รายการตรวจสอบเพื่อทวนสอบความสอดคล้องกับข้อกำหนด ISO27001: 2013

มาตรา	จุดตรวจสอบ	หลักฐานการสอดคล้อง	ผลการประเมิน
4. บริบทขององค์กร 4.1 ความเข้าใจองค์กรและบริบทขององค์กร	4.1 มีกระบวนการเพื่อทำให้องค์กรสามารถพิจารณากำหนด (determined)ประเด็นภายนอกและภายใน (external and internal issues) ที่เกี่ยวข้องกับจุดมุ่งหมายองค์กร (purpose)และที่ส่งผลกระทบต่อความสามารถขององค์กรในการบรรลุผลลัพธ์ (ต่าง ๆ) ที่ตั้งใจไว้ของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรหรือไม่		
4. บริบทขององค์กร 4.2 ความเข้าใจความต้องการและความคาดหวัง	4.2a **มีกระบวนการ**ที่จะสามารถทำให้องค์กรสามารถพิจารณากำหนด (determined)ผู้ที่มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่ 4.2.b **มีกระบวนการ**เพื่อทำให้องค์กรสามารถพิจารณากำหนด (determined)ข้อกำหนดต่างๆ ของผู้ที่มีส่วนได้ส่วนเสียต่าง ๆ เหล่านี้ที่เกี่ยวข้องกับการรักษาความปลอดภัยของสารสนเทศหรือไม่		
4. บริบทขององค์กร 4.3 การพิจารณากำหนด (determined)ขอบเขตของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	4.3.a องค์กรได้พิจารณากำหนด(determined)ขอบข่ายและการประยุกต์ใช้ระบบบริหารในการรักษาความปลอดภัยของสารสนเทศเพื่อจัดตั้ง (established)ขอบเขตของระบบหรือไม่ 4.3.b เมื่อทำการพิจารณากำหนด(determined)ขอบเขตของ ISMS องค์กรได้พิจารณาประเด็นภายนอกและภายใน (external and internal issues)ที่อ้างอิงไว้ใน 4.1 หรือไม่ 4.3.c เมื่อทำการพิจารณากำหนด(determined)ขอบเขตของ ISMS องค์กรได้พิจารณาข้อกำหนดต่าง ๆ ที่อ้างอิงไว้ใน 4.2 หรือไม่ 4.3.d เมื่อทำการพิจารณากำหนด(determined)ขอบเขตของ ISMS องค์กรได้พิจารณาอินเตอร์เฟซและการพึ่งพาต่าง ๆ ระหว่างกิจกรรมต่าง ๆ ที่ปฏิบัติโดยองค์กรและที่ปฏิบัติโดยองค์กรอื่น ๆ หรือไม่ 4.3.e องค์กรได้ทำขอบเขตที่มีพร้อมให้เป็นสารสนเทศที่เป็นเอกสารหรือไม่		
4. บริบทขององค์กร 4.4 ระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ	4.4.a องค์กรได้จัดตั้ง(established) ระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศตามข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013 หรือไม่ 4.4.b องค์กรได้นำไปปฏิบัติ(implemented)ระบบการจัดกำรความมั่นคงปลอดภัยด้านสารสนเทศตามข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013		

	หรือไม่ 4.4.c องค์กรมีกระบวนการต่าง ๆ สำหรับการรักษาระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรตามข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013 หรือไม่ 4.4.d องค์กรมีกระบวนการต่าง ๆ สำหรับการปรับปรุงระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่องตามข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013 หรือไม่		
5 ความเป็นผู้นำ 5.1 ความเป็นผู้นำและความมุ่งมั่น	5.1 a มีความมุ่งมั่นต่อระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ โดยทำให้มั่นใจว่ามีการจัดตั้ง(established)นโยบายการรักษาความปลอดภัยของสารสนเทศและวัตถุประสงค์ในการรักษาความปลอดภัยของสารสนเทศ และสามารถเข้าได้กับทิศทางเชิงกลยุทธ์ขององค์กรหรือไม่ 5.1.b ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและมุ่งมั่นสัญญาต่อระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศโดยทำให้มั่นใจในการรวมข้อกำหนดต่าง ๆ ของระบบบริหารในการรักษาความปลอดภัยของสารสนเทศเข้าในกระบวนการต่าง ๆ ขององค์กรหรือไม่ 5.1.c ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและความมุ่งมั่นต่อระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศโดยทำให้มั่นใจว่ามีทรัพยากรต่าง ๆ ที่จำเป็นสำหรับระบบบริหารในการรักษาความปลอดภัยของสารสนเทศอย่างเพียงพอหรือไม่ 5.1.d ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและความมุ่งมั่นต่อระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศโดยทำการสื่อสารความสำคัญของการบริหารด้านการรักษาความปลอดภัยของสารสนเทศที่มีประสิทธิผล และมีความสอดคล้องกับข้อกำหนดต่างๆ ของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่ 5.1.e ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและความมุ่งมั่นต่อระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศโดยทำให้มั่นใจว่าระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศจะบรรลุผลลัพธ์(ต่าง ๆ) ที่ตั้งใจไว้หรือไม่ 5.1.f ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและความมุ่งมั่นต่อระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศโดยการอำนวยการและสนับสนุนบุคคลต่าง ๆ เพื่อการส่งเสริมประสิทธิผลของระบบการจัดการความ		

	มั่นคงปลอดภัยด้านสารสนเทศหรือไม่ 5.1.g ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและความมุ่งมั่นต่อระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศโดยการส่งเสริมการปรับปรุงอย่างต่อเนื่องหรือไม่ 5.1.h ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและความมุ่งมั่นต่อระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศโดยการสนับสนุนบทบาทบริหารอื่น ๆ ในการแสดงให้เห็นความเป็นผู้นำเมื่อประยุกต์ใช้กับพื้นที่ความรับผิดชอบของตนเองหรือไม่		
5 ความเป็นผู้นำ 5.2 นโยบาย	5.2.a ฝ่ายบริหารสงสุดได้จัดตั้ง(established)นโยบายการรักษาความปลอดภัยของสารสนเทศที่เหมาะสมกับจุดประสงค์(purpose)ขององค์กรหรือไม่ 5.2.b ฝ่ายบริหารสงสุดได้จัดตั้ง(established)นโยบายการรักษาความปลอดภัยของสารสนเทศที่รวมวัตถุประสงค์ในการรักษาความปลอดภัยของสารสนเทศ (ดูที่ 6.2) หรือให้กรอบการทำงานสำหรับการตั้งวัตถุประสงค์ในการรักษาความปลอดภัยของสารสนเทศหรือไม่ 5.2.c ฝ่ายบริหารสงสุดได้จัดตั้ง(established)นโยบายการรักษาความปลอดภัยของสารสนเทศที่รวมความมุ่งมั่นในการบรรลุตามข้อกำหนดต่างๆที่บังคับใช้ซึ่งเกี่ยวข้องกับการรักษาความปลอดภัยของสารสนเทศหรือไม่ 5.2.d ฝ่ายบริหารสงสุดได้จัดตั้ง(established)นโยบายการรักษาความปลอดภัยของสารสนเทศที่รวมความมุ่งมั่นในการปรับปรุงระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่องหรือไม่ 5.2.e มีการทำให้นโยบายการรักษาความปลอดภัยของสารสนเทศมีพร้อมใช้เป็นข้อมูลที่เป็นเอกสารหรือไม่ 5.2.f มีการสื่อสารนโยบายการรักษาความปลอดภัยของสารสนเทศภายในองค์กรหรือไม่ 5.2.g นโยบายการรักษาความปลอดภัยของสารสนเทศมีพร้อมสำหรับผู้มีส่วนได้ส่วนเสียอย่างเหมาะสมหรือไม่		
5 ความเป็นผู้นำ 5.3 บทบาทองค์กร ความรับผิดชอบและ	5.3.a ฝ่ายบริหารสูงสุดทำให้มั่นใจว่ามีการมอบหมายและสื่อสารความรับผิดชอบและอำนาจหน้าที่สำหรับบทบาทต่าง ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยของสารสนเทศหรือไม่		

อำนาจหน้าที่	5.3.b ฝ่ายบริหารสูงสุดได้มอบหมายความรับผิดชอบและอำนาจหน้าที่ในการทำให้มั่นใจว่าระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศมีความสอดคล้องกับข้อกำหนดต่างๆ ของ ISO/IEC 27001 หรือไม่ 5.3.c ฝ่ายบริหารสูงสุดได้มอบหมายความรับผิดชอบและอำนาจหน้าที่ในการรายงานสมรรถนะการทำงานของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศให้ฝ่ายบริหารสูงสุดหรือไม่		
6 การวางแผน 6.1 ปฏิบัติการในการหาความเสี่ยงและโอกาสต่าง ๆ 6.1.1 ทั่วไป	6.1.1.a เมื่อทำการวางแผนระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ องค์กรพิจารณาประเด็นต่าง ๆ ที่อ้างอิงใน 4.1 และตามข้อกำหนดต่างๆ ที่อ้างอิงใน 4.2 รวมถึงพิจารณากำหนด (determined)ความเสี่ยงและโอกาสต่าง ๆ ที่ต้องหาเพื่อทำให้มั่นใจว่าระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศจะสามารถบรรลุผลลัพธ์ (ต่าง ๆ) ที่ตั้งใจไว้หรือไม่ 6.1.1.b เมื่อทำการวางแผนระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ องค์กรพิจารณาประเด็นต่าง ๆ ที่อ้างอิงใน 4.1 และตามข้อกำหนดต่างๆ ที่อ้างอิงใน 4.2 รวมถึงพิจารณากำหนด (determined)ความเสี่ยงและโอกาสต่าง ๆ ที่ต้องหาเพื่อป้องกันหรือลดผลกระทบต่าง ๆ ที่ไม่พึงปรารถนาหรือไม่ 6.1.1.c เมื่อทำการวางแผนระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ พิจารณาประเด็นต่าง ๆ ที่อ้างอิงใน 4.1 และตามข้อกำหนดต่างๆ ที่อ้างอิงใน 4.2 รวมถึงพิจารณากำหนด(determined)ความเสี่ยงและโอกาสต่าง ๆ ที่ต้องหาเพื่อบรรลุการปรับปรุงอย่างต่อเนื่องหรือไม่ 6.1.1.d องค์กรวางแผนปฏิบัติการต่าง ๆ เพื่อจัดการความเสี่ยงและโอกาสต่าง ๆ เหล่านี้หรือไม่ 6.1.1.e องค์กรวางแผนวิธีที่จะ 1) รวมและนำไปปฏิบัติ(implemented)ปฏิบัติการต่างๆ เหล่านี้เข้าในกระบวนการของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรและ 2) ประเมินประสิทธิผลของปฏิบัติการต่างๆ เหล่านี้ หรือไม่		
6 การวางแผน 6.1 ปฏิบัติการในการหาความเสี่ยงและโอกาสต่าง ๆ	6.1.2.a องค์กรกำหนดและประยุกต์ใช้กระบวนการการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศที่จัดตั้ง(established)และรักษาเกณฑ์ความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศที่จะรวมถึง 1) เกณฑ์การยอมรับความเสี่ยง และ 2) เกณฑ์สำหรับการประเมิน		

