Unable to locate subtitle

Amazon Web Services – Risiko und Compliance

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Web Services – Risiko und Compliance: ***Unable to locate subtitle***

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, die Kunden zu verwirren oder Amazon in einer Weise herabzusetzen oder zu diskreditieren. Alle anderen Marken, die nicht Eigentum von Amazon sind, sind Eigentum ihrer jeweiligen Inhaber, die mit Amazon verbunden oder nicht verbunden oder von Amazon gesponsert oder nicht gesponsert sein können.

Table of Contents

Amazon Web Services – Risiko und Compliance 1
Überblick 1
Einführung 2
Modell der geteilten Verantwortlichkeit 3
Bewerten und Integrieren von AWS-Kontrollen 5
AWS Risiko- und Compliance-Programm 6
AWS Risikomanagement für Unternehmen 6
Betriebs- und Geschäftsführung 6
Steuerungsumgebung und Automatisierung 7
Bewertung der Kontrollen und kontinuierliche Überwachung 8
AWS-Zertifizierungen, -Programme, -Berichte und Bescheinigungen von Drittanbietern 9
Cloud Security Alliance 10
Cloud-Compliance-Governance für Kunden 11
Fazit 12
Mitwirkende 13
Weitere Informationen 14
Dokumentversionen 15
Hinweise 16

Amazon Web Services – Risiko und Compliance

Veröffentlichungsdatum: 11. März 2021 (Dokumentversionen)

Überblick

AWS bedient eine Vielzahl von Kunden, einschließlich Kunden aus regulierten Branchen. Durch unser Modell der geteilten Verantwortung ermöglichen wir unseren Kunden ein effektives und effizientes Risikomanagement in der IT-Umgebung und gewährleisten ein effektives Risikomanagement durch die Einhaltung etablierter, allgemein anerkannter Frameworks und Programme. Dieses Whitepaper beschreibt die Mechanismen, die AWS implementiert hat, um das Risiko auf der Seite des AWS Modells der gemeinsamen Verantwortung zu verwalten und die Tools, die Kunden nutzen können, um Sicherheit zu gewinnen, dass diese Mechanismen effektiv implementiert werden.

Einführung

AWS und seine Kunden behalten die Kontrolle über die IT-Umgebung. Sicherheit ist daher eine gemeinsame Verantwortung. Bei der Verwaltung von Sicherheit und Compliance in der AWS Cloud hat jede Partei unterschiedliche Verantwortlichkeiten. Die Verantwortung der Kunden hängt davon ab, welche Dienste sie nutzen. Im Allgemeinen sind Kunden jedoch dafür verantwortlich, ihre IT-Umgebung so aufzubauen, dass sie ihren spezifischen Sicherheits- und Compliance-Anforderungen entspricht.

