Unable to locate subtitle

Amazon Web Services: programa de conformidade e gerenciamento de riscos

Amazon Web Services: programa de conformidade e gerenciamento de riscos: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services: programa de conformidade e gerenciamento de riscos

Data de publicação: 11 de março de 2021 (Revisões do documento)

Resumo

A AWS atende a uma variedade de clientes, inclusive em setores regulamentados. Por meio de nosso modelo de responsabilidade compartilhada, permitimos que os clientes gerenciem riscos de forma eficaz e eficiente no ambiente de TI e fornecemos garantia de gerenciamento de risco eficaz por meio da conformidade com estruturas e programas estabelecidos e amplamente reconhecidos. Este whitepaper descreve os mecanismos que a AWS implementou para gerenciar riscos do Modelo de Responsabilidade Compartilhada da AWS, e as ferramentas que os clientes podem aproveitar para obter garantia de que esses mecanismos sejam implementados com eficácia.

Introdução

A AWS e seus clientes compartilham o controle sobre o ambiente de TI. A segurança é uma responsabilidade compartilhada. Quando se trata de gerenciar a segurança e a conformidade na Nuvem AWS, cada parte tem responsabilidades distintas. A responsabilidade do cliente depende dos serviços que ele utiliza. No entanto, em geral, os clientes são responsáveis por criar o ambiente de TI de maneira alinhada com os requisitos específicos de segurança e conformidade.

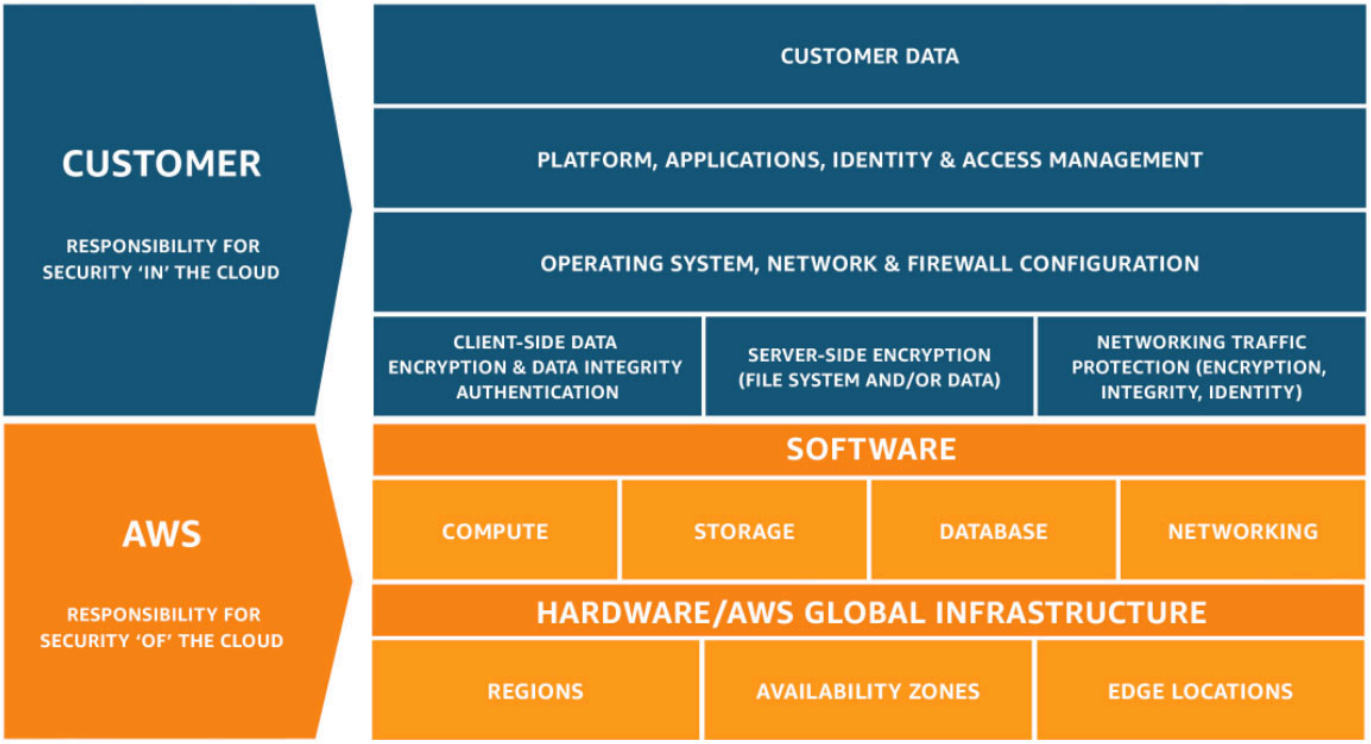
Este documento fornece mais detalhes sobre as responsabilidades de segurança de cada parte e as formas como os clientes podem aproveitar o Programa de conformidade e gerenciamento de riscos da AWS.

