รายการตรวจสอบเพื่อทวนสอบความสอดคล้องกับข้อกำหนด ISO27001: 2013

มาตรา	จุดตรวจสอบ * ขั้นตอน หมายถึง process (กระบวนการ ลำดับขั้นตอน วิธียึดปฏิบัติ)	หลักฐานการสอดคล้อง	ผลการประเมิน
4. บริบทขององค์กร 4.1 ความเข้าใจองค์กรและบริบทขององค์กร	4.1 มีขั้นตอนเพื่อทำให้องค์กรสามารถตัดสินปัญหาภายนอกและภายในที่เกี่ยวข้องกับวัตถุประสงค์ขององค์กรและที่ส่งผลกระทบต่อความสามารถขององค์กรในการบรรลุผลลัพธ์ (ต่าง ๆ) ที่ตั้งใจไว้ของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลขององค์กรหรือไม่		
4. บริบทขององค์กร 4.2 ความเข้าใจความต้องการและความคาดหวัง	4.2a มีขั้นตอนที่จะสามารถทำให้องค์กรสามารถตัดสินผู้ที่มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 4.2.b มีขั้นตอนเพื่อทำให้องค์กรสามารถตัดสินข้อกำหนดต่างๆ ของผู้ที่มีส่วนได้ส่วนเสียต่าง ๆ เหล่านี้ที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลหรือไม่		
4. บริบทขององค์กร 4.3 การตัดสินขอบเขตของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูล	4.3.a องค์กรได้ตัดสินขอบข่ายและการประยุกต์ใช้ระบบบริหารในการรักษาความปลอดภัยของข้อมูลเพื่อจัดตั้งขอบเขตของระบบหรือไม่ 4.3.b เมื่อทำการตัดสินขอบเขตของ ISMS องค์กรได้พิจารณาปัญหาภายนอกและภายในที่อ้างอิงไว้ใน 4.1 หรือไม่ 4.3.c เมื่อทำการตัดสินขอบเขตของ ISMS องค์กรได้พิจารณาข้อกำหนดต่าง ๆ ที่อ้างอิงไว้ใน 4.2 หรือไม่ 4.3.d เมื่อทำการตัดสินขอบเขตของ ISMS องค์กรได้พิจารณาอินเตอร์เฟซและการพึ่งพาต่าง ๆ ระหว่างกิจกรรมต่าง ๆ ที่ปฏิบัติโดยองค์กรและที่ปฏิบัติโดยองค์กรอื่น ๆ หรือไม่ 4.3.e องค์กรได้ทำขอบเขตที่มีพร้อมให้เป็นข้อมูลที่เป็นเอกสารหรือไม่		
4. บริบทขององค์กร 4.4 ระบบบริหารด้านการรักษาความปลอดภัยของข้อมูล	4.4.a องค์กรได้จัดตั้งระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลตามข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013 หรือไม่ 4.4.b องค์กรได้ดำเนินระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลตามข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013 หรือไม่ 4.4.c องค์กรมีขั้นตอนต่าง ๆ สำหรับการรักษาระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลขององค์กรตามข้อกำหนดต่างๆ ของ ISO/IEC		

	27001:2013 หรือไม่ 4.4.d องค์กรมีขั้นตอนต่าง ๆ สำหรับการปรับปรุงระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลอย่างต่อเนื่องตามข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013 หรือไม่		
5 ความเป็นผู้นำ 5.1 ความเป็นผู้นำและคำมั่นสัญญา	มีคำมั่นสัญญาในด้านระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยทำให้มั่นใจว่ามีการจัดตั้งนโยบายการรักษาความปลอดภัยของข้อมูลและวัตถุประสงค์ในการรักษาความปลอดภัยของข้อมูล และสามารถเข้าได้กับทิศทางเชิงกลยุทธ์ขององค์กรหรือไม่ 5.1.b ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและคำมั่นสัญญาในด้านระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยทำให้มั่นใจในการรวมข้อกำหนดต่าง ๆ ของระบบบริหารในการรักษาความปลอดภัยของข้อมูลเข้าในขั้นตอนต่าง ๆ ขององค์กรหรือไม่ 5.1.c ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและคำมั่นสัญญาในด้านระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยทำให้มั่นใจว่ามีทรัพยากรต่าง ๆ ที่จำเป็นสำหรับระบบบริหารในการรักษาความปลอดภัยของข้อมูลพร้อมใช้หรือไม่ 5.1.d ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและคำมั่นสัญญาในด้านระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยทำการสื่อสารความสำคัญของการบริหารด้านการรักษาความปลอดภัยของข้อมูลที่มีประสิทธิภาพ และมีความสอดคล้องกับข้อกำหนดต่างๆ ของระบบบริหารในการรักษาความปลอดภัยของข้อมูลหรือไม่ 5.1.e ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและคำมั่นสัญญาในด้านระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยทำให้มั่นใจว่าระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลจะบรรลุผลลัพธ์(ต่าง ๆ) ที่ตั้งใจไว้หรือไม่ 5.1.f ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและคำมั่นสัญญาในด้านระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยการชี้แนะและสนับสนุนบุคคลต่าง ๆ ในการส่งเสริมประสิทธิภาพของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 5.1.g ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและคำมั่นสัญญาในด้านระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยการส่งเสริมการ		

	ปรับปรุงอย่างต่อเนื่องหรือไม่ 5.1.h ฝ่ายบริหารสูงสุดแสดงให้เห็นความเป็นผู้นำและคำมั่นสัญญาในด้านระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยการสนับสนุนบทบาทบริหารอื่น ๆ ในการแสดงให้เห็นความเป็นผู้นำเมื่อประยุกต์ใช้กับพื้นที่ความรับผิดชอบของตนเองหรือไม่		
5 ความเป็นผู้นำ 5.2 นโยบาย	5.2.a ฝ่ายบริหารสงสุดได้จัดตั้งนโยบายการรักษาความปลอดภัยของข้อมูลที่เหมาะสมกับวัตถุประสงค์ขององค์กรหรือไม่ 5.2.b ฝ่ายบริหารสงสุดได้จัดตั้งนโยบายการรักษาความปลอดภัยของข้อมูลที่รวมวัตถุประสงค์ในการรักษาความปลอดภัยของข้อมูล (ดูที่ 6.2) หรือให้กรอบการทำงานสำหรับการตั้งวัตถุประสงค์ในการรักษาความปลอดภัยของข้อมูลหรือไม่ 5.2.c ฝ่ายบริหารสงสุดได้จัดตั้งนโยบายการรักษาความปลอดภัยของข้อมูลที่รวมคำมั่นสัญญาในการบรรลุตามข้อกำหนดต่างๆ ที่บังคับใช้ซึ่งเกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลหรือไม่ 5.2.d ฝ่ายบริหารสงสุดได้จัดตั้งนโยบายการรักษาความปลอดภัยของข้อมูลที่รวมคำมั่นสัญญาในการปรับปรุงระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลอย่างต่อเนื่องหรือไม่ 5.2.e มีการทำให้นโยบายการรักษาความปลอดภัยของข้อมูลมีพร้อมใช้เป็นข้อมูลที่เป็นเอกสารหรือไม่ 5.2.f มีการสื่อสารนโยบายการรักษาความปลอดภัยของข้อมูลภายในองค์กรหรือไม่ 5.2.g มีการทำนโยบายการรักษาความปลอดภัยของข้อมูลมีพร้อมใช้สำหรับผู้มีส่วนได้ส่วนเสียอย่างเหมาะสมหรือไม่		
5 ความเป็นผู้นำ 5.3 บทบาทองค์กร ความรับผิดชอบและอำนาจหน้าที่	5.3.a ฝ่ายบริหารสูงสุดทำให้มั่นใจว่ามีการมอบหมายและสื่อสารความรับผิดชอบและอำนาจหน้าที่สำหรับบทบาทต่าง ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลหรือไม่ 5.3.b ฝ่ายบริหารสูงสุดได้มอบหมายความรับผิดชอบและอำนาจหน้าที่ในการทำให้มั่นใจว่าระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลมีความสอดคล้องกับข้อกำหนดต่างๆ ของ ISO/IEC 27001 หรือไม่		

