ภาพรวมของความเสี่ยงและการปฏิบัติตามข้อกำหนดของ AWS

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 และเอกสารฉบับนี้ไม่ถือเป็นส่วนหนึ่งของข้อตกลงและไม่ทำให้เกิดการเปลี่ยนแปลงใดๆ กับข้อตกลงระหว่าง AWS กับลูกค้า

สารบัญ

บทคัดย่อ

รายงานฉบับนี้เสนอข้อมูลในการช่วยลูกค้าผนวกรวม AWS เข้ากับกรอบงานการควบคุมที่มีอยู่ รวมถึงแนวทางเบื้องต้นสำหรับการประเมินผลการควบคุมของ AWS

ข้อมูลเบื้องต้น

AWS และลูกค้าต่างมีหน้าที่ร่วมกันในการควบคุมสภาพแวดล้อมด้านไอที ความรับผิดชอบร่วมกันในส่วนของ AWS ประกอบด้วยการจัดหาบริการต่างๆ บนแพลตฟอร์มที่มีความปลอดภัยสูงและได้รับการควบคุม และมอบคุณสมบัติด้านความปลอดภัยหลากหลายรูปแบบที่ลูกค้าสามารถใช้ได้ ส่วนลูกค้ามีหน้าที่รับผิดชอบในการกำหนดค่าสภาพแวดล้อมด้านไอทีของตนให้มีความปลอดภัยและได้รับการควบคุมสำหรับการใช้งานตามวัตถุประสงค์ของตน แม้ลูกค้าจะไม่ได้แจ้งต่อ AWS เกี่ยวกับการใช้งานและการกำหนดค่าของตน แต่ AWS จะมีการแจ้งข้อมูลเกี่ยวกับความปลอดภัยและการควบคุมสภาพแวดล้อมที่เกี่ยวข้องกับลูกค้าให้ทราบ AWS ดำเนินการดังกล่าวด้วยวิธีการต่อไปนี้:

- การขอการรับรองด้านอุตสาหกรรมและการยืนยันจากหน่วยงานภายนอกอิสระที่มีการอธิบายไว้ในเอกสารนี้
- การเผยแพร่ข้อมูลเกี่ยวกับแนวทางปฏิบัติด้านความปลอดภัยและการควบคุมของ AWS ในเอกสารและเนื้อหาของเว็บไซต์
- การจัดหาใบรับรอง รายงาน และเอกสารประกอบอื่นๆ ให้กับลูกค้าของ AWS โดยตรงภายใต้ข้อตกลง NDA (ตามที่กำหนด)

หากต้องการคำอธิบายรายละเอียดเพิ่มเติมเกี่ยวกับความปลอดภัยของ AWS โปรดดูที่ ศูนย์ความปลอดภัยของ AWS

หากต้องการคำอธิบายรายละเอียดเพิ่มเติมเกี่ยวกับการปฏิบัติตามข้อกำหนดของ AWS โปรดดูที่ เพจการปฏิบัติตามข้อกำหนดของ AWS

นอกจากนี้ยังมีเอกสาร ภาพรวมของกระบวนการรักษาความปลอดภัยของ AWS ที่กล่าวถึงการควบคุมความปลอดภัยทั่วไปและความปลอดภัยเฉพาะบริการของ AWS

สภาพแวดล้อมที่ต้องรับผิดชอบร่วมกัน

การย้ายจากโครงสร้างพื้นฐานด้านไอทีไปยังบริการของ AWS ทำให้เกิดโมเดลการรับผิดชอบร่วมกันระหว่างลูกค้าและ AWS โมเดลการดำเนินการร่วมกันนี้สามารถช่วยลดภาระของลูกค้าได้ เนื่องจาก AWS จะเป็นผู้ดำเนินการ จัดการ และควบคุมส่วนประกอบตั้งแต่ระบบปฏิบัติการของโฮสต์และเลเยอร์ระบบเสมือนลงไปจนถึงความปลอดภัยทางกายภาพของสถานที่ตั้งสำหรับการให้บริการ ลูกค้าจะรับผิดชอบในการจัดการระบบปฏิบัติการเยือน (รวมถึงอัปเดตและโปรแกรมแพตช์ด้านความปลอดภัย)

