# The Cyber Security Agency (CSA) Cyber Trust mark certification

Cloud Companion Guide

**October 2023**

*Last updated October 13, 2023*

# 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

# Abstract

This document is provided as a companion guide to the Cyber Security Agency of Singapore's (CSA) Cyber Trust mark certification and provides guidance and a mapping of AWS services and features to applicable domains of the Cyber Trust mark certification program.

# Introduction

The Cyber Trust mark serves as a mark of distinction for organizations to prove that they have put in place good cybersecurity practices and measures that are commensurate with their cybersecurity risk profile. The Cyber Trust mark aims to guide organizations to understand their risk profiles and identify relevant cybersecurity preparedness areas required to mitigate these risks.

The AWS Cloud Companion Guide provides guidance and a mapping of AWS services and features as they align to applicable domains and controls as listed in the Cyber Trust. It aims to provide customers with an understanding of which AWS services and tools can be used to help fulfil the requirements set out in the Cyber Trust mark certification.

The guide does not cover compliance topics such as physical and maintenance controls, or organization-specific requirements such as policies and human resources controls. This makes the guide lightweight and focused only on the particular security considerations for AWS services. For a full list of AWS Compliance Programs, see https://aws.amazon.com/compliance/programs/.

## How to use this guide

While the AWS Cloud Companion Guide for CSA Cyber Trust mark certification is an independent mapping of AWS services against domain requirements, it complements the following documents.

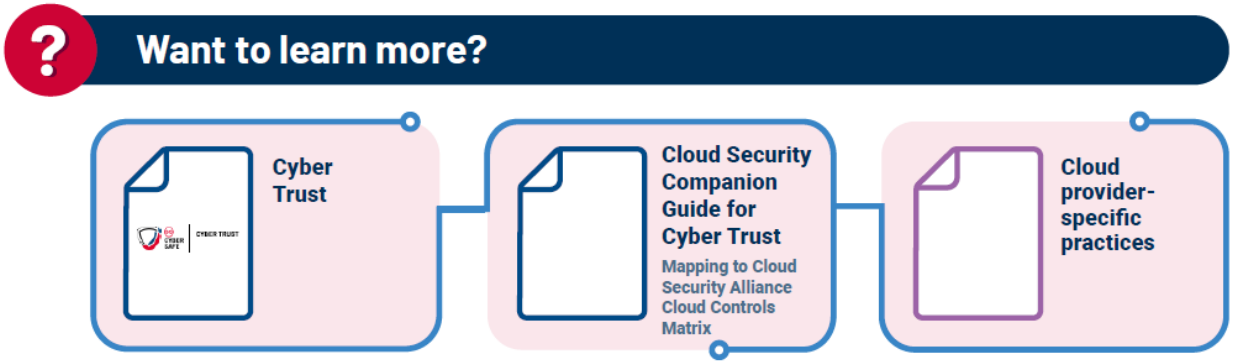


*Fig 1 – CSA Cyber Trust complementary documents*

- **Cyber Trust document** – These outline the cybersecurity certification standards for Cyber Trust and are published as national standards.
- **Cloud Security Companion Guide for Cyber Trust** – Mapping of Cyber Trust to the Cloud Security Alliance Cloud Compliance Matrix (CCM).
- **Cloud provider specific practices** – AWS Cloud Companion Guide for the CSA Cyber Trust mark certification.

## Are you Well-Architected?

The AWS Well-Architected Framework helps you understand the pros and cons of the decisions you make when building systems in the cloud. The six pillars of the Framework allow you to learn architectural best practices for designing and operating reliable, secure, efficient, cost-effective, and sustainable systems. Using the AWS Well-Architected Tool, available at no additional charge in the AWS Management Console, you can review your workloads against these best practices by answering a set of questions for each pillar. For more expert guidance and best practices for your cloud architecture—reference architecture deployments, diagrams, and whitepapers—refer to the AWS Architecture Center.

## AWS Shared Responsibility Model

Security and compliance are shared responsibilities between AWS and the customer. Depending on the services deployed, this shared model can help relieve the customer's operational burden. This is because AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches) and other associated application software, in addition to the configuration of the AWS-provided security group firewall. We recommend that customers carefully consider the services they choose because their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance their security and/or align with their more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection and prevention, encryption, and key management. The nature of this shared responsibility also provides the flexibility and customer control that permits customers to deploy solutions that meet industry-specific certification requirements.

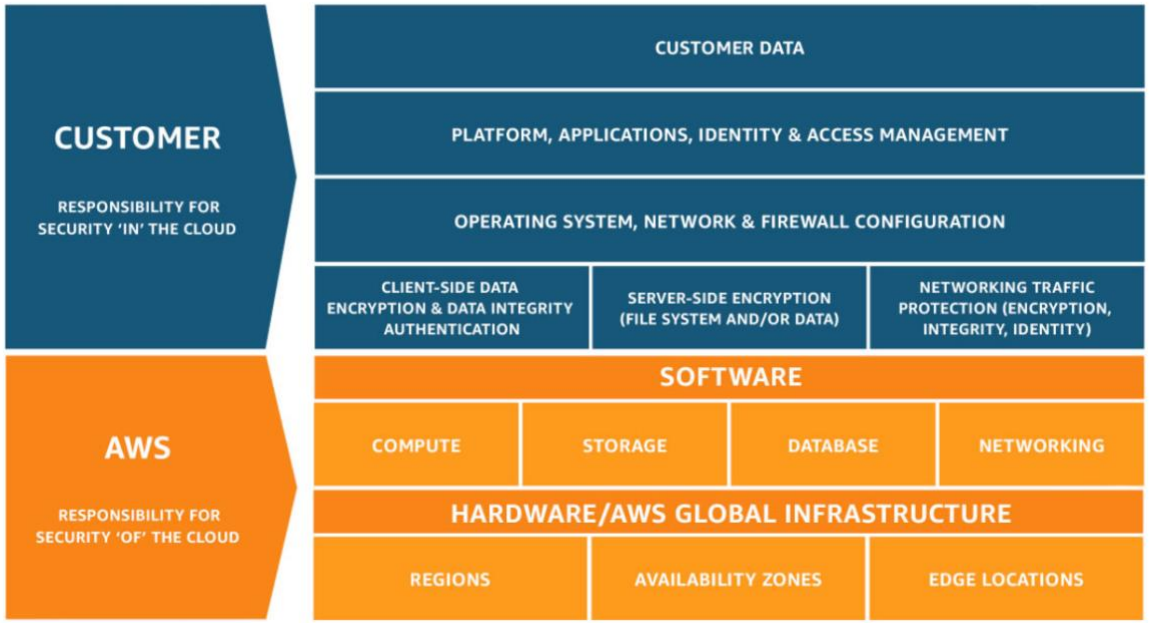


*Fig 2 – The AWS Shared Responsibility Model*

This shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, the management, operation, and verification of IT controls is also a shared responsibility. AWS can help customers by managing those controls associated with the physical infrastructure deployed in the AWS environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required. For more information about how responsibility for certain controls is shared between AWS and its customers, see the AWS Shared Responsibility Model.