	5.3.c ฝ่ายบริหารสูงสุดได้มอบหมายความรับผิดชอบและอำนาจหน้าที่ในการรายงานประสิทธิภาพการทำงานของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลให้ฝ่ายบริหารสูงสุดหรือไม่		
6 การวางแผน 6.1 ปฏิบัติการในการหาความเสี่ยงและโอกาสต่าง ๆ 6.1.1 ทั่วไป	6.1.1.a เมื่อทำการวางแผนระบบบริหารด้านการรักษาความปลอดภัยของข้อมูล องค์กรพิจารณาปัญหาต่าง ๆ ที่อ้างอิงใน 4.1 และตามข้อกำหนดต่างๆ ที่อ้างอิงใน 4.2 รวมถึงตัดสินความเสี่ยงและโอกาสต่าง ๆ ที่ต้องหาเพื่อทำให้มั่นใจว่าระบบบริหารในการรักษาความปลอดภัยของข้อมูลจะสามารถบรรลุผลลัพธ์ (ต่าง ๆ) ที่ตั้งใจไว้หรือไม่ 6.1.1.b เมื่อทำการวางแผนระบบบริหารด้านการรักษาความปลอดภัยของข้อมูล องค์กรพิจารณาปัญหาต่าง ๆ ที่อ้างอิงใน 4.1 และตามข้อกำหนดต่างๆ ที่อ้างอิงใน 4.2 รวมถึงตัดสินความเสี่ยงและโอกาสต่าง ๆ ที่ต้องหาเพื่อป้องกันหรือลดผลกระทบต่าง ๆ ที่ไม่พึงปรารถนาหรือไม่ 6.1.1.c เมื่อทำการวางแผนระบบบริหารด้านการรักษาความปลอดภัยของข้อมูล พิจารณาปัญหาต่าง ๆ ที่อ้างอิงใน 4.1 และตามข้อกำหนดต่างๆ ที่อ้างอิงใน 4.2 รวมถึงตัดสินความเสี่ยงและโอกาสต่าง ๆ ที่ต้องหาเพื่อบรรลุการปรับปรุงอย่างต่อเนื่องหรือไม่ 6.1.1.d องค์กรวางแผนปฏิบัติการต่าง ๆ เพื่อหาความเสี่ยงและโอกาสต่าง ๆ เหล่านี้หรือไม่ 6.1.1.e องค์กรวางแผนวิธีที่จะ 1) รวมและดำเนินปฏิบัติการต่างๆ เหล่านี้เข้าในขั้นตอนของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลขององค์กร และ 2) ประเมินประสิทธิภาพของปฏิบัติการต่างๆ เหล่านี้ หรือไม่		
6 การวางแผน 6.1 ปฏิบัติการในการหาความเสี่ยงและโอกาสต่าง ๆ 6.1.2 การประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูล	6.1.2.a องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลที่จัดตั้งและรักษาเกณฑ์ความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลที่จะรวมถึง 1) เกณฑ์การยอมรับความเสี่ยง และ 2) เกณฑ์สำหรับการปฏิบัติการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 6.1.2.b องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลที่ทำให้มั่นใจว่าการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลซ้ำจะสร้างผลที่สอดคล้อง ถูกต้องและสามารถเปรียบเทียบ หรือไม่ 6.1.2.c องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลที่ 1) บ่งชี้ความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับการ		

	สูญเสียการรักษาข้อมูลความลับ บูรณภาพและการมีข้อมูลพร้อมใช้ภายในขอบเขตของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูล และ 2) บ่งชี้เจ้าของความเสี่ยงต่าง ๆ หรือไม่ 6.1.2.d องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลที่วิเคราะห์ความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลดังต่อไปนี้ 1) ประเมินผลที่ตามมาที่เป็นไปได้ที่จะส่งผลหากผลต่าง ๆ ที่บ่งชี้ใน 6.1.2 c) 1) ถูกทำให้เป็นรูปเป็นร่างขึ้น 2) ประเมินความเป็นไปได้ที่เป็นจริงในการเกิดความเสี่ยงต่าง ๆ ที่บ่งชี้ใน 6.1.2 c) 1) และ 3) ตัดสินระดับความเสี่ยงต่าง ๆ หรือไม่ 6.1.2.e องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลที่ประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลที่วิเคราะห์ความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลดังต่อไปนี้ 1) เปรียบเทียบผลการวิเคราะห์ความเสี่ยงต่าง ๆ กับเกณฑ์ความเสี่ยงที่กำหนดไว้ใน 6.1.2 a) และ 2) จัดลำดับความสำคัญสำหรับความเสี่ยงที่ถูกวิเคราะห์เพื่อดูแลความเสี่ยง หรือไม่ 6.1.2.f องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารเกี่ยวกับการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลหรือไม่		
6 การวางแผน 6.1 ปฏิบัติการในการหาความเสี่ยงและโอกาสต่าง ๆ 6.1.3 การดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูล	6.1.3.a องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลเพื่อคัดเลือกทางเลือกในการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลโดยคำนึงถึงผลการประเมินความเสี่ยงต่าง ๆ หรือไม่ 6.1.3.b องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลเพื่อตัดสินการควบคุมต่างๆ ทั้งหมดที่จำเป็นในการดำเนินทางเลือกในการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูล (ต่าง ๆ) ที่เลือกไว้หรือไม่ 6.1.3.c องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลเพื่อเปรียบเทียบการควบคุมต่าง ๆ ที่ตัดสินไว้ใน 6.1.3.b ข้างต้นกับการควบคุมต่าง ๆ ในภาคผนวก A และตรวจพิสูจน์ว่าไม่มีการควบคุมต่าง ๆ ที่จำเป็นถูกข้ามไป หรือไม่ 6.1.3.d องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลเพื่อสร้างเอกสารแสดงมาตรการในมาตรฐานที่มีการควบคุมต่าง ๆ ที่จำเป็น (ดูที่ 6.1.3.b และ c) และการให้เหตุผลสำหรับ		

	การรวมเข้าไปต่าง ๆ ที่มีการดำเนินการหรือไม่ รวมถึงการให้เหตุผลสำหรับการยกเว้นการควบคุมต่าง ๆ จากภาคผนวก A หรือไม่ 6.1.3.e องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลเพื่อสร้างแผนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 6.1.3.f องค์กรกำหนดและประยุกต์ใช้ขั้นตอนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลเพื่อได้รับอนุมัติจากเจ้าของความเสี่ยงต่างๆ สำหรับแผนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลและการยอมรับความเสี่ยงที่เหลือด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 6.1.3.h องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารเกี่ยวกับขั้นตอนแผนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลหรือไม่		
6 การวางแผน 6.2 วัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลและแผนงานต่างๆ เพื่อทำให้บรรลุ	6.2.a องค์กรจัดตั้งวัตถุประสงค์ต่าง ๆ ด้านการรักษาความปลอดภัยของข้อมูลในหน้าที่งานและระดับต่าง ๆ ที่เกี่ยวข้องหรือไม่ 6.2.b วัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลมีความสอดคล้องกับนโยบายการรักษาความปลอดภัยของข้อมูลหรือไม่ 6.2.c วัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลสามารถวัดผลได้ (หากสามารถปฏิบัติได้) หรือไม่ 6.2.d วัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลมีการคำนึงถึงข้อกำหนดต่าง ๆ ด้านการรักษาความปลอดภัยของข้อมูลที่บังคับใช้ และผลการประเมินความเสี่ยงรวมถึงผลการดูแลความเสี่ยงหรือไม่ 6.2.e มีการสื่อสารวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 6.2.f มีการอัพเดตวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลอย่างเหมาะสมหรือไม่ 6.2.g องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารเกี่ยวกับวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 6.2.h เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูล องค์กรตัดสินสิ่งที่จะต้องทำหรือไม่		

	6.2.i เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูล องค์กรตัดสินทรัพยากรอะไรที่ต้องการหรือไม่ 6.2.j เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูล องค์กรตัดสินบุคคลที่จะรับผิดชอบหรือไม่ 6.2.k เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูล องค์กรตัดสินว่าจะทำเสร็จสมบูรณ์เมื่อไหร่หรือไม่ 6.2.l เมื่อทำการวางแผนวิธีที่จะบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูล องค์กรตัดสินวิธีที่จะประเมินผลต่างๆ หรือไม่		
7 การสนับสนุน 7.1 ทรัพยากร	7.1. มีขั้นตอนที่องค์กรใช้เพื่อตัดสินและให้ทรัพยากรที่จำเป็นสำหรับการจัดตั้ง การดำเนินการ การบำรุงรักษาและการปรับปรุงอย่างต่อเนื่องสำหรับวัตถุประสงค์ต่าง ๆ ของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลที่กำหนดไว้ใน 6.2 หรือไม่		
7. การสนับสนุน 7.2 ความชำนาญ	7.2.a มีขั้นตอนที่องค์กรใช้เพื่อตัดสินความชำนาญที่จำเป็นของบุคคล (ต่าง ๆ) ที่ทำงานภายใต้การควบคุมขององค์กรที่ส่งผลกระทบต่อประสิทธิภาพการทำงานด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 7.2.b มีขั้นตอนที่ใช้เพื่อทำให้มั่นใจว่าบุคคลต่าง ๆ เหล่านี้มีความชำนาญด้านพื้นฐานการศึกษา การฝึกอบรมหรือประสบการณ์ที่เหมาะสมหรือไม่ 7.2.c มีขั้นตอนที่ใช้เพื่อดำเนินปฏิบัติการต่าง ๆ ในการได้รับความชำนาญที่จำเป็นเมื่อมีการบังคับใช้ รวมถึงประเมินประสิทธิภาพของปฏิบัติการต่าง ๆ ที่ดำเนินการหรือไม่ 7.2.d มีการเก็บรักษาข้อมูลที่เป็นเอกสารที่เหมาะสมให้เป็นหลักฐานด้านความชำนาญหรือไม่		
7. การสนับสนุน 7.3 การตระหนักถึง	7.3.a มีขั้นตอนที่องค์กรใช้เพื่อทำให้มั่นใจว่าบุคคลต่าง ๆ ที่ทำงานภายใต้การควบคุมขององค์กรมีการตระหนักถึงนโยบายด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 7.3.b มีขั้นตอนที่องค์กรใช้เพื่อทำให้มั่นใจว่าบุคคลต่าง ๆ ที่ทำงานภายใต้การควบคุมขององค์กรมีการตระหนักถึงการสนับสนุนประสิทธิภาพของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลโดยรวมถึงประโยชน์ต่าง ๆ ของประสิทธิภาพในการทำงานด้านการรักษาความปลอดภัยของข้อมูลที่มีการปรับปรุงแล้ว หรือไม่		

