Guide de l'utilisateur AWS du programme des marchandises contrôlées (PMC)

Novembre 2022

Avis

Les clients sont responsables de leur propre évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre d'information uniquement, (b) décrit les offres et pratiques actuelles d'AWS, lesquelles peuvent être modifiées sans préavis, et (c) ne peut constituer un engagement ou une garantie de la part d'AWS et de ses filiales, fournisseurs ou concédants de licence. Les produits ou services d'AWS sont fournis « tels quels » sans garantie, représentation ou condition d'aucune sorte, qu'elle soit expresse ou implicite. Les responsabilités et engagements d'AWS envers ses clients sont contrôlés par les contrats AWS. Le présent document ne fait partie d'aucun contrat entre AWS et ses clients et n'en modifie aucun.

Table des matières

Résumé

Ce document fournit des informations pour aider les organisations canadiennes de défense et de sécurité réglementées par Services publics et Approvisionnements Canada (SPAC) dans le cadre du Programme des marchandises contrôlées (PMC) à adopter et à accélérer leur utilisation du nuage Amazon Web Services (AWS).

Ce guide décrit les rôles respectifs joués par le client et par AWS dans la gestion et la sécurisation de l'environnement de nuage, donne un aperçu des exigences réglementaires et des directives de SPAC. Il fournit également des ressources supplémentaires que les organisations de défense et de sécurité peuvent utiliser pour concevoir et architecturer leur environnement AWS afin que celui-ci soit sécurisé et réponde aux attentes réglementaires du PMC.

Introduction

Amazon Web Services (AWS) est la plateforme infonuagique la plus complète et la plus largement adoptée au monde, offrant plus de 200 services complets à partir de centres de données répartis dans le monde entier. Des millions de clients, notamment les jeunes pousses à croissance rapide, les très grandes entreprises et les principaux organismes gouvernementaux, font confiance à AWS pour réduire leurs coûts, devenir plus agiles et innover plus rapidement. AWS est conçu pour être l'environnement infonuagique le plus flexible et le plus sécurisé actuellement sur le marché. Notre infrastructure principale répond aux exigences de sécurité de la défense, des banques mondiales et d'autres organisations ultra-sensibles. Elle s'appuie sur une série d'outils de sécurité dans le nuage, avec 230 services et fonctionnalités de sécurité, de conformité et de gouvernance.

Le Programme des marchandises contrôlées (PMC) est un régime d'enregistrement et de conformité obligatoire établi par le gouvernement du Canada et géré par Services publics et Approvisionnement Canada (SPAC). Le programme, encadré par la loi sur la production de défense et par le règlement sur les marchandises contrôlées, régit l'examen, la possession ou le transfert des marchandises contrôlées sur le plan national. Les marchandises contrôlées sont des marchandises, des composants et des données techniques qui présentent une importance militaire ou liée à la sécurité nationale, notamment les articles contrôlés par l'International Traffic in Arms Regulations (ITAR) des États-Unis.

Ce guide est une ressource destinée à aider les organisations de défense et de sécurité à comprendre les exigences de sécurité du PMC lorsqu'elles utilisent AWS. Il comprend une description du cadre de conformité AWS, ainsi que des outils et des mesures de sécurité avancés que les organisations de défense et de sécurité peuvent utiliser pour évaluer, respecter et démontrer leur conformité aux exigences réglementaires applicables dans le cadre du PMC.

Une analyse complète du règlement sur les marchandises contrôlées dépasse le cadre de ce guide. Toutefois, les sections présentées dans la liste suivante abordent les considérations qui surviennent le plus fréquemment dans les interactions avec les organisations de défense et de sécurité au Canada ; elles fournissent également des informations que ces organisations peuvent utiliser pour mieux comprendre les responsabilités d'AWS et leurs propres responsabilités à l'égard du PMC :

- **Sécurité et responsabilité partagée.** Il est important que les organisations de défense et de sécurité comprennent le modèle de responsabilité partagée d'AWS avant d'explorer les exigences spécifiques du PMC. Le modèle de responsabilité partagée d'AWS est fondamental pour comprendre les rôles respectifs du client et d'AWS en matière de sécurité. Il informe sur les mesures que les organisations de défense et de sécurité doivent prendre pour s'assurer de démontrer leur conformité au règlement sur les marchandises contrôlées.
- **Infrastructure mondiale du nuage AWS.** L'infrastructure mondiale du nuage AWS est construite autour de régions et de zones de disponibilité. L'infrastructure mondiale du nuage AWS offre aux clients d'AWS un moyen plus simple et plus efficace de concevoir et d'exploiter des applications et des services, en permettant à ces ressources d'être plus hautement disponibles, plus tolérantes aux pannes et plus évolutives que des environnements traditionnels sur site. Les clients d'AWS peuvent utiliser l'infrastructure mondiale du nuage AWS pour concevoir un environnement AWS conforme à leurs besoins opérationnels et réglementaires, notamment par rapport aux exigences du PMC.
- **Programmes de conformité AWS.** AWS a obtenu des certifications et des attestations de tierces parties pour une variété d'applications spécifiques aux secteurs. AWS a également développé des programmes de conformité pour que ces ressources soient mises à la disposition des clients. Les organisations de défense et de sécurité peuvent utiliser les programmes de conformité AWS pour les aider à satisfaire leurs exigences en matière de réglementation.
- **Programme de marchandise contrôlée.** Cette section présente les considérations communes aux organisations de défense et de sécurité lorsqu'elles examinent certaines des principales exigences du PMC. Elle décrit également comment ces organisations peuvent utiliser les services et les outils AWS pour démontrer leur conformité aux exigences applicables en matière de réglementation. L'annexe de ce guide, Annexe : Considérations AWS pour le programme des marchandises contrôlées, fournit une liste non exhaustive des exigences et des considérations correspondantes lors de l'utilisation d'AWS.