# Mapping AWS services and features to Cyber Trust domains

The CSA Cyber Trust mark certification program comprises the following domains.

| | Tier 1: Supporter | Tier 2: Practitioner | Tier 3: Promoter | Tier 4: Performer | Tier 5: Advocate |
|---|---|---|---|---|---|
| **Cyber Governance and Oversight** | | | | | |
| 1. Governance | | | • | • | • |
| 2. Policies and procedures | | | • | • | • |
| 3. Risk management | • | • | • | • | • |
| 4. Cyber strategy | | | | | • |
| 5. Compliance | • | • | • | • | • |
| 6. Audit | | | | • | • |
| **Cyber Education** | | | | | |
| 7. Training and awareness* | • | • | • | • | • |
| **Information Asset Protection** | | | | | |
| 8. Asset management* | • | • | • | • | • |
| 9. Data protection and privacy* | • | • | • | • | • |
| 10. Backups* | • | • | • | • | • |
| 11. Bring Your Own Device (BYOD) | | | | • | • |
| 12. System security* | • | • | • | • | • |
| 13. Anti-virus/Anti-malware* | • | • | • | • | • |
| 14. Secure Software Development Life Cycle (SDLC) | | | | | • |
| **Secure Access and Environment** | | | | | |
| 15. Access control* | • | • | • | • | • |
| 16. Cyber threat management | | | | • | • |
| 17. Third-party risk and oversight | | | | | • |
| 18. Vulnerability assessment | | | • | • | • |
| 19. Physical/environmental security | | • | • | • | • |
| 20. Network security | | • | • | • | • |
| **Cybersecurity Resilience** | | | | | |
| 21. Incident response* | • | • | • | • | • |
| 22. Business continuity/disaster recovery | | • | • | • | • |
| | 10 DOMAINS | 13 DOMAINS | 16 DOMAINS | 19 DOMAINS | 22 DOMAINS |

*Measures in Cyber Essentials mark

For more information, see Cyber Trust.

The AWS Cloud Companion Guide begins with domain B8. Asset management as it does not provide organization-specific requirements such as policies and human resources controls as noted previously.

# B8. Domain: Asset management

The objective of this domain is to ensure that hardware and software assets in the organization are identified and tracked so that cybersecurity measures and processes can be implemented across the asset lifecycle. Active asset management allows for the organization to monitor risks and enables control of assets within its environment so that only authorized assets are used and installed.

| Mapping for Cyber Trust | AWS service | AWS service description | Security best practices |
|---|---|---|---|
| B.8.1.<br>The organization has identified hardware and software present in the environment and protected it against common cyber threats. | AWS Config | AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time. | Security best practices for AWS Config:<br>• Data Protection in AWS Config<br>• Identity and Access Management for AWS Config<br>• Logging and Monitoring in AWS Config<br>• Using AWS Config with Interface Amazon VPC Endpoints<br>• Incident Response in AWS Config<br>• Compliance Validation for AWS Config<br>• Resilience in AWS Config<br>• Infrastructure Security in AWS Config<br>• Cross-service confused deputy prevention<br>• Security Best Practices for AWS Config |

| | | | |
|---|---|---|---|
| | AWS Cost and Usage Reports (CUR) | The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. | AWS Cost and Usage Reports tracks your AWS usage and provides estimated charges associated with your account. Each report contains line items for each unique combination of AWS products, usage type, and operation that you use in your AWS account.<br><br>For details about security considerations, see Security in AWS Billing and Cost Management<br><br>For more information on access control and IAM permissions to use AWS CUR, see Overview of Managing Access Permissions. |

| | | | |
|---|---|---|---|
| B.8.4<br>The organization has established and implemented a process to classify and handle hardware and software according to their confidentiality and/or sensitivity levels to ensure that they receive adequate security and protection. | Tagging your AWS resources | You can assign metadata to your AWS resources in the form of tags. Each tag is a label consisting of a user-defined key and value. Tags can help you manage, identify, organize, search for, and filter resources. You can create tags to categorize resources by purpose, owner, environment, or other criteria. | Security best practices for tagging:<br>• Data protection in Tag Editor<br>• Identity and access management for Tag Editor<br>• Logging and monitoring in Tag Editor<br>• Compliance validation for Tag Editor<br>• Resilience in Tag Editor<br>• Infrastructure security in Tag Editor |
| B.8.6<br>The organization has established and implemented asset discovery tools that are appropriate and recognized in the industry to scan and discover assets that are connected to its network to ensure that all the assets | AWS Systems Manager Inventory | AWS Systems Manager Inventory provides visibility into your AWS computing environment. | You can use inventory to collect metadata from your managed nodes. You can store this metadata in a central Amazon Simple Storage Service (Amazon S3) bucket, and then use built in tools to query the data and quickly determine which nodes are running the software, the configurations required by your software policy, and which nodes need to be updated. You can also configure and view inventory data from multiple AWS Regions and AWS accounts. |

| | | | |
|---|---|---|---|
| can be managed securely.<br>B.8.9<br>The organization has established and implemented the use of an asset inventory management system that is appropriate and recognized in the industry to track and manage hardware and software assets to ensure accuracy and avoid oversight. | AWS Config | AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time. | Security best practices for AWS Config:<br>• Data Protection in AWS Config<br>• Identity and Access Management for AWS Config<br>• Logging and Monitoring in AWS Config<br>• Using AWS Config with Interface Amazon VPC Endpoints<br>• Incident Response in AWS Config<br>• Compliance Validation for AWS Config<br>• Resilience in AWS Config<br>• Infrastructure Security in AWS Config<br>• Cross-service confused deputy prevention<br>• Security Best Practices for AWS Config |

## B9. Domain: Data protection and privacy

The objective of this domain is to ensure that business-critical data in the organization environment are identified and tracked so that cybersecurity measures and processes can be implemented across the asset lifecycle. It also ensures that data collection, processing, transfer, and storage is secure to protect them from unauthorized access and disclosure.

