การรับรอง โปรแกรม รายงานของ AWS และ การยืนยันจากหน่วยงานภายนอก

มกราคม 2017

© 2017, Amazon Web Services, Inc. หรือบริษัทในเครือ สงวนลิขสิทธิ์

ประกาศ

เอกสารฉบับนี้ให้ไว้เพื่อเป็นข้อมูลเท่านั้น 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

AWS ร่วมมือกับหน่วยงานด้านการรับรองจากภายนอกและผู้ตรวจสอบอิสระ เพื่อมอบข้อมูลที่สำคัญเกี่ยวกับนโยบาย กระบวนการ และการควบคุมที่วางแผนและดำเนินงานโดย AWS ให้กับลูกค้า

CJIS

AWS ปฏิบัติตามมาตรฐานของแผนก Criminal Justice Information Services (CJIS) ของ FBI เราลงนามในข้อตกลงด้านความปลอดภัย CJIS กับลูกค้า รวมถึงยินยอมหรือให้ดำเนินการตรวจสอบภูมิหลังของพนักงานตามที่กำหนดโดยนโยบายด้านความปลอดภัยของ CJIS

ลูกค้าด้านการบังคับใช้กฎหมาย (และคู่ค้าที่จัดการ CJI) สามารถใช้ประโยชน์จากบริการของ AWS เพื่อยกระดับความปลอดภัยและการป้องกันข้อมูลของ CJI โดยใช้บริการและคุณสมบัติด้านความปลอดภัยที่ล้ำหน้าของ AWS อาทิ ระบบบันทึกกิจกรรม (AWS CloudTrail), การเข้ารหัสข้อมูลทั้งระหว่างการใช้งานและระหว่างจัดเก็บ (การเข้ารหัสฝั่งเซิร์ฟเวอร์ของ S3 พร้อมตัวเลือกในการใช้คีย์ของลูกค้าเอง), การจัดการคีย์และการป้องกันที่ครอบคลุม (AWS Key Management Service และ CloudHSM) รวมถึงการจัดการสิทธิ์แบบผนวกรวม (การจัดการข้อมูลประจำตัวแบบเชื่อมโยงของ IAM และการรับรองความถูกต้องแบบหลายปัจจัย)

AWS ได้จัดทำเอกสารคู่มือ Criminal Justice Information Services (CJIS) ในรูปแบบเทมเพลตการวางแผนความปลอดภัยที่สอดคล้องกับขอบเขตนโยบายของ CJIS นอกจากนี้ ยังได้มีการพัฒนาเอกสาร CJIS เพื่อช่วยให้คำแนะนำแก่ลูกค้าสำหรับเตรียมความพร้อมการใช้งานระบบคลาวด์

โปรดไปที่เพจฮับของ CJIS ที่ https://aws.amazon.com/compliance/cjis/

CSA

ในปี 2011 กลุ่มพันธมิตรความปลอดภัยบนระบบคลาวด์ (CSA) เริ่มต้นแผนการ STAR ซึ่งเป็นแนวคิดเพื่อส่งเสริมความโปร่งใสด้านหลักปฏิบัติความปลอดภัยภายในกลุ่มผู้ให้บริการระบบคลาวด์ CSA Security, Trust & Assurance Registry (STAR) คือรีจิสทรีฟรีที่สามารถเข้าถึงได้โดยบุคคลทั่วไป ซึ่งทำหน้าที่บันทึกการควบคุมด้านความปลอดภัยภายในข้อเสนอการประมวลผลระบบคลาวด์ต่างๆ ทั้งนี้เพื่อช่วยให้ผู้ใช้สามารถประเมินระดับความปลอดภัยของผู้ให้บริการที่ตนเองใช้อยู่ หรือกำลังพิจารณาลงนามสัญญาด้วยได้ AWS เป็นผู้ให้บริการที่ขึ้นทะเบียนกับ CSA STAR และผ่านการตอบชุดคำถาม Consensus Assessments Initiative Questionnaire (CAIQ) ของกลุ่มพันธมิตรความปลอดภัยบนระบบคลาวด์ (CSA) แล้ว ชุดคำถาม CAIQ ซึ่งเผยแพร่โดย CSA เสนอวิธีการในการอ้างอิงและบันทึกประเภทการควบคุมด้านความปลอดภัยต่างๆ ที่มี

ภายในระบบโครงสร้างพื้นฐานของ AWS ในรูปแบบข้อเสนอด้านบริการ ชุดคำถาม CAIQ ประกอบด้วยคำถาม 298 ข้อ ที่ผู้ใช้งานคลาวด์หรือผู้ตรวจสอบระบบคลาวด์อาจสอบถามจากผู้ให้บริการระบบคลาวด์

โปรดดูที่ชุดคำถาม CSA Consensus Assessments Initiative Questionnaire

Cyber Essentials Plus

Cyber Essentials Plus คือแผนการรับรองที่สนับสนุนโดยรัฐบาลอังกฤษและส่งเสริมโดยอุตสาหกรรม ซึ่งเริ่มต้นใช้งานภายในประเทศอังกฤษ โดยมีเป้าหมายเพื่อช่วยให้องค์กรแสดงให้เห็นถึงความสามารถด้านความปลอดภัยเชิงปฏิบัติการต่อการโจมตีทางไซเบอร์ที่พบได้ทั่วไป

แผนการรับรองดังกล่าวแสดงให้เห็นถึงการควบคุมแบบพื้นฐานที่ AWS ใช้เพื่อลดความเสี่ยงจากภัยคุกคามทางอินเทอร์เน็ตที่พบได้ทั่วไป ภายในบริบท “10 ขั้นตอนเพื่อความปลอดภัยทางไซเบอร์” ของรัฐบาลอังกฤษ แผนการรับรองนี้ได้รับการสนับสนุนโดยภาคอุตสาหกรรม รวมถึงสหภาพธุรกิจขนาดย่อม สมาพันธ์อุตสาหกรรมอังกฤษ และหน่วยงานด้านการประกันภัยจำนวนหนึ่ง ซึ่งมอบรางวัลจูงใจให้กับธุรกิจต่างๆ ที่ได้รับการรับรองนี้

Cyber Essentials กำหนดการควบคุมเชิงเทคนิคที่จำเป็น โดยกรอบงานการรับประกันที่เกี่ยวข้องนั้น แสดงให้เห็นว่ากระบวนการรับประกันแบบอิสระทำงานให้กับการรับรอง Cyber Essentials Plus ได้อย่างไร ผ่านการประเมินจากภายนอกประจำปีซึ่งกระทำผ่านผู้ประเมินที่ได้รับการรับรอง เนื่องด้วยลักษณะเชิงภูมิภาคของการรับรองดังกล่าว ขอบเขตการรับรองนี้จึงจำกัดเฉพาะภูมิภาคสหภาพยุโรป (ไอร์แลนด์) เท่านั้น

