ข้อมูลเพิ่มเติมประกอบการตรวจรับรอง ตามมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่าย ระบบบาทเนตตามแนวมาตรฐาน ISO/IEC 27001

---

1. เหตุผลและการพิจารณานำมาใช้

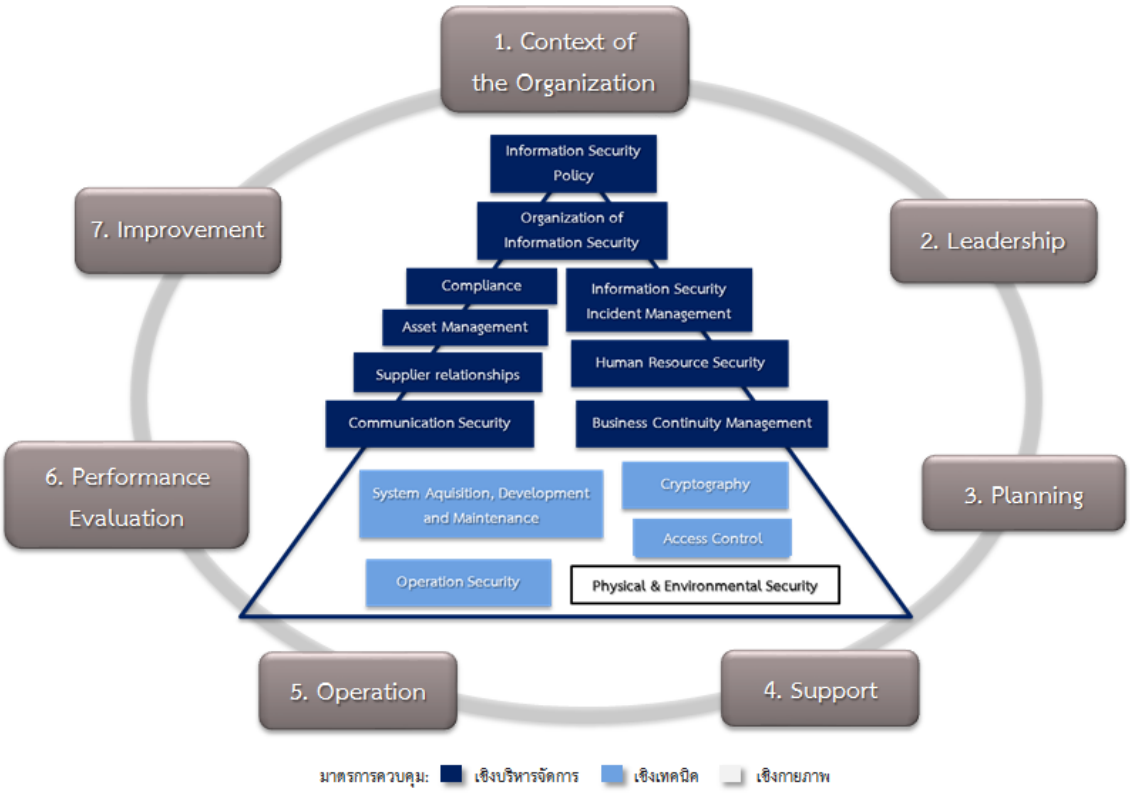
จากประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต กำหนดให้คอมพิวเตอร์ลูกข่ายระบบบาทเนตต้องผ่านการตรวจรับรองตามแนวมาตรฐาน ISO/IEC 27001

ธนาคารแห่งประเทศไทย (ธปท.) จัดทำเอกสารฉบับนี้ขึ้น เพื่อเป็นข้อมูลประกอบสำหรับผู้ใช้บริการบาทเนตทุกราย ทั้งที่เป็นสถาบันการเงินและไม่ใช่สถาบันการเงินในการดำเนินการตรวจรับรองตามประกาศฯ

