ชุดคำถาม CSA Consensus Assessments Initiative Questionnaire

มกราคม 2017

ประกาศ

เอกสารฉบับนี้ให้ไว้เพื่อเป็น ข้อมูลเท่านั้น เนื้อหาของเอกสารนำเสนอข้อมูลผลิตภัณฑ์และบริการ รวมถึงแนวทางปฏิบัติปัจจุบันของ AWS ณ วันที่มีการออกเอกสารฉบับนี้ และสามารถเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบ ลูกค้ามีหน้าที่รับผิดชอบต่อการประเมินข้อมูลในเอกสารฉบับนี้ รวมถึงการใช้ผลิตภัณฑ์หรือบริการใดๆ ของ AWS ด้วยตนเองได้อย่างอิสระ ทั้งนี้ผลิตภัณฑ์และบริการแต่ละอย่างให้บริการ “ตามที่เป็น” โดยไม่มีการรับประกันใดๆ ไม่ว่าโดยนัยหรือโดยชัดแจ้ง เอกสารฉบับนี้ไม่มีการรับประกัน การรับรอง การผูกพันตามสัญญา เงื่อนไขหรือการประกันใดๆ จาก AWS บริษัทในเครือ ผู้จัดหา หรือผู้ให้สิทธิ์การใช้งาน หน้าที่และความรับผิดของ AWS ต่อลูกค้าอยู่ภายใต้การควบคุมโดยข้อตกลงของ AWS และเอกสารฉบับนี้ไม่ถือเป็นส่วนหนึ่งของข้อตกลง และไม่ทำให้เกิดการเปลี่ยนแปลงใดๆ กับข้อตกลงระหว่าง AWS กับลูกค้า

สารบัญ

บทคัดย่อ

ชุดคำถาม CSA Consensus Assessments Initiative Questionnaire แสดงรายการชุดคำถามที่ CSA คาดหวังว่าลูกค้าระบบคลาวด์และ/หรือผู้ตรวจสอบระบบคลาวด์จะสอบถามจากผู้ให้บริการระบบคลาวด์ ชุดคำถามนี้ประกอบด้วยคำถามด้านการรักษาความปลอดภัย การควบคุม และกระบวนการต่างๆ ซึ่งสามารถนำไปใช้งานได้อย่างกว้างขวาง รวมถึงการเลือกผู้ให้บริการระบบคลาวด์และการประเมินด้านความปลอดภัย AWS ได้รวบรวมคำถามทั้งหมดพร้อมด้วยคำตอบสำหรับแต่ละคำถามด้านล่าง

ข้อมูลเบื้องต้น

พันธมิตรความปลอดภัยบนระบบคลาวด์ (CSA) คือ “องค์กรที่ไม่มุ่งหวังผลกำไร ซึ่งมีเป้าหมายเพื่อส่งเสริมการใช้แนวทางปฏิบัติมาตรฐานในการมอบการรับประกันด้านความปลอดภัยภายในการประมวลผลบนระบบคลาวด์ และให้ความรู้เกี่ยวกับการใช้งานการประมวลผลบนระบบคลาวด์เพื่อช่วยรักษาความปลอดภัยให้กับการใช้งานคอมพิวเตอร์ในรูปแบบอื่นๆ” สำหรับข้อมูลเพิ่มเติม โปรดดูที่ https://cloudsecurityalliance.org/about/

ผู้ประกอบกิจการ องค์กร และสมาคมด้านการรักษาความปลอดภัยระดับอุตสาหกรรมจำนวนมากมีส่วนร่วมภายในองค์กรนี้เพื่อให้บรรลุเป้าหมาย

ชุดคำถาม CSA Consensus Assessments Initiative Questionnaire

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ความปลอดภัยของแอปพลิเคชันและอินเทอร์เฟซ *ความปลอดภัยแอปพลิเคชัน*	AIS-01.1	คุณใช้มาตรฐานของอุตสาหกรรม (เกณฑ์วัดมาตรฐาน Build Security in Maturity Model [BSIMM], Open Group ACS Trusted Technology Provider Framework, NIST, ฯลฯ) เพื่อสร้างความปลอดภัยภายในระบบวงจรการพัฒนาระบบ/ซอฟต์แวร์ (SDLC) หรือไม่	วงจรการพัฒนาระบบของ AWS ใช้แนวทางปฏิบัติมาตรฐานของอุตสาหกรรม ซึ่งรวมถึงการตรวจสอบการออกแบบอย่างเป็นทางการโดยทีมรักษาความปลอดภัยของ AWS การกำหนดต้นแบบภัยคุกคาม และการดำเนินการประเมินความเสี่ยง โปรดดูข้อมูลเพิ่มเติมได้จาก ภาพรวมของกระบวนการรักษาความปลอดภัยของ AWS AWS มีการวางกระบวนการสำหรับบริหารการพัฒนาทรัพยากรใหม่ โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 14 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	AIS-01.2	คุณใช้เครื่องมือการวิเคราะห์ซอร์สโค้ดอัตโนมัติ เพื่อตรวจหาข้อบกพร่องด้านความปลอดภัยภายในโค้ดก่อนนำไปใช้งานจริงหรือไม่	
	AIS-01.3	คุณใช้การวิเคราะห์ซอร์สโค้ดด้วยตนเอง เพื่อตรวจหาข้อบกพร่องด้านความปลอดภัยภายในโค้ดก่อนนำไปใช้งานจริงหรือไม่	
	AIS-01.4	คุณตรวจสอบหรือไม่ว่าผู้จัดจำหน่ายด้านซอฟต์แวร์ทั้งหมดปฏิบัติตามมาตรฐานของอุตสาหกรรมด้านความปลอดภัยของวงจรการพัฒนาระบบ/ซอฟต์แวร์ (SDLC)	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	AIS-01.5	(เฉพาะ SaaS เท่านั้น) คุณได้ตรวจสอบแอปพลิเคชันเพื่อค้นหาช่องโหว่ด้านความปลอดภัยและจัดการกับปัญหาใดๆ ที่พบก่อนการนำไปใช้งานจริงหรือไม่	
ความปลอดภัยของแอปพลิเคชันและอินเทอร์เฟซ *ข้อกำหนดด้านการเข้าถึงของลูกค้า*	AIS-02.1	ข้อกำหนดด้านความปลอดภัยด้านสัญญา และข้อกำหนดด้านระเบียบข้อบังคับที่ระบุทั้งหมดสำหรับการเข้าถึงของลูกค้ามีการจัดการในรูปแบบของสัญญา และมีการแก้ไขก่อนให้สิทธิการเข้าถึงข้อมูล สินทรัพย์ และระบบข้อมูลกับลูกค้าหรือไม่	ลูกค้าของ AWS เป็นผู้มีหน้าที่รับผิดชอบว่าการใช้งาน AWS ของตนเองให้สอดคล้องกับกฎหมายและข้อกำหนดที่มีผลบังคับใช้ AWS สื่อสารถึงความปลอดภัยและสภาพแวดล้อมการควบคุมกับลูกค้าผ่านการรับรองด้านอุตสาหกรรมและการยืนยันจากหน่วยงานภายนอก เอกสาร (สามารถดูได้ที่ http://aws.amazon.com/compliance) และการจัดหาการรับรอง รายงาน และเอกสารอื่นๆ ที่เกี่ยวข้องให้กับลูกค้าของ AWS โดยตรง
	AIS- 02.2	มีการระบุและจัดทำเอกสารข้อกำหนดและระดับความไว้ใจทั้งหมดสำหรับการเข้าถึงของลูกค้าหรือไม่	
ความปลอดภัยของแอปพลิเคชันและอินเทอร์เฟซ *ความถูกต้องของข้อมูล*	AIS-03.1	มีการใช้งานตัวจัดการความถูกต้องข้อมูลอินพุตและเอาต์พุต (เช่น การกระทบยอดและการตรวจสอบการแก้ไข) สำหรับอินเทอร์เฟซของแอปพลิเคชันและฐานข้อมูลเพื่อป้องกันข้อผิดพลาดจากการประมวลผลด้วยมือหรือระบบ รวมถึงเพื่อป้องกันการเสียหายของข้อมูลหรือไม่	การควบคุมความถูกต้องข้อมูลของ AWS ตามที่อธิบายไว้ภายในรายงาน AWS SOC แสดงให้เห็นการควบคุมความถูกต้องข้อมูลในทุกขั้นตอน รวมถึงระหว่างการส่งข้อมูล การจัดเก็บ และการประมวลผล นอกจากนี้ คุณสามารถดูข้อมูลเพิ่มเติมได้ที่ มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 14 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ความปลอดภัยของแอปพลิเคชันและอินเทอร์เฟซ *ความปลอดภัย / ความถูกต้องของข้อมูล*	AIS-04.1	สถาปัตยกรรมความปลอดภัยข้อมูลออกแบบโดยใช้มาตรฐานของอุตสาหกรรม (เช่น CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS) หรือไม่	สถาปัตยกรรมความปลอดภัยข้อมูลของ AWS มีการออกแบบโดยผสมผสานแนวทางปฏิบัติชั้นนำของอุตสาหกรรม โปรดดูที่การรับรอง รายงาน และเอกสารของ AWS สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติชั้นนำต่างๆ ที่ AWS ปฏิบัติตาม (ดูได้ที่ http://aws.amazon.com/compliance)
การรับประกันการตรวจสอบและการปฏิบัติตามข้อกำหนด *การวางแผนการตรวจสอบ*	AAC-01.1	คุณมีการแสดงข้อมูลยืนยันการตรวจสอบ โดยใช้รูปแบบที่เป็นที่ยอมรับของอุตสาหกรรมและเป็นระบบหรือไม่ (เช่น CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/ Assurance Program, ฯลฯ)	AWS ได้รับการรับรองด้านอุตสาหกรรมและการยืนยันจากหน่วยงานภายนอก รวมถึงจัดหาข้อมูลการรับรอง รายงาน และเอกสารอื่นๆ ที่เกี่ยวข้องบางรายการให้กับลูกค้าของ AWS โดยตรง

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
การรับประกันการตรวจสอบและการปฏิบัติตามข้อกำหนด *การตรวจสอบอิสระ*	AAC-02.1	คุณอนุญาตให้ผู้เช่าสามารถดูรายงาน SOC2/ISO 27001 หรือรายงานการตรวจสอบ/การรับรองภายนอกที่คล้ายคลึงกันหรือไม่	AWS จัดหาการยืนยันจากหน่วยงานภายนอก การรับรอง และรายงาน Service Organization Controls (SOC) รวมถึงรายงานด้านการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องอื่นๆ ให้กับลูกค้าของเราโดยตรงภายใต้ข้อตกลง NDA การรับรองมาตรฐาน ISO 27001 ของ AWS สามารถดาวน์โหลดได้ ที่นี่ รายงาน SOC 3 ของ AWS สามารถดาวน์โหลดได้ ที่นี่ ระบบความปลอดภัยของ AWS จะตรวจดูที่อยู่ IP ตำแหน่งข้อมูลของบริการที่เชื่อมต่อกับอินเทอร์เน็ตทั้งหมดเป็นประจำเพื่อค้นหาช่องโหว่ (การตรวจสอบนี้ไม่รวมถึงอินสแตนซ์ของลูกค้า) ฝ่ายความปลอดภัยของ AWS จะแจ้งต่อฝ่ายที่เหมาะสมให้แก้ไขช่องโหว่ที่ระบุ นอกจากนี้ ความเสี่ยงด้านช่องโหว่จากภายนอกจะได้รับการประเมินโดยบริษัทด้านความปลอดภัยอิสระอยู่เป็นประจำ ข้อมูลที่พบและคำแนะนำต่างๆ ที่ได้จากการประเมินผลเหล่านี้จะได้รับการจัดหมวดหมู่และส่งมอบให้กับผู้นำของ AWS นอกจากนี้ สภาพแวดล้อมการควบคุมของ AWS ยังได้รับการตรวจสอบทั้งจากภายนอกและภายในรวมถึงมีการประเมินความเสี่ยงอย่างสม่ำเสมอ AWS ร่วมมือกับหน่วยงานด้านการรับรองภายนอกและผู้ตรวจสอบอิสระ เพื่อตรวจสอบและทดสอบสภาพแวดล้อมการควบคุมโดยรวมของ AWS
	AAC-02.2	คุณมีการทดสอบเจาะระบบเครือข่ายสำหรับโครงสร้างพื้นฐานบริการระบบคลาวด์อย่างสม่ำเสมอ ตามที่กำหนดโดยแนวทางปฏิบัติและข้อแนะนำของอุตสาหกรรมหรือไม่	
	AAC-02.3	คุณมีการทดสอบเจาะระบบแอปพลิเคชันสำหรับโครงสร้างพื้นฐานระบบคลาวด์อย่างสม่ำเสมอ ตามที่กำหนดโดยแนวทางปฏิบัติและข้อแนะนำของอุตสาหกรรมหรือไม่	
	AAC-02.4	คุณมีการตรวจสอบภายในอย่างสม่ำเสมอ ตามที่กำหนดโดยแนวทางปฏิบัติและข้อแนะนำของอุตสาหกรรมหรือไม่	
	AAC-02.5	คุณมีการตรวจสอบภายนอกอย่างสม่ำเสมอ ตามที่กำหนดโดยแนวทางปฏิบัติและข้อแนะนำของอุตสาหกรรมหรือไม่	
	AAC-02.6	ผลลัพธ์การทดสอบการเจาะระบบเหล่านี้สามารถดูได้โดยผู้เช่าเมื่อมีการร้องขอหรือไม่	
	AAC-02.7	ผลลัพธ์การตรวจสอบภายในและภายนอกเหล่านี้สามารถดูได้โดยผู้เช่าเมื่อมีการร้องขอหรือไม่	
	AAC-02.8	คุณมีโปรแกรมการตรวจสอบภายในที่ยอมให้มีการตรวจสอบการประเมินผลแบบข้ามสายงานหรือไม่	
การรับประกันการตรวจสอบและการปฏิบัติตามข้อกำหนด *การเชื่อมโยงข้อกำหนดของ*	AAC-03.1	คุณมีความสามารถในการแยกส่วนเชิงลอจิคัลหรือเข้ารหัสข้อมูลลูกค้า เพื่อให้ข้อมูลดังกล่าวสามารถนำไปใช้งานได้โดยผู้เช่าเพียงรายเดียว และไม่ต้องเข้าถึงข้อมูลผู้เช่ารายอื่นโดยไม่ตั้งใจหรือไม่	ข้อมูลทั้งหมดของลูกค้าที่จัดเก็บโดย AWS มีความสามารถด้านความปลอดภัยและการควบคุมการแยกส่วนผู้เช่าที่มีประสิทธิภาพ ลูกค้ายังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง ดังนั้นทางเลือกในการเข้ารหัสข้อมูลจึงเป็นความรับผิดชอบของลูกค้า AWS อนุญาตให้ลูกค้าใช้ระบบกลไกการเข้ารหัสของตนเองสำหรับบริการแทบทุกประเภท

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ระบบข้อมูล	AAC-03.2	คุณมีความสามารถในการกู้คืนข้อมูลสำหรับลูกค้าบางรายโดยเฉพาะ ในกรณีที่เกิดความล้มเหลวหรือข้อมูลสูญหายหรือไม่	รวมถึงการเข้ารหัสแบบ S3, EBS, SimpleDB และ EC2 ช่องทาง IPSec ไปยัง VPC ได้รับการเข้ารหัสเช่นกัน นอกจากนี้ ลูกค้ายังสามารถใช้งาน AWS Key Management Systems (KMS) เพื่อสร้างและควบคุมคีย์การเข้ารหัส (ดูรายละเอียดที่ https://aws.amazon.com/kms/) โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security AWS ให้ลูกค้าสามารถสำรองข้อมูลไปยังเทปของตนได้โดยใช้ผู้ให้บริการสำรองข้อมูลเทปของตนเอง อย่างไรก็ตาม การสำรองข้อมูลเทปไม่ใช่บริการที่มีการจัดหาให้โดย AWS บริการของ Amazon S3 และ Glacier ออกแบบมาเพื่อลดโอกาสเกิดการสูญหายของข้อมูลลงจนเกือบจะเป็นศูนย์ รวมถึงเพิ่มระดับความคงทนเทียบเท่ากับการทำสำเนาออบเจ็กต์ข้อมูลแบบหลายไซต์ด้วยการทำซ้ำการจัดเก็บข้อมูล สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความคงทนของข้อมูลและการทำซ้ำ โปรดดูที่เว็บไซต์ของ AWS
	AAC-03.3	คุณมีความสามารถในการจำกัดการจัดเก็บข้อมูลของลูกค้าไปยังบางประเทศหรือตำแหน่งทางภูมิศาสตร์ใดๆ โดยเฉพาะหรือไม่	ลูกค้าของ AWS คือผู้กำหนดว่าเนื้อหาของพวกเขาจะถูกระบุไว้ภายในภูมิภาคทางกายภาพใด AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าจากภูมิภาคที่ลูกค้าเลือกโดยไม่แจ้งให้ลูกค้าทราบ ยกเว้นจะได้รับการระบุให้ปฏิบัติตามกฎหมาย หรือมีการร้องขอจากหน่วยงานของรัฐ สำหรับรายการภูมิภาคทั้งหมดที่มีให้บริการ โปรดดูที่เพจ โครงสร้างพื้นฐานส่วนกลางของ AWS
	AAC-03.4	คุณมีโปรแกรมซึ่งครอบคลุมความสามารถในการติดตามการเปลี่ยนแปลงในข้อกำหนดด้านระเบียบข้อบังคับกฎหมายที่เกี่ยวข้อง ปรับเปลี่ยนโปรแกรมความปลอดภัยเพื่อรองรับการเปลี่ยนแปลงตามข้อกำหนดทางกฎหมาย และรับประกันการปฏิบัติตามระเบียบข้อบังคับทางกฎหมายที่เกี่ยวข้องหรือไม่	AWS ติดตามข้อกำหนดด้านกฎระเบียบและกฎหมายที่เกี่ยวข้อง โปรดดู มาตรฐาน ISO 27001 ภาคผนวก 18 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *การวางแผนความต่อเนื่องทางธุรกิจ*	BCR-01.1	คุณให้บริการตัวเลือกการเช่าโฮสต์ที่มีความยืดหยุ่นทางภูมิศาสตร์หรือไม่	ศูนย์ข้อมูลสร้างเป็นกลุ่มอยู่ในภูมิภาคต่างๆ ทั่วโลก AWS มาพร้อมกับความยืดหยุ่นสำหรับการวางอินสแตนซ์และการเก็บข้อมูลภายในภูมิภาคทางภูมิศาสตร์หลากหลายแห่ง รวมถึงการกำหนดข้ามพื้นที่ให้บริการภายในแต่ละภูมิภาค ลูกค้าควรออกแบบการใช้งาน AWS ของตนเองให้ใช้ประโยชน์จากภูมิภาคและพื้นที่ให้บริการหลายแห่ง โปรดดูรายละเอียดเพิ่มเติมจากเอกสารภาพรวมความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	BCR-01.2	คุณมอบคุณสมบัติการป้องกันความผิดพลาดบริการโครงสร้างพื้นฐานไปยังผู้ให้บริการอื่นแก่ผู้เช่าหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *การทดสอบความต่อเนื่องทางธุรกิจ*	BCR-02.1	แผนการความต่อเนื่องทางธุรกิจมีการทดสอบตามช่วงเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเชิงองค์กรหรือสภาพแวดล้อมเพื่อรับประกันประสิทธิภาพอันต่อเนื่องของธุรกิจหรือไม่	นโยบายและแผนงานด้านความต่อเนื่องทางธุรกิจของ AWS ได้รับการพัฒนาและทดสอบให้สอดคล้องกับมาตรฐาน ISO 27001 โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 17 สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับ AWS และความต่อเนื่องทางธุรกิจ
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *ไฟฟ้า / การสื่อสารทางไกล*	BCR-03.1	คุณจัดหาเอกสารที่แสดงเส้นทางการส่งผ่านข้อมูลระหว่างระบบให้กับผู้เช่าหรือไม่	ลูกค้าของ AWS เป็นผู้กำหนดว่าเนื้อหาและเซิร์ฟเวอร์ของพวกเขาจะถูกระบุไว้ภายในภูมิภาคทางกายภาพใด AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าจากภูมิภาคที่ลูกค้าเลือกโดยไม่แจ้งให้ลูกค้าทราบ ยกเว้นจะได้รับการระบุให้ปฏิบัติตามกฎหมาย หรือมีการร้องขอจากหน่วยงานของรัฐ รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติม ลูกค้าสามารถเลือกพาธเครือข่ายเพื่อเชื่อมต่อไปยังสถานที่ของ AWS ได้ด้วยตนเอง รวมถึงผ่านเครือข่ายแบบส่วนตัวโดยตรง ซึ่งลูกค้าจะเป็นผู้ควบคุมเส้นทางการถ่ายโอนข้อมูลเอง
	BCR-03.2	ผู้เช่าสามารถระบุวิธีการส่งผ่านข้อมูลของพวกเขา รวมถึงขอบเขตอำนาจทางกฎหมายที่เกี่ยวข้องได้หรือไม่	
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ เอกสารประกอบ	BCR-04.1	มีการจัดเตรียมเอกสารด้านระบบข้อมูลต่างๆ (เช่น คู่มือผู้ใช้งานและผู้ดูแลระบบ ไดอะแกรมสถาปัตยกรรม ฯลฯ) สำหรับบุคลากรที่ได้รับอนุญาต เพื่อรับประกันการกำหนดค่า การติดตั้ง และการปฏิบัติการของระบบข้อมูลหรือไม่	เอกสารระบบข้อมูลมีให้ใช้งานภายในโดยบุคลากรของ AWS ผ่านการใช้งานไซต์แบบอินทราเน็ตของ Amazon โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security/ โปรดดูที่ ISO 27001 ภาคผนวก A ส่วนที่ 12
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *ความเสี่ยงด้านสภาพแวดล้อม*	BCR-05.1	มีการคาดการณ์และวางแผนเกี่ยวกับการป้องกันเชิงกายภาพต่อความเสียหาย (เช่น สาเหตุทางธรรมชาติ ภัยพิบัติธรรมชาติ และการโจมตีโดยตรง) พร้อมวางมาตรการสำหรับรับมือหรือไม่	ศูนย์ข้อมูลของ AWS มีการป้องกันทางกายภาพเพื่อรับมือกับความเสี่ยงด้านสภาพแวดล้อม การป้องกันทางกายภาพของ AWS ต่อความเสี่ยงด้านสภาพแวดล้อมนี้ผ่านการรับรองโดยผู้ตรวจสอบอิสระ และได้รับการรับรองถึงความสอดคล้องกับแนวทางปฏิบัติของมาตรฐาน ISO 27002 โปรดดูที่ มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 11
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *ตำแหน่งที่ตั้งอุปกรณ์*	BCR-06.1	มีศูนย์ข้อมูลใดตั้งอยู่ในพื้นที่ที่มีโอกาสสูงในการเกิดความเสี่ยงด้านสภาพแวดล้อมซึ่งส่งผลกระทบรุนแรงหรือไม่ (น้ำท่วม พายุทอร์นาโด แผ่นดินไหว เฮอร์ริเคน ฯลฯ)	ศูนย์ข้อมูลของ AWS มีการป้องกันทางกายภาพเพื่อรับมือกับความเสี่ยงด้านสภาพแวดล้อม การป้องกันทางกายภาพของ AWS ต่อความเสี่ยงด้านสภาพแวดล้อมนี้ผ่านการรับรองโดยผู้ตรวจสอบอิสระ และได้รับการรับรองถึงความสอดคล้องกับแนวทางปฏิบัติของมาตรฐาน ISO 27002 โปรดดูที่ มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 11