| Mapping for Cyber Trust | AWS Service | AWS service description | Security best practices |
|---|---|---|---|
| B.9.5.<br>The organization has established and implemented policies and procedures to carry out risk classification and handle business-critical data (including personal data, company secrets, intellectual property, etc) according to their confidentiality and sensitivity levels to ensure that they receive adequate security and protection. | Amazon Macie | Amazon Macie is a data security service that uses machine learning (ML) and pattern matching to discover and help protect your sensitive data stored within your Amazon S3 buckets. | Security best practices for Amazon Macie:<br>• Data protection<br>• Identity and access management<br>• Logging and monitoring<br>• Compliance validation<br>• Resilience<br>• Infrastructure security<br>• VPC endpoints (AWS PrivateLink) |

| | | | |
|---|---|---|---|
| B.9.11<br>The organization uses encryption to protect its data and has established and implemented cryptographic policies and processes to ensure that the keys are being handled securely throughout the cryptography key management lifecycle. | AWS Key Management Service | AWS Key Management Service (AWS KMS) is a managed service that makes it simple for you to create and control the cryptographic keys that are used to help protect your data. AWS KMS uses hardware security modules (HSM) to protect and validate your AWS KMS keys under the FIPS 140-2 Cryptographic Module Validation Program | Security best practices for Amazon Key Management Service:<br>• Data protection<br>• Identity and access management<br>• Logging and monitoring<br>• Compliance validation<br>• Resilience<br>• Infrastructure security<br>• Security best practices |

| Mapping for Cyber Trust | AWS Service | AWS Service description | Security best practices |
|---|---|---|---|
| B.10.3<br>The organization has established and implemented automated backup processes to ensure that the backup tasks are carried out without fail and without the need for human intervention. | AWS Backup | AWS Backup enables you to centralize and automate data protection across AWS services. AWS Backup offers a cost-effective, fully managed policy-based service that further simplifies data protection at scale.<br>Sample use cases include backup and restoration capabilities for systems, periodic backups of information, and immutable storage. | Security best practices for AWS Backup:<br><br>• Data protection<br>• Legal hold<br>• Identity and access management<br>• Compliance validation<br>• Resilience<br>• Infrastructure security<br>• AWS PrivateLink |
| | Amazon EBS Snapshots | Amazon EBS provides the ability to create snapshots (backups) of EBS volumes. A point-in-time snapshot takes a copy of the EBS volume and places it in Amazon S3, where it is stored redundantly in multiple Availability Zones. | Ensure Amazon EBS encryption is used. Snapshots of encrypted EBS volumes are automatically encrypted. Amazon EBS encryption uses AWS KMS keys when creating encrypted volumes and snapshots.<br><br>You can also configure Encryption by default on new EBS volumes and snapshot copies that you create.<br><br>You can track the status of EBC snapshots through CloudWatch Events.<br><br>You can use Amazon EBS Snapshot Archive for low-cost long-term storage of rarely-accessed snapshots.<br><br>You can use Amazon Data Lifecycle Manager to automate the creation, retention, and |

| | | | |
|---|---|---|---|
| | | | deletion of snapshots that you use to back up your Amazon EBS volumes.<br>Control the permissions of a snapshot to verify appropriate access. |
| | Amazon S3 Object Lock | Based on the criticality of your data, you can choose to use Amazon S3 Object Lock, where you can store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use Object Lock to help meet regulatory requirements that require WORM storage, or to simply add another layer of protection against object changes and deletion. | Use Amazon S3 Event Notifications to track access and changes to your Object Lock configurations and data using AWS CloudTrail.<br><br>You can use S3 Object Lock with replication to enable automatic, asynchronous copying of locked objects and their retention metadata, across S3 buckets in different or the same AWS Region. |
| | AWS Backup Vault Lock | AWS Backup Vault Lock allows you to deploy and manage your vault's immutability policies, helping protect your backups from accidental or malicious deletions. | Depending on your data retention needs, with AWS Backup Vault Lock, you can set governance mode or compliance mode to configure your vault's immutability policies with greater flexibility and multiple levels of security. Under governance mode, users with the appropriate role-based permissions can test and change retention policies or even remove the lock completely. In compliance mode, the user can specify a lock date after which the vault is locked immutably. Once locked, the acceptable retention periods cannot be changed and the lock cannot be disabled even by the root user. With this feature, the console also provides you with |

| | | | |
|---|---|---|---|
| | | | visibility into your vault's lock status and facilitates reporting across locked vaults. |

## B10. Domain: Backups

The objective of this domain is to ensure that information assets are regularly backed up in a secure and consistent manner so that the organization can restore and recover its systems and data in the event of a cybersecurity or breach of data incident.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Security best practice |
|---|---|---|---|
| B.10.3<br>The organization has established and implemented automated backup processes to ensure that the backup tasks are carried out without fail and without the need for human intervention. | AWS Backup | AWS Backup enables you to centralize and automate data protection across AWS services. AWS Backup offers a cost-effective, fully managed policy based service that further simplifies data protection at scale.<br>Sample use cases include backup and restoration capabilities for systems, periodic backups of information, and immutable storage. | Security best practices for AWS Backup:<br>• Data protection<br>• Legal hold<br>• Identity and access management<br>• Compliance validation<br>• Resilience<br>• Infrastructure security<br>• AWS PrivateLink |

| | | | |
|---|---|---|---|
| B.10.4.<br>The organization has established and implemented backup plan(s) on the types, frequency and storage of backups to ensure that there is clarity of the steps to be taken to backup business-critical data in the organization.<br>B.10.6<br>The organization has established and implemented policies and procedures to perform reviews on the backup status regularly to ensure that failed backup jobs are addressed and remediated. | Amazon EBS Snapshots | Amazon EBS provides the ability to create snapshots (backups) of EBS volumes. A point-in-time snapshot takes a copy of the EBS volume and places it in Amazon S3, where it is stored redundantly in multiple Availability Zones. | Verify that Amazon EBS encryption is used. Snapshots of encrypted EBS volumes are automatically encrypted. Amazon EBS encryption uses AWS KMS keys when creating encrypted volumes and snapshots. You can also configure Encryption by default on new EBS volumes and snapshot copies that you create.<br><br>You can track the status of EBC snapshots through CloudWatch Events.<br>You can utilize Amazon EBS Snapshot Archive for low-cost long-term storage of rarely-accessed snapshots.<br>You can utilize Amazon Data Lifecycle Manager to automate the creation, retention, and deletion of snapshots that you use to back up your Amazon EBS volumes.<br>Control the permissions of a snapshot to ensure appropriate access. |
| | Amazon S3 Object Lock | Based on the criticality of your data, you can choose to use Amazon S3 Object Lock, where you can store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use Object Lock to help align with regulatory requirements that require WORM storage, or to simply add another layer of protection against object changes and deletion. | Use Amazon S3 Event Notifications to track access and changes to your Object Lock configurations and data using AWS CloudTrail.<br><br>You can use S3 Object Lock with replication to enable automatic, asynchronous copying of locked objects and their retention metadata, across S3 buckets in different or the same AWS Region. |

| | | | |
|---|---|---|---|
| | AWS Backup Vault Lock | AWS Backup Vault Lock allows you to deploy and manage your vault's immutability policies, helping protect your backups from accidental or malicious deletions. | Depending on your data retention needs, with AWS Backup Vault Lock, you can set governance mode or compliance mode to configure your vault's immutability policies with greater flexibility and multiple levels of security. Under governance mode, users with the appropriate role-based permissions can test and change retention policies or even remove the lock completely. In compliance mode, the user can specify a lock date after which the vault is locked immutably. Once locked, the acceptable retention periods cannot be changed and the lock cannot be disabled even by the root user. With this feature, the console also provides you with visibility into your vaults' lock status and facilitates reporting across locked vaults. |