6.1.2 การประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ	ความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ 6.1.2.b องค์กรกำหนดและประยุกต์ใช้กระบวนการการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศเพื่อทำให้มั่นใจว่าการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศให้ผลที่เชื่อถือได้ ทำซ้ำได้ และใช้ในการเปรียบเทียบเคียง หรือไม่ 6.1.2.c องค์กรกำหนดและประยุกต์ใช้กระบวนการการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศที่ 1) **บ่งชี้**ความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับการสูญเสียการรักษาข้อมูลความลับ บูรณภาพและการมีข้อมูลพร้อมใช้ (loss of confidentiality, integrity and availability) ภายในขอบเขตของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ และ 2) **บ่งชี้**เจ้าของความเสี่ยง(risk owners)ต่าง ๆ หรือไม่ 6.1.2.d องค์กรกำหนดและประยุกต์ใช้กระบวนการการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศที่**วิเคราะห์**ความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศดังต่อไปนี้ *1) ประเมินผลที่ตามมาที่เป็นไปได้ที่ส่งผล(potential consequences)หากความเสี่ยงต่าง ๆ ที่บ่งชี้ใน 6.1.2 c) 1) ถูกทำให้เป็นรูปเป็นร่างขึ้น (materializes)* *2) ประเมินโอกาสการเกิด(likelihood)ที่อาจเป็นจริงในการเกิดความเสี่ยงต่าง ๆ ที่บ่งชี้ใน 6.1.2 c) 1) และ* *3) กำหนด(determined)ระดับความเสี่ยง (levels of risk)ต่าง ๆ หรือไม่* 6.1.2.e องค์กรกำหนดและประยุกต์ใช้กระบวนการการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศที่**ประเมิน**ความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศที่ดังต่อไปนี้ *1) เปรียบเทียบผลการวิเคราะห์ความเสี่ยงต่าง ๆ กับเกณฑ์ความเสี่ยงที่กำหนดไว้ใน 6.1.2 a) และ* *2) จัดลำดับความสำคัญสำหรับความเสี่ยงที่ถูกวิเคราะห์เพื่อดูแลความเสี่ยง หรือไม่* 6.1.2.f องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารเกี่ยวกับการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่		
6 การวางแผน 6.1 ปฏิบัติการในการ	6.1.3.a องค์กรกำหนดและประยุกต์ใช้กระบวนการการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศเพื่อ *คัดเลือกทางเลือกในการดูแล*		

หาความเสี่ยงและโอกาสต่าง ๆ 6.1.3 การดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ	*ความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศโดยคำนึงถึงผลการประเมินความเสี่ยงต่าง ๆ หรือไม่* 6.1.3.b องค์กรกำหนดและประยุกต์ใช้กระบวนการการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศเพื่อ *กำหนดการควบคุมที่จำเป็นในการนำทางเลือกในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ (ต่าง ๆ) ที่เลือกไว้หรือไม่* 6.1.3.c องค์กรกำหนดและประยุกต์ใช้กระบวนการการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศเพื่อ *เปรียบเทียบการควบคุมต่าง ๆ ที่พิจารณากำหนด(determined)ไว้ใน 6.1.3.b ข้างต้นกับการควบคุมต่าง ๆ ในภาคผนวก A และตรวจพิสูจน์ว่าไม่มีการควบคุมต่าง ๆ ที่จำเป็นถูกข้ามไปหรือไม่* 6.1.3.d องค์กรกำหนดและประยุกต์ใช้กระบวนการการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศเพื่อ *สร้างถ้อยแถลงมาตรการ (Statement of Applicability) ควบคุมต่าง ๆ ที่จำเป็น (ดูที่ 6.1.3.b และ c) และการให้เหตุผลสำหรับการรวมเข้า ไม่ว่านำไปปฏิบัติ (implemented)หรือไม่ก็ตาม รวมถึงการให้เหตุผลสำหรับการยกเว้นการควบคุมต่าง ๆ จากภาคผนวก A* 6.1.3.e องค์กรกำหนดและประยุกต์ใช้กระบวนการการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ*เพื่อ สร้างจัดทำ แผนการจัดการความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ(formulate an information security risk treatment plan)หรือไม่* 6.1.3.f องค์กรกำหนดและประยุกต์ใช้กระบวนการการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศเพื่อ *ให้ได้มาซึ่งการอนุมัติจากเจ้าของความเสี่ยงต่างๆ สำหรับแผนการจัดการความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ(formulate an information security risk treatment plan)และการยอมรับความเสี่ยงที่เหลือด้านการรักษาความปลอดภัยของสารสนเทศ หรือไม่* 6.1.3.h องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารเกี่ยวกับกระบวนการแผนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่		
6 การวางแผน 6.2 วัตถุประสงค์ด้านการรักษาความ	6.2.a องค์กรจัดตั้ง(established)วัตถุประสงค์ต่าง ๆ ด้านการรักษาความปลอดภัยของสารสนเทศ *ในหน้าที่งานและระดับต่าง ๆ ที่เกี่ยวข้องหรือไม่*		

ปลอดภัยของสารสนเทศและแผนงานต่างๆ เพื่อทำให้บรรลุ	6.2.b วัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศมีความ*สอดคล้องกับนโยบายการรักษาความปลอดภัยของสารสนเทศหรือไม่* 6.2.c วัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศสามารถ*วัดผลได้ (หากสามารถปฏิบัติได้) หรือไม่* 6.2.d วัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศมี*การคำนึงถึงข้อกำหนดต่าง ๆ ด้านการรักษาความปลอดภัยของสารสนเทศที่บังคับใช้ และผลการประเมินความเสี่ยงรวมถึงผลการดูแลความเสี่ยงหรือไม่* 6.2.e มีการสื่อสารวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ 6.2.f มีการอัพเดตวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศอย่างเหมาะสมหรือไม่ 6.2.g องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารเกี่ยวกับวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ 6.2.h เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศ *องค์กรพิจารณากำหนด(determined)สิ่งที่จะต้องทำหรือไม่* 6.2.i เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศ *องค์กรพิจารณากำหนด(determined)ทรัพยากรอะไรที่ต้องการหรือไม่* 6.2.j เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศ *องค์กรพิจารณากำหนด(determined)บุคคลที่จะรับผิดชอบหรือไม่* 6.2.k เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศ *องค์กรพิจารณากำหนด(determined)ว่าจะทำเสร็จสมบูรณ์เมื่อไหร่หรือไม่* 6.2.l เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศ *องค์กรพิจารณากำหนด(determined)วิธีที่จะประเมินผลต่างๆ หรือไม่*		

7 การสนับสนุน 7.1 ทรัพยากร	7.1. มีกระบวนการที่องค์กรใช้เพื่อพิจารณากำหนด(determined)และให้ทรัพยากรที่จำเป็นสำหรับการจัดตั้ง(established) การนำไปปฏิบัติ (implemented) การธำรงรักษาและการปรับปรุงอย่างต่อเนื่องสำหรับวัตถุประสงค์ต่าง ๆ ของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนดไว้ใน 6.2 หรือไม่		
7. การสนับสนุน 7.2 ความชำนาญ	7.2.a มีกระบวนการที่องค์กรใช้เพื่อพิจารณากำหนด (determined)ความสามารถที่จำเป็นของบุคคล (ต่าง ๆ) ที่ทำงานภายใต้การควบคุมขององค์กรที่ส่งผลกระทบต่อประสิทธิผลการทำงานด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ 7.2.b มีกระบวนการที่ใช้เพื่อทำให้มั่นใจว่าบุคคลต่าง ๆ เหล่านี้มีความสามารถบนพื้นฐานการศึกษา การฝึกอบรมหรือประสบการณ์ที่เหมาะสมหรือไม่ 7.2.c มีกระบวนการที่ใช้เพื่อดำเนินปฏิบัติการต่าง ๆ เพื่อให้ได้มาซึ่งความสามารถที่จำเป็น รวมถึงประเมินประสิทธิผลของกิจกรรมที่ได้กระทำหรือไม่ 7.2.d มีการเก็บรักษาข้อมูลที่เป็นเอกสารที่เหมาะสมให้เป็นหลักฐานความสามารถหรือไม่		
7. การสนับสนุน 7.3 การตระหนักถึง	7.3.a มีกระบวนการที่องค์กรใช้เพื่อทำให้มั่นใจว่าบุคคลต่าง ๆ ที่ทำงานภายใต้การควบคุมขององค์กรมีการตระหนักถึงนโยบายด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ 7.3.b มีกระบวนการที่องค์กรใช้เพื่อทำให้มั่นใจว่าบุคคลต่าง ๆ ที่ทำงานภายใต้การควบคุมขององค์กรมีการตระหนักถึงการสนับสนุนประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ,รวมถึงประโยชน์จากการปรับปรุงสมรรถนะด้านการรักษาความปลอดภัยของสารสนเทศ หรือไม่ 7.3.c มีกระบวนการที่องค์กรใช้เพื่อทำให้มั่นใจว่าบุคคลต่าง ๆ ที่ทำงานภายใต้การควบคุมขององค์กรมีการตระหนักถึงความเกี่ยวพันของการไม่ปฏิบัติตามข้อกำหนดต่าง ๆ ของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่		
7. การสนับสนุน 7.4 การสื่อสาร	7.4.a มีกระบวนการที่องค์กรใช้เพื่อพิจารณากำหนด(determined)ความจำเป็นการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่ 7.4.b กระบวนการนี้ได้บ่งชี้อะไรที่จะสื่อสารหรือไม่		