ซอฟต์แวร์แอปพลิเคชันที่เกี่ยวข้องอื่นๆ รวมถึงการกำหนดค่าของไฟร์วอลล์กลุ่มการรักษาความปลอดภัยจาก AWS ลูกค้าควรพิจารณาบริการต่างๆ ที่จะเลือกใช้อย่างละเอียดถี่ถ้วน เนื่องจากความรับผิดชอบของพวกเขาจะแตกต่างกันไปตามบริการที่ใช้ การผนวกรวมบริการเหล่านั้นเข้ากับสภาพแวดล้อมด้านไอที และกฎหมายและระเบียบข้อบังคับที่บังคับใช้ ลูกค้าสามารถปรับปรุงความปลอดภัยให้ดียิ่งขึ้นและ/หรือสามารถตอบสนองต่อข้อกำหนดการปฏิบัติตามที่เข้มงวดมากกว่าได้โดยใช้เทคโนโลยี เช่น ไฟร์วอลล์สำหรับโฮสต์ การตรวจจับ/การป้องการการบุกรุกบนโฮสต์ การเข้ารหัสและการจัดการคีย์ ลักษณะของการรับผิดชอบร่วมกันนี้ไม่เพียงมีความยืดหยุ่น แต่ลูกค้ายังสามารถควบคุมว่าจะอนุญาตให้มีการใช้งานโซลูชันที่ตรงกับข้อกำหนดการรับรองเฉพาะอุตสาหกรรมหรือไม่ได้อีกด้วย

รูปแบบความรับผิดชอบร่วมกันของลูกค้า/AWS นี้ยังขยายไปสู่การควบคุมด้านไอทีด้วย การจัดการ การดำเนินการ และการตรวจสอบการควบคุมด้านไอทีก็มีการแบ่งงานร่วมกัน เช่นเดียวกับความรับผิดชอบร่วมระหว่าง AWS และลูกค้าในการใช้งานสภาพแวดล้อมระบบไอที AWS สามารถช่วยลดภาระของลูกค้าในการควบคุมการดำเนินงานโดยการจัดการกับการควบคุมที่เกี่ยวข้องกับโครงสร้างพื้นฐานทางกายภาพซึ่งใช้งานในสภาพแวดล้อมของ AWS ที่อาจได้รับการจัดการโดยลูกค้ามาก่อน เนื่องจากลูกค้าทั้งหมดมีการใช้งานใน AWS แตกต่างกัน ลูกค้าจึงสามารถใช้ประโยชน์จากการเปลี่ยนการจัดการของการควบคุมด้านไอทีบางอย่างไปสู่ AWS ซึ่งทำให้มีสภาพแวดล้อมการควบคุมที่เป็นแบบกระจาย (ใหม่) จากนั้นลูกค้าสามารถใช้เอกสารประกอบการควบคุมและการปฏิบัติตามข้อกำหนดของ AWS ที่จัดหาให้กับพวกเขา (มีการอธิบายไว้ในการรับรองของ AWS และการยืนยันจากหน่วยงานภายนอก) เพื่อดำเนินขั้นตอนการประเมินผลและการตรวจสอบการควบคุมของลูกค้า

การกำกับดูแลการปฏิบัติตามข้อกำหนดที่มีประสิทธิภาพ

ลูกค้าของ AWS ต้องดำเนินการเพื่อให้มีการกำกับดูแลที่เหมาะสมสำหรับสภาพแวดล้อมการควบคุมด้านไอทีทั้งหมดเหมือนเดิม ไม่ว่าจะมีการใช้งานระบบไอทีแบบใดก็ตาม แนวทางปฏิบัติชั้นนำประกอบด้วยการทำความเข้าใจวัตถุประสงค์และข้อกำหนดของการปฏิบัติตามที่จำเป็น (จากแหล่งที่มาที่เกี่ยวข้อง) การสร้างสภาพแวดล้อมการควบคุมที่ตรงตามวัตถุประสงค์และข้อกำหนดเหล่านั้น การทำความเข้าใจการตรวจสอบความถูกต้องที่กำหนดตามระดับความเสี่ยงที่ยอมรับได้ขององค์กร และการตรวจสอบความมีประสิทธิภาพในการดำเนินการของสภาพแวดล้อมการควบคุม การปรับใช้งานใน AWS Cloud ให้องค์กรต่างๆ มีตัวเลือกที่แตกต่างกันในการใช้การควบคุมประเภทต่างๆ และวิธีการตรวจสอบในแบบต่างกัน