	7.3.c มีขั้นตอนที่องค์กรใช้เพื่อทำให้มั่นใจว่าบุคคลต่าง ๆ ที่ทำงานภายใต้การควบคุมขององค์กรมีการตระหนักถึงความเกี่ยวพันของการไม่ปฏิบัติตามข้อกำหนดต่าง ๆ ของระบบบริหารในการรักษาความปลอดภัยของข้อมูลหรือไม่		
7. การสนับสนุน 7.4 การสื่อสาร	7.4.a มีขั้นตอนที่องค์กรใช้เพื่อตัดสินความต้องการสำหรับการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 7.4.b ขั้นตอนนี้ได้บ่งชี้สิ่งที่จะสื่อสารหรือไม่ 7.4.c ขั้นตอนนี้ได้บ่งชี้เวลาที่จะสื่อสารหรือไม่ 7.4.d ขั้นตอนนี้ได้บ่งชี้ว่าจะต้องสื่อสารถึงใครหรือไม่ 7.4.e ขั้นตอนนี้ได้บ่งชี้ว่าใครจะทำการสื่อสารหรือไม่ 7.4.f ขั้นตอนนี้ได้บ่งชี้ขั้นตอนต่าง ๆ ที่จะส่งผลกระทบต่อการสื่อสารหรือไม่		
7. การสนับสนุน 7.5 ข้อมูลที่เป็นเอกสาร 7.5.1 ทั่วไป	7.5.1.a ระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลขององค์กรได้รวมข้อมูลที่เป็นเอกสารซึ่งกำหนดโดย ISO/IEC 27001:2013 หรือไม่ 7.5.1.b ระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลขององค์กรได้รวมข้อมูลที่เป็นเอกสารซึ่งตัดสินโดยองค์กรว่ามีความจำเป็นสำหรับประสิทธิภาพของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่		
7. การสนับสนุน 7.5 ข้อมูลที่เป็นเอกสาร 7.5.2 การสร้างและการอัพเดต	7.5.2.a เมื่อทำการสร้างและอัพเดตข้อมูลที่เป็นเอกสาร องค์กรมีขั้นตอนที่จะทำให้มั่นใจในการบ่งชี้และรายละเอียดที่เหมาะสม (ตัวอย่างเช่น ชื่อเรื่อง วันที่ ผู้เขียนหรือหมายเลขอ้างอิง) หรือไม่ 7.5.2.b เมื่อทำการสร้างและอัพเดตข้อมูลที่เป็นเอกสาร องค์กรมีขั้นตอนที่จะทำให้มั่นใจในรูปแบบ (ตัวอย่างเช่น ภาษา เวอร์ชั่นซอฟต์แวร์ กราฟิก) และสื่อ (ตัวอย่างเช่น กระดาษ ทางอิเลคทรอนิกส์) ที่เหมาะสมหรือไม่ 7.5.2.c เมื่อทำการสร้างและอัพเดตข้อมูลที่เป็นเอกสาร องค์กรมีขั้นตอนที่จะทำให้มั่นใจในการทบทวนและการอนุมัติที่เหมาะสมสำหรับความเหมาะสมและความเพียงพอหรือไม่		
7 การสนับสนุน 7.5 ข้อมูลที่เป็นเอกสาร	7.5.3.a องค์กรมีขั้นตอนในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบบริหารในการรักษาความปลอดภัยของข้อมูลและโดย ISO/IEC 27001:2013 เพื่อทำให้มั่นใจว่าข้อมูลมีพร้อมใช้และเหมาะสมในการใช้งาน		

7.5.3 การควบคุมข้อมูลที่เป็นเอกสาร	สถานที่และเวลาที่ต้องการ หรือไม่ 7.5.3.b องค์กรมีขั้นตอนในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบบริหารในการรักษาความปลอดภัยของข้อมูลและโดย ISO/IEC 27001:2013 เพื่อทำให้มั่นใจว่ามีการปกป้องข้อมูลอย่างเพียงพอ (ตัวอย่างเช่น จากการสูญเสียการรักษาข้อมูลความลับ การใช้งานที่ไม่เหมาะสม หรือการสูญเสียบูรณภาพ) หรือไม่ 7.5.3.c องค์กรมีขั้นตอนในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบบริหารในการรักษาความปลอดภัยของข้อมูลและโดย ISO/IEC 27001:2013 เพื่อกล่าวถึงการกระจาย การเข้าถึง การกู้คืนและการใช้งานตามความเหมาะสม หรือไม่ 7.5.3.d องค์กรมีขั้นตอนในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบบริหารในการรักษาความปลอดภัยของข้อมูลและโดย ISO/IEC 27001:2013 เพื่อกล่าวถึงการจัดเก็บ และการรักษาโดยรวมถึงการรักษาความถูกต้องตามกฎหมายอย่างเหมาะสมหรือไม่ 7.5.3.e องค์กรมีขั้นตอนในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบบริหารในการรักษาความปลอดภัยของข้อมูลและโดย ISO/IEC 27001:2013 เพื่อกล่าวถึงการควบคุมการเปลี่ยนแปลง (ตัวอย่างเช่น การควบคุมเวอร์ชั่น) อย่างเหมาะสมหรือไม่ 7.5.3.f องค์กรมีขั้นตอนในการควบคุมข้อมูลที่เป็นเอกสารที่กำหนดโดยระบบบริหารในการรักษาความปลอดภัยของข้อมูลและโดย ISO/IEC 27001:2013 เพื่อกล่าวถึงการเก็บรักษาและการทิ้งอย่างเหมาะสมหรือไม่ 7.5.3.g องค์กรมีขั้นตอนในการบ่งชี้อย่างเหมาะสมสำหรับข้อมูลที่เป็นเอกสารจากแหล่งที่มาภายนอกซึ่งองค์กรตัดสินว่าจำเป็นสำหรับการวางแผนและการดำเนินงานของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 7.5.3.h องค์กรมีขั้นตอนในควบคุมข้อมูลที่เป็นเอกสารจากแหล่งที่มาภายนอกซึ่งองค์กรตัดสินว่าจำเป็นสำหรับการวางแผนและการดำเนินงานของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่		
8 การดำเนินงาน 8.1 การวางแผนและการควบคุมด้าน	8.1.a มีขั้นตอนที่องค์กรใช้ในการวางแผน ดำเนินการและควบคุมขั้นตอนต่าง ๆ ที่จำเป็นต่อการบรรลุข้อกำหนดต่าง ๆ ด้านการรักษาความปลอดภัยของข้อมูลรวมถึงดำเนินปฏิบัติการต่างๆ ที่ตัดสินไว้ใน 6.1 หรือไม่		