Ce document contient seulement un échantillon non exhaustif de considérations. Il ne constitue pas un conseil juridique ou de conformité ; les clients doivent consulter leurs propres équipes juridiques et de conformité.

Sécurité et responsabilité partagée

Le modèle de responsabilité partagée d'AWS est fondamental pour comprendre les rôles respectifs du client et d'AWS dans le contexte des principes de sécurité du nuage. Il est important que les organisations de défense et de sécurité comprennent le modèle avant d'explorer les exigences spécifiques du PMC.

La sécurité du nuage est une responsabilité partagée. La sécurité dans le nuage est la responsabilité du client. Cela signifie que les clients conservent le contrôle du programme de sécurité qu'ils choisissent de mettre en œuvre pour protéger leurs propres contenus, applications, systèmes et réseaux, comme ils le feraient pour des applications dans un centre de données sur site.

AWS gère la sécurité du nuage en veillant à ce que l'infrastructure du nuage AWS soit conforme aux exigences réglementaires et aux bonnes pratiques mondiales et régionales. AWS exploite, gère et contrôle les composants informatiques, depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles les services fonctionnent.

Le modèle de responsabilité partagée est présenté sous forme de graphique dans la Figure 1.

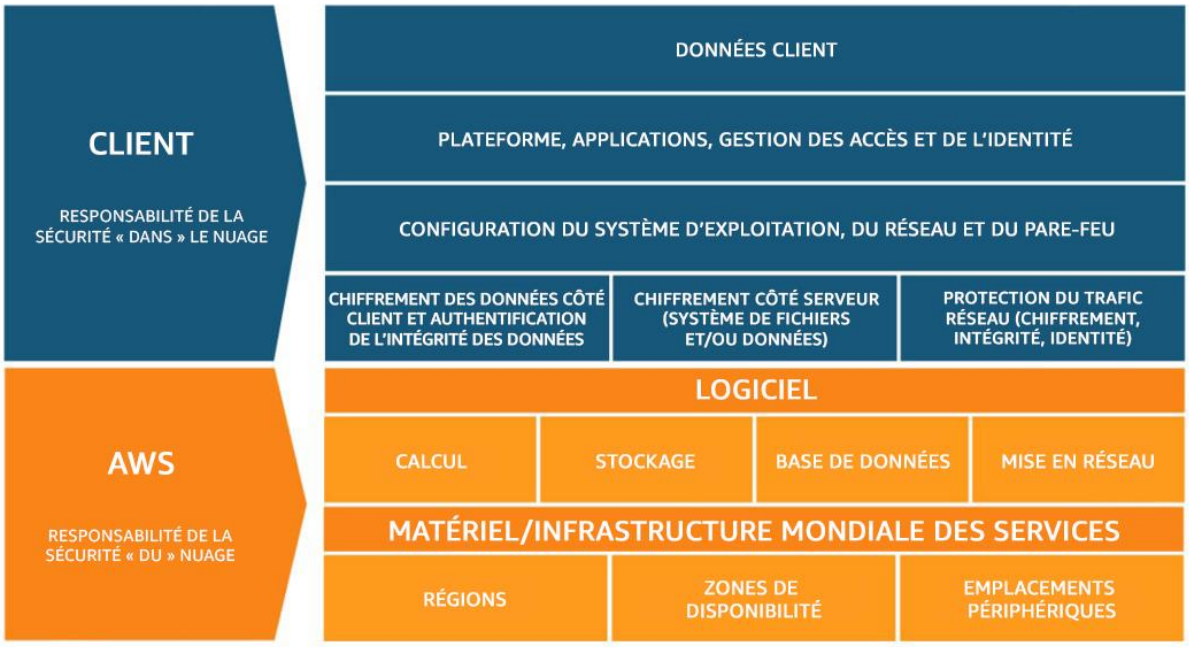

Figure 1 : Modèle de responsabilité partagée d'AWS

Sécurité dans le nuage

Les clients sont responsables de leur sécurité dans le nuage. Les clients d'AWS sont responsables de la gestion des systèmes d'exploitation invités (y compris l'installation des mises à jour et des correctifs de sécurité) et des autres logiciels d'application associés, ainsi que de tous les contrôles de sécurité réseau applicables. Les clients doivent examiner attentivement les services qu'ils choisissent, car leurs responsabilités varient en fonction des services qu'ils utilisent, de l'intégration de ces services dans leur environnement informatique et des lois et réglementations applicables. Il est important de noter que lors de l'utilisation des services AWS, les clients conservent le contrôle de leur contenu et sont responsables de la gestion des exigences critiques de sécurité du contenu, notamment :

- Le contenu qu'ils choisissent de stocker sur AWS
- Les services AWS qui sont utilisés avec le contenu
- Le pays dans lequel leur contenu est stocké
- Le format et la structure de leur contenu et si celui-ci est masqué, anonymisé ou chiffré
- La façon dont leurs données sont chiffrées et l'emplacement de stockage des clés
- Qui a accès à leur contenu et la façon dont ces droits d'accès sont accordés, gérés et révoqués