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *การบำรุงรักษาอุปกรณ์*	BCR-07.1	หากมีการใช้งานโครงสร้างพื้นฐานแบบเสมือน โซลูชันระบบคลาวด์มีคุณสมบัติการคืนค่าและกู้คืนฮาร์ดแวร์แบบอิสระจากกันหรือไม่	ฟังก์ชัน EBS Snapshot ช่วยให้ลูกค้าสามารถเก็บบันทึกและคืนค่าอิมเมจของเครื่องเสมือนได้ตลอดเวลา ลูกค้าสามารถส่งออก AMI ของตนเองและนำไปใช้งานภายในไซต์หรือใช้งานกับผู้ให้บริการอื่นได้ (ภายใต้ข้อจำกัดด้านสิทธิ์การใช้งานซอฟต์แวร์) โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	BCR-07.2	หากมีการใช้งานโครงสร้างพื้นฐานแบบเสมือน คุณมีคุณสมบัติในการคืนค่าเครื่องเสมือนเป็นสถานะก่อนหน้าให้กับผู้เช่าหรือไม่	
	BCR-07.3	หากมีการใช้งานโครงสร้างพื้นฐานแบบเสมือน คุณมีการยอมให้ดาวน์โหลดอิมเมจของเครื่องเสมือนและพอร์ตไปยังผู้ให้บริการคลาวด์รายใหม่หรือไม่	
	BCR-07.4	หากมีการใช้งานโครงสร้างพื้นฐานแบบเสมือน อิมเมจของเครื่องนั้นมีการมอบให้กับลูกค้าในแบบที่ลูกค้าจะสามารถนำอิมเมจดังกล่าวไปทำซ้ำภายในพื้นที่การจัดเก็บของตนเองภายนอกไซต์ได้หรือไม่	
	BCR-07.5	โซลูชันระบบคลาวด์ประกอบด้วยคุณสมบัติการคืนค่าและกู้คืนซอฟต์แวร์/ผู้ให้บริการแบบแยกอิสระหรือไม่	
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *ความล้มเหลวด้านระบบไฟฟ้าของอุปกรณ์*	BCR-08.1	มีระบบกลไกด้านความปลอดภัยและการสำรองการทำงานเพื่อป้องกันอุปกรณ์จากความขัดข้องในการให้บริการหรือไม่ (เช่น ระบบไฟฟ้าขัดข้อง การขัดข้องของเครือข่าย ฯลฯ)	อุปกรณ์ของ AWS ได้รับการป้องกันจากการขัดข้องในการให้บริการที่สอดคล้องตามมาตรฐาน ISO 27001 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001 รายงาน AWS SOC แสดงรายละเอียดเพิ่มเติมเกี่ยวกับการควบคุมที่มีอยู่ เพื่อลดผลกระทบจากการทำงานผิดพลาดหรือจากหายนะทางกายภาพที่เกิดขึ้นกับคอมพิวเตอร์และสถานที่ตั้งศูนย์ข้อมูล นอกจากนี้ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *การวิเคราะห์*	BCR-09.1	คุณแสดงให้ผู้เช่าทราบถึงรายละเอียดต่างๆ อย่างต่อเนื่อง รวมถึงรายงานเกี่ยวกับประสิทธิภาพด้านข้อตกลงระดับการให้บริการ (SLA) เชิงปฏิบัติการหรือไม่	AWS CloudWatch ทำหน้าที่ตรวจสอบทรัพยากรบน AWS Cloud และแอปพลิเคชันที่ลูกค้ารันบน AWS โปรดดูที่ aws.amazon.com/cloudwatch สำหรับรายละเอียดเพิ่มเติม นอกจากนี้ AWS ยังเผยแพร่ข้อมูลด้านความพร้อมการให้บริการของเราผ่าน Service Health Dashboard แบบอัพเดทจนถึง

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ผลกระทบ	BCR-09.2	คุณมีวิธีการทำให้ผู้เช่าสามารถใช้ตัววัดผลด้านความปลอดภัยของข้อมูลตามมาตรฐาน (CSA, CAMM, ฯลฯ) หรือไม่	นาทีล่าสุด โดยสามารถดูได้ที่ status.aws.amazon.com
	BCR-09.3	คุณแสดงให้ลูกค้าทราบถึงรายละเอียดต่างๆ อย่างต่อเนื่อง รวมถึงรายงานเกี่ยวกับประสิทธิภาพของ SLA หรือไม่	
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *นโยบาย*	BCR-10.1	มีนโยบายและกระบวนการต่างๆ ไว้ และสามารถใช้งานได้โดยบุคลากรทุกคนเพื่อสนับสนุนบทบาทด้านปฏิบัติการให้บริการได้อย่างเหมาะสมหรือไม่	นโยบายและกระบวนการต่างๆ จัดทำขึ้นผ่านกรอบงานด้านความปลอดภัยของ AWS โดยอ้างอิงตามมาตรฐาน NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 และข้อกำหนด PCI DSS โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความเสี่ยงและการปฏิบัติตามข้อกำหนดของ AWS ที่ http://aws.amazon.com/compliance
การบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นด้านปฏิบัติการ *นโยบายการเก็บรักษา*	BCR-11.1	คุณมีความสามารถในการควบคุมเชิงเทคนิคเพื่อบังคับใช้นโยบายการเก็บรักษาข้อมูลต่อผู้เช่าหรือไม่	AWS มอบความสามารถให้แก่ลูกค้าในการลบข้อมูลของตนเองได้ อย่างไรก็ดี ลูกค้าของ AWS ยังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง ดังนั้นลูกค้าจึงเป็นผู้รับผิดชอบในการจัดการเก็บรักษาข้อมูลให้ตรงตามข้อกำหนดของตนเอง โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security AWS เห็นชอบกับการปกป้องความเป็นส่วนตัวของลูกค้า และระมัดระวังในการวิเคราะห์ว่าควรปฏิบัติตามข้อเรียกร้องการบังคับใช้กฎหมายใด AWS ไม่ลังเลที่จะท้าทายต่อคำสั่งจากการบังคับใช้กฎหมายหากเราคิดว่าคำสั่งนั้นขาดความสมเหตุสมผล สำหรับข้อมูลเพิ่มเติม โปรดดูที่ https://aws.amazon.com/compliance/data-privacy-faq/
	BCR-11.2	คุณมีกระบวนการที่บันทึกเป็นเอกสารที่ว่าด้วยการตอบสนองต่อคำขอข้อมูลผู้เช่าจากรัฐบาลหรือบุคคลภายนอกหรือไม่	
	BCR-11.4	คุณมีการนำระบบกลไกการสำรองข้อมูลหรือการทำซ้ำมาใช้งาน เพื่อรับรองถึงการปฏิบัติตามข้อบังคับ กฎหมาย สัญญา หรือข้อกำหนดทางธุรกิจหรือไม่	ระบบกลไกการสำรองข้อมูลและการทำซ้ำของ AWS ได้รับการพัฒนาและทดสอบให้สอดคล้องกับมาตรฐาน ISO 27001 โปรดดูที่มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 12 และรายงาน AWS SOC 2 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับระบบกลไกการสำรองข้อมูลและการทำซ้ำของ AWS
	BCR-11.5	คุณมีการทดสอบระบบกลไกการสำรองข้อมูลหรือการทำซ้ำอย่างน้อยปีละหนึ่งครั้งหรือไม่	
การควบคุมการเปลี่ยนแปลงและการจัดการการกำหนดค่า *การพัฒนา / การจัดซื้อใหม่*	CCC-01.1	มีนโยบายและขั้นตอนสำหรับการอนุญาตด้านการจัดการเพื่อกระบวนการพัฒนาหรือการจัดซื้อแอปพลิเคชัน ระบบฐานข้อมูล โครงสร้างพื้นฐานบริการ ปฏิบัติการ และสถานที่หรือไม่	นโยบายและกระบวนการต่างๆ จัดทำขึ้นผ่านกรอบงานด้านความปลอดภัยของ AWS โดยอ้างอิงตามมาตรฐาน NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 และข้อกำหนด PCI DSS ไม่ว่าลูกค้าจะไม่เคยใช้งาน AWS มาก่อนหรือเป็นลูกค้าที่มีประสบการณ์ ก็สามารถดูข้อมูลที่เป็นประโยชน์เกี่ยวกับบริการต่างๆ ตั้งแต่บทนำ จนถึงคุณลักษณะขั้นสูงได้ในส่วนเอกสาร AWS บนเว็บไซต์ของเราที่

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
			https://aws.amazon.com/documentation/
	CCC-01.2	มีเอกสารที่อธิบายเกี่ยวกับการติดตั้ง การกำหนดค่า และการใช้งานผลิตภัณฑ์/บริการ/คุณสมบัติต่างๆ หรือไม่	
การควบคุมการเปลี่ยนแปลงและการจัดการการกำหนดค่า *การพัฒนาแบบเอาต์ซอร์ส*	CCC-02.1	คุณมีการควบคุมเพื่อรับประกันว่าการพัฒนาซอฟต์แวร์ทั้งหมดจะสอดคล้องกับมาตรฐานด้านคุณภาพหรือไม่	โดยปกติแล้ว AWS จะไม่เอาต์ซอร์สการพัฒนาซอฟต์แวร์ AWS มีการกำหนดมาตรฐานด้านคุณภาพในฐานะส่วนหนึ่งของกระบวนการวงจรการพัฒนาระบบ (SDLC) โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 14 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	CCC-02.2	คุณมีการควบคุมเพื่อตรวจสอบหาข้อบกพร่องด้านความปลอดภัยของซอร์สโค้ด สำหรับการพัฒนาซอฟต์แวร์ที่เอาต์ซอร์สไปภายนอกหรือไม่	
การควบคุมการเปลี่ยนแปลงและการจัดการ *การกำหนดค่า* *การทดสอบด้านคุณภาพ*	CCC-03.1	คุณมีการมอบเอกสารซึ่งอธิบายเกี่ยวกับกระบวนการรับประกันด้านคุณภาพให้แก่ผู้เช่าหรือไม่	AWS ได้รับการรับรองตามมาตรฐาน ISO 9001 สิ่งนี้เป็นรับรองอย่างอิสระจากภายนอกถึงระบบคุณภาพของ AWS และเป็นการกำหนดว่ากิจกรรมต่างๆ ของ AWS นั้นสอดคล้องตามข้อกำหนดของ ISO 9001 กระดานข่าวด้านความปลอดภัยของ AWS จะแจ้งให้ลูกค้าทราบเกี่ยวกับเหตุการณ์ด้านความปลอดภัยและความเป็นส่วนตัว ลูกค้าสามารถสมัครรับข้อมูลจากฟีด RSS ของกระดานข่าวด้านความปลอดภัยของ AWS บนเว็บไซต์ของเรา โปรดดูที่ aws.amazon.com/security/security-bulletins/ นอกจากนี้ AWS ยังเผยแพร่ข้อมูลด้านความพร้อมการให้บริการของเราผ่าน Service Health Dashboard แบบอัพเดทจนถึงนาทีล่าสุด โดยสามารถดูได้ที่ status.aws.amazon.com วงจรการพัฒนาระบบของ AWS (SDLC) ใช้แนวทางการปฏิบัติของอุตสาหกรรม ซึ่งรวมถึงการตรวจสอบการออกแบบอย่างเป็นทางการจากทีมรักษาความปลอดภัยของ AWS การกำหนดต้นแบบภัยคุกคาม และการดำเนินการประเมินความเสี่ยง โปรดดูข้อมูลเพิ่มเติมได้จาก ภาพรวมของกระบวนการรักษาความปลอดภัยของ AWS นอกจากนี้ โปรดดูมาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 14 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	CCC-03.2	มีเอกสารที่อธิบายเกี่ยวกับปัญหาซึ่งเป็นที่ทราบกันดี ซึ่งพบในผลิตภัณฑ์/บริการบางรายการหรือไม่	
	CCC-03.3	มีการกำหนดนโยบายและกระบวนการเพื่อคัดแยกและแก้ไขปัญหาจากบัก รวมถึงช่องโหว่ด้านความปลอดภัยที่มีการรายงานสำหรับข้อเสนอผลิตภัณฑ์และบริการหรือไม่	
	CCC-03.4	มีระบบกลไกเพื่อรับประกันว่าการดีบักและองค์ประกอบของโค้ดทดสอบทั้งหมดได้ถูกนำออกจากเวอร์ชันซอฟต์แวร์ที่นำเสนอหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
การควบคุมการเปลี่ยนแปลงและการจัดการการกำหนดค่า *การติดตั้งซอฟต์แวร์โดยไม่ได้รับอนุญาต*	CCC-04.1	คุณกำหนดการควบคุมเพื่อจำกัดและตรวจสอบการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตภายในระบบหรือไม่	โปรแกรม กระบวนการ และขั้นตอนต่างๆ ของ AWS สำหรับจัดการซอฟต์แวร์ประสงค์ร้ายนั้นสอดคล้องกับมาตรฐานของ ISO 27001 โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 12 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
การควบคุมการเปลี่ยนแปลงและการจัดการการกำหนดค่า *การเปลี่ยนแปลงสำหรับการใช้งานจริง*	CCC-05.1	คุณมีการมอบเอกสารให้แก่ผู้เช่า ซึ่งเอกสารดังกล่าวอธิบายถึงขั้นตอนการจัดการด้านการเปลี่ยนแปลงการใช้งานจริงและบทบาท / สิทธิ์ / ความรับผิดชอบของผู้เช่าหรือไม่	รายงาน AWS SOC แสดงภาพรวมของการควบคุมที่มีเพื่อจัดการกับการเปลี่ยนแปลงภายในสภาพแวดล้อม AWS นอกจากนี้ โปรดดูมาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 12 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ความปลอดภัยข้อมูลและการจัดการวงจรข้อมูล *การจัดหมวดหมู่*	DSI-01.1	คุณมอบคุณสมบัติในการระบุเครื่องเสมือนโดยใช้แท็กด้านนโยบาย/ข้อมูลเมตาหรือไม่ (เช่น สามารถใช้แท็กเพื่อจำกัดจำนวนระบบปฏิบัติการเยือนที่เริ่มต้นระบบได้/สร้างอินสแตนซ์/ส่งผ่านข้อมูลในประเทศที่ไม่ถูกต้อง)	เครื่องเสมือนมีการกำหนดสิทธิ์ให้กับลูกค้าโดยเป็นส่วนหนึ่งของบริการ EC2 ลูกค้ายังคงมีอำนาจควบคุมประเภทของทรัพยากรที่ใช้ รวมถึงตำแหน่งการจัดเก็บทรัพยากร โปรดดูรายละเอียดเพิ่มเติมจากเว็บไซต์ AWS ที่ http://aws.amazon.com
	DSI-01.2	คุณมีการมอบคุณสมบัติในการระบุตัวตนฮาร์ดแวร์ผ่าน แท็กด้านนโยบาย/ข้อมูลเมตา/แท็กด้านฮาร์ดแวร์ หรือไม่ (เช่น TXT/TPM, VN-Tag ฯลฯ)	AWS มีความสามารถในการแท็กทรัพยากร EC2 ในฐานะข้อมูลเมตารูปแบบหนึ่ง แท็ก EC2 สามารถใช้เพื่อสร้างชื่อที่จดจำได้ง่าย ปรับปรุงประสิทธิภาพการค้นหา และยกระดับการทำงานร่วมกันระหว่างผู้ใช้หลายราย AWS Management Console ก็รองรับการแท็กเช่นกัน
	DSI-01.3	คุณมีความสามารถในการใช้ตำแหน่งทางภูมิศาสตร์ของระบบเพื่อเป็นปัจจัยการรับรองความถูกต้องหรือไม่	AWS มอบความสามารถในการกำหนดการเข้าถึงของผู้ใช้งานแบบมีเงื่อนไข โดยอ้างอิงจากที่อยู่ IP ลูกค้าสามารถเพิ่มเงื่อนไขเพื่อใช้ควบคุมวิธีการใช้งาน AWS ของผู้ใช้ เช่น เวลาของวัน ที่อยู่ IP ต้นทาง หรือการตรวจสอบว่าผู้ใช้มีการใช้งาน SSL หรือไม่
	DSI-01.4	คุณสามารถมอบข้อมูลตำแหน่งทางกายภาพ/ทางภูมิศาสตร์ของพื้นที่จัดเก็บข้อมูลผู้เช่าได้หรือไม่ หากมีการร้องขอ	AWS มาพร้อมกับความยืดหยุ่นสำหรับการวางอินสแตนซ์และการเก็บข้อมูลภายในภูมิภาคทางภูมิศาสตร์หลากหลายแห่ง ลูกค้าของ AWS เป็นผู้กำหนดว่าเนื้อหาและเซิร์ฟเวอร์ของพวกเขาจะถูกระบุไว้ภายในภูมิภาคทางกายภาพใด AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าจากภูมิภาคที่ลูกค้าเลือกโดยไม่แจ้งให้ลูกค้าทราบ ยกเว้นจะได้รับการระบุให้ปฏิบัติตามกฎหมาย หรือมีการร้องขอจากหน่วยงานของรัฐ ณ เวลาที่เอกสารฉบับนี้จัดทำขึ้น AWS ประกอบด้วย 12 ภูมิภาค ได้แก่: สหรัฐอเมริกาฝั่งตะวันออก (เวอร์จิเนียตอนเหนือ), สหรัฐอเมริกาฝั่งตะวันตก (โอริกอน), สหรัฐอเมริกาฝั่งตะวันตก (แคลิฟอร์เนียตอนเหนือ), AWS GovCloud (สหรัฐอเมริกา) (โอริกอน), สหภาพยุโรป (ไอร์แลนด์), สหภาพยุโรป (แฟรงก์เฟิร์ต) , เอเชียแปซิฟิก (โซล),
	DSI-01.5	คุณสามารถมอบข้อมูลตำแหน่งทางกายภาพ/ทางภูมิศาสตร์ของพื้นที่จัดเก็บข้อมูลผู้เช่าได้ล่วงหน้าหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
			เอเชียแปซิฟิก (สิงคโปร์), เอเชียแปซิฟิก (โตเกียว), เอเชียแปซิฟิก (ซิดนีย์), จีน (ปักกิ่ง) และอเมริกาใต้ (เซาเปาโล)
	DSI-01.6	คุณปฏิบัติตามมาตรฐานการติดป้ายข้อมูลแบบเป็นระบบหรือไม่ (เช่น ISO 15489, Oasis XML Catalog Specification, คำแนะนำด้านประเภทข้อมูลของ CSA)	ลูกค้าของ AWS ยังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง และอาจใช้มาตรฐานการติดป้ายข้อมูลแบบเป็นระบบเพื่อให้เหมาะกับข้อกำหนดของตนเอง
	DSI-01.7	คุณยินยอมให้ผู้เช่าระบุตำแหน่งทางภูมิศาสตร์ที่ยอมรับได้สำหรับการกำหนดเส้นทางข้อมูล หรือการสร้างทรัพยากรหรือไม่	AWS มาพร้อมกับความยืดหยุ่นสำหรับการวางอินสแตนซ์และการเก็บข้อมูลภายในภูมิภาคทางภูมิศาสตร์หลากหลายแห่ง ลูกค้าของ AWS เป็นผู้กำหนดว่าเนื้อหาและเซิร์ฟเวอร์ของพวกเขาจะถูกระบุไว้ภายในภูมิภาคทางกายภาพใด AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าจากภูมิภาคที่ลูกค้าเลือกโดยไม่แจ้งให้ลูกค้าทราบ ยกเว้นจะได้รับการระบุให้ปฏิบัติตามกฎหมาย หรือมีการร้องขอจากหน่วยงานของรัฐ ณ เวลาที่เอกสารฉบับนี้จัดทำขึ้น AWS ประกอบด้วย 12 ภูมิภาค ได้แก่: สหรัฐอเมริกาฝั่งตะวันออก (เวอร์จิเนียตอนเหนือ), สหรัฐอเมริกาฝั่งตะวันตก (โอริกอน), สหรัฐอเมริกาฝั่งตะวันตก (แคลิฟอร์เนียตอนเหนือ), AWS GovCloud (สหรัฐอเมริกา) (โอริกอน), สหภาพยุโรป (ไอร์แลนด์), สหภาพยุโรป (แฟรงก์เฟิร์ต) , เอเชียแปซิฟิก (โซล), เอเชียแปซิฟิก (สิงคโปร์), เอเชียแปซิฟิก (โตเกียว), เอเชียแปซิฟิก (ซิดนีย์), จีน (ปักกิ่ง) และอเมริกาใต้ (เซาเปาโล)
ความปลอดภัยข้อมูลและการจัดการวงจรข้อมูล *รายการข้อมูล / โฟลว์*	DSI-02.1	คุณมีการจัดทำรายการข้อมูล จัดทำเอกสาร และเก็บรักษาโฟลว์ข้อมูล สำหรับข้อมูลที่อยู่ภายในแอปพลิเคชันของบริการ รวมถึงเครือข่ายและระบบโครงสร้างพื้นฐานหรือไม่ (ทั้งที่มีอยู่ถาวรและแบบชั่วคราว)	ลูกค้าของ AWS คือผู้กำหนดว่าเนื้อหาของพวกเขาจะถูกระบุไว้ภายในภูมิภาคทางกายภาพใด AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าจากภูมิภาคที่ลูกค้าเลือกโดยไม่แจ้งให้ลูกค้าทราบ ยกเว้นจะได้รับการระบุให้ปฏิบัติตามกฎหมาย หรือมีการร้องขอจากหน่วยงานของรัฐ ณ เวลาที่เอกสารฉบับนี้จัดทำขึ้น AWS ประกอบด้วย 12 ภูมิภาค ได้แก่: สหรัฐอเมริกาฝั่งตะวันออก (เวอร์จิเนียตอนเหนือ), สหรัฐอเมริกาฝั่งตะวันตก (โอริกอน), สหรัฐอเมริกาฝั่งตะวันตก (แคลิฟอร์เนียตอนเหนือ), AWS GovCloud (สหรัฐอเมริกา) (โอริกอน), สหภาพยุโรป (ไอร์แลนด์), สหภาพยุโรป (แฟรงก์เฟิร์ต) , เอเชียแปซิฟิก (โซล), เอเชียแปซิฟิก (สิงคโปร์), เอเชียแปซิฟิก (โตเกียว), เอเชียแปซิฟิก (ซิดนีย์), จีน (ปักกิ่ง) และอเมริกาใต้ (เซาเปาโล)
	DSI-02.2	คุณสามารถรับรองได้หรือไม่ว่าข้อมูลจะไม่ถูกโอนย้ายผ่านการพำนักอยู่ภายในพื้นที่เชิงภูมิศาสตร์ที่กำหนดไว้	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ความปลอดภัยข้อมูลและการจัดการวงจรข้อมูล *การทำธุรกรรมระบบอีคอมเมิร์ซ*	DSI-03.1	คุณจัดหาบริการระเบียบวิธีการเข้ารหัสข้อมูลแบบเปิด (3.4ES, AES, ฯลฯ) ให้แก่ผู้เช่าหรือไม่ เพื่อให้ผู้เช่าสามารถป้องกันข้อมูลของตนเองได้หากจำเป็นต้องมีการส่งผ่านข้อมูลผ่านเครือข่ายสาธารณะ (เช่น อินเทอร์เน็ต)	API ของ AWS ทั้งหมดพร้อมใช้งานผ่านตำแหน่งข้อมูลที่ได้รับการปกป้องด้วย SSH ซึ่งมาพร้อมกับการรับรองความถูกต้องของเซิร์ฟเวอร์ AWS อนุญาตให้ลูกค้าใช้ระบบกลไกการเข้ารหัสของตนเองสำหรับบริการแทบทุกประเภท รวมถึงการเข้ารหัสแบบ S3, EBS, SimpleDB และ EC2 ช่องทาง IPSec ไปยัง VPC ได้รับการเข้ารหัสเช่นกัน นอกจากนี้ ลูกค้ายังสามารถใช้งาน AWS Key Management Systems (KMS) เพื่อสร้างและควบคุมคีย์การเข้ารหัส (ดูรายละเอียดที่ https://aws.amazon.com/kms/) ลูกค้ายังสามารถใช้เทคโนโลยีการเข้ารหัสของบุคคลที่สามได้เช่นกัน โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	DSI-03.2	คุณใช้ระเบียบวิธีการเข้ารหัสแบบเปิดทุกครั้งที่องค์ประกอบภายในโครงสร้างพื้นฐานจำเป็นต้องสื่อสารกับส่วนอื่นๆ ผ่านเครือข่ายสาธารณะหรือไม่ (เช่น การทำซ้ำข้อมูลบนอินเทอร์เน็ตจากสภาพแวดล้อมหนึ่งไปยังอีกสภาพแวดล้อมหนึ่ง)	
ความปลอดภัยข้อมูลและการจัดการวงจรข้อมูล *การจัดการ / การติดป้าย / นโยบายด้านความปลอดภัย*	DSI-04.1	มีนโยบายและขั้นตอนสำหรับการติดป้าย จัดการ และสำหรับความปลอดภัยของข้อมูลและออบเจ็กต์ที่ประกอบด้วยข้อมูลหรือไม่	ลูกค้าของ AWS ยังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง และอาจใช้มาตรฐานการติดป้ายข้อมูล รวมถึงนโยบายและขั้นตอนการจัดการเพื่อให้เหมาะกับข้อกำหนดของตนเอง
	DSI-04.2	มีการใช้งานระบบกลไกสำหรับการรับค่าป้ายกับออบเจ็กต์ที่ทำหน้าที่เป็นคอนเทนเนอร์รวมสำหรับข้อมูลหรือไม่	
ความปลอดภัยข้อมูลและการจัดการวงจรข้อมูล *ข้อมูลที่ไม่ใช่สำหรับการใช้งานจริง*	DSI-05.1	คุณมีกระบวนการเพื่อรับรองว่าข้อมูลสำหรับการใช้งานจริงจะไม่ถูกทำซ้ำ หรือมีการนำไปใช้งานภายในสภาพแวดล้อมที่ไม่ใช่สำหรับการใช้งานจริงหรือไม่	ลูกค้า AWS ยังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง AWS มอบความสามารถให้กับลูกค้าในการรักษาและพัฒนาสภาพแวดล้อมสำหรับการใช้งานจริงและสภาพแวดล้อมที่ไม่ใช่สำหรับการใช้งานจริง ลูกค้ามีหน้าที่รับผิดชอบเพื่อรับรองว่าข้อมูลสำหรับการใช้งานจริงของตนเองนั้นจะไม่ถูกทำซ้ำภายในสภาพแวดล้อมที่ไม่ใช่สำหรับการใช้งานจริง
ความปลอดภัยข้อมูลและการจัดการวงจรข้อมูล *การเป็นเจ้าของ / การดูแล*	DSI-06.1	มีการกำหนด มอบหมาย จัดทำเอกสาร หรือสื่อสารเกี่ยวกับความรับผิดชอบในแง่การดูแลข้อมูลหรือไม่	ลูกค้า AWS ยังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง โปรดดูข้อมูลเพิ่มเติมได้จากข้อตกลงสำหรับลูกค้าของ AWS
ความปลอดภัยข้อมูลและการจัดการวงจรข้อมูล *การกำจัดทำลายอย่างปลอดภัย*	DSI-07.1	คุณสนับสนุนการลบออกอย่างปลอดภัย (เช่น การลบสภาพแม่เหล็ก/การล้างแบบเข้ารหัส) สำหรับข้อมูลเก็บถาวรและข้อมูลสำรอง ตามที่กำหนดโดยผู้เช่าหรือไม่	เมื่ออุปกรณ์เก็บข้อมูลสิ้นสุดอายุการใช้งาน การดำเนินการ AWS จะมีขั้นตอนในการปลดการทำงานซึ่งออกแบบมาเพื่อป้องกันไม่ให้ข้อมูลของลูกค้าถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาต AWS ใช้เทคนิคตามที่ระบุใน DoD 5220.22-M (“National Industrial Security Program Operating Manual”) หรือ NIST