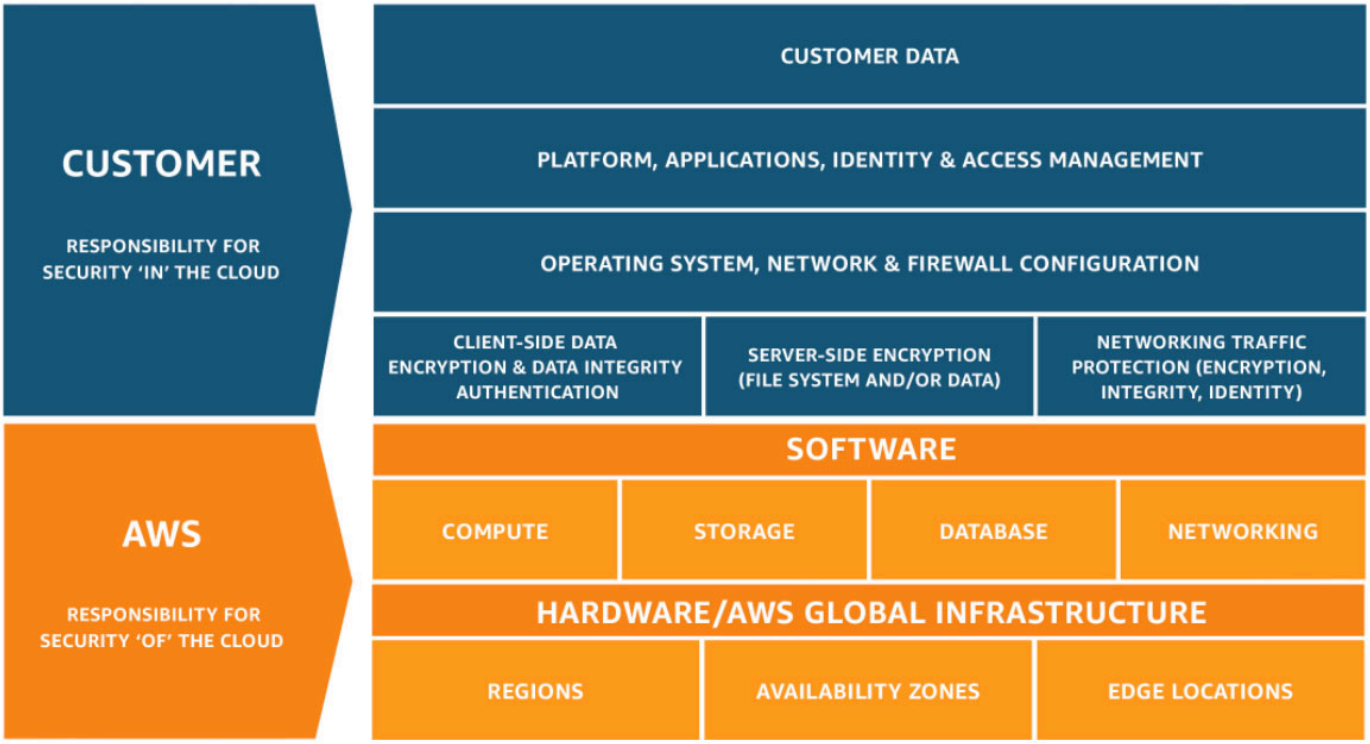
Dieses Dokument enthält weitere Einzelheiten zu den Sicherheitsverantwortungen jeder Partei und darüber, wie Kunden vom AWS-Risiko- und Compliance-Programm profitieren können.

Modell der geteilten Verantwortlichkeit

Sicherheit und Compliance stellen eine geteilte Verantwortlichkeit zwischen AWS und dem Kunden dar. Abhängig von den bereitgestellten Diensten kann dieses gemeinsam genutzte Modell dazu beitragen, die betriebliche Belastung des Kunden zu verringern. AWS betreibt, verwaltet und steuert die Komponenten des Hostbetriebssystems und der Virtualisierungsebene und sorgt zudem für die physische Sicherheit der Standorte, an denen die Services betrieben werden. Der Kunde übernimmt Verantwortung für das Gastbetriebssystem und dessen Verwaltung (einschließlich Updates und Sicherheits-Patches), für andere damit verbundene Anwendungssoftware sowie für die Konfiguration der von AWS bereitgestellten Firewall für die Sicherheitsgruppe.

Die Auswahl der Services durch den Kunden muss gut überlegt sein, da die Zuständigkeiten des Kunden von den genutzten Services, deren Integration in ihre IT-Umgebung sowie den geltenden Gesetzen und Vorschriften abhängen. Durch Nutzung von Technologien wie Host-basierte Firewalls, Host-basierte Erkennung und Verhinderung des unbefugten Eindringens in Computersysteme, Verschlüsselung und Schlüsselverwaltung können Kunden die Sicherheit erhöhen und/oder ihre strengere Compliance-Anforderungen erfüllen.