Modelo de responsabilidade compartilhada

Segurança e conformidade são responsabilidades compartilhadas entre a AWS e o cliente. Dependendo dos serviços implantados, esse modelo compartilhado pode ajudar a aliviar a carga operacional do cliente. É por isso que a AWS opera, gerencia e controla os componentes desde o sistema operacional de host e a camada de virtualização até a segurança física das instalações em que o serviço opera. O cliente assume o gerenciamento e a responsabilidade pelo sistema operacional convidado (inclusive atualizações e patches de segurança), por outro software de aplicação associado, além da configuração do firewall do grupo de segurança fornecido pela AWS.

É recomendável que clientes examinem cuidadosamente os serviços escolhidos, pois as responsabilidades variam de acordo com os serviços utilizados, a integração desses serviços ao ambiente de TI e as leis e regulamentos aplicáveis. Os clientes podem aumentar a segurança e/ou atender aos mais rigorosos requisitos de conformidade ao utilizar tecnologia como firewalls baseados em host, detecção/prevenção de invasões com base em host, criptografia e gerenciamento de chaves.

A natureza dessa responsabilidade compartilhada também fornece a flexibilidade e o controle do cliente, que permitem a clientes implantar soluções que atendam a requisitos de certificação específicos do setor.



Esse modelo de responsabilidade compartilhada também se estende a controles de TI. Assim como a responsabilidade de operar o ambiente de TI é compartilhada entre a AWS e os clientes, o gerenciamento, a operação e a verificação de controles de TI também são uma responsabilidade compartilhada. A AWS pode ajudar os clientes gerenciando esses controles associados à infraestrutura física implantada no ambiente da AWS. Os clientes podem usar a documentação sobre controle e conformidade da AWS para executar procedimentos de avaliação e verificação de controle, conforme necessário. Para obter exemplos de como a responsabilidade por certos controles é compartilhada entre a AWS e os clientes, consulte o Modelo de Responsabilidade Compartilhada da AWS.

Avaliação e integração de controles da AWS

A AWS fornece uma ampla variedade de informações sobre o ambiente de controle de TI por meio de artigos técnicos, relatórios, certificações e declarações de terceiros. Esta documentação ajuda os clientes a compreender os controles vigentes, relevantes aos serviços da AWS que eles usam, e como esses controles foram validados. Essas informações também ajudam os clientes a considerar e validar se os controles no ambiente de TI estendido estão operando com eficiência.

Tradicionalmente, auditores internos e/ou externos validam o projeto e a eficácia operacional de controles por meio de orientações de processo e avaliação de evidências. Esse tipo de observação e verificação direta, pelo cliente ou auditor externo do cliente, costuma ser realizado para validar controles em implantações on-premises tradicionais.

Quando provedores de serviços são usados (como a AWS), os clientes podem solicitar e avaliar declarações e certificações de terceiros. Essas declarações e certificações podem ajudar a garantir ao cliente a eficácia do projeto e operacional do objetivo de controle e dos controles validados por um terceiro qualificado e independente. Como resultado, embora alguns controles possam ser gerenciados pela AWS, o ambiente de controle ainda pode ser uma estrutura unificada em que clientes podem considerar e verificar se os controles estão operando de forma eficaz e acelerando o processo de análise de conformidade.