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	DSI-07.2	คุณสามารถอธิบายขั้นตอนที่มีการเผยแพร่สำหรับการออกจากข้อตกลงการให้บริการ ซึ่งรวมถึงการรับประกันว่าจะมีการล้างข้อมูลของผู้เช่าออกจากทรัพยากรการประมวลผลทั้งหมด หลังจากที่ลูกค้าออกจากสภาพแวดล้อมหรือจากทรัพยากรได้หรือไม่	800-88 (“Guidelines for Media Sanitization”) เพื่อทำลายข้อมูลอันเป็นส่วนหนึ่งของกระบวนการปลดการทำงาน หากไม่สามารถปลดการทำงานอุปกรณ์ฮาร์ดแวร์ได้ด้วยกระบวนการดังกล่าว อุปกรณ์จะถูกลบสภาพแม่เหล็กหรือทำลายทิ้งตามวิธีที่เป็นมาตรฐานอุตสาหกรรม โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security โวลุ่ม Amazon EBS จะแสดงให้คุณเห็นในรูปแบบอุปกรณ์บล็อกแบบ Raw ที่ยังไม่ฟอร์แมต ซึ่งมีการล้างข้อมูลก่อนเปิดให้ใช้งาน การล้างข้อมูลจะเกิดขึ้นในทันทีก่อนการนำกลับมาใช้ใหม่ เพื่อให้คุณมั่นใจได้ว่ากระบวนการล้างข้อมูลจะเสร็จสมบูรณ์ดี หากคุณมีขั้นตอนที่กำหนดให้ต้องล้างข้อมูลทั้งหมดด้วยวิธีการเฉพาะ เช่น ตามที่ระบุรายละเอียดใน DoD 5220.22-M (“National Industrial Security Program Operating Manual”) หรือ NIST 800-88 (“Guidelines for Media Sanitization”) คุณสามารถดำเนินการดังกล่าวใน Amazon EBS ได้ คุณควรดำเนินการล้างข้อมูลพิเศษก่อนลบโวลุ่ม เพื่อให้เป็นไปตามข้อกำหนดที่ระบุไว้ การเข้ารหัสข้อมูลสำคัญเป็นแนวทางการรักษาความปลอดภัยที่ดี และ AWS จะมอบความสามารถในการเข้ารหัสโวลุ่ม EBS และสแนปช็อตด้วย AES-256 การเข้ารหัสจะเกิดขึ้นบนเซิร์ฟเวอร์ที่โฮสต์ EC2 Instance ซึ่งจะเข้ารหัสข้อมูลเมื่อทำการย้ายข้อมูลระหว่าง EC2 Instance กับพื้นที่เก็บข้อมูล EBS เพื่อให้สามารถทำเช่นนี้อย่างมีประสิทธิภาพและมีความหน่วงต่ำ คุณสมบัติการเข้ารหัส EBS จะใช้งานได้เฉพาะในอินสแตนซ์ของ EC2 ประเภทที่มีประสิทธิภาพมากกว่าเท่านั้น (เช่น M3, C3, R3, G2)
ความปลอดภัยของศูนย์ข้อมูล *การจัดการสินทรัพย์*	DCS-01.1	คุณมีการเก็บรักษารายการสินทรัพย์สำคัญทั้งหมด และรวมถึงการเป็นเจ้าของสินทรัพย์หรือไม่	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 สินทรัพย์ด้านฮาร์ดแวร์ของ AWS จะถูกกำหนดเจ้าของ ติดตาม และตรวจสอบโดยบุคลากรของ AWS ด้วยการใช้เครื่องมือจัดการสินทรัพย์จดทะเบียนของ AWS ทีมงานด้านการจัดซื้อและห่วงโซ่อุปทานจะรับหน้าที่รักษาความสัมพันธ์กับผู้จัดจำหน่ายของ AWS ทั้งหมด โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 8 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	DCS-01.2	คุณมีการเก็บรักษารายการข้อมูลความสัมพันธ์ระหว่างผู้จัดจำหน่ายสำคัญทั้งหมดโดยสมบูรณ์หรือไม่	
ความปลอดภัยของศูนย์ข้อมูล *จุดเชื่อมต่อแบบควบคุม*	DCS-02.1	มีการใช้การรักษาความปลอดภัยทางกายภาพที่ส่วนนอกหรือไม่ (เช่น รั้ว กำแพง ตัวป้องกัน เจ้าหน้าที่รักษาความปลอดภัย ประตู การตรวจตราทางอิเล็กทรอนิกส์ ระบบกลไกการรับรองความถูกต้องเชิงกายภาพ แผนกต้อนรับ และ	มีการควบคุมการเข้าถึงทางกายภาพ แต่ไม่จำกัดเฉพาะการควบคุมส่วนนอก เช่น การกั้นรั้ว กำแพง การใช้เจ้าหน้าที่รักษาความปลอดภัย การตรวจตราทางกล้องวงจรปิด ระบบการตรวจหาการบุกรุก และวิธีการทางอิเล็กทรอนิกส์อื่นๆ รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติมเกี่ยวกับกิจกรรมการควบคุมเฉพาะที่ดำเนินการโดย AWS โปรดดูข้อมูลเพิ่มเติมได้ที่ มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 11 AWS ผ่านการตรวจสอบและรับรองโดย

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
		การจัดทีมลาดตระเวณความปลอดภัย)	ผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ความปลอดภัยของศูนย์ข้อมูล *การระบุอุปกรณ์*	DCS-03.1	มีการใช้การระบุอุปกรณ์ด้วยระบบอัตโนมัติ เพื่อเป็นวิธีการในการตรวจสอบการรับรองความถูกต้องการเชื่อมต่อ โดยอ้างอิงจากตำแหน่งที่ตั้งของอุปกรณ์ที่ทราบหรือไม่	AWS จัดการการระบุอุปกรณ์ให้สอดคล้องตามมาตรฐาน ISO 27001 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ความปลอดภัยของศูนย์ข้อมูล *การอนุญาตภายนอกไซต์*	DCS-04.1	คุณมอบเอกสารให้แก่ผู้เช่า ซึ่งอธิบายถึงสถานการณ์การใช้งานที่ข้อมูลอาจมีการย้ายจากที่ตั้งทางกายภาพหนึ่งไปยังอีกแห่งหนึ่งหรือไม่ (เช่น การสำรองข้อมูลภายนอกไซต์ การย้ายเมื่อเกิดข้อผิดพลาดเพื่อความต่อเนื่องของธุรกิจ และการทำซ้ำ)	ลูกค้าของ AWS สามารถกำหนดได้ว่าจะระบุข้อมูลของพวกเขาไว้ภายในภูมิภาคทางกายภาพใด AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าจากภูมิภาคที่ลูกค้าเลือกโดยไม่แจ้งให้ลูกค้าทราบ ยกเว้นจะได้รับการระบุให้ปฏิบัติตามกฎหมาย หรือมีการร้องขอจากหน่วยงานของรัฐ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
ความปลอดภัยของศูนย์ข้อมูล *อุปกรณ์ภายนอกไซต์*	DCS-05.1	คุณสามารถแสดงหลักฐานแก่ผู้เช่าเพื่อแสดงข้อมูลเกี่ยวกับนโยบายและขั้นตอนต่างๆ ที่ครอบคลุมการจัดการสินทรัพย์และการนำอุปกรณ์มาใช้งานใหม่ได้หรือไม่	เพื่อให้สอดคล้องตามมาตรฐาน ISO 27001 เมื่ออุปกรณ์เก็บข้อมูลสิ้นสุดอายุการใช้งาน การดำเนินการ AWS จะมีขั้นตอนในการปลดการทำงาน ซึ่งออกแบบมาเพื่อป้องกันไม่ให้ข้อมูลของลูกค้าถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาต AWS ใช้เทคนิคตามที่ระบุใน DoD 5220.22-M (“National Industrial Security Program Operating Manual”) หรือ NIST 800-88 (“Guidelines for Media Sanitization”) เพื่อทำลายข้อมูลอันเป็นส่วนหนึ่งของกระบวนการปลดการทำงาน หากไม่สามารถปลดการทำงานอุปกรณ์ฮาร์ดแวร์ได้ด้วยกระบวนการดังกล่าว อุปกรณ์จะถูกลบสภาพแม่เหล็กหรือทำลายทิ้งตามวิธีที่เป็นมาตรฐานอุตสาหกรรม โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 8 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ความปลอดภัยของศูนย์ข้อมูล *นโยบาย*	DCS-06.1	คุณสามารถแสดงหลักฐานได้หรือไม่ ว่าได้มีการกำหนดนโยบาย มาตรฐาน และกระบวนการเพื่อรักษาสภาพแวดล้อมการทำงานให้ปลอดภัยภายในสำนักงาน ห้อง สถานที่ และพื้นที่ปลอดภัย	AWS ร่วมมือกับหน่วยงานด้านการรับรองภายนอกและผู้ตรวจสอบอิสระ เพื่อทบทวนและตรวจสอบการปฏิบัติตามข้อกำหนดของกรอบงานการปฏิบัติตามของเรา รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติมเกี่ยวกับกิจกรรมด้านการควบคุมความปลอดภัยทางกายภาพที่ดำเนินการโดย AWS โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 11 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	DCS-06.2	คุณสามารถแสดงหลักฐานได้หรือไม่ ว่าบุคลากรของคุณและบุคลากรภายนอกที่มีส่วนเกี่ยวข้องนั้นได้รับการฝึกอบรมตามนโยบาย มาตรฐาน และกระบวนการที่คุณระบุ	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 พนักงานของ AWS ทุกคนต้องผ่านการฝึกอบรมความปลอดภัยด้านข้อมูลเป็นระยะๆ ซึ่งกำหนดให้มีการยอมรับเพื่อสำเร็จหลักสูตร นอกจากนี้ยังมีการตรวจสอบการปฏิบัติตามเป็นระยะ เพื่อรับรองว่าพนักงานมีความเข้าใจและปฏิบัติตามนโยบายที่กำหนดไว้ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับการรับรองมาตรฐาน ISO 27001 นอกจากนี้ รายงาน AWS SOC 1 และ SOC 2 จะแสดงรายละเอียดเพิ่มเติม
ความปลอดภัยของศูนย์ข้อมูล *การอนุญาตพื้นที่ปลอดภัย*	DCS-07.1	คุณยินยอมให้ผู้เช่าระบุตำแหน่งทางภูมิศาสตร์ ที่ข้อมูลของผู้เช่าสามารถเข้ามา/ออกไป ได้หรือไม่ (เพื่อรองรับกับการพิจารณาด้านขอบเขตอำนาจทางกฎหมาย โดยอ้างอิงจากตำแหน่งข้อมูลที่จัดเก็บเทียบกับ ตำแหน่งที่เข้าถึง)	ลูกค้าของ AWS เป็นผู้กำหนดว่าจะระบุข้อมูลของพวกเขาไว้ภายในภูมิภาคทางกายภาพใด AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าจากภูมิภาคที่ลูกค้าเลือกโดยไม่แจ้งให้ลูกค้าทราบ ยกเว้นจะได้รับการระบุให้ปฏิบัติตามกฎหมาย หรือมีการร้องขอจากหน่วยงานของรัฐ ณ เวลาที่เอกสารฉบับนี้จัดทำขึ้น AWS ประกอบด้วย 12 ภูมิภาค ได้แก่: สหรัฐอเมริกาฝั่งตะวันออก (เวอร์จิเนียตอนเหนือ), สหรัฐอเมริกาฝั่งตะวันตก (โอริกอน), สหรัฐอเมริกาฝั่งตะวันตก (แคลิฟอร์เนียตอนเหนือ), AWS GovCloud (สหรัฐอเมริกา) (โอริกอน), สหภาพยุโรป (ไอร์แลนด์), สหภาพยุโรป (แฟรงก์เฟิร์ต) , เอเชียแปซิฟิก (โซล), เอเชียแปซิฟิก (สิงคโปร์), เอเชียแปซิฟิก (โตเกียว), เอเชียแปซิฟิก (ซิดนีย์), จีน (ปักกิ่ง) และอเมริกาใต้ (เซาเปาโล)
ความปลอดภัยของศูนย์ข้อมูล *การเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต*	DCS-08.1	คุณมีการตรวจสอบ ควบคุม และแยกจุดสื่อสารขาเข้าและขาออก เช่น พื้นที่การบริการ และตำแหน่งอื่นๆ ที่ผู้ซึ่งไม่ได้รับอนุญาตสามารถเข้าถึงได้ออกจากพื้นที่จัดเก็บข้อมูลและกระบวนการหรือไม่	มีการควบคุมการเข้าถึงทางกายภาพอย่างเข้มงวด ทั้งส่วนนอกสุดและจุดทางเข้าของอาคาร ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะ การใช้เจ้าหน้าที่รักษาความปลอดภัยมืออาชีพที่ใช้การตรวจตราทางกล้องวงจรปิด ระบบการตรวจหาการบุกรุก และวิธีการทางอิเล็กทรอนิกส์อื่นๆ เจ้าหน้าที่ที่ได้รับอนุญาตจะต้องผ่านการตรวจสอบสองปัจจัยอย่างน้อยสองครั้ง จึงจะเข้าสู่ชั้นต่างๆ ของศูนย์ข้อมูลได้ จุดเชื่อมต่อทางกายภาพไปยังตำแหน่งของเซิร์ฟเวอร์มีการตรวจตราและบันทึกภาพโดยใช้กล้องวงจรปิด (CCTV) ตามที่ระบุไว้ภายในนโยบายด้านความปลอดภัยทางกายภาพของศูนย์ข้อมูล AWS ระบบกลไกด้านความปลอดภัยทางกายภาพของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอกระหว่างช่วงการตรวจสอบการปฏิบัติตามข้อกำหนดของ SOC, PCI DSS, ISO 27001 และ FedRAMP ของเรา
ความปลอดภัยของศูนย์ข้อมูล *การเข้าถึงของผู้ใช้*	DCS-09.1	คุณมีการจำกัดการเข้าถึงทางกายภาพไปยังสินทรัพย์ข้อมูลและฟังก์ชันตามผู้ใช้และบุคลากรสนับสนุนหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
การเข้ารหัสและการจัดการคีย์ *การให้สิทธิ์*	EKM-01.1	คุณมีนโยบายการจัดการคีย์ ที่ผูกคีย์เข้ากับเจ้าของที่สามารถระบุตัวตนได้หรือไม่	AWS มอบความสามารถให้ลูกค้าใช้ระบบกลไกการเข้ารหัสของตนเองสำหรับบริการแทบทุกประเภท รวมถึงการเข้ารหัสแบบ S3, EBS และ EC2 เซสชัน VPC ก็ได้รับการเข้ารหัสเช่นกัน นอกจากนี้ ลูกค้ายังสามารถใช้งาน AWS Key Management Systems (KMS) เพื่อสร้างและควบคุมคีย์การเข้ารหัส (ดูรายละเอียดที่ https://aws.amazon.com/kms/) สำหรับภายใน AWS วางรูปแบบและจัดการคีย์การเข้ารหัสสำหรับการเข้ารหัสที่จำเป็น ซึ่งใช้งานภายในโครงสร้างของ AWS คีย์ที่มีปลอดภัยซึ่งสร้างโดย AWS และตัวจัดการข้อมูลประจำตัวจะถูกใช้เพื่อสร้าง ป้องกัน และกระจายคีย์แบบสมมาตร และใช้เพื่อรักษาความปลอดภัยและกระจายสิ่งต่อไปนี้ ข้อมูลประจำตัวของ AWS ที่จำเป็นบนโฮสต์, คีย์สาธารณะ/ส่วนตัวของ RSA และการรับรอง X.509 กระบวนการเข้ารหัสของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอก เพื่อยืนยันความสอดคล้องตามข้อกำหนดของ SOC, PCI DSS, ISO 27001 และ FedRAMP
การเข้ารหัสและการจัดการคีย์ *การสร้างคีย์*	EKM-02.1	คุณมีความสามารถในการอนุญาตให้สร้างคีย์การเข้ารหัสเฉพาะสำหรับผู้เช่าแต่ละรายหรือไม่	AWS อนุญาตให้ลูกค้าใช้ระบบกลไกการเข้ารหัสของตนเองสำหรับบริการแทบทุกประเภท รวมถึงการเข้ารหัสแบบ S3, EBS และ EC2 ช่องทาง IPSec ไปยัง VPC ได้รับการเข้ารหัสเช่นกัน นอกจากนี้ ลูกค้ายังสามารถใช้งาน AWS Key Management Systems (KMS) เพื่อสร้างและควบคุมคีย์การเข้ารหัส (ดูรายละเอียดที่ https://aws.amazon.com/kms/) โปรดดูรายละเอียดเพิ่มเติมเกี่ยวกับ KMS จากรายงาน SOC ของ AWS นอกจากนี้ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security สำหรับภายใน AWS วางรูปแบบและจัดการคีย์การเข้ารหัสสำหรับการเข้ารหัสที่จำเป็น ซึ่งใช้งานภายในโครงสร้างของ AWS AWS สร้าง ควบคุม และแจกจ่ายคีย์การเข้ารหัสแบบสมมาตรโดยใช้เทคโนโลยีการจัดการคีย์ที่ผ่านการรับรองของ NIST และกระบวนการภายในระบบข้อมูลของ AWS คีย์ที่มีปลอดภัยซึ่งสร้างโดย AWS และตัวจัดการข้อมูลประจำตัวจะถูกใช้เพื่อสร้าง ป้องกัน และกระจายคีย์แบบสมมาตร และใช้เพื่อรักษาความปลอดภัยและกระจายสิ่งต่อไปนี้ ข้อมูลประจำตัวของ AWS ที่จำเป็นบนโฮสต์, คีย์สาธารณะ/ส่วนตัวของ RSA และการรับรอง X.509 กระบวนการเข้ารหัสของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอก เพื่อยืนยันความสอดคล้องตามข้อกำหนดของ SOC, PCI DSS, ISO 27001 และ FedRAMP
	EKM-02.2	คุณมีความสามารถในการจัดการคีย์การเข้ารหัสแทนผู้เช่าหรือไม่	
	EKM-02.3	คุณดูแลกระบวนการจัดการคีย์หรือไม่	
	EKM-02.4	คุณมีการบันทึกข้อมูลการเป็นเจ้าของสำหรับแต่ละช่วงระยะเวลาภายในวงจรของคีย์เข้ารหัสหรือไม่	
	EKM-02.5	คุณใช้เฟรมเวิร์กภายนอก/โอเพ่นซอร์ส/จดทะเบียน เพื่อจัดการคีย์การเข้ารหัสหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
การเข้ารหัสและการจัดการคีย์ *การเข้ารหัส*	EKM-03.1	คุณมีการเข้ารหัสข้อมูลผู้เช่าที่ไม่ได้ใช้งาน (บนดิสก์/พื้นที่จัดเก็บ) ภายในสภาพแวดล้อมหรือไม่	AWS อนุญาตให้ลูกค้าใช้ระบบกลไกการเข้ารหัสของตนเองสำหรับบริการแทบทุกประเภท รวมถึงการเข้ารหัสแบบ S3, EBS และ EC2 ช่องทาง IPSec ไปยัง VPC ได้รับการเข้ารหัสเช่นกัน นอกจากนี้ ลูกค้ายังสามารถใช้งาน AWS Key Management Systems (KMS) เพื่อสร้างและควบคุมคีย์การเข้ารหัส (ดูรายละเอียดที่ https://aws.amazon.com/kms/) โปรดดูรายละเอียดเพิ่มเติมเกี่ยวกับ KMS จากรายงาน SOC ของ AWS นอกจากนี้ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	EKM-03.2	คุณใช้การเข้ารหัสเพื่อป้องกันข้อมูลและอิมเมจของเครื่องเสมือนระหว่างการขนย้ายข้าม/ระหว่าง เครือข่ายและไฮเปอร์ไวเซอร์หรือไม่	
	EKM-03.3	คุณสนับสนุนคีย์การเข้ารหัสที่สร้างโดยผู้เช่า หรืออนุญาตให้ผู้เช่าทำการเข้ารหัสข้อมูลข้อมูลประจำตัวที่ไม่มีสิทธิ์การเข้าถึงการรับรองคีย์แบบสาธารณะหรือไม่ (เช่น การเข้ารหัสแบบอิงข้อมูลประจำตัว)	
	EKM-03.4	คุณมีเอกสารที่อธิบายและระบุรายละเอียดเกี่ยวกับนโยบายการจัดการ กระบวนการ และแนวทางการเข้ารหัสหรือไม่	
การเข้ารหัสและการจัดการคีย์ *พื้นที่จัดเก็บและการเข้าถึง*	EKM-04.1	คุณมีแพลตฟอร์มและการเข้ารหัสที่เหมาะสมกับข้อมูล ซึ่งใช้รูปแบบเปิด/ได้รับการตรวจสอบและใช้อัลกอริธึมแบบมาตรฐานหรือไม่	AWS อนุญาตให้ลูกค้าใช้ระบบกลไกการเข้ารหัสของตนเองสำหรับบริการแทบทุกประเภท รวมถึงการเข้ารหัสแบบ S3, EBS และ EC2 นอกจากนี้ ลูกค้ายังสามารถใช้งาน AWS Key Management Systems (KMS) เพื่อสร้างและควบคุมคีย์การเข้ารหัส (ดูรายละเอียดที่ https://aws.amazon.com/kms/) โปรดดูรายละเอียดเพิ่มเติมเกี่ยวกับ KMS จากรายงาน SOC ของ AWS AWS วางรูปแบบและจัดการคีย์การเข้ารหัสสำหรับการเข้ารหัสที่จำเป็น ซึ่งใช้งานภายในโครงสร้างของ AWS AWS สร้าง ควบคุม และแจกจ่ายคีย์การเข้ารหัสแบบสมมาตรโดยใช้เทคโนโลยีการจัดการคีย์ที่ผ่านการรับรองของ NIST และกระบวนการภายในระบบข้อมูลของ AWS คีย์ที่มีปลอดภัยซึ่งสร้างโดย AWS และตัวจัดการข้อมูลประจำตัวจะถูกใช้เพื่อสร้าง ป้องกัน และกระจายคีย์แบบสมมาตร และใช้เพื่อรักษาความปลอดภัยและกระจายสิ่งต่อไปนี้ ข้อมูลประจำตัวของ AWS ที่จำเป็นบนโฮสต์, คีย์สาธารณะ/ส่วนตัวของ RSA และการรับรอง X.509 กระบวนการเข้ารหัสของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอก เพื่อยืนยันความสอดคล้องตามข้อกำหนดของ SOC, PCI DSS, ISO 27001 และ FedRAMP
	EKM-04.2	คีย์การเข้ารหัสได้รับการดูแลโดยผู้ใช้งานคลาวด์ หรือโดยผู้ให้บริการด้านการจัดการคีย์ที่น่าเชื่อถือหรือไม่	
	EKM-04.3	คุณจัดเก็บคีย์การเข้ารหัสไว้บนระบบคลาวด์หรือไม่	
	EKM-04.4	คุณมีการจัดการคีย์และหน้าที่การใช้งานคีย์แยกกันหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
การกำกับดูแลและการจัดการความเสี่ยง *ข้อกำหนดพื้นฐาน*	GRM-01.1	คุณมีการบันทึกข้อมูลพื้นฐานด้านความปลอดภัยสำหรับทุกองค์ประกอบภายในโครงสร้างพื้นฐานหรือไม่ (เช่น ไฮเปอร์ไวเซอร์ ระบบปฏิบัติการ เราเตอร์ เซิร์ฟเวอร์ DNS ฯลฯ)	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 AWS มีการดูแลบรรทัดฐานด้านระบบสำหรับส่วนประกอบที่มีความสำคัญ โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 14 และ 18 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001 ลูกค้าสามารถใช้งานอิมเมจเครื่องเสมือนของตนเองได้ VM Import ช่วยให้ลูกค้าสามารถนำเข้าอิมเมจเครื่องเสมือนจากสภาพแวดล้อมเดิมของลูกค้าไปยังอินสแตนซ์ของ Amazon EC2 ได้โดยง่าย
	GRM-01.2	คุณมีความสามารถในการตรวจสอบและรายงานสถานะการปฏิบัติตามข้อกำหนดของโครงสร้างพื้นฐานตามบรรทัดฐานด้านความปลอดภัยข้อมูลได้อย่างต่อเนื่องหรือไม่	
	GRM-01.3	คุณอนุญาตให้ผู้ใช้งานใช้อิมเมจเครื่องเสมือนที่น่าเชื่อถือของตนเอง เพื่อยืนยันความสอดคล้องกับมาตรฐานภายในของผู้ใช้งานหรือไม่	
การกำกับดูแลและการจัดการความเสี่ยง *การประเมินความเสี่ยง*	GRM-02.1	คุณมอบข้อมูลสภาพการควบคุมความปลอดภัยให้กับผู้เช่าเพื่อให้ผู้เช่าใช้การตรวจสอบอย่างต่อเนื่องตามมาตรฐานอุตสาหกรรมหรือไม่ (ซึ่งช่วยให้เกิดการตรวจสอบอย่างต่อเนื่องโดยผู้เช่าถึงสถานะการควบคุมทั้งแบบกายภาพและแบบลอจิคัล)	AWS มีการเผยแพร่รายงานของผู้ตรวจสอบอิสระและการรับรองต่างๆ เพื่อมอบข้อมูลให้กับลูกค้าเกี่ยวกับนโยบาย กระบวนการ และการควบคุมที่วางแผนและดำเนินงานโดย AWS การรับรองและรายงานที่เกี่ยวข้องสามารถมอบให้กับลูกค้าของ AWS ได้ การตรวจสอบแบบต่อเนื่องสำหรับการควบคุมแบบลอจิคัลสามารถดำเนินการได้เองโดยลูกค้าบนระบบของลูกค้าเอง
	GRM-02.2	คุณมีการประเมินความเสี่ยงที่เกี่ยวข้องกับข้อกำหนดด้านการกำกับดูแลข้อมูลอย่างน้อยปีละหนึ่งครั้งหรือไม่	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 ทาง AWS มีโปรแกรมประเมินความเสี่ยงเพื่อลดโอกาสและจัดการความเสี่ยง นอกจากนี้ AWS ยังได้รับการรับรองตามมาตรฐาน ISO 27018 ความสอดคล้องกับมาตรฐาน ISO 27018 เป็นหลักฐานที่แสดงให้ลูกค้าเห็นว่า AWS มีระบบการควบคุมสำหรับรองรับด้านการป้องกันความเป็นส่วนตัวของเนื้อหาลูกค้า สำหรับข้อมูลเพิ่มเติม โปรดดูที่คำถามที่พบบ่อยเกี่ยวกับการปฏิบัติตาม ISO 27018 ของ AWS ที่ http://aws.amazon.com/compliance/iso-27018-faqs/
การกำกับดูแลและการจัดการความเสี่ยง *การเฝ้าติดตามการจัดการ*	GRM-03.1	ผู้จัดการฝ่ายเทคนิค ฝ่ายธุรกิจ และฝ่ายบริหารของคุณมีหน้าที่รับผิดชอบในด้านการรับรู้และปฏิบัติตามนโยบายด้านความปลอดภัย กระบวนการ และมาตรฐานต่างๆ ทั้งสำหรับตนเองและบุคลากรของตนตามที่เกี่ยวข้องกับขอบเขตความรับผิดชอบของผู้จัดการ	สภาพแวดล้อมการควบคุมที่ Amazon เริ่มต้นที่ระดับสูงสุดภายในองค์กร ผู้บริหารและผู้มีอำนาจระดับสูงมีบทบาทสำคัญในการวางรากฐานสำหรับคุณค่าหลักและแนวทางของบริษัท พนักงานทุกคนจะได้รับทราบเกี่ยวกับหลักปฏิบัติทางธุรกิจและหลักจริยธรรมของบริษัท และต้องผ่านการฝึกอบรมเป็นระยะ นอกจากนี้ยังมีการตรวจสอบการปฏิบัติตามเพื่อให้พนักงานมีความเข้าใจและปฏิบัติตามนโยบายที่กำหนดไว้ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความเสี่ยงและ

