คำตอบของ AWS
สำหรับคำถามเกี่ยวกับ
การปฏิบัติตามข้อกำหนดที่สำคัญ

มกราคม 2017


amazon
web services

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

เอกสารฉบับนี้เป็นการตอบคำถามที่พบได้บ่อยเกี่ยวกับการปฏิบัติตามข้อกำหนดสำหรับการประมวลผลบนระบบคลาวด์ที่เกี่ยวข้องกับ AWS คำตอบของคำถามเหล่านี้อาจน่าสนใจเมื่อมีการประเมินผลและใช้งานสภาพแวดล้อมการประมวลผลบนระบบคลาวด์และสามารถช่วยในการจัดการด้านการควบคุมของลูกค้า AWS

คำถามและคำตอบเกี่ยวกับการปฏิบัติตามข้อกำหนดที่สำคัญ

ประเภท	คำถามเกี่ยวกับการประมวลผลบนระบบคลาวด์	ข้อมูลของ AWS
ความเป็นเจ้าของในการควบคุม	ใครเป็นเจ้าของการควบคุมสำหรับโครงสร้างพื้นฐานที่ใช้ระบบคลาวด์	สำหรับส่วนที่ใช้งานใน AWS นั้น AWS จะควบคุมส่วนประกอบทางกายภาพของเทคโนโลยีนั้น ลูกค้าเป็นเจ้าของและควบคุมส่วนอื่นๆ ที่เหลือ รวมถึงการควบคุมจุดเชื่อมต่อและการส่งผ่าน เพื่อช่วยให้ลูกค้าเข้าใจได้ดียิ่งขึ้นเกี่ยวกับการควบคุมที่เรามีอยู่และการควบคุมเหล่านั้นสามารถทำงานได้มีประสิทธิภาพเพียงใด เราเผยแพร่รายงาน SOC 1 Type II พร้อมการควบคุมที่กำหนดไว้สำหรับ EC2, S3 และ VPC รวมทั้งการควบคุมความปลอดภัยทางกายภาพและทางสภาพแวดล้อมอย่างละเอียด การควบคุมเหล่านี้กำหนดความจำเพาะที่ระดับสูงซึ่งควรตอบสนองต่อความต้องการของลูกค้าได้มากที่สุด ลูกค้า AWS ที่ลงนามในข้อตกลงที่จะไม่เปิดเผยข้อมูลกับ AWS สามารถขอรับสำเนาของรายงาน SOC 1 Type II ได้
การตรวจสอบด้านไอที	การตรวจสอบของผู้ให้บริการระบบคลาวด์สามารถทำได้อย่างไร	การตรวจสอบเลเยอร์และการควบคุมส่วนใหญ่ที่อยู่เหนือการควบคุมทางกายภาพจะยังคงเป็นหน้าที่ของลูกค้า ข้อกำหนดของการควบคุมแบบลอจิคัลและกายภาพที่กำหนดโดย AWS มีการบันทึกไว้ในรายงาน SOC 1 Type II และทีมตรวจสอบและการปฏิบัติตามข้อกำหนดสามารถทบทวนรายงานนั้นได้ นอกจากนี้ยังมี AWS ISO 27001 และการรับรองอื่นๆ ให้ผู้ตรวจสอบทบทวนด้วยเช่นกัน
การปฏิบัติตามข้อกำหนด Sarbanes-Oxley	การปฏิบัติตามข้อกำหนด SOX ทำได้อย่างไร หากมีการใช้ระบบที่อยู่ในขอบเขตในสภาพแวดล้อมของผู้ให้บริการระบบคลาวด์	หากลูกค้าประมวลผลข้อมูลทางการเงินใน AWS Cloud ผู้ตรวจสอบของลูกค้าสามารถตรวจสอบดูว่าระบบ AWS บางส่วนอยู่ภายในขอบเขตของข้อกำหนด Sarbanes-Oxley (SOX) หรือไม่ ผู้ตรวจสอบของลูกค้าต้องตัดสินใจเกี่ยวกับความสามารถในการนำมาใช้สำหรับ SOX ด้วยตนเอง เนื่องจากการควบคุมการเข้าถึงแบบลอจิคัลส่วนใหญ่มีการจัดการโดยลูกค้า ลูกค้าจึงเป็นผู้ที่เหมาะสมที่สุดในการตัดสินว่ากิจกรรมการควบคุมตรงกับมาตรฐานที่เกี่ยวข้องกันหรือไม่ หากผู้ตรวจสอบ SOX ร้องขอเป็นการเฉพาะเกี่ยวกับการควบคุมทางกายภาพของ AWS พวกเขาสามารถอ้างอิงรายงาน AWS SOC 1 Type II ที่ระบุรายละเอียดการควบคุมที่ AWS จัดหาให้ได้
การปฏิบัติตามข้อกำหนดของ HIPAA	การปฏิบัติตามข้อกำหนดของ HIPAA สามารถทำได้ขณะมีการใช้งานในสภาพแวดล้อมของผู้ให้บริการระบบคลาวด์หรือไม่	ข้อกำหนดของ HIPAA นำมาใช้กับและได้รับการควบคุมโดยลูกค้าของ AWS แพลตฟอร์ม AWS รองรับการใช้งานโซลูชันต่างๆ ที่ตรงกับข้อกำหนดการรับรองเฉพาะอุตสาหกรรม เช่น HIPAA ลูกค้าสามารถใช้บริการของ AWS เพื่อดูแลระดับการรักษาความปลอดภัยที่เทียบเท่าหรือสูงกว่าระดับที่กำหนดไว้เพื่อปกป้องบันทึกข้อมูลด้านสุขภาพแบบอิเล็กทรอนิกส์ ลูกค้าได้สร้างแอปพลิเคชันด้านการดูแลสุขภาพที่สอดคล้องกับกฎด้านความปลอดภัยและความเป็นส่วนตัวของ HIPAA บน AWS AWS มีข้อมูลเพิ่มเติมเกี่ยวกับการปฏิบัติตามข้อกำหนดของ HIPAA บนเว็บไซต์ รวมถึงเอกสารเกี่ยวกับหัวข้อนี้