## B12. Domain: System security

The objective of this domain is to ensure that cybersecurity measures and safeguards are implemented and maintained to secure the organization's systems. These measures and safeguards include secure configuration, logging, updates and patching.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Security best practice |
|---|---|---|---|

| | | | |
|---|---|---|---|
| B12.3<br>The organization has defined and applied a patch management process to test and install the updates and patches securely to ensure that there are no adverse effects.<br><br>B.12.6<br>The organization has defined and applied a patch management process to test and install the updates and patches securely to ensure that there are no adverse effects.<br><br>B.12.9<br>The organization has established and implemented a secure logging policy and procedure with the requirements, guidelines and detailed steps to store, retain | AWS Systems Manager Patch Manager | Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed nodes with both security-related updates and other types of updates. | AWS Identity and Access Management (IAM) – Use IAM to control which users, groups, and roles have access to Patch Manager operations. For more information, see How AWS Systems Manager works with IAM and Configure instance permissions for Systems Manager.<br><br>AWS CloudTrail – Use CloudTrail to record an auditable history of patching operation events initiated by users, roles, or groups. For more information, see Logging AWS Systems Manager API calls with AWS CloudTrail.<br><br>AWS Security Hub – Patch compliance data from Patch Manager can be sent to AWS Security Hub. Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status. It also monitors the patching status of your fleet. For more information, see Integrating Patch Manager with AWS Security Hub.<br><br>AWS Config – Set up recording in AWS Config to view Amazon EC2 instance management data in the Patch Manager Dashboard. For more information, see Viewing patch Dashboard summaries (console). |

| | | | |
|---|---|---|---|
| and delete the logs from unauthorized access.<br><br>B.12.10<br>The organization has established and implemented policies and procedures with the requirements, guidelines and detailed steps to perform and install patches/updates to ensure that the system(s) is/are patched or updated within the defined timeframes according to their priority. | | | |

| | | | |
|---|---|---|---|
| | Guidance for Log Storage on AWS | Guidance for Log Storage on AWS provides guidance on how to build a secure a resilient log storage. | Guidance includes information on Storing logs centrally in Amazon S3, ensuring the integrity of logs within your log storage, managing logs in log storage, adding new logs to log storage and granting access to the logs.<br>Logs on AWS should include:<br>• AWS CloudTrail<br>• Amazon CloudWatch Logs<br>• VPC Flow Logs<br>• Amazon S3 Logs<br>• AWS WAF Logs<br>• AWS Config Logs<br>• Amazon CloudFront Logs<br>• Application Load Balancer Logs.<br>• Amazon GuardDuty Findings<br>• Amazon EC2 logs<br>• Amazon EKS logs |

| | | | |
|---|---|---|---|
| B.12.11<br>The organization has implemented a configuration management tool/solution that is appropriate and recognised in the industry to ensure that the system's configurations are maintained in a desired and consistent state.<br><br>B.12.12<br>The organization has established and implemented policies and procedures to ensure that the system's configuration requirements are aligned with the industry benchmarks and standards, e.g., CIS configuration benchmarks. | AWS Security Hub | AWS Security Hub is a cloud security posture management (CSPM) service that performs security best practice checks, aggregates alerts, and enables automated remediation. | AWS Security Hub currently supports the following standards:<br><br>• AWS Foundational Security Best Practices (FSBP) standard<br>• Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and v1.4.0<br>• National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5<br>• Payment Card Industry Data Security Standard (PCI DSS)<br>• Service-managed standards |

| | | | |
|---|---|---|---|
| | AWS Config | AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time. | Security best practices for AWS Config:<br><br>• Data Protection in AWS Config<br>• Identity and Access Management for AWS Config<br>• Logging and Monitoring in AWS Config<br>• Using AWS Config with Interface Amazon VPC Endpoints<br>• Incident Response in AWS Config<br>• Compliance Validation for AWS Config<br>• Resilience in AWS Config<br>• Infrastructure Security in AWS Config<br>• Cross-service confused deputy prevention<br>• Security Best Practices for AWS Config |

## B13. Domain: Anti-virus/Anti-malware

The objective of this domain is to ensure that protection measures and technologies are implemented, maintained, and updated to continuously monitor and defend against malicious software which may disrupt or damage the network. This domain also addresses the processes put in place to manage successful malicious software attacks, so that further damage and spread to the network and environment is prevented.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Security best practices |
|---|---|---|---|
| B.13.3<br>The organization has established and implemented the use of anti-virus or anti-malware solution(s) that is/are appropriate and recognized in the industry with features such as real-time malware detection to ensure that it can protect the organization adequately. | Amazon GuardDuty Malware Protection | Amazon GuardDuty Malware Protection helps you detect the potential presence of malware by scanning the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the Amazon Elastic Compute Cloud (Amazon EC2) instances and container workloads. | You can choose to customize malware scanning options on Amazon GuardDuty for Amazon EC2 instances or container workloads to include:<br>• Snapshot retention<br>• Inclusion or exclusion of EC2 instances and EBS volumes |

| | | | |
|---|---|---|---|
| B.13.4<br>The organization has established and implemented web filtering to protect the business from surfing malicious sites. | Amazon Route53 DNS Resolver Firewall | Route 53 Resolver DNS Firewall allows you to filter and regulate outbound DNS traffic for your virtual private cloud (VPC). | With Resolver DNS Firewall, you can filter and regulate outbound DNS traffic for your VPC.<br>To do this, you create reusable collections of filtering rules in DNS Firewall rule groups, associate the rule groups to your VPC, and then monitor the activity in DNS Firewall logs and metrics. With DNS Firewall, you can monitor and control the domains that your applications can query. You can deny access to the domains that you know to be malicious and allow other queries to pass through.<br><br>Alternatively, you can deny access to all domains except for the ones that you explicitly trust. |

| | | | |
|---|---|---|---|
| | AWS Network Firewall | AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC). You can use Network Firewall to monitor and protect your Amazon VPC traffic in a number of ways, including the following:<br><br>• Pass traffic through only from known AWS service domains or IP address endpoints, such as Amazon S3.<br>• Use custom lists of known bad domains to limit the types of domain names that your applications can access.<br>• Perform deep packet inspection on traffic entering or leaving your VPC.<br>• Use stateful protocol detection to filter protocols like HTTPS, independent of the port used. | Security best practices for AWS Network Firewall:<br><br>• Data protection in Network Firewall<br>• Identity and Access Management for AWS Network Firewall<br>• AWS logging and monitoring tools<br>• Compliance validation and security best practices for Network Firewall<br>• Resilience in Network Firewall<br>• Infrastructure security in AWS Network Firewall |