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
		และพนักงานหรือไม่	การปฏิบัติตามข้อกำหนดของ AWS ที่ http://aws.amazon.com/compliance
การกำกับดูแลและการจัดการความเสี่ยง *โปรแกรมการจัดการ*	GRM-04.1	คุณมอบเอกสารซึ่งอธิบายเกี่ยวกับโปรแกรมการจัดการความปลอดภัยทางข้อมูล (ISMP) ให้แก่ผู้เช่าหรือไม่	AWS มอบการรับรอง ISO 27001 ของเราให้กับลูกค้า การรับรอง ISO 27001 เน้นย้ำในด้าน ISMS ของ AWS โดยเฉพาะ และเป็นตัวชี้วัดว่ากระบวนการภายในของ AWS ปฏิบัติตามมาตรฐาน ISO อย่างไร การรับรองดังกล่าวหมายความว่า ผู้ตรวจสอบอิสระภายนอกที่ได้รับการแต่งตั้งได้ประเมินกระบวนการและการควบคุมของเรา และรับรองว่ามีความสอดคล้องตามมาตรฐานการรับรองของ ISO 27001 สำหรับข้อมูลเพิ่มเติม โปรดดูที่เว็บไซต์ คำถามที่พบบ่อยเกี่ยวกับการปฏิบัติตามมาตรฐาน ISO 27001 ของ AWS ที่ http://aws.amazon.com/compliance/iso-27001-faqs/
	GRM-04.2	คุณมีการตรวจสอบโปรแกรมการจัดการความปลอดภัยทางข้อมูล (ISMP) อย่างน้อยปีละหนึ่งครั้งหรือไม่	
การกำกับดูแลและการจัดการความเสี่ยง *การสนับสนุนการจัดการ / การมีส่วนร่วม*	GRM-05.1	คุณรับรองได้หรือไม่ว่าผู้ให้บริการของคุณปฏิบัติตามนโยบายด้านความเป็นส่วนตัวและความปลอดภัยข้อมูล	AWS วางกรอบงานและนโยบายด้านความปลอดภัยของข้อมูล ซึ่งรวบรวมกรอบงานที่มีการรับรองของ ISO 27001 โดยอ้างอิงจากการควบคุมตาม ISO 27002, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 และ National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems) AWS จัดการความสัมพันธ์กับภายนอกให้สอดคล้องตามมาตรฐาน ISO 27001 ข้อกำหนดสำหรับบริษัทภายนอกของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอกระหว่างช่วงการตรวจสอบการปฏิบัติตามมาตรฐาน PCI DSS, ISO 27001 และ FedRAMP ข้อมูลเกี่ยวกับโปรแกรมการปฏิบัติตามข้อกำหนดของ AWS มีการเผยแพร่แก่สาธารณะบนเว็บไซต์ของเราที่ http://aws.amazon.com/compliance/
การกำกับดูแลและการจัดการความเสี่ยง *นโยบาย*	GRM-06.1	นโยบายด้านความเป็นส่วนตัวและความปลอดภัยข้อมูลสอดคล้องกับมาตรฐานของอุตสาหกรรมหรือไม่ (ISO-27001, ISO-22307, CoBIT ฯลฯ)	
	GRM-06.2	คุณมีข้อตกลงเพื่อรับประกันว่าผู้ให้บริการของคุณจะปฏิบัติตามนโยบายด้านความเป็นส่วนตัวและความปลอดภัยข้อมูลหรือไม่	
	GRM-06.3	คุณสามารถแสดงหลักฐานการเชื่อมโยงการตรวจสอบ วิเคราะห์สถานะการควบคุม สถาปัตยกรรม และกระบวนการของคุณตามระเบียบข้อบังคับ และ/หรือมาตรฐานได้หรือไม่	
	GRM-06.4	คุณมีการเปิดเผยข้อมูลหรือไม่ว่าบริษัทของคุณปฏิบัติตามระเบียบข้อบังคับ มาตรฐาน และ/หรือการควบคุมใดบ้าง	
การกำกับดูแลและการจัดการความเสี่ยง *การบังคับใช้*	GRM-07.1	มีข้อกำหนดทางวินัยอย่างเป็นทางการ หรือนโยบายการลงโทษสำหรับพนักงานที่ละเมิดนโยบายและกระบวนการด้านความปลอดภัยหรือไม่	AWS มีนโยบายด้านความปลอดภัยและจัดให้มีการฝึกอบรมด้านความปลอดภัยแก่พนักงาน เพื่อให้พนักงานมีความรู้ในด้านความปลอดภัยข้อมูลเหมาะสมกับบทบาทและหน้าที่ความรับผิดชอบของตนเอง พนักงานที่ละเมิดมาตรฐานหรือขั้นตอนของ Amazon จะถูก

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
นโยบาย	GRM-07.2	พนักงานของคุณทราบหรือไม่ว่าสามารถดำเนินการใดได้บ้างหากเกิดกรณีที่มีการละเมิดจากนโยบายและขั้นตอนของพวกเขา	ตรวจสอบและดำเนินการทางวินัยอย่างเหมาะสมตามมา (เช่น ตักเตือน ลงโทษทางพฤติกรรม พักงาน และ/หรือให้ออกจากงาน) โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security โปรดดู ISO 27001 ภาคผนวก A ส่วนที่ 7 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
การกำกับดูแลและการจัดการความเสี่ยง *ผลกระทบด้านการเปลี่ยนแปลงนโยบาย / ธุรกิจ*	GRM-08.1	มีการปรับปรุงนโยบายด้านความปลอดภัย ขั้นตอน มาตรฐาน และการควบคุมภายในผลลัพธ์การประเมินความเสี่ยง เพื่อรับประกันว่าข้อมูลเหล่านี้มีความเกี่ยวข้องและมีประสิทธิภาพหรือไม่	มีการปรับปรุงนโยบายด้านความปลอดภัยของ AWS กระบวนการ มาตรฐาน และการควบคุมเป็นประจำทุกปี เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 โปรดดูข้อมูลเพิ่มเติมได้จากหัวข้อ ISO 27001 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับการรับรองมาตรฐาน ISO 27001
การกำกับดูแลและการจัดการความเสี่ยง *การตรวจสอบนโยบาย*	GRM-09.1	คุณได้มีการแจ้งให้ผู้เช่าทราบหรือไม่ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญภายในนโยบายด้านความเป็นส่วนตัวและ/หรือความปลอดภัยข้อมูล	เอกสารความปลอดภัย AWS Cloud และเอกสารความเสี่ยงและการปฏิบัติตามข้อกำหนดของเรา ซึ่งดูได้ที่ http://aws.amazon.com/security และ http://aws.amazon.com/compliance ได้รับการปรับปรุงอยู่เสมอเพื่อสะท้อนให้เห็นถึงการเปลี่ยนแปลงในนโยบายของ AWS
	GRM-09.2	คุณมีการตรวจสอบนโยบายด้านความเป็นส่วนตัวและความปลอดภัยอย่างน้อยที่สุดปีละหนึ่งครั้งหรือไม่	รายงาน AWS SOC แสดงรายละเอียดที่เกี่ยวข้องกับการตรวจสอบนโยบายด้านความเป็นส่วนตัวและความปลอดภัย
การกำกับดูแลและการจัดการความเสี่ยง *การประเมินผล*	GRM-10.1	มีการประเมินความเสี่ยงอย่างเป็นทางการเพื่อให้สอดคล้องกับกรอบงานระดับองค์กร และมีการดำเนินการอย่างน้อยปีละหนึ่งครั้งหรือตามระยะเวลาที่กำหนด เพื่อระบุความเป็นไปได้และผลกระทบของความเสี่ยงที่ระบุทั้งหมด โดยใช้กระบวนการเชิงปริมาณและเชิงคุณภาพหรือไม่	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 ทาง AWS ได้กำหนดโปรแกรมประเมินความเสี่ยงเพื่อลดโอกาสและจัดการความเสี่ยง AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับการรับรองมาตรฐาน ISO 27001 โปรดดูเอกสารความเสี่ยงและการปฏิบัติตามข้อกำหนดของ AWS (ดูที่ aws.amazon.com/security) สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับกรอบงานการจัดการความเสี่ยงของ AWS
	GRM-10.2	มีการระบุความเป็นไปได้และผลกระทบที่เกี่ยวข้องกับความเสี่ยงสืบเนื่องและความเสี่ยงส่วนที่เหลือแบบแยกอิสระ โดยพิจารณาหมวดหมู่ความเสี่ยงทั้งหมดหรือไม่ (เช่น ผลลัพธ์การตรวจสอบ การวิเคราะห์ภัยคุกคามและช่องโหว่ และการปฏิบัติตามระเบียบข้อบังคับ)	
การกำกับดูแลและการจัดการ	GRM-	คุณมีโปรแกรมที่บันทึกเป็นเอกสาร ซึ่งครอบคลุมทั้งองค์กร	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 ทาง AWS มีโปรแกรมประเมินความเสี่ยงเพื่อลดโอกาสและจัดการ

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ความเสี่ยง *โปรแกรม*	11.1	เพื่อการจัดการกับความเสี่ยงหรือไม่	ความเสี่ยง การจัดการของ AWS มีแผนการธุรกิจเชิงกลยุทธ์ ซึ่งประกอบด้วยการระบุความเสี่ยงและการปรับใช้การควบคุมเพื่อลดและจัดการกับความเสี่ยง ฝ่ายบริหารของ AWS จะประเมินแผนธุรกิจเชิงกลยุทธ์ซ้ำอย่างน้อยปีละสองครั้ง กระบวนการดังกล่าวกำหนดให้การจัดการระบุความเสี่ยงต่างๆ ภายในขอบเขตความรับผิดชอบของตนเอง และใช้มาตรการที่เหมาะสมซึ่งออกแบบมาเพื่อรับมือกับความเสี่ยงเหล่านั้น โปรแกรมการจัดการความเสี่ยงของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอกระหว่างช่วงการตรวจสอบการปฏิบัติตามมาตรฐาน PCI DSS, ISO 27001 และ FedRAMP
	GRM-11.2	คุณเผยแพร่ข้อมูลของโปรแกรมการจัดการกับความเสี่ยงแบบครอบคลุมทั้งองค์กรหรือไม่	
ทรัพยากรบุคคล *การคืนสินทรัพย์*	HRS-01.1	มีการวางระบบเพื่อตรวจสอบการละเมิดความเป็นส่วนตัว พร้อมทั้งแจ้งผู้เช่าโดยทันทีหรือไม่ หากเหตุการณ์การละเมิดความเป็นส่วนตัวนั้นอาจส่งผลต่อข้อมูลของผู้เช่า	ลูกค้าของ AWS เป็นผู้รับผิดชอบการตรวจสอบสภาพแวดล้อมของตนเองสำหรับการละเมิดความเป็นส่วนตัว รายงาน AWS SOC แสดงภาพรวมของการควบคุมที่มีเพื่อตรวจสอบสภาพแวดล้อมที่จัดการโดย AWS
	HRS-01.2	นโยบายด้านความเป็นส่วนตัวของคุณสอดคล้องกับมาตรฐานของอุตสาหกรรมหรือไม่	
ทรัพยากรบุคคล *การตรวจสอบภูมิหลัง*	HRS-02.1	ตามกฎหมายท้องถิ่น ระเบียบข้อบังคับ หลักจริยธรรม และข้อจำกัดทางสัญญา คุณมีการตรวจสอบภูมิหลังของผู้สมัครเป็นพนักงาน คู่สัญญา และบริษัทภายนอกที่เกี่ยวข้องหรือไม่	AWS จะดำเนินการตรวจสอบภูมิหลังทางอาชญากรรมตามที่กฎหมายอนุญาต ในฐานะกระบวนการหนึ่งของแนวทางการคัดกรองพนักงานก่อนการจ้างงานที่สอดคล้องกับตำแหน่งและระดับสิทธิ์เข้าถึงของพนักงานสำหรับสถานที่ของ AWS รายงาน AWS SOC แสดงรายละเอียดเพิ่มเติมเกี่ยวกับการควบคุมต่างๆ ที่มีการนำมาใช้กับการตรวจสอบภูมิหลัง
ทรัพยากรบุคคล *ข้อตกลงการจ้างงาน*	HRS-03.1	คุณฝึกอบรมพนักงานโดยเฉพาะ ตามบทบาทและการควบคุมความปลอดภัยข้อมูลที่พนักงานแต่ละคนได้รับหน้าที่หรือไม่	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 พนักงานของ AWS ทุกคนจะต้องผ่านการฝึกอบรมตามบทบาทของตนเองเป็นระยะ ซึ่งรวมถึงการฝึกอบรมความปลอดภัยของ AWS และกำหนดให้มีการยอมรับเพื่อสำเร็จหลักสูตร นอกจากนี้ยังมีการตรวจสอบการปฏิบัติตามเป็นระยะ เพื่อรับรองว่าพนักงานมีความเข้าใจและปฏิบัติตามนโยบายที่กำหนดไว้ โปรดดูรายละเอียดเพิ่มเติมจากรายงาน SOC พนักงานทุกคนที่ทำงานสนับสนุนระบบและอุปกรณ์ AWS จะต้องลงชื่อในเอกสารข้อตกลงที่จะไม่เปิดเผยข้อมูลก่อนได้รับสิทธิ์การเข้าถึง นอกจากนี้ เมื่อได้รับการว่าจ้างแล้ว พนักงานจะต้องอ่านและยอมรับนโยบายการใช้งานที่ยอมรับได้และนโยบายหลักปฏิบัติทางธุรกิจและหลักจริยธรรม (หลักปฏิบัติ) ของ AWS
	HRS-03.2	คุณจัดทำเอกสารการรับรู้ของพนักงานเกี่ยวกับการฝึกอบรมที่พนักงานได้รับหรือไม่	
	HRS-03.3	บุคลากรทุกรายของคุณจำเป็นต้องลงนามในเอกสารข้อตกลงที่จะไม่เปิดเผยข้อมูล (NDA) หรือข้อตกลงรักษาความลับ โดยเป็นเงื่อนไขของการว่าจ้างเพื่อป้องกันข้อมูลของลูกค้า/ผู้เช่าหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	HRS-03.4	การประสบผลสำเร็จและการเสร็จสิ้นโปรแกรมฝึกอบรมภายในระยะเวลาที่กำหนด เป็นเงื่อนไขเบื้องต้นสำหรับการได้รับและครอบครองสิทธิ์การเข้าถึงระบบที่มีความอ่อนไหวหรือไม่	
	HRS-03.5	บุคลากรของคุณได้รับการฝึกอบรมและรับทราบเกี่ยวกับโปรแกรมการรับรู้อย่างน้อยปีละหนึ่งครั้งหรือไม่	
ทรัพยากรบุคคล *การยกเลิกการจ้างงาน*	HRS-04.1	คุณมีเอกสารนโยบาย ขั้นตอน และแนวทางปฏิบัติเพื่อกำกับดูแลการเปลี่ยนแปลงที่เกี่ยวข้องกับการจ้างงานและ/หรือการยกเลิกการจ้างงานหรือไม่	ทีมทรัพยากรบุคคลของ AWS จะระบุความรับผิดชอบของการจัดการภายในเพื่อให้มีการดำเนินการตามสำหรับการยกเลิกการจ้างงานและการเปลี่ยนบทบาทหน้าที่ของพนักงานและผู้จำหน่าย รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติม
	HRS-04.2	ขั้นตอนและแนวทางปฏิบัติด้านบนครอบคลุมถึงการยกเลิกการเข้าถึงและการส่งคืนสินทรัพย์อย่างทันท่วงทีหรือไม่	สิทธิ์เข้าถึงจะถูกยกเลิกโดยอัตโนมัติเมื่อบันทึกข้อมูลพนักงานถูกยกเลิกในระบบทรัพยากรบุคคลของ Amazon ด้วยเช่นกัน เมื่อมีการเปลี่ยนแปลงหน้าที่ในงานของพนักงานเกิดขึ้น จะต้องมีการอนุมัติสิทธิ์เข้าถึงที่ต่อเนื่องให้กับทรัพยากร ไม่เช่นนั้นจะถูกยกเลิกโดยอัตโนมัติ รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติมเกี่ยวกับการยกเลิกการเข้าถึงของผู้ใช้ นอกจากนี้ คุณสามารถดูรายละเอียดเพิ่มเติมได้จากเอกสารความปลอดภัยของ AWS ในส่วน “วงจรการทำงานของพนักงาน” โปรดดู ISO 27001 ภาคผนวก A ส่วนที่ 7 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ทรัพยากรบุคคล *อุปกรณ์พกพา / เคลื่อนที่*	HRS-05.1	มีการกำหนดนโยบายและขั้นตอน ตลอดจนมาตรการอันเข้มงวด เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญของคุณและผู้เช่าผ่านทางอุปกรณ์พกพาและอุปกรณ์เคลื่อนที่หรือไม่ (เช่น แล็ปท็อป โทรศัพท์มือถือ และอุปกรณ์ผู้ช่วยดิจิทัลส่วนบุคคล (PDA)) ซึ่งโดยทั่วไปอุปกรณ์เหล่านี้มีความเสี่ยงสูงกว่าอุปกรณ์ที่ไม่ใช่แบบพกพา (เช่น คอมพิวเตอร์เดสก์ท็อปภายในสถานที่ทำงานขององค์กรผู้ให้บริการ)	ลูกค้ายังคงเป็นผู้ควบคุมและมีหน้าที่รับผิดชอบข้อมูลของตนเอง รวมถึงสินทรัพย์ประเภทสื่อที่เกี่ยวข้อง ดังนั้นจึงเป็นหน้าที่ของลูกค้าในการจัดการความปลอดภัยอุปกรณ์เคลื่อนที่ และการเข้าถึงเนื้อหาของลูกค้า