DoD SRG ระดับ 2 และ 4

โมเดลความปลอดภัยของระบบคลาวด์ (SRG) ของกระทรวงกลาโหมสหรัฐฯ (DoD) กำหนดการประเมินผลและกระบวนการอนุญาตอย่างเป็นทางการสำหรับผู้ให้บริการระบบคลาวด์ (CSP) เพื่อรับการอนุญาตด้านการเตรียมใช้งานจากกระทรวงกลาโหม สำหรับการใช้งานโดยลูกค้าของกระทรวง การอนุญาตด้านการเตรียมใช้งานภายใต้โมเดล SRG ให้การรับรองแบบนำกลับมาใช้ใหม่ได้ ซึ่งรับรองการปฏิบัติตามมาตรฐานของกระทรวงกลาโหมสหรัฐฯ และช่วยลดระยะเวลาที่จำเป็นสำหรับเจ้าของภารกิจ

กระทรวงกลาโหมในการประเมินและอนุญาตระบบต่างๆ เพื่อการใช้งานบน AWS ณ ปัจจุบัน AWS ได้รับการอนุญาตด้านการเตรียมใช้งานที่ระดับ 2 และ 4 ของ SRG

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับพื้นฐานการควบคุมความปลอดภัยที่กำหนดสำหรับระดับ 2, 4, 5 และ 6 สามารถดูได้ที่ http://iase.disa.mil/cloud_security/Pages/index.aspx

โปรดไปที่เพจฮับของกระทรวงกลาโหมสหรัฐฯ (DoD) ที่ https://aws.amazon.com/compliance/dod/

FedRAMP SM

AWS เป็นผู้ให้บริการระบบคลาวด์ที่ปฏิบัติตามข้อกำหนดของ Federal Risk and Authorization Management Program (FedRAMP) AWS ผ่านการทดสอบที่ดำเนินโดยหน่วยงานด้านการประเมินภายนอก (3PAO) ซึ่งรับรองโดย FedRAMP และได้รับมอบอำนาจตัวแทนในการปฏิบัติการ (ATO) สองชุดจากกระทรวงสาธารณสุขของสหรัฐฯ (HHS) หลังจากแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดของ FedRAMP ที่ระดับผลกระทบปานกลาง (Moderate) บริษัทตัวแทนของรัฐบาลสหรัฐฯ ทุกราย สามารถใช้งานแพ็คเกจ AWS Agency ATO ที่จัดเก็บภายในที่จัดเก็บของ FedRAMP เพื่อประเมิน AWS สำหรับความเหมาะสมกับแอปพลิเคชันและเวิร์กโหลด การมอบการอนุญาตเพื่อใช้งาน AWS และการโอนย้ายเวิร์กโหลดมายังสภาพแวดล้อมของ AWS ได้ Agency ATO ของ FedRAMP ทั้งสองชุดครอบคลุมภูมิภาคทั้งหมดของสหรัฐอเมริกา (ภูมิภาค AWS GovCloud (US) และภูมิภาคสหรัฐอเมริกาฝั่งตะวันออก/ตะวันตกของ AWS)

บริการต่อไปนี้อยู่ภายในขอบเขตของการรับรองของภูมิภาคตามที่ระบุด้านบน:

- **Amazon Redshift** – Amazon Redshift เป็นคลังข้อมูลในระดับเพตาไบต์ที่ได้รับการจัดการ ช่วยให้คุณสามารถวิเคราะห์ข้อมูลทั้งหมดได้ด้วยเครื่องมือ Business Intelligence ที่มีอย่างคุ้มค่าการลงทุน สำหรับข้อมูลเพิ่มเติม โปรดดู ที่นี่
- **Amazon Elastic Compute Cloud (Amazon EC2)** – Amazon EC2 มอบความสามารถในการประมวลผลที่ปรับขนาดได้ในระบบคลาวด์ EC2 ออกแบบมาเพื่อให้นักพัฒนาสามารถประมวลผลระดับเว็บได้ง่ายขึ้น สำหรับข้อมูลเพิ่มเติม โปรดดู ที่นี่

- **Amazon Simple Storage Service (S3)** – Amazon S3 มีอินเทอร์เฟสเว็บเซอร์วิสที่เรียบง่าย ซึ่งสามารถใช้เพื่อจัดเก็บและเรียกดูข้อมูลทุกขนาดจากทุกที่บนเว็บได้ตลอดเวลา สำหรับข้อมูลเพิ่มเติม โปรดดู ที่นี่
- **Amazon Virtual Private Cloud (VPC)** – Amazon VPC มอบความสามารถให้คุณเตรียมใช้งานเซกชันแบบแยกตามความสมเหตุสมผลในระบบ AWS ซึ่งคุณสามารถเปิดใช้ทรัพยากร AWS ในเครือข่ายเสมือนที่คุณกำหนดไว้ได้ สำหรับข้อมูลเพิ่มเติม โปรดดู ที่นี่
- **Amazon Elastic Block Store (EBS)** – Amazon EBS ให้ปริมาณการจัดเก็บข้อมูลที่พร้อมใช้งาน คาดการณ์ได้ และมีความน่าเชื่อถือสูง และสามารถนำไปเชื่อมต่อกับ Amazon EC2 Instance ที่ใช้งานและแสดงเป็นอุปกรณ์ภายในอินสแตนซ์ได้ สำหรับข้อมูลเพิ่มเติม โปรดดู ที่นี่
- **AWS Identity and Access Management (IAM)** – IAM ช่วยให้คุณควบคุมการเข้าถึงบริการและทรัพยากร AWS ได้อย่างปลอดภัยสำหรับผู้ใช้ IAM ช่วยให้คุณสามารถสร้างและจัดการผู้ใช้และกลุ่มของ AWS รวมถึงใช้การกำหนดสิทธิ์เพื่ออนุญาตหรือปฏิเสธการเข้าถึงทรัพยากร AWS ของผู้ใช้ได้ สำหรับข้อมูลเพิ่มเติม โปรดดู ที่นี่

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการปฏิบัติตามระเบียบ FedRAMPsm ของ AWS โปรดดูที่ คำถามที่พบบ่อยเกี่ยวกับ AWS FedRAMPsm ที่ https://aws.amazon.com/compliance/fedramp/

FERPA

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) คือกฎหมายรัฐบาลกลางว่าด้วยการคุ้มครองความเป็นส่วนตัวของบันทึกข้อมูลการศึกษาผู้เรียน กฎหมายนี้มีผลบังคับใช้กับทุกโรงเรียนที่ได้รับเงินทุนภายใต้โปรแกรมที่บังคับใช้โดยกระทรวงการศึกษาของสหรัฐฯ FERPA ให้สิทธิ์บางประการแก่ผู้ปกครองในด้านที่เกี่ยวข้องกับบันทึกข้อมูลการศึกษาของบุตรตนเอง สิทธิ์ดังกล่าวจะถูกส่งมอบให้กับผู้เรียน เมื่อผู้เรียนมีอายุครบ 18 ปี หรือเข้ารับการศึกษาในระดับสูงกว่าระดับมัธยมปลาย ผู้เรียนที่ได้รับการส่งมอบสิทธิ์แล้ว จะเรียกว่า “ผู้เรียนที่ได้รับสิทธิ์”

