ตารางที่ 1การระบุขอบเขตตามมาตรฐาน ISO/IEC 2700 11หัวข้อ

ISO/IEC 27001: ขอบเขตของการระบุความเสี่ยง
1.Security Policy-A5 (นโยบายการรักษาความปลอดภัย)
วัตถุประสงค์
1.1 A 5.1สนับสนุนการรักษาความปลอดภัยข้อมูล
1.2 A 5.2ทบทวนการรักษาความปลอดภัยข้อมูลอย่างน้อยปีละ 1 ครั้ง
2.Organizing Information Security-A6 (การจัดโครงสร้างระบบการรักษาด้านความปลอดภัยขององค์กร)
วัตถุประสงค์ เพื่อการบริหารความปลอดภัยของข้อมูลภายในองค์กร
2.1 A.6.1.5การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements
2.2 A 6.1.6 ควบคุมการเข้าถึงข้อมูลที่มีชั้นความลับ
3. Asset Management – A7 (การจัดการทรัพย์สิน)
วัตถุประสงค์ เพื่อบริหารจัดการทรัพย์สินให้เกิดความปลอดภัย
3.1 A 7.1.1การควบคุมการเข้า –ออก (Physical entry Control)
3.2 A7.1.2การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of Assets)
3.3 A7.1.5 การมีข้อตกลงในการรักษาความลับ
3.4 A 7.3.2กำหนดเกณฑ์ในการแยกหมวดหมู่ให้ชัดเจน (Classification)

ตารางที่ 1 (ต่อ)

ISO/IEC 27001: ขอบเขตของการระบุความเสี่ยง
4. Human Resource Security- A8 (การรักษาความปลอดภัยในระดับบุคลากร)
วัตถุประสงค์การบริหารจัดการสิทธิในการเข้าถึง/การใช้บ
4.1 A.8.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)
4.2 A.8.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)
4.3 A.8.2.2 การสร้างความตระหนักการให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)
4.4 A.8.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)
4.5 A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)
5. Physical and Environmental Security- A9 (การรักษาความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม)
วัตถุประสงค์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
5.1 A 9.1.2 การควบคุมการเข้า – ออก (Physical entry Control)
5.2 A 9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment Security)
5.3 A 9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)
5.4 A9.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal of re-use of equipment)
5.5 A9.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)

ตารางที่ 1 (ต่อ)

ISO/IEC 27001: ขอบเขตของการระบุความเสี่ยง
6.Communication and Operations Management- A10 (การสื่อสารและการบริหารการปฏิบัติงาน)
วัตถุประสงค์ป้องกันการให้บริการทางเครือข่าย
6.1 A 10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating Procedures)
6.2 A 10.1.2การควบคุมการเปลี่ยนแปลง
6.3 A10.3.1การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)
6.4 A10.4.1การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)
6.5A10.5.1การสำรองข้อมูล (Information Back-up)
6.6 A10.6.1มาตรการทางเครือข่าย (Network controls)
6.7 A10.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system us
7. Access Control – A11 (การควบคุมการเข้าถึงระบบ) มีจุดมุ่งหมายเพื่อควบคุมการเข้าถึงข้อมูลป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
7.1 A11.2.1 การลงทะเบียนพนักงาน (User registration)
7.2 A11.5.2การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)
7.2 A11.5.4การใช้งานโปรแกรมประเภทยูทิลิตี้(Use of System Utilities)
7.3 A11.5.5การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

ตารางที่ 1 (ต่อ)

ISO/IEC 27001: ขอบเขตของการระบุความเสี่ยง
8. Information systems acquisition, development and maintenance-A12 (การดูแลและพัฒนาระบบ) มีวัตถุประสงค์ดังนี้
8.1A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)
8.2A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)
8.3A.12.5.1ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)
ต 8.4A.12.6.1มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)
า9. Information security incident management-A13 (การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย) ซึ่งมีมาตรการ2ส่วนคือ
ร 9.1 A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses) า 9.2 A.14.1.2การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)
ง10. ความต่อเนื่องทางธุรกิจ- A14
ที่ 10.1 A.14.1.2การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)
11. Compliance-A15 (ไม่ขัดต่อกฎหมาย)
111.1 A15.1.2 ป้องกันการขัดต่อกฎหมายแพ่งและอาญากฎระเบียบและสัญญาต่างๆ
11.2A15.2เพื่อทำให้แน่ใจว่าระบบนั้นไม่ขัดต่อนโยบายการรักษาความปลอดภัยขององค์กรหรือมาตรฐาน

(