การปฏิบัติตามข้อกำหนดและการกำกับดูแลที่มีประสิทธิภาพของลูกค้าสามารถใช้แนวทางพื้นฐานต่อไปนี้:

1. ทบทวนข้อมูลจาก AWS ร่วมกับข้อมูลอื่นๆ เพื่อทำความเข้าใจสภาพแวดล้อมด้านไอทีทั้งหมดให้มากที่สุดเท่าที่จะเป็นไปได้ แล้วจัดทำเอกสารข้อกำหนดการปฏิบัติตามทั้งหมด
2. กำหนดและดำเนินการตามวัตถุประสงค์การควบคุมที่ตรงตามข้อกำหนดการปฏิบัติตามขององค์กร
3. ระบุและจัดทำเอกสารการควบคุมที่เป็นเจ้าของโดยฝ่ายภายนอก
4. ตรวจสอบว่าวัตถุประสงค์การควบคุมทั้งหมดตรงตามที่กำหนดและการควบคุมที่สำคัญทั้งหมดมีการออกแบบและดำเนินการอย่างมีประสิทธิภาพ

การใช้การกำกับดูแลการปฏิบัติตามในลักษณะนี้จะช่วยให้บริษัทต่างๆ เกิดความเข้าใจที่ดียิ่งขึ้นเกี่ยวกับสภาพแวดล้อมการควบคุมของตนและจะช่วยอธิบายกิจกรรมการตรวจสอบที่จะดำเนินการได้อย่างชัดเจน

การประเมินผลและการผนวกรวมการควบคุมของ AWS

AWS มีข้อมูลหลากหลายที่เกี่ยวข้องกับสภาพแวดล้อมการควบคุมด้านไอทีให้กับลูกค้าในรูปของเอกสาร รายงาน การรับรอง และการยืนยันจากหน่วยงานภายนอกอื่นๆ เอกสารประกอบฉบับนี้จะช่วยลูกค้าในการทำความเข้าใจการควบคุมที่เกี่ยวข้องกับบริการของ AWS ที่พวกเขาใช้และวิธีการที่การควบคุมเหล่านี้ได้รับการตรวจสอบความถูกต้อง ข้อมูลนี้ยังช่วยลูกค้าในการดำเนินการที่ต้องคำนึงถึงและตรวจสอบว่าการควบคุมในสภาพแวดล้อมด้านไอทีที่ขยายเพิ่มนั้นดำเนินการได้อย่างมีประสิทธิภาพ

แต่เดิมนั้น ความมีประสิทธิภาพในการออกแบบและการดำเนินการตามวัตถุประสงค์ของการควบคุมและการควบคุมได้รับการตรวจสอบโดยผู้ตรวจสอบภายในและ/หรือภายนอกผ่านทางสรุปรายละเอียดของกระบวนการและการประเมินผลหลักฐานยืนยัน การสังเกตการณ์/การตรวจสอบความถูกต้องโดยตรงโดยลูกค้าหรือผู้ตรวจสอบภายนอกของลูกค้าโดยทั่วไปแล้วเป็นการดำเนินการเพื่อตรวจสอบการควบคุม ในกรณีที่มีการใช้ผู้ให้บริการอย่าง AWS บริษัทจะร้องขอและประเมินผลการรับรองและการยืนยันจากหน่วยงานภายนอกเพื่อให้ได้รับการรับประกันคุณภาพที่เหมาะสมสำหรับความมีประสิทธิภาพของการออกแบบ และการดำเนินการของวัตถุประสงค์ของการควบคุมและ

การควบคุมต่างๆ ดังนั้น ถึงแม้ว่าการควบคุมที่สำคัญของลูกค้าสามารถจัดการได้โดย AWS แต่สภาพแวดล้อมการควบคุมสามารถยังคงเป็นเฟรมเวิร์กแบบรวมที่มีการนำการควบคุมทั้งหมดมาใช้และตรวจสอบว่าดำเนินการอย่างมีประสิทธิภาพ การยืนยันจากหน่วยงานภายนอกและการรับรองของ AWS ไม่เพียงให้การตรวจสอบความถูกต้องของสภาพแวดล้อมการควบคุมในระดับที่สูงขึ้นเท่านั้น แต่ยังช่วยลูกค้าลดข้อกำหนดที่ต้องดำเนินงานการตรวจสอบความถูกต้องบางอย่างสำหรับสภาพแวดล้อมด้านไอทีของพวกเขาใน AWS Cloud