AWS ช่วยให้หน่วยงานที่ครอบคลุมโดย FERPA รวมถึงกลุ่มธุรกิจที่เกี่ยวข้องใช้ประโยชน์จากสภาพแวดล้อมที่ปลอดภัยของ AWS ในการดำเนินการ จัดการ และจัดเก็บข้อมูลการศึกษาที่ได้รับความคุ้มครอง

นอกจากนี้ AWS ยังมี เอกสารที่ให้ความสำคัญกับ FERPA ให้แก่ลูกค้าผู้สนใจศึกษาข้อมูลเพิ่มเติมเกี่ยวกับวิธีการใช้บริการของ AWS เพื่อดำเนินการและจัดการข้อมูลทางการศึกษา

เอกสาร FERPA Compliance on AWS (การปฏิบัติตามข้อกำหนด FERPA บน AWS) อธิบายวิธีการที่องค์กรต่างๆ สามารถใช้ AWS เพื่อดำเนินการระบบที่เอื้อต่อการปฏิบัติตามข้อกำหนด FERPA:

FIPS 140-2

Federal Information Processing Standard (FIPS) Publication 140-2 เป็นมาตรฐานความปลอดภัยของรัฐบาลสหรัฐฯ ซึ่งระบุถึงข้อกำหนดด้านความปลอดภัยสำหรับโมดูลการเข้ารหัสที่ใช้เพื่อปกป้องข้อมูลที่มีความสำคัญ เพื่อสนับสนุนลูกค้าที่ต้องปฏิบัติตามข้อกำหนด FIPS 140-2 การยกเลิก SSL ภายใน AWS GovCloud (US) นั้นทำงานโดยใช้ฮาร์ดแวร์ที่ผ่านการตรวจสอบตาม FIPS 140-2 AWS ทำงานร่วมกับลูกค้า AWS GovCloud (US) เพื่อให้ข้อมูลที่จำเป็นในการจัดการด้านการปฏิบัติตามข้อกำหนดเมื่อใช้สภาพแวดล้อมของ AWS GovCloud (สหรัฐอเมริกา)

FISMA และ DIACAP

AWS ช่วยให้บริษัทตัวแทนของรัฐบาลสหรัฐฯ ดำเนินการตามและรักษาการปฏิบัติตามข้อกำหนดของ Federal Information Security Management Act (FISMA) โครงสร้างพื้นฐานของ AWS ได้รับการประเมินโดยผู้ประเมินอิสระสำหรับระบบต่างๆ ของรัฐบาลระหว่างขั้นตอนการรับรองโดยเจ้าของระบบ หน่วยงานราชการพลเรือนและหน่วยงานของกระทรวงกลาโหมสหรัฐฯ หลายหน่วยงานได้ผ่านการอนุญาตด้านความปลอดภัยสำหรับระบบที่โฮสต์บน AWS ตามกระบวนการของกรอบงานการจัดการความเสี่ยง (RMF) ที่ระบุภายใน NIST 800-37 และ DoD Information Assurance Certification and Accreditation Process (DIACAP)

GxP

GxP เป็นอักษรย่อซึ่งหมายถึงระเบียบข้อบังคับและแนวทางปฏิบัติที่มีผลบังคับใช้กับองค์กรด้านชีววิทยาที่ผลิตอาหารและผลิตภัณฑ์ด้านการแพทย์ เช่น ยา อุปกรณ์การแพทย์ และแอปพลิเคชันซอฟต์แวร์ทางการแพทย์ เนื้อหาและวัตถุประสงค์โดยรวมของข้อกำหนด GxP คือเพื่อรับรองว่าผลิตภัณฑ์อาหารและยานั้นจะปลอดภัยกับผู้บริโภค

และเพื่อรับประกันด้านความถูกต้องแม่นยำของข้อมูลที่ใช้สำหรับการตัดสินใจด้านความปลอดภัยที่เกี่ยวข้องกับผลิตภัณฑ์

AWS มีการจัดทำ เอกสาร GxP ซึ่งระบุรายละเอียดแนวทางแบบครอบคลุมสำหรับการใช้งาน AWS กับระบบ GxP เอกสารดังกล่าวให้คำแนะนำสำหรับการใช้งาน ผลิตภัณฑ์ AWS ภายใต้บริบทของ GxP และเนื้อหาดังกล่าวได้มีการจัดทำขึ้นร่วมกับลูกค้ากลุ่มเภสัชกรรมและการแพทย์ของ AWS รวมถึงคู่ค้าด้านซอฟต์แวร์ซึ่งใช้ผลิตภัณฑ์ AWS กับระบบ GxP ที่ผ่านการตรวจสอบของตนเอง

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ GxP บนระบบ AWS โปรดติดต่อฝ่ายการขายและพัฒนาธุรกิจของ AWS

สำหรับข้อมูลเพิ่มเติม สามารถดูได้ที่คำถามที่พบบ่อยเกี่ยวกับการปฏิบัติตามข้อกำหนดของ GxP ที่ https://aws.amazon.com/compliance/gxp-part-11-annex-11/

HIPAA

AWS ช่วยให้หน่วยงานที่ครอบคลุม รวมถึงกลุ่มธุรกิจที่เกี่ยวข้องกับกฎหมาย U.S. Health Insurance Portability and Accountability Act (HIPAA) สามารถใช้สภาพแวดล้อมของ AWS เพื่อดำเนินการ รักษา และจัดเก็บข้อมูลด้านสุขภาพที่มีการคุ้มครอง และ AWS จะทำการลงนามในข้อตกลงการมีส่วนร่วมทางธุรกิจกับลูกค้าเหล่านี้ นอกจากนี้ AWS ยังเผยแพร่เอกสารที่ให้ความสำคัญกับ HIPAA แก่ลูกค้าผู้สนใจศึกษาข้อมูลเพิ่มเติมเกี่ยวกับวิธีการใช้บริการของ AWS เพื่อดำเนินการและจัดการข้อมูลทางด้านสุขภาพ เอกสาร การวางสถาปัตยกรรมสำหรับความปลอดภัย HIPAA และการปฏิบัติตามข้อกำหนดของ Amazon Web Services อธิบายถึงวิธีการที่องค์กรสามารถใช้ AWS เพื่อดำเนินระบบที่เอื้อต่อการปฏิบัติให้สอดคล้องตามข้อกำหนดของ HIPAA และ Health Information Technology for Economic and Clinical Health (HITECH)