	7.4.c กระบวนการนี้ได้บ่งชี้เมื่อใดที่จะสื่อสารหรือไม่ 7.4.d กระบวนการนี้ได้บ่งชี้ว่าจะต้องสื่อสารถึงใครหรือไม่ 7.4.e กระบวนการนี้ได้บ่งชี้ว่าใครเป็นผู้ทำการสื่อสารหรือไม่ 7.4.f กระบวนการนี้ได้บ่งชี้กระบวนการต่าง ๆ ที่จะส่งผลกระทบต่อการสื่อสารหรือไม่		
7. การสนับสนุน 7.5 ข้อมูลที่เป็นเอกสาร 7.5.1 ทั่วไป	7.5.1.a ระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรได้รวมเอกสารสารสนเทศที่เป็นเอกสารซึ่งกำหนดโดย ISO/IEC 27001:2013 หรือไม่ 7.5.1.b ระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรได้รวมเอกสารสารสนเทศที่พิจารณากำหนด(determined)โดยองค์กร ว่ามีความจำเป็นสำหรับประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่		
7. การสนับสนุน 7.5 ข้อมูลที่เป็นเอกสาร 7.5.2 การสร้างและการอัพเดต	7.5.2.a เมื่อทำการสร้างและอัพเดตสารสนเทศที่เป็นเอกสาร องค์กรมีกระบวนการที่จะทำให้มั่นใจในการบ่งชี้และรายละเอียดที่เหมาะสม (ตัวอย่างเช่น ชื่อเรื่อง วันที่ ผู้เขียนหรือหมายเลขอ้างอิง) หรือไม่ 7.5.2.b เมื่อทำการสร้างและอัพเดตสารสนเทศที่เป็นเอกสาร องค์กรมีกระบวนการที่จะทำให้มั่นใจในรูปแบบ (ตัวอย่างเช่น ภาษา เวอร์ชั่น ซอฟต์แวร์ กราฟิก) และสื่อ (ตัวอย่างเช่น กระดาษ ทางอิเลคทรอนิกส์) ที่เหมาะสมหรือไม่ 7.5.2.c เมื่อทำการสร้างและอัพเดตสารสนเทศที่เป็นเอกสาร องค์กรมีกระบวนการที่จะทำให้มั่นใจในการทบทวนและการอนุมัติที่เหมาะสม สำหรับความเหมาะสมและความเพียงพอของเอกสารสารสนเทศหรือไม่		
7 การสนับสนุน 7.5 ข้อมูลที่เป็นเอกสาร 7.5.3 การควบคุมข้อมูลที่เป็นเอกสาร	7.5.3.a องค์กรมีกระบวนการในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศและโดย ISO/IEC 27001:2013 เพื่อทำให้มั่นใจว่าข้อมูลมีพร้อมใช้และเหมาะสมในการใช้งานสถานที่และเวลาที่ต้องการ หรือไม่ 7.5.3.b องค์กรมีกระบวนการในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศและโดย ISO/IEC 27001:2013 เพื่อทำให้มั่นใจว่ามีการปกป้องข้อมูลอย่างเพียงพอ (ตัวอย่างเช่น จากการสูญเสียการรักษาข้อมูลความลับ การใช้งานที่ไม่		

	เหมาะสม หรือการสูญเสียบูรณภาพ) หรือไม่ 7.5.3.c องค์กรมีกระบวนการในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศและโดย ISO/IEC 27001:2013 เพื่อจัดการ การแจกจ่าย การเข้าถึง การกู้คืนและการใช้งานตามความเหมาะสม หรือไม่ 7.5.3.d องค์กรมีกระบวนการในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศและโดย ISO/IEC 27001:2013 เพื่อจัดการ การจัดเก็บ และการรักษาโดยรวมถึงการรักษาความถูกต้องตามกฎหมายอย่างเหมาะสมหรือไม่ 7.5.3.e องค์กรมีกระบวนการในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศและโดย ISO/IEC 27001:2013 เพื่อจัดการ การควบคุมการเปลี่ยนแปลง (ตัวอย่างเช่น การควบคุมเวอร์ชั่น) อย่างเหมาะสมหรือไม่ 7.5.3.f องค์กรมีกระบวนการในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศและโดย ISO/IEC 27001:2013 เพื่อจัดการ การเก็บรักษาและการทิ้งอย่างเหมาะสมหรือไม่ 7.5.3.g องค์กรมีกระบวนการในการบ่งชี้อย่างเหมาะสมสำหรับสารสนเทศที่เป็นเอกสารจากแหล่งที่มาภายนอกซึ่งองค์กรพิจารณากำหนด (determined)ว่าจำเป็นสำหรับการวางแผนและการนำไปปฏิบัติงานของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่ 7.5.3.h องค์กรมีกระบวนการในควบคุมสารสนเทศที่เป็นเอกสารจากแหล่งที่มาภายนอกซึ่งองค์กรพิจารณากำหนด(determined)ว่าจำเป็นสำหรับการวางแผนและการนำไปปฏิบัติ(implemented)ของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่		
8 การดำเนินงาน 8.1 การวางแผนและการควบคุมด้านการดำเนินงาน	8.1.a มีกระบวนการที่องค์กรใช้ในการวางแผน นำไปปฏิบัติ (implemented)และควบคุมกระบวนการต่าง ๆ ที่จำเป็นต่อการบรรลุข้อกำหนดต่าง ๆ ด้านการรักษาความปลอดภัยของสารสนเทศรวมถึงดำเนินปฏิบัติการต่างๆ ที่พิจารณากำหนด(determined)ไว้ใน 6.1 หรือไม่ 8.1.b องค์กรได้ดำเนินแผนงานต่าง ๆ ในการบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศขององค์กรตามที่พิจารณากำหนด (determined)ไว้ใน 6.2 หรือไม่		

	8.1.c องค์กรเก็บสารสนเทศที่เป็นเอกสารในขอบเขตที่จำเป็นต่อการมีความเชื่อมั่นว่ามีการดำเนินกระบวนการต่างๆ ตามแผนหรือไม่ 8.1.d องค์กรควบคุมการเปลี่ยนแปลงต่างๆ ตามแผนและทบทวนผลที่ตามมาต่าง ๆ สำหรับการเปลี่ยนแปลงที่ไม่ได้ตั้งใจไว้โดยดำเนินปฏิบัติการในการบรรเทาผลกระทบย้อนกลับต่างๆ ตามที่จำเป็นหรือไม่ 8.1.e องค์กรทำให้มั่นใจว่ามีการพิจารณากำหนดและควบคุมกระบวนการที่จ้างผู้ส่งมอบภายนอก(outsource)หรือไม่		
8 การดำเนินงาน 8.2 การบริหารความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ	8.2.a มีกระบวนการที่ใช้ในการนำไปปฏิบัติซึ่งการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ ตามแผนที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น หรือมีการนำเสนอ โดยมีการคำนึงถึงเกณฑ์ที่ได้จัดทำไว้ใน 6.1.2 a) หรือไม่ 8.2.b องค์กรเก็บรักษาสารสนเทศที่เป็นเอกสารสำหรับผลที่ได้จากการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่		
8. การดำเนินงาน 8.3 การดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ ข้อมูล	8.3.a องค์กรกำลังดำเนินการตามแผนการจัดการความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ(information security risk treatment plan) หรือไม่ 8.3.b องค์กรเก็บรักษาสารสนเทศที่เป็นเอกสารสำหรับผลการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศตามแผน(information security risk treatment plan)หรือไม่		
9 การประเมินประสิทธิผลในการทำงาน 9.1 การสังเกตการณ์ การวัดผล การวิเคราะห์และการประเมินผล	9.1.a มีกระบวนการที่ใช้ในการประเมินประสิทธิผลการทำงานด้านการรักษาความปลอดภัยของสารสนเทศและประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่ 9.1.b กระบวนการพิจารณากำหนด อะไรที่จะต้องทำการเฝ้าระวังติดตามและวัดผล,โดยรวมถึงกระบวนการและการควบคุมต่างๆ ด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ 9.1.c กระบวนการพิจารณากำหนด วิธีการต่างๆ สำหรับเฝ้าระวังติดตาม การวัดผล การวิเคราะห์และการประเมินผลอย่างเหมาะสมเพื่อทำให้มั่นใจในความถูกต้องใช้ได้ของผล (valid results)หรือไม่ 9.1.d กระบวนการพิจารณากำหนด จะต้องเฝ้าระวังติดตามและวัดผลเมื่อไหร่หรือไม่		

	9.1.e กระบวนการพิจารณากำหนด ผู้ที่ต้องทำการเฝ้าระวังติดตามและวัดผลหรือไม่ 9.1.f กระบวนการพิจารณากำหนด ว่าเมื่อไหร่ที่จะวิเคราะห์และประเมินผลต่างๆ จากการเฝ้าระวังติดตามและการวัดผลหรือไม่ 9.1.g กระบวนการพิจารณากำหนด ว่าใครจะต้องทำการวิเคราะห์และประเมินผลต่าง ๆ เหล่านี้หรือไม่ 9.1.h องค์กรเก็บรักษาสารสนเทศที่เป็นเอกสารที่เหมาะสมให้เป็นหลักฐานของผลการสังเกตการณ์และการวัดผลหรือไม่		
9 การประเมินประสิทธิผลในการทำงาน 9.2 ภายใน	9.2.a มีกระบวนการที่ใช้ในการทำให้มั่นใจว่าองค์กรนำไปปฏิบัติ (implemented)ตรวจติดตามภายในในช่วงเวลาตามแผนหรือไม่ 9.2.b การตรวจติดตามภายในให้ข้อมูลว่าระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศมีความสอดคล้องกับข้อกำหนดต่างๆ ขององค์กรสำหรับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่ 9.2.c การตรวจติดตามภายในให้ข้อมูลว่าระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศมีความสอดคล้องกับข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013 หรือไม่ 9.2.d การตรวจติดตามภายในให้ข้อมูลว่ามีการดำเนินและรักษาระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศอย่างมีประสิทธิผลหรือไม่ 9.2.e องค์กรวางแผน จัดทำ นำไปปฏิบัติ และธำรงรักษา โปรแกรมการตรวจติดตาม(ต่าง ๆ) โดยรวมถึงความถี่ วิธีการ ความรับผิดชอบ ข้อกำหนดในการวางแผนต่างๆ และการรายงานหรือไม่ 9.2.f โปรแกรมการตรวจติดตาม (ต่าง ๆ) มีการพิจารณาความสำคัญของกระบวนการต่าง ๆ ที่เกี่ยวข้องและผลการตรวจติดตามครั้งที่แล้วหรือไม่ 9.2.g องค์กรกำหนดเกณฑ์และขอบเขตการตรวจติดตามสำหรับแต่ละการตรวจติดตามหรือไม่ 9.2.h องค์กรคัดเลือกผู้ตรวจติดตามและนำไปปฏิบัติตรวจติดตามที่ทำให้มั่นใจใน objectivity และ impartiality ของกระบวนการการตรวจติดตาม		