ข้อมูลการควบคุมด้านไอทีของ AWS

AWS ให้ข้อมูลการควบคุมด้านไอทีกับลูกค้าในลักษณะต่อไปนี้:

ข้อกำหนดการควบคุมเฉพาะ ลูกค้าของ AWS สามารถระบุการควบคุมที่สำคัญที่จัดการโดย AWS ได้ การควบคุมที่สำคัญเป็นสิ่งจำเป็นต่อสภาพแวดล้อมการควบคุมของลูกค้าและต้องมีการยืนยันจากหน่วยงานภายนอกสำหรับความมีประสิทธิภาพของการดำเนินการของการควบคุมที่สำคัญเหล่านี้ เพื่อให้มีการปฏิบัติตามข้อกำหนดการปฏิบัติตาม เช่น การตรวจสอบทางการเงินประจำปี สำหรับวัตถุประสงค์นี้ AWS จะเผยแพร่การควบคุมด้านไอทีเฉพาะแบบเฉพาะเจาะจงจำนวนมากในรายงาน Service Organization Controls 1 (SOC 1) Type II รายงาน SOC 1 หรือแต่เดิมคือ Statement on Auditing Standards (SAS) No. 70 ซึ่งเป็นรายงานขององค์กรด้านบริการ ระบุมาตรฐานการตรวจสอบที่มีการยอมรับอย่างแพร่หลายที่มีการพัฒนาโดย American Institute of Certified Public Accountants (AICPA) การตรวจสอบ SOC 1 เป็นการตรวจสอบเชิงลึกเกี่ยวกับความมีประสิทธิภาพของการออกแบบและการดำเนินการสำหรับวัตถุประสงค์การควบคุมและกิจกรรมการควบคุมที่กำหนดของ AWS (ซึ่งเป็นวัตถุประสงค์การควบคุมและกิจกรรมการควบคุมส่วนประกอบของโครงสร้างพื้นฐานที่ AWS จัดการ) “Type II” หมายถึง ข้อเท็จจริงที่ว่าการควบคุมแต่ละอย่างที่อธิบายไว้ในรายงานไม่เพียงมีการประเมินผลความเพียงพอของการออกแบบเท่านั้น แต่ยังมีการทดสอบความมีประสิทธิภาพของการดำเนินการโดยผู้ตรวจสอบจากภายนอกด้วย เนื่องด้วยความเป็นอิสระและความสามารถของผู้ตรวจสอบจากภายนอกของ AWS การควบคุมต่างๆ ที่ระบุในรายงานจึงควรทำให้ลูกค้าเกิดความเชื่อมั่นในระดับที่สูงขึ้นต่อสภาพแวดล้อมการควบคุมของ AWS การควบคุมของ AWS เป็นการดูว่าการออกแบบและการดำเนินการมีประสิทธิภาพสำหรับวัตถุประสงค์ของการปฏิบัติตามหลายอย่าง รวมถึง Sarbanes-Oxley (SOX) ข้อที่ 404 การตรวจสอบรายงานทางการเงิน โดยทั่วไปแล้ว การใช้

รายงาน SOC 1 Type II ยังได้รับอนุญาตโดยหน่วยงานด้านการรับรองภายนอกอื่นๆ (เช่น ผู้ตรวจสอบมาตรฐาน ISO 27001 สามารถขอรายงาน SOC 1 Type II เพื่อให้มีการประเมินผลสำหรับลูกค้าของพวกเขาได้)

กิจกรรมการควบคุมเฉพาะอื่นๆ เกี่ยวข้องกับการปฏิบัติตามมาตรฐานของอุตสาหกรรมการชำระเงินผ่านบัตรเครดิต (PCI) และกฎหมาย Federal Information Security Management Act (FISMA) ของ AWS AWS ปฏิบัติตามมาตรฐาน FISMA Moderate และมาตรฐานการรักษาความปลอดภัยข้อมูลของ PCI มาตรฐาน PCI และ FISMA เหล่านี้เป็นบทบัญญัติและต้องมีการตรวจสอบความถูกต้องจากหน่วยงานอิสระว่า AWS ปฏิบัติตามมาตรฐานที่เผยแพร่