ลูกค้าสามารถเลือกใช้บริการใดๆ ของ AWS ภายในบัญชีที่กำหนดให้เป็นบัญชี HIPAA แต่ลูกค้าควรดำเนินกระบวนการ จัดเก็บ และส่งผ่าน PHI ภายในบริการที่มีสิทธิ์ HIPAA ตามที่ระบุใน BAA เท่านั้น ณ ปัจจุบัน มีบริการเก้ารายการที่มีสิทธิ์ HIPAA ได้แก่:

- Amazon DynamoDB
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)

- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS) ซึ่งใช้งานเฉพาะเอนจิน MySQL และ Oracle
- Amazon Simple Storage Service (S3)

AWS ปฏิบัติตามโปรแกรมจัดการความเสี่ยงที่อ้างอิงตามมาตรฐาน เพื่อรับประกันว่าบริการที่มีสิทธิ์ HIPAA นั้นสนับสนุนความปลอดภัย การควบคุม และกระบวนการเชิงบริหารควบคุมที่กำหนดโดย HIPAA โดยเฉพาะ การใช้งานบริการดังกล่าวเพื่อจัดเก็บและประมวลผล PHI ช่วยให้ลูกค้าของเรารวมถึง AWS สามารถตอบสนองต่อข้อกำหนดของ HIPAA ที่ใช้กับโมเดลการดำเนินงานเชิงอรรถประโยชน์ของเราได้ AWS ให้ความสำคัญและเพิ่มบริการที่มีสิทธิ์ใหม่ๆ โดยพิจารณาจากความต้องการของลูกค้า

สำหรับข้อมูลเพิ่มเติม โปรดดูที่ คำถามที่พบบ่อยเกี่ยวกับการปฏิบัติตาม HIPAA และ การวางสถาปัตยกรรมสำหรับความปลอดภัย HIPAA และการปฏิบัติตามข้อกำหนดของ Amazon Web Services

IRAP

โปรแกรม Information Security Registered Assessors Program (IRAP) ช่วยให้ลูกค้าของรัฐบาลออสเตรเลียสามารถตรวจสอบได้ว่ามีการใช้การควบคุม รวมถึงระบุโมเดลความรับผิดชอบที่เหมาะสมเพื่อรับมือกับความต้องการตามที่ระบุในคู่มือ Australian Signals Directorate (ASD) Information Security Manual (ISM)

Amazon Web Services ผ่านการประเมินแบบอิสระ ที่กำหนดให้มีการวางมาตรการควบคุม ISM อย่างเหมาะสมทั้งหมดในส่วนที่เกี่ยวข้องกับการดำเนินการ การจัดเก็บ และการส่งผ่านของ Unclassified (DLM) สำหรับภูมิภาคซิดนีย์ของ AWS

สำหรับข้อมูลเพิ่มเติม โปรดดูที่ คำถามที่พบบ่อยเกี่ยวกับการปฏิบัติตาม IRAP ที่ https://aws.amazon.com/compliance/irap/ และความสอดคล้องของ AWS กับการพิจารณาด้านความปลอดภัยการประมวลผลระบบคลาวด์ของ Australian Signals Directorate (ASD)

ISO 9001

AWS ได้รับการรับรองตามมาตรฐาน ISO 9001, การรับรองมาตรฐาน ISO 9001 ของ AWS สนับสนุนลูกค้าซึ่งพัฒนา โอนย้าย และใช้งานระบบไอทีที่มีการควบคุมเชิงคุณภาพภายใน AWS Cloud โดยตรง ลูกค้าสามารถใช้รรายงานการปฏิบัติตามข้อกำหนดของ AWS เพื่อเป็นหลักฐานสำหรับโปรแกรม ISO 9001 ของตนเองและโปรแกรมคุณภาพเฉพาะของอุตสาหกรรม เช่น GxP สำหรับอุตสาหกรรมวิทยาศาสตร์ชีวภาพ, ISO 13485 ในกลุ่มอุปกรณ์การแพทย์, AS9100 ในกลุ่มการบินและอวกาศ และ ISO/TS 16949 ในกลุ่มยานยนต์ ลูกค้า AWS ที่ไม่มีข้อกำหนดด้านระบบคุณภาพ ก็สามารถใช้ประโยชน์จากการรับรองเพิ่มเติมและความโปร่งใสจากการรับรองตามมาตรฐาน ISO 9001 ได้เช่นกัน

การรับรองมาตรฐาน ISO 9001 ครอบคลุมระบบการจัดการคุณภาพสำหรับขอบเขตบริการ AWS และภูมิภาคการปฏิบัติการ (ด้านล่าง) และการให้บริการเฉพาะ ดังนี้

- AWS CloudFormation
- AWS Cloud Hardware Security Model (HSM)
- Amazon CloudFront
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache

- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service (SWF)
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- โครงสร้างพื้นฐานเชิงกายภาพที่สำคัญและสภาพแวดล้อมการจัดการของ AWS

การรับรองมาตรฐาน ISO 9001 ของ AWS ครอบคลุมภูมิภาคของ AWS ดังนี้ สหรัฐอเมริกาฝั่งตะวันออก (เวอร์จิเนียตอนเหนือ), สหรัฐอเมริกาฝั่งตะวันตก (โอริกอน), สหรัฐอเมริกาฝั่งตะวันตก (แคลิฟอร์เนียตอนเหนือ), AWS GovCloud (สหรัฐอเมริกา), อเมริกาใต้ (เซาเปาโล), สหภาพยุโรป (ไอร์แลนด์), สหภาพยุโรป (แฟรงก์เฟิร์ต), เอเชียแปซิฟิก (สิงคโปร์), เอเชียแปซิฟิก (ซิดนีย์) และเอเชียแปซิฟิก (โตเกียว)

ISO 9001:2008 เป็นมาตรฐานระดับสากลสำหรับการจัดการคุณภาพของผลิตภัณฑ์และบริการ มาตรฐาน 9001 กำหนดระบบการจัดการคุณภาพ โดยอ้างอิงจากหลักการแปดประการ ซึ่งระบุโดยคณะกรรมการด้านเทคนิคสำหรับการจัดการและการรับประกันด้านคุณภาพแห่งองค์การระหว่างประเทศว่าด้วยการวางมาตรฐาน (ISO) หลักการดังกล่าวประกอบด้วย

- การให้ความสำคัญกับลูกค้า
- การเป็นผู้นำ
- การมีส่วนร่วมของประชาชน
- แนวทางการดำเนินการ
- แนวทางของระบบในการจัดการ
- การพัฒนาอย่างต่อเนื่อง
- แนวทางการตัดสินใจโดยอิงกับข้อเท็จจริง
- ความสัมพันธ์กับผู้จำหน่ายที่เอื้อประโยชน์ร่วมกัน

สามารถดาวน์โหลดการรับรองมาตรฐาน ISO 9001 ของ AWS ได้ที่ https://d0.awsstatic.com/certifications/iso_9001_certification.pdf

นอกจากนี้ AWS ยังมีข้อมูลเพิ่มเติม รวมถึงคำถามที่พบบ่อยเกี่ยวกับการรับรองมาตรฐาน ISO 9001 ซึ่งดูได้ที่ https://aws.amazon.com/compliance/iso-9001-faqs/