# B14. Domain: Secure Software Development Lifecycle (SDLC)

The objective of this domain is to ensure that security specifications and practices are incorporated into the system's SDLC so that the software can be developed in a secure and consistent manner.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Security best practices |
|---|---|---|---|
| B.14.6<br>The organization has established and implemented security guidelines and requirements in its system and/or application development, e.g., secure coding to ensure that it adheres to the security principles. | Amazon Inspector | Amazon Inspector is an automated vulnerability management service that continually scans Amazon Web Services (AWS) workloads for software vulnerabilities and unintended network exposure. Amazon Inspector currently supports vulnerability reporting for Amazon Elastic Compute Cloud (Amazon EC2) instances and container images stored in Amazon Elastic Container Registry (Amazon ECR) | Security best practices for Amazon Inspector:<br>• Data protection in Amazon Inspector<br>• Identity and Access Management for Amazon Inspector<br>• Monitoring Amazon Inspector<br>• Compliance validation for Amazon Inspector<br>• Resilience in Amazon Inspector<br>• Infrastructure security in Amazon Inspector<br>• Incident response in Amazon Inspector |
| B.14.7<br>The organization has established and implemented the change management policy and process to ensure that changes or deployment to | AWS CodeCommit | AWS CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. CodeCommit reduces the need for you to manage your own source control system or worry about scaling its infrastructure. | Security Best Practices for AWS CodeCommit:<br>• Data protection in AWS CodeCommit<br>• Identity and Access Management for AWS CodeCommit<br>• Resilience in AWS CodeCommit<br>• Infrastructure security in AWS CodeCommit |

| | | | |
|---|---|---|---|
| the production environment is reviewed and tested securely with a rollback plan in place to ensure that the change is controlled.<br><br>B.14.8<br>The organization has established and implemented a policy and process to perform security testing on the system or application before deployment to ensure that the security weaknesses and vulnerabilities are identified. | Amazon CodeGuru Security | Amazon CodeGuru Security is a static application security tool that uses machine learning to detect security policy violations and vulnerabilities. | Security best practices for Amazon CodeGuru Security:<br><br>• Data protection in Amazon CodeGuru Security<br>• Identity and access management for Amazon CodeGuru Security<br>• Compliance validation for Amazon CodeGuru Security<br>• Resilience in Amazon CodeGuru Security<br>• Infrastructure Security in Amazon CodeGuru Security |

| | | | |
|---|---|---|---|
| | Amazon CodeWhisperer | Amazon CodeWhisperer is a machine learning (ML)-powered service that helps improve developer productivity by generating code recommendations based on their comments in natural language and code in the integrated development environment (IDE). | Security best practices for Amazon CodeWhisperer:<br>• Resilience in Amazon CodeWhisperer<br>• Vulnerability analysis and management in Amazon CodeWhisperer<br>• Best practices for administrative security with IAM Identity Center and CodeWhisperer<br>• Data protection<br>• Compliance validation for Amazon CodeWhisperer<br>• Security best practices in Amazon CodeWhisperer<br>• Infrastructure security in Amazon CodeWhisperer<br>• Identity and Access Management for Amazon CodeWhisperer<br>• Amazon CodeWhisperer and interface VPC endpoints (AWS PrivateLink) |
| | AWS Secrets Manager | AWS Secrets Manager helps you to securely encrypt, store, and retrieve credentials for your databases and other services. Instead of hardcoding credentials in your apps, you can make calls to Secrets Manager to retrieve your credentials whenever needed. Secrets Manager helps you protect access to your IT resources and data by enabling you to rotate and manage access to your secrets. | Security best practices for AWS Secrets Manager:<br>• Mitigate the risks of using the AWS CLI to store your AWS Secrets Manager secrets<br>• Data protection in AWS Secrets Manager<br>• Secret encryption and decryption in AWS Secrets Manager<br>• Infrastructure security in AWS Secrets Manager<br>• Resiliency in AWS Secrets Manager |

# B15. Domain: Access control

The objective of this domain is to ensure that sufficient access management controls and formalized processes are in place so that the access to the organization's assets and data by employees, contractors and third parties are only granted on the principle of least privilege, and managed in a controlled and consistent manner.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Security best practices |
|---|---|---|---|
| B.15.1<br>The organization has implemented all the cybersecurity requirements to ensure that there are cybersecurity measures in place over who has access to the data and assets. | AWS Identity and Access Management | AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access. | Security best practices for AWS IAM:<br>• AWS security credentials<br>• AWS security audit guidelines<br>• Data protection in AWS Identity and Access Management<br>• Logging and monitoring in AWS Identity and Access Management<br>• Compliance validation for AWS Identity and Access Management<br>• Resilience in AWS Identity and Access Management<br>• Infrastructure security in AWS Identity and Access Management<br>• Configuration and vulnerability analysis in AWS Identity and Access Management<br>• Security best practices and use cases in AWS Identity and Access Management<br>• AWS managed policies for AWS Identity and Access Management Access Analyzer |

| | | | |
|---|---|---|---|
| | AWS Identity Center | IAM Identity Center provides one place where you can create or connect workforce users and centrally manage their access across your AWS accounts and applications. You can use multi-account permissions to assign your workforce users access to AWS accounts. You can use application assignments to assign your users access to IAM Identity Center enabled applications, cloud applications, and customer Security Assertion Markup Language (SAML 2.0) applications. | Security best practices for AWS Identity Center:<br>• Identity and access management for IAM Identity Center<br>• IAM Identity Center console and API authorization<br>• Logging and monitoring in IAM Identity Center<br>• Compliance validation for IAM Identity Center<br>• Resilience in IAM Identity Center<br>• Infrastructure security in IAM Identity Center |

| | | | |
|---|---|---|---|
| B.15.11<br>The organization has established and implemented a privileged access solution that is appropriate and recognized in the industry to authenticate users and authorize access based on their roles to ensure that there is a more efficient and effective way of managing access. | Temporary elevated Access with AWS IAM Identity Center | AWS IAM Identity Center (successor to AWS Single Sign-On) provides you with options for temporary elevated access management for both vendor-managed and supported solutions as well as self-managed and self-supported solutions. | For more information about privileged access, see Temporary elevated access. |

## B16. Domain: Cyber threat management

The objective of this domain is to ensure that the organization actively identifies threats and security anomalies within their operating environment, across systems, network devices and employees so that early detection and response activities can be carried out.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Security best practices |
|---|---|---|---|
| B.16.5<br>The organization has defined and allocated the roles and responsibilities to carry out log monitoring and review on its systems, investigating the incidents and reporting to relevant stakeholders. | Systems Manager Incident Manager | Incident Manager, a capability of AWS Systems Manager, is designed to help you mitigate and recover from incidents affecting your applications hosted on AWS. This includes setting up engagement plans that specifies individual contacts and escalation paths to ensure visibility among stakeholders and active participation during the incident response process. | Security best practices for AWS Systems Manager Incident Manager:<br><br>• Data protection in Incident Manager<br>• Identity and Access Management for AWS Systems Manager Incident Manager<br>• Working with shared contacts and response plans in Incident Manager<br>• Compliance validation for AWS Systems Manager Incident Manager<br>• Resilience in AWS Systems Manager Incident Manager<br>• Infrastructure security in AWS Systems Manager Incident Manager<br>• Working with AWS Systems Manager Incident Manager and interface VPC endpoints (AWS PrivateLink)<br>• Configuration and vulnerability analysis in Incident Manager<br>• Security best practices in AWS Systems Manager Incident Manager |