การปฏิบัติตามมาตรฐานการควบคุมทั่วไป หากลูกค้าของ AWS ต้องการให้เป็นไปตามวัตถุประสงค์การควบคุมที่หลากหลาย สามารถดำเนินการประเมินผลของการรับรองของอุตสาหกรรมของ AWS ได้ ด้วยการรับรอง AWS ISO 27001, AWS ปฏิบัติตามมาตรฐานการรักษาความปลอดภัยที่กว้างขวางและครอบคลุม และปฏิบัติตามแนวทางปฏิบัติในการรักษาสภาพแวดล้อมที่ปลอดภัย ด้วยมาตรฐานการรักษาความปลอดภัยข้อมูลของ PCI (PCI DSS) AWS ปฏิบัติตามมาตรการควบคุมที่สำคัญสำหรับบริษัทที่จัดการข้อมูลบัตรเครดิต ด้วยการปฏิบัติตามมาตรฐาน FISMA ของ AWS, AWS ปฏิบัติตามมาตรการควบคุมเฉพาะที่หลากหลายที่กำหนดโดยหน่วยงานรัฐบาลของสหรัฐฯ การปฏิบัติตามมาตรฐานทั่วไปเหล่านี้ให้ลูกค้าทราบข้อมูลเชิงลึกเกี่ยวกับลักษณะที่ครอบคลุมของการควบคุมและกระบวนการด้านความปลอดภัยที่มีอยู่สามารถนำมาใช้ได้เมื่อจัดการกับการปฏิบัติตาม

ภูมิภาคสากลของ AWS

ศูนย์ข้อมูลสร้างเป็นกลุ่มอยู่ในภูมิภาคต่างๆ ทั่วโลก รวมถึง: สหรัฐอเมริกาฝั่งตะวันออก (เวอร์จิเนียตอนเหนือ), สหรัฐอเมริกาฝั่งตะวันตก (โอริกอน), สหรัฐอเมริกาฝั่งตะวันตก (แคลิฟอร์เนียตอนเหนือ), AWS GovCloud (สหรัฐอเมริกา) (โอริกอน), สหภาพยุโรป (แฟรงก์เฟิร์ต), สหภาพยุโรป (ไอร์แลนด์), เอเชียแปซิฟิก (โซล), เอเชียแปซิฟิก (สิงคโปร์), เอเชียแปซิฟิก (โตเกียว), เอเชียแปซิฟิก (ซิดนีย์), ภูมิภาคของจีน (ปักกิ่ง) และอเมริกาใต้ (เซาเปาโล)

สำหรับรายการภูมิภาคทั้งหมดที่มีให้บริการ โปรดดูที่เพจ [โครงสร้างพื้นฐานส่วนกลางของ AWS]

โปรแกรมความเสี่ยงและปฏิบัติตามข้อกำหนดของ AWS

AWS ให้ข้อมูลเกี่ยวกับโปรแกรมความเสี่ยงและปฏิบัติตามข้อกำหนดเพื่อให้ลูกค้าสามารถรวมการควบคุมต่างๆ ของ AWS เข้ากับกรอบงานการกำกับดูแลของตน ข้อมูลนี้สามารถช่วยลูกค้าจัดเอกสารกรอบงานการควบคุมและการกำกับดูแลทั้งหมดกับ AWS ซึ่งมีการรวมเป็นส่วนที่สำคัญของกรอบงานนั้น

การจัดการความเสี่ยง

ฝ่ายบริหารของ AWS จัดทำแผนธุรกิจเชิงกลยุทธ์ ซึ่งประกอบด้วยการระบุความเสี่ยงและการดำเนินการควบคุมเพื่อช่วยลดและจัดการกับความเสี่ยง ฝ่ายบริหารของ AWS จะประเมินแผนธุรกิจเชิงกลยุทธ์ซ้ำอย่างน้อยปีละสองครั้ง กระบวนการดังกล่าวกำหนดให้การจัดการระบุความเสี่ยงต่างๆ ภายในขอบเขตความรับผิดชอบของตนเอง และใช้มาตรการที่เหมาะสมซึ่งออกแบบมาเพื่อรับมือกับความเสี่ยงเหล่านั้น

