

# Configuration Manual

MSc Research Project  
MSc Cybersecurity

Diwaker Prasad  
Student ID: 23119411

School of Computing  
National College of Ireland

Supervisor: Kamil Mahajan

**National College of Ireland**  
**MSc Project Submission Sheet**  
**School of Computing**



**Student Name:** Diwaker Prasad

**Student ID:** 23119411

**Programme:** MSc Cybersecurity

**Year:** 2023

**Module:** MSc Internship

**Lecturer:** .....

**Submission**

**Due Date:** 2<sup>nd</sup> September 2024

**Project Title:** Configuration Manual

**Word Count:** 24449 **Page Count:** 12

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** .....

**Date:** .....

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
<b>Attach a Moodle submission receipt of the online project submission,</b> to each project (including multiple copies).	<input type="checkbox"/>
<b>You must ensure that you retain a HARD COPY of the project,</b> both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# Configuration Manual

Diwaker Prasad  
23119411

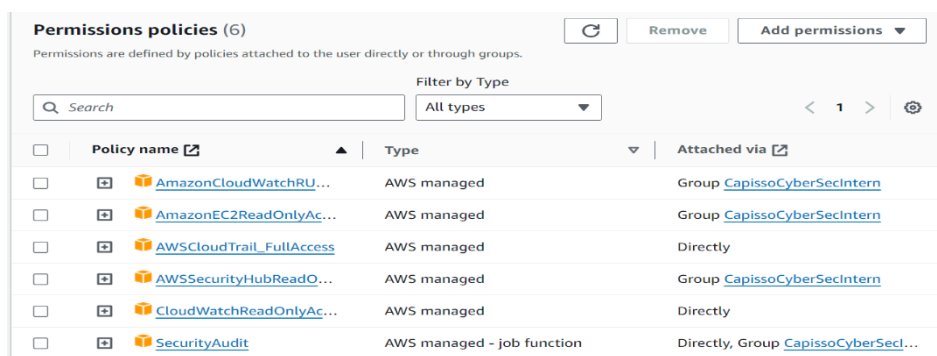
## 1. Introduction

This guide gives an organization step by step guide on how to configure AWS services in a way to meet GDPR compliance and related CIS Controls. Every category contains particular settings, illustrations, commands, and Web addresses for more information.

## 2. Prerequisites

Before starting the configuration, ensure you have:

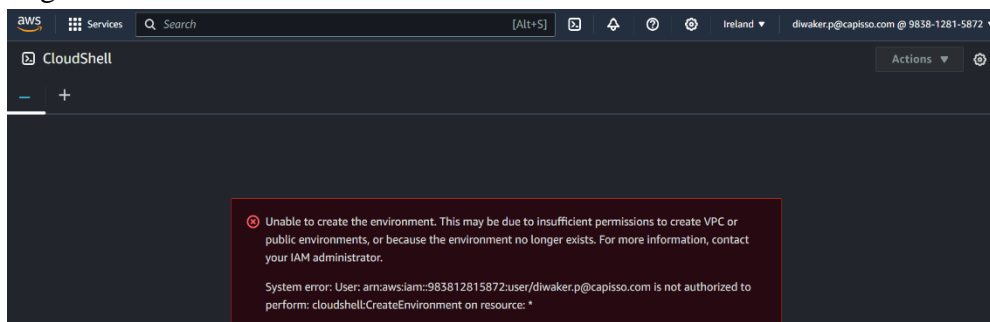
- **AWS Account:** Getting a standard user admin level access to the AWS account.
- **IAM Permissions:** Make certain that you have the necessary rights to set up IAM, S3, RDS and such.



The screenshot shows the 'Permissions policies (6)' page in the AWS IAM console. It lists several AWS managed policies attached to a user. The table has columns for Policy name, Type, and Attached via.

Policy name	Type	Attached via
AmazonCloudWatchRU...	AWS managed	Group <a href="#">CapissoCyberSecIntern</a>
AmazonEC2ReadOnlyAc...	AWS managed	Group <a href="#">CapissoCyberSecIntern</a>
AWSCloudTrail_FullAccess	AWS managed	Directly
AWSSecurityHubReadO...	AWS managed	Group <a href="#">CapissoCyberSecIntern</a>
CloudWatchReadOnlyAc...	AWS managed	Directly
SecurityAudit	AWS managed - job function	Directly, Group <a href="#">CapissoCyberSecIntern</a>

- **AWS CLI:** AWS CLI is a service from AWS used for accomplishing command-line operations, and for it to operate it has to be installed, and the configuration put in place. Otherwise, it can be installed by using Command Line Interface from Amazon and the source can be accessed through [1].