ประเภท	คำถามเกี่ยวกับการประมวลผลบนระบบคลาวด์	ข้อมูลของ AWS
การปฏิบัติตามข้อกำหนดของ GLBA	การปฏิบัติตามข้อกำหนดการรับรองของ GLBA สามารถทำได้ขณะมีการใช้งานในสภาพแวดล้อมของผู้ให้บริการระบบคลาวด์หรือไม่	ข้อกำหนดของ GLBA ส่วนใหญ่นำมาใช้กับและได้รับการควบคุมโดยลูกค้าของ AWS AWS มีวิธีการให้ลูกค้าใช้ปกป้องข้อมูล จัดการสิทธิ์ และสร้างแอปพลิเคชันที่เป็นไปตามมาตรฐานของ GLBA บนโครงสร้างพื้นฐาน AWS หากลูกค้าต้องการการรับประกันคุณภาพที่เฉพาะเจาะจงว่ามีการใช้งานการควบคุมความปลอดภัยทางกายภาพอย่างมีประสิทธิภาพ พวกเขาสามารถดูได้ที่รายงาน AWS SOC 1 Type II ตามที่เกี่ยวข้อง
การปฏิบัติตามระเบียบข้อบังคับของรัฐบาลกลาง	หน่วยงานรัฐบาลสหรัฐฯ สามารถปฏิบัติตามระเบียบข้อบังคับด้านความปลอดภัยและความเป็นส่วนตัวขณะใช้งานในสภาพแวดล้อมของผู้ให้บริการระบบคลาวด์หรือไม่	หน่วยงานของรัฐบาลสหรัฐฯ สามารถปฏิบัติตามมาตรฐานการปฏิบัติตามข้อกำหนดจำนวนมาก รวมถึงกฎหมายว่าด้วยการจัดการความปลอดภัยด้านสารสนเทศของรัฐบาลกลาง (FISMA) ฉบับปี 2002, โปรแกรมการจัดการความเสี่ยงและการอนุญาตของรัฐบาลกลาง (FedRAMP), เอกสารมาตรฐานการประมวลผลข้อมูลของรัฐบาลกลาง (FIPS) 140-2 และระเบียบข้อบังคับว่าด้วยการควบคุมการขนส่งอาวุธนานาชาติ (ITAR) การปฏิบัติตามกฎหมายและข้อบังคับอื่นๆ ยังอาจนำมาปรับให้เหมาะสมได้ ขึ้นอยู่กับข้อกำหนดที่ระบุไว้ในข้อกฎหมายที่บังคับใช้
ตำแหน่งที่ตั้งข้อมูล	ข้อมูลของลูกค้าอยู่ที่ไหน	ลูกค้าของ AWS เป็นผู้กำหนดว่าเนื้อหาและเซิร์ฟเวอร์ของพวกเขาจะถูกระบุไว้ภายในภูมิภาคทางกายภาพใด การทำซ้ำข้อมูลสำหรับออบเจ็กต์ข้อมูล S3 ดำเนินการภายในกลุ่มศูนย์ข้อมูลที่อยู่ในภูมิภาคซึ่งมีการจัดเก็บข้อมูลและไม่มีการทำซ้ำไปยังกลุ่มของศูนย์ข้อมูลอื่นในภูมิภาคอื่นๆ ลูกค้าของ AWS เป็นผู้กำหนดว่าเนื้อหาและเซิร์ฟเวอร์ ของพวกเขาจะถูกระบุไว้ภายในภูมิภาคทางกายภาพใด AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าจากภูมิภาคที่ลูกค้าเลือกโดยไม่แจ้งให้ลูกค้าทราบ ยกเว้นจะได้รับการระบุให้ปฏิบัติตามกฎหมาย หรือมีการร้องขอจากหน่วยงานของรัฐ สำหรับรายการภูมิภาคทั้งหมดที่มีให้บริการ โปรดดูที่ aws.amazon.com/about-aws/global-infrastructure
การค้นหาทางอิเล็กทรอนิกส์	ผู้ให้บริการระบบคลาวด์ตอบสนองความต้องการของลูกค้าในการทำให้ได้ตามขั้นตอนและข้อกำหนดของการค้นหาทางอิเล็กทรอนิกส์หรือไม่	AWS จัดหาโครงสร้างพื้นฐาน และลูกค้าจัดการส่วนที่เหลือทั้งหมด รวมถึงระบบปฏิบัติการ การกำหนดค่าเครือข่าย และแอปพลิเคชันที่มีการติดตั้ง ลูกค้ามีหน้าที่ปฏิบัติตามกระบวนการทางกฎหมายที่เกี่ยวข้องกับการระบุตัวตน การเก็บรวบรวม การประมวลผล การวิเคราะห์ และการจัดทำเอกสารอิเล็กทรอนิกส์ที่มีการจัดเก็บและประมวลผลโดยใช้ AWS อย่างเหมาะสม หากมีการร้องขอ AWS สามารถทำงานกับลูกค้าที่ต้องการความช่วยเหลือจาก AWS ในกระบวนพิจารณาตามกฎหมาย
การเยี่ยมชมศูนย์ข้อมูล	ผู้ให้บริการระบบคลาวด์อนุญาตให้ลูกค้าเยี่ยมชมศูนย์ข้อมูลหรือไม่	ไม่ เนื่องจากศูนย์ข้อมูลของเราให้บริการลูกค้าหลายราย AWS ไม่อนุญาตให้ลูกค้าเยี่ยมชมศูนย์ข้อมูล เนื่องจากจะเป็นการเปิดเผยข้อมูลของลูกค้าหลายรายต่อบุคคลที่สามที่เข้าถึงข้อมูล เพื่อตอบสนองความต้องการนี้ของลูกค้า ผู้ตรวจสอบอิสระและเชี่ยวชาญจะตรวจสอบการมีอยู่และการทำงานของการควบคุมในลักษณะเป็นส่วนหนึ่งของรายงาน SOC 1 Type II ของเรา การตรวจสอบความถูกต้องจากหน่วยงานภายนอกที่มีการยอมรับอย่างแพร่หลายนี้จะนำเสนอข้อมูลที่เป็นกลางเกี่ยวกับความมีประสิทธิภาพของการควบคุมที่มีอยู่ ลูกค้า AWS ที่ลงนามในข้อตกลงที่จะไม่เปิดเผยข้อมูลกับ AWS สามารถขอรับสำเนาของรายงาน SOC 1 Type II ได้ การ

