Visão geral dos riscos e da conformidade da AWS

Janeiro de 2017

Avisos

Este documento é fornecido apenas para fins informativos. Ele relaciona as atuais ofertas de produtos e práticas da AWS a contar da data de emissão deste documento, que estão sujeitas a alterações sem aviso prévio. Os clientes são responsáveis por fazer sua própria avaliação independente das informações deste documento e de qualquer uso dos produtos ou serviços da AWS, cada um dos quais é fornecido “no estado em que se encontra”, sem garantia de qualquer tipo, expressa ou implícita. Este documento não cria quaisquer garantias, representações, compromissos contratuais ou condições da AWS, suas afiliadas, seus fornecedores ou licenciadores. As responsabilidades da AWS com seus clientes são controladas pelos contratos da AWS, e este documento não modifica nem faz parte de qualquer contrato entre a AWS e seus clientes.

Índice

Resumo

Este documento fornece informações básicas para ajudar clientes a integrar a AWS em sua estrutura de controle existente, incluindo uma abordagem básica para avaliar os controles da AWS.

Introdução

A AWS e seus clientes compartilham o controle sobre o ambiente de TI. A participação da AWS nesta responsabilidade compartilhada inclui fornecer seus serviços em uma plataforma altamente segura e controlada, bem como disponibilizar uma grande variedade de recursos de segurança para uso pelos clientes. A responsabilidade dos clientes inclui a configuração de seus ambientes de TI de forma segura e controlada para os seus propósitos. Mesmo se os clientes não comunicarem o seu uso e as suas configurações para a AWS, a AWS comunica a sua segurança e o ambiente de controle relevante para os clientes. A AWS faz isso da seguinte maneira:

- Obtendo certificações do setor e declarações de terceiros independentemente do descrito neste documento.
- Publicando informações sobre as práticas de controle e segurança da AWS nos whitepapers e no conteúdo do site.
- Fornecendo certificados, relatórios e outra documentação diretamente para clientes da AWS mediante acordo de confidencialidade (ou NDA, Non-Disclosure Agreement), conforme necessário.

Para obter uma descrição mais detalhada da segurança da AWS, consulte o Centro de segurança da AWS.

Para obter uma descrição mais detalhada sobre a conformidade da AWS, consulte a página Conformidade com a AWS.

Adicionalmente, o whitepaper AWS Overview of Security Processes cobre os controles gerais de segurança e a segurança específica dos serviços da AWS.

Ambiente de responsabilidade compartilhada

A movimentação da infraestrutura de TI para os serviços da AWS cria um modelo de responsabilidade compartilhada entre o cliente e a AWS. Esse modelo compartilhado pode auxiliar a reduzir os encargos operacionais do cliente na medida em que a AWS opera, gerencia e controla os componentes do sistema operacional do host e a camada de virtualização, incluindo a segurança física das instalações em que o serviço opera. O cliente assume a gestão e a responsabilidade pelo sistema operacional convidado (inclusive atualizações e patches de segurança), por outro software de aplicativo associado, bem como

pela configuração do firewall do grupo de segurança fornecido pela AWS. Os clientes devem examinar cuidadosamente os serviços que escolherem, pois suas respectivas responsabilidades variam de acordo com os serviços utilizados, a integração desses serviços ao seu ambiente de TI e as leis e regulamentos aplicáveis. Os clientes podem aumentar a segurança e/ou atender aos seus mais rigorosos requisitos de conformidade utilizando tecnologias como firewalls baseados em hosts, detecção/prevenção de intrusões baseadas em host, criptografia e gerenciamento de chaves. A natureza desta responsabilidade compartilhada também fornece a flexibilidade e o controle do cliente que permitem a implantação de soluções que atendem aos requisitos de certificação específicos do setor.