Étant donné que ce sont les clients, et non AWS, qui contrôlent ces facteurs importants, les clients restent responsables de leurs choix. La responsabilité du client est déterminée par les services de nuage AWS qu'il choisit. Il en découle un calcul de l'ampleur des opérations de configuration à exécuter par les clients dans le cadre de leurs responsabilités en matière de sécurité. Par exemple, un service comme Amazon Elastic Compute Cloud (Amazon EC2) exige du client qu'il effectue toutes les tâches de configuration et de gestion de la sécurité nécessaires pour un ordinateur à usage général. Les clients qui déploient une instance Amazon EC2 sont responsables de la gestion du système d'exploitation invité (notamment des mises à jour et des correctifs de sécurité), de tout logiciel d'application ou utilitaire installé par le client sur l'instance, ainsi que de la configuration du pare-feu fourni par AWS (appelé groupe de sécurité) sur chaque instance. Pour des services d'extraction, tels que Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB, AWS exploite la couche d'infrastructure, le système d'exploitation et les plateformes, et les clients accèdent aux points de terminaison des services pour stocker et récupérer les données. Les clients sont tenus de gérer leurs données (notamment les options de chiffrement), de classifier leurs ressources et d'utiliser les outils de gestion des identités et des accès pour appliquer les autorisations appropriées.

Sécurité du nuage

L'infrastructure et les services AWS sont autorisés à opérer dans le cadre de plusieurs normes de conformité et certifications industrielles dans différents pays et secteurs. Les clients peuvent utiliser les certifications de conformité AWS pour valider la mise en œuvre et l'efficacité des contrôles de sécurité AWS, notamment les bonnes pratiques et les certifications de sécurité reconnues au niveau international.

Le programme de conformité AWS s'appuie sur les actions suivantes :

- **Valider** que les services et les installations AWS à travers le monde conservent un environnement de contrôle omniprésent qui fonctionne de manière efficace. L'environnement de contrôle AWS englobe les personnes, les processus et la technologie nécessaires pour établir et gérer un environnement qui soutient l'efficacité opérationnelle du cadre de contrôle AWS. AWS a intégré dans son cadre de contrôle des contrôles applicables spécifiques au nuage identifiés par les principaux organismes du secteur infonuagique. AWS surveille ces groupes industriels afin d'identifier les pratiques de pointe que les clients peuvent mettre en œuvre et d'aider davantage les clients à gérer leur environnement de contrôle.
- **Démontrer** la posture de conformité d'AWS pour aider les clients à vérifier la conformité aux exigences industrielles et gouvernementales. AWS s'engage auprès d'organismes de certification externes et d'auditeurs indépendants pour fournir aux clients des informations concernant les politiques, les processus et les contrôles établis et exploités par AWS. Les clients peuvent utiliser ces informations pour exécuter leurs procédures d'évaluation et de vérification des contrôles, comme l'exige la norme de conformité applicable.
- **Surveiller**, par l'intermédiaire de contrôles de sécurité applicables, qu'AWS reste conforme aux normes et aux bonnes pratiques mondiales.

Programme de conformité AWS

Le programme de conformité AWS aide les clients à comprendre les contrôles robustes en place chez AWS pour conserver la sécurité et la conformité dans le nuage. En associant des fonctionnalités de service axées sur la gouvernance et faciles à auditer à des normes de conformité ou d'audit applicables, les outils de conformité AWS s'appuient sur des programmes traditionnels et aident les clients à établir et à exploiter un environnement de contrôle de la sécurité AWS.

Certifications et attestations tierces

AWS a obtenu des certifications et des attestations de tierces parties indépendantes pour une variété d'applications mondiales et spécifiques aux secteurs. Les points suivants sont particulièrement pertinents pour les organisations canadiennes de défense et de sécurité réglementées par le PMC :

- **Centre canadien pour la cybersécurité (CCC).** Dans le cadre de son processus d'évaluation de la sécurité des TI des fournisseurs de services d'informatique en nuage (ITSM.50.100), le Centre canadien pour la cybersécurité évalue les services infonuagiques pour s'assurer qu'ils répondent aux exigences de sécurité du gouvernement du Canada. Cette évaluation est une exigence obligatoire pour qu'AWS puisse fournir des services infonuagiques aux ministères et aux organismes du gouvernement fédéral canadien. À ce jour, 120 services AWS ont été évalués par l'intermédiaire du profil des mesures de la sécurité d'informatique en nuage moyen du CCC, qui convient aux informations et aux systèmes classés jusqu'à la catégorie PROTÉGÉ B/Intégrité moyenne/Disponibilité moyenne. Pour de plus amples informations, veuillez consulter la page Web Évaluation CCC.
- **SOC.** Les rapports de contrôles des systèmes et des organisations (SOC) sont des rapports d'examens indépendants effectués par une tierce partie qui démontrent comment AWS respecte les principaux contrôles et objectifs en termes de conformité. L'objectif de ces rapports est d'aider les clients et leurs auditeurs à comprendre les contrôles AWS qui ont été établis pour soutenir les opérations et la conformité. Pour de plus amples informations, veuillez consulter la page Web Conformité SOC.