การดำเนินงาน	8.1.b องค์กรได้ดำเนินแผนงานต่าง ๆ ในการบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลขององค์กรตามที่ตัดสินไว้ใน 6.2 หรือไม่ 8.1.c องค์กรเก็บข้อมูลที่เป็นเอกสารในขอบเขตที่จำเป็นต่อการมีความเชื่อมั่นว่ามีการดำเนินขั้นตอนต่างๆ ตามแผนหรือไม่ 8.1.d องค์กรควบคุมการเปลี่ยนแปลงต่างๆ ตามแผนและทบทวนผลที่ตามมาต่าง ๆ สำหรับการเปลี่ยนแปลงที่ไม่ได้ตั้งใจไว้โดยดำเนินปฏิบัติการในการบรรเทาผลกระทบย้อนกลับต่างๆ ตามที่จำเป็นหรือไม่ 8.1.e องค์กรทำให้มั่นใจว่ามีการตัดสินและควบคุมขั้นตอนที่จ้างผู้รับเหมาหรือไม่		
8 การดำเนินงาน 8.2 การบริหารความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูล	8.2.a มีขั้นตอนที่ใช้ในการดำเนินการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลในช่วงเวลาตามแผนหรือเมื่อมีการนำเสนอหรือมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้นโดยคำนึงถึงเกณฑ์ที่จัดตั้งไว้ใน 6.1.2 a) หรือไม่ 8.2.b องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารสำหรับผลการประเมินความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลหรือไม่		
8. การดำเนินงาน 8.3 การดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูล ข้อมูล	8.3.a องค์กรกำลังดำเนินแผนการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 8.3.b องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารสำหรับผลการดูแลความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลหรือไม่		
9 การประเมินประสิทธิภาพในการทำงาน 9.1 การสังเกตการณ์ การวัดผล การวิเคราะห์และการประเมินผล	9.1.a มีขั้นตอนที่ใช้ในการประเมินประสิทธิภาพการทำงานด้านการรักษาความปลอดภัยของข้อมูลและประสิทธิภาพของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 9.1.b ขั้นตอนตัดสินความต้องการอะไรที่จะต้องทำการสังเกตการณ์และวัดผลโดยรวมถึงขั้นตอนและการควบคุมต่างๆ ด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 9.1.c ขั้นตอนตัดสินวิธีการต่างๆ สำหรับการสังเกตการณ์ การวัดผล การวิเคราะห์และการประเมินผลอย่างเหมาะสมเพื่อทำให้มั่นใจในผลที่ถูกต้องหรือไม่ 9.1.d ขั้นตอนตัดสินว่าจะต้องดำเนินการสังเกตการณ์และการวัดผลเมื่อไหร่		

	หรือไม่ 9.1.e ขั้นตอนตัดสินผู้ที่จะสังเกตการณ์และวัดผลหรือไม่ 9.1.f ขั้นตอนตัดสินว่าเมื่อไหร่ที่จะวิเคราะห์และประเมินผลต่างๆ จากการสังเกตการณ์และการวัดผลหรือไม่ 9.1.g ขั้นตอนตัดสินว่าใครจะวิเคราะห์และประเมินผลต่าง ๆ เหล่านี้หรือไม่ 9.1.h องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารที่เหมาะสมให้เป็นหลักฐานของผลการสังเกตการณ์และการวัดผลหรือไม่		
9 การประเมินประสิทธิภาพในการทำงาน 9.2 ภายใน	9.2.a มีขั้นตอนที่ใช้ในการทำให้มั่นใจว่าองค์กรดำเนินการตรวจติดตามภายในในช่วงเวลาตามแผนหรือไม่ 9.2.b การตรวจติดตามภายในให้ข้อมูลว่าระบบบริหารในการรักษาความปลอดภัยของข้อมูลมีความสอดคล้องกับข้อกำหนดต่างๆ ขององค์กรสำหรับระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 9.2.c การตรวจติดตามภายในให้ข้อมูลว่าระบบบริหารในการรักษาความปลอดภัยของข้อมูลมีความสอดคล้องกับข้อกำหนดต่างๆ ของ ISO/IEC 27001:2013 หรือไม่ 9.2.d การตรวจติดตามภายในให้ข้อมูลว่ามีการดำเนินและรักษาระบบบริหารในการรักษาความปลอดภัยของข้อมูลอย่างมีประสิทธิภาพหรือไม่ 9.2.e องค์กรวางแผน จัดตั้ง ดำเนินการและรักษาโปรแกรมการตรวจติดตาม (ต่าง ๆ) โดยรวมถึงความถี่ วิธีการ ความรับผิดชอบ ข้อกำหนดในการวางแผนต่างๆ และการรายงานหรือไม่ 9.2.f โปรแกรมการตรวจติดตาม (ต่าง ๆ) มีการพิจารณาความสำคัญของขั้นตอนต่าง ๆ ที่เกี่ยวข้องและผลการตรวจติดตามครั้งที่แล้วหรือไม่ 9.2.g องค์กรกำหนดเกณฑ์และขอบเขตการตรวจติดตามสำหรับแต่ละการตรวจติดตามหรือไม่ 9.2.h องค์กรคัดเลือกผู้ตรวจติดตามและดำเนินการตรวจติดตามที่ทำให้มั่นใจในความเป็นกลางและความยุติธรรมของขั้นตอนการตรวจติดตามหรือไม่		

	9.2.i องค์กรทำให้มั่นใจว่ามีการรายงานผลการตรวจติดตามต่าง ๆ ถึงฝ่ายบริหารที่เกี่ยวข้องหรือไม่ 9.2.j องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารให้เป็นหลักฐานสำหรับโปรแกรมการตรวจติดตาม (ต่าง ๆ) และผลการตรวจติดตามหรือไม่		
9. การประเมินประสิทธิภาพในการทำงาน 9.3 การทบทวนของฝ่ายบริหาร	9.3.a มีขั้นตอนที่ฝ่ายบริหารสูงสุดใช้เพื่อทบทวนระบบบริหารการรักษาความปลอดภัยของข้อมูลขององค์กรในช่วงเวลาตามแผนเพื่อทำให้มั่นใจในความเหมาะสม ความเพียงพอและประสิทธิภาพอย่างต่อเนื่องหรือไม่ 9.3.b การทบทวนได้รวมการพิจารณาสถานะของปฏิบัติการต่างๆ จากการทบทวนของฝ่ายบริหารครั้งที่แล้วหรือไม่ 9.3.c การทบทวนได้รวมการพิจารณาการเปลี่ยแนปลงต่าง ๆ ในปัญหาภายนอกและภายในที่เกี่ยวข้องกับระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 9.3.d การทบทวนได้รวมการพิจารณาข้อคิดเห็นด้านประสิทธิภาพการทำงานสำหรับการรักษาความปลอดภัยของข้อมูลโดยรวมถึงแนวโน้มต่าง ๆ ใน 1) ความไม่สอดคล้องและปฏิบัติการแก้ไขต่าง ๆ 2) ผลการสังเกตการณ์และการวัดผลต่าง ๆ 3) ผลการตรวจติดตามต่าง ๆ และ 4) การบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 9.3.e การทบทวนได้รวมการพิจารณาข้อคิดเห็นจากผู้มีส่วนได้ส่วนเสียหรือไม่ 9.3.f การทบทวนได้รวมการพิจารณาผลการประเมินความเสี่ยงต่าง ๆ และสถานะของแผนการดูแลความเสี่ยงหรือไม่ 9.3.g การทบทวนได้รวมการพิจารณาโอกาสสำหรับการปรับปรุงอย่างต่อเนื่องหรือไม่ 9.3.h ผลลัพธ์ต่าง ๆ ของการทบทวนของฝ่ายบริหารได้รวมการตัดสินใจต่าง ๆ เกี่ยวกับโอกาสสำหรับการปรับปรุงอย่างต่อเนื่องและการเปลี่ยแนปลงต่าง ๆ ที่จำเป็นสำหรับระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ 9.3.i องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารให้เป็นหลักฐานสำหรับผลการทบทวนของฝ่ายบริหารหรือไม่		
10.1 ความไม่	10.1.a มีขั้นตอนที่องค์กรใช้เพื่อตอบสนองต่อความไม่สอดคล้องและ 1)		

สอดคล้องและปฏิบัติการแก้ไข	ดำเนินปฏิบัติการในการควบคุมและแก้ไข รวมถึง 2) จัดการกับผลที่ตามมาต่าง ๆ อย่างเหมาะสมหรือไม่ 10.1.b มีขั้นตอนที่องค์กรใช้เพื่อประเมินความต้องการสำหรับปฏิบัติการในการขจัดสาเหตุของความไม่สอดคล้องต่าง ๆ เพื่อที่จะไม่เกิดซ้ำหรือเกิดขึ้นในที่อื่นใดด้วย 1) การทบทวนความไม่สอดคล้อง 2) การตัดสินสาเหตุของความไม่สอดคล้อง และ 3) การตัดสินว่ามีความไม่สอดคล้องที่เหมือนกันหรืออาจเกิดขึ้นได้หรือไม่ 10.1.c มีขั้นตอนที่องค์กรใช้เพื่อดำเนินปฏิบัติการที่จำเป็นหรือไม่ 10.1.d มีขั้นตอนที่องค์กรใช้เพื่อทบทวนประสิทธิภาพของปฏิบัติการแก้ไขที่ดำเนินการหรือไม่ 10.1.e มีขั้นตอนที่องค์กรใช้เพื่อทำการเปลี่ยนแปลงต่าง ๆ สำหรับระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลหากจำเป็น หรือไม่ 10.1.f มีขั้นตอนที่องค์กรใช้เพื่อทำให้มั่นใจว่าปฏิบัติการแก้ไขต่าง ๆ มีความเหมาะสมกับผลกระทบต่างๆ ของความไม่สอดคล้องที่เผชิญหน้าหรือไม่ 10.1.g องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารให้เป็นหลักฐานสำหรับลักษณะของความไม่สอดคล้องต่าง ๆ และปฏิบัติการซึ่งดำเนินการต่อมาหรือไม่ 10.1.h องค์กรเก็บรักษาข้อมูลที่เป็นเอกสารให้เป็นหลักฐานสำหรับผลของปฏิบัติการแก้ไขหรือไม่		
10 การปรับปรุง 10.2 การปรับปรุงอย่างต่อเนื่อง	10.2 มีขั้นตอนที่ใช้ในการปรับปรุงความเหมาะสม ความเพียงพอและประสิทธิภาพของระบบบริหารด้านการรักษาความปลอดภัยของข้อมูลอย่างต่อเนื่องหรือไม่		

