาตุศรีพิทักษ์

รองนายกรัฐมนตรี

ประธานกรรมการการมาตรฐานแห่งชาติ

หลักเกณฑ์ วิธีการ และเงื่อนไข
การกำหนดสาขาและขอบข่าย และการสุ่มตัวอย่าง
เพื่อการรับรองระบบงานหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ

๑. ขอบข่าย

เอกสารนี้ กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการกำหนดสาขาและขอบข่าย และจำนวนตัวอย่างที่จะตรวจประเมินความสามารถผู้ประเมินของหน่วยรับรองขณะตรวจประเมินผู้ประกอบกิจการที่ขอรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ

๒. เอกสารอ้างอิง

๒.๑ หลักเกณฑ์ วิธีการ และเงื่อนไขการรับรองระบบงานหน่วยรับรอง

๒.๒ หลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินหน่วยรับรอง

๒.๓ ประกาศกำหนดสาขาการตรวจสอบและรับรองสำหรับหน่วยรับรองและหน่วยตรวจ

๒.๔ มอก. 2000 การจัดประเภทอุตสาหกรรมตามกิจกรรมทางเศรษฐกิจทุกประเภทตามมาตรฐานสากล

๒.๕ ISO/IEC 27006 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

๓. นิยาม

ความหมายของคำที่ใช้ในเอกสารนี้ให้เป็นไปตามนิยามที่กำหนดไว้ในหลักเกณฑ์ วิธีการ และเงื่อนไขการรับรองระบบงานหน่วยรับรอง และนิยามดังต่อไปนี้

๓.๑ สาขาและขอบข่ายทั่วไป หมายถึง กิจกรรมที่มีกระบวนการในการดำเนินงานไม่ซับซ้อน หรือใช้เทคโนโลยีพื้นฐาน และไม่ต้องใช้ความรู้ความชำนาญเฉพาะด้าน และ/หรือ กิจกรรมที่มีผลกระทบ และ/หรือ ความเสี่ยงต่อเศรษฐกิจ สังคม และความมั่นคงปลอดภัยด้านสารสนเทศไม่มาก

๓.๒ สาขาและขอบข่ายเฉพาะ หมายถึง กิจกรรมที่มีกระบวนการในการดำเนินงานซับซ้อน หรือใช้เทคโนโลยีขั้นสูง และต้องใช้ความรู้ความชำนาญเฉพาะด้านสูง และ/หรือ กิจกรรมที่มีผลกระทบ และ/หรือ ความเสี่ยงต่อเศรษฐกิจ สังคม และความมั่นคงปลอดภัยด้านสารสนเทศมาก

๔. การกำหนดสาขาและขอบข่าย

การกำหนดสาขาและขอบข่ายในการรับรองระบบงานหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศจะอ้างอิงตามการแบ่งประเภทอุตสาหกรรมตามกิจกรรมทางเศรษฐกิจ (หมวด A-Q) ตามมาตรฐาน มอก. 2000 และ Annex A ของ ISO/IEC 27006 โดยจำแนกสาขาและขอบข่ายเป็น ๒ กลุ่ม คือ สาขาและขอบข่ายทั่วไป และสาขาและขอบข่ายเฉพาะ รายละเอียดดังตารางที่ ๑ และ ๒ ตามลำดับ

ตารางที่ ๑ สาขาและขอบข่ายทั่วไป

หมวด	กิจกรรมทางเศรษฐกิจ
A	เกษตรกรรม การล่าสัตว์ และการป่าไม้
B	การประมง
C	การทำเหมืองแร่และเหมืองหิน
D	การผลิต ยกเว้น - การพิมพ์สิ่งพิมพ์ป้องกันการปลอมแปลง (Security Printing) - การผลิตถ่านหิน ผลิตภัณฑ์ปิโตรเลียมที่ผ่านการกลั่น และเชื้อเพลิงนิวเคลียร์ - การผลิตอาวุธและกระสุน - การผลิตอากาศยานและยานอวกาศ
F	การก่อสร้าง
G	การขายส่ง การขายปลีก การซ่อมแซมยานยนต์ รถจักรยานยนต์ ของใช้ส่วนบุคคล และของใช้ภายในบ้าน
H	โรงแรมและภัตตาคาร
I	กิจกรรมสนับสนุนและช่วยเหลือเกี่ยวกับการขนส่ง กิจกรรมของตัวแทนการท่องเที่ยว ยกเว้น สถานที่เก็บสินค้าประเภทก๊าซและน้ำมัน สารเคมี
K	การค้าอสังหาริมทรัพย์ การให้เช่า และกิจกรรมทางธุรกิจ ยกเว้น คอมพิวเตอร์และกิจกรรมที่เกี่ยวข้อง
O	การบริการชุมชน สังคม และการบริการส่วนบุคคลอื่นๆ ยกเว้น การกระจายเสียงทางวิทยุ และแพร่ภาพทางโทรทัศน์
P	บ้านส่วนบุคคลพร้อมลูกจ้าง

ตารางที่ ๒ สาขาและขอบข่ายเฉพาะ

หมวด	กิจกรรมทางเศรษฐกิจ
D	การพิมพ์สิ่งพิมพ์ป้องกันการปลอมแปลง (Security Printing)
D	การผลิตถ่านหิน ผลิตภัณฑ์ปิโตรเลียมที่ผ่านการกลั่น และเชื้อเพลิงนิวเคลียร์
D	การผลิตอาวุธและกระสุน
D	การผลิตอากาศยานและยานอวกาศ
E	การไฟฟ้า ก๊าซ และน้ำ
I	การขนส่งทางบก การขนส่งทางท่อ
I	การขนส่งทางน้ำ
I	การขนส่งทางอากาศ