นอกจากนี้ สภาพแวดล้อมการควบคุมของ AWS ยังได้รับการประเมินความเสี่ยงหลายลักษณะ ทั้งจากภายนอกและภายใน ทีมการปฏิบัติตามข้อกำหนดและความปลอดภัยของ AWS ได้วางกรอบงานและนโยบายด้านความปลอดภัยของข้อมูลตามวัตถุประสงค์การควบคุมสำหรับข้อมูลและกรอบงานเทคโนโลยี (COBIT) ที่เกี่ยวข้อง และได้ผนวกรวมกรอบงานที่สามารถรับรองได้ของ ISO 27001 เข้าไว้ด้วยโดยอ้างอิงจากการควบคุมตาม 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 Rev 3 (Recommended Security Controls for Federal Information Systems) AWS ดูแลนโยบายด้านความปลอดภัย จัดให้มีการการฝึกอบรมด้านความปลอดภัยแก่พนักงาน และดำเนินการตรวจสอบความปลอดภัยในการใช้งาน การทบทวนเหล่านี้จะประเมินการรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล รวมถึงความสอดคล้องกันกับนโยบายการรักษาความปลอดภัยข้อมูล

ระบบความปลอดภัยของ AWS จะตรวจดูที่อยู่ IP ตำแหน่งข้อมูลของบริการที่เชื่อมต่อกับอินเทอร์เน็ตทั้งหมดเป็นประจำเพื่อค้นหาช่องโหว่ (การตรวจสอบนี้ไม่รวมถึงอินสแตนซ์ของลูกค้า) ฝ่ายความปลอดภัยของ AWS จะแจ้งต่อฝ่ายที่เหมาะสมให้แก้ไขช่องโหว่ที่ระบุ นอกจากนี้ ความเสี่ยงด้านช่องโหว่จากภายนอกจะได้รับการประเมินโดยบริษัทด้านความปลอดภัยอิสระอยู่เป็นประจำ ข้อมูลที่พบและคำแนะนำต่างๆ ที่ได้จากการประเมินผลเหล่านี้จะได้รับการจัดหมวดหมู่และส่งมอบให้กับผู้นำของ AWS การสแกนเหล่านี้

ดำเนินการในลักษณะของการตรวจสอบสถานะและการมีอยู่ของโครงสร้างพื้นฐานของ AWS ที่สำคัญ และไม่ได้หมายถึงการแทนที่การสแกนช่องโหว่ของลูกค้าเองที่ต้องเป็นไปตามข้อกำหนดการปฏิบัติตามข้อกำหนดเฉพาะ ลูกค้าสามารถยื่นขออนุญาตเพื่อทำการสแกนโครงสร้างพื้นฐานระบบคลาวด์ของตนเองได้ ตราบเท่าที่การดำเนินการดังกล่าวจำกัดเฉพาะภายในอินสแตนซ์ของลูกค้าเอง และไม่เป็นการละเมิดนโยบายการใช้งานที่ยอมรับได้ของ AWS ผู้ใช้งานสามารถยื่นการอนุมัติล่วงหน้าสำหรับการสแกนเหล่านี้ โดยส่งคำขอผ่าน แบบฟอร์มการยื่นขอทดสอบการเจาะระบบ / ตรวจหาช่องโหว่ของ AWS

สภาพแวดล้อมการควบคุม

AWS จัดการสภาพแวดล้อมการควบคุมแบบครอบคลุมที่มีนโยบาย กระบวนการ และกิจกรรมการควบคุมที่ใช้ประโยชน์สภาพแวดล้อมการควบคุมโดยรวมของ Amazon ในหลายด้าน สภาพแวดล้อมการควบคุมนี้มีไว้เพื่อการให้ข้อเสนอการบริการของ AWS ที่มีการรักษาความปลอดภัย สภาพแวดล้อมการควบคุมร่วมจะครอบคลุมบุคลากร กระบวนการ และเทคโนโลยีที่จำเป็นในการสร้างและดูแลรักษาสภาพแวดล้อมที่สนับสนุนความมีประสิทธิภาพในการดำเนินการของกรอบงานการควบคุมของ AWS AWS มีการผนวกรวมการควบคุมเฉพาะระบบคลาวด์ที่เกี่ยวข้องที่ระบุโดยองค์กรอุตสาหกรรม การประมวลผลระบบคลาวด์ชั้นนำลงในกรอบงานการควบคุมของ AWS AWS ยังคงติดตามตรวจสอบกลุ่มอุตสาหกรรมเหล่านี้อย่างต่อเนื่องเพื่อค้นหาแนวคิดที่จะเป็นแนวทางปฏิบัติชั้นนำสำหรับใช้ช่วยเหลือลูกค้าให้จัดการสภาพแวดล้อมการควบคุมของตนเองได้ดียิ่งขึ้น