รายการตรวจสอบเพื่อทวนสอบความสอดคล้องกับข้อกำหนด ISO27001: 2013(การประเมินมาตรการควบคุม)

มาตรา	จุดตรวจสอบ	หลักฐานการสอดคล้อง	ผลการประเมิน
A.5 นโยบายการรักษาความปลอดภัยของข้อมูล A.5.1 ทิศทางการบริหารด้านการรักษาความปลอดภัยของข้อมูล วัตถุประสงค์: เพื่อให้ทิศทางและการสนับสนุนการบริหารด้านการรักษาความปลอดภัยของข้อมูลตามข้อกำหนดทางธุรกิจและกฎหมายรวมถึงกฎระเบียบที่เกี่ยวข้อง	A.5.1.1 มีการกำหนดชุดเอกสารสำหรับนโยบายด้านการรักษาความปลอดภัยของข้อมูล ได้รับการอนุมัติจากฝ่ายบริหาร ทำการเผยแพร่และทำการสื่อสารถึงพนักงานทุกคนและบุคคลภายนอกที่เกี่ยวข้องหรือไม่ A.5.1.2 มีการทบทวนนโยบายการรักษาความปลอดภัยของข้อมูลในช่วงเวลาตามแผนหรือหากมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้นเพื่อทำให้มั่นใจในความเหมาะสม ความเพียงพอและประสิทธิภาพอย่างต่อเนื่องหรือไม่		
A.6 องค์กรด้านการรักษาความปลอดภัยของข้อมูล A.6.1 องค์กรภายใน วัตถุประสงค์: เพื่อจัดตั้งกรอบการทำงานของฝ่ายบริหารในการริเริ่มและควบคุมการปฏิบัติและดำเนินการด้านการรักษาความปลอดภัยของข้อมูลภายในองค์กร	A.6.1.1 มีการกำหนดและจัดสรรความรับผิดชอบด้านการรักษาความปลอดภัยของข้อมูลทั้งหมดหรือไม่ A.6.1.2 มีการแยกพื้นที่ของหน้าที่ที่มีความขัดแย้งและพื้นที่ความรับผิดชอบเพื่อลดโอกาสในการดัดแปลงแก้ไขที่ไม่ได้รับอนุญาตหรือไม่ได้ตั้งใจหรือใช้งานผิดสำหรับสินทรัพย์ขององค์กรหรือไม่ A.6.1.3 มีการรักษาการติดต่อที่เหมาะสมกับผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ A.6.1.4 มีการรักษาการติดต่อที่เหมาะสมกับกลุ่มผลประโยชน์พิเศษหรือฟอรั่มผู้เชี่ยวชาญด้านการรักษาความปลอดภัยและสมาคมทางอาชีพอื่น ๆ หรือไม่ A.6.1.5 มีการกล่าวถึงการรักษาความปลอดภัยของข้อมูลในฝ่ายบริหารโครงการโดยไม่คำนึงถึงประเภทของโครงการหรือไม่		
A.6 องค์กรด้านการรักษาความปลอดภัยของข้อมูล A.6.2 อุปกรณ์มือถือและการทำงานทางไกล	A.6.2.1 มีการปรับใช้นโยบายและมาตรการการรักษาความปลอดภัยสนับสนุนสำหรับการบริหารความเสี่ยงต่าง ๆ ที่เกิดจากการใช้อุปกรณ์มือถือหรือไม่		

วัตถุประสงค์: เพื่อทำให้มั่นใจในการรักษาความปลอดภัยสำหรับการทำงานทางไกลและการใช้อุปกรณ์มือถือ	A.6.2.2 มีการดำเนินนโยบายและมาตรการการรักษาความปลอดภัยสนับสนุนเพื่อปกป้องข้อมูลที่ถูกเข้าถึง ประมวลหรือจัดเก็บที่สถานประกอบการทำงานทางไกลหรือไม่		
A.7 การรักษาความปลอดภัยด้านทรัพยากรบุคคล A.7.1 ก่อนการว่าจ้าง วัตถุประสงค์: เพื่อทำให้มั่นใจว่าพนักงานและผู้รับเหมาต่าง ๆ มีความเข้าใจความรับผิดชอบของตนเองและมีความเหมาะสมสำหรับบทบาทต่าง ๆ ที่ถูกพิจารณา	A.7.1.1. มีการดำเนินการตรวจสอบในการตรวจพิสูจน์ภูมิหลังผู้สมัครทุกคนสำหรับการว่าจ้างตามกฎหมาย กฎระเบียบและหลักจริยธรรมที่เกี่ยวข้อง รวมถึงการตรวจสอบพอเหมาะกับข้อกำหนดทางธุรกิจต่าง ๆ การแบ่งประเภทข้อมูลที่จะเข้าถึงและความเสี่ยงที่รับรู้หรือไม่ A.7.1.2. ข้อตกลงตามสัญญากับพนักงานและผู้รับเหมามีการกล่าวถึงความรับผิดชอบของพนักงานและผู้รับเหมารวมถึงองค์กรในด้านการรักษาความปลอดภัยของข้อมูลหรือไม่		
A.7 การรักษาความปลอดภัยด้านทรัพยากรบุคคล A.7.2 ระหว่างการว่าจ้าง วัตถุประสงค์: เพื่อทำให้มั่นใจว่าพนักงานและผู้รับเหมาต่าง ๆ มีความตระหนักถึงและบรรลุความรับผิดชอบด้านการรักษาความปลอดภัยของข้อมูลของตนเอง	A.7.2.1 ฝ่ายบริหารกำหนดให้พนักงานและผู้รับเหมาทุกคนประยุกต์ใช้การรักษาความปลอดภัยของข้อมูลตามนโยบายและกระบวนการทำงานต่าง ๆ ที่จัดตั้งไว้ขององค์กรหรือไม่ A.7.2.2 พนักงานทุกคนขององค์กรและผู้รับเหมาที่เกี่ยวข้องได้รับการศึกษาและการฝึกอบรมด้านการตระหนักถึงที่เหมาะสม รวมถึงการอัพเดตทั่วไปในด้านนโยบายและกระบวนการทำงานขององค์กรตามที่เกี่ยวข้องกับหน้าที่งานของตนเองหรือไม่ A.7.2.3 มีขั้นตอนด้านระเบียบวินัยที่เป็นทางการและถูกสื่อสารในการดำเนินการกับพนักงานที่ทำการละเมิดการรักษาความปลอดภัยของข้อมูลหรือไม่		
A.7 การรักษาความปลอดภัยด้านทรัพยากรบุคคล A.7.3 การสิ้นสุดและการเปลี่ยนแปลงการว่าจ้าง วัตถุประสงค์: เพื่อป้องกันผลประโยชน์ขององค์กรให้เป็นส่วนหนึ่งของขั้นตอนการเปลี่ยนแปลงหรือสิ้นสุดการว่าจ้าง	A.7.3.1 มีการกำหนดและสื่อสารความรับผิดชอบและหน้าที่ด้านการรักษาความปลอดภัยของข้อมูลที่ยังคงมีผลใช้ได้หลังการสิ้นสุดการว่าจ้างถึงพนักงานหรือผู้รับเหมารวมถึงการบังคับใช้หรือไม่		
A.8 การบริหารสินทรัพย์	A.8.1.1 มีการบ่งชี้สินทรัพย์ที่เกี่ยวข้องกับข้อมูลและสิ่งอำนวย		

