AWS User Guide to Canada's Controlled Goods Program (CGP)

October 17, 2022

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Introduction ... 1

Security and shared responsibility ... 3

Security in the cloud ... 4

Security of the cloud ... 5

AWS Compliance Program ... 5

Certifications and third-party attestations ... 6

AWS Artifact ... 7

Controlled Goods Program ... 7

Cloud service provider registration ... 8

Registrant security plan ... 8

Getting started ... 9

Additional resources ... 10

Contributors ... 11

Document revisions ... 11

Appendix: AWS considerations for the Controlled Goods Program ... 12

Procedures to control the examination, possession, and transfer of controlled goods13

Describe how controlled goods in electronic format are protected ... 14

Describe how access to controlled goods is monitored ... 18

Breaches: Investigating and reporting ... 19

Abstract

This document provides information to assist Canadian defence and security organizations that are regulated by Public Services and Procurement Canada (PSPC) under the Controlled Goods Program (CGP) as they adopt and accelerate their use of the Amazon Web Services (AWS) Cloud.

This guide describes the respective roles that the customer and AWS each play in managing and securing the cloud environment, provides an overview of the regulatory requirements and guidance from PSPC, and provides additional resources that defence and security organizations can use to design and architect their AWS environment to be secure and meet CGP regulatory expectations.

Introduction

Amazon Web Services (AWS) is the world’s most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster. AWS is architected to be the most flexible and secure cloud computing environment available today. Our core infrastructure is built to satisfy the security requirements for the military, global banks, and other high-sensitivity organizations. This is backed by a deep set of cloud security tools, with 230 security, compliance, and governance services and features.

The Controlled Goods Program (CGP) is a mandatory registration and compliance regime established by the Government of Canada and managed by Public Services and Procurement Canada (PSPC). The program is legislated under the Defence Production Act and Controlled Goods Regulations, and regulates the examination, possession, or transfer of domestic controlled goods. Controlled goods consist of goods, components, and technical data that have military or national security significance, including United States International Traffic in Arms Regulations (ITAR) controlled articles.

This guide is a resource to assist defence and security organizations to understand the CGP’s security requirements when they use AWS. It includes a description of the AWS compliance framework and advanced tools and security measures, which defence and security organizations can use to help evaluate, meet, and demonstrate compliance with their applicable regulatory requirements under the CGP.

A full analysis of the Controlled Goods Regulations is beyond the scope of this guide. However, the sections outlined in the following list address the considerations that most frequently arise in interactions with defence and security organizations in Canada and provide information that these organizations can use to better understand both AWS responsibilities and their own responsibilities with regards to the CGP:

- **Security and shared responsibility.** It is important that defence and security organizations understand the AWS Shared Responsibility Model before exploring the specific requirements of the CGP. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS for security, and informs the steps defence and security organizations need to take to ensure they demonstrate compliance with the Controlled Goods Regulations.

- **AWS Global Cloud Infrastructure.** The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. The AWS Global Cloud Infrastructure offers AWS customers an easier and more effective way to design and operate applications and services, making these resources more highly available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use the AWS Global Cloud Infrastructure to design an AWS environment that is consistent with their business and regulatory needs, including requirements under the CGP.

- **AWS compliance programs.** AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Defence and security organizations can use the AWS compliance programs to help satisfy their regulatory requirements.

- **Controlled Goods Program.** This section sets out common considerations for defence and security organizations as they consider some of the key requirements under the CGP, and it describes how these organizations can use AWS services and tools to demonstrate compliance with their applicable regulatory requirements. The appendix in this guide, Appendix: AWS considerations for the Controlled Goods Program, provides a non-exhaustive list of requirements and corresponding considerations when using AWS.

This document contains only a non-exhaustive sample of considerations. This is not legal or compliance advice, and customers should consult with their own legal and compliance teams.

Security and shared responsibility

The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles, and it is important that defence and security organizations understand the model before they explore the specific requirements under the CGP.

Cloud security is a shared responsibility. Security *in* the cloud is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, applications, systems, and networks, as they would for applications in an on-premises data center.

AWS manages security *of* the cloud by ensuring that AWS Cloud Infrastructure complies with global and regional regulatory requirements and best practices. AWS operates, manages, and controls the IT components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

The Shared Responsibility Model is depicted graphically in Figure 1.