	หรือไม่ 9.2.i องค์กรทำให้มั่นใจว่ามีการรายงานผลการตรวจติดตามต่าง ๆ ถึงฝ่ายบริหารที่เกี่ยวข้องหรือไม่ 9.2.j องค์กรเก็บรักษาสารสนเทศที่เป็นเอกสารเป็นหลักฐานสำหรับโปรแกรมการตรวจติดตาม (ต่าง ๆ) และผลการตรวจติดตามหรือไม่		
9. การประเมินประสิทธิผลในการทำงาน 9.3 การทบทวนของฝ่ายบริหาร	9.3.a มีกระบวนการที่ฝ่ายบริหารสูงสุดใช้เพื่อทบทวนระบบบริหารการรักษาความปลอดภัยของสารสนเทศขององค์กรในช่วงเวลาตามแผนเพื่อทำให้มั่นใจในความเหมาะสม ความเพียงพอและประสิทธิผลอย่างต่อเนื่องหรือไม่ 9.3.b การทบทวนได้รวมการพิจารณาสถานะของปฏิบัติการต่างๆ จากการทบทวนของฝ่ายบริหารครั้งที่แล้วหรือไม่ 9.3.c การทบทวนได้รวมการพิจารณาการเปลี่ยแนปลงต่าง ๆ ในประเด็นภายนอกและภายใน (external and internal issues)ที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่ 9.3.d การทบทวนได้รวมการพิจารณาข้อคิดเห็นด้านประสิทธิผลการทำงานสำหรับการรักษาความปลอดภัยของสารสนเทศโดยรวมถึงแนวโน้มต่าง ๆ ใน 1) ความไม่สอดคล้องและปฏิบัติการแก้ไขต่าง ๆ 2) ผลการสังเกตการณ์และการวัดผลต่าง ๆ 3) ผลการตรวจติดตามต่าง ๆ และ 4) การบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ 9.3.e การทบทวนได้รวมการพิจารณาข้อมูลป้อนกลับจากผู้มีส่วนได้ส่วนเสียหรือไม่ 9.3.f การทบทวนได้รวมการพิจารณาผลการประเมินความเสี่ยงต่าง ๆ และสถานะของแผนการดูแลความเสี่ยง (Risk Treatment Plan)หรือไม่ 9.3.g การทบทวนได้รวมการพิจารณาโอกาสสำหรับการปรับปรุงอย่างต่อเนื่องหรือไม่ 9.3.h ผลลัพธ์ต่าง ๆ ของการทบทวนของฝ่ายบริหารได้รวมการพิจารณากำหนด การตัดสินใจต่าง ๆ เกี่ยวกับโอกาสสำหรับการปรับปรุงอย่างต่อเนื่องและการเปลี่ยนแปลงต่าง ๆ ที่จำเป็นสำหรับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหรือไม่		

	9.3.i องค์กรเก็บรักษาสารสนเทศที่เป็นเอกสารให้เป็นหลักฐานสำหรับผลการทบทวนของฝ่ายบริหารหรือไม่		
10.1 ความไม่สอดคล้องและปฏิบัติการแก้ไข	10.1.a มีกระบวนการที่องค์กรใช้เพื่อตอบสนองต่อความไม่สอดคล้องและ 1) ดำเนินปฏิบัติการในการควบคุมและแก้ไข รวมถึง 2) จัดการกับผลที่ตามมาต่าง ๆ อย่างเหมาะสมหรือไม่ 10.1.b มีกระบวนการที่องค์กรใช้เพื่อประเมินความต้องการสำหรับปฏิบัติการในการขจัดสาเหตุของความไม่สอดคล้องต่าง ๆ เพื่อที่จะไม่เกิดซ้ำหรือเกิดขึ้นในที่อื่นใดด้วย 1) การทบทวนความไม่สอดคล้อง 2) การพิจารณากำหนดสาเหตุของความไม่สอดคล้อง และ 3) การพิจารณากำหนดว่ามีความไม่สอดคล้องที่เหมือนกันหรืออาจเกิดขึ้นได้หรือไม่ 10.1.c มีกระบวนการที่องค์กรใช้เพื่อดำเนินปฏิบัติที่จำเป็นหรือไม่ 10.1.d มีกระบวนการที่องค์กรใช้เพื่อทบทวนประสิทธิผลของปฏิบัติการแก้ไขที่นำไปปฏิบัติหรือไม่ 10.1.e มีกระบวนการที่องค์กรใช้เพื่อทำการเปลี่ยนแปลงต่าง ๆ สำหรับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศหากจำเป็น หรือไม่ 10.1.f มีกระบวนการที่องค์กรใช้เพื่อทำให้มั่นใจว่าปฏิบัติการแก้ไขต่าง ๆ มีความเหมาะสมกับผลกระทบต่างๆ ของความไม่สอดคล้องที่พบหรือไม่ 10.1.g องค์กรเก็บรักษาสารสนเทศที่เป็นเอกสารให้เป็นหลักฐานสำหรับลักษณะของความไม่สอดคล้องต่าง ๆ และปฏิบัติการซึ่งนำไปปฏิบัติต่อมาหรือไม่ 10.1.h องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารให้เป็นหลักฐานสำหรับผลของปฏิบัติการแก้ไขหรือไม่		
10 การปรับปรุง 10.2 การปรับปรุงอย่างต่อเนื่อง	10.2 มีกระบวนการที่ใช้ในการปรับปรุงความเหมาะสม ความเพียงพอและประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่องหรือไม่		

รายการตรวจสอบเพื่อทวนสอบความสอดคล้องกับข้อกำหนด ISO27001: 2013(การประเมินมาตรการควบคุม)

มาตรา	จุดตรวจสอบ	หลักฐานการสอดคล้อง	ผลการประเมิน
A.5 นโยบายการรักษาความปลอดภัยของสารสนเทศ A.5.1 ทิศทางการบริหารด้านการรักษาความปลอดภัยของสารสนเทศ วัตถุประสงค์: เพื่อให้ทิศทางและการสนับสนุนการบริหารด้านการรักษาความปลอดภัยของสารสนเทศตามข้อกำหนดทางธุรกิจและกฎหมายรวมถึงกฎระเบียบที่เกี่ยวข้อง	A.5.1.1 มีการกำหนดชุดเอกสารสำหรับนโยบาย(คำสั่ง กฎ ระเบียบ ข้อบังคับ)ด้านการรักษาความปลอดภัยของสารสนเทศได้รับการอนุมัติจากฝ่ายบริหาร ทำการเผยแพร่และทำการสื่อสารถึงพนักงานทุกคนและบุคคลภายนอกที่เกี่ยวข้องหรือไม่ A.5.1.2 มีการทบทวนนโยบาย(คำสั่ง กฎ ระเบียบ ข้อบังคับ) การรักษาความปลอดภัยของสารสนเทศในช่วงเวลาตามแผนหรือหากมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้นเพื่อทำให้มั่นใจในความเหมาะสม ความเพียงพอและประสิทธิผลอย่างต่อเนื่องหรือไม่		
A.6 องค์กรด้านการรักษาความปลอดภัยของสารสนเทศ A.6.1 องค์กรภายใน วัตถุประสงค์: เพื่อจัดตั้ง(established)กรอบการทำงานของฝ่ายบริหารในการริเริ่มและควบคุมการปฏิบัติและนำไปปฏิบัติ(implemented)ด้านการรักษาความปลอดภัยของสารสนเทศภายในองค์กร	A.6.1.1 มีการกำหนดและมอบหมายความรับผิดชอบด้านการรักษาความปลอดภัยของสารสนเทศทั้งหมดหรือไม่ A.6.1.2 ส่วนงานที่อาจมีความขัดแย้งในเรื่องความรับผิดชอบได้มีการคัดแยก เพื่อลดโอกาสในการปรับเปลี่ยน แก้ไขโดยไม่ได้รับอนุญาตหรือไม่ ไม่ว่าตั้งใจหรือไม่ตั้งใจสำหรับสินทรัพย์ขององค์กรหรือไม่ A.6.1.3 มีการติดต่อประสานงานกับผู้มีอำนาจหน้าที่ที่เกี่ยวข้องอย่างเหมาะสมและสม่ำเสมอหรือไม่ A.6.1.4 มีการติดต่อที่เหมาะสมกับกลุ่มสนใจพิเศษหรือฟอรั่มผู้เชี่ยวชาญด้านการรักษาความปลอดภัยและสมาคมทางอาชีพอื่น ๆ หรือไม่ A.6.1.5 มีการจัดการการรักษาความปลอดภัยของสารสนเทศในฝ่ายบริหารโครงการโดยไม่คำนึงถึงประเภทของโครงการหรือไม่		
A.6 องค์กรด้านการรักษาความปลอดภัยของสารสนเทศ A.6.2 อุปกรณ์มือถือและการ	A.6.2.1 มีการใช้นโยบาย(คำสั่ง กฎ ระเบียบ ข้อบังคับ)และมาตรการการรักษาความปลอดภัยสนับสนุนสำหรับการบริหารความเสี่ยงต่าง ๆ ที่เกิดจากการใช้อุปกรณ์มือถือหรือไม่		