  Il existe deux types de rapport AWS SOC particulièrement pertinents :

  - **SOC 2.** Fournit aux clients et aux utilisateurs de leurs services ayant un besoin professionnel une évaluation indépendante de l'environnement de contrôle AWS concernant la sécurité, la disponibilité et la confidentialité des systèmes.
  - **SOC 3.** Fournit aux clients et aux utilisateurs de leurs services ayant un besoin professionnel une évaluation indépendante de l'environnement de contrôle AWS concernant la sécurité, la disponibilité et la confidentialité des systèmes, sans divulguer les informations internes AWS.

- La norme **ISO 27001** est une norme de gestion de la sécurité qui spécifie les bonnes pratiques de gestion de la sécurité et tous les contrôles de sécurité qui suivent les directives de bonnes pratiques de la norme ISO 27002. La base de cette certification est le développement et la mise en œuvre d'un programme de sécurité rigoureux, notamment un système de gestion de la sécurité de l'information qui définit la façon dont AWS gère en permanence la sécurité de manière holistique et complète. Pour de plus amples informations sur la certification ISO 27001 d'AWS ou pour la télécharger, veuillez consulter la page Web Conformité ISO 27001.
- La norme **ISO 27017** fournit des directives sur les aspects de sécurité des informations infonuagiques, recommandant la mise en œuvre de contrôles de sécurité des informations spécifiques au nuage qui complètent les directives des normes ISO 27001 et ISO 27002. Ce code de pratique fournit des directives supplémentaires sur la mise en œuvre des contrôles de sécurité, qui sont spécifiques aux fournisseurs de services infonuagiques. Pour de plus amples informations sur la certification ISO 27017 d'AWS ou pour la télécharger, veuillez consulter la page Web Conformité ISO 27017.
- La norme **ISO 22301** spécifie les exigences pour qu'une organisation mette en œuvre, maintienne et améliore un système de gestion de la continuité des activités. Le respect de cette norme garantit qu'AWS dispose de systèmes efficaces pour prévenir, préparer, répondre et récupérer d'événements inattendus et perturbateurs. Cela aide également les clients à atteindre et à respecter les normes de résilience et de sécurité les plus élevées. Pour de plus amples informations sur la certification ISO 22301 d'AWS ou pour la télécharger, veuillez consulter la page Web Conformité ISO 22301.

En associant des fonctionnalités de service axées sur la gouvernance et faciles à auditer à des certifications, à des attestations et à des normes d'audit applicables, les outils de conformité AWS s'appuient sur des programmes traditionnels et aident les clients à établir et à exploiter un environnement AWS.

Pour de plus amples informations sur les certifications et les attestations AWS, veuillez consulter la page Web Programme de conformité AWS. Pour de plus amples informations sur les contrôles de sécurité généraux et sur la sécurité spécifique aux services d'AWS, veuillez consulter la page Web Bonnes pratiques pour la sécurité, l'identité et la conformité.

AWS Artifact

Les clients peuvent télécharger des rapports et des détails sur plus de 2 600 contrôles de sécurité par l'intermédiaire d'AWS Artifact, un portail automatisé de rapports de conformité disponible dans la console de gestion AWS. Le portail AWS Artifact offre un accès à la demande aux documents relatifs à la sécurité et à la conformité d'AWS, notamment les rapports SOC, les évaluations CCC et les certifications des organismes d'accréditation dans toutes les régions du monde et dans tous les secteurs de conformité.

Programme des marchandises contrôlées

Le Programme des marchandises contrôlées (PMC) est un régime d'enregistrement et de conformité obligatoire établi par le gouvernement du Canada et géré par SPAC (Services publics et Approvisionnement Canada). Le programme, encadré par la Loi sur la production de défense et par le règlement sur les marchandises contrôlées, régit l'examen, la possession ou le transfert des marchandises contrôlées sur le plan national. Les marchandises contrôlées sont des marchandises, des composants et des données techniques qui présentent une importance militaire ou liée à la sécurité nationale, notamment les articles contrôlés par l'International Traffic in Arms Regulations (ITAR) des États-Unis.

Les organisations doivent s'inscrire au PMC pour examiner, posséder ou transférer des marchandises contrôlées au Canada. Elles doivent également respecter les conditions d'inscription précisées dans le règlement sur les marchandises contrôlées. Chaque déclarant est tenu d'établir et de mettre en œuvre un plan de sécurité qui définit, notamment, les procédures utilisées pour contrôler l'examen, la possession et le transfert des marchandises contrôlées, ainsi que les procédures utilisées pour signaler et enquêter sur les violations de sécurité.

Enregistrement des fournisseurs de services infonuagiques

Le 9 avril 2021, SPAC a publié des directives concernant l'utilisation des services infonuagiques. Les directives exigent que les fournisseurs de services infonuagiques soient enregistrés dans le PMC. Elles stipulent également que les déclarants doivent vérifier qu'un fournisseur de services infonuagiques détient une inscription PMC valide avant de stocker leurs données PMC dans le nuage.

Amazon Web Services Canada, Inc. est un déclarant dans le PMC et notre inscription figure dans le répertoire des inscriptions PMC.