Dieses Modell der geteilten Zuständigkeiten sorgt für Flexibilität und Kundenkontrolle, durch die wir Lösungen einsetzen können, die die branchenspezifischen Anforderungen für die Zertifizierung erfüllen.



Das Modell der geteilten Verantwortung von Kunde/AWS kann auch auf IT-Kontrollen ausgedehnt werden. Ebenso wie sich AWS und seine Kunden die Verantwortung für den Betrieb der IT-Umgebung teilen, werden die Verwaltung, der Betrieb und die Überprüfung von IT-Kontrollen von den Beteiligten übernommen. AWS kann Kunden helfen, indem es die Kontrollen im Zusammenhang mit der in der AWS-Umgebung bereitgestellten physischen Infrastruktur verwaltet. Kunden können dann die ihnen zur Verfügung stehende AWS-Kontroll- und -Compliance-Dokumentation verwenden, um ggf. ihre Verfahren zur Kontrollbewertung und -überprüfung auszuführen. Beispiele dafür, wie die Verantwortung für bestimmte Kontrollen zwischen AWS und seinen Kunden geteilt wird, finden Sie im AWS-Modell der geteilten Verantwortung.

Bewerten und Integrieren von AWS-Kontrollen

AWS bietet seinen Kunden umfassende Informationen über seine IT-Kontroll-Umgebung, beispielsweise durch Whitepapers, Berichte, Zertifizierungen oder Bestätigungen von Dritten. Diese Dokumentation hilft Benutzern, mehr über die relevanten Kontrollfunktionen der von ihnen verwendeten AWS-Services zu erfahren und zu verstehen, wie diese Kontrollfunktionen eingestuft wurden. Diese Informationen helfen Kunden auch dabei, zu erkennen und zu überprüfen, ob die Kontrollen in ihrer erweiterten IT-Umgebung effektiv funktionieren.

Traditionell validieren interne und/oder externe Prüfer das Design und die betriebliche Wirksamkeit von Kontrollen durch exemplarische Vorgehensweisen und Nachweisbewertungen. Diese Art der direkten Beobachtung und Überprüfung durch den externen Prüfer des Kunden oder des Kunden wird im Allgemeinen durchgeführt, um Kontrollen in traditionellen lokalen Bereitstellungen zu validieren.

In Fällen, in denen Dienstanbieter eingesetzt werden (wie AWS), können Kunden Bescheinigungen und Zertifizierungen von Drittanbietern anfordern und bewerten. Diese Bescheinigungen und Zertifizierungen können dem Kunden helfen, das Design und die betriebliche Wirksamkeit von Kontrollzielen und Kontrollen zu gewährleisten, die von einem qualifizierten, unabhängigen Dritten validiert wurden. Obwohl einige Kontrollen möglicherweise von AWS verwaltet werden, kann die Kontrollumgebung daher immer noch ein einheitliches Framework sein, in dem Kunden sehen und überprüfen können, ob die Kontrollen effektiv funktionieren und den Compliance-Überprüfungsprozess beschleunigen können.

AWS-Bescheinigungen und Zertifizierungen von Drittanbietern bieten Kunden Transparenz und unabhängige Validierung der Steuerungsumgebung. Solche Bescheinigungen und Zertifizierungen können dazu beitragen, Kunden von der Anforderung zu entlasten, bestimmte Validierungsarbeiten für ihre IT-Umgebung in der AWS-Cloud selbst durchzuführen.

AWS Risiko- und Compliance-Programm

AWS hat ein Risiko- und Compliance-Programm im gesamten Unternehmen integriert. Dieses Programm zielt darauf ab, Risiken in allen Phasen der Serviceentwicklung und -bereitstellung zu verwalten und die risikobezogenen Aktivitäten des Unternehmens kontinuierlich zu verbessern und neu zu bewerten. Die Komponenten des integrierten AWS-Risiko- und Compliance-Programms werden in den folgenden Abschnitten ausführlicher erörtert.

