Unable to locate subtitle

Amazon Web Services : Risques et conformité

Amazon Web Services : Risques et conformité: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services : Risques et conformité

Date de publication : 11 mars 2021 (Révisions du document)

Résumé

AWS est au service de nombreux clients, y compris ceux des secteurs réglementés. Grâce à notre modèle de responsabilité partagée, nous permettons aux clients de gérer les risques de manière efficace et efficiente dans l'environnement informatique, et nous garantissons une gestion efficace des risques grâce à notre conformité aux cadres et programmes établis et largement reconnus. Ce document présente les mécanismes mis en place par AWS pour gérer les risques côté AWS du modèle de responsabilité partagée, ainsi que les outils que les clients peuvent utiliser pour s'assurer pleinement de l'implémentation efficace desdits mécanismes.

Introduction

AWS et ses clients partagent le contrôle de l'environnement informatique. La sécurité est donc une responsabilité partagée. En ce qui concerne la gestion de la sécurité et de la conformité dans le cloud AWS, chaque partie a des responsabilités distinctes. La responsabilité d'un client dépend des services qu'il utilise. Cependant, en général, les clients sont responsables de la construction de leur environnement informatique d'une manière qui correspond à leurs exigences spécifiques en matière de sécurité et de conformité.

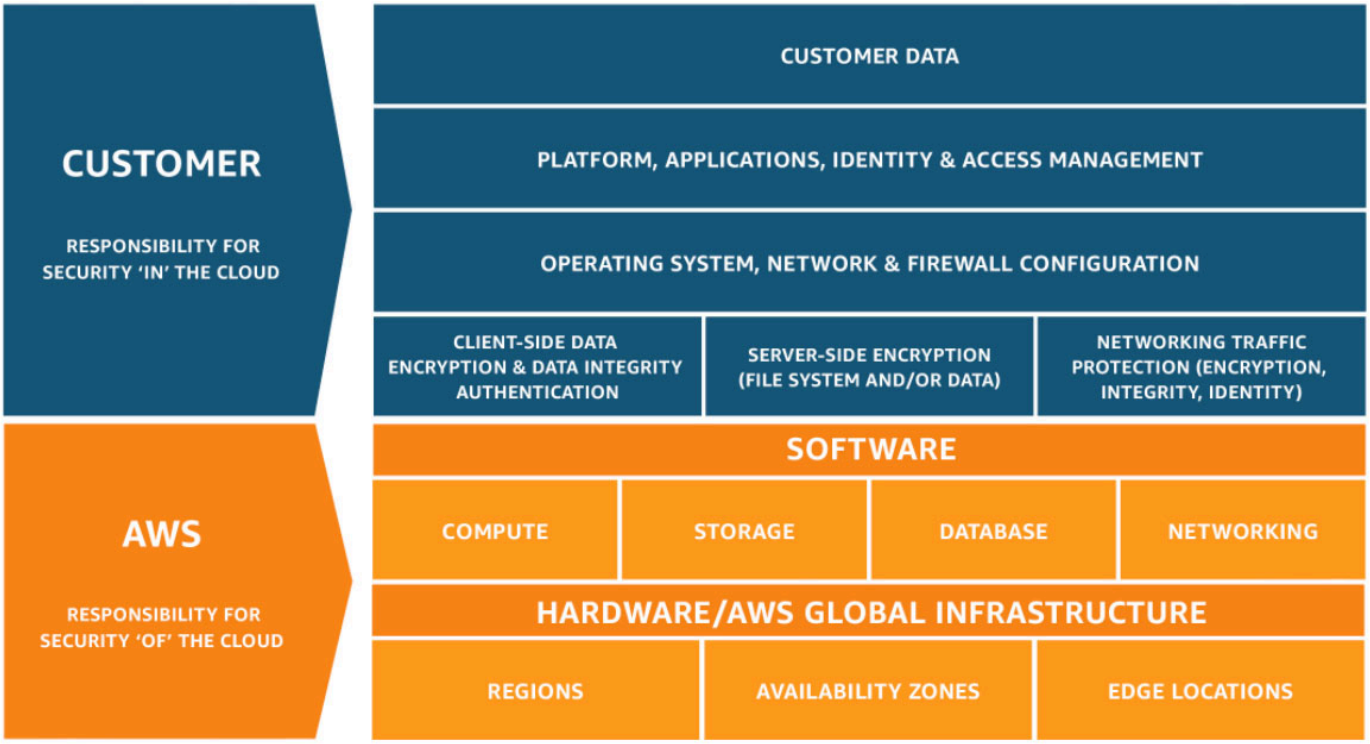
Ce livre blanc fournit plus de détails sur les responsabilités de chaque partie en matière de sécurité et sur la manière dont les clients peuvent bénéficier du programme AWS de gestion des risques et de la conformité.