Plan de sécurité des déclarants

Le règlement sur les marchandises contrôlées précise les conditions qu'une organisation doit remplir pour être inscrite au PMC. Dans le cadre de ce guide, la clause la plus pertinente est la section 10(e). Cette clause exige qu'un déclarant établisse et mette en œuvre un plan de sécurité qui énonce, notamment, les procédures utilisées pour contrôler l'examen, la possession et le transfert de marchandises contrôlées, ainsi que les procédures utilisées pour signaler et enquêter sur les violations de sécurité des marchandises contrôlées.

Pour aider les déclarants à élaborer leurs plans de sécurité, SPAC a publié un modèle de plan facultatif sur son site Web, qui décrit le contenu attendu. Les principaux éléments suivants sont les plus pertinents pour les données relatives aux marchandises contrôlées stockées dans AWS :

- Description des marchandises contrôlées
- Procédures de contrôle de l'examen, de la possession et du transfert de marchandises contrôlées
- Violations : enquêtes et rapports

AWS propose de nombreux services que les organisations de défense et de sécurité peuvent utiliser dans le cadre d'un plan de sécurité PMC. Pour de plus amples informations sur la manière de répondre aux exigences d'un plan de sécurité PMC avec AWS, veuillez consulter Annexe : Considérations AWS pour le programme des marchandises contrôlées.

Démarrez

Le parcours d'adoption du nuage de chaque organisation est unique. Par conséquent, pour gérer avec succès votre adoption, vous devez comprendre l'état actuel de votre organisation, l'état cible souhaité et la transition nécessaire pour atteindre l'état cible. Vous pouvez alors fixer des objectifs et créer des flux de travail qui permettront au personnel de s'épanouir dans le nuage.

Pour les organisations de défense et de sécurité au Canada, les prochaines étapes sont généralement les suivantes :

- Contactez votre représentant AWS pour savoir comment le réseau de partenaires AWS, les architectes de solutions AWS, les équipes Professional Services et les formateurs peuvent vous aider à adopter le nuage. Si vous n'avez pas de représentant AWS, veuillez nous contacter.
- Obtenez et examinez une copie des derniers rapports AWS SOC 2, de l'évaluation CCC et de la certification ISO 27001 sur le portail AWS Artifact (accessible par l'intermédiaire de la console de gestion AWS).
- Considérez la pertinence et l'application des livres blancs sur la sécurité AWS et du CIS AWS Foundations Benchmark en fonction de votre périple dans le nuage et de vos cas d'utilisation. Ces bonnes pratiques acceptées par le secteur et publiées par le Center for Internet Security vont au-delà des conseils de sécurité de haut niveau déjà disponibles, en fournissant aux utilisateurs d'AWS des recommandations claires, étape par étape, pour la mise en œuvre et l'évaluation.
- Explorez d'autres pratiques de gouvernance et de gestion des risques si nécessaire à la lumière de votre diligence raisonnable et de votre évaluation des risques, en utilisant les outils et les ressources référencés dans ce guide et dans la section « Ressources supplémentaires ».
- Contactez votre représentant AWS pour obtenir des informations supplémentaires sur l'accord d'entreprise AWS.

En plus d'aider nos clients à maximiser l'utilisation de la technologie fournie par AWS, l'équipe technique d'AWS peut soutenir nos clients de sorte que ceux-ci mettent en œuvre une architecture, des produits et des services qui leur permettent de répondre aux exigences de conformité du PMC.

Ressources supplémentaires

Cette section présente des ressources supplémentaires pour aider les organisations de défense et de sécurité à réfléchir à la sécurité, à la conformité et à la conception d'un environnement AWS sécurisé et résilient.

- AWS Secure Environment Accelerator (ASEA). La solution en code source libre ASEA est conçue pour aider les clients à répondre aux exigences du profil des mesures de la sécurité d'informatique en nuage moyen du CCC. Basée sur l'architecture de référence de sécurité AWS, la solution ASEA déploie un environnement AWS multi-compte avec des contrôles de sécurité préconfigurés. Elle permet aux organisations d'être rapidement opérationnelles sur AWS et de soutenir l'innovation et l'expérimentation dans le nuage tout en respectant des exigences de sécurité strictes.
- Guide de référence rapide en matière de sécurité et de conformité. AWS dispose de nombreuses fonctionnalités de conformité que les clients peuvent utiliser pour leurs charges de travail réglementées dans le nuage AWS. Ces fonctionnalités vous permettent d'atteindre un niveau de sécurité supérieur à l'échelle. La conformité basée sur le nuage offre un coût d'entrée plus faible, des opérations plus faciles et une meilleure agilité en fournissant davantage de supervision, de contrôle de sécurité et d'automatisation centrale.
- Cadre AWS Well-Architected. Le cadre AWS Well-Architected a été développé pour aider les architectes en solutions infonuagiques à créer l'infrastructure la plus sûre, la plus performante, la plus résiliente et la plus efficace possible pour leurs applications. Le cadre est basé sur six piliers : l'excellence opérationnelle, la sécurité, la fiabilité, l'efficacité des performances, l'optimisation des coûts et la durabilité. Ce cadre offre aux clients et aux partenaires une approche cohérente pour évaluer les architectures. Il fournit également des directives pour vous aider à mettre en œuvre des conceptions qui répondront aux besoins des applications au fil du temps.

