

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

June 2024



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.

© 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

Overview	1
Security and Shared Responsibility.....	2
Security in the Cloud	3
Security of the Cloud.....	4
AWS Compliance Programs.....	5
Certifications and Third-Party Attestations	5
AWS Artifact.....	7
Controlled Goods Program.....	7
Overview	7
Cloud Service Provider Registration	8
Registrant Security Plan.....	8
Getting Started	9
Additional Resources	10
Document revisions.....	11
Appendix: AWS Considerations for the Controlled Goods Program.....	12
Procedures to control the examination, possession and transfer of controlled goods.	13
Describe how controlled goods in electronic format are protected	14
Describe how access to controlled goods is monitored	18
Breaches: Investigating and reporting.....	19

About this Guide

This document provides information to assist Canadian defence and security organizations that are regulated by the *Controlled Goods Regulations*, administered 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 that defence and security organizations can consider when using AWS; 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.

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.

Overview

AWS provides organizations the secure, resilient global cloud infrastructure and services they need to differentiate themselves today and adapt to the needs of tomorrow. Through continuous innovation, AWS delivers stringent security requirements, the greatest breadth and depth of services, deep industry expertise, and an expansive partner network. Building on AWS empowers organizations to modernize their infrastructure, meet rapidly changing customer requirements and expectations, and drive business growth. AWS offers IT services in categories ranging from compute, storage, database, and networking to artificial intelligence and machine learning. Across the world, organizations of all types have used AWS services to build their own applications for engineering, system development, and operational support.

The [Controlled Goods Program](#) (CGP) is a mandatory registration and compliance regime for organization who examine, possess and/or transfer controlled goods 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 defence articles originating from the United States that are controlled by the [United States Munitions List—part 121 of the United States International Traffic in Arms Regulations](#).

This guide is a resource to assist defence and security organizations 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 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 below 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 their and AWS' 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, as well as a high-speed global network. The AWS Global Cloud Infrastructure offers AWS customers an easier and more effective way to design and operate applications and services, making them 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 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 compliance resources available to customers. Defence and security organizations can leverage AWS's 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 requirements under the CGP, and it describes how they can leverage AWS services and tools to demonstrate compliance with their applicable regulatory requirements. The appendix, AWS Considerations for Controlled Goods Program Requirements, provides a non-exhaustive list of requirements and corresponding considerations when using AWS.

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 exploring 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 at Figure 1.