| | | | |
|---|---|---|---|
| | AWS account contact and security contact information | You can store contact information about the primary account contact for your AWS account. You can also add or edit contact information for the alternate security account contact, which receives security related notifications, including notifications from the AWS Trust and Safety Team. | Update the alternate security contacts for your AWS accounts and AWS organization for timely security notifications. |

| | | | |
|---|---|---|---|
| B.16.6<br><br>The organization has implemented Security Information and Event Management (SIEM) to store the logs centrally for correlation and to ensure that the logs are monitored more effectively. | SIEM on Amazon OpenSearch Service | SIEM on Amazon OpenSearch Service is a solution for collecting multiple types of logs from multiple AWS accounts, correlating and visualizing the logs to help investigate security incidents. | As soon as AWS services logs are put into a specified Amazon S3 bucket, a purpose-built AWS Lambda function automatically loads those logs into SIEM on OpenSearch Service, enabling you to view visualized logs in the dashboard and correlate multiple logs to investigate security incidents. |

| | | | |
|---|---|---|---|
| | Amazon Security Lake | Amazon Security Lake is a fully managed security data lake service. You can use Security Lake to automatically centralize security data from AWS environments, SaaS providers, on premises, cloud sources, and third-party sources into a purpose-built data lake that's stored in your AWS account. | Security best practices for Amazon Security Lake:<br>• Identity and access management for Amazon Security Lake<br>• Data protection in Amazon Security Lake<br>• Compliance validation for Amazon Security Lake<br>• Security best practices for Security Lake<br>• Resilience in Amazon Security Lake<br>• Infrastructure security in Amazon Security Lake<br>• Configuration and vulnerability analysis in Security Lake<br>• Monitoring Amazon Security Lake |

| | | | |
|---|---|---|---|
| | Guidance for Log Storage on AWS | Guidance for Log Storage on AWS provides guidance on how to build a secure a resilient log storage. | Guidance includes information on: Storing logs centrally in Amazon S3, Verifying the integrity of logs within your log storage, managing logs in log storage, adding new logs to log storage and granting access to the logs.<br><br>Logs on AWS should include:<br><br>• AWS CloudTrail<br>• Amazon CloudWatch Logs<br>• VPC Flow Logs<br>• Amazon S3 Logs<br>• AWS WAF Logs<br>• AWS Config Logs<br>• Amazon CloudFront Logs<br>• Application Load Balancer Logs.<br>• Amazon GuardDuty Findings<br>• Amazon EC2 logs<br>• Amazon EKS logs |

| | | | |
|---|---|---|---|
| | AWS CloudTrail Lake | AWS CloudTrail Lake is a managed data lake that lets organizations aggregate, immutably store, and query events recorded by CloudTrail for auditing, security investigation, and operational troubleshooting.<br>This new service simplifies CloudTrail analysis workflows by integrating collection, storage, preparation, and optimization for analysis and query in the same product. | AWS CloudTrail Lake does not require you to move and ingest CloudTrail logs elsewhere, which helps maintain data fidelity and decreases dealing with low-rate limits that throttle your logs. It also provides near real-time latencies, because it is fine-tuned to process high-volume structured logs, making them available for incident investigation. Also, CloudTrail Lake provides a multi-attribute query experience with SQL and is capable of scheduling and handling multiple concurrent queries. |
| B16.7<br><br>The organization has established and implemented a security baseline profile on its systems to analyze and | AWS Control Tower | AWS Control Tower simplifies AWS experiences by orchestrating multiple AWS services on your behalf while maintaining the security and compliance needs of your organization, following prescriptive best practices. | Security best practices for AWS Control Tower:<br><br>• Data Protection<br>• Identity and access management<br>• Compliance Validation<br>• Resilience<br>• Infrastructure Security |

| | | | |
|---|---|---|---|
| perform monitoring to ensure that anomalies are identified. | AWS Security Hub | AWS Security Hub is a cloud security posture management (CSPM) service that performs security best practice checks, aggregates alerts, and enables automated remediation. | AWS Security Hub currently supports the following standards:<br><br>• AWS Foundational Security Best Practices (FSBP) standard<br>• Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and v1.4.0<br>• National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5<br>• Payment Card Industry Data Security Standard (PCI DSS)<br>• Service-managed standards |

| | | | |
|---|---|---|---|
| | AWS Config | AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time. | Security best practices for AWS Config:<br><br>• Data Protection in AWS Config<br>• Identity and Access Management for AWS Config<br>• Logging and Monitoring in AWS Config<br>• Using AWS Config with Interface Amazon VPC Endpoints<br>• Incident Response in AWS Config<br>• Compliance Validation for AWS Config<br>• Resilience in AWS Config<br>• Infrastructure Security in AWS Config<br>• Cross-service confused deputy prevention<br>• Security Best Practices for AWS Config |

| | | | |
|---|---|---|---|
| B.16.9<br><br>The organization has established and implemented advanced analytics processes and solutions that are appropriate and recognized in the industry to detect against abnormal systems and user behavior, user behavior analytics.<br><br>B.16.11 | Amazon GuardDuty | Amazon GuardDuty is a continuous security monitoring service. Amazon GuardDuty can help to identify unexpected and potentially unauthorized or malicious activity in your AWS environment. | Security best practices for Amazon GuardDuty:<br><br>• Data protection in Amazon GuardDuty<br>• Logging Amazon GuardDuty API calls with AWS CloudTrail<br>• Identity and Access Management for Amazon GuardDuty<br>• Compliance validation for Amazon GuardDuty<br>• Resilience in Amazon GuardDuty<br>• Infrastructure security in Amazon GuardDuty |

| | | | |
|---|---|---|---|
| The organization has established and implemented measures and processes to proactively search for threats that are hidden in its IT environment. | Amazon Detective | Amazon Detective makes it simple to analyze, investigate, and quickly identify the root cause of security findings or suspicious activities. Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to help you visualize and conduct faster and more efficient security investigations. | Security best practices for Amazon Detective:<br>• Data protection in Amazon Detective<br>• Identity and access management for Amazon Detective<br>• Using service-linked roles for Detective<br>• AWS managed policies for Amazon Detective<br>• Logging and monitoring in Amazon Detective<br>• Compliance validation for Amazon Detective<br>• Resilience in Amazon Detective<br>• Infrastructure security in Amazon Detective<br>• Security best practices for Amazon Detective |