ทำงานทางไกล วัตถุประสงค์: เพื่อทำให้มั่นใจในการรักษาความปลอดภัยสำหรับการทำงานทางไกลและการใช้อุปกรณ์มือถือ	A.6.2.2 มีการดำเนินตามนโยบาย(คำสั่ง กฎ ระเบียบข้อบังคับ)และมาตรการการรักษาความปลอดภัยสนับสนุนเพื่อปกป้องสารสนเทศที่ถูกเข้าถึง ประมวลผลหรือจัดเก็บที่สถานประกอบการทำงานทางไกล(teleworking sites) หรือไม่		
A.7 การรักษาความปลอดภัยด้านทรัพยากรบุคคล A.7.1 ก่อนการว่าจ้าง วัตถุประสงค์: เพื่อทำให้มั่นใจว่าพนักงานและผู้รับเหมาต่าง ๆ มีความเข้าใจความรับผิดชอบของตนเองและมีความเหมาะสมสำหรับบทบาทต่าง ๆ ที่ถูกพิจารณา	A.7.1.1. มีการตรวจสอบพิสูจน์ภูมิหลังผู้สมัครทุกคนสำหรับการว่าจ้างตามกฎหมาย กฎระเบียบและหลักจริยธรรมที่เกี่ยวข้อง รวมถึงการตรวจสอบพอเหมาะกับข้อกำหนดทางธุรกิจต่าง ๆ ตามประเภทของสารสนเทศที่จะเข้าถึงและความเสี่ยงที่รับรู้หรือไม่ A.7.1.2. มีข้อสัญญากับพนักงานและผู้รับเหมาที่กล่าวถึงความรับผิดชอบของพนักงานและผู้รับเหมา รวมถึงองค์กรในด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่		
A.7 การรักษาความปลอดภัยด้านทรัพยากรบุคคล A.7.2 ระหว่างการว่าจ้าง วัตถุประสงค์: เพื่อทำให้มั่นใจว่าพนักงานและผู้รับเหมาต่าง ๆ มีความตระหนักถึงและบรรลุความรับผิดชอบด้านการรักษาความปลอดภัยของสารสนเทศของตนเอง	A.7.2.1 ฝ่ายบริหารกำหนดให้พนักงานและผู้รับเหมาทุกคนประยุกต์ใช้การรักษาความปลอดภัยของสารสนเทศตามนโยบายและกระบวนการทำงานต่าง ๆ ที่จัดทำไว้ขององค์กรหรือไม่ A.7.2.2 พนักงานทุกคนขององค์กรและผู้รับเหมาที่เกี่ยวข้องได้รับการศึกษาและการฝึกอบรมด้านการตระหนักถึงที่เหมาะสม รวมถึงการอัพเดตทั่วไปในด้านนโยบายและกระบวนการทำงานขององค์กรตามที่เกี่ยวข้องกับหน้าที่งานของตนเองหรือไม่ A.7.2.3 มีกระบวนการด้านกฎระเบียบวินัยที่เป็นทางการและได้รับการสื่อสารให้กับพนักงานที่อาจทำการละเมิดกฎการรักษาความปลอดภัยของสารสนเทศหรือไม่		
A.7 การรักษาความปลอดภัยด้านทรัพยากรบุคคล A.7.3 การสิ้นสุดและการเปลี่ยนแปลงการว่าจ้าง วัตถุประสงค์: เพื่อป้องกันผลประโยชน์ขององค์กรให้เป็นส่วนหนึ่งของกระบวนการการเปลี่ยนแปลงหรือสิ้นสุดการว่าจ้าง	A.7.3.1 มีการกำหนดและสื่อสารความรับผิดชอบและหน้าที่ด้านการรักษาความปลอดภัยของสารสนเทศที่ยังคงมีผลใช้ได้หลังการสิ้นสุดการว่าจ้างถึงพนักงานหรือผู้รับเหมารวมถึงการบังคับใช้หรือไม่		

A.8 การบริหารสินทรัพย์ A.8.1 ความรับผิดชอบต่อสินทรัพย์ วัตถุประสงค์: เพื่อบ่งชี้สินทรัพย์ขององค์กรและกำหนดความรับผิดชอบในการป้องกันที่เหมาะสม	A.8.1.1 มีการบ่งชี้สินทรัพย์ที่เกี่ยวข้องกับสารสนเทศและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล มีการทำรายการสินทรัพย์เหล่านี้ให้เป็นระเบียบ และมีการทำให้ทันสมัยหรือไม่ A.8.1.2 มีการมอบหมายผู้รับผิดชอบ (owner) เพื่อการรักษาสินทรัพย์ต่าง ๆ ทั้งหมดในรายการหรือไม่ A.8.1.3 มีกฎสำหรับการบ่งชี้ ทำให้เป็นเอกสารและการนำไปปฏิบัติ สำหรับการใช้งานข้อมูลและสินทรัพย์ที่เกี่ยวกับข้อมูลและสิ่งอำนวยความสะดวกในการประมวลข้อมูลหรือไม่ A.8.1.4 พนักงานและผู้ใช้งานที่เป็นบุคคลภายนอกทุกคนได้ส่งคืนสินทรัพย์ขององค์กรทั้งหมดที่อยู่ในการครอบครองเมื่อสิ้นสุดการว่าจ้าง สัญญาหรือข้อตกลงแล้วหรือไม่		
A.8 การบริหารสินทรัพย์ A.8.2 การจัดประเภทข้อมูล วัตถุประสงค์: เพื่อทำให้มั่นใจว่าข้อมูลได้รับการป้องกันในระดับที่เหมาะสมตามความสำคัญของข้อมูลสำหรับองค์กร	A.8.2.1 มีการแบ่งประเภทข้อมูลในด้านข้อกำหนดทางกฎหมาย ต่าง ๆ มูลค่า ภาวะวิกฤต และความละเอียดอ่อนต่อการเปิดเผยหรือการดัดแปลงแก้ไขที่ไม่ได้รับอนุญาตหรือไม่ A.8.2.2 มีการพัฒนาและดำเนินชุดกระบวนการทำงานต่าง ๆ ที่เหมาะสมสำหรับการการติดป้ายข้อมูล (information labeling) ตามรายการการแบ่งประเภทข้อมูลที่องค์กรปรับใช้หรือไม่ A.8.2.3 มีการจัดทำและดำเนินกระบวนการทำงานสำหรับการจัดการสินทรัพย์ตามรายการการแบ่งประเภทข้อมูลที่องค์กรประยุกต์ใช้หรือไม่		
A.8 การบริหารสินทรัพย์ A.8.3 การจัดการสื่อ วัตถุประสงค์:เพื่อป้องกันการเปิดเผย การดัดแปลงแก้ไข การนำออกหรือการทำลายข้อมูลที่จัดเก็บบนสื่อโดยไม่ได้รับอนุญาต	A.8.3.1 มีการดำเนินกระบวนการทำงานสำหรับการบริหารสื่อที่ถอดออกได้ตามรายการการแบ่งประเภทข้อมูลที่องค์กรปรับใช้หรือไม่ A.8.3.2 มีการทิ้งสื่ออย่างปลอดภัยในเวลาที่ไม่ต้องการแล้วโดยใช้กระบวนการทำงานที่เป็นทางการหรือไม่ A.8.3.3 มีการปกป้องสื่อที่บรรจุข้อมูลจากการเข้าถึงที่ไม่ได้รับอนุญาต การใช้ผิด หรือการขโมยขณะขนส่ง หรือไม่		
A.9 การควบคุมการเข้าถึง A.9.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึง	A.9.1.1 มีการจัดทำเอกสารและทบทวนนโยบาย(คำสั่ง กฎระเบียบ ข้อบังคับ) การควบคุมการเข้าถึงโดยอิงตามข้อกำหนดทางธุรกิจและการรักษาความปลอดภัยของสารสนเทศหรือไม่		

วัตถุประสงค์: เพื่อจำกัดการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลข้อมูล	A.9.1.2 มีการให้ผู้ใช้งานเท่านั้นที่จะเข้าถึงเครือข่ายและบริการของเครือข่ายที่ผู้ใช้งานได้รับอนุญาตเฉพาะในการใช้งานหรือไม่		
A.9 การควบคุมการเข้าถึง A.9.2 การบริหารการเข้าถึงสำหรับผู้ใช้งาน วัตถุประสงค์: เพื่อทำให้มั่นใจในการเข้าถึงของผู้ใช้ที่ได้รับอนุญาตและเพื่อป้องกันการเข้าถึงระบบและบริการที่ไม่ได้รับอนุญาต	A.9.2.1 มีการดำเนินกระบวนการการลงทะเบียนหรือถอนทะเบียนผู้ใช้งานเพื่อทำให้สามารถมอบหมายสิทธิการเข้าถึงหรือไม่ A.9.2.2 มีการดำเนินกระบวนการการให้การเข้าถึงสำหรับผู้ใช้งานอย่างเป็นทางการในการมอบหมายหรือถอนสิทธิการเข้าถึงสำหรับผู้ใช้งานทุกประเภทสำหรับระบบและบริการต่าง ๆ ทั้งหมดหรือไม่ A.9.2.3 มีการจำกัดและควบคุมการจัดสรรและการใช้สิทธิการเข้าถึงที่มีสิทธิพิเศษหรือไม่ A.9.2.4 มีการควบคุมการจัดสรรข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ (secret authentication information) ผ่านกระบวนการการบริหารที่เป็นทางการหรือไม่ A.9.2.5 เจ้าของสินทรัพย์ต่าง ๆ ได้ทบทวนสิทธิการเข้าถึงของผู้ใช้งานต่าง ๆ ในช่วงเวลาปกติหรือไม่ A.9.2.6 มีการถอนสิทธิการเข้าถึงของพนักงานทุกคนและผู้ใช้งานที่เป็นบุคคลภายนอกสำหรับข้อมูลและสิ่งอำนวยความสะดวกในการประมวลข้อมูลออกเมื่อสิ้นสุดการว่าจ้าง สัญญา หรือข้อตกลงหรือปรับแก้ตามการเปลี่ยนแปลงหรือไม่		
A.9 การควบคุมการเข้าถึง A.9.3 ความรับผิดชอบของผู้ใช้งาน วัตถุประสงค์: เพื่อทำให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลด้านการพิสูจน์ตัวตน	A.9.3.1 ผู้ใช้งานต่าง ๆ จะต้องปฏิบัติตามแนวทางปฏิบัติขององค์กรในการใช้งานข้อมูลการพิสูจน์ตัวตนที่เป็นความลับ (secret authentication information) หรือไม่		
A.9 การควบคุมการเข้าถึง A.9.4 การควบคุมการเข้าถึงระบบและแอพพลิเคชั่น	A.9.4.1 มีการจำกัดการเข้าถึงข้อมูลและหน้าที่งานของระบบแอพพลิเคชั่นตามนโยบายการควบคุมการเข้าถึงหรือไม่ A.9.4.2 หากนโยบายการควบคุมการเข้าถึงมีการกำหนดไว้ ได้มี		