AWS Risikomanagement für Unternehmen

AWS verfügt über ein Business Risk Management (BRM) -Programm, das mit AWS-Geschäftsbereichen zusammenarbeitet, um dem AWS-Verwaltungsrat und der AWS-Geschäftsleitung eine ganzheitliche Sicht auf die wichtigsten Risiken in AWS zu bieten. Das BRM-Programm demonstriert eine unabhängige Risikoüberwachung der AWS-Funktionen. Insbesondere führt das BRM-Programm Folgendes aus:

- Risikobewertungen und Risikoüberwachung der wichtigsten AWS-Funktionsbereiche
- Identifiziert und fördert die Behebung von Risiken
- Führt ein Register bekannter Risiken

Um die Beseitigung von Risiken voranzutreiben, meldet das BRM-Programm die Ergebnisse seiner Bemühungen und eskaliert gegebenenfalls an Direktoren und Vizepräsidenten im gesamten Unternehmen, um bzgl. Geschäftsentscheidungen zu informieren.

Betriebs- und Geschäftsführung

AWS verwendet eine Kombination aus wöchentlichen, monatlichen und vierteljährlichen Besprechungen und Berichten, um unter anderem die Kommunikation der Risiken über alle Komponenten des Risikomanagementprozesses hinweg sicherzustellen. Darüber hinaus implementiert AWS einen Eskalationsprozess, um dem Management Einblick in Risiken mit hoher Priorität im gesamten Unternehmen zu bieten. Diese Bemühungen zusammen tragen dazu bei, dass das Risiko im Einklang mit der Komplexität des AWS-Geschäftsmodells verwaltet wird.

Darüber hinaus sind Vizepräsidenten (Geschäftsinhaber) durch eine kaskadierende Verantwortungsstruktur für die Überwachung ihres Geschäfts verantwortlich. Zu diesem Zweck führt

AWS wöchentliche Besprechungen durch, um betriebliche Kennzahlen zu überprüfen und wichtige Trends und Risiken zu identifizieren, bevor sie sich auf das Geschäft auswirken.

Die Geschäftsleitung und die leitenden Angestellten spielen bei der Bestimmung der Firmenphilosophie und bei der Festlegung der Grundwerte des Unternehmens eine entscheidende Rolle. Jeder Mitarbeiter muss den Verhaltenskodex des Unternehmens befolgen, der in regelmäßigen Schulungen vermittelt wird. Compliance-Überprüfungen erfolgen, damit Mitarbeiter vorgegebene Richtlinien verstehen und befolgen.

Die Organisationsstruktur von AWS schafft einen Rahmen für die Planung, Ausführung und Kontrolle des Geschäftsbetriebs. Im Rahmen der Organisationsstruktur werden Rollen und Zuständigkeiten zugewiesen, um eine geeignete Stellenbesetzung, betriebliche Effizienz und Aufgabentrennung sicherzustellen. Die Geschäftsleitung hat Mitarbeitern in Schlüsselpositionen wichtige Kompetenzen eingeräumt und angemessene Berichtslwege für sie vorgesehen. Als Teil des Verifizierungsprozesses des Unternehmens für Einstellungen werden Ausbildung, bisherige Arbeitsverhältnisse und in manchen Fällen Hintergrundprüfungen einbezogen, soweit dies durch Gesetze und Regelungen für Mitarbeiter im Hinblick auf die Position des Mitarbeiters und die Zugriffsebene auf AWS-Einrichtungen angemessen ist. Neue Mitarbeiter werden in ihrer Einstellungs- und Integrationsphase von Amazon strukturiert mit den Tools, Prozessen, Systemen, Richtlinien und Verfahren des Unternehmens vertraut gemacht.

Steuerungsumgebung und Automatisierung

AWS implementiert Sicherheitskontrollen als grundlegendes Element für das Risikomanagement im gesamten Unternehmen. Die AWS-Steuerungsumgebung besteht aus den Standards, Prozessen und Strukturen, die die Grundlage für die Implementierung eines Mindestsatzes von Sicherheitsanforderungen in AWS bilden.