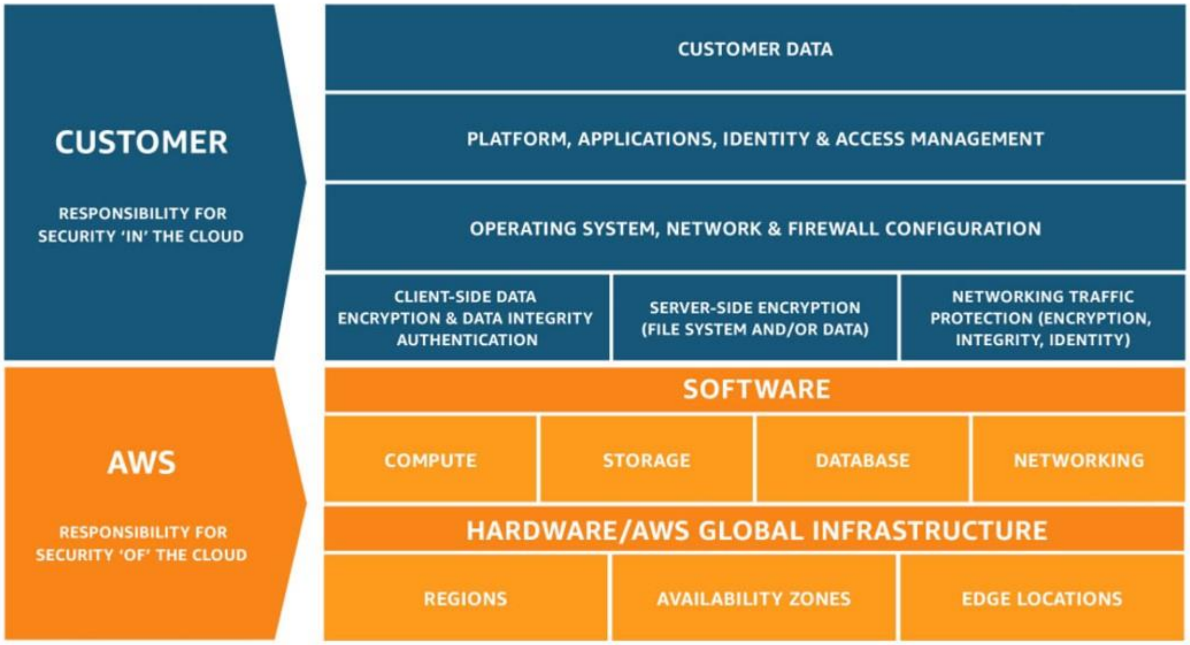
CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Figure 1: AWS Shared Responsibility Model

Security in the cloud

Customers are responsible for their security in the cloud. AWS customers are responsible for managing guest operating systems (including installing updates and security patches) and other associated application software, as well as any applicable network security controls. Customers should carefully consider the services they choose, because their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS
- The AWS services that are used with the content
- The country where their content is stored
- The format and structure of their content and whether it is masked, anonymized, or encrypted
- How their data is encrypted, and where the keys are stored
- Who has access to their content and how those access rights are granted, managed, and revoked

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility will be determined by the AWS cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) requires the customer to perform all of the necessary security configuration and management tasks for a general-purpose computer. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instance, and the configuration of the AWS provided firewall (called a security group) on each instance. For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access service endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using identity and access management tools to enforce the appropriate permissions.

Security of the cloud

AWS infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of the AWS security controls, including internationally recognized security best practices and certifications.

The AWS Compliance Program is based on the following actions:

- **Validation** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that customers can implement, and to better assist customers with managing their control environment.
- **Demonstrating** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with information regarding the policies, processes, and controls established and operated by AWS. Customers can use this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.
- **Monitoring**, through applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS Compliance Program

The AWS Compliance Program helps customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS compliance enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.

Certifications and third-party attestations

AWS has obtained certifications and independent third-party attestations for a variety of global and industry-specific workloads. The following are of particular relevance to Canadian defence and security organizations regulated under the CGP:

- **Canadian Centre for Cyber Security (CCCS).** As part of their Cloud Service Provider IT Security Assessment Process (ITSM.50.100), CCCS assesses cloud services to ensure that they meet Government of Canada security requirements. This assessment is a mandatory requirement for AWS to provide cloud services to Canadian federal government departments and agencies. To date,120 AWS services have been assessed by using the CCCS Medium Cloud Security Profile, which is appropriate for information and systems categorized up to PROTECTED B/Medium Integrity/Medium Availability. For more information, see the CCCS Assessment webpage.
- **SOC.** System and Organization Controls (SOC) reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls that have been established to support operations and compliance. For more information, see the SOC Compliance webpage.

  There are two particularly relevant types of AWS SOC reports:

  - **SOC 2.** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
  - **SOC 3.** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality, without disclosing AWS internal information.
- **ISO 27001** is a security management standard that specifies security management best practices and comprehensive security controls that follow the best practice guidance of ISO 27002. The basis of this certification is the development and implementation of a rigorous security program, including an Information Security Management System that defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.