ISO 27001

AWS ได้รับการรับรองมาตรฐาน ISO 27001 สำหรับระบบการจัดการความปลอดภัยข้อมูล (ISMS) ของเรา ซึ่งครอบคลุมระบบโครงสร้างพื้นฐานของ AWS, ศูนย์ข้อมูล และบริการดังต่อไปนี้

- AWS CloudFormation
- Amazon CloudFront
- AWS Cloudtrail
- AWS Directory Service
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- AWS Direct Connect

- Amazon EC2 VM Import/Export
- AWS Cloud Hardware Security Model (HSM)
- Elastic Load Balancing (ELB)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- โครงสร้างพื้นฐานเชิงกายภาพที่สำคัญ (รวมถึง GovCloud) และสภาพแวดล้อมการจัดการของ AWS

ISO 27001/27002 เป็นมาตรฐานความปลอดภัยสากลที่มีการใช้งานอย่างกว้างขวาง และเป็นตัววางข้อกำหนดและแนวทางปฏิบัติมาตรฐานสำหรับแนวทางอย่างเป็นระบบ เพื่อใช้

จัดการข้อมูลองค์กรและข้อมูลลูกค้า โดยอาศัยการอ้างอิงการประเมินความเสี่ยงเป็นระยะให้เหมาะสมกับสถานการณ์ภัยคุกคามที่มีการเปลี่ยนแปลงอย่างไม่หยุดยั้ง เพื่อให้ได้มาซึ่งการรับรองดังกล่าว องค์กรต้องพิสูจน์ให้เห็นได้ว่ามีการแนวทางอย่างเป็นระบบและต่อเนื่องสำหรับการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลซึ่งส่งผลกับการรักษาความลับ ความถูกต้อง และความพร้อมใช้งานข้อมูล ทั้งขององค์กรและของลูกค้า การรับรองนี้เป็นสิ่งยืนยันถึงความมุ่งมั่นของ Amazon ในการให้ข้อมูลที่สำคัญเกี่ยวกับการควบคุมและแนวทางปฏิบัติด้านความปลอดภัยของเรา

การรับรองมาตรฐาน ISO 27001 ของ AWS ครอบคลุมภูมิภาคของ AWS ดังนี้ สหรัฐอเมริกาฝั่งตะวันออก (เวอร์จิเนียตอนเหนือ), สหรัฐอเมริกาฝั่งตะวันตก (โอริกอน), สหรัฐอเมริกาฝั่งตะวันตก (แคลิฟอร์เนียตอนเหนือ), AWS GovCloud (สหรัฐอเมริกา), อเมริกาใต้ (เซาเปาโล), สหภาพยุโรป (ไอร์แลนด์), สหภาพยุโรป (แฟรงก์เฟิร์ต), เอเชียแปซิฟิก (สิงคโปร์), เอเชียแปซิฟิก (ซิดนีย์) และเอเชียแปซิฟิก (โตเกียว)

สามารถดาวน์โหลดการรับรอง ISO 27001 ของ AWS ได้ที่ https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf

นอกจากนี้ AWS ยังมีข้อมูลเพิ่มเติม รวมถึงคำถามที่พบบ่อยเกี่ยวกับการรับรองมาตรฐาน ISO 27001 ซึ่งดูได้ที่ https://aws.amazon.com/compliance/iso-27001-faqs/

ISO 27017

ISO 27017 เป็นหลักปฏิบัติล่าสุดที่เผยแพร่โดยองค์การระหว่างประเทศว่าด้วยการวางมาตรฐาน (ISO) หลักปฏิบัตินี้ให้คำแนะนำในการใช้การควบคุมความปลอดภัยข้อมูลที่เกี่ยวข้องกับบริการระบบคลาวด์โดยเฉพาะ

AWS ได้รับการรับรองมาตรฐาน ISO 27017 สำหรับระบบการจัดการความปลอดภัยข้อมูล (ISMS) ของเรา ซึ่งครอบคลุมระบบโครงสร้างพื้นฐานของ AWS, ศูนย์ข้อมูล และบริการดังต่อไปนี้

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)

- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway

- AWS WAF (ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน)
- Elastic Load Balancing
- VM Import/Export

สามารถดาวน์โหลดการรับรองมาตรฐาน ISO 27017 ของ AWS ได้ที่ https://d0.awsstatic.com/certifications/iso_27017_certification.pdf

นอกจากนี้ AWS ยังมีการเผยแพร่ข้อมูลเพิ่มเติม รวมถึงคำถามที่พบบ่อยเกี่ยวกับการรับรองมาตรฐาน ISO 27017 ซึ่งดูได้ที่ https://aws.amazon.com/compliance/iso-27017-faqs/

ISO 27018

ISO 27018 เป็นหลักปฏิบัติสากลชุดแรกที่มุ่งให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลบนระบบคลาวด์ หลักปฏิบัติดังกล่าวมีพื้นฐานจากมาตรฐานการรักษาความปลอดภัยข้อมูล ISO 27002 และให้คำแนะนำในการใช้การควบคุมของ ISO 27002 ซึ่งสามารถใช้ได้กับข้อมูลที่ระบุตัวคนได้ (PII) บนระบบคลาวด์สาธารณะ นอกจากนี้ ยังมีชุดการควบคุมเพิ่มเติมรวมถึงคำแนะนำที่เกี่ยวข้อง โดยมีเป้าหมายสำหรับจัดการกับการป้องกันข้อมูล PII บนระบบคลาวด์สาธารณะในขอบข่ายที่ยังไม่ครอบคลุมโดยชุดการควบคุมของมาตรฐาน ISO 27002

AWS ได้รับการรับรองมาตรฐาน ISO 27018 สำหรับระบบการจัดการความปลอดภัยข้อมูล (ISMS) ของเราซึ่งครอบคลุมระบบโครงสร้างพื้นฐานของ AWS, ศูนย์ข้อมูล และบริการดังต่อไปนี้

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache

- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน)
- Elastic Load Balancing
- VM Import/Export

สามารถดาวน์โหลดการรับรองมาตรฐาน ISO 27018 ของ AWS ได้ที่
https://d0.awsstatic.com/certifications/iso_27018_certification.pdf

นอกจากนี้ AWS ยังรวบรวมข้อมูลเพิ่มเติม รวมถึงคำถามที่พบบ่อยเกี่ยวกับการรับรองมาตรฐาน ISO 27018 ซึ่งดูได้ที่ https://aws.amazon.com/compliance/iso-27018-faqs/