As declarações e certificações de terceiros da AWS oferecem aos clientes visibilidade e validação independente do ambiente de controle. Essas declarações e certificações podem ajudar a liberar os clientes da exigência de realizar certos trabalhos de validação para o ambiente de TI na Nuvem AWS.

Programa de conformidade e gerenciamento de riscos da AWS

A AWS integrou um programa de conformidade e gerenciamento de riscos em toda a organização. Este programa visa gerenciar riscos em todas as fases do design e implantação de serviços, e melhorar e reavaliar continuamente as atividades relacionadas a riscos da organização. Os componentes do programa integrado de conformidade e gerenciamento de riscos da AWS são detalhados nas seções a seguir.

Gerenciamento de riscos de negócios da AWS

A AWS tem um programa de gerenciamento de riscos de negócios (BRM) que faz parceria com as unidades de negócios da AWS para fornecer ao conselho de administração e à liderança sênior da AWS uma visão holística dos principais riscos em toda a AWS. O programa BRM demonstra supervisão de risco independente sobre as funções da AWS. O programa BRM faz o seguinte:

- Realiza avaliações e monitoramento de riscos das principais áreas funcionais da AWS.
- Identifica e conduz a correção de riscos.
- Mantém um registro de riscos conhecidos.

Para conduzir a remediação de riscos, o programa BRM relata os resultados de seus esforços e encaminha, quando necessário, para diretores e vice-presidentes da empresa a fim de informar a tomada de decisões de negócios.

Gerenciamento operacional e de negócios

A AWS usa uma combinação de reuniões e relatórios semanais, mensais e trimestrais para, entre outras coisas, garantir a comunicação de riscos em todos os componentes do processo de gerenciamento de riscos. Além disso, a AWS implementa um processo de escalação para fornecer visibilidade ao gerenciamento dos riscos de alta prioridade em toda a organização. Esses esforços, em conjunto, ajudam a garantir que o risco seja gerenciado de forma consistente com a complexidade do modelo de negócios da AWS.

Além disso, por meio de uma estrutura de responsabilidade em cascata, os vice-presidentes (proprietários de empresas) são responsáveis pela supervisão dos negócios. Para isso, a AWS

realiza reuniões semanais para analisar métricas operacionais e identificar as principais tendências e riscos antes que isso afete os negócios.

As lideranças executiva e sênior têm um papel importante na definição de valores centrais e do tom da AWS. Cada funcionário recebe o código de conduta e ética nos negócios da empresa, bem como realiza treinamentos periódicos. As auditorias de conformidade são realizadas para que os funcionários entendam e sigam as políticas estabelecidas.

A AWS fornece uma estrutura organizacional para planejar, executar e controlar as operações de negócios. A estrutura organizacional atribui funções e responsabilidades para fornecer uma equipe adequada, eficiência das operações e a segregação de funções. A gerência também estabeleceu linhas apropriadas de subordinação para a equipe principal. Os processos de verificação de contratação da empresa incluem educação, empregos anteriores e, em alguns casos, verificações de histórico na forma permitida pela legislação e pelas regulamentações trabalhistas, de acordo com o cargo do funcionário e com o nível de acesso a recursos da AWS. A empresa segue um processo estruturado de ambientação para familiarizar novos funcionários com ferramentas, processos, sistemas, políticas e procedimentos da Amazon.

Ambiente de controle e automação

A AWS implementa controles de segurança como um elemento fundamental para gerenciar riscos em toda a organização. O ambiente de controle da AWS é composto pelos padrões, processos e estruturas que fornecem a base para implementar um conjunto mínimo de requisitos de segurança em toda a AWS.