## 2. Identity and Access Management (IAM)

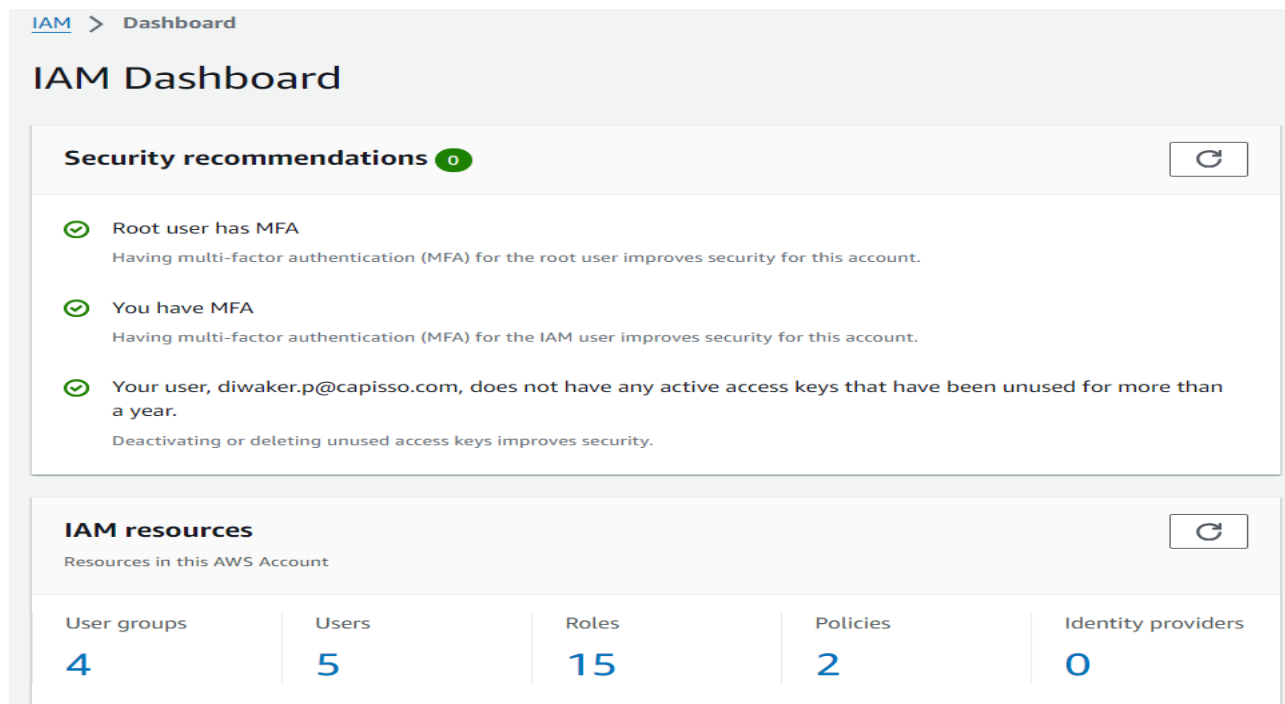
### 2.1. Enable Multi-Factor Authentication (MFA) for the Root Account

- **Objective:** Secure root account further more with an additional layer of security [1].

**Steps:**

1. Navigate to the AWS cloud and sign into the [console](#) with the help of root credential.
2. Clicking on the 'IAM' button brings you to the IAM Dashboard which is further reached by searching the AWS Console for 'IAM'.
3. On the IAM Dashboard go to Security Status and then Manage MFA.
4. It is also important to do what the screen tells you to do so as to enable the MFA. Select the preferred virtual second factor (like Google Authenticator) and tap on the QR code that the application affords.
5. The final step is to enter the authentication codes shown on your MFA device.

6. More importantly, keep the codes which were given during the setup of the application safely stored.
- **Compliance References:**
    - **GDPR Compliance:** Ensuring the security of the data personal is one of the provision of the regulation and is highlighted under Article 32 of the regulation.
    - **CIS Control:** Control 16 (Account Monitoring and Control), IG1



## 2.2. Create IAM Users and Groups with Specific Permissions

- **Objective:** Limit user rights to the barest minimum; grant roles based on the operations or assignments of an employee[2].

### Steps:

1. In IAM Dashboard navigate to Users and then click on Add User.
2. Input a username, then choose Programmatic access if the user needs an API, you also can also grant AWS Management Console access.
3. Click Next: Permissions and select what kind of permission assignment method you will take.
4. Set up the existing ones to be attached directly and the format is a selection of a number of predefined policies available.
5. Linked with traditional user management, the new specific actions are the following:
6. This will then become your actual custom policy (for advanced usage).
7. Check the settings of the user and then click on Create User to generate the user.
8. Save the login details and make sure that they are shared with the user in a secure way.