ประเภท	คำถามเกี่ยวกับการประมวลผลบนระบบคลาวด์	ข้อมูลของ AWS
		ตรวจสอบจากหน่วยงานอิสระสำหรับความปลอดภัยทางกายภาพของศูนย์ข้อมูลยังเป็นส่วนหนึ่งของการตรวจสอบตามมาตรฐาน ISO 27001, การประเมินของ PCI, การตรวจสอบ ITAR และโปรแกรมการทดสอบ FedRAMPsm
การเข้าถึงโดยบุคคลที่สาม	บุคคลที่สามได้รับอนุญาตให้เข้าถึงศูนย์ข้อมูลของผู้ให้บริการระบบคลาวด์หรือไม่	AWS ควบคุมการเข้าถึงศูนย์ข้อมูลอย่างเข้มงวด แม้แต่กับพนักงานภายในก็ตาม บุคคลที่สามไม่ได้รับอนุญาตให้เข้าถึงศูนย์ข้อมูลของ AWS ยกเว้นเมื่อได้รับอนุมัติอย่างชัดแจ้งโดยผู้จัดการศูนย์ข้อมูล AWS ที่เหมาะสม ตามนโยบายการเข้าถึงของ AWS ดูที่รายงาน SOC 1 Type II สำหรับการควบคุมเฉพาะที่เกี่ยวข้องกับการเข้าถึงทางกายภาพ การรับรองความถูกต้องในการเข้าถึงศูนย์ข้อมูล และการควบคุมที่เกี่ยวข้องอื่นๆ
การดำเนินการที่ได้รับสิทธิพิเศษ	การดำเนินการที่ได้รับสิทธิพิเศษได้รับการตรวจสอบและควบคุมหรือไม่	การควบคุมที่มีอยู่จะจำกัดการเข้าถึงระบบและข้อมูล และการเข้าถึงระบบและข้อมูลยังถูกจำกัดและตรวจสอบอีกด้วย นอกจากนี้ ข้อมูลและอินสแตนซ์เซิร์ฟเวอร์ของลูกค้ายังมีการแยกจากกันแบบลอจิคัลออกจากของลูกค้ารายอื่นๆ โดยค่าเริ่มต้น การควบคุมการเข้าถึงของผู้ใช้งานที่ได้รับสิทธิพิเศษจะมีการตรวจสอบโดยผู้ตรวจสอบอิสระระหว่างการตรวจสอบของ AWS SOC 1, ISO 27001, PCI, ITAR และ FedRAMPsm
การเข้าถึงของบุคคลภายใน	ผู้ให้บริการระบบคลาวด์จัดการกับภัยคุกคามจากการเข้าถึงแบบไม่เหมาะสมของบุคคลภายในต่อข้อมูลและแอปพลิเคชันของลูกค้าหรือไม่	AWS มีการควบคุม SOC 1 แบบเฉพาะเพื่อจัดการกับภัยคุกคามจากการเข้าถึงแบบไม่เหมาะสมของบุคคลภายใน และแผนริเริ่มการรับรองแบบสาธารณะและการปฏิบัติตามข้อกำหนดที่กล่าวถึงในเอกสารฉบับนี้ เพื่อจัดการกับการเข้าถึงของบุคคลภายใน การรับรองและการยืนยันจากหน่วยงานภายนอกทั้งหมดจะประเมินผลการควบคุมเชิงป้องกันและเชิงตรวจสอบของการเข้าถึงแบบลอจิคัล นอกจากนี้ ยังมีการประเมินความเสี่ยงเป็นประจำ ซึ่งมุ่งเน้นเกี่ยวกับวิธีการควบคุมและติดตามการเข้าถึงของบุคคลภายใน
ระบบผู้เช่าหลายราย	การแบ่งแยกลูกค้ามีการดำเนินการอย่างปลอดภัยหรือไม่	สภาพแวดล้อม AWS เป็นสภาพแวดล้อมหลายผู้เช่าแบบเสมือน AWS ดำเนินกระบวนการในการจัดการด้านความปลอดภัย การควบคุมของ PCI และการควบคุมด้านความปลอดภัยอื่นๆ ที่ออกแบบมาเพื่อแยกลูกค้าแต่ละรายออกจากลูกค้ารายอื่นๆ ระบบ AWS ได้รับการออกแบบมาเพื่อป้องกันมิให้ลูกค้าเข้าถึงโฮสต์หรืออินสแตนซ์ทางกายภาพที่ไม่ได้กำหนดให้กับพวกเขาโดยการกรองผ่านซอฟต์แวร์การจำลองเสมือน สถาปัตยกรรมนี้ได้รับการตรวจสอบโดยผู้ตรวจประเมินความปลอดภัยอิสระที่ผ่านการรับรอง (QSA) ของ PCI และพบว่ามีอยู่ในการปฏิบัติตามข้อกำหนดทั้งหมดของ PCI DSS เวอร์ชัน 3.1 ที่เผยแพร่ในเดือนเมษายน 2015 **หมายเหตุ**: AWS ยังมีตัวเลือกการเช่าแบบรายเดียวด้วย อินสแตนซ์เฉพาะคือ Amazon EC2 Instance ที่เปิดใช้งานภายใน Amazon Virtual Private Cloud (Amazon VPC) โดยรันฮาร์ดแวร์เฉพาะสำหรับลูกค้ารายเดียว อินสแตนซ์เฉพาะให้คุณได้รับประโยชน์จากข้อดีของ Amazon VPC และ AWS Cloud อย่างเต็มที่ขณะที่มีการแยกอินสแตนซ์การประมวลผล Amazon EC2 ที่ระดับฮาร์ดแวร์
ช่องโหว่ไฮเปอร์ไวเซอร์	ผู้ให้บริการระบบคลาวด์จัดการกับช่องโหว่ไฮเปอร์ไวเซอร์ที่รู้จักหรือไม่	ปัจจุบัน Amazon EC2 ใช้ไฮเปอร์ไวเซอร์ Xen เวอร์ชันที่มีการปรับแต่งระดับสูง ไฮเปอร์ไวเซอร์ได้รับการประเมินสำหรับช่องโหว่และเส้นทางการโจมตีใหม่ๆ และที่มีอยู่เดิมโดยทีมเจาะระบบภายนอกและภายใน และเหมาะอย่างยิ่งสำหรับการดูแลการแยกส่วนอย่าง