A.8.1 ความรับผิดชอบต่อสินทรัพย์ วัตถุประสงค์: เพื่อบ่งชี้สินทรัพย์ขององค์กรและกำหนดความรับผิดชอบในการป้องกันที่เหมาะสม	ความสะดวกในการประมวลข้อมูล มีการทำสินทรัพย์คงคลังเหล่านี้ให้เป็นระเบียบ และมีการบำรุงรักษาหรือไม่ A.8.1.2 มีการรักษาสินทรัพย์ต่าง ๆ ทั้งหมดในคงคลังที่มีการมอบหมายเจ้าของหรือไม่ A.8.1.3 มีการบ่งชี้ ทำเอกสารและดำเนินกฎระเบียบสำหรับการใช้งานข้อมูลและสินทรัพย์เกี่ยวกับข้อมูลและสิ่งอำนวยความสะดวกในการประมวลข้อมูลที่ยอมรับได้หรือไม่ 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 ที่เหมาะสมสำหรับการการติดป้ายข้อมูลตามรายการการแบ่งประเภทข้อมูลที่องค์กรปรับใช้หรือไม่ A.8.2.3 มีการพัฒนาและดำเนินกระบวนการทำงานสำหรับการจัดการสินทรัพย์ตามรายการการแบ่งประเภทข้อมูลที่องค์กรปรับใช้หรือไม่		
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 การใช้ผิดหรือการชัดจังหวะขณะโอนถ่ายข้อมูล หรือไม่		
A.9 การควบคุมการเข้าถึง A.9.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึง วัตถุประสงค์: เพื่อจำกัดการ	A.9.1.1 มีการจัดตั้ง ทำเอกสารและทบทวนนโยบายการควบคุมการเข้าถึงโดยอิงตามข้อกำหนดทางธุรกิจและการรักษาความปลอดภัยของข้อมูลหรือไม่ A.9.1.2 มีการให้ผู้ใช้งานเท่านั้นที่จะเข้าถึงเครือข่ายและบริการ		

เข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลข้อมูล	ของเครือข่ายที่ผู้ใช้งานได้รับอนุญาตเฉพาะในการใช้งานหรือไม่		
A.9 การควบคุมการเข้าถึง A.9.2 การบริหารการเข้าถึงสำหรับผู้ใช้งาน วัตถุประสงค์: เพื่อทำให้มั่นใจในการเข้าถึงของผู้ใช้ที่ได้รับอนุญาตและเพื่อป้องกันการเข้าถึงระบบและบริการที่ไม่ได้รับอนุญาต	A.9.2.1 มีการดำเนินขั้นตอนการลงทะเบียนหรือถอนทะเบียนผู้ใช้งานเพื่อทำให้สามารถมอบหมายสิทธิการเข้าถึงหรือไม่ A.9.2.2 มีการดำเนินขั้นตอนการให้การเข้าถึงสำหรับผู้ใช้งานอย่างเป็นทางการในการมอบหมายหรือถอนสิทธิการเข้าถึงสำหรับผู้ใช้งานทุกประเภทสำหรับระบบและบริการต่าง ๆ ทั้งหมดหรือไม่ A.9.2.3 มีการจำกัดและควบคุมการจัดสรรและการใช้สิทธิการเข้าถึงที่มีสิทธิพิเศษหรือไม่ A.9.2.4 มีการควบคุมการจัดสรรข้อมูลการพิสูจน์ตัวตนที่เป็นความลับผ่านขั้นตอนการบริหารที่เป็นทางการหรือไม่ 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 จะต้องปฏิบัติตามแนวทางปฏิบัติขององค์กรในการใช้งานข้อมูลการพิสูจน์ตัวตนที่เป็นความลับหรือไม่		
A.9 การควบคุมการเข้าถึง A.9.4 การควบคุมการเข้าถึงระบบและแอพพลิเคชั่น วัตถุประสงค์: เพื่อป้องกันการเข้าถึงระบบและแอพพลิเคชั่นที่ไม่ได้รับอนุญาต	A.9.4.1 มีการจำกัดการเข้าถึงข้อมูลและหน้าที่งานของระบบแอพพลิเคชั่นตามนโยบายการควบคุมการเข้าถึงหรือไม่ A.9.4.2 หากนโยบายการควบคุมการเข้าถึงมีการกำหนด ได้มีการควบคุมการเข้าถึงระบบและแอพพลิเคชั่นด้วยกระบวนการทำงานในการเข้าสู่ระบบที่ปลอดภัยหรือไม่ A.9.4.3 ระบบการบริหารรหัสผ่านมีปฏิสัมพันธ์และทำให้มั่นใจ		

	ในรหัสผ่านที่มีคุณภาพหรือไม่ A.9.4.4 การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ ที่อาจสามารถทำให้ผ่านข้ามการควบคุมของระบบและแอพพลิเคชั่นมีหรือไม่ A.9.4.5. มีการจำกัดการเข้าถึงรหัสต้นทางของโปรแกรมหรือไม่		
A.10 การเข้ารหัส A.10.1 การควบคุมด้วยการเข้ารหัส วัตถุประสงค์: เพื่อทำให้มั่นใจในการใช้งานการเข้ารหัสที่เหมาะสมและมีประสิทธิภาพเพื่อป้องกันการรักษาข้อมูลความลับความถูกต้องและ/หรือบูรณภาพของข้อมูล	A.10.1.1 มีการพัฒนาและดำเนินนโยบายการใช้การควบคุมด้วยการเข้ารหัสเพื่อปกป้องข้อมูลหรือไม่ A.10.1.2 มีการพัฒนานโยบายการใช้งาน การป้องกันและอายุการใช้งานของคีย์การเข้ารหัส และมีการดำเนินการผ่านวงจรอายุทั้งหมดหรือไม่		
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 และมีการประยุกต์ใช้ด้วยหรือไม่ A.11.1.5 มีการออกแบบกระบวนการทำงานสำหรับการทำงานในพื้นที่ปลอดภัย และมีการประยุกต์ใช้ด้วยหรือไม่ A.11.1.6 มีการควบคุมจุดเข้าถึงต่าง ๆ อาทิเช่น พื้นที่ส่งมอบและการโหลดรวมถึงจุดอื่น ๆ ที่บุคคลที่ไม่ได้รับอนุญาตสามารถ		

	เข้าในสถานที่ต่างๆ และหากเป็นไปได้ ให้แยกต่างหากจากสิ่งอำนวยความสะดวกในการประมวลข้อมูลเพื่อหลีกเลี่ยงการเข้าถึงที่ไม่ได้รับอนุญาตหรือไม่		
A.11 การรักษาความปลอดภัยทางกายภาพและสิ่งแวดล้อม A.11.2 อุปกรณ์ วัตถุประสงค์: เพื่อป้องกันการสูญเสีย ความเสียหาย การขโมย หรือการทำให้สินทรัพย์อยู่ในอันตรายและการขัดจังหวะการดำเนินงานขององค์กร	A.11.2.1 มีการจัดตั้งและปกป้องอุปกรณ์เพื่อลดความเสี่ยงต่าง 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 มีการใช้นโยบายจัดเก็บเอกสารสำหรับเอกสารที่เป็นกระดาษและสื่อจัดเก็บที่ถอดออกได้รวมถึงนโยบายการใช้งานคอมพิวเตอร์สำหรับสิ่งอำนวยความสะดวกในการประมวลข้อมูลหรือไม่		
A.12 การรักษาความปลอดภัย	A.12.1.1 มีการทำเอกสารกระบวนการทำงานในการดำเนินงาน		

ด้านการดำเนินงาน A.12.1 กระบวนการทำงานด้านการดำเนินงานและความรับผิดชอบต่างๆ วัตถุประสงค์: เพื่อทำให้มั่นใจในการดำเนินงานที่ถูกต้องและปลอดภัยของสิ่งอำนวยความสะดวกในการประมวลข้อมูล	และทำให้มีพร้อมใช้สำหรับผู้ใช้งานทุกคนที่ต้องการหรือไม่ A.12.1.2 มีการควบคุมการเปลี่ยนแปลงสำหรับองค์กร ขั้นตอนทางธุรกิจ สิ่งอำนวยความสะดวกในการประมวลข้อมูลและระบบที่ส่งผลกระทบต่อขั้นตอนการรักษาความปลอดภัยของข้อมูลหรือไม่ A.12.1.3 มีการสังเกตการณ์ ปรับแต่งการใช้ทรัพยากรหรือไม่ และทำการวางแผนจากข้อกำหนดด้านสมรรถนะในอนาคตเพื่อทำให้มั่นใจในประสิทธิภาพการทำงานของระบบที่ต้องการหรือไม่ A.12.1.4 มีการแยกการพัฒนา การทดสอบและสภาพแวดล้อมในการดำเนินงานออกต่างหากเพื่อลดความเสี่ยงจากการเข้าถึงหรือการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตสำหรับสภาพแวดล้อมในการดำเนินงานหรือไม่		
A.12 การรักษาความปลอดภัยด้านการดำเนินงาน A.12.2 การป้องกันมัลแวร์ (malware) วัตถุประสงค์: เพื่อทำให้มั่นใจว่ามีการปกป้องข้อมูลและสิ่งอำนวยความสะดวกในการประมวลข้อมูลจากมัลแวร์	A.12.2.1 มีการดำเนินการควบคุมด้านการตรวจพบ 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 วัตถุประสงค์: เพื่อบันทึกเหตุการณ์ต่างๆ และสร้าง	A.12.4.1 มีการสร้าง เก็บและทบทวนสมุดบันทึกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น ความผิดพลาดและเหตุการณ์ด้านการรักษาความปลอดภัยของข้อมูลเป็นประจำหรือไม่ A.12.4.2 มีการป้องกันสิ่งอำนวยความสะดวกในการเข้าออกระบบและข้อมูลการเข้าออกระบบจากการปลอมแปลงและการ		