Während Prozesse und Standards, die in der AWS-Steuerungsumgebung enthalten sind, für sich allein stehen, nutzt AWS auch Aspekte der gesamten Steuerungsumgebung von Amazon. Zu den wirksam eingesetzten Tools gehören:

- Tools, die in allen Amazon-Unternehmen verwendet werden, z. B. das Tool zur Verwaltung der Aufgabentrennung
- Bestimmte Amazon-weite Geschäftsfunktionen wie Recht, Personalwesen und Finanzen

In Fällen, in denen AWS die allgemeine Steuerungsumgebung von Amazon nutzt, sind die Standards und Prozesse, die diese Mechanismen regeln, speziell auf das AWS-Geschäft zugeschnitten.

Das bedeutet, dass die Erwartungen für ihre Verwendung und Anwendung innerhalb der AWS-Steuerungsumgebung von den Erwartungen für ihre Verwendung und Anwendung in der gesamten Amazon-Umgebung abweichen können. Die AWS-Steuerungsumgebung dient letztlich als Grundlage für die sichere Bereitstellung von AWS-Serviceangeboten.

Die Steuerungsautomatisierung ist eine Möglichkeit für AWS, menschliche Eingriffe in bestimmte wiederkehrende Prozesse der AWS-Steuerungsumgebung zu reduzieren. Es ist der Schlüssel für eine effektive Implementierung der Informationssicherheitskontrolle und das damit verbundene Risikomanagement. Die Steuerungsautomatisierung zielt darauf ab, potenzielle Inkonsistenzen bei der Prozessausführung proaktiv zu minimieren, die aufgrund der Fehlerhaftigkeit von Menschen auftreten können, die einen sich wiederholenden Prozess ausführen. Durch die Automatisierung der Steuerung werden mögliche Prozessabweichungen eliminiert. Dies bietet ein höheres Maß an Sicherheit, dass eine Kontrolle wie vorgesehen angewendet wird.

Die Entwicklungsteams von AWS in allen Sicherheitsfunktionen sind für die Entwicklung der AWS-Steuerungsumgebung verantwortlich, um nach Möglichkeit ein höheres Maß an Steuerungsautomatisierung zu unterstützen. Beispiele für automatisierte Kontrollen bei AWS sind:

- Governance und Überwachung: Richtlinienversionierung und Genehmigung
- Personalmanagement: Automatisierte Schulungsbereitstellung, schnelle Kündigung der Mitarbeiter
- Entwicklung und Konfigurationsmanagement: Pipelines zur Codebereitstellung, Codescannen, Codesicherung, integrierte Bereitstellungstests
- Identitäts- und Zugriffsmanagement: Automatisierte Aufgabentrennung, Zugriffsprüfungen, Berechtigungsmanagement
- Überwachung und Protokollierung: Automatisierte Protokollsammlung und Korrelation, alarmierend
- Physische Sicherheit: Automatisierte Prozesse im Zusammenhang mit AWS-Rechenzentren, einschließlich Hardwareverwaltung, Sicherheitsschulungen für Rechenzentren, Zugriffsarmierung und physisches Zugriffsmanagement
- Scanning und Patch-Management: Automatisierte Schwachstellensuche, Patch-Verwaltung und Bereitstellung

Bewertung der Kontrollen und kontinuierliche Überwachung

AWS implementiert eine Vielzahl von Aktivitäten vor und nach der Servicebereitstellung, um das Risiko innerhalb der AWS-Umgebung weiter zu reduzieren. Diese Aktivitäten integrieren Sicherheits- und Compliance-Anforderungen während des Entwurfs und der Entwicklung jedes AWS-Service

und überprüfen dann, ob die Services sicher funktionieren, nachdem sie in Produktion (Einführung) gebracht wurden.