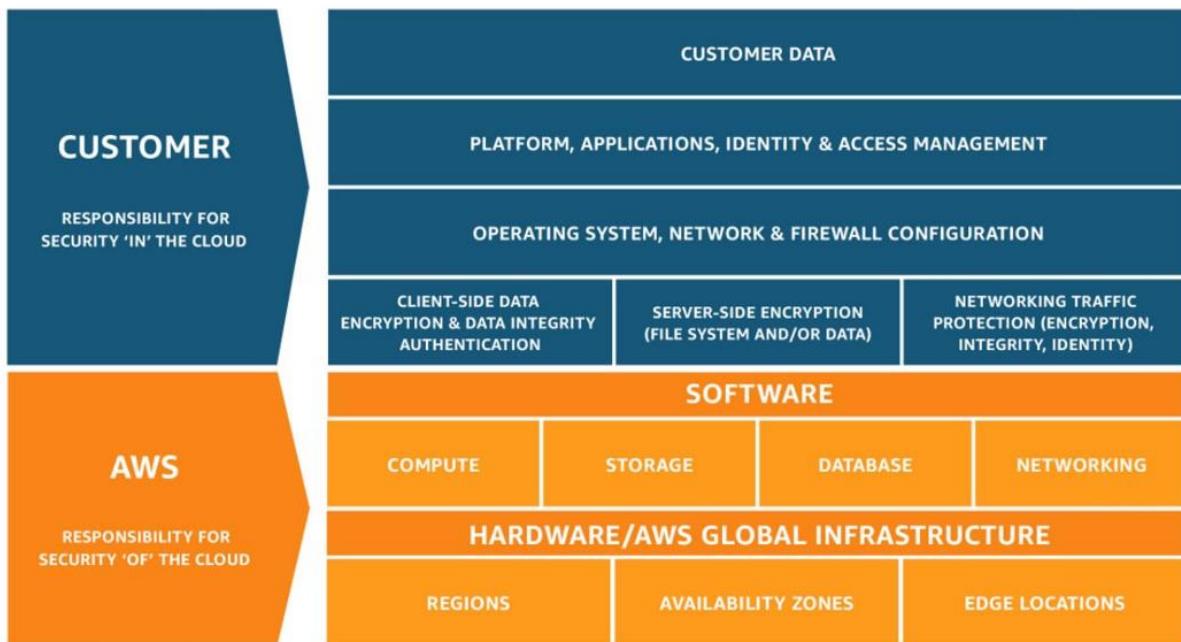


Figure 1: AWS Shared Responsibility Model

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, as 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; and
- 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 of 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 instances, 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 (IAM) tools to enforce the appropriate permissions.

Security of the Cloud

AWS's infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use AWS's compliance certifications to validate the implementation and effectiveness of AWS's 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 Programs

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 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, 150 AWS services have been assessed as meeting 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 AWS's [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 established to support operations and compliance. For more information, see AWS's [SOC Compliance](#) webpage.

There are two particularly relevant types of AWS SOC Reports:

- **SOC 2:** Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, confidentiality, and privacy.
- **SOC 3:** Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, confidentiality, and privacy without disclosing AWS internal information.

ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following 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 AWS's [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 information security control implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see AWS's [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 AWS's [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

Overview

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 defense articles originating from the United States that are controlled by the [United States Munitions List—part 121 of the United States International Traffic in Arms Regulations](#).

Organizations must register with 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 May 7th 2024, PSPC issued [guidance](#) regarding the use of cloud services. The guidance suggests that cloud service providers should be registered with the CGP. Alternatively, unregistered cloud service providers may be at risk of contravening the Act due to the nature of their services, business practices and technical operations, such as technical support or maintenance of data subject to the CGP.

Amazon Web Services Canada, Inc. is a registrant with 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 stored in AWS:

- Record keeping of the controlled goods.
 - This record must identify a description of any controlled goods received, the date of their receipt and an identification of the company from which they were transferred.
 - Any controlled goods transferred, the date of the transfer and the identity and address of the company to whom they were transferred.
 - The manner and date of disposition 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 execute 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 Solution 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 via 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.
- Dive deeper on 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 below are additional resources to help defence and security organizations think about security, compliance, and designing a secure and resilient AWS environment.

- [AWS Control Tower](#) with the [Landing Zone Accelerator on AWS \(LZA\)](#), when used with the [Canadian Centre for Cyber Security \(CCCS\) Cloud Medium configuration](#), is an industry-specific deployment designed in collaboration with Canadian national security, defence, law enforcement, and federal, provincial, and municipal government customers. It accelerates compliance with their strict and unique security and compliance requirements. The [CCCS Cloud Medium Reference Architecture](#) deploys a multi-account AWS environment with pre-configured security controls, allowing organizations to quickly get up and running on AWS, supporting innovation and experimentation in the cloud while meeting stringent security requirements.
- [AWS Compliance Quick Reference Guide](#): AWS has many compliance-enabling features that customers can use for their regulated workloads in the AWS cloud. These features allow 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 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 (i.e., 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 (i.e., security of the cloud). Defence and security organizations can leverage NIST CSF and AWS resources to elevate their risk management practices.

For additional help, visit the [Security, Identity and Compliance Whitepapers](#).