ประเภท	คำถามเกี่ยวกับการประมวลผลบนระบบคลาวด์	ข้อมูลของ AWS
		ชัดเจนระหว่างเครื่องเสมือนแบบ Guest การรักษาความปลอดภัยไฮเปอร์ไวเซอร์ Xen ของ AWS ได้รับการประเมินผลโดยผู้ตรวจสอบอิสระในระหว่างการประเมินและการตรวจสอบอยู่เป็นประจำ ดูที่รายงานความปลอดภัยของ AWS สำหรับข้อมูลเพิ่มเติมเกี่ยวกับไฮเปอร์ไวเซอร์ Xen และการแยกอินสแตนซ์
การจัดการช่องโหว่	ระบบได้รับการแก้ไขข้อบกพร่องอย่างเหมาะสมหรือไม่	AWS มีหน้าที่ในการแก้ไขข้อบกพร่องของระบบที่สนับสนุนการให้บริการกับลูกค้า เช่น บริการไฮเปอร์ไวเซอร์และการเชื่อมต่อระบบเครือข่าย โดยมีการดำเนินการตามที่กำหนดในนโยบาย AWS และเป็นไปตามข้อกำหนดของมาตรฐาน ISO 27001, NIST และ PCI ลูกค้าเป็นผู้ควบคุมระบบปฏิบัติการเยือน ซอฟต์แวร์ และแอปพลิเคชันของตนเอง รวมถึงมีหน้าที่รับผิดชอบในการแก้ไขข้อบกพร่องของระบบของตนเอง
การเข้ารหัส	บริการที่จัดหาให้รองรับการเข้ารหัสใช่หรือไม่	ใช่ AWS อนุญาตให้ลูกค้าใช้ระบบกลไกการเข้ารหัสของตนเองสำหรับบริการแทบทุกประเภท รวมถึงการเข้ารหัสแบบ S3, EBS, SimpleDB และ EC2 ช่องทาง IPSec ไปยัง VPC ได้รับการเข้ารหัสเช่นกัน Amazon S3 ยังเสนอ Server Side Encryption ให้เป็นตัวเลือกสำหรับลูกค้าด้วย ลูกค้ายังสามารถใช้เทคโนโลยีการเข้ารหัสของบุคคลที่สามได้เช่นกัน โปรดดูข้อมูลเพิ่มเติมจากรายงานความปลอดภัยของ AWS
ความเป็นเจ้าของข้อมูล	สิทธิ์ต่อข้อมูลของลูกค้าของผู้ให้บริการระบบคลาวด์เป็นแบบใด	ลูกค้า AWS ยังคงเป็นผู้ควบคุมและเป็นเจ้าของข้อมูลของตนเอง AWS เห็นชอบกับการปกป้องความเป็นส่วนตัวของลูกค้า และระมัดระวังในการวิเคราะห์ว่าควรปฏิบัติตามข้อเรียกร้องการบังคับใช้กฎหมายใด AWS ไม่ลังเลที่จะท้าทายต่อคำสั่งจากการบังคับใช้กฎหมายหากเราคิดว่าคำสั่งนั้นขาดความสมเหตุสมผล
การแยกข้อมูล	ผู้ให้บริการระบบคลาวด์แยกข้อมูลของลูกค้าอย่างเหมาะสมหรือไม่	ข้อมูลทั้งหมดของลูกค้าที่จัดเก็บโดย AWS มีความสามารถด้านความปลอดภัยและการควบคุมการแยกส่วนผู้เช่าที่มีประสิทธิภาพ Amazon S3 มีการควบคุมการเข้าถึงข้อมูลขั้นสูง โปรดดูข้อมูลเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยของบริการข้อมูลเฉพาะจากรายงานความปลอดภัยของ AWS
บริการแบบผสมรวม	ผู้ให้บริการระบบคลาวด์ใช้บริการระบบคลาวด์ของผู้ให้บริการรายอื่นเพื่อให้บริการหรือไม่	AWS ไม่ใช้ผู้ให้บริการระบบคลาวด์ของบุคคลที่สามเพื่อการให้บริการต่างๆ ของ AWS กับลูกค้า
การควบคุมทางกายภาพและทางสภาพแวดล้อม	การควบคุมเหล่านี้มีการดำเนินงานโดยผู้ให้บริการระบบคลาวด์ที่ระบุหรือไม่	ใช่ การควบคุมเหล่านี้มีการระบุไว้โดยเฉพาะในรายงาน SOC 1 Type II นอกจากนี้ การรับรองอื่นๆ ที่ AWS สนับสนุน เช่น ISO 27001 และ FedRAMP[sm] กำหนดให้มีการควบคุมทางกายภาพและทางสภาพแวดล้อมที่เป็นแนวทางปฏิบัติเช่นกัน
การป้องกันฝั่งไคลเอ็นต์	ผู้ให้บริการระบบคลาวด์ให้ลูกค้าสามารถรักษาความปลอดภัยและจัดการการเข้าถึงจากไคลเอ็นต์ เช่น พีซีและอุปกรณ์เคลื่อนที่หรือไม่	ใช่ AWS ให้ลูกค้าสามารถจัดการแอปพลิเคชันบนไคลเอ็นต์และบนอุปกรณ์เคลื่อนที่ตามความต้องการของพวกเขาเอง