Zu den Risikomanagement- und Compliance-Aktivitäten gehören zwei Vorabaktivitäten und zwei Aktivitäten nach dem Start. Die Aktivitäten vor dem Start sind:

- Überprüfung des AWS Application Security Risikomanagements, um zu überprüfen, ob Sicherheitsrisiken identifiziert und gemindert wurden
- Überprüfung der Architekturbereitschaft, damit Kunden die Einhaltung der Compliance-Vorschriften sicherstellen können

Zum Zeitpunkt seiner Bereitstellung wurde ein Service strengen Bewertungen anhand detaillierter Sicherheitsanforderungen unterzogen, um die hohen Sicherheitsanforderungen von AWS zu erfüllen. Die Aktivitäten nach dem Start sind:

- Laufende Überprüfung von AWS Application Security, um sicherzustellen, dass der Sicherheitsstatus des Service beibehalten
- Laufende Schwachstellenverwaltungsscans

Diese Kontrollbewertungen und die kontinuierliche Überwachung ermöglichen es regulierten Kunden, sicher konforme Lösungen für AWS-Services zu entwickeln. Eine Liste der Services im Bereich verschiedener Compliance-Programme finden Sie auf der Webseite zu AWS Services in Scope.

AWS-Zertifizierungen, -Programme, -Berichte und Bescheinigungen von Drittanbietern

AWS unterzieht sich regelmäßig unabhängigen Bescheinigungsprüfungen durch Dritte, um sicherzustellen, dass die Kontrollaktivitäten wie beabsichtigt funktionieren. Insbesondere wird AWS anhand einer Vielzahl globaler und regionaler Sicherheitsrahmen geprüft, die von Region und Branche abhängen. AWS nimmt an über 50 verschiedenen Prüfprogrammen teil.

Die Ergebnisse dieser Prüfungen werden von der Bewertungsstelle dokumentiert und allen AWS-Kunden über AWS Artifact zur Verfügung gestellt. AWS Artifact ist ein kostenloses Self-Service-Portal für den On-Demand-Abruf von AWS Compliance-Berichten. Wenn neue Berichte veröffentlicht werden, werden sie in AWS Artifact verfügbar gemacht, sodass Kunden die Sicherheit und Konformität von AWS kontinuierlich überwachen und sofort auf neue Berichte zugreifen können.

Abhängig von den lokalen regulatorischen oder vertraglichen Anforderungen eines Landes oder einer Branche kann AWS auch direkt mit Kunden oder staatlichen Prüfern Prüfungen unterzogen werden. Diese Audits bieten eine zusätzliche Überwachung der AWS-Steuerungsumgebung, um sicherzustellen, dass Kunden über die Tools verfügen, mit denen sie selbstbewusst, konform und risikobasiert mit AWS-Services arbeiten können.

Weitere Informationen zu den AWS-Zertifizierungsprogrammen, Berichten und Bescheinigungen von Drittanbietern finden Sie auf der Webseite des AWS-Compliance-Programms. Sie können auch die AWS Services in Scope Webseite besuchen, um servicespezifische Informationen zu erhalten.

Cloud Security Alliance

AWS nimmt an der freiwilligen Selbstbewertung Security, Trust & Assurance Registry (STAR) der CSA teil, um zu dokumentieren, dass wir die von der CSA veröffentlichten bewährten Methoden befolgen. Der CSA ist „die weltweit führende Organisation, die sich der Definition und Sensibilisierung für Best Practices zur Gewährleistung einer sicheren Cloud-Computing-Umgebung verschrieben hat“ .Das CSA Consensus Assessments Initiative Questionnaire (CAIQ) enthält eine Reihe von Fragen, die der CSA einem Cloud-Kunden erwartet und/oder ein Cloud-Auditor würde nach einem Cloud-Anbieter fragen. Dazu zählen eine Reihe von Fragen zu Sicherheit, Kontrolle und Prozessen, die anschließend für eine breite Palette von Zwecken genutzt werden können, z. B. bei der Auswahl des Cloud-Anbieters und der Sicherheitsbewertung.