Modèle de responsabilité partagée

AWS et le client se partagent la responsabilité d'assurer la sécurité et la conformité. Selon les services déployés, ce modèle partagé peut aider à alléger la charge opérationnelle du client. En effet, les services AWS exploitent, gèrent et contrôlent les composants depuis le système d'exploitation hôte jusqu'à la sécurité physique des installations dans lesquelles les services sont exploités, en passant par la couche de virtualisation. Le client assume toujours la responsabilité et la gestion du système d'exploitation « invité » (notamment les mises à jour et les correctifs de sécurité) et d'autres logiciels d'application connexes, en plus de la configuration du pare-feu du groupe de sécurité fourni par AWS.

Nous recommandons que les clients choisissent attentivement les services, car leurs responsabilités varient en fonction des services utilisés, de l'intégration de ces services dans leur environnement informatique, ainsi que de la législation et de la réglementation applicables. Les clients ont la possibilité de renforcer la sécurité et/ou de satisfaire à des exigences de conformité plus strictes en exploitant des technologies telles que les pare-feu basés sur l'hôte, la détection et la prévention des intrusions sur l'hôte, le chiffrement et la gestion de clés.

La nature de cette responsabilité partagée offre, en outre, une flexibilité et un contrôle du client permettant le déploiement de solutions qui remplissent les exigences de certification spécifiques du secteur.



Ce modèle de responsabilité partagée s'étend également aux contrôles informatiques. De la même manière que l'exploitation de l'environnement informatique est partagée entre AWS et ses clients, la gestion, l'utilisation et la vérification des contrôles informatiques sont elles aussi une responsabilité partagée. AWS peut aider les clients en gérant les contrôles associés à l'infrastructure physique déployée dans l'environnement AWS. Les clients peuvent alors utiliser la documentation disponible sur le contrôle et la conformité d'AWS pour réaliser leurs procédures d'évaluation et de vérification, le cas échéant. Pour obtenir des exemples de partage de la responsabilité de certains contrôles entre AWS et ses clients, consultez le modèle de responsabilité partagée d'AWS.

Évaluation et intégration des contrôles AWS

AWS fournit à ses clients une grande variété d'informations concernant son environnement de contrôle informatique par le biais de documents techniques, de rapports et de certifications, ainsi que d'attestations délivrées par des organismes tiers. Cette documentation aide les clients à comprendre les contrôles en place liés aux services AWS qu'ils utilisent et comment ces contrôles ont été validés. Ces informations aident également les clients à déterminer et à vérifier que les contrôles de leur environnement informatique étendu fonctionnent efficacement.

Traditionnellement, les auditeurs internes et/ou externes valident la conception et l'efficacité opérationnelle des contrôles par des procédures pas à pas et une évaluation des preuves. Ce type d'observation et de vérification directes, par le client ou l'auditeur externe du client, est généralement effectué pour valider les contrôles dans les déploiements traditionnels sur site.

Dans le cas où des prestataires de services sont utilisés (tels qu'AWS), les clients peuvent demander et évaluer des attestations et des certifications tierces. Ces attestations et certifications peuvent aider à garantir au client la conception et l'efficacité opérationnelle de l'objectif de contrôle et des contrôles validés par un tiers qualifié et indépendant. Par conséquent, bien que certains contrôles puissent être gérés par AWS, l'environnement de contrôle peut toujours être un cadre unifié dans lequel les clients peuvent comptabiliser et vérifier que les contrôles fonctionnent efficacement et accélèrent le processus d'examen de conformité.