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ทรัพยากรบุคคล *ข้อตกลงที่จะไม่เปิดเผยข้อมูล*	HRS-06.1	ข้อกำหนดด้านการไม่เปิดเผยข้อมูล หรือข้อตกลงรักษาความลับ ซึ่งสะท้อนให้เห็นความจำเป็นขององค์กรในการปกป้องข้อมูลและรายละเอียดเชิงปฏิบัติการ มีการระบุไว้ จัดทำเป็นเอกสาร และมีการตรวจสอบเป็นระยะหรือไม่	ฝ่ายปรึกษาด้านกฎหมายของ Amazon มีหน้าที่จัดการและตรวจสอบแก้ไขข้อตกลง NDA ของ Amazon เป็นระยะเพื่อสะท้อนให้เห็นถึงความจำเป็นทางธุรกิจของ AWS
ทรัพยากรบุคคล *บทบาท / ความรับผิดชอบ*	HRS-07.1	คุณมอบเอกสารระบุบทบาทให้กับผู้เช่า ซึ่งชี้แจงถึงความรับผิดชอบด้านการจัดการดูแลเทียบกับของผู้เช่าหรือไม่	เอกสารความปลอดภัยของ AWS Cloud และเอกสารความเสี่ยงและการปฏิบัติตามข้อกำหนดของ AWS จะแสดงรายละเอียดเกี่ยวกับบทบาทและความรับผิดชอบของ AWS และความรับผิดชอบของลูกค้า คุณสามารถดูเอกสารได้ที่ http://aws.amazon.com/security และ http://aws.amazon.com/compliance
ทรัพยากรบุคคล *การใช้งานที่ยอมรับได้*	HRS-08.1	คุณมอบเอกสารที่อธิบายถึงวิธีการที่คุณอาจเข้าถึงข้อมูลและข้อมูลเมตาของผู้เช่าหรือไม่	AWS มีนโยบายควบคุมการเข้าถึงอย่างเป็นทางการ นโยบายดังกล่าวผ่านการตรวจสอบและปรับปรุงทุกปี (หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญภายในระบบ ซึ่งส่งผลกระทบต่อนโยบายดังกล่าว) นโยบายนี้ครอบคลุมหัวข้อเกี่ยวกับวัตถุประสงค์ ขอบเขต บทบาท ความรับผิดชอบ และข้อผูกมัดด้านการจัดการ AWS ใช้แนวคิดของการให้สิทธิ์การใช้งานระดับต่ำสุด และมีการมอบการเข้าถึงเฉพาะที่จำเป็นสำหรับผู้ใช้เพื่อปฏิบัติงานตามหน้าที่ของตนเองเท่านั้น ลูกค้ายังคงเป็นผู้ควบคุมและมีหน้าที่รับผิดชอบข้อมูลของตนเอง รวมถึงสินทรัพย์ประเภทสื่อที่เกี่ยวข้อง ดังนั้นจึงเป็นหน้าที่ของลูกค้าในการจัดการความปลอดภัยอุปกรณ์เคลื่อนที่ และการเข้าถึงเนื้อหาของลูกค้า โปรดดูหลักปฏิบัติของมาตรฐาน ISO 27001 และ 27018 สำหรับข้อมูลเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับการรับรองมาตรฐาน ISO 27001 และ ISO 27018
	HRS-08.2	คุณมีการรวบรวมหรือสร้างข้อมูลเมตาเกี่ยวกับการใช้งานข้อมูลของผู้เช่าผ่านการใช้เทคโนโลยีการตรวจสอบหรือไม่ (เช่น โปรแกรมค้นหา ฯลฯ)	
	HRS-08.3	คุณอนุญาตให้ผู้เช่าเลือกไม่ยินยอมให้มีการเข้าถึงข้อมูล/ข้อมูลเมตาผ่านการใช้เทคโนโลยีการตรวจสอบหรือไม่	
ทรัพยากรบุคคล *การฝึกอบรม / การรับรู้*	HRS-09.1	คุณจัดให้มีโปรแกรมฝึกอบรมการรับรู้ด้านความปลอดภัยอย่างเป็นทางการซึ่งจำแนกตามบทบาท สำหรับการเข้าถึงและการจัดการข้อมูลที่เกี่ยวข้องกับระบบคลาวด์ สำหรับพนักงานทุกคนที่มีสิทธิ์เข้าถึงข้อมูลผู้เช่าหรือไม่ (เช่น ระบบผู้เช่าหลายราย, สัญชาติ, โมเดลการให้บริการคลาวด์ที่แยกปัญหาด้านการทำงาน และผลประโยชน์ทับซ้อน)	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 พนักงานของ AWS ทุกคนต้องผ่านการฝึกอบรมความปลอดภัยด้านข้อมูลเป็นระยะๆ ซึ่งกำหนดให้มีการยอมรับเพื่อสำเร็จหลักสูตร นอกจากนี้ยังมีการตรวจสอบการปฏิบัติตามเป็นระยะ เพื่อรับรองว่าพนักงานมีความเข้าใจและปฏิบัติตามนโยบายที่กำหนดไว้ บทบาทและความรับผิดชอบของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอกระหว่างช่วงการตรวจสอบการปฏิบัติตามมาตรฐาน SOC, PCI DSS, ISO 27001 และ FedRAMP ของเรา

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	HRS-09.2	ผู้ดูแลระบบและผู้ดูแลข้อมูลผ่านการฝึกอบรมอย่างเหมาะสมในหัวข้อความรับผิดชอบทางด้านกฎหมาย ซึ่งเกี่ยวข้องกับความปลอดภัยและความถูกต้องของข้อมูลหรือไม่	
ทรัพยากรบุคคล *ความรับผิดชอบของผู้ใช้*	HRS-10.1	มีการแจ้งให้ผู้ใช้ทราบถึงความรับผิดชอบของพวกเขา ในการรับรู้และปฏิบัติตามนโยบายด้านความปลอดภัยที่เผยแพร่ ขั้นตอน มาตรฐาน และข้อกำหนดด้านระเบียบข้อบังคับที่ใช้งานหรือไม่	AWS ใช้วิธีการสื่อสารภายในที่หลากหลายวิธีในระดับโลก เพื่อช่วยให้พนักงานเข้าใจบทบาทและความรับผิดชอบของแต่ละบุคคล และเพื่อแจ้งให้ทราบถึงเหตุการณ์สำคัญอย่างทันท่วงที วิธีการดังกล่าวรวมถึงการกำหนดทิศทางและโปรแกรมการฝึกอบรมสำหรับพนักงานใหม่ ตลอดจนข้อความอีเมล และการแจ้งข้อมูลผ่านระบบอินทราเน็ตของ Amazon โปรดดูมาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 7 และ 8 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001 นอกจากนี้ คุณยังสามารถดูรายละเอียดเพิ่มเติมได้จากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	HRS-10.2	มีการแจ้งให้ผู้ใช้รับทราบถึงความรับผิดชอบในการดูแลสภาพแวดล้อมการทำงานให้มีความปลอดภัยหรือไม่	
	HRS-10.3	มีการแจ้งให้ผู้ใช้รับทราบถึงความรับผิดชอบในการดูแลอุปกรณ์ที่ไม่ได้ใช้งานในรูปแบบที่ปลอดภัยหรือไม่	
ทรัพยากรบุคคล *Workspace*	HRS-11.1	นโยบายและขั้นตอนการจัดการข้อมูลของคุณครอบคลุมผลประโยชน์ที่ขัดกันของผู้เช่าและระดับการบริการหรือไม่	นโยบายการจัดการข้อมูลของ AWS สอดคล้องกับมาตรฐาน ISO 27001 โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 8 และ 9 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001 รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติมเกี่ยวกับกิจกรรมการควบคุมเฉพาะที่ดำเนินการโดย AWS เพื่อป้องกันการเข้าถึงทรัพยากรของ AWS โดยไม่ได้รับอนุญาต AWS มีการระบุหมวดหมู่ของเหตุการณ์ที่สามารถตรวจสอบได้สำหรับระบบและอุปกรณ์ทั้งหมดภายในระบบของ AWS ทีมการให้บริการจะกำหนดค่าคุณลักษณะการตรวจสอบเพื่อบันทึกเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยอย่างต่อเนื่อง เพื่อให้สอดคล้องกับข้อกำหนด บันทึกข้อมูลการตรวจสอบประกอบด้วยชุดขององค์ประกอบข้อมูล เพื่อสนับสนุนข้อกำหนดด้านการวิเคราะห์ที่จำเป็น นอกจากนี้ บันทึกข้อมูลการตรวจสอบยังสามารถใช้งานได้โดยทีมความปลอดภัยของ AWS หรือทีมอื่นๆ ที่เหมาะสมเพื่อใช้ทำการตรวจสอบหรือวิเคราะห์ได้ตามต้องการ หรือเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยหรือส่งผลต่อธุรกิจ
	HRS-11.2	นโยบายและขั้นตอนการจัดการข้อมูลของคุณมีการตรวจสอบการแก้ไข หรือฟังก์ชันความถูกต้องของซอฟต์แวร์สำหรับการเข้าถึงข้อมูลผู้เช่าโดยไม่ได้รับอนุญาตหรือไม่	
	HRS-11.3	โครงสร้างพื้นฐานการจัดการเครื่องเสมือนประกอบด้วยการตรวจสอบการแก้ไขหรือฟังก์ชันตรวจสอบความถูกต้องซอฟต์แวร์ เพื่อตรวจหาการเปลี่ยนแปลงที่กระทำกับรุ่น/การกำหนดค่าของเครื่องเสมือนหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การเข้าถึงเครื่องมือการตรวจสอบ*	IAM-01.1	คุณมีการจำกัด เก็บบันทึก และตรวจสอบการเข้าถึงระบบการจัดการความปลอดภัยข้อมูลหรือไม่ (เช่น ไฮเปอร์ไวเซอร์, ไฟร์วอลล์, ตัวสแกนหาช่องโหว่, ตัวดักจับเครือข่าย, API, ฯลฯ)	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 AWS ได้สร้างนโยบายและขั้นตอนแบบเป็นทางการ เพื่อร่างมาตรฐานขั้นต่ำสำหรับการเข้าถึงทรัพยากรของ AWS รายงาน AWS SOC จะสรุปการควบคุมที่มีเพื่อบริหารการจัดเตรียมการเข้าถึงทรัพยากรของ AWS โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	IAM-01.2	คุณมีการตรวจสอบและบันทึกการเข้าถึงที่ได้รับสิทธิพิเศษ (ระดับผู้ดูแลระบบ) สำหรับการเข้าถึงระบบการจัดการความปลอดภัยข้อมูลหรือไม่	AWS มีการระบุหมวดหมู่ของเหตุการณ์ที่สามารถตรวจสอบได้สำหรับระบบและอุปกรณ์ทั้งหมดภายในระบบของ AWS ทีมการให้บริการจะกำหนดค่าคุณลักษณะการตรวจสอบเพื่อบันทึกเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยอย่างต่อเนื่อง เพื่อให้สอดคล้องกับข้อกำหนด ระบบการจัดเก็บบันทึกออกแบบมาเพื่อมอบบริการที่ปรับขนาดได้และพร้อมใช้งานสูง ซึ่งสามารถเพิ่มความสามารถในการทำงานได้เมื่อความต้องการพื้นที่จัดเก็บบันทึกเพิ่มมากขึ้น บันทึกข้อมูลการตรวจสอบประกอบด้วยชุดขององค์ประกอบข้อมูล เพื่อสนับสนุนข้อกำหนดด้านการวิเคราะห์ที่จำเป็น นอกจากนี้ บันทึกข้อมูลการตรวจสอบยังสามารถใช้งานได้โดยทีมความปลอดภัยของ AWS หรือทีมอื่นๆ ที่เหมาะสมเพื่อใช้ทำการตรวจสอบหรือวิเคราะห์ได้ตามต้องการ หรือเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยหรือส่งผลต่อธุรกิจ บุคลากรที่ได้รับมอบหมายภายในทีมของ AWS จะได้รับการแจ้งเตือนแบบอัตโนมัติทันที หากเกิดเหตุการณ์ความล้มเหลวในการประมวลผลการตรวจสอบ ความล้มเหลวในการประมวลผลการตรวจสอบประกอบด้วย ข้อผิดพลาดด้านซอฟต์แวร์/ฮาร์ดแวร์ เป็นต้น เมื่อได้รับการแจ้งเตือนแล้ว บุคลากรที่ได้รับการแจ้งเตือนจะออกบัตรผ่านรับแจ้งปัญหา และติดตามเหตุการณ์จนกว่าจะได้รับการแก้ไข กระบวนการบันทึกและตรวจสอบของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอก เพื่อยืนยันความสอดคล้องตามข้อกำหนดและการปฏิบัติตาม SOC, PCI DSS, ISO 27001 และ FedRAMP
ข้อมูลประจำตัวและการจัดการการเข้าถึง *นโยบายการเข้าถึงของผู้ใช้*	IAM-02.1	คุณมีการควบคุมเพื่อทำให้มั่นใจว่ามีการกำจัดการเข้าถึงระบบที่ไม่จำเป็นสำหรับวัตถุประสงค์ทางธุรกิจได้อย่างทันท่วงทีหรือไม่	รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติมเกี่ยวกับการยกเลิกการเข้าถึงของผู้ใช้ นอกจากนี้ คุณสามารถดูรายละเอียดเพิ่มเติมได้จากเอกสารความปลอดภัยของ AWS ในส่วน “วงจรการทำงานของพนักงาน” โปรดดู ISO 27001 ภาคผนวก A ส่วนที่ 9 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	IAM-02.2	คุณมีตัววัดสำหรับตรวจสอบความเร็วในการกำจัดการเข้าถึงระบบที่ไม่จำเป็นสำหรับวัตถุประสงค์ทางธุรกิจหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การวินิจฉัยปัญหา / การเข้าถึงพอร์ตการกำหนดค่า*	IAM-03.1	คุณใช้งานเครือข่ายแบบปลอดภัยโดยตรง เพื่อมอบการเข้าถึงการจัดการไปยังโครงสร้างพื้นฐานของบริการคลาวด์หรือไม่	การควบคุมที่ใช้งานจะจำกัดการเข้าถึงไปยังระบบและข้อมูล นอกจากนี้การมอบการเข้าถึงไปยังระบบและข้อมูลยังถูกจำกัดและตรวจสอบโดยนโยบายการเข้าถึงของ AWS นอกจากนี้ ข้อมูลและอินสแตนซ์เซิร์ฟเวอร์ของลูกค้ายังมีการแยกจากกันแบบลอจิคัลออกจากของลูกค้ารายอื่นๆ โดยค่าเริ่มต้น การควบคุมการเข้าถึงของผู้ใช้งานที่ได้รับสิทธิพิเศษ จะมีการตรวจสอบโดยผู้ตรวจสอบอิสระระหว่างการตรวจสอบของ AWS SOC, ISO 27001, PCI, ITAR และ FedRAMP
ข้อมูลประจำตัวและการจัดการการเข้าถึง *นโยบายและขั้นตอน*	IAM-04.1	คุณมีการจัดการและจัดเก็บข้อมูลประจำตัวของพนักงานทุกคนที่มีสิทธิ์เข้าถึงโครงสร้างพื้นฐานด้านไอที รวมถึงระดับการเข้าถึงของแต่ละคนหรือไม่	
	IAM-04.2	คุณมีการจัดการและเก็บข้อมูลประจำตัวของผู้ใช้สำหรับบุคลากรทุกคนที่มีสิทธิ์เข้าถึงเครือข่าย รวมถึงระดับการเข้าถึงของแต่ละคนหรือไม่	
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การแบ่งแยกหน้าที่*	IAM-05.1	คุณได้มอบเอกสารให้แก่ผู้เช่า ซึ่งอธิบายเกี่ยวกับวิธีการที่คุณแบ่งแยกหน้าที่การทำงานภายในข้อเสนอด้านบริการระบบคลาวด์หรือไม่	ลูกค้ายังคงเป็นผู้ควบคุมอำนาจในการจัดการการแบ่งแยกหน้าที่ของทรัพยากร AWS ของตนเอง สำหรับภายใน AWS ปฏิบัติตามระเบียบสอดคล้องกับมาตรฐาน ISO 27001 ในด้านการจัดการการแบ่งแยกหน้าที่ โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 6 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การจำกัดการเข้าถึงซอร์สโค้ด*	IAM-06.1	มีการควบคุมเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตไปยังแอปพลิเคชัน โปรแกรม หรือซอร์สโค้ดของออบเจ็กต์หรือไม่ รวมทั้งรับประกันว่าข้อมูลเหล่านี้สามารถเข้าถึงได้เฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 AWS ได้สร้างนโยบายและขั้นตอนแบบเป็นทางการ เพื่อร่างมาตรฐานขั้นต่ำสำหรับการเข้าถึงทรัพยากรของ AWS รายงาน AWS SOC จะสรุปการควบคุมที่มีเพื่อบริหารการจัดเตรียมการเข้าถึงทรัพยากรของ AWS โปรดดูรายละเอียดเพิ่มเติมจากเอกสารขั้นตอนความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	IAM-06.2	มีการควบคุมเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตไปยังแอปพลิเคชัน โปรแกรม หรือซอร์สโค้ดภายในออบเจ็กต์ของผู้เช่าหรือไม่ รวมทั้งรับประกันว่าข้อมูลเหล่านี้สามารถเข้าถึงได้เฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น	
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การเข้าถึงโดยบุคคลที่สาม*	IAM-07.1	คุณมีความสามารถในการกู้คืนความเสียหายจากการล้มเหลวหลายครั้งได้หรือไม่	AWS มาพร้อมกับความยืดหยุ่นสำหรับการวางอินสแตนซ์และการเก็บข้อมูลภายในภูมิภาคทางภูมิศาสตร์หลากหลายแห่ง รวมถึงการกำหนดข้ามพื้นที่ให้บริการภายในแต่ละภูมิภาค Availability Zone แต่ละโซนออกแบบมาให้เป็นโซนที่ความล้มเหลวจะไม่ขึ้นต่อกัน ในกรณีที่เกิดความล้มเหลว กระบวนการอัตโนมัติจะย้ายการรับส่งข้อมูลของลูกค้าออกจากพื้นที่
	IAM-07.2	คุณมีการตรวจสอบความต่อเนื่องของบริการกับผู้ให้บริการอัพสตรีม ในกรณีเกิดความล้มเหลวโดยผู้ให้บริการ	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
		หรือไม่	ที่ได้รับผลกระทบ รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติม ดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 15 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับการรับรองมาตรฐาน ISO 27001
	IAM-07.3	คุณมีผู้ให้บริการมากกว่าหนึ่งรายสำหรับบริการแต่ละชุดที่คุณต้องพึ่งพาหรือไม่	
	IAM-07.4	คุณมอบการเข้าถึงการสำรองการใช้งานเชิงปฏิบัติการและบทสรุปด้านความต่อเนื่องรวมถึงบริการต่างๆ ที่คุณต้องพึ่งพาหรือไม่	
	IAM-07.5	คุณมอบความสามารถให้กับผู้เช่าในการประกาศสภาวะความเสียหายหรือไม่	
	IAM-07.6	คุณมีตัวเลือกระบบสำรองที่ทริกเกอร์โดยผู้เช่าหรือไม่	
	IAM-07.7	คุณมีการแบ่งปันแผนการด้านความต่อเนื่องทางธุรกิจและแผนการสำรองการทำงานกับผู้เช่าหรือไม่	
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การจำกัดการเข้าถึงของผู้ใช้ / การอนุญาต*	IAM-08.1	คุณมีการบันทึกวิธีการที่คุณมอบและรับรองการเข้าถึงข้อมูลของผู้เช่าหรือไม่	ลูกค้า AWS ยังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง การควบคุมที่มีอยู่จะจำกัดการเข้าถึงระบบและข้อมูล และการเข้าถึงระบบและข้อมูลยังถูกจำกัดและตรวจสอบอีกด้วย นอกจากนี้ ข้อมูลและอินสแตนซ์เซิร์ฟเวอร์ของลูกค้ายังมีการแยกออกจากกันแบบลอจิคัลจากลูกค้ารายอื่นๆ โดยค่าเริ่มต้น การควบคุมการเข้าถึงของผู้ใช้งานที่ได้รับสิทธิพิเศษ จะมีการตรวจสอบโดยผู้ตรวจสอบอิสระระหว่างการตรวจสอบของ AWS SOC, ISO 27001, PCI, ITAR และ FedRAMP
	IAM-08.2	คุณมีวิธีการในการปรับระเบียบวิธีการแยกหมวดหมู่ข้อมูลของผู้ให้บริการและผู้เช่าให้สอดคล้องกันเพื่อวัตถุประสงค์ด้านการควบคุมการเข้าถึงหรือไม่	
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การอนุญาตการเข้าถึงของผู้ใช้*	IAM-09.1	ฝ่ายบริหารของคุณมีการจัดเตรียมการอนุญาตและข้อจำกัดสำหรับการเข้าถึงของผู้ใช้ (เช่น พนักงาน คู่สัญญา ลูกค้า (ผู้เช่า) คู่ค้าเชิงธุรกิจ และ/หรือผู้จำหน่าย) ก่อนจะมีการเข้าถึงข้อมูลและแอปพลิเคชัน (ทางกายภาพและแบบเสมือน) ระบบโครงสร้างพื้นฐาน และส่วนประกอบของเครือข่ายที่คุณเป็นเจ้าของหรืออยู่ในการดูแลหรือไม่	ตัวระบุผู้ใช้แบบเฉพาะจะถูกสร้างขึ้นระหว่างกระบวนการเวิร์กโฟลว์เตรียมการให้บริการภายในระบบจัดการทรัพยากรบุคคลของ AWS กระบวนการจัดเตรียมอุปกรณ์ช่วยรับประกันว่าจะมีตัวระบุเฉพาะสำหรับอุปกรณ์ กระบวนการทั้งสองชุดต้องผ่านการอนุมัติจากผู้จัดการเพื่อสร้างบัญชีผู้ใช้หรืออุปกรณ์ ตัวรับรองความถูกต้องเริ่มต้นจะถูกส่งมอบให้กับผู้ใช้งานด้วยตนเอง และส่งมอบให้กับอุปกรณ์ระหว่างกระบวนการจัดเตรียม ผู้ใช้ภายในสามารถเชื่อมโยงคีย์ SSH แบบสาธารณะเข้ากับบัญชีของตนได้ ตัวรับรองความถูกต้องของบัญชีระบบจะถูกมอบให้กับผู้ร้องขอระหว่างกระบวนการจัดทำบัญชี หลังจากที่ข้อมูลประจำตัวของผู้ร้องขอได้รับการตรวจสอบแล้ว

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	IAM-09.2	เมื่อมีการร้องขอ คุณให้สิทธิ์การเข้าถึงของผู้ใช้ (เช่น พนักงาน คู่สัญญา ลูกค้า (ผู้เช่า) คู่ค้าเชิงธุรกิจ และ/หรือผู้จำหน่าย) เพื่อใช้เข้าถึงข้อมูลและแอปพลิเคชัน (ทางกายภาพและแบบเสมือน) ระบบโครงสร้างพื้นฐาน และส่วนประกอบของเครือข่ายที่คุณเป็นเจ้าของหรืออยู่ในการดูแลหรือไม่	AWS มีการควบคุมเพื่อรองรับภัยคุกคามจากการเข้าถึงแบบไม่เหมาะสมของบุคคลภายใน การรับรองและการยืนยันจากหน่วยงานภายนอกทั้งหมดจะประเมินผลการควบคุมเชิงป้องกันและเชิงตรวจสอบของการเข้าถึงแบบลอจิคัล นอกจากนี้ ยังมีการประเมินความเสี่ยงเป็นประจำ ซึ่งมุ่งเน้นเกี่ยวกับวิธีการควบคุมและติดตามการเข้าถึงของบุคคลภายใน
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การตรวจสอบการเข้าถึงของผู้ใช้*	IAM-10.1	คุณมีการกำหนดให้มีการยื่นการรับรองการให้สิทธิ์สำหรับผู้ใช้งานและผู้ดูแลระบบทั้งหมดอย่างน้อยปีละหนึ่งครั้งหรือไม่ (ยกเว้นผู้ใช้ที่ดูแลโดยผู้เช่า)	เพื่อให้เป็นไปตามมาตรฐาน ISO 27001 สิทธิ์การเข้าถึงทั้งหมดจะได้รับการตรวจสอบเป็นประจำ โดยต้องมีการอนุมัติซ้ำอย่างชัดแจ้ง มิฉะนั้นจะมีการยกเลิกการเข้าถึงทรัพยากรโดยอัตโนมัติ การควบคุมในส่วนที่เฉพาะเจาะจงกับการตรวจสอบการเข้าถึงของผู้ใช้มีการอธิบายไว้ภายในรายงาน SOC ข้อยกเว้นภายในการควบคุมการให้สิทธิ์ผู้ใช้งาน มีระบุไว้ภายในรายงาน SOC โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 9 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	IAM-10.2	หากตรวจพบว่าผู้ใช้มีการได้รับสิทธิ์ที่ไม่เหมาะสม จะมีการบันทึกการดำเนินการแก้ไขและการรับรองทั้งหมดหรือไม่	
	IAM-10.3	คุณจะแบ่งปันรายงานการแก้ไขการให้สิทธิ์และการรับรองผู้ใช้กับผู้เช่าหรือไม่ หากมีความเป็นไปได้ว่าอาจมีการยินยอมให้เกิดการเข้าถึงอย่างไม่เหมาะสมต่อข้อมูลของผู้เช่า	
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การยกเลิกการเข้าถึงของผู้ใช้*	IAM-11.1	คุณมีการยกเลิกการจัดเตรียม ยกเลิก หรือแก้ไขการเข้าถึงของผู้ใช้ไปยังระบบขององค์กร สินทรัพย์ข้อมูล และข้อมูลต่างๆ อย่างทันท่วงทีเมื่อมีการเปลี่ยนแปลงสถานะของพนักงาน คู่สัญญา ลูกค้า คู่ค้าเชิงธุรกิจ หรือบริษัทภายนอกที่เกี่ยวข้องหรือไม่	สิทธิ์เข้าถึงจะถูกยกเลิกโดยอัตโนมัติเมื่อบันทึกข้อมูลพนักงานถูกยกเลิกในระบบทรัพยากรบุคคลของ Amazon ด้วยเช่นกัน เมื่อมีการเปลี่ยนแปลงหน้าที่ในงานของพนักงานเกิดขึ้น จะต้องมีการอนุมัติสิทธิ์เข้าถึงที่ต่อเนื่องให้กับทรัพยากร ไม่เช่นนั้นจะถูกยกเลิกโดยอัตโนมัติ รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติมเกี่ยวกับการยกเลิกการเข้าถึงของผู้ใช้ นอกจากนี้ คุณสามารถดูรายละเอียดเพิ่มเติมได้จากเอกสารความปลอดภัยของ AWS ในส่วน “วงจรการทำงานของพนักงาน” โปรดดู ISO 27001 ภาคผนวก A ส่วนที่ 9 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	IAM-11.2	การเปลี่ยนแปลงใดๆ ภายในสถานะการเข้าถึงของลูกค้ามีวัตถุประสงค์เพื่อหมายรวมถึงการยกเลิกการจ้าง การยกเลิกสัญญาและข้อตกลง การเปลี่ยนแปลงการว่าจ้างหรือการโอนย้ายภายในองค์กรหรือไม่	
ข้อมูลประจำตัวและการจัดการการเข้าถึง *ข้อมูลประจำตัว*	IAM-12.1	คุณสนับสนุนการใช้งาน หรือการผสมผสานการใช้งานร่วมกับโซลูชันการลงชื่อเข้าใช้ครั้งเดียว (SSO) ของลูกค้าที่มีอยู่กับบริการหรือไม่	บริการ AWS Identity and Access Management (IAM) มอบการเชื่อมโยงข้อมูลประจำตัวเข้ากับ AWS Management Console การรับรองความถูกต้องแบบหลายปัจจัยเป็นคุณสมบัติเสริมที่ลูกค้าเลือกใช้งานได้ โปรดดูรายละเอียดเพิ่มเติมจากเว็บไซต์ AWS ที่