2. เนื้อหา

2.1 มาตรฐาน ISO/IEC 27001

การขอรับรองตามมาตรฐาน ISO/IEC 27001 ต้องดำเนินการตามข้อกำหนดหลัก 7 เรื่อง ครอบคลุมมาตรการควบคุมทั้งหมด 14 หัวข้อ โดยสามารถแบ่งออกเป็น 3 ด้าน ได้แก่ เชิงบริหารจัดการ เชิงระบบ และเชิงกายภาพ ดังภาพที่ 1



ภาพที่ 1 มาตรการบริหารจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001

ข้อกำหนดหลัก 7 เรื่อง

1. บริบทขององค์กร (Context of the Organization)
2. ภาวะผู้นำ (Leadership)
3. การวางแผน (Planning)
4. การสนับสนุน (Support)
5. การดำเนินการ (Operation)
6. การประเมินประสิทธิภาพและประสิทธิผล (Performance Evaluation)
7. การปรับปรุง (Improvement)

มาตรการควบคุม 14 หัวข้อ

1. นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information security policies)
2. โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร (Organization of information security)
3. ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบุคลากร (Human resource security)
4. การบริหารจัดการทรัพย์สิน (Asset management)
5. การควบคุมการเข้าถึง (Access control)
6. การเข้ารหัสข้อมูล (Cryptography)
7. ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)
8. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านการดำเนินการ (Operations security)
9. ความมั่นคงปลอดภัยทางด้านการสื่อสาร (Communications security)
10. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)
11. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
12. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสนเทศ (Information security incident management)
13. ประเด็นด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)
14. การปฏิบัติตามข้อกำหนด (Compliance)

2.2 ขอบเขต

ขอบเขตของการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ของผู้ใช้บริการบาทเนต เกี่ยวข้องกับบริบทองค์กรและการบริหารจัดการความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ลูกข่ายระบบบาทเนตในส่วนที่มีการเชื่อมต่อโดยตรงมาที่ ธปท. ซึ่งจะครอบคลุมตั้งแต่ระดับ ความมั่นคงทางกายภาพ ระบบงานโปรแกรมที่เกี่ยวข้อง ข้อมูล อุปกรณ์ และการบริหารจัดการเทคโนโลยีสารสนเทศ ทั้งนี้ ผู้ใช้บริการบาทเนตจะต้องพิจารณาความเสี่ยงของสินทรัพย์สารสนเทศที่เกี่ยวข้อง โดยมีตัวอย่างดังนี้