หมวด	กิจกรรมทางเศรษฐกิจ
I	การไปรษณีย์และการโทรคมนาคม
I	สถานที่เก็บสินค้าประเภทก๊าซและน้ำมัน สารเคมี
J	การเป็นตัวกลางทางการเงิน
K	กิจกรรมด้านคอมพิวเตอร์และกิจกรรมที่เกี่ยวข้อง
L	การบริหารราชการและการป้องกันประเทศ การประกันสังคมแบบบังคับ
M	การศึกษา
N	การบริการเกี่ยวกับสุขภาพและสังคมสงเคราะห์
O	การกระจายเสียงทางวิทยุ และแพร่ภาพทางโทรทัศน์

หมายเหตุ มอก. 2000 แบ่งประเภทอุตสาหกรรมตามกิจกรรมทางเศรษฐกิจของผลิตภัณฑ์และการบริการ โดยแบ่งเป็นหมวด A – หมวด Q ทั้งนี้ หมวด Q กิจกรรมองค์การระหว่างประเทศและองค์การต่างประเทศอื่นๆ และสมาชิก เป็นสาขาและขอบข่ายที่ไม่ให้การรับรองระบบงาน

๕. การสุ่มตัวอย่าง

๕.๑ สำนักงานจะพิจารณาตรวจประเมินความสามารถผู้ประเมินของหน่วยรับรองขณะตรวจประเมินผู้ประกอบกิจการ (Witnessing) ชนิดเต็มรูปแบบ (หน่วยรับรองประเมินเพื่อให้การรับรองครั้งแรก หรือประเมินใหม่) เป็นลำดับแรก

ผู้ประเมินของหน่วยรับรองครอบคลุมทั้ง ผู้ประเมินที่เป็นบุคลากรประจำ (Full-time staff) และผู้ประเมินที่ไม่ใช่บุคลากรประจำ (Part-time staff)

๕.๒ สำนักงานสามารถเลือกสาขาและขอบข่ายและผู้ประเมินที่จะตรวจประเมินความสามารถได้ตามความเหมาะสม รวมถึงสำนักงานสงวนสิทธิ์ในการพิจารณาเลือกตัวอย่างที่มีนัยสำคัญต่อผลกระทบ และ/หรือความเสี่ยงต่อความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้เป็นตัวแทนสาขาและขอบข่ายที่ขอรับการรับรองระบบงาน

๕.๓ การสุ่มตัวอย่างการ Witnessing ในแต่ละกรณี ให้เป็นดังนี้

๕.๓.๑ การรับรองระบบงานครั้งแรก

๑) สาขาและขอบข่ายทั่วไป

สุ่มตัวอย่างอย่างน้อย ๑ ตัวอย่าง โดยพิจารณาจาก

- จำนวนผู้ประกอบกิจการที่ได้รับการรับรองจากหน่วยรับรอง
- จำนวนผู้ประเมินของหน่วยรับรอง
- ผลการดำเนินงานของหน่วยรับรอง และข้อมูลที่เกี่ยวข้องกับผลการดำเนินงานของผู้ประกอบกิจการที่ได้รับการรับรอง

๒) สาขาและขอบข่ายเฉพาะ

สุ่มตัวอย่างอย่างน้อยร้อยละ ๒๐ ของจำนวนสาขาและขอบข่ายเฉพาะที่ขอการรับรองระบบงาน เศษที่เหลือให้ปัดขึ้นเป็นจำนวนเต็ม

๕.๓.๒ การขอขยายสาขาและขอบข่ายการรับรองระบบงาน การสุ่มตัวอย่างให้ใช้หลักเกณฑ์ตามข้อ ๕.๓.๑ โดยอนุโลม

๕.๓.๓ การตรวจติดตามผล

สุ่มตัวอย่างอย่างน้อย ๑ ตัวอย่าง โดยพิจารณาจาก

- จำนวนผู้ประกอบกิจการที่ได้รับการรับรองจากหน่วยรับรอง
- จำนวนผู้ประเมินของหน่วยรับรอง
- ผลการดำเนินงานของหน่วยรับรอง และข้อมูลที่เกี่ยวข้องกับผลการดำเนินงานของผู้ประกอบกิจการที่ได้รับการรับรอง

๕.๓.๔ การต่ออายุการรับรองระบบงาน

สุ่มตัวอย่างตามจำนวนที่ระบุในตารางที่ ๓ โดยพิจารณาจากจำนวนผู้ประกอบกิจการที่ได้รับการรับรองกิจกรรมจากหน่วยรับรอง

ตารางที่ ๓ จำนวนตัวอย่าง กรณีการต่ออายุการรับรองระบบงาน

จำนวนผู้ประกอบกิจการที่ได้รับการรับรองกิจกรรมจากหน่วยรับรอง	**จำนวนตัวอย่าง**
๑ – ๕๐	อย่างน้อย ๑
๕๑ – ๑๐๐	อย่างน้อย ๒
มากกว่า ๑๐๐	อย่างน้อย ๓

๕.๔ หากหน่วยรับรองไม่สามารถจัดสรรการประเมินชนิดเต็มรูปแบบตามข้างต้นได้ สำนักงานอาจพิจารณา Witnessing การตรวจติดตามผล (Surveillance) โดยจำนวนตัวอย่างจะเป็น ๒ เท่าของชนิดเต็มรูปแบบ และการตรวจติดตามผลในแต่ละครั้งต้องครอบคลุมกระบวนการหลักของผู้ประกอบกิจการ