Les attestations et certifications tierces d'AWS fournissent aux clients une visibilité et une validation indépendante de l'environnement de contrôle. Ces attestations et certifications peuvent aider à soulager les clients de l'obligation d'effectuer eux-mêmes certains travaux de validation pour leur environnement informatique dans le cloud AWS.

Programme AWS de gestion des risques et de la conformité

AWS a intégré un programme de gestion des risques et de la conformité dans l'ensemble de l'organisation. Ce programme vise à gérer les risques à toutes les étapes de la conception et du déploiement des services et à améliorer et réévaluer continuellement les activités liées aux risques de l'organisation. Les composants du programme intégré de gestion des risques et de la conformité d'AWS sont abordés plus en détail dans les sections suivantes.

Gestion des risques commerciaux AWS

AWS dispose d'un programme de gestion des risques commerciaux (BRM) qui s'associe aux unités commerciales AWS pour fournir au conseil d'administration et à la haute direction d'AWS une vue globale des risques clé au sein d'AWS. Le programme BRM démontre une surveillance indépendante des risques sur les fonctions AWS. Plus précisément, le programme BRM réalise les opérations suivantes :

- Évalue et surveille les risques dans les domaines fonctionnels clé d'AWS
- Identifie et pilote la remédiation des risques
- Tient à jour un registre des risques connus

Pour favoriser la remédiation des risques, le programme BRM rend compte des résultats de ses efforts et, si nécessaire, en informe les directeurs et les vice-présidents de l'entreprise pour éclairer la prise de décisions commerciales.

Gestion opérationnelle et commerciale

AWS utilise une combinaison de réunions et de rapports hebdomadaires, mensuels et trimestriels pour, entre autres, garantir la communication des risques sur tous les composants du processus de gestion des risques. En outre, AWS met en œuvre un processus de remontée pour fournir une visibilité de la direction sur les risques hautement prioritaires au sein de l'organisation. Ensemble, ces efforts contribuent à garantir que les risques sont gérés de manière cohérente avec la complexité du modèle commercial AWS.

En outre, grâce à une structure de responsabilité en cascade, les vice-présidents (propriétaires d'entreprise) sont responsables de la surveillance de leur entreprise. À cette fin, AWS organise des

réunions hebdomadaires pour examiner les métriques opérationnelles et identifier les risques et tendances clé avant qu'ils n'affectent l'activité.

Les cadres et dirigeants jouent un rôle essentiel dans la mise en place des valeurs essentielles à AWS et donnent le ton. Chaque employé se voit remettre le code de déontologie et d'éthique de l'entreprise, et doit régulièrement suivre une formation. Des audits de conformité sont réalisés afin que les employés comprennent et suivent les politiques mises en place.

L'organigramme d'AWS fournit un cadre pour la planification, l'exécution et le contrôle des opérations métier. Cet organigramme organisationnel inclut des rôles et des responsabilités afin de s'assurer d'une dotation en personnel adéquate, de l'efficacité des opérations et de la séparation des fonctions. La direction a également pris soin d'établir les rapports hiérarchiques appropriés pour les postes clés. Les procédures de vérification lors du recrutement de personnel pour la société incluent la vérification des diplômes, des emplois précédents et, dans certains cas, des antécédents, conformément à la législation et la réglementation en vigueur et en rapport avec les fonctions occupées et le niveau d'accès aux installations AWS. L'entreprise suit une démarche structurée d'accueil afin que les nouveaux employés se familiarisent avec les outils, les processus, les systèmes, les politiques et les procédures d'Amazon.

Environnement de contrôle et automatisation

AWS met en œuvre des contrôles de sécurité en tant qu'élément fondamental pour gérer les risques au sein de l'organisation. L'environnement de contrôle AWS comprend les normes, les processus et les structures qui fournissent la base pour la mise en œuvre d'un ensemble minimum d'exigences de sécurité sur AWS.