1) **กระบวนการทำงาน (Process)**
   กระบวนการ กระบวนการย่อย หรือกิจกรรมที่สำคัญที่หากแก้ไข เสียหาย สูญเสียไปแล้วจะมีผลต่อการปฏิบัติงานตามภารกิจของผู้ใช้บริการบาทเนต
2) **ข้อมูลและสารสนเทศ (Information)**
   ข้อมูลสำคัญในระบบสารสนเทศ สารสนเทศที่เป็นข้อมูลบุคคล สารสนเทศที่เป็นข้อมูลเกี่ยวกับยุทธศาสตร์ หรือกลยุทธ์ขององค์กร สารสนเทศที่สำคัญที่มีมูลค่าสูงที่ต้องจัดเก็บรักษา
3) **ฮาร์ดแวร์ (Hardware)**
   อุปกรณ์ที่เกี่ยวข้องในการใช้บริการระบบบาทเนตสำหรับชุดปฏิบัติงานจริงและชุดสำรองที่เชื่อมต่อกับ ธปท. โดยตรง เช่น Gateway Server สำหรับการเชื่อมโยงแบบ Host to Host และเครื่องคอมพิวเตอร์สำหรับการส่งข้อความผ่าน EFS (BAHTNET) เป็นต้น
4) **ซอฟต์แวร์ (Software)**
   ซอฟต์แวร์ที่ผู้ใช้บริการบาทเนตจำเป็นต้องมีเพื่อใช้งานระบบบาทเนต และซอฟต์แวร์สนับสนุนอื่น ๆ เช่น Operating System, Web Browser, PDF Reader และซอฟต์แวร์ Antivirus เป็นต้น
5) **เครือข่ายคอมพิวเตอร์ (Network)**
   เครือข่ายคอมพิวเตอร์ ที่เกี่ยวข้องกับกับการเชื่อมโยงของเครื่องลูกข่ายของระบบบาทเนตภายใต้การดูแลขององค์กร
6) **เครื่องแม่ข่ายเสมือน (Virtual Machine)**
   เครื่องแม่ข่ายเสมือนที่เกี่ยวข้องกับการใช้บริการระบบบาทเนตผ่านคอมพิวเตอร์ลูกข่าย รวมทั้งเครื่องแม่ข่ายเสมือนของระบบที่เกี่ยวข้องกับการบริหารจัดการ และการบำรุงรักษา
7) **บุคลากร (Personnel)**
   บุคลากรที่เกี่ยวข้องกับการดำเนินกิจกรรมด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ผู้ใช้งานระบบบาทเนต ครอบคลุมทั้งพนักงานของผู้ใช้บริการบาทเนตและบุคลากรของผู้ให้บริการภายนอก (Outsource) ซึ่งปฏิบัติงานในสถานที่ของผู้ใช้บริการบาทเนต เป็นต้น
8) **สถานที่และระบบสนับสนุน (Site)**
   อาคาร สถานที่ตั้ง ศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง สิ่งแวดล้อมภายนอก และทางกายภาพ พื้นที่การแบ่งเขตโซนภายในสถานที่ ระบบสนับสนุนในการดูแลอาคารสถานที่ อุปกรณ์เครื่องมือสนับสนุนต่าง ๆ

9) **องค์กร (Organization)**

โครงสร้างขององค์กร ตลอดจนผู้ให้บริการภายนอก ที่เกี่ยวข้องกับการใช้งานคอมพิวเตอร์ลูกข่ายระบบบาทเนต

สิ่งที่ไม่เกี่ยวข้องในขอบเขต

1) ระบบงานภายในอื่น ๆ ของผู้ใช้บริการบาทเนต
2) เครือข่ายคอมพิวเตอร์ระหว่างผู้ใช้บริการบาทเนต กับ ธปท. ที่กำกับดูแลโดยผู้ให้บริการภายนอก (อุปกรณ์ของผู้ให้บริการภายนอก)
3) ระบบหรืออุปกรณ์ที่อยู่ภายใต้การบริหารจัดการของ ธปท.

ขอบเขตของการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ของผู้ใช้บริการบาทเนต สามารถสรุปได้ดังภาพที่ 2

ภาพที่ 2 ขอบเขตของการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ของผู้ใช้บริการบาทเนต

3. การรายงานผลการตรวจประเมินหรือตรวจรับรอง

เมื่อผู้ใช้บริการบาทเนตผ่านการตรวจประเมินและตรวจรับรอง ISO/IEC 27001 แล้ว ให้จัดส่งสำเนาเอกสารที่ได้รับจากการดำเนินการดังกล่าว มาที่ ธปท. ดังนี้

3.1 กรณีที่ผ่านการตรวจรับรองภายในปี 2560

1) นำส่งรายงานผลการตรวจรับรอง และประกาศนียบัตรรับรอง สามารถส่งแยกกันได้

2) กรณีรักษาสภาพ หากเป็นรอบการตรวจ Surveillance ให้ส่งเฉพาะรายงานผลการตรวจรับรองได้

3.2 กรณีผ่านการตรวจประเมินภายในปี 2560 และผ่านการตรวจรับรองภายใน ปี 2561

1) ปี 2560 : นำส่งรายงานการตรวจประเมิน

2) ปี 2561 : ใช้หลักเกณฑ์เช่นเดียวกับข้อ 3.1