Embora os processos e padrões incluídos como parte do ambiente de controle da AWS sejam independentes, a AWS também aproveita aspectos do ambiente de controle geral da Amazon. As ferramentas utilizadas incluem:

- Ferramentas usadas em todos os negócios da Amazon, como a ferramenta que gerencia a separação de tarefas.
- Certas funções de negócios em toda a Amazon, como jurídico, recursos humanos e finanças.

Nos casos em que a AWS utiliza o ambiente de controle geral da Amazon, os padrões e processos que regem esses mecanismos são personalizados especificamente para os negócios da AWS. Isso significa que as expectativas de uso e aplicação no ambiente de controle da AWS podem diferir das expectativas para uso e aplicação no ambiente geral da Amazon. Em última análise, o ambiente de controle da AWS atua como a base para a entrega segura de ofertas de serviços da AWS.

A automação de controle é uma forma da AWS reduzir a intervenção humana em determinados processos recorrentes que compõem o ambiente de controle da AWS. Ela é fundamental para a implementação eficaz do controle de segurança da informação e o gerenciamento associado de riscos. A automação de controle busca minimizar proativamente possíveis inconsistências na execução do processo que podem surgir devido à natureza falha dos seres humanos que conduzem um processo repetitivo. Por meio da automação de controle, os possíveis desvios do processo são eliminados. Isso fornece maiores níveis de garantia de que um controle será aplicado conforme projetado.

As equipes de engenharia da AWS em todas as funções de segurança são responsáveis pela engenharia do ambiente de controle da AWS para oferecer suporte a níveis maiores de automação de controle sempre que possível. Exemplos de controles automatizados na AWS incluem:

- Governança e supervisão: versionamento e aprovação de políticas.
- Gestão de pessoal: entrega automatizada de treinamento, rescisão rápida de funcionários.
- Gerenciamento de configuração e desenvolvimento: pipelines de implantação de código, verificação de código, backup de código, teste de implantação integrada.
- Gerenciamento de identidade e acesso: segregação automatizada de funções, revisões de acesso, gerenciamento de permissões.
- Monitoramento e registro: coleta e correlação automatizadas de registros, alarmes.
- Segurança física: processos automatizados relacionados a datacenters da AWS, incluindo gerenciamento de hardware, treinamento de segurança de datacenter, alarmes de acesso e gerenciamento de acesso físico.
- Verificação e gerenciamento de patches: verificação automatizada de vulnerabilidades, gerenciamento de patches e implantação.

Avaliação de controles e monitoramento contínuo

A AWS implementa uma variedade de atividades antes e depois da implantação do serviço para reduzir ainda mais o risco no ambiente da AWS. Essas atividades integram requisitos de segurança e conformidade durante o projeto e o desenvolvimento de cada serviço da AWS e validam se os serviços estão operando com segurança depois de serem movidos para produção (lançados).

As atividades de gerenciamento de riscos e conformidade incluem duas atividades de pré-lançamento e duas de pós-lançamento. As atividades de pré-lançamento são:

- Análise do gerenciamento de riscos de segurança de aplicações da AWS para validar se os riscos foram identificados e mitigados.
- Revisão da prontidão da arquitetura para ajudar os clientes a garantir a conformidade com os regimes.

No momento de sua implantação, um serviço deverá ter passado por avaliações rigorosas em relação aos requisitos de segurança detalhados para atender aos altos padrões de segurança da AWS. As atividades pós-lançamento são:

- Análise contínua da segurança de aplicações da AWS para garantir que os procedimentos de segurança do serviço sejam mantidos.
- Verificação contínua do gerenciamento de vulnerabilidades.

Essas avaliações de controle e o monitoramento contínuo permitem que os clientes regulamentados criem com confiança soluções em conformidade nos serviços da AWS. Para obter uma lista de serviços no escopo de vários programas de conformidade, consulte a página da Web Serviços da AWS no escopo.

Certificações, programas, relatórios e declarações de terceiros da AWS

A AWS passa regularmente por auditorias independentes de certificação de terceiros para garantir que as atividades de controle operem conforme o esperado. Mais especificamente, a AWS é auditada em relação a uma variedade de estruturas de segurança globais e regionais, de acordo com a região e o setor. A AWS participa de mais de 50 programas de auditoria diferentes.