หลักฐาน	เข้าถึงที่ไม่ได้รับอนุญาตหรือไม่ 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 ข้อกำหนดและกิจกรรมในการตรวจติดตามมีความเกี่ยวข้องกับการตรวจสอบระบบปฏิบัติการที่วางแผนและตกลงกันอย่างระมัดระวังเพื่อลดการขัดจังหวะขั้นตอนทางธุรกิจหรือไม่		
A.13 การรักษาความปลอดภัยด้านการสื่อสาร A.13.1 การบริหารการรักษาความปลอดภัยของเครือข่าย วัตถุประสงค์: เพื่อทำให้มั่นใจในการป้องกันข้อมูลในเครือข่าย	A.13.1.1 มีการบริหารและควบคุมเครือข่ายต่าง ๆ เพื่อป้องกันข้อมูลในระบบและแอพพลิเคชั่นหรือไม่ A.13.1.2 มีการบ่งชี้กลไกการรักษาความปลอดภัย ระดับการให้บริการและข้อกำหนดด้านการบริหารของการให้บริการเครือข่ายทั้งหมด และรวมอยู่ในข้อตกลงการให้บริการว่าจะมีการให้บริการต่าง ๆ เหล่านี้ภายในบริษัทหรือโดยผู้รับเหมาหรือไม่		

ต่างๆ และสิ่งอำนวยความสะดวกในการประมวลข้อมูลสนับสนุน	A.13.1.3 มีการแยกกลุ่มการให้บริการข้อมูล ผู้ใช้งานและระบบข้อมูลบนเครือข่ายต่าง ๆ หรือไม่		
A.13 การรักษาความปลอดภัยด้านการสื่อสาร A.13.2 การโอนถ่ายข้อมูล วัตถุประสงค์: เพื่อรักษาการรักษาความปลอดภัยของข้อมูลที่โอนถ่ายภายในองค์กรและกับองค์กรภายนอก	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: เพื่อทำให้มั่นใจว่าการรักษาความปลอดภัยของข้อมูลเป็นส่วนสำคัญของระบบข้อมูลตลอดทั้งวงจรชีวิตรวมถึงข้อกำหนดต่างๆ สำหรับระบบข้อมูลที่ให้บริการทั่วเครือข่ายสาธารณะ	A.14.1.1 ข้อกำหนดเกี่ยวกับการรักษาความปลอดภัยของข้อมูลได้รวมอยู่ในข้อกำหนดต่างๆ 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 การรักษาความปลอดภัยในขั้นตอนการพัฒนาและสนับสนุน วัตถุประสงค์: เพื่อทำให้มั่นใจว่า	A.14.2.1 มีการจัดตั้งกฎระเบียบสำหรับการพัฒนาซอฟต์แวร์และระบบและมีการประยุกต์ใช้กฎระเบียบต่างๆ เพื่อการพัฒนาภายในองค์กรหรือไม่ A.14.2.2 มีการควบคุมการเปลี่ยนแปลงต่าง ๆ สำหรับระบบภายในวงจรชีวิตในการพัฒนาด้วยการใช้กระบวนการทำงานในการควบคุมการเปลี่ยนแปลงที่เป็นทางการหรือไม่		

มีการออกแบบและดำเนินการรักษาความปลอดภัยของข้อมูลภายในวงจรชีวิตในการพัฒนาระบบข้อมูล	A.14.2.3 เมื่อแพลตฟอร์มปฏิบัติการมีการเปลี่ยนแปลง ได้มีการทบทวนแอพพลิเคชั่นที่สำคัญทางธุรกิจและทำการทดสอบเพื่อทำให้มั่นใจว่าไม่มีผลกระทบย้อนกลับต่อการดำเนินงานขององค์กรหรือการรักษาความปลอดภัยหรือไม่ A.14.2.4 มีการกีดกันการดัดแปลงแก้ไขต่าง ๆ สำหรับชุดซอฟต์แวร์ มีการจำกัดการเปลี่ยนแปลงที่จำเป็นและมีการควบคุมการเปลี่ยนแปลงต่างๆ ทั้งหมดอย่างเข้มงวดหรือไม่ A.14.2.5 มีการจัดตั้ง ทำเอกสาร รักษาและประยุกต์ใช้หลักการต่างๆ เกี่ยวกับระบบความปลอดภัยด้านวิศวกรรมสำหรับความพยายามในการดำเนินระบบข้อมูลหรือไม่ A.14.2.6 องค์กรจัดตั้งและปกป้องสภาพแวดล้อมในการพัฒนาที่ปลอดภัยอย่างเหมาะสมสำหรับความพยายามในการพัฒนาและบูรณาการระบบหรือไม่ สภาพแวดล้อมในการพัฒนาที่ปลอดภัยเหล่านี้ได้ครอบคลุมวงจรชีวิตในการพัฒนาระบบทั้งหมดหรือไม่ A.14.2.7 องค์กรได้ชี้แนะและสังเกตการณ์กิจกรรมการพัฒนาระบบที่ใช้ผู้รับเหมาหรือไม่ A.14.2.8 มีการดำเนินการทดสอบการทำงานด้านการรักษาความปลอดภัยระหว่างการพัฒนาหรือไม่ A.14.2.9 มีการจัดตั้งโปรแกรมการทดสอบการยอมรับและเกณฑ์ที่เกี่ยวข้องสำหรับระบบข้อมูลใหม่ การอัพเกรดและเวอร์ชั่นใหม่หรือไม่		
A.14 การครอบครอง การพัฒนาและการบำรุงรักษาระบบ A.14.3 ข้อมูลการทดสอบ วัตถุประสงค์: เพื่อทำให้มั่นใจในการป้องกันข้อมูลที่ใช้เพื่อการทดสอบ	A.14.3.1 มีการคัดเลือกข้อมูลการทดสอบอย่างระมัดระวัง รวมถึงป้องกันและควบคุมหรือไม่		
A.15 ความสัมพันธ์กับซัพพลายเออร์	A.15.1.1 มีการตกลงข้อกำหนดด้านการรักษาความปลอดภัยของข้อมูลสำหรับการบรรเทาความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับ		

A.15.1 การรักษาความปลอดภัยของข้อมูลในความสัมพันธ์กับซัพพลายเออร์ วัตถุประสงค์: เพื่อทำให้มั่นใจในการป้องกันสินทรัพย์ขององค์กรที่ซัพพลายเออร์สามารถเข้าถึงได้	การเข้าถึงสินทรัพย์ขององค์กรของแต่ละซัพพลายเออร์กับซัพพลายเออร์ และทำเป็นเอกสารหรือไม่ A.15.1.2 มีการจัดตั้งและตกลงข้อกำหนดด้านการรักษาความปลอดภัยของข้อมูลที่เกี่ยวข้องทั้งหมดกับแต่ละซัพพลายเออร์ที่อาจเข้าถึง ประมวลผล จัดเก็บ สื่อสารหรือให้ส่วนประกอบโครงสร้างพื้นฐานด้าน IT สำหรับข้อมูลขององค์กรหรือไม่ A.15.1.3 ข้อตกลงกับซัพพลายเออร์ต่าง ๆ ได้รวมข้อกำหนดในการหาความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลที่เกี่ยวข้องกับข้อมูลและการให้บริการด้านเทคโนโลยีการสื่อสารรวมถึงห่วงโซ่อุปทานสินค้าหรือไม่		
A.15 ความสัมพันธ์กับซัพพลายเออร์ A.15.2 การบริหารการส่งมอบบริการของซัพพลายเออร์ วัตถุประสงค์: เพื่อรักษาการรักษาความปลอดภัยของข้อมูลในระดับที่ตกลงกันและการส่งมอบบริการตามข้อตกลงของซัพพลายเออร์	A.15.2.1 องค์กรมีการสังเกตการณ์ ทบทวนและตรวจติดตามการส่งมอบบริการของซัพพลายเออร์เป็นประจำหรือไม่ A.15.2.2 มีการบริหารการเปลี่ยนแปลงต่างๆ สำหรับการให้บริการโดยซัพพลายเออร์ซึ่งรวมถึงการบำรุงรักษาและการปรับปรุงนโยบายการรักษาความปลอดภัยของข้อมูลที่มีอยู่ กระบวนการทำงานและการควบคุมต่าง ๆ โดยคำนึงถึงภาวะวิกฤตของข้อมูลทางธุรกิจ ระบบและขั้นตอนต่าง ๆ ที่เกี่ยวข้องและการประเมินความเสี่ยงต่าง ๆ ซ้ำหรือไม่		
A.16 การบริหารอุบัติการณ์ด้านการรักษาความปลอดภัยของข้อมูล A.16.1 การบริหารอุบัติการณ์และการปรับปรุงด้านการรักษาความปลอดภัยของข้อมูล วัตถุประสงค์: เพื่อทำให้มั่นใจในวิธีการที่สอดคล้องและมีประสิทธิภาพสำหรับการบริหารอุบัติการณ์ด้านการรักษาความปลอดภัยของข้อมูลรวมถึงการสื่อสารด้านเหตุการณ์การรักษาความปลอดภัยและจุดอ่อนต่างๆ	A.16.1.1 มีการกำหนดความรับผิดชอบของฝ่ายบริหารและกระบวนการทำงานเพื่อทำให้มั่นใจในการตอบสนองที่รวดเร็ว มีประสิทธิภาพและเป็นระเบียบต่ออุบัติการณ์ด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ A.16.1.2 มีการรายงานเหตุการณ์ด้านการรักษาความปลอดภัยของข้อมูลผ่านช่องทางการบริการที่เหมาะสมโดยเร็วที่สุดเท่าที่จะเป็นไปได้หรือไม่ A.16.1.3 มีการกำหนดให้พนักงานและผู้รับเหมาที่ใช้ระบบข้อมูลขององค์กรและบริการจะต้องจดบันทึกและรายงานจุดอ่อนด้านการรักษาความปลอดภัยของข้อมูลที่สังเกตเห็นหรือที่สงสัยในระบบหรือการให้บริการต่างๆ หรือไม่ A.16.1.4 มีการประเมินเหตุการณ์ด้านการรักษาความปลอดภัยของข้อมูลและมีการตัดสินว่าเหตุการณ์ต่าง ๆ ต้องแยกประเภท		