- Cadre de cybersécurité du NIST. Le livre blanc AWS NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud (Cadre de cybersécurité du NIST : alignement sur le cadre du NIST dans le nuage AWS) montre comment les organisations commerciales et celles du secteur public peuvent évaluer l'environnement AWS par rapport au cadre de cybersécurité du NIST, mais aussi améliorer les mesures de sécurité qu'elles mettent en œuvre et exploitent (c'est-à-dire, la sécurité dans le nuage). Le livre blanc fournit également une lettre d'un auditeur tiers attestant que l'offre de nuage AWS est conforme aux pratiques de gestion des risques du cadre de cybersécurité du NIST (c'est-à-dire, la sécurité du nuage). Les organisations de défense et de sécurité peuvent utiliser le cadre de cybersécurité du NIST et les ressources AWS pour améliorer leurs pratiques de gestion des risques.

Pour obtenir de l'aide supplémentaire, veuillez consulter les livres blancs sur la sécurité, l'identité et la conformité.

Contributeurs

Les contributeurs de ce document incluent :

Michael Davie, AWS Security Assurance

Révisions de document

Date	Description
Novembre 2022	Première publication

Annexe : Considérations AWS pour le programme des marchandises contrôlées

Les sections suivantes répertorient les exigences les plus pertinentes identifiées dans le modèle de plan de sécurité du PMC de SPAC, ainsi que des considérations supplémentaires sur la façon dont les clients peuvent soutenir leurs efforts de conformité vis-à-vis des exigences applicables du PMC.

Chaque exigence est répertoriée et accompagnée de considérations conçues pour aider les clients de la défense et de la sécurité lors de l'utilisation d'AWS. Des liens vers les bonnes pratiques applicables du cadre AWS Well-Architected sont également fournis. Le cadre fournit les bonnes pratiques pour les architectes de solutions infonuagiques afin de construire une infrastructure sécurisée, hautement performante, résiliente et efficace pour une variété d'applications et de charges de travail. Basé sur six piliers (excellence opérationnelle, sécurité, fiabilité, efficacité des performances, optimisation des coûts et durabilité), le cadre fournit une approche cohérente qui permet aux clients d'évaluer les architectures sous plusieurs angles et de mettre en œuvre des conceptions évolutives dans le temps.

Les tableaux des sections suivantes sont organisés selon les colonnes suivantes :

- **Exigence.** Cette colonne répertorie les exigences identifiées dans le modèle de plan de sécurité du PMC de SPAC.
- **Considérations AWS.** Cette colonne explique les considérations AWS pour répondre aux exigences définies par SPAC. Cela peut faire référence à la sécurité et à la conformité du nuage, à la manière dont AWS met en œuvre et gère les contrôles, et/ou aux services AWS que les organisations de défense et de sécurité peuvent utiliser pour répondre à une exigence particulière.
- **Considérations sur la mise en œuvre.** Cette colonne répertorie les bonnes pratiques de sécurité dans le nuage issues du cadre AWS Well-Architected que les organisations de défense et de sécurité peuvent mettre en œuvre comme point de départ pour soutenir leurs efforts de conformité. Des détails sur chaque bonne pratique et sur les services AWS associés que les clients peuvent utiliser figurent dans les ressources du cadre AWS Well-Architected liées.

Cette section contient seulement un échantillon non exhaustif de considérations. Il ne constitue pas un conseil juridique ou de conformité ; les clients doivent consulter leurs propres équipes juridiques et de conformité.

Procédures de contrôle de l'examen, de la possession et du transfert de marchandises contrôlées

Exigence	Considérations AWS	Considérations sur la mise en □uvre (pratiques Well-Architected)
Seuls les dirigeants, les administrateurs et les employés qui ont fait l'objet d'une évaluation de sécurité et qui ont été approuvés par le responsable désigné sont autorisés à avoir accès aux marchandises contrôlées.	**Responsabilité du client** Les clients conservent la propriété et le contrôle de leur contenu lorsqu'ils utilisent les services AWS. Ils ne cèdent ni la propriété ni le contrôle de leur contenu à AWS. Les clients ont un contrôle total sur les services qu'ils utilisent et sur les personnes qu'ils autorisent à accéder à leur contenu et aux services, notamment les informations d'identification requises. Les clients contrôlent la manière dont ils configurent leurs environnements et sécurisent leur contenu, notamment en chiffrant ou non leur contenu (au repos et en transit), ainsi que les autres fonctions et outils de sécurité qu'ils utilisent et la manière dont ils les utilisent. AWS ne modifie pas les paramètres de configuration du client, car ces paramètres sont déterminés et contrôlés par le client. Les clients d'AWS ont la liberté de concevoir leur architecture de sécurité pour répondre à leurs besoins de conformité. Il s'agit d'une différence essentielle par rapport aux solutions d'hébergement traditionnelles où le fournisseur décide de l'architecture. AWS permet de classer les données organisationnelles en fonction de leur degré de sensibilité. Grâce aux balises de ressources, aux politiques AWS Identity and Access Management (IAM), à AWS Key Management Service (AWS KMS) et à AWS CloudHSM, les clients peuvent définir et mettre en œuvre des politiques de classification et de contrôle d'accès applicables aux données.	SEC 2 : gestion des identités pour les personnes et les machines SEC 3 : gestion des autorisations pour les personnes et les machines SEC 7 : classification des données

Décrire comment sont protégées les marchandises contrôlées au format électronique