## B18. Domain: Vulnerability assessment

The objective of this domain is to ensure that vulnerability assessment and management are established to keep the organization's network and systems safe from known exploitation. This domain also ensures processes to identify, evaluate, mitigate, and report on security vulnerabilities in systems and the software.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Configuration guidance |
|---|---|---|---|
| B.18.7<br><br>The organization has established and implemented measures and processes to track, review, evaluate and address the vulnerabilities uncovered as part of the assessments to ensure that the vulnerabilities are being remediated | Amazon Inspector | Amazon Inspector is an automated vulnerability management service that continually scans Amazon Web Services (AWS) workloads for software vulnerabilities and unintended network exposure. Amazon Inspector currently supports vulnerability reporting for Amazon Elastic Compute Cloud (Amazon EC2) instances and container images stored in Amazon Elastic Container Registry (Amazon ECR) | Security best practices for Amazon Inspector:<br><br>• Data protection in Amazon Inspector<br>• Identity and Access Management for Amazon Inspector<br>• Monitoring Amazon Inspector<br>• Compliance validation for Amazon Inspector<br>• Resilience in Amazon Inspector<br>• Infrastructure security in Amazon Inspector<br>• Incident response in Amazon Inspector |

| | | | |
|---|---|---|---|
| according to their severity. | AWS Security Hub | AWS Security Hub is a cloud security posture management (CSPM) service that performs security best practice checks, aggregates alerts, and enables automated remediation. | AWS Security Hub currently supports the following standards:<br>• AWS Foundational Security Best Practices (FSBP) standard<br>• Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and v1.4.0<br>• National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5<br>• Payment Card Industry Data Security Standard (PCI DSS)<br>• Service-managed standards |

| | | | |
|---|---|---|---|
| | ECR Container Registry (Amazon ECR) Image Scanning | Amazon ECR image scanning helps in identifying software vulnerabilities in your container images. | When an image scanning is configured for your private registry, you may specify that all repositories be scanned or you can specify filters to scope which repositories are scanned.<br>When basic scanning is used, you may specify scan on push filters to specify which repositories are set to do an image scan when new images are pushed. Repositories not matching a basic scanning scan on push filter will be set to the manual scan frequency which means to perform a scan, you must manually trigger the scan.<br>When enhanced scanning is used, you may specify separate filters for scan on push and continuous scanning. Repositories not matching an enhanced scanning filter will have scanning disabled. If you are using enhanced scanning and specify separate filters for scan on push and continuous scanning where multiple filters match the same repository, then Amazon ECR enforces the continuous scanning filter over the scan on push filter for that repository. |

| | | | |
|---|---|---|---|
| B.18.10<br><br>The organization has established and implemented metrics and thresholds including dashboards to provide reporting and tracking of open, overdue and severe vulnerabilities noted within its systems to provide visibility on tracking and remediations within established timelines. | AWS Systems Manager Patch Manager | Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed nodes with both security-related updates and other types of updates. | **AWS Identity and Access Management (IAM)** – Use IAM to control which users, groups, and roles have access to Patch Manager operations. For more information, see How AWS Systems Manager works with IAM and Configure instance permissions for Systems Manager.<br><br>**AWS CloudTrail** – Use CloudTrail to record an auditable history of patching operation events initiated by users, roles, or groups. For more information, see Logging AWS Systems Manager API calls with AWS CloudTrail.<br><br>**AWS Security Hub** – Patch compliance data from Patch Manager can be sent to AWS Security Hub. Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status. It also monitors the patching status of your fleet. For more information, see Integrating Patch Manager with AWS Security Hub.<br><br>**AWS Config** – Set up recording in AWS Config to view Amazon EC2 instance management data in the Patch Manager Dashboard. For more information, see Viewing patch Dashboard summaries (console). |

| | | | |
|---|---|---|---|
| | Manage and view Systems Manager patch and compliance data using Amazon QuickSight solution | With Amazon QuickSight, you can query, analyze, and visualize Systems Manager Inventory data. You can also publish interactive dashboards. You can use Amazon QuickSight with Amazon Athena table dataset to create dashboards and widgets for displaying compliance information. | Security best practices for Amazon QuickSight:<br>• Data protection<br>• Identity and access management<br>• Incident response, logging, and monitoring<br>• Compliance validation<br>• Resilience<br>• Infrastructure security<br>• Best practices<br>• AWS managed policies |

## B20. Domain: Network security

The objective of this domain is to ensure that sufficient cybersecurity measures and processes are established to secure the confidentiality and accessibility of the organization's network and data.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Configuration guidance |
|---|---|---|---|

| | | | |
|---|---|---|---|
| B.20.2<br>The organization has configured and implemented access control (i.e., an allowlist or deny list) to its network to enforce network security policy and ensure that unauthorized users or devices are kept out.<br>B.20.3<br>The organization has established and implemented the use of stateful firewall over basic packet filtering firewall to ensure that packets are filtered with more context for greater effectiveness.<br><br>B.20.6<br>The organization has defined and applied a process to | Network Access Control Lists (ACLs) | A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level. You can use the default network ACL for your VPC, or you can create a custom network ACL for your VPC with rules that are like the rules for your security groups to add an additional layer of security to your VPC. | Security best practices for Amazon VPC:<br><br>• Data protection in Amazon Virtual Private Cloud<br>• Identity and access management for Amazon VPC<br>• Infrastructure security in Amazon VPC<br>• Control traffic to your AWS resources using security groups<br>• Control traffic to subnets using network ACLs<br>• Resilience in Amazon Virtual Private Cloud<br>• Compliance validation for Amazon Virtual Private Cloud<br>• Security best practices for your VPC |

| | | | |
|---|---|---|---|
| carry out network segmentation to segregate into private and public networks with the private network holding all the business-critical data and having no connection to the Internet to ensure that it is isolated from external threats. | | | |

| | | | |
|---|---|---|---|
| | Amazon VPC Security Groups | Security groups are virtual firewalls that controls the traffic allowed to and from the resources in your virtual private cloud (VPC). You can choose the ports and protocols to allow for inbound traffic and for outbound traffic. | Security best practices for Amazon VPC:<br>• Data protection in Amazon Virtual Private Cloud<br>• Identity and access management for Amazon VPC<br>• Infrastructure security in Amazon VPC<br>• Control traffic to your AWS resources using security groups<br>• Control traffic to subnets using network ACLs<br>• Resilience in Amazon Virtual Private Cloud<br>• Compliance validation for Amazon Virtual Private Cloud<br>• Security best practices for your VPC |

| | | | |
|---|---|---|---|
| | AWS Network Firewall | AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC).<br><br>You can use Network Firewall to monitor and protect your Amazon VPC traffic in a number of ways, including the following:<br><br>Pass traffic through only from known AWS service domains or IP address endpoints, such as Amazon S3.<br><br>Use custom lists of known bad domains to limit the types of domain names that your applications can access.<br><br>Perform deep packet inspection on traffic entering or leaving your VPC.<br><br>Use stateful protocol detection to filter protocols like HTTPS, independent of the port used. | Security best Practices for AWS Network Firewall:<br><br>• Data protection in Network Firewall<br>• Identity and Access Management for AWS Network Firewall<br>• AWS logging and monitoring tools<br>• Compliance validation and security best practices for Network Firewall<br>• Resilience in Network Firewall<br>• Infrastructure security in AWS Network Firewall |