ITAR

ภูมิภาค AWS GovCloud (US) สนับสนุนการปฏิบัติตามระเบียบข้อบังคับว่าด้วยการควบคุมการขนส่งอาวุธนานาชาติของสหรัฐฯ (ITAR) ในฐานะส่วนหนึ่งของการจัดการโปรแกรมการปฏิบัติตามระเบียบของ ITAR อย่างครอบคลุม องค์กรที่อยู่ภายใต้ข้อกำหนดด้านการส่งออกของ ITAR จะต้องควบคุมการส่งออกที่ไม่ได้ตั้งใจ โดยจำกัดการเข้าถึงข้อมูลที่ได้รับการคุ้มครองให้กับประชาชนสหรัฐฯ และจำกัดการเข้าถึงตำแหน่งที่ตั้งทางกายภาพของข้อมูลเฉพาะประเทศสหรัฐฯ เท่านั้น AWS GovCloud (สหรัฐอเมริกา) มอบสภาพแวดล้อมที่มีที่ตั้งทางกายภาพอยู่ภายในสหรัฐฯ และจำกัดการเข้าถึงได้โดยบุคลากรของ AWS ที่เป็นประชาชนสหรัฐฯ เท่านั้น จึงทำให้บริษัทที่มีคุณสมบัติเหมาะสมสามารถส่งผ่าน ดำเนินการ และจัดเก็บข้อมูลและบทความที่มีการป้องกันตามข้อกำหนดของ ITAR ได้ สภาพแวดล้อมของ AWS GovCloud (US) ได้รับการตรวจสอบโดยบริษัทอิสระจากภายนอก เพื่อรับรองว่ามีการใช้การควบคุมที่เหมาะสมต่อการปฏิบัติตามข้อกำหนดโปรแกรมการส่งออกตามข้อกำหนดนี้

MPAA

สมาคมภาพยนต์อเมริกัน (MPAA) ได้กำหนดชุดของแนวทางปฏิบัติมาตรฐานเพื่อใช้สำหรับการจัดเก็บ ประมวลผล และส่งมอบเนื้อหาสื่อที่มีการคุ้มครองอย่างปลอดภัย (http://www.fightfilmtheft.org/facility-security-program.html) บริษัทด้านสื่อใช้แนวทางปฏิบัติมาตรฐานนี้เพื่อการประเมินความเสี่ยงและความปลอดภัยของเนื้อหา รวมถึงโครงสร้างพื้นฐานของตนเอง AWS ได้พิสูจน์ให้เห็นถึงการดำเนินการสอดคล้องกับแนวทางปฏิบัติมาตรฐานของ MPAA และโครงสร้างพื้นฐานของ AWS ก็มีความสอดคล้องตามการควบคุมด้านโครงสร้างพื้นฐานของ MPAA ที่ใช้งานทั้งหมด แม้ว่าทาง MPAA จะไม่มีการเสนอ “การรับรอง” ใดๆ แต่ลูกค้าภาคอุตสาหกรรมสื่อก็สามารถใช้เอกสาร MPAA ของ AWS สำหรับเสริมการประเมินความเสี่ยง และการประเมินเนื้อหาประเภท MPAA บน AWS ได้

โปรดดูรายละเอียดเพิ่มเติมจากเพจฮับการปฏิบัติตาม MPAA ของ AWS ที่ https://aws.amazon.com/compliance/mpaa/

การรับรอง MTCS Tier 3

ระบบความปลอดภัยบนคลาวด์แบบมัลติเทียร์ (MTCS) เป็นมาตรฐานการจัดการด้านความปลอดภัยเชิงปฏิบัติการของประเทศสิงคโปร์ (SPRING SS 584:2013) ซึ่งอ้างอิงจากมาตรฐานของระบบการจัดการความปลอดภัยข้อมูล (ISMS) ของ ISO 27001/02 การประเมินการรับรองนี้ กำหนดให้ Amazon ดำเนินกิจกรรมต่อไปนี้

- ประเมินความเสี่ยงด้านความปลอดภัยข้อมูลของเราอย่างเป็นระบบ โดยคำนึงถึงผลกระทบของภัยคุกคามและความเสี่ยงขององค์กร
- ออกแบบและใช้งานชุดการควบคุมความปลอดภัยข้อมูลโดยครอบคลุม รวมถึงใช้การจัดการความเสี่ยงในรูปแบบอื่นๆ เพื่อจัดการกับความเสี่ยงด้านความปลอดภัยขององค์กรและสถาปัตยกรรม
- ใช้กระบวนการจัดการที่ครอบคลุม เพื่อรับประกันว่าการควบคุมความปลอดภัยข้อมูลนั้นสอดคล้องกับความต้องการด้านความปลอดภัยข้อมูลของเราอย่างสม่ำเสมอ

โปรดดูเพจฮับของ MTCS ที่ https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/

NIST

ในเดือนมิถุนายนปี 2015 สถาบันแห่งชาติด้านมาตรฐานและและเทคโนโลยี (NIST) ได้เผยแพร่แนวทางปฏิบัติ 800-171 “แนวทางปฏิบัติฉบับสมบูรณ์สำหรับการป้องกันข้อมูลของรัฐบาลที่สำคัญซึ่งจัดเก็บโดยผู้รับเหมา” คำแนะนำดังกล่าวมีผลบังคับใช้กับการป้องกันข้อมูลที่ไม่เป็นความลับซึ่งมีการควบคุม (CUI) บนระบบที่ไม่ใช่ของรัฐ

AWS ปฏิบัติตามแนวทางปฏิบัติดังกล่าวอยู่แล้ว และลูกค้าสามารถปฏิบัติตามข้อกำหนดของ NIST 800-171 ได้อย่างมีประสิทธิภาพโดยทันที แนวทางปฏิบัติ NIST 800-171 อธิบายส่วนย่อยของข้อกำหนด NIST 800-53 ซึ่งเป็นแนวทางปฏิบัติที่ AWS ได้ผ่านการตรวจสอบแล้วภายใต้โปรแกรมของ FedRAMP พื้นฐานการควบคุมความปลอดภัย FedRAMP Moderate นั้นมีความเข้มงวดกว่าข้อกำหนดที่แนะนำตามรายละเอียดในบทที่ 3 ของคำแนะนำ 800-171 และมีการรวมเอาการควบคุมความปลอดภัยจำนวนมาก ซึ่งเกินกว่าที่ระบุโดยระบบ FISMA Moderate ที่ป้องกันข้อมูล CUI สามารถดูการเชื่อมโยงโดยละเอียดได้ภายในเอกสาร NIST Special Publication 800-171 เริ่มต้นที่หน้า D2 (หรือหน้า 37 ของเอกสาร PDF)