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ของ ID ผู้ใช้	IAM-12.2	คุณใช้มาตรฐานแบบเปิดเพื่อมอบความสามารถในการรับรองความถูกต้องให้กับผู้เช่าหรือไม่	http://aws.amazon.com/mfa บริการ AWS Identity and Access Management (IAM) สนับสนุนการเชื่อมโยงข้อมูลประจำตัวสำหรับการมอบสิทธิ์การเข้าถึงไปยัง AWS Management Console หรือ API ของ AWS ด้วยการเชื่อมโยงข้อมูลประจำตัว ข้อมูลประจำตัวภายนอก (ผู้ใช้งานที่มีการเชื่อมโยง) จะได้รับมอบสิทธิ์การเข้าถึงอย่างปลอดภัยเพื่อเข้าถึงทรัพยากรในบัญชี AWS ของคุณโดยไม่จำเป็นต้องสร้างผู้ใช้งาน IAM ข้อมูลประจำตัวภายนอกเหล่านี้ อาจมาจากผู้ให้บริการข้อมูลประจำตัวที่องค์กรของคุณใช้งาน (เช่น Microsoft Active Directory หรือจาก AWS Directory Service) หรือจากผู้ให้บริการข้อมูลประจำตัวบนเว็บ เช่น Amazon Cognito, การล็อกอินด้วย Amazon, Facebook, Google หรือผู้ให้บริการ OpenID Connect (OIDC) ที่เข้ากันได้
	IAM-12.3	คุณรองรับมาตรฐานการเชื่อมโยงข้อมูลประจำตัว (SAML, SPML, WS-Federation, ฯลฯ) เพื่อเป็นช่องทางสำหรับรับรองความถูกต้อง/อนุญาตผู้ใช้หรือไม่	
	IAM-12.4	คุณมีความสามารถในการบังคับใช้นโยบาย (เช่น XACML) เพื่อบังคับใช้ข้อจำกัดเชิงนโยบายหรือเชิงกฎหมายของภูมิภาคกับการเข้าถึงของผู้ใช้หรือไม่	
	IAM-12.5	คุณมีระบบการจัดการข้อมูลประจำตัว (ช่วยให้สามารถจัดหมวดหมู่ข้อมูลสำหรับผู้เช่า) เพื่อให้สามารถใช้การมอบสิทธิ์เข้าถึงข้อมูลโดยอ้างอิงจากบทบาทหรือตามบริบทหรือไม่	
	IAM-12.6	คุณมอบตัวเลือกการรับรองความถูกต้องที่มีประสิทธิภาพ (การรับรองแบบหลายปัจจัย) ให้แก่ผู้เช่า สำหรับการเข้าถึงของผู้ใช้หรือไม่ (การรับรองแบบดิจิตัล โทเค็น ระบบชีวมาตร ฯลฯ)	
	IAM-12.7	คุณยินยอมให้ผู้เช่าใช้บริการรับรองข้อมูลประจำตัวของบริษัทภายนอกหรือไม่	
	IAM-12.8	คุณสนับสนุนการบังคับใช้นโยบายรหัสผ่าน (ความยาวขั้นต่ำ อายุ ประวัติ ความซับซ้อน) และการล็อคบัญชี (เกณฑ์ขั้นต่ำ ระยะเวลาการล็อค) หรือไม่	AWS Identity and Access Management (IAM) ช่วยให้ลูกค้าควบคุมการเข้าถึงบริการและทรัพยากร AWS โดยผู้ใช้ได้อย่างปลอดภัย คุณสามารถดูข้อมูลเพิ่มเติมเกี่ยวกับ IAM ได้จากเว็บไซต์ที่ https://aws.amazon.com/iam/ รายงาน AWS SOC จะแสดงรายละเอียดเกี่ยวกับกิจกรรมการควบคุมเฉพาะที่ดำเนินการโดย AWS
	IAM-12.9	คุณอนุญาตให้ผู้เช่า/ลูกค้าระบุนโยบายรหัสผ่านและการล็อคบัญชีสำหรับบัญชีของตนเองหรือไม่	
	IAM-12.10	คุณสนับสนุนความสามารถในการบังคับเปลี่ยนรหัสผ่านเมื่อล็อกอินครั้งแรกหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	IAM-12.11	คุณมีระบบกลไกเพื่อปลดล็อคบัญชีที่ถูกล็อคหรือไม่ (เช่น ระบบบริการตนเองผ่านอีเมล การระบุคำถามท้าทาย การปลดล็อคด้วยตนเอง)	
ข้อมูลประจำตัวและการจัดการการเข้าถึง *การเข้าถึงโปรแกรมอรรถประโยชน์*	IAM-13.1	มีการจำกัดการใช้งานและตรวจสอบโปรแกรมที่สามารถจัดการกับพาร์ติชันแบบเสมือนได้ในระดับสำคัญ (เช่น การสั่งปิดเครื่อง ลอกแบบ ฯลฯ) อย่างเหมาะสมหรือไม่	เพื่อให้สอดคล้องตามมาตรฐาน ISO 27001 มีการจำกัดการใช้งานและตรวจสอบโปรแกรมอรรถประโยชน์ของระบบอย่างเหมาะสม รายงาน AWS SOC จะแสดงรายละเอียดเกี่ยวกับกิจกรรมการควบคุมเฉพาะที่ดำเนินการโดย AWS โปรดดูรายละเอียดเพิ่มเติมจากเอกสารขั้นตอนความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	IAM-13.2	คุณมีความสามารถในการตรวจสอบการโจมตีที่มุ่งเป้าหมายไปยังโครงสร้างพื้นฐานแบบเสมือนโดยตรงได้หรือไม่ (เช่น การทำ Shimming, Blue Pill, Hyper Jumping ฯลฯ)	
	IAM-13.3	มีการใช้การควบคุมเชิงเทคนิคเพื่อป้องกันการโจมตีที่มุ่งเป้าหมายไปยังโครงสร้างพื้นฐานแบบเสมือนหรือไม่	
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *การลงบันทึกตรวจสอบ / การตรวจสอบการบุกรุก*	IVS-01.1	มีการใช้เครื่องมือตรวจสอบความถูกต้องไฟล์ (โฮสต์) และเครื่องมือตรวจสอบผู้บุกรุกเครือข่าย (IDS) เพื่อช่วยในการตรวจสอบอย่างทันท่วงที ตรวจสอบโดยวิเคราะห์หาสาเหตุต้นตอ และเพื่อตอบสนองต่อเหตุการณ์หรือไม่	โปรแกรมรับมือเหตุการณ์ของ AWS (การตรวจสอบ การสืบสวน และการรับมือกับเหตุการณ์) ได้รับการพัฒนาเพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 และมีการจำกัดการใช้งานและตรวจสอบโปรแกรมของระบบอย่างเหมาะสม รายงาน AWS SOC แสดงรายละเอียดเพิ่มเติมเกี่ยวกับการควบคุมต่างๆ ที่มีการนำมาใช้เพื่อจำกัดการเข้าถึงระบบ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารขั้นตอนความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	IVS-01.2	มีการจำกัดการเข้าถึงบันทึกการตรวจสอบโดยผู้ใช้งานแบบกายภาพและแบบลอจิคัลเพื่อให้เข้าถึงได้เฉพาะบุคลากรที่ได้รับอนุญาตหรือไม่	
	IVS-01.3	คุณสามารถแสดงหลักฐานได้หรือไม่ ว่ามีการเชื่อมโยงการตรวจสอบวิเคราะห์สถานะของระเบียบข้อบังคับและมาตรฐานด้านการควบคุม/สถาปัตยกรรม/และกระบวนการต่างๆ	
	IVS-01.4	มีการจัดเก็บบันทึกการตรวจสอบรวมไว้ที่ศูนย์กลางหรือไม่	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 ระบบข้อมูลของ AWS ใช้ระบบนาฬิการะบบภายใน ซึ่งซิงโครไนซ์ผ่าน NTP (Network Time Protocol)

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	IVS-01.5	คุณมีการตรวจดูบันทึกการตรวจสอบเป็นประจำสำหรับเหตุการณ์ความปลอดภัยหรือไม่ (เช่น โดยการใช้เครื่องมืออัตโนมัติ)	AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001 AWS ใช้ประโยชน์จากระบบการตรวจสอบอัตโนมัติเพื่อมอบประสิทธิภาพและความพร้อมให้บริการในระดับสูง การตรวจสอบเชิงรุกสามารถใช้งานได้ผ่านเครื่องมือออนไลน์หลากหลายรูปแบบ สำหรับการใช้งานทั้งภายในและภายนอก มีการติดตั้งระบบภายใน AWS อย่างครอบคลุมเพื่อการตรวจสอบตัววัดผลการปฏิบัติการหลัก และยังมีการกำหนดค่าการแจ้งเตือนให้แจ้งเจ้าหน้าที่ฝ่ายปฏิบัติการและฝ่ายบริหาร เมื่อมีการละเมิดเกณฑ์การเตือนล่วงหน้าของตัววัดผลการปฏิบัติการหลัก มีการใช้กำหนดการแบบเตรียมพร้อมสำหรับการปฏิบัติงาน เพื่อให้เจ้าหน้าที่พร้อมรับมือกับปัญหาด้านการปฏิบัติงานตลอดเวลา ซึ่งรวมถึงระบบเพจเจอร์ เพื่อให้มีการแจ้งเตือนเจ้าหน้าที่ปฏิบัติการอย่างรวดเร็วและเชื่อถือได้ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *การตรวจสอบการเปลี่ยนแปลง*	IVS-02.1	คุณมีการลงบันทึกและแจ้งเตือนการเปลี่ยนแปลงใดๆ ที่ดำเนินการกับอิมเมจของเครื่องเสมือน โดยไม่คำนึงถึงสถานะการทำงานหรือไม่ (เช่น ระงับ ปิด หรือทำงานอยู่)	เครื่องเสมือนมีการกำหนดสิทธิ์ให้กับลูกค้าโดยเป็นส่วนหนึ่งของบริการ EC2 ลูกค้ายังคงมีอำนาจควบคุมประเภทของทรัพยากรที่ใช้ รวมถึงตำแหน่งการจัดเก็บทรัพยากร โปรดดูรายละเอียดเพิ่มเติมจากเว็บไซต์ AWS ที่ http://aws.amazon.com
	IVS-02.2	เมื่อมีการเปลี่ยนแปลงภายในเครื่องเสมือน หรือเมื่อมีการย้ายอิมเมจและมีการรับรองความถูกต้องของอิมเมจในภายหลัง คุณได้มีการแจ้งให้ลูกค้าทราบผ่านวิธีการแบบอิเล็กทรอนิกส์โดยทันทีหรือไม่ (เช่น ผ่านพอร์ทัล หรือการแจ้งเตือน)	
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *การซิงโครไนซ์นาฬิกา*	IVS-03.1	คุณใช้โปรโตคอลการบริการด้านเวลาที่มีการซิงโครไนซ์กัน (เช่น NTP) เพื่อรับรองว่าระบบทั้งหมดมีการอ้างอิงถึงเวลาเดียวกันหรือไม่	เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 ระบบข้อมูลของ AWS ใช้ระบบนาฬิการะบบภายใน ซึ่งซิงโครไนซ์ผ่าน NTP (Network Time Protocol) AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *การวางแผนความจุ /*	IVS-04.1	คุณมีการมอบเอกสารที่อธิบายข้อมูลเกี่ยวกับการใช้งานระดับของระบบ (เครือข่าย, พื้นที่จัดเก็บ, หน่วยความจำ, I/O, ฯลฯ) ที่เกินขนาด สำหรับระบบที่คุณมี รวมถึงเงื่อนไขและสถานการณ์ที่เกี่ยวข้องหรือไม่	รายละเอียดเกี่ยวกับข้อกำหนดการให้บริการของ AWS และวิธีการยื่นขอบริการเพิ่มเติมโดยเฉพาะ สามารถดูได้จากเว็บไซต์ของ AWS ที่ http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html AWS จัดการความจุและการใช้งานข้อมูลให้สอดคล้องกับมาตรฐาน ISO 27001 AWS ผ่านการตรวจสอบ

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ทรัพยากร	IVS-04.2	คุณจำกัดการใช้ความสามารถในการใช้งานหน่วยความจำเกินขนาดที่มีภายในไฮเปอร์ไวเซอร์หรือไม่	และรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	IVS-04.3	ข้อกำหนดด้านความจุของระบบของคุณ มีการพิจารณาถึงความต้องการความจุปัจจุบัน ความจุที่วางแผน และที่คาดการณ์ไว้สำหรับระบบทั้งหมดเพื่อมอบบริการแก่ผู้เช่าหรือไม่	
	IVS-04.4	มีการตรวจสอบประสิทธิภาพการทำงานของระบบและปรับปรุงอย่างต่อเนื่องเพื่อให้ตรงกับระเบียบข้อบังคับ สัญญา และข้อกำหนดเชิงธุรกิจ สำหรับระบบทั้งหมดที่ใช้เพื่อมอบบริการให้แก่ผู้เช่าหรือไม่	
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *การจัดการ - การจัดการความเสี่ยง*	IVS-05.1	เครื่องมือหรือบริการที่ใช้ประเมินความเสี่ยงรองรับกับเทคโนโลยีระบบเสมือนที่ใช้งานหรือไม่ (เช่น การรับรู้ระบบเสมือน)	ปัจจุบัน Amazon EC2 ใช้ไฮเปอร์ไวเซอร์ Xen เวอร์ชันที่มีการปรับแต่งระดับสูง ไฮเปอร์ไวเซอร์ได้รับการประเมินสำหรับช่องโหว่และเส้นทางการโจมตีใหม่ๆ และที่มีอยู่เดิมโดยทีมเจาะระบบภายนอกและภายในและเหมาะอย่างยิ่งสำหรับการดูแลการแยกส่วนอย่างชัดเจนระหว่างเครื่องเสมือนแบบ Guest การรักษาความปลอดภัยไฮเปอร์ไวเซอร์ Xen ของ AWS ได้รับการประเมินผลโดยผู้ตรวจสอบอิสระในระหว่างการประเมินและการตรวจสอบอยู่เป็นประจำ และมีการสแกนหาความเสี่ยงทั้งภายนอกและภายในเป็นประจำ ในระบบปฏิบัติการของโฮสต์ เว็บแอปพลิเคชัน และฐานข้อมูลที่ใช้งานโฮสต์ในสภาพแวดล้อม AWS โดยใช้เครื่องมือต่างๆ การสแกนหาความเสี่ยงและหลักปฏิบัติในการแก้ไขความเสี่ยงมีการตรวจสอบอยู่เสมอ เพื่อให้สอดคล้องกับการปฏิบัติตามมาตรฐานของ PCI DSS และ FedRAMP
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *การรักษาความปลอดภัยเครือข่าย*	IVS-06.1	สำหรับบริการ IaaS คุณได้ให้คำแนะนำกับลูกค้าเกี่ยวกับวิธีการสร้างสถาปัตยกรรมความปลอดภัยหลายระดับ ซึ่งเทียบเท่ากับการใช้งานโซลูชันแบบเสมือนหรือไม่	เว็บไซต์ของ AWS มอบคำแนะนำเกี่ยวกับการสร้างสถาปัตยกรรมความปลอดภัยแบบหลายระดับภายในเอกสารหลายฉบับ ซึ่งสามารถดูได้จากเว็บไซต์สาธารณะของ AWS ที่ http://aws.amazon.com/documentation/
	IVS-06.2	คุณมีการปรับปรุงไดอะแกรมสถาปัตยกรรมเครือข่ายที่มีการระบุโฟลว์ของข้อมูลระหว่างโดเมน/โซนความปลอดภัยอย่างสม่ำเสมอหรือไม่	อุปกรณ์การป้องกันแบบแบ่งเขตซึ่งใช้ชุดกฎ รายการควบคุมการเข้าถึง (ACL) และการกำหนดค่า จะควบคุมกระแสข้อมูลระหว่างเส้นใยของเครือข่าย Amazon มีเส้นใยเครือข่ายหลายชุด ซึ่งแต่ละชุดจะถูกแยกออกจากกันโดยอุปกรณ์ที่ควบคุมกระแสข้อมูล

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	IVS-06.3	คุณมีการตรวจสอบการเข้าถึง/การเชื่อมต่อที่อนุญาต (เช่น กฎไฟร์วอลล์) ระหว่างโดเมน/โซนความปลอดภัยภายในเครือข่ายเพื่อหาความเหมาะสมหรือไม่	ระหว่างเส้นใยของเครือข่าย กระแสของข้อมูลระหว่างเส้นใยจะถูกกำหนดโดยการอนุญาตที่ผ่านการรับรองหรือรายการควบคุมการเข้าถึง (ACL) ที่อยู่ภายในอุปกรณ์เหล่านี้ อุปกรณ์เหล่านี้ทำหน้าที่ควบคุมกระแสของข้อมูลระหว่างเส้นใย ตามที่กำหนดโดย ACL เหล่านี้ ACL จะถูกระบุและรับรองโดยบุคลากรที่เหมาะสม และมีการจัดการและติดตั้งโดยใช้เครื่องมือจัดการ ACL ของ AWS ทีมของ Information Security ของ Amazon คือผู้อนุมัติ ACL เหล่านี้ ชุดกฎไฟร์วอลล์ที่ได้รับการอนุมัติและรายการควบคุมการเข้าถึงระหว่างเส้นใยเครือข่ายจะจำกัดโฟลว์ข้อมูลที่ส่งไปยังบริการระบบข้อมูลที่เฉพาะเจาะจง รายการควบคุมการเข้าถึงและชุดกฎจะได้รับการตรวจสอบและรับรอง จากนั้นจะถูกนำส่งไปยังอุปกรณ์การป้องกันภายในขอบเขตโดยอัตโนมัติเป็นระยะ (อย่างน้อยทุก 24 ชั่วโมง) เพื่อรับประกันว่าชุดกฎและรายการควบคุมการเข้าถึงเป็นปัจจุบันเสมอ การจัดการเครือข่ายของ AWS ได้รับการตรวจสอบอย่างสม่ำเสมอโดยผู้ตรวจสอบอิสระจากภายนอกเพื่อเป็นขั้นตอนหนึ่งของการปฏิบัติตามข้อกำหนดของ SOC, PCI DSS, ISO 27001 และ FedRAMP ของ AWS AWS ใช้การให้สิทธิ์การใช้งานระดับต่ำสุดภายในทุกส่วนประกอบของโครงสร้างพื้นฐาน AWS มีการจำกัดพอร์ตและโปรโตคอลที่ไม่มีวัตถุประสงค์ทางธุรกิจเฉพาะ AWS ปฏิบัติตามแนวทางอย่างเข้มงวดเพื่อใช้งานเฉพาะคุณสมบัติและฟังก์ชันที่จำเป็นในระดับต่ำที่สุดเพื่อการใช้งานอุปกรณ์ มีการสแกนเครือข่ายพอร์ตหรือโปรโตคอลใดๆ ที่ไม่จำเป็นและมีการใช้งานจะได้รับการแก้ไขให้ถูกต้อง และมีการสแกนหาความเสี่ยงทั้งภายนอกและภายในเป็นประจำ ในระบบปฏิบัติการของโฮสต์ เว็บแอปพลิเคชัน และฐานข้อมูลที่ใช้งานโฮสต์ในสภาพแวดล้อม AWS โดยใช้เครื่องมือต่างๆ การสแกนหาความเสี่ยงและหลักปฏิบัติในการแก้ไขความเสี่ยงมีการตรวจสอบอยู่เสมอ เพื่อให้ AWS สอดคล้องกับการปฏิบัติตามมาตรฐานของ PCI DSS และ FedRAMP
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *การเสริมประสิทธิภาพระบบปฏิบัติการและการควบคุมพื้นฐาน*	IVS-07.1	มีการเสริมระบบปฏิบัติการเพื่อมอบการใช้งานเฉพาะพอร์ต โปรโตคอล และบริการที่จำเป็นต่อความต้องการทางธุรกิจ โดยใช้การควบคุมทางเทคนิค (เช่น การป้องกันไวรัส การตรวจสอบและบันทึกความถูกต้องไฟล์) ในฐานะส่วนหนึ่งของมาตรฐานบิลด์พื้นฐานหรือเทมเพลตหรือไม่	
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *สภาพแวดล้อมการใช้งานจริง / ที่ไม่ใช่สำหรับการใช้งานจริง*	IVS-08.1	สำหรับข้อเสนอบริการแบบ SaaS หรือ PaaS คุณมอบสภาพแวดล้อมแบบแยกสำหรับการใช้งานจริงและกระบวนการทดสอบให้แก่ผู้เช่าหรือไม่	ลูกค้าของ AWS มีหน้าที่รับผิดชอบและสามารถสร้างรวมถึงดูแลสภาพแวดล้อมการใช้งานจริงและการทดสอบของตนเอง เว็บไซต์ของ AWS มีคำแนะนำในการสร้างสภาพแวดล้อมโดยใช้บริการของ AWS ซึ่งดูได้ที่ http://aws.amazon.com/documentation/
	IVS-08.2	สำหรับข้อเสนอบริการแบบ IaaS คุณให้คำแนะนำเกี่ยวกับวิธีการสร้างสภาพแวดล้อมที่เหมาะสมกับการใช้งานจริงและการทดสอบแก่ผู้เช่าหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	IVS-08.3	คุณได้มีการแยกสภาพแวดล้อมการใช้งานจริงและสภาพแวดล้อมที่ไม่ใช่สำหรับการใช้งานจริงออกจากกัน ทั้งแบบกายภาพและลอจิคัลหรือไม่	ลูกค้าของ AWS ยังคงเป็นผู้รับผิดชอบในการจัดการการแยกส่วนเครือข่ายของตนเอง เพื่อให้สอดคล้องกับข้อกำหนดของตนเองที่ระบุ สำหรับภายใน การแบ่งแยกเครือข่ายของ AWS ปฏิบัติตามระเบียบสอดคล้องกับมาตรฐาน ISO 27001 โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 13 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *การแยกส่วน*	IVS-09.1	ระบบและสภาพแวดล้อมเครือข่ายมีการป้องกันโดยไฟร์วอลล์ หรือไฟร์วอลล์แบบเสมือนเพื่อรับรองข้อกำหนดเชิงธุรกิจและความปลอดภัยของลูกค้าหรือไม่	
	IVS-09.2	สภาพแวดล้อมของระบบและเครือข่ายได้รับการป้องกันโดยไฟร์วอลล์หรือไฟร์วอลล์เสมือนเพื่อรับรองการปฏิบัติตามข้อกำหนดตามกฎหมาย ระเบียบข้อบังคับ และสัญญาหรือไม่	
	IVS-09.3	สภาพแวดล้อมของระบบและเครือข่ายได้รับการป้องกันโดยไฟร์วอลล์หรือไฟร์วอลล์เสมือนเพื่อรับรองการแยกออกจากกันของสภาพแวดล้อมการใช้งานจริงและสภาพแวดล้อมที่ไม่ใช่สำหรับการใช้งานจริงหรือไม่	
	IVS-09.4	ระบบและสภาพแวดล้อมเครือข่ายมีการป้องกันโดยไฟร์วอลล์ หรือไฟร์วอลล์แบบเสมือนเพื่อรับรองการป้องกันและการแยกกันของข้อมูลสำคัญหรือไม่	
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *ความปลอดภัยของระบบ VM - การปกป้องข้อมูล vMotion*	IVS-10.1	มีการใช้ช่องทางการสื่อสารที่ปลอดภัยและมีการเข้ารหัส เมื่อทำการโอนย้ายเซิร์ฟเวอร์กายภาพ แอปพลิเคชัน หรือข้อมูลไปยังเซิร์ฟเวอร์แบบเสมือนหรือไม่	AWS มอบความสามารถให้ลูกค้าใช้ระบบกลไกการเข้ารหัสของตนเองสำหรับบริการแทบทุกประเภท รวมถึงการเข้ารหัสแบบ S3, EBS และ EC2 เซสชัน VPC ก็ได้รับการเข้ารหัสเช่นกัน
	IVS-10.2	คุณใช้เครือข่ายที่แยกออกจากเครือข่ายระดับการใช้งานจริงหรือไม่ เมื่อทำการโอนย้ายเซิร์ฟเวอร์กายภาพ แอปพลิเคชัน หรือข้อมูลไปยังเซิร์ฟเวอร์แบบเสมือน	ลูกค้า AWS ยังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง AWS มอบความสามารถให้กับลูกค้าในการรักษาและพัฒนาสภาพแวดล้อมสำหรับการใช้งานจริงและสภาพแวดล้อมที่ไม่ใช่สำหรับการใช้งานจริง ลูกค้ามีหน้าที่รับผิดชอบเพื่อรับรองว่าข้อมูลสำหรับการใช้งานจริงของตนเองนั้นจะไม่ถูกทำซ้ำภายในสภาพแวดล้อมที่ไม่ใช่สำหรับการใช้งานจริง