Document revisions

Date	Description
August 2022	First publication
June 2024	Updated to reflect new CGP Cloud Guidance

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](#), which 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 may leverage 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	<p>Customer Responsibility</p> <p>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.</p> <p>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.</p> <p>AWS does not change customer configuration settings, as 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.</p> <p>AWS provides ways to categorize organizational data based on levels of sensitivity. By using resource tags, AWS IAM policies, and AWS KMS, customers can define and implement policies for data classification and access control.</p>	<p>SEC 2: Manage identities for people and machines</p> <p>SEC 3: Manage permissions for people and machines</p> <p>SEC 7: Classify data</p>

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	<p>A customer's AWS environment should be treated as a separate site and should have its own CGP security plan.</p> <p>See the other sections of this appendix for relevant considerations.</p>	Security Pillar
Location of the computer and/or network server	<p>Customer Responsibility</p> <p>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.</p> <p>AWS customers designate in which geographic region their content will be located. With AWS, customers can:</p> <ul style="list-style-type: none"> • 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 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/network server is protected	<p>Customer Responsibility</p> <p>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.</p> <p>The specific security mechanisms applied to your environment will depend on the environment 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 environment securely, and should be used as a baseline when designing your architecture. The AWS Control Tower with the Landing Zone Accelerator on AWS (LZA) 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.</p> <p>AWS Responsibility</p> <p>AWS has implemented global data protection best practices in order to help customers establish, operate, and leverage our security control environment. These security protections and control processes are independently validated by multiple independent third-party assessments.</p> <p>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.</p> <p>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.</p>	<p><u>Security Pillar</u></p> <p>SEC 5: Protect network resources</p> <p>SEC 6: Protect compute resources</p> <p>SEC 8: Protect data at rest</p> <p>SEC 9: Protect data in transit</p>

Requirement	AWS Considerations	Implementation Considerations (Well Architected Practices)
How the controlled goods are stored on the computer and/or network server	<p>Customer Responsibility</p> <p>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.</p> <p>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 Managed Service (KMS) or AWS CloudHSM. Both KMS and CloudHSM allow for the application of fine-grained access control policies, and log key access and use via AWS CloudTrail.</p>	<p>PERF 3: Select a storage solution</p> <p>PERF 4: Select a database solution</p> <p>SEC 8: Protect data at rest</p>
Measures to safeguard laptop computers or other portable devices that contain controlled goods when travelling	<p>Customer Responsibility</p> <p>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.</p>	<p>Best Practices for Deploying Amazon WorkSpaces</p> <p>Best Practices for Deploying Amazon AppStream 2.0</p>
Procedures that are in place for remote access to controlled goods, for example, a secure means of access such as virtual private network (VPN)	<p>Customer Responsibility</p> <p>Customers can establish secure VPN connections to their AWS environment 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.</p>	<p>REL 2: Plan your network topology</p> <p>SEC 5: Protect network resources</p> <p>SEC 9: Protect data in transit</p>

Requirement	AWS Considerations	Implementation Considerations (Well Architected Practices)
The location of back-up data containing controlled goods	<p>Customer Responsibility</p> <p>AWS customers can leverage the features of the AWS infrastructure and AWS services to meet a wide range of resiliency goals.</p> <p>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 region 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.</p>	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	<p>Customer Responsibility</p> <p>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.</p> <p>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.</p> <p>Amazon CloudWatch is a resource monitoring & management that gives a complete visibility of cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes.</p> <p>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.</p>	<p>OPS 10: Manage workload and operations events</p> <p>SEC 4: Detect and investigate security events</p>

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	<p>Customer Responsibility</p> <p>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 they remain effective and fit-for-purpose.</p> <p>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.</p> <p>AWS Responsibility</p> <p>AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment.</p> <p>The Incident Response Test Plan is executed 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/detection avenues (i.e., customer reporting/detecting, AWS reporting/detecting).</p>	<p>OPS 10: Manage workload and operations events</p> <p>SEC 4: Detect and investigate security events</p> <p>SEC 10: Anticipate, respond to, and recover from incidents</p>