Esse modelo de responsabilidade compartilhada entre o cliente e a AWS também se estende aos controles de TI. Assim como a responsabilidade para operar o ambiente de TI é compartilhada entre a AWS e os seus clientes, o mesmo ocorre com o gerenciamento, a operação e a verificação de controles compartilhados de TI. A AWS pode auxiliar a reduzir os encargos operacionais de controles do cliente gerenciando os controles associados à infraestrutura física implementada no ambiente da AWS que, anteriormente, eram gerenciados pelo cliente. Já que cada cliente é implementado de forma diferente na AWS, os clientes podem aproveitar a mudança de gerenciamento de determinados controles de TI para a AWS, resultando em um (novo) ambiente de controle distribuído. Os clientes podem utilizar a documentação de conformidade e controle da AWS disponível (descrita em Declarações de terceiros e certificações da AWS) para realizar procedimentos de avaliação e verificação de controle, conforme necessário.

Governança rígida de conformidade

Como sempre, os clientes da AWS têm de continuar a manter uma governança adequada sobre todo o ambiente de controle de TI, independentemente de como a TI é implementada. As principais práticas incluem a compreensão dos objetivos de conformidade e requisitos exigidos (com base em fontes relevantes), a criação de um ambiente de controle que atenda a esses requisitos e objetivos, uma compreensão de validação necessária com base na tolerância ao risco da organização e a verificação da eficácia operacional do ambiente de controle da organização. A implementação na nuvem da AWS oferece às empresas opções diferentes para aplicar diversos tipos de controles e vários métodos de verificação.

Gestão e conformidade rígida do cliente podem incluir a seguinte abordagem básica:

1. Revise as informações disponíveis na AWS juntamente com outras informações para entender o máximo possível sobre o ambiente de TI e, em seguida, documente todos os requisitos de conformidade.
2. Projete e implemente os objetivos de controle para atender aos requisitos de conformidade corporativa.
3. Identifique e documente controles pertencentes a terceiros.
4. Verifique se todos os objetivos de controle são atendidos e todos os controles principais foram projetados com eficiência e se apresentam com bom funcionamento.

Abordar a gestão de conformidade dessa forma ajudará as empresas a obterem uma melhor compreensão do ambiente de controle e ajudará a delinear claramente as atividades de verificação a serem executadas.

Avaliação e integração dos controles da AWS

A AWS fornece uma ampla variedade de informações relacionadas ao seu ambiente de controle de TI por meio de whitepapers, relatórios, certificações e depoimentos de terceiros. Esta documentação ajuda os clientes a compreenderem os controles vigentes relevantes aos serviços da AWS que eles usam e como esses controles foram validados. Essas informações ajudam os clientes a prestarem contas e a validarem se os controles no seu ambiente de TI estendido estão operando de modo eficaz.

Tradicionalmente, o projeto e a eficácia operacional de objetivos de controle e controles são validados por auditores internos e/ou externos através do acompanhamento do processo e da avaliação de evidências. A observação/verificação direta, pelo cliente ou auditor externo do cliente, é geralmente realizada para validar controles. No caso de utilização de prestadores de serviços, tais como a AWS, solicita-se que as empresas avaliem declarações de terceiros e certificações a fim de obter uma garantia razoável do projeto e eficácia operacional do objetivo de controle e dos controles. Como resultado, embora os controles essenciais do cliente possam ser gerenciados pela AWS, o ambiente de controle ainda pode ser uma estrutura unificada, onde todos os

controles são considerados e verificados como operacionais com eficácia. Declarações de terceiros e certificações da AWS podem não apenas fornecer um nível mais alto de validação do ambiente de controle, mas podem também eximir os clientes do requisito de terem de realizar determinados trabalhos de validação para seu ambiente de TI na nuvem da AWS.

Informações de controle de TI da AWS

A AWS fornece informações de controle de TI aos clientes das seguintes maneiras:

Definição de controle específico. Os clientes da AWS podem identificar os principais controles gerenciados pela AWS. Controles essenciais são críticos para o ambiente de controle do cliente e exigem uma declaração externa da eficácia operacional desses controles essenciais para que possam estar em ordem com os requisitos de conformidade — tais como a auditoria financeira anual. Para esse fim, a AWS publica uma ampla variedade de controles de TI específicos em seu relatório de controles organizacionais de serviço 1 (SOC 1), tipo II. O relatório SOC 1, anteriormente o relatório de declaração sobre as normas de auditoria (SAS) nº 70, empresas de serviços, é um padrão de auditoria amplamente reconhecido desenvolvido pelo American Institute of Certified Public Accountants (AICPA). A auditoria SOC 1 é uma auditoria aprofundada do projeto e da eficácia operacional de atividades de controle e objetivos de controle definidos da AWS (que incluem objetivos de controle e atividades de controle sobre a parte da infraestrutura que a AWS gerencia). O “tipo II” refere-se ao fato de que cada um dos controles descritos no relatório não é avaliado apenas em relação à adequação do projeto, mas também é testado em relação à eficácia operacional pelo auditor externo. Em virtude da independência e competência do auditor externo da AWS, os controles identificados no relatório devem fornecer aos clientes um elevado nível de confiança no ambiente de controle da AWS. Os controles da AWS podem ser considerados desenvolvidos e operacionais com eficácia para muitos fins de conformidade, incluindo auditorias de demonstrativos financeiros de acordo com a seção 404 da Sarbanes-Oxley (SOX). A utilização de relatórios SOC 1 tipo II geralmente também é permitida por outros órgãos externos de certificação (p.ex., auditores do ISO 27001 podem solicitar um relatório SOC 1 tipo II para concluir suas avaliações para os clientes).

Outras atividades de controle específicas relacionam-se à conformidade com a Payment Card Industry (PCI, Setor de cartões de pagamento) e a Federal Information Security Management Act (FISMA, Lei federal de gerenciamento de segurança da informação) da AWS. A AWS está em conformidade com os padrões da FISMA, nível moderado, e com o padrão de segurança de dados do PCI. Os padrões do PCI e da FISMA são muito prescritivos e requerem uma validação independente de que a AWS está aderindo aos padrões publicados.

Conformidade padrão do controle geral. Se um cliente da AWS requer que um amplo conjunto de objetivos de controle seja atendido, é possível realizar uma avaliação das certificações do setor da AWS. Com a certificação ISO 27001 da AWS, a AWS está em conformidade com um amplo e abrangente padrão de segurança e segue as práticas recomendadas para manter um ambiente seguro. Com o PCI Data Security Standard (PCI DSS, padrão de segurança de dados do PCI), a AWS está em conformidade com um conjunto de controles importantes para as empresas que lidam com informações de cartão de crédito. Com a conformidade da AWS com os padrões da FISMA, a AWS está em conformidade com uma ampla variedade de controles específicos exigidos pelas agências governamentais americanas. A conformidade com esses padrões gerais disponibiliza aos clientes informações detalhadas sobre a natureza abrangente dos controles e processos de segurança em vigor e pode ser considerada ao gerenciar a conformidade.

Regiões globais da AWS

Os datacenters são construídos em clusters em várias regiões globais, incluindo: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), AWS GovCloud (EUA) (Oregon), UE (Frankfurt), UE (Irlanda), Ásia-Pacífico (Seul), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio), Ásia-Pacífico (Sydney), China (Pequim) e América do Sul (São Paulo).

Para ver uma lista completa das regiões, consulte a página Infraestrutura global da AWS.

Programa de conformidade e riscos da AWS

A AWS fornece informações sobre seu programa de conformidade e gerenciamento de riscos para permitir que os clientes incorporem controles da AWS em sua estrutura de gestão. Essas informações podem ajudar os clientes a documentar uma estrutura de gestão e de controle completa com a AWS incluída como uma parte importante dessa estrutura.

Gerenciamento de risco

A gerência da AWS desenvolveu um plano estratégico de negócios, que inclui a identificação de riscos e a implementação de controles para reduzir ou gerenciar riscos. A gerência da AWS avalia o plano estratégico de negócios pelo menos duas vezes por ano. Esse processo requer que o gerenciamento identifique riscos em suas áreas de responsabilidade, bem como implemente medidas adequadas projetadas para solucionar esses riscos.

Além disso, o ambiente de controle da AWS está sujeito a várias avaliações internas e externas de riscos. As equipes de segurança e conformidade da AWS estabeleceram políticas e uma estrutura de segurança da informação com base na estrutura dos Control Objectives for Information and related Technology (COBIT, Objetivos de controle para informações e tecnologia relacionada) e integraram com eficácia a estrutura certificável pela ISO 27001, com base nos controles da ISO 27002, nos Princípios de serviços de confiança do AICPA (American Institute of Certified Public Accountants), no PCI DSS v3.1 e na Publicação 800-53 Rev. 3 (Controles de segurança recomendados para sistemas de informação federais) do National Institute of Standards and Technology (NIST). A AWS mantém a política de segurança, oferece treinamento de segurança para os funcionários e realiza revisões de segurança do aplicativo. Essas avaliações verificam a confidencialidade, a integridade e a disponibilidade de dados, bem como a conformidade com a política de segurança da informação.