- **ISO 27017** provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27001 and ISO 27002 standards. This code of practice provides additional security control implementation guidance that is specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.
- **ISO 22301** specifies requirements for an organization to implement, maintain, and improve a business continuity management system. Adherence to this standard ensures that AWS has effective systems in place to prevent, prepare for, respond to, and recover from unexpected and disruptive events, and helps customers achieve and maintain the highest-grade resiliency and security standards. For more information, or to download the AWS ISO 22301 certification, see the ISO 22301 Compliance webpage.

By tying together governance-focused, audit-friendly service features with such certifications, attestations, and audit standards, AWS Compliance enablers build on traditional programs and help customers to establish and operate in an AWS environment.

For more information about other AWS certifications and attestations, see the AWS Compliance Program webpage. For information about general AWS security controls and service-specific security, see the Best Practices for Security, Identity, & Compliance webpage.

AWS Artifact

Customers can download reports and details about more than 2,600 security controls by using AWS Artifact, an automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, CCCS assessments, and certifications from accreditation bodies across geographies and compliance verticals.

Controlled Goods Program

The Controlled Goods Program (CGP) is a mandatory registration and compliance regime established by the Government of Canada and managed by Public Services and Procurement Canada (PSPC). The program is legislated under the Defence Production Act and Controlled Goods Regulations, and regulates the examination, possession, or transfer of domestic controlled goods. Controlled goods consist of goods, components, and technical data that have military or national security significance, including United States International Traffic in Arms Regulations (ITAR) controlled articles.

Organizations must register in the CGP to examine, possess, or transfer controlled goods in Canada, and must meet the conditions of registration specified in the Controlled Goods Regulations. Each registrant is required to establish and implement a security plan that sets out, among other things, the procedures used to control the examination, possession, and transfer of controlled goods, and the procedures used to report and investigate security breaches.

Cloud service provider registration

On April 9, 2021, PSPC issued guidance regarding the use of cloud services. The guidance requires suppliers of cloud services to be registered in the CGP, and stipulates that registrants must verify that a cloud supplier holds a valid CGP registration before storing their CGP data in the cloud.

Amazon Web Services Canada, Inc. is a registrant under the CGP, and our registration is listed in the CGP registration directory.

Registrant security plan

The Controlled Goods Regulations specify the conditions that an organization must meet in order to be a registrant under the CGP. For the purposes of this guide, the most relevant clause is section 10(e), which requires that a registrant establish and implement a security plan that sets out, among other things, the procedures used to control the examination, possession, and transfer of controlled goods, and the procedures used to report and investigate security breaches in relation to controlled goods.

To assist registrants in developing their security plans, PSPC has published an optional plan template on their website, which outlines the expected content. The following major headings are the most relevant to controlled goods data that is stored in AWS:

- Description of the controlled goods
- Procedures to control the examination, possession, and transfer of controlled goods
- Breaches: Investigating and reporting

AWS has many services that defence and security organizations can use as part of a CGP security plan. For further information on addressing the requirements of a CGP security plan with AWS, see Appendix: AWS considerations for the Controlled Goods Program.

Getting started

Each organization’s cloud adoption journey is unique and, therefore, to successfully manage your adoption, you need to understand your organization’s current state, the desired target state, and the transition required to achieve the target state. Knowing this will help you set goals and create work streams that will enable staff to thrive in the cloud.

For defence and security organizations in Canada, next steps typically include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solutions Architects, Professional Services teams, and training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us.
- Obtain and review a copy of the latest AWS SOC 2 reports, CCCS assessment, and ISO 27001 certification from the AWS Artifact portal (accessible through the AWS Management Console).
- Consider the relevance and application of the AWS security whitepapers, and the CIS AWS Foundations Benchmark, as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Explore other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources referenced throughout this guide and in the Additional resources section.
- Speak with your AWS representative to obtain additional information regarding the AWS Enterprise Agreement.

In addition to helping our customers maximize the use of the technology provided by AWS, the AWS technical team can support our customers so they can implement architecture, products, and services that allow them to meet compliance requirements under the CGP.

Additional resources

Set out in this section are additional resources to help defence and security organizations think about security, compliance, and designing a secure and resilient AWS environment.