Alors que les processus et les normes inclus dans l'environnement de contrôle AWS sont autonomes, AWS exploite également certains aspects de l'environnement de contrôle global d'Amazon. Les outils exploités incluent :

- Outils utilisés dans toutes les activités Amazon, tels que l'outil qui gère la séparation des tâches
- Certaines fonctions commerciales à l'échelle d'Amazon, telles que les services juridiques, les ressources humaines et les finances

Dans les cas où AWS exploite l'environnement de contrôle global d'Amazon, les normes et les processus qui régissent ces mécanismes sont spécifiquement adaptés à l'activité d'AWS. Cela signifie que les attentes relatives à leur utilisation et à leur application au sein de l'environnement

de contrôle AWS peuvent différer des attentes relatives à leur utilisation et à leur application dans l'environnement Amazon global. L'environnement de contrôle AWS sert finalement de base à la prestation sécurisée des offres de services AWS.

L'automatisation du contrôle permet à AWS de réduire l'intervention humaine dans certains processus récurrents comprenant l'environnement de contrôle AWS. Elle est essentielle à la mise en œuvre efficace du contrôle de la sécurité de l'information et à la gestion des risques. L'automatisation du contrôle vise à minimiser de manière proactive les incohérences potentielles dans l'exécution des processus qui pourraient survenir sous la forme d'erreurs humaines au cours de processus répétitifs. Grâce à l'automatisation du contrôle, les éventuels écarts de processus sont éliminés. Elle offre ainsi de meilleurs niveaux d'assurance qu'un contrôle appliqué tel qu'il a été conçu.

Les équipes d'ingénierie d'AWS pour l'ensemble des fonctions de sécurité sont responsables de l'ingénierie de l'environnement de contrôle AWS afin de prendre en charge de meilleurs niveaux d'automatisation du contrôle dès que possible. Voici des exemples de contrôles automatisés chez AWS :

- Gouvernance et surveillance : gestion des versions et approbation des politiques
- Gestion du personnel : offre de formation automatisée, licenciement rapide des employés
- Gestion du développement et de la configuration : pipelines de déploiement de code, analyse du code, sauvegarde du code, test de déploiement intégré
- Identity and Access Management : séparation automatisée des tâches, vérifications des accès, gestion des autorisations
- Surveillance et journalisation : collecte et corrélation automatisées des journaux, alarmes
- Sécurité physique : processus automatisés liés aux centres de données AWS, y compris la gestion du matériel, la formation à la sécurité des centres de données, les alarmes d'accès et la gestion des accès physiques
- Analyse et gestion des correctifs : analyse automatique des vulnérabilités, gestion des correctifs et déploiement

Évaluation des contrôles et surveillance continue

AWS met en œuvre diverses activités avant et après le déploiement du service afin de réduire davantage les risques au sein de l'environnement AWS. Ces activités intègrent les exigences de sécurité et de conformité lors de la conception et du développement de chaque service AWS, puis valident que les services fonctionnent en toute sécurité après leur mise en production (lancement).

Les activités de gestion des risques et de la conformité comprennent deux activités préalables au lancement et deux activités postérieures au lancement. Les activités préalables au lancement sont les suivantes :

- Évaluation de la gestion des risques liés à la sécurité des applications AWS pour vérifier que les risques de sécurité ont été identifiés et atténués
- Évaluation de l'état de préparation de l'architecture pour aider les clients à garantir la conformité

Au moment de son déploiement, un service aura fait l'objet d'évaluations rigoureuses par rapport à des exigences de sécurité détaillées afin de répondre aux exigences élevées d'AWS en matière de sécurité. Les activités postérieures au lancement sont les suivantes :

- Évaluation continue de la sécurité des applications AWS pour garantir le maintien de la posture de sécurité des services
- Analyse continue de la gestion des vulnérabilités

Ces évaluations de contrôle et cette surveillance continue permettent aux clients réglementés de créer en toute confiance des solutions conformes sur les services AWS. Pour obtenir la liste des services concernés par les différents programmes de conformité, consultez la page web Services AWS concernés.

Certifications AWS, programmes, rapports et attestations d'organismes tiers

AWS fait régulièrement l'objet d'audits d'attestation tiers indépendants afin de garantir que les activités de contrôle fonctionnent comme prévu. Plus précisément, AWS fait l'objet d'un audit par rapport à divers cadres de sécurité mondiaux et régionaux en fonction de la région et du secteur d'activité. AWS participe à plus de 50 programmes d'audit différents.