สภาพแวดล้อมการควบคุมที่ Amazon เริ่มต้นที่ระดับสูงสุดภายในองค์กร ผู้บริหารและผู้มีอำนาจระดับสูงมีบทบาทสำคัญในการวางรากฐานสำหรับคุณค่าหลักและแนวทางของบริษัท พนักงานทุกคนจะได้รับทราบเกี่ยวกับหลักปฏิบัติทางธุรกิจและหลักจริยธรรมของบริษัท และต้องผ่านการฝึกอบรมเป็นระยะ นอกจากนี้ ยังมีการตรวจสอบการปฏิบัติตามเพื่อให้พนักงานมีความเข้าใจและปฏิบัติตามนโยบายที่กำหนดไว้

โครงสร้างเชิงองค์กรของ AWS ให้กรอบสำหรับการวางแผน การดำเนินการ และการควบคุมการดำเนินงานของธุรกิจ โครงสร้างเชิงองค์กรกำหนดบทบาทและความรับผิดชอบเพื่อให้มีการสรรหาพนักงานอย่างเพียงพอ ความมีประสิทธิภาพของการดำเนินการ และการแบ่งแยกหน้าที่ ฝ่ายบริหารยังได้กำหนดผู้มีอำนาจและสายการบังคับบัญชาที่เหมาะสมสำหรับบุคลากรที่สำคัญด้วย สิ่งที่กำหนดให้เป็นส่วนประกอบของกระบวนการตรวจสอบความถูกต้องในการจ้างงานของ AWS คือ การศึกษา การจ้างงานก่อนหน้า และในบางกรณี มีการตรวจสอบภูมิหลังตามที่กฎหมายอนุญาตและตามข้อบังคับ

สำหรับพนักงานที่สอดคล้องกับตำแหน่งและระดับสิทธิ์เข้าถึงของพนักงานสำหรับสถานที่ของ AWS บริษัทปฏิบัติตามกระบวนการเตรียมความพร้อมที่มีแบบแผนเพื่อให้พนักงานใหม่ทำความคุ้นเคยกับเครื่องมือ กระบวนการ ระบบ นโยบาย และขั้นตอนของ Amazon

ความปลอดภัยของข้อมูล

AWS ใช้โปรแกรมความปลอดภัยของข้อมูลที่เป็นทางการซึ่งออกแบบมาเพื่อปกป้องการรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของระบบและข้อมูลของลูกค้า AWS เผยแพร่เอกสารด้านความปลอดภัยที่กล่าวถึงวิธีการที่ AWS สามารถช่วยลูกค้าดูแลข้อมูลของตนให้ปลอดภัยที่มีอยู่บนเว็บไซต์สาธารณะ

การติดต่อ AWS

ลูกค้าสามารถขอรับรายงานและการรับรองที่จัดทำโดยผู้ตรวจสอบจากหน่วยงานอื่นหรือสามารถขอข้อมูลเพิ่มเติมเกี่ยวกับการปฏิบัติตามข้อกำหนดของ AWS โดยการติดต่อฝ่ายการขายและพัฒนาธุรกิจของ AWS เจ้าหน้าที่จะนำลูกค้าไปยังทีมที่เหมาะสมขึ้นอยู่กับลักษณะของการสอบถาม สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการปฏิบัติตามของ AWS โปรดดูที่ไซต์ การปฏิบัติตามของ AWS หรือส่งคำถามโดยตรงไปที่ mailto:awscompliance@amazon.com

แหล่งข้อมูลเพิ่มเติม

สำหรับข้อมูลเพิ่มเติม ดูที่แหล่งข้อมูลต่อไปนี้:

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

การปรับปรุงเอกสาร

วันที่	คำอธิบาย
มกราคม 2017	ย้ายไปใช้เทมเพลตใหม่
มกราคม 2016	เผยแพร่ครั้งแรกเมื่อ