- AWS Secure Environment Accelerator (ASEA). The ASEA is an open-source solution designed to assist customers in meeting the requirements of the CCCS Medium Cloud Security Profile. Based on the AWS Security Reference Architecture, the ASEA deploys a multi-account AWS environment with pre-configured security controls. It allows organizations to get up and running in AWS quickly, and to support innovation and experimentation in the cloud while meeting strict security requirements.
- AWS Security & Compliance Quick Reference Guide. AWS has many compliance-enabling features that customers can use for their regulated workloads in the AWS Cloud. These features help you to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, easier operations, and improved agility by providing more oversight, security control, and central automation.
- AWS Well-Architected Framework. The AWS Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. The framework consists of six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help you implement designs that will scale application needs over time.

- NIST Cybersecurity Framework (CSF). The AWS whitepaper NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud demonstrates how commercial and public sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (that is, security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS Cloud offering’s conformance to NIST CSF risk management practices (that is, security of the cloud). Defence and security organizations can use NIST CSF and AWS resources to elevate their risk management practices.

For additional help, see the Security, Identity, and Compliance whitepapers.

Contributors

Contributors to this document include:

Michael Davie, AWS Security Assurance

Document revisions

Date	Description
October 2022	First publication

Appendix: AWS considerations for the Controlled Goods Program

The following sections list the most relevant requirements identified in PSPC’s CGP security plan template, along with additional considerations on how customers can support their compliance efforts toward their applicable requirements under the CGP.

Each requirement is listed along with considerations to assist defence and security customers when using AWS, as well as links to the applicable best practices from the AWS Well-Architected Framework. The Framework provides best practices for cloud architects to build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. Based on six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—the Framework provides a consistent approach for customers to evaluate architectures from multiple perspectives, and to implement designs that will scale over time.

The tables in the next sections are organized into the following columns:

- **Requirement.** This column lists requirements identified in PSPC’s CGP security plan template.
- **AWS considerations.** This column explains the AWS considerations for addressing the requirements defined by PSPC. It may refer to the security and compliance of the cloud, how AWS implements and manages the controls, and/or AWS services that defence and security organizations can use to address a particular requirement.
- **Implementation considerations.** This column lists best practices for security in the cloud from the AWS Well-Architected Framework, which defence and security organizations can implement as a starting point to support their compliance efforts. Details on each best practice and associated AWS services that customers can use can be found in the linked AWS Well-Architected Framework resources.

This section contains only a non-exhaustive sample of considerations. This is not legal or compliance advice, and customers should consult with their own legal and compliance teams.

Procedures to control the examination, possession, and transfer of controlled goods

Requirement	AWS considerations	Implementation considerations (Well-Architected practices)
Only officers, directors, and employees who have been security assessed and approved by the designated official are authorized to have access to controlled goods	**Customer responsibility** Customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Customers have complete control over which services they use and whom they empower to access their content and services, including what credentials will be required. Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS does not change customer configuration settings, because these settings are determined and controlled by the customer. AWS customers have freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS provides ways to categorize organizational data based on levels of sensitivity. By using resource tags, AWS Identity and Access Management (IAM) policies, AWS Key Management Service (AWS KMS), and AWS CloudHSM, customers can define and implement policies for data classification and access control.	SEC 2: Manage identities for people and machines SEC 3: Manage permissions for people and machines SEC 7: Classify data

Describe how controlled goods in electronic format are protected

Requirement	AWS considerations	Implementation considerations (Well-Architected practices)
Procedures in place for the protection of controlled goods that are stored on a cloud-based server	A customer's AWS environment should be treated as a separate site and should have its own CGP security plan. See the other sections of this appendix for relevant considerations.	Security pillar
Location of the computer and/or network server	**Customer responsibility** The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location in the world, consisting of multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. These Availability Zones offer customers the ability to operate applications and services which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment. AWS customers designate in which geographic Region their content will be located. With AWS, customers can: • Determine where their content will be stored, including the type of storage and geographic Region of that storage. • Replicate and back up their content in more than one Region, and AWS will not move or replicate customer content outside of the customer's chosen Region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users. • If certain artificial intelligence services are used, opt out of having their data used or stored to support the improvement of those services.	REL 10: Fault isolation AI services opt-out policies

Requirement	AWS considerations	Implementation considerations (Well-Architected practices)
How the computer and/or network server is protected	**Customer responsibility** AWS gives customers ownership and control over their content through tools that allow customers to determine where their content will be stored, how it will be secured in transit or at rest, and how access to their AWS environment will be managed. The specific security mechanisms applied to your environment will depend on the environment that is architected, the services used, and how the data is stored and accessed. The Security pillar of the AWS Well-Architected Framework provides prescriptive guidance on how to configure your environment securely, and should be used as a baseline when designing your architecture. The AWS Secure Environment Accelerator also provides a deployable starting point that implements many AWS best practices, and was designed to help customers address the requirements of the CCCS Medium cloud security profile. **AWS responsibility** AWS has implemented global data protection best practices in order to help customers establish, operate, and use our security control environment. These security protections and control processes are independently validated by multiple independent third-party assessments. In its agreements with customers, AWS makes specific security commitments that apply broadly to customer content in each Region in which the customer chooses to store their data. For example, see Section 3 of the AWS Customer Agreement. AWS customers also have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs. For more information about AWS Enterprise Agreements, contact your AWS representative.	Security pillar SEC 5: Protect network resources SEC 6: Protect compute resources SEC 8: Protect data at rest SEC 9: Protect data in transit