	เป็นอุบัติการณ์ด้านการรักษาความปลอดภัยของข้อมูลหรือไม่ A.16.1.5 มีการตอบสนองอุบัติการณ์ด้านการรักษาความปลอดภัยของข้อมูลตามกระบวนการทำงานที่เป็นเอกสารหรือไม่ A.16.1.6 มีการใช้ความรู้ที่ได้รับจากการวิเคราะห์และการแก้ไขอุบัติการณ์ด้านการรักษาความปลอดภัยของข้อมูลเพื่อลดความเป็นไปได้หรือผลกระทบของอุบัติการณ์ในอนาคตหรือไม่ A.16.1.7 องค์กรได้กำหนดและประยุกต์ใช้กระบวนการทำงานในการบ่งชี้ การจัดเก็บ การครอบครอง และการข้อมูลที่สามารถใช้เป็นหลักฐานหรือไม่		
A.17 ด้านต่าง ๆ เกี่ยวกับการรักษาความปลอดภัยของข้อมูลสำหรับการบริหารความต่อเนื่องทางธุรกิจ A.17.1 ความต่อเนื่องด้านการรักษาความปลอดภัยของข้อมูล วัตถุประสงค์: เพื่อให้ความต่อเนื่องด้านการรักษาความปลอดภัยของข้อมูลฝังตัวอยู่ในระบบบริหารความต่อเนื่องทางธุรกิจขององค์กร	A.17.1.1 องค์กรได้ตัดสินข้อกำหนดต่างๆ สำหรับการรักษาความปลอดภัยของข้อมูลและการบริการต่อเนื่องด้านการรักษาความปลอดภัยของข้อมูลในสถานการณ์ย้อนกลับ ตัวอย่างเช่น ระหว่างวิกฤตหรือภัยพิบัติ หรือไม่ A.17.1.2 องค์กรได้จัดตั้ง ทำเอกสารและดำเนินการ รวมถึงรักษาขั้นตอน กระบวนการทำงานและการควบคุมต่าง ๆ เพื่อทำให้มั่นใจในระดับที่จำเป็นสำหรับการต่อเนื่องด้านการรักษาความปลอดภัยของข้อมูลระหว่างสถานการณ์ย้อนกลับหรือไม่ A.17.1.3 องค์กรได้ตรวจสอบการควบคุมการต่อเนื่องด้านการรักษาความปลอดภัยของข้อมูลที่จัดตั้งและดำเนินการในช่วงเวลาตามแผนเพื่อทำให้มั่นใจว่าการควบคุมมีผลใช้ได้และมีประสิทธิภาพระหว่างสถานการณ์ย้อนกลับหรือไม่		
A.17 ด้านต่าง ๆ เกี่ยวกับการรักษาความปลอดภัยของข้อมูลสำหรับการบริหารความต่อเนื่องทางธุรกิจ A.17.2 ความซ้ำซ้อน วัตถุประสงค์: เพื่อทำให้มั่นใจในการมีสิ่งอำนวยความสะดวกในการประมวลข้อมูลพร้อมใช้	A.17.2.1 มีการดำเนินการสิ่งอำนวยความสะดวกในการประมวลข้อมูลที่มีความซ้ำซ้อนเพียงพอที่จะบรรลุข้อกำหนดในการมีพร้อมใช้หรือไม่?		
A.18 ความสอดคล้อง A.18.1 ความสอดคล้องกับข้อกำหนดทางกฎหมายและตามสัญญา	A.18.1.1 มีการบ่งชี้ ทำเอกสาร ข้อกำหนดทางกฎหมาย พระราชบัญญัติ กฎระเบียบและตามสัญญาทั้งหมดรวมถึงวิธีการขององค์กรในการบรรลุข้อกำหนดต่าง ๆ เหล่านี้อย่างชัดเจนและคอยอัพเดตแต่ละระบบข้อมูลและองค์กรหรือไม่		

วัตถุประสงค์: เพื่อหลีกเลี่ยงการละเมิดข้อบังคับตามกฎหมาย พระราชบัญญัติ กฎระเบียบ หรือตามสัญญาที่เกี่ยวกับข้อกำหนดการรักษาความปลอดภัยของข้อมูลและข้อกำหนดด้านการรักษาความปลอดภัยอื่น ๆ	A.18.1.2 มีการดำเนินกระบวนการทำงานที่เหมาะสมเพื่อทำให้มั่นใจในความสอดคล้องกับข้อกำหนดทางกฎหมาย กฎระเบียบ และตามสัญญาที่เกี่ยวกับสิทธิทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์หรือไม่ A.18.1.3 มีการป้องกันบันทึกต่าง ๆ จากการสูญเสีย การทำลาย การปลอมแปลง การเข้าถึงที่ไม่ได้รับอนุญาตและการปล่อยที่ไม่ได้รับอนุญาตตามข้อกำหนดทางกฎหมาย กฎระเบียบ สัญญา และทางธุรกิจ หรือไม่ A.18.1.4 มีการทำให้มั่นใจในความเป็นส่วนตัวและการปกป้องข้อมูลที่สามารถบ่งชี้ตัวบุคคลตามที่กำหนดในกฎหมายและกฎระเบียบเมื่อบังคับใช้หรือไม่ A.18.1.5 มีการใช้การควบคุมการเข้ารหัสโดยสอดคล้องกับข้อตกลง กฎหมายและกฎระเบียบที่เกี่ยวข้องทั้งหมดหรือไม่		
A.18 ความสอดคล้อง A.18.2 การทบทวนด้านการรักษาความปลอดภัยของข้อมูล วัตถุประสงค์: เพื่อทำให้มั่นใจว่ามีการปฏิบัติและดำเนินการรักษาความปลอดภัยของข้อมูลตามนโยบายและกระบวนการทำงานขององค์กร	A.18.2.1 มีการทบทวนวิธีการขององค์กรในการบริหารการรักษาความปลอดภัยของข้อมูลและการดำเนินงาน (ตัวอย่างเช่น วัตถุประสงค์ในการควบคุม การควบคุม นโยบาย ขั้นตอนและกระบวนการทำงานต่าง ๆ สำหรับการรักษาความปลอดภัยของข้อมูล) อย่างเป็นอิสระในช่วงเวลาตามแผนหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้นหรือไม่ A.18.2.2 ผู้จัดการต่าง ๆ ได้ทบทวนความสอดคล้องของการประมวลข้อมูลและกระบวนการทำงานภายในพื้นที่รับผิดชอบของตนเองด้วยนโยบายการรักษาความปลอดภัยที่เหมาะสม มาตรฐานและข้อกำหนดด้านการรักษาความปลอดภัยอื่นๆ หรือไม่ A.18.2.3 มีการทบทวนระบบข้อมูลด้านความสอดคล้องกับนโยบายและมาตรฐานการรักษาความปลอดภัยของข้อมูลขององค์กรเป็นประจำหรือไม่		