ประเภท	คำถามเกี่ยวกับการประมวลผลบนระบบคลาวด์	ข้อมูลของ AWS
ความปลอดภัยของเซิร์ฟเวอร์	ผู้ให้บริการระบบคลาวด์ให้ลูกค้าสามารถรักษาความปลอดภัยเซิร์ฟเวอร์เสมือนของตนเองได้หรือไม่	ใช่ AWS ให้ลูกค้าสามารถใช้สถาปัตยกรรมการรักษาความปลอดภัยของตนเองได้ ดูที่รายงานความปลอดภัยของ AWS สำหรับรายละเอียดเกี่ยวกับความปลอดภัยของเซิร์ฟเวอร์และเครือข่าย
Identity and Access Management	บริการนี้มีความสามารถของ IAM หรือไม่	AWS มีข้อเสนอการจัดการข้อมูลประจำตัวและการเข้าถึงทรัพยากร ซึ่งให้ลูกค้าสามารถจัดการกับข้อมูลตนของผู้ใช้ กำหนดข้อมูลประจำตัวในการรักษาความปลอดภัย จัดการผู้ใช้ในแบบกลุ่ม และจัดการสิทธิ์สำหรับผู้ใช้ในแบบรวมศูนย์ โปรดดูข้อมูลเพิ่มเติมจากเว็บไซต์ของ AWS
การหยุดทำงานเพื่อบำรุงรักษาตามกำหนดการ	ผู้ให้บริการระบุเวลาที่ระบบจะถูกปิดสำหรับการบำรุงรักษาหรือไม่	AWS ไม่ได้กำหนดให้ระบบออฟไลน์สำหรับการดำเนินการบำรุงรักษาปกติและการแก้ไขข้อบกพร่องระบบ โดยปกติแล้ว การบำรุงรักษาและการแก้ไขข้อบกพร่องของระบบของ AWS เองจะไม่ส่งผลกระทบกับลูกค้า ส่วนการบำรุงรักษาอินสแตนซ์มีการควบคุมโดยลูกค้า
ความสามารถในการปรับขนาด	ผู้ให้บริการให้ลูกค้าสามารถปรับขนาดนอกเหนือจากข้อตกลงดั้งเดิมหรือไม่	AWS Cloud เป็นแบบกระจาย มีการรักษาความปลอดภัยและมีการยืดหยุ่นสูง ซึ่งให้ลูกค้าสามารถปรับขนาดได้อย่างต้องการ ลูกค้าสามารถปรับเพิ่มลดขนาดได้ โดยมีการจ่ายเงินสำหรับส่วนที่พวกเขาใช้เท่านั้น
ความพร้อมให้บริการ	ผู้ให้บริการยืนยันถึงความพร้อมให้บริการระดับสูงหรือไม่	AWS ยืนยันถึงความพร้อมให้บริการระดับสูงในข้อตกลงระดับการบริการ (SLA) ตัวอย่างเช่น Amazon EC2 ยืนยันถึงเปอร์เซ็นต์อัพไทม์รายปีอย่างน้อยที่สุด 99.95% ระหว่างปีที่มีการใช้งาน Amazon S3 ยืนยันถึงเปอร์เซ็นต์อัพไทม์รายเดือนอย่างน้อยที่สุด 99.9% โดยจะมีการให้เครดิตบริการสำหรับกรณีที่ตัววัดผลความพร้อมใช้งานไม่ตรงตามที่กำหนด
การโจมตีแบบ Distributed Denial of Service (DDoS)	ผู้ให้บริการป้องกันบริการของตนเองจากการโจมตีแบบ DDoS หรือไม่	เครือข่าย AWS มีการปกป้องให้ปลอดภัยจากปัญหาด้านการรักษาความปลอดภัยเครือข่ายแบบดั้งเดิม และลูกค้ายังสามารถดำเนินการป้องกันเพิ่มเติมต่อไปได้ ดูที่รายงานความปลอดภัยของ AWS สำหรับข้อมูลเพิ่มเติมเกี่ยวกับหัวข้อนี้ รวมถึงการพูดคุยถึงการโจมตีแบบ DDoS
การเคลื่อนย้ายข้อมูล	ข้อมูลที่จัดเก็บโดยผู้ให้บริการสามารถส่งออกตามคำขอของลูกค้าได้หรือไม่	AWS อนุญาตให้ลูกค้าเคลื่อนย้ายข้อมูลตามที่ต้องการทั้งภายในและออกนอกพื้นที่จัดเก็บของ AWS บริการ AWS Import/Export สำหรับ S3 จะช่วยย้ายข้อมูลขนาดใหญ่ไปยังและออกจาก AWS โดยใช้อุปกรณ์เก็บข้อมูลแบบพกพาในการโอนย้ายได้
ความต่อเนื่องทางธุรกิจของผู้ให้บริการ	ผู้ให้บริการดำเนินโปรแกรมความต่อเนื่องทางธุรกิจหรือไม่	AWS ดำเนินโปรแกรมความต่อเนื่องทางธุรกิจ ข้อมูลรายละเอียดมีการระบุอยู่ในรายงานความปลอดภัยของ AWS
ความต่อเนื่องทางธุรกิจของลูกค้า	ผู้ให้บริการให้ลูกค้าสามารถดำเนินแผนความต่อเนื่องทางธุรกิจหรือไม่	AWS ให้ลูกค้าสามารถดำเนินแผนความต่อเนื่องที่ชัดเจน รวมถึงการใช้การสำรองข้อมูลอินสแตนซ์ของเว็บเซิร์ฟเวอร์ประจำ การทำซ้ำของระบบสำรองข้อมูล สถาปัตยกรรมในการใช้งานแบบหลายภูมิภาค/Availability Zone