| | | | |
|---|---|---|---|
| B.20.9<br>The organization has established and implemented network intrusion detection on the organization's network to monitor and detect malicious network traffic to ensure that they can be identified and addressed in a timely manner.<br>B.20.11<br>The organization has established and implemented network intrusion prevention on the organization's network to block malicious network traffic and ensure that it is protected from threats. | AWS Network Firewall | AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC).<br>You can use Network Firewall to monitor and protect your Amazon VPC traffic in a number of ways, including the following:<br>Pass traffic through only from known AWS service domains or IP address endpoints, such as Amazon S3.<br>Use custom lists of known bad domains to limit the types of domain names that your applications can access.<br>Perform deep packet inspection on traffic entering or leaving your VPC.<br>Use stateful protocol detection to filter protocols like HTTPS, independent of the port used. | Security Best Practices for AWS Network Firewall:<br>• Data protection in Network Firewall<br>• Identity and Access Management for AWS Network Firewall<br>• AWS logging and monitoring tools<br>• Compliance validation and security best practices for Network Firewall<br>• Resilience in Network Firewall<br>• Infrastructure security in AWS Network Firewall |

| | | | |
|---|---|---|---|
| | AWS Web Application Firewall | AWS WAF is a web application firewall that lets you monitor and manage web requests that are forwarded to protected AWS resources. With AWS WAF, you can protect resources such as Amazon CloudFront distributions, Amazon API Gateway REST APIs, Application Load Balancers, and AWS AppSync GraphQL APIs. You can use AWS WAF to inspect web requests for matches to conditions that you specify, such as the IP address that the requests originate from, the value of a specific request component, or the rate at which requests are being sent. AWS WAF can manage matching requests in a variety of ways, including counting them, blocking or allowing them, or sending challenges like CAPTCHA puzzles to the client user or browser. | Security best practices for AWS WAF:<br><br>• Data protection<br>• Identity and access management<br>• Logging and monitoring<br>• Compliance validation<br>• Resilience<br>• Infrastructure security |

## B21. Domain: Incident response

The objective of this domain is to ensure that the organization has formalized an incident response plan with regular exercises conducted to maintain the effectiveness of the current incident management setup. This allows the organization to detect, respond to, and recover from cybersecurity incidents in a timely, professional, and appropriate manner in an event of a cybersecurity incident.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Configuration guidance |
|---|---|---|---|
| B.21.6<br>The organization has defined and established the policies and procedures on the requirements, guidelines and detailed steps to conduct investigation into the incident to gather evidence to ensure that they are able to identify the root cause. | Systems Manager Incident Manager | Incident Manager, a capability of AWS Systems Manager, is designed to help you mitigate and recover from incidents affecting your applications hosted on AWS. This includes setting up engagement plans that specifies individual contacts and escalation paths to provide visibility among stakeholders and active participation during the incident response process. | Security best practices for AWS Systems Manager Incident Manager:<br>• Data protection in Incident Manager<br>• Identity and Access Management for AWS Systems Manager Incident Manager<br>• Working with shared contacts and response plans in Incident Manager<br>• Compliance validation for AWS Systems Manager Incident Manager<br>• Resilience in AWS Systems Manager Incident Manager<br>• Infrastructure security in AWS Systems Manager Incident Manager<br>• Working with AWS Systems Manager Incident Manager and interface VPC endpoints (AWS PrivateLink)<br>• Configuration and vulnerability analysis in Incident Manager<br>• Security best practices in AWS Systems Manager Incident Manager |

# B22. Domain: Business continuity and disaster recovery

The objective of this domain is to ensure that the organization has identified critical assets and business processes so that recovery priorities can be established. Business continuity and disaster recovery management ensures that the organization has developed and maintained capabilities, plans and testing to prepare employees so that the organization is able to withstand disruptions and continue operations.

| Mapping for Cyber Trust | AWS Service | AWS Service description | Configuration guidance |
|---|---|---|---|
| B.22.2<br>The organization has identified the critical assets in the organization that require high availability and performed measures to ensure that there are redundancies for them.<br><br>B.22.5<br>The organization has established and implemented the business continuity and disaster recovery policies with the requirements, roles and responsibilities, and guidelines including the recovery time objectives (RTO) and recovery point objectives | AWS Backup | AWS Backup enables you to centralize and automate data protection across AWS services. AWS Backup offers a cost-effective, fully managed policy-based service that further simplifies data protection at scale.<br>Sample use cases include backup and restoration capabilities for systems, periodic backups of information, and immutable storage. | Security best practices for AWS Backup:<br><br>• Data protection<br>• Legal hold<br>• Identity and access management<br>• Compliance validation<br>• Resilience<br>• Infrastructure security<br>• AWS PrivateLink |

| Mapping for Cyber Trust | AWS Service | AWS Service description | Configuration guidance |
|---|---|---|---|
| (RPO) to ensure that business resumption can be carried out in accordance with the system's criticality.<br><br>B.22.6<br>The organization has established and implemented a business continuity and disaster recovery plan to respond and recover against the common business disruption scenarios including those caused by cybersecurity incidents to ensure cyber resiliency. | | | |
| | AWS Elastic Disaster Recovery | AWS Elastic Disaster Recovery (AWS DRS) minimizes downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery. | Security best practices for AWS Elastic Disaster Recovery:<br><br>• Overview<br>• Identity and access management for AWS Elastic Disaster Recovery |

| Mapping for Cyber Trust | AWS Service | AWS Service description | Configuration guidance |
|---|---|---|---|
| | | | • Resilience in AWS Elastic Disaster Recovery<br>• Infrastructure security in AWS Elastic Disaster Recovery<br>• Compliance validation for AWS Elastic Disaster Recovery<br>• Cross-service confused deputy prevention |
| B.22.8<br>The organization has established and implemented the policy and process to test on its business continuity and disaster recovery plan regularly at least on an annual basis to ensure the effectiveness of the plan in achieving its objectives. | AWS Fault Injection Simulator | AWS Fault Injection Simulator (AWS FIS) is a managed service that enables you to perform fault injection experiments on your AWS workloads. Fault injection is based on the principles of chaos engineering. These experiments stress an application by creating disruptive events so that you can observe how your application responds. You can then use this information to improve the performance and resiliency of your applications so that they behave as expected. | Security best practices for AWS Fault Injection Simulator:<br>• Data protection<br>• Identity and access management<br>• Infrastructure security<br>• AWS PrivateLink |

# Conclusion

The Cloud Companion Guide for the CSA Cyber Trust mark certification aims to help organizations of all sizes implement AWS-specific services to help them achieve effective security controls. By understanding which security services and tools are available on AWS, and which controls are applicable to them, customers are able to build secure workloads and applications on AWS.

# Contributors

Contributors to this document include:

- Kimberly Chow, Security Solutions Architect, ASEAN
- Leo Da Silva, Security Solutions Architect, ASEAN

# Additional resources

For more information, refer to:

- AWS Architecture Center
- AWS Security Reference Architecture
- AWS Compliance Programs

# Document revisions

| Date | Description |
|---|---|
| **October, 2023** | Incorporated substantive edits. |
| **September, 2023** | Initial edits. |

| Date | Description |
| --- | --- |
| **October 13, 2023** | First publication |