Os resultados dessas auditorias são documentados pelo órgão avaliador e disponibilizados para todos os clientes da AWS por meio do AWS Artifact. O AWS Artifact é um portal de autoatendimento gratuito para acesso sob demanda a relatórios de conformidade da AWS. Quando novos relatórios são publicados, eles são disponibilizados no AWS Artifact, permitindo que os clientes monitorem continuamente a segurança e a conformidade da AWS com acesso imediato a novos relatórios.

Dependendo dos requisitos regulatórios ou contratuais locais de um país ou setor, a AWS também pode passar por auditorias diretamente com clientes ou auditores governamentais. Essas auditorias fornecem supervisão adicional do ambiente de controle da AWS para garantir que os clientes tenham

as ferramentas necessárias para operar com confiança, em conformidade e com base em riscos usando os serviços da AWS.

Para obter informações mais detalhadas sobre os programas de certificação da AWS, relatórios e declarações de terceiros, visite a página do Programas de conformidade da AWS na Web. Você também pode visitar a página da Web Serviços da AWS no escopo para obter informações específicas do serviço.

Cloud Security Alliance

A AWS participa da autoavaliação voluntária Security, Trust & Assurance Registry (STAR – Registro de segurança, confiança e garantia) da Cloud Security Alliance (CSA) para documentar a conformidade com as práticas recomendadas publicadas pela CSA. A CSA é “a organização líder mundial dedicada a definir e aumentar a conscientização sobre as práticas recomendadas para ajudar a garantir um ambiente de computação em nuvem seguro”. O Consensus Assessments Initiative Questionnaire (CAIQ – Questionário da iniciativa de avaliações de consenso) da CSA fornece um conjunto de perguntas que ela antecipa que um cliente e/ou auditor de nuvem faria a um provedor de nuvem. Ele fornece uma série de perguntas sobre segurança, controle e processo, que podem ser usadas de diversas formas, incluindo avaliação de segurança e seleção de provedor de nuvem.

Há dois recursos disponíveis para os clientes que documentam o alinhamento da AWS com o CAIQ da CSA. O primeiro é o whitepaper CSA CAIQ e o segundo é um mapeamento de controle mais detalhado para nossos controles SOC-2 que está disponível via AWS Artifact. Para obter mais informações sobre a participação da AWS no CAIQ da CSA, consulte o site do AWS CSA.

Conformidade e governança do cliente na nuvem

Os clientes da AWS são responsáveis por manter a governança adequada em todo o ambiente de controle de TI, independentemente de como ou onde a TI é implantada. As principais práticas incluem:

- Compreender os objetivos de conformidade e os requisitos necessários (de fontes relevantes).
- Estabelecer um ambiente controlado que atenda a esses objetivos e requisitos.
- Compreender a validação requisitada baseada na tolerância de risco da organização.
- Verificar a eficácia operacional do ambiente de controle.

A implantação na Nuvem AWS oferece às empresas diferentes opções para aplicar diversos tipos de controles e vários métodos de verificação.

A forte conformidade e governança do cliente pode incluir a seguinte abordagem básica:

1. Analisar o Modelo de Responsabilidade Compartilhada da AWS, a documentação de segurança da AWS, relatórios de conformidade da AWS e outras informações disponíveis na AWS, junto com outras documentações específicas do cliente. Tente entender ao máximo o ambiente de TI inteiro e, depois, documente todos os requisitos de conformidade em uma estrutura de controle de nuvem abrangente.
2. Projetar e implementar objetivos de controle para atender aos requisitos de conformidade da empresa, conforme estabelecido no Modelo de Responsabilidade Compartilhada da AWS.
3. Identificar e documentar controles de propriedade de terceiros.
4. Verificar se todos os objetivos de controle são atendidos e se os controles principais foram projetados e operam de forma eficaz.