PCI DSS ระดับ 1

AWS มีความสอดคล้องตามระดับ 1 (Level 1) ตามมาตรฐานการรักษาความปลอดภัยสำหรับอุตสาหกรรมการชำระเงินผ่านบัตรเครดิต (PCI DSS) ลูกค้าสามารถรันแอปพลิเคชันบนโครงสร้างพื้นฐานเทคโนโลยีที่สอดคล้องกับข้อกำหนด PCI เพื่อใช้จัดเก็บ ประมวลผล และส่งผ่านข้อมูลบัตรเครดิตในระบบคลาวด์ได้ เมื่อเดือนกุมภาพันธ์ 2013 คณะกรรมการมาตรฐานด้านความปลอดภัยของ PCI ได้เผยแพร่หลักเกณฑ์การประมวลผลแบบคลาวด์สำหรับ PCI DSS หลักเกณฑ์ดังกล่าวให้รายละเอียดแก่ลูกค้าที่จัดการสภาพแวดล้อมข้อมูลผู้ถือบัตร เพื่อการพิจารณาวิธีการรักษาการควบคุม PCI DSS ในระบบคลาวด์ AWS ได้นำหลักเกณฑ์การประมวลผลบนระบบคลาวด์ของ PCI DSS มารวมไว้ภายในแพ็คเกจ AWS PCI Compliance Package สำหรับลูกค้า แพ็คเกจ AWS PCI Compliance Package ประกอบด้วย เอกสารยืนยันการปฏิบัติตามมาตรฐาน (AoC) PCI ของ AWS ซึ่งแสดงให้เห็นว่า AWS ได้ผ่านการรับรองตามมาตรฐานของการเป็นผู้ให้บริการระดับ Level 1 ภายใต้เงื่อนไข PCI DSS เวอร์ชัน 3.1 และเอกสารสรุปความรับผิดชอบของ PCI ของ AWS ซึ่งอธิบายถึงวิธีการรับผิดชอบร่วมกันด้านการปฏิบัติตามข้อกำหนดระหว่าง AWS และลูกค้าบนระบบคลาวด์

บริการด้านล่างต่อไปนี้รวมอยู่ในขอบเขตสำหรับ PCI DSS Level 1

- Auto Scaling
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)

- Amazon Glacier
- AWS Key Management Service (KMS)
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Workflow Service SWF
- Amazon Virtual Private Cloud (VPC)
- **โครงสร้างพื้นฐานเชิงกายภาพที่สำคัญ (รวมถึง GovCloud) และสภาพแวดล้อมการจัดการของ AWS**

ขอบเขตการให้บริการและภูมิภาคสำหรับการรับรอง AWS PCI DSS Level 1 ฉบับล่าสุดสามารถดูได้ที่ https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

SOC 1/ISAE 3402

Amazon Web Services เผยแพร่รายงาน Service Organization Controls 1 (SOC 1), Type II การตรวจสอบสำหรับรายงานดังกล่าวดำเนินการโดยมีความสอดคล้องตามข้อกำหนดสถาบันผู้สอบบัญชีรับอนุญาตของประเทศสหรัฐอเมริกา (AICPA) ดังนี้: AT 801 (เดิมคือ SSAE 16) และ International Standards for Assurance Engagements No. 3402 (ISAE 3402) รายงานแบบมาตรฐานร่วมฉบับนี้ มีวัตถุประสงค์เพื่อให้ตรงตามข้อกำหนดด้านการตรวจสอบทางการเงินที่หลากหลายของหน่วยงานการตรวจสอบของสหรัฐฯ และหน่วยงานสากล การตรวจสอบรายงาน SOC 1 ยืนยันว่าวัตถุประสงค์การควบคุมของ AWS มีการวางแผนอย่างเหมาะสม และการควบคุมแต่ละรายการที่ระบุเพื่อการปกป้องข้อมูลลูกค้านั้นทำงานได้อย่างมีประสิทธิภาพ รายงานฉบับนี้เป็นเอกสารที่ใช้แทนรายงาน Statement on Auditing Standards No. 70 (SAS 70) Type II

วัตถุประสงค์การควบคุมของ AWS SOC 1 มีการระบุไว้ที่นี่ ข้อมูลในรายงานเอง ระบุถึงกิจกรรมการควบคุมที่สนับสนุนวัตถุประสงค์แต่ละข้อเหล่านี้ และผลลัพธ์ของกระบวนการทดสอบการควบคุมแต่ละรายการจากผู้ตรวจสอบอิสระ

ขอบข่ายวัตถุประสงค์	คำอธิบายวัตถุประสงค์
องค์กรด้านความปลอดภัย	มีการควบคุมที่เหมาะสมเพียงพอ เพื่อรับประกันว่ามีการวางแผนและสื่อสารนโยบายด้านความปลอดภัยข้อมูลตลอดทั่วทั้งองค์กร
การเข้าถึงของผู้ใช้ที่เป็นพนักงาน	มีการควบคุมที่เหมาะสมเพียงพอ เพื่อรับประกันว่ามีการวางขั้นตอนต่างๆ สำหรับการเพิ่ม แก้ไข และลบบัญชีผู้ใช้ที่เป็นพนักงานของ Amazon อย่างทันท่วงที และมีการตรวจสอบเป็นระยะ
ความปลอดภัยลอจิคัล	มีการควบคุมที่เหมาะสมเพียงพอ เพื่อรับประกันว่ามีการกำหนดนโยบายและระบบกลไกเพื่อจำกัดการเข้าถึงข้อมูลอย่างเหมาะสม ทั้งจากภายนอกและภายใน และข้อมูลลูกค้ามีการแยกออกจากข้อมูลลูกค้ารายอื่นอย่างเหมาะสม
การจัดการข้อมูลแบบปลอดภัย	มีการควบคุมที่เหมาะสมเพียงพอ เพื่อรับประกันว่าการจัดการข้อมูลระหว่างจุดเริ่มต้นของลูกค้ามายังตำแหน่งจัดเก็บของ AWS นั้นมีความปลอดภัยและมีการแม็ปอย่างแม่นยำ
ความปลอดภัยเชิงกายภาพและการป้องกันทางสภาพแวดล้อม	มีการควบคุมที่เหมาะสมเพียงพอ เพื่อรับประกันว่าการเข้าถึงข้อมูลทางกายภาพมีการจำกัดเฉพาะบุคลากรที่ได้รับอนุญาต และมีการวางระบบกลไกไว้เพื่อลดผลกระทบจากการทำงานผิดพลาด หรือความเสียหายเชิงกายภาพต่อสถานที่ของศูนย์ข้อมูล
การจัดการการเปลี่ยนแปลง	มีการควบคุมที่เหมาะสมเพียงพอ เพื่อรับประกันว่าการเปลี่ยนแปลงใดๆ (รวมถึงกรณีฉุกเฉิน / ไม่เป็นไปตามกำหนดการ และการกำหนดค่า) ที่เกิดขึ้นกับทรัพยากรด้านไอทีที่มีอยู่ จะมีการบันทึก อนุญาต ทดสอบ อนุมัติ และจัดทำเอกสารไว้
ความถูกต้องข้อมูล ความพร้อมใช้งาน และการสำรองการทำงาน	มีการควบคุมที่เหมาะสมเพียงพอ เพื่อรับประกันว่ามีการดูแลความถูกต้องข้อมูลในทุกขั้นตอน รวมถึงระหว่างการส่งข้อมูล การจัดเก็บ และการประมวลผล
การรับมือกับเหตุการณ์	มีการควบคุมที่เหมาะสมเพียงพอ เพื่อรับประกันว่าเหตุการณ์ใดๆ ที่เกิดขึ้นกับระบบจะได้รับการลงบันทึก วิเคราะห์ และแก้ไข