วัตถุประสงค์: เพื่อป้องกันการเข้าถึงระบบและแอพพลิเคชั่นที่ไม่ได้รับอนุญาต	การควบคุมการเข้าถึงระบบและแอพพลิเคชั่นด้วยกระบวนการทำงานในการเข้าสู่ระบบที่ปลอดภัยหรือไม่ A.9.4.3 ระบบการบริหารรหัสผ่านมีปฏิสัมพันธ์และทำให้มั่นใจในรหัสผ่านที่มีคุณภาพหรือไม่ A.9.4.4 การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ ที่อาจสามารถทำให้ผ่านข้ามการควบคุมของระบบและแอพพลิเคชั่นมีหรือไม่ A.9.4.5. มีการจำกัดการเข้าถึงรหัสต้นทางของโปรแกรมหรือไม่		
A.10 การเข้ารหัส A.10.1 การควบคุมด้วยการเข้ารหัส วัตถุประสงค์: เพื่อทำให้มั่นใจในการใช้งานการเข้ารหัสที่เหมาะสมและมีประสิทธิผลเพื่อป้องกันการรักษาข้อมูลความลับความถูกต้องและ/หรือบูรณภาพของข้อมูล	A.10.1.1 มีการพัฒนาและดำเนินนโยบาย(คำสั่ง กฎ ระเบียบ ข้อบังคับ) การใช้การควบคุมด้วยการเข้ารหัสเพื่อปกป้องข้อมูลหรือไม่ A.10.1.2 มีการพัฒนานโยบาย(คำสั่ง กฎ ระเบียบ ข้อบังคับ) การใช้งาน การป้องกันและอายุการใช้งานของคีย์การเข้ารหัสและมีการปฏิบัติ ตลอดวงจรอายุ (whole life cycle) หรือไม่		
A.11 การรักษาความปลอดภัยทางกายภาพและสิ่งแวดล้อม A.11.1 พื้นที่ปลอดภัย วัตถุประสงค์: เพื่อป้องกันการเข้าถึงทางกายภาพที่ไม่ได้รับอนุญาต ความเสียหายและการเข้าแทรกแซงข้อมูลขององค์กรและสิ่งอำนวยความสะดวกในการประมวลข้อมูล	A.11.1.1 มีการกำหนดและใช้แนวขอบการรักษาความปลอดภัยเพื่อป้องกันพื้นที่ต่าง ๆ ที่บรรจุข้อมูลที่อ่อนไหวง่ายหรือสำคัญ รวมถึงสิ่งอำนวยความสะดวกในการประมวลข้อมูลหรือไม่ A.11.1.2 มีการป้องกันพื้นที่ปลอดภัยด้วยการควบคุมการเข้าอย่างเหมาะสมเพื่อทำให้มั่นใจว่ามีเพียงบุคลากรที่ได้รับอนุญาตที่จะเข้าถึงได้เท่านั้นหรือไม่ A.11.1.3 มีการออกแบบการรักษาความปลอดภัยทางกายภาพสำหรับสำนักงาน ห้องและสิ่งอำนวยความสะดวกต่าง ๆ และมีการประยุกต์ใช้ด้วยหรือไม่ A.11.1.4 มีการออกแบบการป้องกันทางกายภาพสำหรับภัยพิบัติทางธรรมชาติ การจู่โจมที่ประสงค์ร้ายหรืออุบัติเหตุต่าง ๆ และมีการประยุกต์ใช้ A.11.1.5 มีการออกแบบกระบวนการทำงานสำหรับการทำงาน		

	ในพื้นที่ปลอดภัย และมีการประยุกต์ใช้ด้วยหรือไม่ A.11.1.6 มีการควบคุมจุดเข้าถึงต่าง ๆ อาทิเช่น พื้นที่ส่งมอบและการโหลดรวมถึงจุดอื่น ๆ ที่บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าในสถานที่ต่างๆ และหากเป็นไปได้ ให้แยกต่างหากจากสิ่งอำนวยความสะดวกในการประมวลข้อมูลเพื่อหลีกเลี่ยงการเข้าถึงที่ไม่ได้รับอนุญาตหรือไม่		
A.11 การรักษาความปลอดภัยทางกายภาพและสิ่งแวดล้อม A.11.2 อุปกรณ์ วัตถุประสงค์: เพื่อป้องกันการสูญเสีย ความเสียหาย การขโมยหรือการทำให้สินทรัพย์อยู่ในอันตรายและการขัดจังหวะการดำเนินงานขององค์กร	A.11.2.1 มีการจัดทำและปกป้องอุปกรณ์เพื่อลดความเสี่ยงต่าง ๆ จากการคุกคามและอันตรายทางสิ่งแวดล้อมรวมถึงโอกาสในการเข้าถึงที่ไม่ได้รับอนุญาตหรือไม่ A.11.2.2 มีการป้องกันอุปกรณ์จากไฟฟ้าดับและการหยุดชะงักอื่น ๆ ที่เกิดจากความล้มเหลวของสาธารณูปโภคสนับสนุนหรือไม่ A.11.2.3 มีการป้องกันไฟฟ้าและโทรคมนาคมต่าง ๆ ที่เดินสายเคเบิ้ลในการลำเลียงข้อมูลหรือสนับสนุนการให้บริการข้อมูลจากการสกัดกั้น การแทรกแซงหรือความเสียหายหรือไม่ A.11.2.4 มีการบำรุงรักษาอุปกรณ์อย่างถูกต้องเพื่อทำให้มั่นใจในการมีพร้อมใช้อย่างต่อเนื่องและบูรณภาพหรือไม่ A.11.2.5 ไม่มีการนำอุปกรณ์ ข้อมูลหรือซอฟต์แวร์ออกนอกสถานประกอบการโดยไม่ได้รับการอนุญาตก่อนหรือไม่ A.11.2.6 มีการประยุกต์ใช้การรักษาความปลอดภัยกับสินทรัพย์นอกสถานประกอบการโดยคำนึงถึงความเสี่ยงที่แตกต่างของการทำงานนอกสถานที่ขององค์กรหรือไม่ A.11.2.7 มีการตรวจสอบอุปกรณ์ทุกรายการที่บรรจุสื่อจัดเก็บเพื่อทำให้มั่นใจว่ามีการนำข้อมูลที่อ่อนไหวง่ายและซอฟต์แวร์ที่มีใบอนุญาตออกหรือทำการเขียนทับอย่างปลอดภัยก่อนทำการทิ้งหรือใช้ซ้ำหรือไม่ A.11.2.8 ผู้ใช้ต่าง ๆ ทำให้มั่นใจว่าอุปกรณ์ที่ไม่ได้ใส่ข้อมูลมีการป้องกันอย่างเหมาะสมหรือไม่ A.11.2.9 มีการใช้นโยบายจัดเก็บเอกสารสำหรับเอกสารที่เป็น		

	กระดาษและสื่อจัดเก็บที่ถอดออกได้รวมถึงนโยบายการใช้งานคอมพิวเตอร์สำหรับสิ่งอำนวยความสะดวกในการประมวลข้อมูลหรือไม่		
A.12 การรักษาความปลอดภัยด้านการดำเนินงาน A.12.1 กระบวนการทำงานด้านการดำเนินงานและความรับผิดชอบต่างๆ วัตถุประสงค์: เพื่อทำให้มั่นใจในการดำเนินงานที่ถูกต้องและปลอดภัยของสิ่งอำนวยความสะดวกในการประมวลข้อมูล	A.12.1.1 มีการทำเอกสารกระบวนการทำงานในการดำเนินงานและทำให้มีพร้อมใช้สำหรับผู้ใช้งานทุกคนที่ต้องการหรือไม่ A.12.1.2 มีการควบคุมการเปลี่ยนแปลงสำหรับองค์กร กระบวนการทางธุรกิจ สิ่งอำนวยความสะดวกในการประมวลข้อมูลและระบบที่ส่งผลกระทบต่อกระบวนการการรักษาความปลอดภัยของสารสนเทศหรือไม่ A.12.1.3 มีการสังเกตการณ์ ปรับแต่งการใช้ทรัพยากรหรือไม่และทำการวางแผนจากข้อกำหนดด้านสมรรถนะในอนาคตเพื่อทำให้มั่นใจในประสิทธิผลการทำงานของระบบที่ต้องการหรือไม่ A.12.1.4 มีการแยกการพัฒนา การทดสอบและสภาพแวดล้อมในการดำเนินงานออกต่างหากเพื่อลดความเสี่ยงจากการเข้าถึงหรือการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตสำหรับสภาพแวดล้อมในการดำเนินงานหรือไม่		
A.12 การรักษาความปลอดภัยด้านการดำเนินงาน A.12.2 การป้องกันมัลแวร์ (malware) วัตถุประสงค์: เพื่อทำให้มั่นใจว่ามีการปกป้องข้อมูลและสิ่งอำนวยความสะดวกในการประมวลข้อมูลจากมัลแวร์	A.12.2.1 มีการนำไปปฏิบัติ(implemented)ควบคุมด้านการตรวจพบ การป้องกันและการฟื้นฟูเพื่อป้องกันมัลแวร์ และรวมกับการตระหนักถึงของผู้ใช้งานที่เหมาะสมหรือไม่		
A.12 การรักษาความปลอดภัยด้านการดำเนินงาน A.12.3 การสำรองข้อมูล วัตถุประสงค์:เพื่อป้องกันการสูญเสียข้อมูล	A.12.3.1 มีการทำสำเนาการสำรองภาพข้อมูล ซอฟต์แวร์และระบบ รวมถึงทำการทดสอบเป็นประจำตามนโยบายการสำรองที่ตกลงกันไว้หรือไม่		
A.12 การรักษาความปลอดภัยด้านการดำเนินงาน A.12.4 การเข้าออกระบบและการสังเกตการณ์	A.12.4.1 มีการสร้าง เก็บและทบทวนสมุดบันทึกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น ความผิดพลาดและเหตุการณ์ด้านการรักษาความปลอดภัยของสารสนเทศเป็นประจำหรือไม่		