Abordar a governança de conformidade dessa forma ajudará os clientes a compreender melhor o ambiente de controle e a delinear claramente as atividades de verificação a serem executadas.

Conclusão

Fornecer infraestrutura e serviços altamente seguros e resilientes aos clientes é uma das principais prioridades da AWS. Nosso compromisso com os clientes está focado em trabalhar para conquistar continuamente a confiança dos clientes e garantir que eles mantenham a confiança na operação segura de workloads na AWS. Para conseguir isso, a AWS integrou mecanismos de conformidade e gerenciamento de riscos que incluem:

- A implementação de uma ampla variedade de controles de segurança e ferramentas automatizadas.
- Monitoramento e avaliação contínuos dos controles de segurança para ajudar a garantir a eficácia operacional da AWS e a adesão estrita aos regimes de conformidade.
- Avaliação de risco independente pelo programa AWS Business Risk Management.
- Mecanismos de gerenciamento operacional e de negócios.

Além disso, a AWS passa regularmente por auditorias independentes de terceiros para garantir que as atividades de controle operem conforme o esperado. Essas auditorias, além das muitas certificações que a AWS obteve, fornecem um nível adicional de validação do ambiente de controle da AWS que beneficia os clientes.

Quando somados aos controles de segurança gerenciados pelo cliente, esses esforços permitem que a AWS inove com segurança em nome dos clientes e os ajude a melhorar os procedimentos de segurança ao criar na AWS.

Colaboradores

Os colaboradores desse documento incluem:

- Marta Taggart, gerente sênior de programas, Segurança da AWS
- Bradley Roach, gerente de riscos, gerenciamento de riscos comerciais da AWS
- Patrick Woods, especialista sênior em segurança, Segurança da AWS

Leitura adicional

A AWS fornece aos clientes informações sobre o ambiente de segurança e controle ao:

- Obter e manter certificações do setor e declarações independentes de terceiros, conforme listado na página Programa de conformidade da AWS.
- Publicar de forma consistente informações sobre as práticas de segurança e controle da AWS em whitepapers e conteúdo da Web, como o Blog de segurança da AWS.
- Fornecer descrições detalhadas de como a AWS utiliza a automação em escala para gerenciar nossa infraestrutura de serviços na AWS Builders Library.
- Aumentar a transparência fornecendo certificados de conformidade, relatórios e outras documentações diretamente a clientes da AWS por meio do portal de autoatendimento conhecido como AWS Artifact.
- Fornecer recursos de conformidade da AWS e documentar e publicar de maneira consistente respostas a consultas na página da Web Perguntas frequentes sobre conformidade da AWS.
- Os clientes podem seguir os princípios de design no AWS Well-Architected Framework para obter orientação sobre como abordar a configuração acima da linha de workloads criados na AWS.

Revisões do documento

Para ser notificado sobre atualizações deste whitepaper, inscreva-se no RSS feed.

update-history-change	update-history-description	update-history-date
Atualizações menores	Revisado quanto à precisão técnica	10 de março de 2021
Whitepaper atualizado	Esta versão inclui alterações substanciais, como a remoção de informações de referência sobre programas e esquemas de conformidade, pois essas informações estão disponíveis nas páginas da Web Programas de conformidade da AWS e Serviços da AWS no escopo pelo programa de conformidade. Além disso, removemos a seção que cobre questões comuns de conformidade porque essas informações agora estão disponíveis na página da Web Perguntas frequentes sobre conformidade da AWS.	1 de novembro de 2020
Publicação inicial	Publicação do whitepaper Amazon Web Services: programa de conformidade e gerenciamento de riscos	1 de maio de 2011

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento. Este documento é: (a) fornecido apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não cria nenhum compromisso ou garantia da AWS e suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos no “estado em que se encontram”, sem garantias, declarações ou condições de qualquer tipo, explícitas ou implícitas. As responsabilidades e obrigações da AWS com seus clientes são regidas por contratos da AWS, e este documento não modifica nem faz parte de nenhum contrato entre a AWS e seus clientes.