รายงาน SOC 1 ออกแบบมาเพื่อให้ความสำคัญกับการควบคุมภายในองค์กรด้านการบริการ ซึ่งมีแนวโน้มจะเกี่ยวข้องกับการตรวจสอบรายงานทางการเงินของหน่วยงานลูกค้า เนื่องจากกลุ่มฐานลูกค้าของ AWS นั้นกว้างขวางอย่างมาก และบริการของ AWS ก็มีการใช้งานอย่างกว้างขวางเช่นกัน การใช้ประโยชน์ด้านการควบคุมสำหรับรายงานทางการเงินของลูกค้านั้นจึงแตกต่างไปในแต่ละราย ดังนั้น รายงาน AWS SOC 1 จึงออกแบบมาเพื่อครอบคลุมการควบคุมหลักๆ โดยเฉพาะ โดยเน้นที่การควบคุมซึ่งมีแนวโน้มจำเป็นต่อการตรวจสอบทางด้านการเงิน รวมถึงครอบคลุมการควบคุมทั่วไปด้านไอที เพื่อรองรับสถานการณ์ด้านการใช้งานและการตรวจสอบที่หลากหลาย สิ่งนี้ช่วยให้ลูกค้าสามารถใช้โครงสร้างพื้นฐาน AWS เพื่อจัดเก็บและประมวลผลข้อมูลที่สำคัญ รวมถึงข้อมูลซึ่งเป็นองค์ประกอบที่จำเป็นภายในขั้นตอนการรายงานทางการเงิน AWS มีการประเมินรายการควบคุมเหล่านี้เป็นระยะ เพื่อพิจารณาถึงความคิดเห็นลูกค้าและการใช้งานรายงานการตรวจสอบที่สำคัญนี้

AWS มีความมุ่งมั่นในการปรับปรุงรายงาน SOC 1 อย่างต่อเนื่อง และจะดำเนินการตรวจสอบแบบเป็นระยะเช่นนี้ต่อไป ขอบเขตเนื้อหาของรายงาน SOC 1 ครอบคลุมหัวข้อดังนี้:

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- Amazon Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)

- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow (SWF)
- Amazon Simple Queue Service (SQS)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- Amazon Workspaces

SOC 2

นอกจากรายงาน SOC 1 แล้ว AWS ยังเผยแพร่รายงาน Service Organization Controls 2 (SOC 2), Type II ด้วย รายงาน SOC 2 นั้นคล้ายคลึงกับรายงาน SOC 1 ในด้านการประเมินการควบคุม อย่างไรก็ตาม รายงาน SOC 2 เป็นรายงานการยืนยันที่ขยายการประเมินการควบคุมเพื่อให้ครอบคลุมชุดเกณฑ์ที่กำหนดโดย Trust Services Principles ของสถาบันผู้สอบบัญชีรับอนุญาตของประเทศสหรัฐอเมริกา (AICPA) หลักการดังกล่าวระบุการแนวทางการควบคุมชั้นนำที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน ความถูกต้องในการประมวลผล การเก็บรักษาความลับ และความเป็นส่วนตัว ซึ่งมีผลกับองค์กรด้านบริการเช่น AWS รายงาน AWS SOC 2 เป็นการประเมินความมีประสิทธิภาพในการออกแบบและการปฏิบัติการของการควบคุม ซึ่งสอดคล้องกับเกณฑ์ด้านความปลอดภัยและหลักการด้านความพร้อมใช้งานที่กำหนดไว้ภายในเกณฑ์ Trust Services Principles ของ AICPA รายงานนี้ช่วยเพิ่มความโปร่งใส่ให้กับความปลอดภัยและความพร้อมใช้งานของ AWS โดยอ้างอิงตามมาตรฐานแนวทางปฏิบัติชั้นนำทางอุตสาหกรรมที่วางไว้ และเป็นสิ่งยืนยันเพิ่มเติมถึงความมุ่งมั่นของ AWS ในการปกป้องข้อมูลลูกค้า ขอบเขตของรายงาน SOC 2 ครอบคลุมบริการเดียวกันกับที่ครอบคลุมโดยรายงาน SOC 1 โปรดดูคำอธิบายรายงาน SOC 1 ด้านบนเพื่อดูบริการที่อยู่ภายในขอบเขต

SOC 3

AWS เผยแพร่รายงาน Service Organization Controls 3 (SOC 3) รายงาน SOC 3 เป็นเอกสารสรุปรายงาน AWS SOC 2 ที่บุคคลทั่วไปสามารถดูได้ รายงานดังกล่าวประกอบด้วยความคิดเห็นของผู้ตรวจสอบภายนอกเกี่ยวกับปฏิบัติการของมาตรการควบคุม (อ้างอิงจาก Security Trust Principles ของ AICPA ที่รวมไว้ภายในรายงาน SOC 2) การยืนยันจากฝ่ายบริหารของ AWS ในหัวข้อเกี่ยวกับประสิทธิภาพของมาตรการควบคุม และภาพรวมของโครงสร้างพื้นฐานและบริการของ AWS รายงาน AWS SOC 3 ครอบคลุมศูนย์ข้อมูลของ AWS ทั้งหมดทั่วโลกที่สนับสนุนบริการที่อยู่ภายในขอบเขต เอกสารรายงานนี้เป็นทรัพยากรที่มีประโยชน์สำหรับลูกค้าเพื่อใช้ตรวจสอบว่า AWS ได้รับการรับประกันจากผู้ตรวจสอบภายนอก โดยไม่จำเป็นต้องดำเนินขั้นตอนยื่นขอรายงาน SOC 2 ขอบเขตของรายงาน SOC 3 ครอบคลุมบริการเดียวกันกับที่ครอบคลุมโดยรายงาน SOC 1 โปรดดูคำอธิบายรายงาน SOC 1 ด้านบนเพื่อดูบริการที่อยู่ภายในขอบเขต สามารถดูรายงาน AWS SOC 3 ได้ ที่นี่

แหล่งข้อมูลเพิ่มเติม

สำหรับข้อมูลเพิ่มเติม ดูที่แหล่งข้อมูลต่อไปนี้:

- ภาพรวมของความเสี่ยงและการปฏิบัติตามข้อกำหนดของ AWS
- คำตอบของ AWS สำหรับคำถามเกี่ยวกับการปฏิบัติตามข้อกำหนดที่สำคัญ
- ชุดคำถาม CSA Consensus Assessments Initiative Questionnaire

การปรับปรุงเอกสาร

วันที่	คำอธิบาย
มกราคม 2017	ย้ายไปใช้เทมเพลตใหม่
มกราคม 2016	เผยแพร่ครั้งแรกเมื่อ