วัตถุประสงค์: เพื่อบันทึกเหตุการณ์ต่างๆ และสร้างหลักฐาน	A.12.4.2 มีการป้องกันสิ่งอำนวยความสะดวกในการเข้าออกระบบและข้อมูลการเข้าออกระบบจากการปลอมแปลงและการเข้าถึงที่ไม่ได้รับอนุญาตหรือไม่ A.12.4.3 มีการป้องกันและทบทวนผู้ดูแลระบบและผู้ปฏิบัติการระบบที่ต้องเข้าออกระบบและการเข้าออกระบบเป็นประจำหรือไม่ A.12.4.4 นาฬิกาต่าง ๆ ของระบบการประมวลข้อมูลที่เกี่ยวข้องทั้งหมดภายในองค์กรหรือโดเมนการรักษาความปลอดภัยถูกตั้งเวลาให้ตรงกับแหล่งเวลาอ้างอิงที่เดียวหรือไม่		
A.12 การรักษาความปลอดภัยด้านการดำเนินงาน A.12.5 การควบคุมซอฟต์แวร์ปฏิบัติการ วัตถุประสงค์: เพื่อทำให้มั่นใจในบูรณภาพของระบบปฏิบัติการ	A.12.5.1 มีการดำเนินกระบวนการทำงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการหรือไม่		
A.12 การรักษาความปลอดภัยด้านการดำเนินงาน A.12.6 การบริหารช่องโหว่ทางเทคนิค วัตถุประสงค์: เพื่อป้องกันการใช้ช่องโหว่ทางเทคนิค	A.12.6.1 มีการได้รับข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบข้อมูลที่ใช้ในลักษณะที่ทันเวลาหรือไม่ มีการประเมินการเปิดขององค์กรต่อโหว่ต่าง ๆ ดังกล่าว และมีการใช้มาตรการที่เหมาะสมเพื่อหาความเสี่ยงที่เกี่ยวข้องหรือไม่ A.12.6.2 มีการกำหนดและดำเนินกฎระเบียบที่กำกับดูแลการติดตั้งซอฟต์แวร์โดยผู้ใช้งานหรือไม่		
A.12 การรักษาความปลอดภัยด้านการดำเนินงาน A.12.7 การพิจารณาการตรวจติดตามระบบข้อมูล วัตถุประสงค์: เพื่อลดผลกระทบของกิจกรรมการตรวจติดตามสำหรับระบบปฏิบัติการ	A.12.7.1 ข้อกำหนดและกิจกรรมในการตรวจติดตามมีความเกี่ยวข้องกับการตรวจสอบระบบปฏิบัติการที่วางแผนและตกลงกันอย่างระมัดระวังเพื่อลดการขัดจังหวะกระบวนการทางธุรกิจหรือไม่		
A.13 การรักษาความปลอดภัยด้านการสื่อสาร A.13.1 การบริหารการรักษาความปลอดภัยของเครือข่าย	A.13.1.1 มีการบริหารและควบคุมเครือข่ายต่าง ๆ เพื่อป้องกันข้อมูลในระบบและแอพพลิเคชั่นหรือไม่ A.13.1.2 มีการบ่งชี้กลไกการรักษาความปลอดภัย ระดับการ		

วัตถุประสงค์: เพื่อทำให้มั่นใจในการป้องกันข้อมูลในเครือข่ายต่างๆ และสิ่งอำนวยความสะดวกในการประมวลข้อมูลสนับสนุน	ให้บริการและข้อกำหนดด้านการบริหารของการให้บริการเครือข่ายทั้งหมด และรวมอยู่ในข้อตกลงการให้บริการว่าจะมีการให้บริการต่าง ๆ เหล่านี้ภายในบริษัทหรือโดยผู้รับเหมาหรือไม่ A.13.1.3 มีการแยกกลุ่มการให้บริการข้อมูล ผู้ใช้งานและระบบข้อมูลบนเครือข่ายต่าง ๆ หรือไม่		
A.13 การรักษาความปลอดภัยด้านการสื่อสาร A.13.2 การโอนถ่ายข้อมูล วัตถุประสงค์: เพื่อรักษาการรักษาความปลอดภัยของสารสนเทศที่โอนถ่ายภายในองค์กรและกับองค์กรภายนอก	A.13.2.1 มีนโยบายการโอนถ่ายอย่างเป็นทางการ กระบวนการทำงานและการควบคุมต่าง ๆ เพื่อป้องกันการโอนถ่ายข้อมูลผ่านการใช้สิ่งอำนวยความสะดวกด้านการสื่อสารทุกประเภทหรือไม่ A.13.2.2 มีข้อตกลงต่าง ๆ เพื่อกล่าวถึงการโอนถ่ายที่ปลอดภัยสำหรับข้อมูลทางธุรกิจระหว่างองค์กรกับบุคคลภายนอกหรือไม่ A.13.2.3 มีการป้องกันข้อมูลที่เกี่ยวข้องในการส่งข้อความทางอิเล็คทรอนิกส์อย่างเหมาะสมหรือไม่ A.13.2.4 มีการบ่งชี้ ทบทวนเป็นประจำเกี่ยวกับข้อกำหนดต่างๆ สำหรับข้อตกลงในการรักษาข้อมูลความลับหรือการไม่เปิดเผยที่สะท้อนให้เห็นความต้องการขององค์กรในการป้องกันข้อมูล รวมทั้งทำเป็นเอกสารหรือไม่		
A.14 การครอบครอง การพัฒนาและการบำรุงรักษาระบบ A.14.1 ข้อกำหนดด้านการรักษาความปลอดภัยของระบบข้อมูล วัตถุประสงค์: เพื่อทำให้มั่นใจว่าการรักษาความปลอดภัยของสารสนเทศเป็นส่วนสำคัญของระบบข้อมูลตลอดทั้งวงจรชีวิต รวมถึงข้อกำหนดต่างๆ สำหรับระบบข้อมูลที่ให้บริการทั่วเครือข่ายสาธารณะ	A.14.1.1 ข้อกำหนดเกี่ยวกับการรักษาความปลอดภัยของสารสนเทศได้รวมอยู่ในข้อกำหนดต่างๆ สำหรับระบบข้อมูลใหม่หรือการยกระดับข้อมูลที่มีอยู่หรือไม่ สำหรับระบบหรือไม่ A.14.1.2 มีการป้องกันข้อมูลที่เกี่ยวข้องในการให้บริการแอพพลิเคชั่นที่ส่งผ่านเครือข่ายสาธารณะจากกิจกรรมที่หลอกลวง ข้อพิพาททางสัญญา รวมถึงการเปิดเผยและการดัดแปลงแก้ไขที่ไม่ได้รับอนุญาต หรือไม่ A.14.1.3 มีการป้องกันข้อมูลที่เกี่ยวข้องในธุรกรรมการให้บริการแอพพลิเคชั่นเพื่อป้องกันการโอนที่ไม่สมบูรณ์ การส่งผิดเส้นทาง การเปลี่ยนข้อความที่ไม่ได้รับอนุญาต การเปิดเผยที่ไม่ได้รับอนุญาต การทำซ้ำหรือการเล่นซ้ำข้อความที่ไม่ได้รับอนุญาตหรือไม่		
A.14 การครอบครอง การพัฒนาและการบำรุงรักษาระบบ A.14.2 การรักษาความปลอดภัยในกระบวนการการพัฒนาและ	A.14.2.1 มีการจัดทำกฎระเบียบสำหรับการพัฒนาซอฟต์แวร์และระบบและมีการประยุกต์ใช้กฎระเบียบต่างๆ เพื่อการพัฒนาภายในองค์กรหรือไม่		

สนับสนุน วัตถุประสงค์: เพื่อทำให้มั่นใจว่ามีการออกแบบและนำไปปฏิบัติ (implemented)รักษาความปลอดภัยของสารสนเทศภายในวงจรชีวิตในการพัฒนาระบบข้อมูล	A.14.2.2 มีการควบคุมการเปลี่ยนแปลงต่าง ๆ สำหรับระบบภายในวงจรชีวิตในการพัฒนาด้วยการใช้กระบวนการทำงานในการควบคุมการเปลี่ยนแปลงที่เป็นทางการหรือไม่ A.14.2.3 เมื่อแพลตฟอร์มปฏิบัติการมีการเปลี่ยนแปลง ได้มีการทบทวนแอพพลิเคชั่นที่สำคัญทางธุรกิจและทำการทดสอบเพื่อทำให้มั่นใจว่าไม่มีผลกระทบย้อนกลับต่อการดำเนินงานขององค์กรหรือการรักษาความปลอดภัยหรือไม่ A.14.2.4 มีการกีดกันการดัดแปลงแก้ไขต่าง ๆ สำหรับชุดซอฟต์แวร์ มีการจำกัดการเปลี่ยนแปลงที่จำเป็นและมีการควบคุมการเปลี่ยนแปลงต่างๆ ทั้งหมดอย่างเข้มงวดหรือไม่ A.14.2.5 มีการจัดทำเอกสาร รักษาและประยุกต์ใช้หลักการต่างๆ เกี่ยวกับระบบความปลอดภัยด้านวิศวกรรมสำหรับความพยายามในการดำเนินระบบสารสนเทศ (information system implementation efforts) หรือไม่ A.14.2.6 องค์กรทำและปกป้องสภาพแวดล้อมในการพัฒนาที่ปลอดภัยอย่างเหมาะสมสำหรับความพยายามในการพัฒนาและบูรณาการระบบหรือไม่ สภาพแวดล้อมในการพัฒนาที่ปลอดภัยเหล่านี้ได้ครอบคลุมวงจรชีวิตในการพัฒนาระบบทั้งหมดหรือไม่ A.14.2.7 องค์กรได้ควบคุมและเฝ้าระวังกิจกรรมการพัฒนาระบบโดยผู้รับเหมาจ้างช่วงหรือไม่ A.14.2.8 มีการนำทดสอบการทำงานด้านการรักษาความปลอดภัยระหว่างการพัฒนาหรือไม่ A.14.2.9 มีการทำโปรแกรมการทดสอบการยอมรับและเกณฑ์ที่เกี่ยวข้องสำหรับระบบสารสนเทศใหม่ ,การอัพเกรด และเวอร์ชั่นใหม่หรือไม่		
A.14 การครอบครอง การพัฒนาและการบำรุงรักษาระบบ A.14.3 ข้อมูลการทดสอบ วัตถุประสงค์: เพื่อทำให้มั่นใจในการป้องกันข้อมูลที่ใช้เพื่อการ	A.14.3.1 มีการคัดเลือกข้อมูลการทดสอบอย่างระมัดระวัง รวมถึงป้องกันและควบคุมหรือไม่		