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *ความปลอดภัย VMM - การเสริมไฮเปอร์ไวเซอร์*	IVS-11.1	คุณมีการจำกัดการเข้าถึงของบุคลากรในการเข้าถึงฟังก์ชันการจัดการไฮเปอร์ไวเซอร์ ทั้งหมดรวมถึงการเข้าถึงคอนโซลระดับผู้ดูแล สำหรับระบบที่โฮสต์ระบบเสมือน โดยใช้หลักการให้สิทธิ์การใช้งานระดับต่ำสุดและสนับสนุนโดยการควบคุมเชิงเทคนิคหรือไม่ (เช่น ใช้การรับรองความถูกต้องสองปัจจัย, การติดตามการตรวจสอบ, การกรองที่อยู่ IP, การใช้ไฟร์วอลล์ และการสื่อสารแบบปกปิด TLS ไปยังคอนโซลระดับผู้ดูแล)	AWS ใช้แนวคิดของการให้สิทธิ์การใช้งานระดับต่ำสุดและมีการมอบการเข้าถึงเฉพาะที่จำเป็นสำหรับผู้ใช้เพื่อปฏิบัติงานตามหน้าที่ของตนเองเท่านั้น เมื่อมีการสร้างบัญชีผู้ใช้ บัญชีผู้ใช้จะถูกสร้างโดยให้สิทธิ์การเข้าถึงในระดับน้อยที่สุด การเข้าถึงในระดับที่เหนือกว่าการให้สิทธิ์การใช้งานระดับต่ำสุดจะต้องได้รับการอนุญาตอย่างเหมาะสม โปรดดูรายละเอียดเพิ่มเติมเกี่ยวกับการควบคุมการเข้าถึงได้จากรายงาน AWS SOC
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *ความปลอดภัยระบบไร้สาย*	IVS-12.1	มีการวางนโยบายและขั้นตอนการกำหนดและใช้งานระบบกลไกเพื่อป้องกันส่วนนอกของสภาพแวดล้อมเครือข่ายแบบไร้สาย รวมถึงจำกัดการส่งข้อมูลไร้สายที่ไม่ได้รับอนุญาตหรือไม่	เรามีนโยบาย ขั้นตอน และระบบกลไกในการป้องกันสภาพแวดล้อมเครือข่ายของ AWS ไว้แล้ว การควบคุมความปลอดภัยของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอกระหว่างช่วงการตรวจสอบการปฏิบัติตามข้อกำหนดของ SOC, PCI DSS, ISO 27001 และ FedRAMP
	IVS-12.2	มีนโยบายและขั้นตอน รวมถึงมีการกำหนดและใช้งานระบบกลไกเพื่อรับประกันว่ามีการใช้งานการตั้งค่าความปลอดภัยแบบไร้สาย ซึ่งใช้การเข้ารหัสที่แข็งแกร่งสำหรับการรับรองความถูกต้องและการส่งข้อมูล และเป็นการตั้งค่าแทนที่ค่าเริ่มต้นของผู้จำหน่ายหรือไม่ (เช่น คีย์การเข้ารหัส, รหัสผ่าน, สตริงคอมมูนิตี SNMP)	
	IVS-12.3	มีนโยบายและขั้นตอน รวมถึงมีการกำหนดและใช้งานระบบกลไกเพื่อป้องกันสภาพแวดล้อมเครือข่ายแบบไร้สาย และตรวจสอบการมีอยู่ของอุปกรณ์เครือข่ายที่ไม่ได้รับอนุญาต (หลอกลวง) เพื่อตัดการเชื่อมต่อจากเครือข่ายได้อย่างทันท่วงทีหรือไม่	
ความปลอดภัยโครงสร้างพื้นฐานและการจำลองเสมือน *สถาปัตยกรรมเครือข่าย*	IVS-13.1	ไดอะแกรมสถาปัตยกรรมเครือข่ายของคุณระบุสภาพแวดล้อมที่มีความเสี่ยงสูงและกระแสของข้อมูลที่อาจส่งผลกระทบต่อการปฏิบัติตามข้อกำหนดของกฎหมายไว้อย่างชัดเจนหรือไม่	ลูกค้าของ AWS ยังคงเป็นผู้รับผิดชอบในการจัดการการแยกส่วนเครือข่ายของตนเอง เพื่อให้สอดคล้องกับข้อกำหนดของตนเองที่ระบุ สำหรับภายใน การแบ่งแยกเครือข่ายของ AWS ปฏิบัติตามระเบียบที่สอดคล้องกับมาตรฐาน ISO 27001 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการ

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
			รับรอง ISO 27001
	IVS-13.2	คุณมีการใช้มาตรการทางเทคนิค และใช้เทคนิคการป้องกันแบบ Defense in Depth (เช่น การตรวจสอบแพ็คเก็ตแบบลึก, การจำกัดการส่งข้อมูล และการทำ Black-hole) เพื่อตรวจสอบและรับมือกับการโจมตีผ่านเครือข่ายที่เกี่ยวข้องกับรูปแบบการส่งข้อมูลขาเข้าและขาออกที่ผิดปกติ (เช่น การทำ MAC Spoofing และการโจมตีแบบ ARP Poisoning) และ/หรือการโจมตีแบบ Distributed Denial-of-Service (DDoS) ได้อย่างทันท่วงทีหรือไม่	ระบบความปลอดภัยของ AWS จะตรวจดูที่อยู่ IP ตำแหน่งข้อมูลของบริการที่เชื่อมต่อกับอินเทอร์เน็ตทั้งหมดเป็นประจำเพื่อค้นหาช่องโหว่ (การตรวจสอบนี้ไม่รวมถึงอินสแตนซ์ของลูกค้า) ฝ่ายความปลอดภัยของ AWS จะแจ้งต่อฝ่ายที่เหมาะสมให้แก้ไขช่องโหว่ที่ระบุ นอกจากนี้ ความเสี่ยงด้านช่องโหว่จากภายนอกจะได้รับการประเมินโดยบริษัทด้านความปลอดภัยอิสระอยู่เป็นประจำ ข้อมูลที่พบและคำแนะนำต่างๆ ที่ได้จากการประเมินผลเหล่านี้จะได้รับการจัดหมวดหมู่และส่งมอบให้กับผู้นำของ AWS นอกจากนี้ สภาพแวดล้อมการควบคุมของ AWS ยังได้รับการประเมินความเสี่ยงอย่างสม่ำเสมอ ทั้งจากภายนอกและภายใน AWS ร่วมมือกับหน่วยงานด้านการรับรองภายนอกและผู้ตรวจสอบอิสระ เพื่อตรวจสอบและทดสอบสภาพแวดล้อมการควบคุมโดยรวมของ AWS การควบคุมความปลอดภัยของ AWS ได้รับการตรวจสอบโดยผู้ตรวจสอบอิสระจากภายนอกระหว่างช่วงการตรวจสอบการปฏิบัติตามข้อกำหนดของ SOC, PCI DSS, ISO 27001 และ FedRAMP
ความสามารถในการทำงานร่วมกันและการเคลื่อนย้าย *API*	IPY-01	คุณมีการเผยแพร่รายการ API ทั้งหมดที่มีภายในบริการ พร้อมระบุรายละเอียดว่า API รายการใดเป็นแบบมาตรฐานหรือแบบกำหนดเองหรือไม่	โปรดดูรายละเอียดเกี่ยวกับ API ของ AWS ได้จากเว็บไซต์ของ AWS ที่ https://aws.amazon.com/documentation/ เพื่อให้สอดคล้องกับมาตรฐาน ISO 27001 AWS ได้สร้างนโยบายและขั้นตอนแบบเป็นทางการ เพื่อร่างมาตรฐานขั้นต่ำสำหรับการเข้าถึงทรัพยากรของ AWS รายงาน AWS SOC จะสรุปการควบคุมที่มีเพื่อบริหารการจัดเตรียมการเข้าถึงทรัพยากรของ AWS โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
ความสามารถในการทำงานร่วมกันและการเคลื่อนย้าย *คำขอข้อมูล*	IPY-02	หากมีการร้องขอ คุณมีข้อมูลที่ไม่มีโครงสร้างของลูกค้าภายในรูปแบบที่เป็นมาตรฐานของอุตสาหกรรมหรือไม่ (เช่น .doc, .xls หรือ .pdf)	
ความสามารถในการทำงานร่วมกันและการเคลื่อนย้าย *นโยบายและกฎหมาย*	IPY-03.1	คุณมีการเผยแพร่นโยบายและกระบวนการ (เช่น ข้อตกลงระดับการบริการ) ที่ครอบคลุมการใช้งาน API สำหรับความสามารถในการใช้งานร่วมกันระหว่างบริการและแอปพลิเคชันภายนอกหรือไม่	
	IPY-03.2	คุณมีการเผยแพร่นโยบายและกระบวนการ (เช่น ข้อตกลงระดับการบริการ) ที่ครอบคลุมการโอนย้ายข้อมูลแอปพลิเคชันมาที่บริการ หรือออกจากการบริการหรือไม่	ลูกค้ายังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง ลูกค้าสามารถเลือกวิธีการโอนย้ายแอปพลิเคชันและข้อมูล ทั้งระหว่างภายในและออกนอกระบบแพลตฟอร์ม AWS ได้ตามดุลยพินิจของตนเอง

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ความสามารถในการทำงานร่วมกันและการเคลื่อนย้าย *โปรโตคอลเครือข่ายมาตรฐาน*	IPY-04.1	การนำเข้า/ส่งออกข้อมูล และการจัดการบริการสามารถกระทำได้ผ่านโปรโตคอลเครือข่ายที่ปลอดภัย (เช่น ข้อความแบบเข้ารหัสและการรับรองความถูกต้อง) และได้รับการยอมรับตามมาตรฐานอุตสาหกรรมหรือไม่	AWS อนุญาตให้ลูกค้าเคลื่อนย้ายข้อมูลตามที่ต้องการทั้งภายในและออกนอกพื้นที่จัดเก็บของ AWS โปรดดูข้อมูลเพิ่มเติมเกี่ยวกับตัวเลือกการจัดเก็บได้ที่ http://aws.amazon.com/choosing-a-cloud-platform
	IPY-04.2	คุณได้มีการมอบเอกสารแก่ลูกค้า (ผู้เช่า) ซึ่งแสดงรายละเอียดของความสามารถในการใช้งานร่วมกันและมาตรฐานโปรโตคอลเครือข่ายการเคลื่อนย้ายที่เกี่ยวข้องหรือไม่	
ความสามารถในการทำงานร่วมกันและการเคลื่อนย้าย *การจำลองเสมือน*	IPY-05.1	คุณมีการใช้แพลตฟอร์มการจำลองเสมือนที่เป็นที่รู้จักทางอุตสาหกรรม รวมถึงรูปแบบการจำลองเสมือนแบบมาตรฐาน (เช่น OVF) เพื่อรับรองความสามารถในการใช้งานร่วมกันหรือไม่	ปัจจุบัน Amazon EC2 ใช้ไฮเปอร์ไวเซอร์ Xen เวอร์ชันที่มีการปรับแต่งระดับสูง ไฮเปอร์ไวเซอร์ได้รับการประเมินสำหรับช่องโหว่และเส้นทางการโจมตีใหม่ๆ และที่มีอยู่เดิมโดยทีมเจาะระบบภายนอกและภายในและเหมาะอย่างยิ่งสำหรับการดูแลการแยกส่วนอย่างชัดเจนระหว่างเครื่องเสมือนแบบ Guest การรักษาความปลอดภัยไฮเปอร์ไวเซอร์ Xen ของ AWS ได้รับการประเมินผลโดยผู้ตรวจสอบอิสระในระหว่างการประเมินและการตรวจสอบอยู่เป็นประจำ โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security
	IPY-05.2	คุณมีการบันทึกและทำเอกสารแสดงการเปลี่ยนแปลงแบบกำหนดเองที่ได้ดำเนินการกับไฮเปอร์ไวเซอร์ที่ใช้งานรวมถึงสุคการจำลองเสมือนเฉพาะของโซลูชันทั้งหมดเพื่อให้ลูกค้าตรวจสอบหรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *การป้องกันมัลแวร์*	MOS-01	คุณจัดให้มีการฝึกอบรมการป้องกันมัลแวร์สำหรับอุปกรณ์มือถือโดยเฉพาะ ในฐานะส่วนหนึ่งของการอบรมการรับรู้ด้านความปลอดภัยข้อมูลหรือไม่	โปรแกรม กระบวนการ และขั้นตอนต่างๆ ของ AWS สำหรับการป้องกันไวรัส / จัดการซอฟต์แวร์ประสงค์ร้ายนั้นสอดคล้องกับมาตรฐานของ ISO 27001 โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 12 สำหรับข้อมูลเพิ่มเติม
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *ร้านค้าแอปพลิเคชัน*	MOS-02	คุณมีการจัดทำเอกสารและเผยแพร่รายการร้านค้าแอปพลิเคชันที่ได้รับการรับรองสำหรับการเข้าถึงโดยอุปกรณ์มือถือหรือการจัดเก็บข้อมูลบริษัทและ/หรือระบบของบริษัทหรือไม่	AWS กำหนดกรอบงานและนโยบายด้านความปลอดภัยของข้อมูล และได้รวบรวมกรอบงานที่มีการรับรองของ ISO 27001 โดยอ้างอิงจากการควบคุมตาม ISO 27002, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 และ National Institute of Standards and Technology (NIST) Publication 800-53