A segurança da AWS examina regularmente todos os endereços IP de endpoint de serviço voltados à Internet quanto à existência de vulnerabilidades (essas verificações não incluem instâncias de clientes). A segurança da AWS notificará as partes adequadas para solucionar quaisquer vulnerabilidades identificadas. Além disso, avaliações de ameaça de vulnerabilidade externa são realizadas regularmente por empresas de segurança independentes. As conclusões e

recomendações resultantes dessas avaliações são categorizadas e entregues à liderança da AWS. Essas verificações são feitas para avaliar a saúde e a viabilidade da infraestrutura subjacente da AWS e não se destinam a substituir as verificações de vulnerabilidade do cliente necessárias para atender aos seus requisitos de conformidade específicos. Os clientes podem solicitar permissão para conduzir pesquisas de sua infraestrutura em nuvem, contanto que elas se limitem a instâncias do cliente e não violem a política de uso aceitável da AWS. A prévia aprovação para esses tipos de verificações pode ser iniciada enviando-se uma solicitação por meio do formulário AWS Vulnerability/Penetration Testing Request (Solicitação de teste de penetração/vulnerabilidade da AWS).

Ambiente de controle

A AWS gerencia um ambiente de controle abrangente que inclui políticas, processos e atividades de controle que utilizam diversos aspectos do ambiente de controle geral da Amazon. Esse ambiente de controle está em vigor para a entrega segura de ofertas de serviços da AWS. O ambiente de controle coletivo abrange as pessoas, os processos e a tecnologia necessários para estabelecer e manter um ambiente que ofereça suporte à eficácia operacional da estrutura de controle da AWS. A AWS integrou controles específicos de nuvem aplicáveis identificados pelos principais órgãos do setor de computação em nuvem na estrutura de controle da AWS. A AWS continua acompanhando esses grupos de setor quanto a ideias sobre como as práticas de liderança podem ser implementadas para melhor atender aos clientes no gerenciamento de seu ambiente de controle.

O ambiente de controle na Amazon começa no mais alto nível da empresa. As lideranças executiva e sênior desempenham um papel importante no estabelecimento de valores fundamentais e do objetivo da empresa. Cada funcionário recebe o código de ética e conduta nos negócios da empresa, além de realizar treinamento periódico. 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 diferenciação de direitos. A gerência também estabeleceu autoridade e 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 seu nível de acesso aos recursos da AWS. A empresa segue um processo estruturado de integração para familiarizar novos funcionários com as ferramentas, processos, sistemas, políticas e procedimentos da Amazon.

Segurança da informação

A AWS implementou um programa formal de segurança da informação, o qual foi desenvolvido para proteger a confidencialidade, integridade e disponibilidade de sistemas e dados dos clientes. A AWS publicou um whitepaper de segurança que está disponível no site público. Ele aborda como a AWS pode ajudar os clientes a proteger seus dados.

Contato com a AWS

Os clientes podem solicitar os relatórios e as certificações produzidas pelos nossos auditores terceirizados ou solicitar mais informações sobre a conformidade da AWS entrando em contato com o departamento de desenvolvimento de vendas e negócios da AWS. O representante encaminha os clientes para a equipe adequada dependendo da natureza da consulta. Para obter informações adicionais sobre a conformidade da AWS, consulte o site Conformidade da AWS ou envie perguntas diretamente para mailto:awscompliance@amazon.com.

Outras fontes de leitura

Para obter informações adicionais, consulte estas fontes:

- Questionário da iniciativa de avaliação de consenso da CSA
- Certificações, programas, relatórios e atestados de terceiros da AWS
- Respostas da AWS para as principais questões de conformidade

Revisões do documento

Data	Descrição
Janeiro de 2017	Migração para novo modelo
Janeiro de 2016	Primeira publicação