Les résultats de ces audits sont documentés par l'organisme d'évaluation et mis à la disposition de tous les clients AWS via AWS Artifact. AWS Artifact est un portail en libre-service sans frais offrant un accès à la demande aux rapports de conformité AWS. Lorsque de nouveaux rapports sont publiés, ils sont mis à disposition dans AWS Artifact, ce qui permet aux clients de contrôler en permanence la sécurité et la conformité d'AWS avec un accès immédiat aux nouveaux rapports.

En fonction des exigences réglementaires ou contractuelles locales d'un pays ou d'un secteur d'activité, AWS peut également subir des audits directement auprès de clients ou d'auditeurs

gouvernementaux. Ces audits fournissent une supervision supplémentaire de l'environnement de contrôle AWS afin de garantir que les clients disposent des outils nécessaires pour fonctionner en toute confiance, en conformité et en fonction des risques en utilisant les services AWS.

Pour plus d'informations sur les programmes de certification AWS, les rapports et les attestations tierces, consultez la page web du programme de conformité AWS. Vous pouvez également consulter la page web Services AWS concernés pour obtenir des informations spécifiques au service.

Cloud Security Alliance (CSA)

AWS participe bénévolement à l'auto-évaluation STAR (Security, Trust & Assurance Registry) de Cloud Security Alliance (CSA) afin de documenter sa conformité aux bonnes pratiques publiées par CSA. CSA est « la première organisation au monde dédiée à la définition et à la sensibilisation aux bonnes pratiques afin de garantir un environnement de cloud computing sécurisé » .Le CAIQ (Consensus Assessments Initiative Questionnaire) de CSA fournit un ensemble de questions anticipées par CSA qu'un client du cloud et/ou qu'un auditeur de cloud poserait à un fournisseur de cloud. Il inclut une série de questions sur la sécurité, les contrôles et les procédures qui peuvent servir à diverses fins, notamment pour choisir un fournisseur de cloud et en évaluer la sécurité.

Deux ressources sont mises à la disposition des clients pour documenter l'alignement d'AWS sur le CAIQ de CSA. La première est le livre blanc CAIQ de CSA et la deuxième est un mappage de contrôle plus détaillé avec nos contrôles SOC-2, disponible via AWS Artifact. Pour plus d'informations sur la participation d'AWS au CAIQ de CSA, veuillez consulter le site AWS CSA.

Gouvernance de conformité du cloud client

Les clients AWS ont la responsabilité de maintenir une gouvernance adéquate sur l'ensemble de leur environnement de contrôle informatique, quel que soit le mode et l'endroit où l'informatique est déployée. Les principales pratiques incluent :

- La compréhension des objectifs et des exigences de conformité requis (en s'appuyant sur des sources pertinentes)
- L'établissement d'un environnement de contrôle qui répond à ces objectifs et ces exigences
- La compréhension de la validation nécessaire en fonction de la tolérance au risque de l'organisation
- La vérification de l'efficacité opérationnelle de leur environnement de contrôle

Le déploiement au sein du cloud AWS permet aux entreprises de choisir entre différentes options afin d'appliquer divers types de contrôles et différentes méthodes de vérification.

Une conformité et une gouvernance stricte du client en termes peuvent nécessiter une approche de base de ce type :

1. Examiner le modèle de responsabilité partagée d'AWS, la documentation de sécurité AWS, les rapports de conformité AWS et d'autres informations disponibles auprès d'AWS, ainsi que d'autres documents spécifiques au client. Essayez de comprendre autant que possible l'ensemble de l'environnement informatique, puis documentez toutes les exigences de conformité dans un cadre de contrôle du cloud complet.
2. Concevez et mettez en œuvre des objectifs de contrôle pour répondre aux exigences de conformité de l'entreprise telles que définies dans le modèle de responsabilité partagée d'AWS.
3. Identifiez et documentez les contrôles détenus par des tiers.
4. Vérifiez la réalisation de tous les objectifs de contrôle clé, ainsi que de la conception et de l'exécution efficaces de tous les contrôles clés.

En adoptant une telle approche de conformité en matière de gouvernance, les clients acquièrent une meilleure compréhension de leur environnement de contrôle et peuvent plus facilement détailler clairement les opérations de vérification à effectuer.