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *แอปพลิเคชันที่ผ่านการรับรอง*	MOS-03	คุณมีความสามารถในการบังคับใช้นโยบาย (เช่น XACML) เพื่อประกันว่าแอปพลิเคชันที่สามารถโหลดลงบนอุปกรณ์เคลื่อนที่จะมีเพียงแอปพลิเคชันที่ผ่านการรับรองและแอปพลิเคชันจากร้านค้าแอปพลิเคชันที่ได้รับการรับรองเท่านั้นหรือไม่	(Recommended Security Controls for Federal Information Systems) ลูกค้ายังคงเป็นผู้ควบคุมและมีหน้าที่รับผิดชอบข้อมูลของตนเอง รวมถึงสินทรัพย์ประเภทสื่อที่เกี่ยวข้อง ดังนั้นจึงเป็นหน้าที่ของลูกค้าในการจัดการความปลอดภัยอุปกรณ์เคลื่อนที่ และการเข้าถึงเนื้อหาของลูกค้า
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *ซอฟต์แวร์ที่ผ่านการรับรองสำหรับการใช้งานแบบ BYOD*	MOS-04	นโยบายด้าน BYOD รวมถึงการฝึกอบรมของคุณระบุไว้อย่างชัดเจนหรือไม่ ว่าแอปพลิเคชันและร้านค้าแอปพลิเคชันใดที่ผ่านการรับรองเพื่อการใช้งานบนอุปกรณ์แบบ BYOD	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *การรับรู้และการฝึกอบรม*	MOS-05	คุณมีการกำหนดนโยบายเกี่ยวกับอุปกรณ์เคลื่อนที่ไว้เป็นเอกสารภายในการอบรมพนักงาน โดยระบุไว้อย่างชัดเจนถึงอุปกรณ์เคลื่อนที่การใช้งานที่ยอมรับได้ รวมถึงข้อกำหนดด้านอุปกรณ์เคลื่อนที่หรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *บริการบนระบบคลาวด์*	MOS-06	คุณมีการจัดทำบันทึกรายการของบริการบนระบบคลาวด์ที่ได้รับการรับรองไว้แล้ว ซึ่งอนุญาตให้ใช้สำหรับการใช้งานและจัดเก็บข้อมูลธุรกิจขององค์กรผ่านอุปกรณ์เคลื่อนที่หรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *ความเข้ากันได้*	MOS-07	คุณมีการจัดทำเอกสารแสดงกระบวนการรับรองแอปพลิเคชัน ซึ่งเกี่ยวข้องกับการทดสอบอุปกรณ์ระบบปฏิบัติการ และปัญหาความเข้ากันได้ของแอปพลิเคชันหรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *สิทธิ์ของอุปกรณ์*	MOS-08	คุณมีนโยบาย BYOD ที่ระบุอุปกรณ์และข้อกำหนดด้านสิทธิ์เพื่อการอนุญาตใช้งานแบบ BYOD หรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *รายการอุปกรณ์*	MOS-09	คุณมีการเก็บรักษารายการอุปกรณ์เคลื่อนที่ทั้งหมดที่จัดเก็บและเข้าถึงข้อมูลขององค์กร โดยรายการดังกล่าวประกอบด้วยสถานะอุปกรณ์ (หรือระบบและระดับการแก้ไขข้อบกพร่อง การสูญหายหรือการปลดการใช้งาน และผู้รับมอบอุปกรณ์) หรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *การจัดการอุปกรณ์*	MOS-10	คุณมีการติดตั้งโซลูชันการจัดการอุปกรณ์เคลื่อนที่จากศูนย์กลาง เพื่อใช้งานกับอุปกรณ์เคลื่อนที่ทุกชุดที่ได้รับอนุญาตให้จัดเก็บ ส่งผ่าน หรือประมวลผลข้อมูลขององค์กรหรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *การเข้ารหัส*	MOS-11	นโยบายด้านอุปกรณ์เคลื่อนที่ของคุณกำหนดให้มีการใช้งานการเข้ารหัส สำหรับทั้งอุปกรณ์หรือสำหรับข้อมูลที่ระบุว่าเป็นข้อมูลสำคัญ โดยสามารถบังคับใช้ได้ผ่านการควบคุมเชิงเทคโนโลยีสำหรับอุปกรณ์เคลื่อนที่ทุกชุดหรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *การทำ Jailbreak / Root*	MOS-12.1	นโยบายด้านอุปกรณ์เคลื่อนที่ของคุณห้ามการหลีกเลี่ยงการควบคุมความปลอดภัยภายในตัวบนอุปกรณ์เคลื่อนที่หรือไม่ (เช่น การ Jailbreak หรือ Root)	
	MOS-12.2	คุณมีการควบคุมเชิงตรวจสอบและป้องกันบนอุปกรณ์ หรือผ่านระบบจัดการอุปกรณ์จากศูนย์กลาง เพื่อป้องกันการหลีกเลี่ยงการควบคุมความปลอดภัยภายในตัวอุปกรณ์หรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *กฎหมาย*	MOS-13.1	นโยบาย BYOD ของคุณมีการระบุอย่างชัดเจนเกี่ยวกับความคาดหวังด้านความเป็นส่วนตัว ข้อกำหนดสำหรับการฟ้องร้อง การค้นหาทางอิเล็กทรอนิกส์ และการจัดเก็บทางกฎหมายหรือไม่	ลูกค้ายังคงเป็นผู้ควบคุมและมีหน้าที่รับผิดชอบข้อมูลของตนเอง รวมถึงสินทรัพย์ประเภทสื่อที่เกี่ยวข้อง ดังนั้นจึงเป็นหน้าที่ของลูกค้าในการจัดการความปลอดภัยอุปกรณ์เคลื่อนที่ และการเข้าถึงเนื้อหาของลูกค้า
	MOS-13.2	คุณมีการควบคุมเชิงตรวจสอบและป้องกันบนอุปกรณ์ หรือผ่านระบบจัดการอุปกรณ์จากศูนย์กลาง เพื่อป้องกันการ	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
		หลีกเลี่ยงการควบคุมความปลอดภัยภายในตัวอุปกรณ์หรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *หน้าจอการล็อก*	MOS-14	คุณมีการกำหนดและบังคับใช้หน้าจอการล็อกอัตโนมัติสำหรับอุปกรณ์ BYOD และอุปกรณ์ที่เป็นเจ้าของโดยองค์กร ผ่านการควบคุมทางเทคนิคหรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *ระบบปฏิบัติการ*	MOS-15	คุณจัดการการเปลี่ยนแปลงทั้งหมดที่ดำเนินการกับระบบปฏิบัติการของอุปกรณ์เคลื่อนที่ ระดับการแก้ไขข้อบกพร่อง และแอปพลิเคชันผ่านกระบวนการจัดการการเปลี่ยนแปลงขององค์กรหรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *รหัสผ่าน*	MOS-16.1	คุณมีนโยบายด้านรหัสผ่านสำหรับอุปกรณ์เคลื่อนที่จัดหาให้โดยองค์กรและ/หรืออุปกรณ์เคลื่อนที่แบบ BYOD หรือไม่	
	MOS-16.2	คุณมีการบังคับใช้นโยบายรหัสผ่าน ผ่านการควบคุมเชิงเทคนิคหรือไม่ (เช่น MDM)	
	MOS-16.3	นโยบายรหัสผ่านของคุณห้ามไม่ให้มีการเปลี่ยนแปลงข้อกำหนดด้านการรับรองความถูกต้อง (เช่น ความยาวรหัสผ่าน / PIN) ผ่านอุปกรณ์เคลื่อนที่หรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *นโยบาย*	MOS-17.1	คุณมีนโยบายที่กำหนดให้ผู้ใช้ BYOD ทำการสำรองข้อมูลกับข้อมูลองค์กรที่ระบุไว้หรือไม่	
	MOS-17.2	คุณมีนโยบายที่กำหนดให้ผู้ใช้ BYOD ห้ามการใช้งานร้านค้าแอปพลิเคชันที่ไม่ได้รับการรับรองหรือไม่	
	MOS-17.3	คุณมีนโยบายที่กำหนดให้ผู้ใช้ BYOD ใช้งานซอฟต์แวร์ป้องกันมัลแวร์หรือไม่ (สำหรับกรณีที่รองรับ)	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *การลบข้อมูล*	MOS-18.1	ฝ่ายไอทีของคุณมีบริการลบข้อมูลจากระยะไกล หรือลบข้อมูลองค์กร สำหรับอุปกรณ์ BYOD ที่ยอมรับโดยองค์กรหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
จากระยะไกล	MOS-18.2	ฝ่ายไอทีของคุณมีบริการลบข้อมูลจากระยะไกล หรือลบข้อมูลองค์กร สำหรับอุปกรณ์มือถือที่จัดหาโดยองค์กรหรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *โปรแกรมแพทช์ด้านความปลอดภัย*	MOS-19.1	อุปกรณ์เคลื่อนที่ของคุณติดตั้งโปรแกรมแพทช์ที่เกี่ยวข้องกับความปลอดภัยรุ่นล่าสุด เมื่อมีการเผยแพร่เพื่อการใช้งานทั่วไปโดยผู้ผลิตอุปกรณ์หรือผู้ให้บริการหรือไม่	
	MOS-19.2	อุปกรณ์เคลื่อนที่ของคุณยินยอมให้มีการรับรองผ่านระยะไกล เพื่อดาวน์โหลดโปรแกรมแพทช์ด้านความปลอดภัยล่าสุดจากบุคลากรด้านไอทีขององค์กรหรือไม่	
ความปลอดภัยบนอุปกรณ์เคลื่อนที่ *ผู้ใช้*	MOS-20.1	นโยบาย BYOD ของคุณมีการชี้แจงถึงระบบและเซิร์ฟเวอร์ที่อนุญาต เพื่อการใช้งานหรือเพื่อเข้าถึงบนอุปกรณ์ที่รองรับใช้งาน BYOD หรือไม่	
	MOS-20.2	นโยบาย BYOD ของคุณระบุบทบาทผู้ใช้ที่ได้รับอนุญาตการเข้าถึงผ่านอุปกรณ์ที่รองรับใช้งาน BYOD หรือไม่	
การจัดการเหตุการณ์ด้านความปลอดภัย การค้นพบทางอิเล็กทรอนิกส์ และกระบวนการนิติวิทยาศาสตร์บนระบบคลาวด์ *ผู้ติดต่อ / ผู้มีอำนาจการซ่อมบำรุง*	SEF-01.1	คุณมีการจัดเตรียมผู้ประสานงานและบุคคลติดต่อสำหรับการติดต่อกับหน่วยงานภายในท้องที่ เพื่อให้สอดคล้องตามระเบียบข้อบังคับที่เหมาะสมและสัญญาหรือไม่	AWS ดูแลด้านการประสานงานกับหน่วยงานในอุตสาหกรรม องค์กรด้านความเสี่ยงและการปฏิบัติตามข้อกำหนด หน่วยงานรัฐในพื้นที่ และหน่วยงานด้านกฎระเบียบข้อบังคับ ตามที่ระบุโดยมาตรฐาน ISO 27001 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
การจัดการเหตุการณ์ด้านความปลอดภัย การค้นพบทางอิเล็กทรอนิกส์ และกระบวนการนิติวิทยาศาสตร์	SEF-02.1	คุณมีแผนการรับมือกับเหตุการณ์ด้านความปลอดภัยที่จัดทำไว้เป็นเอกสารหรือไม่	โปรแกรม แผนการ และขั้นตอนสำหรับรับมือเหตุการณ์ของ AWS ได้รับการพัฒนาและทดสอบความสอดคล้องกับมาตรฐาน ISO 27001 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001 รายงาน AWS SOC จะแสดงรายละเอียดเกี่ยวกับกิจกรรมการควบคุมเฉพาะที่ดำเนินการโดย AWS
	SEF-02.2	คุณมีการผนวกรวมข้อกำหนดซึ่งกำหนดเองโดยผู้เช่าลงในแผนการรับมือเหตุการณ์ความปลอดภัยหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
บนระบบคลาวด์ *การจัดการเหตุการณ์*	SEF-02.3	คุณมีการเผยแพร่เอกสารบทบาทและความรับผิดชอบ ซึ่งระบุถึงความรับผิดชอบของคุณและผู้เช่าระหว่างเกิดเหตุการณ์ความปลอดภัยหรือไม่	ข้อมูลทั้งหมดของลูกค้าที่จัดเก็บโดย AWS มีความสามารถด้านความปลอดภัยและการควบคุมการแยกส่วนผู้เช่าที่มีประสิทธิภาพ รายละเอียดเพิ่มเติมสามารถดูได้จากจากเอกสารความปลอดภัยบน AWS Cloud (ที่ http://aws.amazon.com/security)
	SEF-02.4	คุณมีการทดสอบแผนการรับมือเหตุการณ์ความปลอดภัยของคุณในปีที่ผ่านมาหรือไม่	
การจัดการเหตุการณ์ด้านความปลอดภัย การค้นพบทางอิเล็กทรอนิกส์ และกระบวนการนิติวิทยาศาสตร์บนระบบคลาวด์ *การรายงานเหตุการณ์*	SEF-03.1	ระบบจัดการเหตุการณ์และข้อมูลความปลอดภัย (SIEM) ของคุณ ผนวกรวมแหล่งข้อมูลต่างๆ (บันทึกแอป บันทึกไฟร์วอลล์ บันทึก IDS บันทึกการเข้าถึงทางกายภาพ ฯลฯ) เพื่อใช้สำหรับการวิเคราะห์โดยละเอียดและการแจ้งเตือนหรือไม่	
	SEF-03.2	กรอบงานการบันทึกและตรวจสอบของคุณอนุญาตให้มีการแยกแยะเหตุการณ์เฉพาะของผู้เช่าแต่ละรายหรือไม่	
การจัดการเหตุการณ์ด้านความปลอดภัย การค้นพบทางอิเล็กทรอนิกส์ และกระบวนการนิติวิทยาศาสตร์บนระบบคลาวด์ *การเตรียมความพร้อมทางกฎหมายสำหรับการตอบสนองต่อเหตุการณ์*	SEF-04.1	แผนการตอบสนองต่อเหตุการณ์สอดคล้องกับมาตรฐานของอุตสาหกรรมในด้านกระบวนการจัดการความต่อเนื่องของการครอบครองรักษาวัตถุพยานที่ยอมรับได้ตามกฎหมายหรือไม่	
	SEF-04.2	ความสามารถในการตอบสนองต่อเหตุการณ์รวมถึงการใช้การรวบรวมข้อมูลเชิงนิติวิทยาศาสตร์ รวมถึงเทคนิคการวิเคราะห์ที่ยอมรับได้ตามกฎหมายหรือไม่	
	SEF-04.3	คุณมีความสามารถในการสนับสนุนการระงับการฟ้องร้อง (การตรึงข้อมูลจากระยะเวลาที่กำหนดในช่วงเวลา) สำหรับผู้เช่าเฉพาะราย โดยไม่จำเป็นต้องตรึงข้อมูลผู้เช่ารายอื่นหรือไม่	
	SEF-04.4	คุณบังคับใช้และรับรองการแยกข้อมูลของผู้เช่า เมื่อมีการยื่นข้อมูลเพื่อตอบสนองต่อหมายศาลหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
การจัดการเหตุการณ์ด้านความปลอดภัย การค้นพบทางอิเล็กทรอนิกส์ และกระบวนการนิติวิทยาศาสตร์บนระบบคลาวด์ *ตัววัดการตอบสนองต่อเหตุการณ์*	SEF-05.1	คุณตรวจสอบและแสดงปริมาณของประเภท จำนวน และผลกระทบของเหตุการณ์ด้านความปลอดภัยข้อมูลทั้งหมดหรือไม่	ตัววัดด้านความปลอดภัยของ AWS มีการตรวจสอบและวิเคราะห์โดยสอดคล้องกับมาตรฐาน ISO 27001 โปรดดู ISO 27001 ภาคผนวก A ส่วนที่ 16 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	SEF-05.2	หากมีการร้องขอ คุณจะแบ่งปันข้อมูลเชิงสถิติของข้อมูลเหตุการณ์ความปลอดภัยต่อผู้เช่าหรือไม่	
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *คุณภาพและความถูกต้องข้อมูล*	STA-01.1	คุณมีการตรวจสอบและอธิบายถึงสาเหตุของข้อผิดพลาดเชิงคุณภาพและความเสี่ยงที่เกี่ยวข้อง รวมถึงทำงานร่วมกับคู่ค้าระบบห่วงโซ่อุปทานคลาวด์เพื่อแก้ไขหรือไม่	ลูกค้าคือเจ้าของข้อมูล และเป็นผู้ควบคุมคุณภาพข้อมูล รวมถึงข้อผิดพลาดเชิงคุณภาพของข้อมูลที่อาจเกิดขึ้นผ่านการใช้งานบริการ AWS ของตนเอง โปรดดูรายงาน AWS SOC สำหรับรายละเอียดเฉพาะที่เกี่ยวข้องกับความถูกต้องข้อมูลและการจัดการการเข้าถึง (รวมถึงการเข้าถึงแบบให้สิทธิ์การใช้งานระดับต่ำสุด)
	STA-01.2	คุณออกแบบและใช้การควบคุมเพื่อลด และจำกัดความเสี่ยงความปลอดภัยข้อมูลผ่านการแบ่งแยกภาระหน้าที่อย่างเหมาะสม การเข้าถึงแบบอิงบทบาท และการเข้าถึงแบบให้สิทธิ์การใช้งานระดับต่ำสุดสำหรับพนักงานทุกภายในห่วงโซ่อุปทานหรือไม่	
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *การรายงานเหตุการณ์*	STA-02.1	คุณมีการเผยแพร่ข้อมูลเหตุการณ์ด้านความปลอดภัยแก่ลูกค้าและผู้ให้บริการที่ได้รับผลกระทบทั้งหมดเป็นระยะๆ ผ่านกระบวนการทางอิเล็กทรอนิกส์หรือไม่ (เช่น พอร์ทัล)	โปรแกรม แผนการ และขั้นตอนสำหรับรับมือเหตุการณ์ของ AWS ได้รับการพัฒนาและทดสอบความสอดคล้องกับมาตรฐาน ISO 27001 รายงาน AWS SOC จะแสดงรายละเอียดเกี่ยวกับกิจกรรมการควบคุมเฉพาะที่ดำเนินการโดย AWS รายละเอียดเพิ่มเติมสามารถดูได้จากจากเอกสารความปลอดภัยบน AWS Cloud (ที่ http://aws.amazon.com/security)
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *บริการด้านเครือข่าย / โครงสร้างพื้นฐาน*	STA-03.1	คุณเก็บรวบรวมข้อมูลความจุและการใช้งาน สำหรับองค์ประกอบทั้งหมดที่เกี่ยวข้องภายในข้อเสนอบริการระบบคลาวด์หรือไม่	AWS จัดการความจุและการใช้งานข้อมูลให้สอดคล้องกับมาตรฐาน ISO 27001 AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	STA-03.2	คุณจัดทำรายงานการวางแผนและการใช้งานความจุให้แก่ผู้เช่าหรือไม่	
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *การประเมิน*	STA-04.1	คุณดำเนินการประเมินภายในประจำปีเพื่อตรวจสอบการปฏิบัติตามและประสิทธิภาพของนโยบาย กระบวนการ รวมถึงมาตรการและตัววัดที่รองรับ	ทีมงานด้านการจัดซื้อและห่วงโซ่อุปทานจะรับหน้าที่รักษาความสัมพันธ์กับผู้จัดจำหน่ายของ AWS ทั้งหมด โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 15 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความ

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ภายในของผู้ให้บริการ		หรือไม่	สอดคล้องกับมาตรฐานการรับรอง ISO 27001
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *ข้อตกลงบริษัทภายนอก*	STA-05.1	คุณเลือกและตรวจสอบผู้ให้บริการที่เอาต์ซอร์สให้สอดคล้องกับกฎหมายประจำประเทศที่ข้อมูลมีการนำไปประมวลผล จัดเก็บ หรือส่งผ่านหรือไม่	ข้อกำหนดความปลอดภัยบุคลากรสำหรับผู้ให้บริการภายนอกที่ทำงานสนับสนุนบริการและอุปกรณ์ของ AWS มีการวางกรอบไว้ภายใต้ข้อตกลงร่วมกันที่จะไม่เปิดเผยข้อมูล ระหว่างบริษัทแม่ของ AWS คือ Amazon.com และผู้ให้บริการภายนอกที่เกี่ยวข้อง ฝ่ายปรึกษาด้านกฎหมายของ Amazon และทีมงานด้านจัดซื้อจะระบุข้อกำหนดความปลอดภัยบุคลากรสำหรับผู้ให้บริการภายนอกของ AWS ภายในข้อตกลงสัญญาระหว่างผู้ให้บริการภายนอก เกณฑ์ขั้นต่ำสุดสำหรับบุคลากรทั้งหมดที่ทำงานกับข้อมูลของ AWS คือ ต้องผ่านกระบวนการคัดกรองสำหรับการตรวจสอบภูมิหลังก่อนการทำงาน และลงนามข้อตกลงที่จะไม่เปิดเผยข้อมูล (NDA) ก่อนจะได้รับมอบสิทธิ์การเข้าถึงข้อมูลของ AWS โดยปกติแล้ว AWS จะไม่เอาต์ซอร์สการพัฒนาซอฟต์แวร์บริการของ AWS ไปยังผู้ทำสัญญาช่วง
	STA-05.2	คุณเลือกและตรวจสอบผู้ให้บริการที่เอาต์ซอร์สให้สอดคล้องกับกฎหมายประจำประเทศที่เป็นแหล่งกำเนิดต้นทางของข้อมูลหรือไม่	
	STA-05.3	ฝ่ายปรึกษาด้านกฎหมายของคุณตรวจสอบข้อตกลงกับบริษัทภายนอกทั้งหมดหรือไม่	
	STA-05.4	ข้อตกลงกับบริษัทภายนอกรวมถึงการจัดเตรียมด้านความปลอดภัยและการปกป้องข้อมูลและสินทรัพย์หรือไม่	
	STA-05.5	คุณมีการมอบรายการ รวมถึงสำเนาของข้อตกลง กระบวนการย่อยทั้งหมดให้กับลูกค้า พร้อมทั้งปรับปรุงรายละเอียดข้อมูลดังกล่าวหรือไม่	
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *การตรวจสอบการจัดการห่วงโซ่อุปทาน*	STA-06.1	คุณมีการตรวจสอบการจัดการความเสี่ยงและกระบวนการจัดการของคู่ค้า เพื่อคำนึงถึงความเสี่ยงที่สืบเนื่องจากสมาชิกรายอื่นๆ ภายในห่วงโซ่อุปทานของคู่ค้ารายดังกล่าวหรือไม่	AWS มีการวางข้อกำหนดอย่างเป็นทางการกับผู้จำหน่ายหลักภายนอก และใช้ระบบกลไกการจัดการความสัมพันธ์ที่เหมาะสม เพื่อให้สอดคล้องกับลักษณะความสัมพันธ์เชิงธุรกิจ กระบวนการจัดการบริษัทภายนอกของ AWS ได้รับการตรวจสอบอย่างสม่ำเสมอโดยผู้ตรวจสอบอิสระจากภายนอกเพื่อเป็นขั้นตอนหนึ่งของการปฏิบัติตามข้อกำหนดของ SOC และ ISO 27001
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *ตัววัดห่วงโซ่อุปทาน*	STA-07.1	มีการวางนโยบายและขั้นตอน รวมถึงมีการใช้กระบวนการเชิงธุรกิจและตัววัดเชิงเทคนิคที่รองรับ เพื่อการควบคุมข้อตกลง (เช่น SLA) ระหว่างผู้ให้บริการและลูกค้า (ผู้เช่า) ให้มีความสมบูรณ์ ถูกต้อง และเกี่ยวข้องหรือไม่	

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
	STA-07.2	คุณมีความสามารถในการวัดและตอบสนองกับการไม่ปฏิบัติตามการจัดเตรียมและ/หรือเงื่อนไขตลอดทั้งห่วงโซ่อุปทานหรือไม่ (อัพสตรีม/ดาวน์สตรีม)	
	STA-07.3	คุณสามารถจัดการกับข้อขัดแย้งหรือความไม่สอดคล้องในระดับบริการ ซึ่งเกิดจากความสัมพันธ์ที่แตกต่างกันของผู้จำหน่ายหรือไม่	
	STA-07.4	คุณมีการตรวจสอบข้อตกลง นโยบาย และกระบวนการทั้งหมดอย่างน้อยปีละหนึ่งครั้งหรือไม่	
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *การประเมินจากบริษัทภายนอก*	STA-08.1	คุณสามารถรับประกันความปลอดภัยข้อมูลอย่างเหมาะสมตลอดทั้งห่วงโซ่อุปทานข้อมูลโดยดำเนินการตรวจสอบประจำปีหรือไม่	
	STA-8.2	การตรวจสอบประจำปีของคุณรวมผู้ให้บริการภายนอก/คู่ค้าทั้งหมดที่ห่วงโซ่อุปทานข้อมูลของคุณต้องพึ่งพาหรือไม่	
การจัดการห่วงโซ่อุปทาน ความโปร่งใส และความรับผิดชอบ *การตรวจสอบจากบริษัทภายนอก*	STA-09.1	คุณอนุญาตให้ผู้เช่าทำการประเมินช่องโหว่แบบอิสระด้วยตนเองหรือไม่	ลูกค้าสามารถยื่นขออนุญาตเพื่อทำการสแกนโครงสร้างพื้นฐานระบบคลาวด์ของตนเองได้ ตราบเท่าที่การดำเนินการดังกล่าวจำกัดเฉพาะภายในอินสแตนซ์ของลูกค้าเอง และไม่เป็นการละเมิดนโยบายการใช้งานที่ยอมรับได้ของ AWS ผู้ใช้งานสามารถยื่นการอนุมัติล่วงหน้าสำหรับการสแกนเหล่านี้ โดยส่งคำขอผ่าน แบบฟอร์มการยื่นขอทดสอบการเจาะระบบ / ตรวจหาช่องโหว่ของ AWS ฝ่ายความปลอดภัยของ AWS ร่วมมือกับบริษัทด้านความปลอดภัยอิสระเพื่อดำเนินการประเมินความเสี่ยงด้านช่องโหว่จากภายนอก รายงาน AWS SOC จะแสดงรายละเอียดเพิ่มเติมเกี่ยวกับกิจกรรมการควบคุมเฉพาะที่ดำเนินการโดย AWS
	STA-09.2	คุณว่าจ้างบริการจากบริษัทภายนอก เพื่อทำการสแกนหาช่องโหว่และทดสอบการเจาะระบบแอปพลิเคชันและเครือข่ายเป็นระยะหรือไม่	
การจัดการความเสี่ยงและภัยคุกคาม *การป้องกันไวรัส / ซอฟต์แวร์*	TVM-01.1	คุณติดตั้งโปรแกรมป้องกันมัลแวร์ที่รองรับหรือเชื่อมต่อกับข้อเสนอด้านบริการระบบคลาวด์ ภายในระบบทั้งหมดหรือไม่	โปรแกรม กระบวนการ และขั้นตอนต่างๆ ของ AWS สำหรับการป้องกันไวรัส / จัดการซอฟต์แวร์ประสงค์ร้ายนั้นสอดคล้องกับมาตรฐานของ ISO 27001 โปรดดูรายงาน AWS SOC สำหรับรายละเอียดเพิ่มเติม นอกจากนี้ โปรดดูมาตรฐาน ISO 27001 ภาคผนวก A

กลุ่มการควบคุม	CID	คำถามประเมินความสอดคล้อง	คำตอบของ AWS
ประสงค์ร้าย	TVM-01.2	คุณยืนยันได้หรือไม่ว่าระบบการตรวจจับภัยคุกคามด้านความปลอดภัยที่ใช้ลายเซ็นรายการ หรือรูปแบบพฤติกรรมนั้น ได้รับการปรับปรุงภายในทุกส่วนประกอบของโครงสร้างพื้นฐานตามระยะเวลาที่เหมาะสมตามมาตรฐานอุตสาหกรรม	ส่วนที่ 12 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
การจัดการความเสี่ยงและภัยคุกคาม *การจัดการช่องโหว่ / โปรแกรมแพทช์*	TVM-02.1	คุณมีการสแกนหาช่องโหว่ในระดับชั้นเครือข่ายอย่างสม่ำเสมอ ตามที่กำหนดโดยแนวทางปฏิบัติของอุตสาหกรรมหรือไม่	ลูกค้ายังคงเป็นผู้ควบคุมระบบปฏิบัติการเยือน ซอฟต์แวร์ และแอปพลิเคชันของตนเอง รวมถึงมีหน้าที่รับผิดชอบในการสแกนหาความเสี่ยงและทำการแก้ไขข้อบกพร่องระบบของตนเอง ลูกค้าสามารถยื่นขออนุญาตเพื่อทำการสแกนโครงสร้างพื้นฐานระบบคลาวด์ของตนเองได้ ตราบเท่าที่การดำเนินการดังกล่าวจำกัดเฉพาะภายในอินสแตนซ์ของลูกค้าเอง และไม่เป็นการละเมิดนโยบายการใช้งานที่ยอมรับได้ของ AWS ระบบความปลอดภัยของ AWS จะตรวจดูที่อยู่ IP ตำแหน่งข้อมูลของบริการที่เชื่อมต่อกับอินเทอร์เน็ตทั้งหมดเป็นประจำเพื่อค้นหาความเสี่ยง ฝ่ายความปลอดภัยของ AWS จะแจ้งต่อฝ่ายที่เหมาะสมให้แก้ไขช่องโหว่ที่ระบุ โดยปกติแล้ว การบำรุงรักษาและการแก้ไขข้อบกพร่องของระบบของ AWS เองจะไม่ส่งผลกระทบกับลูกค้า โปรดดูรายละเอียดเพิ่มเติมจากเอกสารความปลอดภัยบน AWS Cloud ที่ http://aws.amazon.com/security โปรดดู มาตรฐาน ISO 27001 ภาคผนวก A ส่วนที่ 12 สำหรับรายละเอียดเพิ่มเติม AWS ผ่านการตรวจสอบและรับรองโดยผู้ตรวจสอบอิสระ เพื่อยืนยันความสอดคล้องกับมาตรฐานการรับรอง ISO 27001
	TVM-02.2	คุณมีการสแกนหาช่องโหว่ในระดับชั้นแอปพลิเคชันอย่างสม่ำเสมอ ตามที่กำหนดโดยแนวทางปฏิบัติของอุตสาหกรรมหรือไม่	
	TVM-02.3	คุณมีการสแกนหาช่องโหว่ในระดับชั้นของระบบปฏิบัติการภายในเครื่องอย่างสม่ำเสมอ ตามที่กำหนดโดยแนวทางปฏิบัติของอุตสาหกรรมหรือไม่	
	TVM-02.4	คุณจะเผยแพร่ผลลัพธ์การสแกนความเสี่ยงแก่ผู้เช่าเมื่อมีการร้องขอหรือไม่	
	TVM-02.5	คุณมีความสามารถในการแก้ไขช่องโหว่ได้อย่างรวดเร็วสำหรับอุปกรณ์การประมวล แอปพลิเคชัน และระบบทั้งหมดหรือไม่	
	TVM-02.6	คุณจะมีการเผยแพร่กรอบเวลาการแก้ไขข้อบกพร่องระบบที่อ้างอิงตามความเสี่ยงให้กับผู้เช่าหรือไม่ หากมีการร้องขอ	
การจัดการความเสี่ยงและภัยคุกคาม *โค้ดเคลื่อนที่*	TVM-03.1	มีการอนุญาตโค้ดเคลื่อนที่ก่อนนำไปติดตั้งและใช้งาน รวมถึงมีการตรวจสอบการกำหนดค่าของโค้ด เพื่อรับรองว่าโค้ดเคลื่อนที่ที่ได้รับอนุญาตสามารถใช้งานได้ตามที่ระบุโดยนโยบายด้านความปลอดภัยที่ชัดเจนหรือไม่	AWS ให้ลูกค้าสามารถจัดการแอปพลิเคชันบนไคลเอ็นต์และบนอุปกรณ์เคลื่อนที่ตามความต้องการของพวกเขาเอง
	TVM-03.2	มีการป้องกันไม่ให้โค้ดเคลื่อนที่ซึ่งไม่ได้รับอนุญาตสามารถดำเนินการได้หรือไม่	

แหล่งข้อมูลเพิ่มเติม

สำหรับข้อมูลเพิ่มเติม ดูที่แหล่งข้อมูลต่อไปนี้:

- ภาพรวมของความเสี่ยงและการปฏิบัติตามข้อกำหนดของ AWS
- การรับรอง โปรแกรม รายงานของ AWS และการยืนยันจากหน่วยงานภายนอก
- คำตอบของ AWS สำหรับคำถามเกี่ยวกับการปฏิบัติตามข้อกำหนดที่สำคัญ

การปรับปรุงเอกสาร

วันที่	คำอธิบาย
มกราคม 2017	ย้ายไปใช้เทมเพลตใหม่
มกราคม 2016	เผยแพร่ครั้งแรกเมื่อ