Den Kunden stehen zwei Ressourcen zur Verfügung, die die Ausrichtung von AWS an den CSA CAIQ dokumentieren. Das erste ist das CSA CAIQ Whitepaper, und das zweite ist eine detailliertere Steuerungszuordnung zu unseren SOC-2-Steuerelementen, die über AWS Artifact verfügbar ist. Weitere Informationen über die AWS-Teilnahme an CSA CAIQ finden Sie auf der AWS CSA-Website.

Cloud-Compliance-Governance für Kunden

AWS-Kunden sind für die Aufrechterhaltung einer angemessenen Governance ihrer gesamten IT-Steuerungsumgebung verantwortlich, unabhängig davon, wie oder wo die IT bereitgestellt wird. Zu den führenden Praktiken gehören:

- Verstehen der zu erfüllenden Compliance-Ziele und -Anforderungen (aus relevanten Quellen)
- Einrichten einer Kontrollumgebung, die diese Ziele und Anforderungen erfüllt
- Verstehen der erforderlichen, auf der Risikotoleranz der Organisation basierenden, Validierung
- Bestätigen der operativen Effektivität der Kontrollumgebung

Die Bereitstellung in der AWS-Cloud bietet Unternehmen unterschiedliche Möglichkeiten zum Anwenden verschiedener Arten von Kontrollen und Überprüfungsmethoden.

Eine strenge Compliance und Überwachung auf Kundenseite kann dem folgenden einfachen Ansatz folgen:

1. Überprüfung des AWS Shared Responsibility Model, der AWS-Sicherheitsdokumentation, der AWS-Konformitätsberichte und anderer von AWS verfügbarer Informationen zusammen mit anderen kundenspezifischen Dokumentationen. Versuchen Sie, so viel wie möglich von der gesamten IT-Umgebung zu verstehen, und dokumentieren Sie dann alle Compliance-Anforderungen in einem umfassenden Cloud-Control-Framework.
2. Entwerfen und Implementieren von Kontrollzielen zur Erfüllung der Compliance-Anforderungen des Unternehmens, wie im AWS Shared Responsibility Model festgelegt.
3. Identifizierung und Dokumentation von Kontrollen im Besitz externer Parteien.
4. Bestätigen, dass alle Kontrollziele erfüllt werden und alle wichtigen Kontrollen effektiv entworfen sind und betrieben werden

Wenn sich Unternehmen der Überwachung von Compliance auf diese Weise annähern, machen sie sich besser mit ihrem Kontrollumfeld vertraut und können dadurch die durchzuführenden Überprüfungsaufgaben besser erledigen.

Fazit

Die Bereitstellung einer hochsicheren und ausfallsicheren Infrastruktur und Services für unsere Kunden hat für AWS oberste Priorität. Unser Engagement für unsere Kunden konzentriert sich darauf, kontinuierlich das Vertrauen der Kunden zu gewinnen und sicherzustellen, dass die Kunden weiterhin darauf vertrauen, ihre Workloads sicher in AWS zu betreiben. Um dies zu erreichen, hat AWS Risiko- und Compliance-Mechanismen integriert, die Folgendes umfassen:

- Die Implementierung einer Vielzahl von Sicherheitskontrollen und automatisierten Tools
- Kontinuierliche Überwachung und Bewertung der Sicherheitskontrollen, um die betriebliche Effektivität von AWS und die strikte Einhaltung der Compliance-Vorschriften sicherzustellen
- Unabhängige Risikobewertung durch das AWS Business Risk Management-Programm
- Betriebs- und Geschäftsverwaltungsmechanismen

Darüber hinaus wird AWS regelmäßig unabhängigen Prüfungen durch Dritte unterzogen, um sicherzustellen, dass die Kontrollaktivitäten wie beabsichtigt funktionieren. Diese Audits bieten zusammen mit den vielen Zertifizierungen, die AWS erhalten hat, eine zusätzliche Validierungsstufe der AWS-Kontrollumgebung, von der Kunden profitieren.