Conclusion

Fournir une infrastructure et des services hautement sécurisés et résilients à nos clients est une priorité absolue pour AWS. Notre engagement envers nos clients est axé sur le fait de continuellement gagner la confiance des clients et de garantir que les clients restent confiants dans l'exploitation sécurisée de leurs charges de travail sur AWS. Pour y parvenir, AWS a intégré des mécanismes de gestion des risques et de la conformité qui incluent :

- La mise en œuvre d'un large éventail de contrôles de sécurité et d'outils automatisés
- La surveillance et l'évaluation continues des contrôles de sécurité pour garantir l'efficacité opérationnelle d'AWS et le strict respect des régimes de conformité
- L'évaluation indépendante des risques par le programme de gestion des risques commerciaux AWS
- Des mécanismes de gestion opérationnelle et commerciale

En outre, AWS fait régulièrement l'objet d'audits tiers indépendants afin de garantir que les activités de contrôle fonctionnent comme prévu. Ces audits, ainsi que les nombreuses certifications qu'AWS a obtenues, fournissent un niveau supplémentaire de validation de l'environnement de contrôle AWS dont bénéficient les clients.

Associés aux contrôles de sécurité gérés par le client, ces efforts permettent à AWS d'innover en toute sécurité pour le compte des clients et d'aider les clients à améliorer leur posture de sécurité lorsqu'ils s'appuient sur AWS.

Participants

Les contributeurs à ce document sont les suivants :

- Marta Taggart, responsable de programme principale, sécurité AWS
- Bradley Roach, responsable des risques, gestion des risques commerciaux AWS
- Patrick Woods, spécialiste de la sécurité principal, sécurité AWS

Autres lectures

AWS fournit aux clients des informations concernant son environnement de sécurité et de contrôle en :

- Obtenant et en maintenant des certifications sectorielles et des attestations tierces indépendantes, telles qu'elles figurent sur la page du programme de conformité AWS.
- Publiant régulièrement des informations sur les pratiques de sécurité et de contrôle d'AWS dans des livres blancs et du contenu web, comme le blog sur la sécurité AWS.
- Fournissant des descriptions détaillées de la façon dont AWS utilise l'automatisation à grande échelle pour gérer notre infrastructure de services dans l'Amazon Builders' Library.
- Améliorant la transparence en fournissant des certificats de conformité, des rapports et d'autres documents directement aux clients AWS via le portail en libre-service connu sous le nom d'AWS Artifact.
- Fournissant des ressources de conformité AWS, et en documentant et en publiant systématiquement les réponses aux questions sur la page web des Questions fréquentes (FAQ) sur la conformité AWS.
- Les clients peuvent suivre les principes de conception énoncés dans l'AWS Well-Architected Framework pour savoir comment aborder la configuration rentable de leurs charges de travail basées sur AWS.

Révisions du document

Pour être informé des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

update-history-change	update-history-description	update-history-date
Mises à jour mineures	Exactitude technique vérifiée	10 mars 2021
Livre blanc mis à jour	Cette version inclut des modifications importantes qui comprennent la suppression des informations de référence sur les programmes et les schémas de conformité, car ces informations sont disponibles sur les pages web des Programmes de conformité AWS et des Services AWS concernés par le programme de conformité. En outre, nous avons supprimé la section traitant des questions de conformité courantes, car ces informations sont désormais disponibles sur la page web des Questions fréquentes (FAQ) sur la conformité AWS.	1er novembre 2020
Publication initiale	Amazon Web Services : livre blanc sur les risques et la conformité publié	1er mai 2011

Mentions légales

Les clients sont chargés d'évaluer par eux-même les informations contenues dans ce document. Le présent document : (a) est fourni à titre informatif uniquement, (b) représente les offres et pratiques actuelles de produits AWS, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ou assurance de la part d'AWS et de ses affiliés, fournisseurs ou concédants de licences. Les produits ou services AWS sont fournis « en l'état » sans garantie, représentation ou condition, de quelque nature que ce soit, explicite ou implicite. Les responsabilités et obligations d'AWS envers ses clients sont déterminées par les contrats AWS, et le présent document ne fait pas partie d'un contrat entre AWS et ses clients, ni le modifie.