ทดสอบ			
A.15 ความสัมพันธ์กับซัพพลายเออร์ A.15.1 การรักษาความปลอดภัยของสารสนเทศในความสัมพันธ์กับซัพพลายเออร์ วัตถุประสงค์: เพื่อทำให้มั่นใจในการป้องกันสินทรัพย์ขององค์กรที่ซัพพลายเออร์สามารถเข้าถึงได้	A.15.1.1 มีการตกลงข้อกำหนดด้านการรักษาความปลอดภัยของสารสนเทศสำหรับการบรรเทาความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับการเข้าถึงสินทรัพย์ขององค์กรของแต่ละซัพพลายเออร์ และทำเป็นเอกสารหรือไม่ A.15.1.2 มีการจัดทำข้อกำหนดด้านการรักษาความปลอดภัยของสารสนเทศที่เกี่ยวข้องทั้งหมดกับแต่ละซัพพลายเออร์ที่อาจเข้าถึง ทำการประมวลผล จัดเก็บ สื่อสารหรือให้ส่วนประกอบโครงสร้างพื้นฐานด้าน IT สำหรับข้อมูลขององค์กรหรือไม่ A.15.1.3 ข้อตกลงกับซัพพลายเออร์ต่าง ๆ ได้รวมข้อกำหนดในการหาความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศที่เกี่ยวข้องกับข้อมูลและการให้บริการด้านเทคโนโลยีการสื่อสารรวมถึงห่วงโซ่อุปทานสินค้าหรือไม่		
A.15 ความสัมพันธ์กับซัพพลายเออร์ A.15.2 การบริหารการส่งมอบบริการของซัพพลายเออร์ วัตถุประสงค์: เพื่อรักษาการรักษาความปลอดภัยของสารสนเทศในระดับที่ตกลงกันและการส่งมอบบริการตามข้อตกลงของซัพพลายเออร์	A.15.2.1 องค์กรมีการสังเกตการณ์ ทบทวนและตรวจติดตามการส่งมอบบริการของซัพพลายเออร์เป็นประจำหรือไม่ A.15.2.2 มีการบริหารการเปลี่ยนแปลงต่างๆ สำหรับการให้บริการโดยซัพพลายเออร์ซึ่งรวมถึงการบำรุงรักษาและการปรับปรุงนโยบายการรักษาความปลอดภัยของสารสนเทศที่มีอยู่ กระบวนการทำงานและการควบคุมต่าง ๆ โดยคำนึงถึงภาวะวิกฤตของข้อมูลทางธุรกิจ ระบบและกระบวนการต่าง ๆ ที่เกี่ยวข้องและการประเมินความเสี่ยงต่าง ๆ ซ้ำหรือไม่		
A.16 การบริหารอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศ A.16.1 การบริหารอุบัติการณ์และการปรับปรุงด้านการรักษาความปลอดภัยของสารสนเทศ วัตถุประสงค์: เพื่อทำให้มั่นใจในวิธีการที่สอดคล้องและมีประสิทธิผลสำหรับการบริหารอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศรวมถึงการสื่อสารด้านเหตุการณ์การ	A.16.1.1 มีการกำหนดความรับผิดชอบของฝ่ายบริหารและกระบวนการทำงานเพื่อทำให้มั่นใจในการตอบสนองที่รวดเร็ว มีประสิทธิผลและเป็นระเบียบต่ออุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ A.16.1.2 มีการรายงานเหตุการณ์ด้านการรักษาความปลอดภัยของสารสนเทศผ่านช่องทางการบริการที่เหมาะสมโดยเร็วที่สุดเท่าที่จะเป็นไปได้หรือไม่ A.16.1.3 มีการกำหนดให้พนักงานและผู้รับเหมาที่ใช้ระบบข้อมูลขององค์กรและบริการจะต้องจดบันทึกและรายงานจุดอ่อนด้านการรักษาความปลอดภัยของสารสนเทศที่สังเกตเห็นหรือที่สงสัยในระบบหรือการให้บริการต่างๆ หรือไม่		

รักษาความปลอดภัยและจุดอ่อนต่างๆ	A.16.1.4 มีการประเมินเหตุการณ์ด้านการรักษาความปลอดภัยของสารสนเทศและมีการพิจารณากำหนด(determined)ว่าเหตุการณ์ต่าง ๆ ต้องแยกประเภทเป็นอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศหรือไม่ A.16.1.5 มีการตอบสนองอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศตามกระบวนการทำงานที่เป็นเอกสารหรือไม่ A.16.1.6 มีการใช้ความรู้ที่ได้รับจากการวิเคราะห์และการแก้ไขอุบัติการณ์ด้านการรักษาความปลอดภัยของสารสนเทศเพื่อลดความเป็นไปได้หรือผลกระทบของอุบัติการณ์ในอนาคตหรือไม่ A.16.1.7 องค์กรได้กำหนดและประยุกต์ใช้กระบวนการทำงานในการบ่งชี้ การจัดเก็บ การครอบครอง และการข้อมูลที่สามารถใช้เป็นหลักฐานหรือไม่		
A.17 ด้านต่าง ๆ เกี่ยวกับการรักษาความปลอดภัยของสารสนเทศสำหรับการบริหารความต่อเนื่องทางธุรกิจ A.17.1 ความต่อเนื่องด้านการรักษาความปลอดภัยของสารสนเทศ วัตถุประสงค์: เพื่อให้ความต่อเนื่องด้านการรักษาความปลอดภัยของสารสนเทศฝังตัวอยู่ในระบบบริหารความต่อเนื่องทางธุรกิจขององค์กร	A.17.1.1 องค์กรได้พิจารณากำหนด(determined)ข้อกำหนดต่างๆ สำหรับการรักษาความปลอดภัยของสารสนเทศและการบริการต่อเนื่องด้านการรักษาความปลอดภัยของสารสนเทศในสถานการณ์ย้อนกลับ ตัวอย่างเช่น ระหว่างวิกฤตหรือภัยพิบัติหรือไม่ A.17.1.2 องค์กรได้จัดทำเอกสารและนำไปปฏิบัติ รวมถึงธำรงรักษากระบวนการ กระบวนการทำงานและการควบคุมต่าง ๆ เพื่อทำให้มั่นใจในระดับที่จำเป็นสำหรับการต่อเนื่องด้านการรักษาความปลอดภัยของสารสนเทศระหว่างสถานการณ์ย้อนกลับ (adverse situation) หรือไม่ A.17.1.3 องค์กรได้ตรวจสอบการควบคุมการต่อเนื่องด้านการรักษาความปลอดภัยของสารสนเทศที่จัดทำและนำไปปฏิบัติในช่วงเวลาตามแผนเพื่อทำให้มั่นใจว่าการควบคุมมีผลใช้ได้และมีประสิทธิผลระหว่างสถานการณ์ย้อนกลับ(adverse situation) หรือไม่		
A.17 ด้านต่าง ๆ เกี่ยวกับการรักษาความปลอดภัยของสารสนเทศสำหรับการบริหารความต่อเนื่องทางธุรกิจ	A.17.2.1 มีการนำไปปฏิบัติสิ่งอำนวยความสะดวกในการประมวลข้อมูลที่มีความซ้ำซ้อนเพียงพอที่จะบรรลุข้อกำหนดในการมีพร้อมใช้หรือไม่?		

A.17.2 ความซ้ำซ้อน วัตถุประสงค์: เพื่อทำให้มั่นใจในการมีสิ่งอำนวยความสะดวกในการประมวลข้อมูลพร้อมใช้			
A.18 ความสอดคล้อง A.18.1 ความสอดคล้องกับข้อกำหนดทางกฎหมายและตามสัญญา วัตถุประสงค์: เพื่อหลีกเลี่ยงการละเมิดข้อบังคับตามกฎหมาย พระราชบัญญัติ กฎระเบียบ หรือตามสัญญาที่เกี่ยวกับข้อกำหนดการรักษาความปลอดภัยของสารสนเทศและข้อกำหนดด้านการรักษาความปลอดภัยอื่น ๆ	A.18.1.1 มีการบ่งชี้ ทำเอกสาร ข้อกำหนดทางกฎหมาย พระราชบัญญัติ กฎระเบียบและตามสัญญาทั้งหมดรวมถึงวิธีการขององค์กรในการบรรลุข้อกำหนดต่าง ๆ เหล่านี้อย่างชัดเจนและคอยอัพเดตแต่ละระบบข้อมูลและองค์กรหรือไม่ A.18.1.2 มีการดำเนินกระบวนการทำงานที่เหมาะสมเพื่อทำให้มั่นใจในความสอดคล้องกับข้อกำหนดทางกฎหมาย กฎระเบียบและตามสัญญาที่เกี่ยวกับสิทธิทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์หรือไม่ A.18.1.3 มีการป้องกันบันทึกต่าง ๆ จากการสูญเสีย การทำลาย การปลอมแปลง การเข้าถึงที่ไม่ได้รับอนุญาตและการปล่อยที่ไม่ได้รับอนุญาตตามข้อกำหนดทางกฎหมาย กฎระเบียบ สัญญาและทางธุรกิจ หรือไม่ A.18.1.4 มีการทำให้มั่นใจในความเป็นส่วนตัวและการปกป้องข้อมูลที่สามารถบ่งชี้ตัวบุคคลตามที่กำหนดในกฎหมายและกฎระเบียบเมื่อบังคับใช้หรือไม่ A.18.1.5 มีการใช้การควบคุมการเข้ารหัสโดยสอดคล้องกับข้อตกลง กฎหมายและกฎระเบียบที่เกี่ยวข้องทั้งหมดหรือไม่		
A.18 ความสอดคล้อง A.18.2 การทบทวนด้านการรักษาความปลอดภัยของสารสนเทศ วัตถุประสงค์: เพื่อทำให้มั่นใจว่ามีการปฏิบัติและนำไปปฏิบัติ (implemented)รักษาความปลอดภัยของสารสนเทศตามนโยบายและกระบวนการทำงานขององค์กร	A.18.2.1 มีการทบทวนวิธีการขององค์กรในการบริหารการรักษาความปลอดภัยของสารสนเทศและการดำเนินงาน (ตัวอย่างเช่น วัตถุประสงค์ในการควบคุม การควบคุม นโยบายการปลอดภัย กระบวนการและกระบวนการทำงานต่าง ๆ สำหรับการรักษาความปลอดภัยของสารสนเทศ) อย่างเป็นอิสระในช่วงเวลาตามแผนหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้นหรือไม่ A.18.2.2 ผู้จัดการต่าง ๆ ได้ทบทวนความสอดคล้องของการประมวลข้อมูลและกระบวนการทำงานภายในพื้นที่รับผิดชอบของตนเองด้วยนโยบายการรักษาความปลอดภัยที่เหมาะสมมาตรฐานและข้อกำหนดด้านการรักษาความปลอดภัยอื่นๆ หรือไม่		

	A.18.2.3 มีการทบทวนระบบข้อมูลด้านความสอดคล้องกับนโยบายและมาตรฐานการรักษาความปลอดภัยของสารสนเทศขององค์กรเป็นประจำหรือไม่		