Zusammen mit den vom Kunden verwalteten Sicherheitskontrollen ermöglichen diese Bemühungen AWS, im Namen der Kunden auf sichere Weise Innovationen zu entwickeln und Kunden dabei zu helfen, ihre Sicherheitslage beim Aufbau von AWS zu verbessern.

Mitwirkende

An diesem Dokument haben folgende Personen mitgewirkt:

- Marta Taggart, Senior Program Managerin, AWS-Sicherheit
- Bradley Roach, Risikomanager, AWS-Risikomanagement für Unternehmen
- Patrick Woods, leitender Sicherheitsspezialist, AWS-Sicherheit

Weitere Informationen

AWS bietet Kunden Informationen zu seiner Sicherheits- und Kontrollumgebung durch:

- Erlangung und Pflege von Branchenzertifizierungen und unabhängigen Bescheinigungen durch Dritte, wie auf der Seite des AWS-Compliance-Programms aufgeführt.
- Konsequente Veröffentlichung von Informationen über die AWS-Sicherheits- und Kontrollpraktiken in Whitepapern und Webinhalten wie dem AWS Security Blog.
- Ausführliche Beschreibungen, wie AWS Skalierung zur Verwaltung unserer Serviceinfrastruktur in der AWS Builders Library einsetzt.
- Verbesserung der Transparenz durch Bereitstellung von Konformitätszertifikaten, Berichten und anderen Dokumentationen direkt für AWS-Kunden über das Self-Service-Portal AWS Artifact.
- Bereitstellung von AWS-Compliance-Ressourcen und konsequentes Dokumentieren und Veröffentlichen von Antworten auf Fragen auf der AWS-Webseite zu Compliance
- Kunden können die Entwurfsprinzipien im AWS Well-Architected Framework befolgen, um zu erfahren, wie sie die obige Konfiguration ihrer auf AWS basierenden Workloads angehen können.

Dokumentversionen

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Update-Historie-Änderung	Update-Historie-Beschreibung	Update-Historie-Datum
Kleinere Updates	Auf technische Genauigkeit geprüft	10. März 2021
Whitepaper aktualisiert	Diese Version enthält wesentliche Änderungen, einschließlich des Entfernens der Referenzinformationen zu Compliance-Programmen und -Schemata, da diese Informationen auf den Webseiten des AWS Compliance Programs und AWS Services in Scope by Compliance Program verfügbar sind. Darüber hinaus haben wir den Abschnitt mit häufigen Compliance-Fragen entfernt, da diese Informationen jetzt auf der AWS-Website mit häufig gestellten Fragen zur Einhaltung von Vorschriften verfügbar sind.	1. November 2020
Erste Veröffentlichung	Amazon Web Services: Risiko- und Compliance-Whitepaper (Englisch)	1 Mai 2011

Hinweise

Kunden sind eigenverantwortlich für die unabhängige Bewertung der Informationen in diesem Dokument zuständig. Dieses Dokument: (a) dient rein zu Informationszwecken, (b) spiegelt die aktuellen Produktangebote und Verfahren von AWS wider, die sich ohne vorherige Mitteilung ändern können, und (c) impliziert keinerlei Verpflichtungen oder Zusicherungen seitens AWS und dessen Tochtergesellschaften, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Gewährleistungen, Zusicherungen oder Bedingungen bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden wird durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen zwischen AWS und seinen Kunden und ändert diese Vereinbarungen auch nicht.

© 2021 Amazon Web Services Inc. bzw. Tochtergesellschaften des Unternehmens. Alle Rechte vorbehalten.