ประเภท	คำถามเกี่ยวกับการประมวลผลบนระบบคลาวด์	ข้อมูลของ AWS
ความคงทนของข้อมูล	บริการระบุความคงทนของข้อมูลหรือไม่	Amazon S3 มีโครงสร้างพื้นฐานการจัดเก็บข้อมูลที่มีความคงทนสูง ออบเจ็กต์จะได้รับการจัดเก็บบนหลายอุปกรณ์ในสถานที่ตั้งต่างๆ ที่อยู่ในภูมิภาคของ Amazon S3 เมื่อจัดเก็บแล้ว Amazon S3 จะรักษาความคงทนของออบเจ็กต์ด้วยการตรวจหาและแก้ไขความซ้ำซ้อนที่สูญหายใดๆ อย่างรวดเร็ว และ Amazon S3 ยังตรวจสอบความถูกต้องของข้อมูลที่จัดเก็บเป็นประจำโดยใช้ checksum หากตรวจพบความเสียหาย ระบบจะซ่อมแซมโดยใช้ข้อมูลซ้ำ ข้อมูลที่จัดเก็บใน S3 ได้รับการออกแบบมาให้มีความคงทน 99.999999999% และมีออบเจ็กต์ที่พร้อมใช้งาน 99.99% ตลอดช่วงปีที่ระบุ
การสำรองข้อมูล	บริการมีการสำรองข้อมูลไปยังเทปหรือไม่	AWS ให้ลูกค้าสามารถสำรองข้อมูลไปยังเทปของตนได้โดยใช้ผู้ให้บริการสำรองข้อมูลเทปของตนเอง อย่างไรก็ตาม การสำรองข้อมูลเทปไม่ใช่บริการที่มีการจัดหาให้โดย AWS บริการ Amazon S3 ออกแบบมาเพื่อลดโอกาสเกิดการสูญหายของข้อมูลลงจนเกือบจะเป็นศูนย์ รวมถึงเพิ่มระดับความคงทนเทียบเท่ากับการทำสำเนาออบเจ็กต์ข้อมูลแบบหลายไซต์ด้วยการทำซ้ำการจัดเก็บข้อมูล สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความคงทนของข้อมูลและการทำซ้ำ โปรดดูที่เว็บไซต์ของ AWS
การเพิ่มราคา	ผู้ให้บริการจะเพิ่มราคาโดยไม่คาดคิดหรือไม่	AWS มีประวัติการลดราคาบ่อยครั้ง เนื่องจากราคาในการจัดหาบริการเหล่านี้ลดลงเมื่อเวลาผ่านไป AWS มีการลดราคาอย่างต่อเนื่องในช่วงหลายปีที่ผ่านมา
ความยั่งยืน	บริษัทของผู้ให้บริการมีความสามารถในการรักษาความยั่งยืนในระยะยาวหรือไม่	AWS เป็นผู้ให้บริการระบบคลาวด์ระดับชั้นนำและเป็นกลยุทธ์ทางธุรกิจในระยะยาวของ Amazon.com AWS มีความสามารถในการรักษาความยั่งยืนในระยะยาวอย่างแน่นอน

แหล่งข้อมูลเพิ่มเติม

สำหรับข้อมูลเพิ่มเติม ดูที่แหล่งข้อมูลต่อไปนี้:

- ภาพรวมของความเสี่ยงและการปฏิบัติตามข้อกำหนดของ AWS
- การรับรอง โปรแกรม รายงานของ AWS และการยืนยันจากหน่วยงานภายนอก
- ชุดคำถาม CSA Consensus Assessments Initiative Questionnaire

การปรับปรุงเอกสาร

วันที่	คำอธิบาย
มกราคม 2017	ย้ายไปใช้เทมเพลตใหม่
มกราคม 2016	เผยแพร่ครั้งแรกเมื่อ