Exigence	Considérations AWS	Considérations sur la mise en œuvre (pratiques Well-Architected)
Procédures en place pour la protection des marchandises contrôlées qui sont stockées sur un serveur basé sur le nuage	L'environnement AWS d'un client doit être traité comme un site distinct et doit avoir son propre plan de sécurité PMC. Consultez les autres sections de cette annexe pour des considérations pertinentes.	Pilier de sécurité
Localisation de l'ordinateur et/ou du serveur de réseau	**Responsabilité du client** L'infrastructure mondiale du nuage AWS est construite autour de régions et de zones de disponibilité. Une région est un emplacement physique dans le monde, composé de plusieurs zones de disponibilité. Les zones de disponibilité se composent d'un ou de plusieurs centres de données distincts, chacun doté d'une alimentation, d'un réseau et d'une connectivité redondants, tous situés dans des installations séparées. Ces zones de disponibilité offrent aux clients la possibilité d'exploiter des applications et des services dont la disponibilité, la tolérance aux pannes et l'évolutivité sont plus élevées que dans un environnement traditionnel sur site. Les clients d'AWS désignent la région géographique dans laquelle leur contenu sera placé. Avec AWS, les clients peuvent : • Déterminer où leur contenu sera stocké, y compris le type de stockage et la région géographique de ce stockage. • Répliquer et sauvegarder leur contenu dans plus d'une région. De plus, AWS ne déplacera ni ne répliquera le contenu du client en dehors de la ou des régions choisies par le client, sauf si la loi l'exige et si cela est nécessaire pour maintenir les services AWS et les fournir à nos clients et à leurs utilisateurs finaux. • Si certains services d'intelligence artificielle sont utilisés, refuser que leurs données soient utilisées ou stockées pour contribuer à l'amélioration de ces services.	REL 10 : isolement des pannes Politiques d'exclusion des services d'IA

Exigence	Considérations AWS	Considérations sur la mise en œuvre (pratiques Well-Architected)
Comment l'ordinateur et/ou le serveur de réseau est protégé	**Responsabilité du client** AWS donne aux clients la propriété et le contrôle de leur contenu grâce à des outils qui permettent aux clients de déterminer où leur contenu sera stocké, comment il sera sécurisé en transit ou au repos, et comment l'accès à leur environnement AWS sera géré. Les mécanismes de sécurité spécifiques appliqués à votre environnement dépendront de l'architecture de ce dernier, des services utilisés et de la manière dont les données sont stockées et accédées. Le pilier Sécurité du cadre AWS Well-Architected fournit des conseils prescriptifs sur la manière de configurer votre environnement de manière sécurisée. Il doit être utilisé comme base de référence lors de la conception de votre architecture. L'AWS Secure Environment Accelerator fournit également un point de départ déployable qui met en œuvre de nombreuses bonnes pratiques AWS. Il a été conçu pour aider les clients à répondre aux exigences du profil des mesures de la sécurité d'informatique en nuage moyen du CCC. **Responsabilité AWS** AWS a mis en œuvre les bonnes pratiques mondiales en matière de protection des données afin d'aider les clients à établir, à exploiter et à utiliser notre environnement de contrôle de la sécurité. Ces protections de sécurité et ces processus de contrôle sont validés de manière indépendante par de multiples évaluations effectuées par des tiers indépendants. Dans ses accords avec les clients, AWS prend des engagements de sécurité spécifiques qui s'appliquent largement au contenu du client dans chaque région dans laquelle celui-ci choisit de stocker ses données. Par exemple, consultez la section 3 du Contrat client AWS. Les clients d'AWS ont également la possibilité de conclure un accord d'entreprise avec AWS. Les accords d'entreprise donnent aux clients la possibilité de personnaliser les accords qui répondent le mieux à leurs besoins. Pour de plus amples informations sur les accords d'entreprise AWS, contactez votre représentant AWS.	Pilier de sécurité SEC 5 : protection des ressources du réseau SEC 6 : protection des ressources de calcul SEC 8 : protection des données au repos SEC 9 : protection des données en transit

Exigence	Considérations AWS	Considérations sur la mise en œuvre (pratiques Well-Architected)
Comment les marchandises contrôlées sont stockées sur l'ordinateur et/ou le serveur du réseau	**Responsabilité du client** Les clients d'AWS peuvent choisir parmi une variété de solutions de stockage pour répondre à leurs besoins particuliers. La solution de stockage optimale pour un système varie en fonction du type de méthode d'accès (bloc, fichier, objet ou base de données), des modèles d'accès, du débit requis, de la fréquence des accès et des mises à jour, ainsi que des contraintes de disponibilité et de durabilité. Lors de la sélection et de la configuration d'une solution de stockage, les clients doivent également tenir compte de la manière dont les données seront chiffrées au repos et dont les clés associées seront gérées, par exemple dans AWS Key Management Service (AWS KMS) ou AWS CloudHSM. AWS KMS et CloudHSM permettent d'appliquer des politiques de contrôle d'accès très précises et de journaliser l'accès et l'utilisation des clés par l'intermédiaire d'AWS CloudTrail.	PERF 3 : sélection d'une solution de stockage PERF 4 : sélection d'une solution de base de données SEC 8 : protection des données au repos
Mesures de protection des ordinateurs portables ou d'autres dispositifs portables contenant des marchandises contrôlées lors des déplacements	**Responsabilité du client** Les clients peuvent réduire le risque que les données relatives aux marchandises contrôlées soient stockées sur des appareils portables en utilisant Amazon WorkSpaces ou Amazon AppStream 2.0, qui peuvent permettre un accès sécurisé aux données relatives aux marchandises contrôlées sans que les données quittent AWS.	Bonnes pratiques pour le déploiement d'Amazon WorkSpaces Bonnes pratiques pour le déploiement d'Amazon AppStream 2.0
Procédures mises en place pour l'accès à distance aux marchandises contrôlées ; par exemple, un moyen d'accès sécurisé tel qu'un réseau privé virtuel (VPN)	**Responsabilité du client** Les clients peuvent établir des connexions VPN sécurisées à leur environnement AWS en utilisant une combinaison d'AWS Site-to-Site VPN pour se connecter à partir de leur environnement sur site, et d'AWS Client VPN pour se connecter à partir de dispositifs de point de terminaison.	REL 2 : planification de la topologie de votre réseau SEC 5 : protection des ressources du réseau SEC 9 : protection des données en transit