Requirement	AWS considerations	Implementation considerations (Well-Architected practices)
How the controlled goods are stored on the computer and/or network server	**Customer responsibility** AWS customers can choose from a variety of storage solutions to meet their particular requirements. The optimal storage solution for a system varies based on the kind of access method (block, file, object, or database), patterns of access, required throughput, frequency of access and update, and availability and durability constraints. When selecting and configuring a storage solution, customers should also consider how the data will be encrypted at rest and how the associated keys will be managed, such as in AWS Key Management Service (AWS KMS) or AWS CloudHSM. Both AWS KMS and CloudHSM allow for the application of fine-grained access control policies, and log key access and use through AWS CloudTrail.	PERF 3: Select a storage solution PERF 4: Select a database solution SEC 8: Protect data at rest
Measures to safeguard laptop computers or other portable devices that contain controlled goods when travelling	**Customer responsibility** Customers can reduce the risk of controlled goods data being stored on portable devices by using Amazon WorkSpaces or Amazon AppStream 2.0, which can allow secure access to controlled goods data without the data leaving AWS.	Best Practices for Deploying Amazon WorkSpaces Best Practices for Deploying Amazon AppStream 2.0
Procedures that are in place for remote access to controlled goods; for example, a secure means of access such as a virtual private network (VPN)	**Customer responsibility** Customers can establish secure VPN connections to their AWS environment by using a combination of AWS Site-to-Site VPN to connect from their on-premises environment, and AWS Client VPN to connect from endpoint devices.	REL 2: Plan your network topology SEC 5: Protect network resources SEC 9: Protect data in transit

Requirement	AWS considerations	Implementation considerations (Well-Architected practices)
The location of back-up data containing controlled goods	**Customer responsibility** AWS customers can use the features of the AWS infrastructure and AWS services to meet a wide range of resiliency goals. Using multiple Availability Zones, even within a single Region, can enhance resiliency as compared to an on-premises environment. Availability Zones are designed to mitigate against the risk of natural disaster and other disruptions that may occur. Availability Zones are physically separated within a metropolitan area and are in different flood plains. Each Availability Zone is also designed as an independent failure zone, and automated processes move customer traffic away from the affected area in the case of failure. Customers can achieve extremely high recovery-time and recovery-point objectives by using multiple Availability Zones and data replication.	REL 9: Back up data

Describe how access to controlled goods is monitored

Requirement	AWS considerations	Implementation considerations (Well-Architected practices)
Describe how access to controlled goods is monitored	**Customer responsibility** AWS offers customers tools for governance and data traceability. AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, and AWS Config to track, monitor, analyze, and audit events. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts. With AWS CloudTrail, customers can log, continuously monitor, and retain account activity related to actions across AWS infrastructure. AWS CloudTrail provides an event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. Amazon CloudWatch is a resource monitoring and management service that gives visibility into cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes. AWS Config is a resource configuration management service that records and evaluates configurations of your AWS resources to enable compliance auditing, resource change tracking, and security analysis.	OPS 10: Manage workload and operations events SEC 4: Detect and investigate security events

Breaches: Investigating and reporting

Requirement	AWS considerations	Implementation considerations (Well-Architected practices)
Investigative steps must be initiated with regards to a security breach involving controlled goods	**Customer responsibility** Customers' information security response plans must include the mechanisms for managing all relevant stages of an incident, including escalation and reporting. Customers should regularly review and test their information security response plans to ensure that they remain effective and fit-for-purpose. AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub, and Amazon Detective to track, monitor, analyze, and audit events. **AWS responsibility** AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. The Incident Response Test Plan is performed annually, in conjunction with the Incident Response plan. The test plan includes multiple scenarios, potential vectors of attack, the inclusion of the systems integrator in reporting and coordination (when applicable), and varying reporting and detection avenues (customer reporting and detecting, AWS reporting and detecting).	OPS 10: Manage workload and operations events SEC 4: Detect and investigate security events SEC 10: Anticipate, respond to, and recover from incidents