Exigence	Considérations AWS	Considérations sur la mise en œuvre (pratiques Well-Architected)
Emplacement des données de sauvegarde contenant des marchandises contrôlées	**Responsabilité du client** Les clients d'AWS peuvent utiliser les fonctionnalités de l'infrastructure et des services AWS pour accéder à un large éventail d'objectifs de résilience. L'utilisation de plusieurs zones de disponibilité, même dans une seule région, peut améliorer la résilience par rapport à un environnement sur site. Les zones de disponibilité sont conçues pour atténuer le risque de catastrophe naturelle et d'autres perturbations susceptibles de se produire. Les zones de disponibilité sont physiquement séparées au sein d'une zone métropolitaine et se trouvent dans des zones inondables différentes. Chaque zone de disponibilité est également conçue comme une zone de défaillance indépendante, et des processus automatisés éloignent le trafic client de la zone affectée en cas de défaillance. Les clients peuvent atteindre des objectifs extrêmement élevés en matière de temps de récupération et de points de récupération s'ils utilisent plusieurs zones de disponibilité et la réplication des données.	REL 9 : sauvegarde des données

Décrire comment l'accès aux marchandises contrôlées est surveillé

Exigence	Considérations AWS	Considérations sur la mise en □uvre (pratiques Well-Architected)
Décrire comment l'accès aux marchandises contrôlées est surveillé	**Responsabilité du client** AWS offre aux clients des outils de gouvernance et de traçabilité des données. Les clients d'AWS peuvent utiliser des outils comme AWS CloudTrail, Amazon CloudWatch et AWS Config pour suivre, surveiller, analyser et auditer les événements. AWS CloudTrail est un service qui permet la gouvernance, la conformité, l'audit opérationnel et l'audit des risques des comptes AWS. Avec AWS CloudTrail, les clients peuvent journaliser, surveiller en permanence et conserver l'activité du compte liée aux actions effectuées sur l'infrastructure AWS. AWS CloudTrail fournit un historique des événements liés à l'activité du compte AWS, notamment les actions effectuées par l'intermédiaire de la console de gestion AWS, des kits de développement SDK AWS, des outils de ligne de commande et d'autres services AWS. Cet historique des événements simplifie l'analyse de la sécurité, le suivi des modifications des ressources et le dépannage. Amazon CloudWatch est un service de surveillance et de gestion des ressources qui offre une visibilité sur les ressources et les applications en nuage pour collecter des mesures, surveiller les fichiers journaux, définir des alarmes et réagir automatiquement aux modifications. AWS Config est un service de gestion de la configuration des ressources qui enregistre et évalue les configurations de vos ressources AWS pour permettre l'audit de conformité, le suivi des modifications des ressources et l'analyse de la sécurité.	OPS 10 : gestion des applications et des événements liés aux opérations SEC 4 : détection et enquête sur les événements de sécurité

Violations : enquêtes et rapports

Exigence	Considérations AWS	Considérations sur la mise en □uvre (pratiques Well-Architected)
Une enquête doit être initiée en cas de violation de sécurité impliquant des marchandises contrôlées	**Responsabilité du client** Les plans d'intervention des clients en matière de sécurité des informations doivent inclure les mécanismes permettant de gérer toutes les étapes pertinentes d'un incident, notamment l'escalade et la création de rapports. Les clients doivent régulièrement examiner et tester leurs plans d'intervention en matière de sécurité des informations afin de s'assurer qu'ils restent efficaces et adaptés à leur objectif. Les clients d'AWS peuvent utiliser des outils comme AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub et Amazon Detective pour suivre, surveiller, analyser et auditer les événements. **Responsabilité AWS** AWS a mis en œuvre une politique et un programme de réponse aux incidents formels et documentés. La politique porte sur l'objectif, la portée, les rôles, les responsabilités et l'engagement de la direction. Le plan de test de la réponse aux incidents est réalisé chaque année, en même temps que le plan de réponse aux incidents. Le plan de test comprend plusieurs scénarios, des vecteurs d'attaque potentiels, l'inclusion de l'intégrateur de systèmes dans la création de rapports et la coordination (le cas échéant), ainsi que différentes méthodes de création de rapports et de détection (création de rapports et détection par le client, création de rapports et détection par AWS).	OPS 10 : gestion des applications et des événements liés aux opérations SEC 4 : détection et enquête sur les événements de sécurité SEC 10 : anticipation, réponse et récupération après incident