### Compliance References:

- **GDPR Compliance:** Article 25 (Data Protection by Design and by Default)

- **CIS Control: Control 4 (Controlled Use of Administrative Privileges), IG1**

**Set permissions**  
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Permissions options**

- ☒ **Add user to group**  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- ☐ **Copy permissions**  
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- ☐ **Attach policies directly**  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

**User groups (1/4)**

Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/> admin	2	AdministratorAccess	2020-11-30 (5 years ago)
<input type="checkbox"/> BillingGroup	0	Billing	2024-04-29 (3 months ago)
<input type="checkbox"/> CapisnoCyberSecIntern	1	AWSSecurityHubReadOnlyAccess, ...	2024-06-21 (1 month ago)
<input type="checkbox"/> Minimal	0	AWSElasticBeanstalkEnhancedHe...	2021-06-15 (3 years ago)

**Enforce**

## 2.3. MFA for All IAM Users

- **Objective:** Ensure all the user accounts have implement of MFA to avoid anybody gaining access to the system [3].

### Steps:

1. From the IAM Dashboard, click on Users.
2. Select a user and navigate to the Security credentials tab.
3. Under Assigned MFA device, click on Manage.
4. Select Activate MFA and follow the on-screen instructions to set up the MFA device.
5. Repeat these steps for each user account.

- **Compliance References:**

- **GDPR Compliance:** Article 32 (Security of Processing of Personal Data)
- **CIS Control:** Control 16 (Account Monitoring and Control), IG2

## 3. Logging and Monitoring

### 3.1. Enable AWS CloudTrail in All Regions

- **Objective:** With the track of API, monitor usage across all AWS services and their activities to protect and quantify the events performed [4].

### Steps:

1. Go to the [CloudTrail Console](#).
2. Go to the menu on the left and click on Trails and then Trails again and select Create trail.
3. Under Who do you want to apply this trail? Name your trail and check the 'All' selection.
4. Choose the S3 Bucket to use for the logs (if necessary create a new one).
5. Allow validation of the log file and the possibility of encrypting it with AWS KMS to secure the logs.
6. Click on the 'Create' button.

- **Compliance References:**

- **GDPR Compliance:** Article 30 (Records of Processing Activities)
- **CIS Control:** Control 6 (Maintenance, Monitoring, and Analysis of Audit Logs), IG1

**Choose trail attributes**

**General details**  
A trail created in the console is a multi-region trail. [Learn more](#)

**Trail name**  
Enter a display name for your trail.  
Logs  
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization  
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

**Storage location** [Info](#)

- ☒ **Create new S3 bucket**  
Create a bucket to store logs for the trail.
- ☐ **Use existing S3 bucket**  
Choose an existing bucket to store logs for this trail.

**Trail log bucket and folder**  
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.  
aws-cloudtrail-logs-983816816892-b6ab330f

Trails									
					Copy events to Lake		Delete	Create trail	
	Name ▲	Home region ▼	Multi-region trail ▼	Insights ▼	Organization trail ▼	S3 bucket ▼	Log file prefix ▼	CloudWatch Logs log group ▼	Status ▼
<input type="radio"/>	<a href="#">management-events</a>	Europe (Ireland)	Yes	Disabled	No	<a href="#">aws-cloudtrail-logs- [redacted]</a>	-	-	Logging

### 3.2. Set Up Amazon CloudWatch Alarms for Monitoring

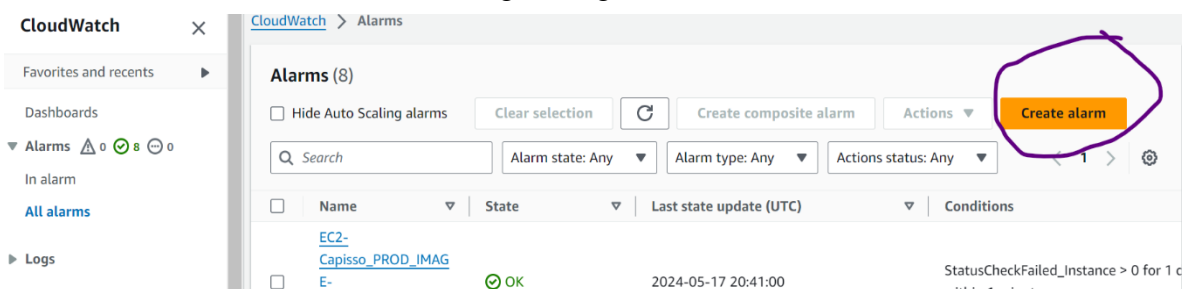
- **Objective:** Monitor AWS resources and trigger alarms based on specified metrics to respond quickly to potential issues.

#### Steps:

1. Navigate to the [CloudWatch Console](#).
2. Click on **Alarms** in the left-hand menu, then click **Create alarm**.
3. Choose a metric to monitor, such as CPU utilization, error rates, or request latency.
4. Set conditions for the alarm (e.g., trigger if CPU > 80% for 5 minutes).
5. Define the action to take when the alarm is triggered, such as sending an email notification via SNS.
6. Review the settings and click **Create Alarm**.

- **Compliance References:**

- **GDPR Compliance:** Article 32 (Security of Processing)
- **CIS Control:** Control 8 (Audit Log Management), IG2



## 4. Data Encryption

### 4.1. Enable Server-Side Encryption for S3 Buckets

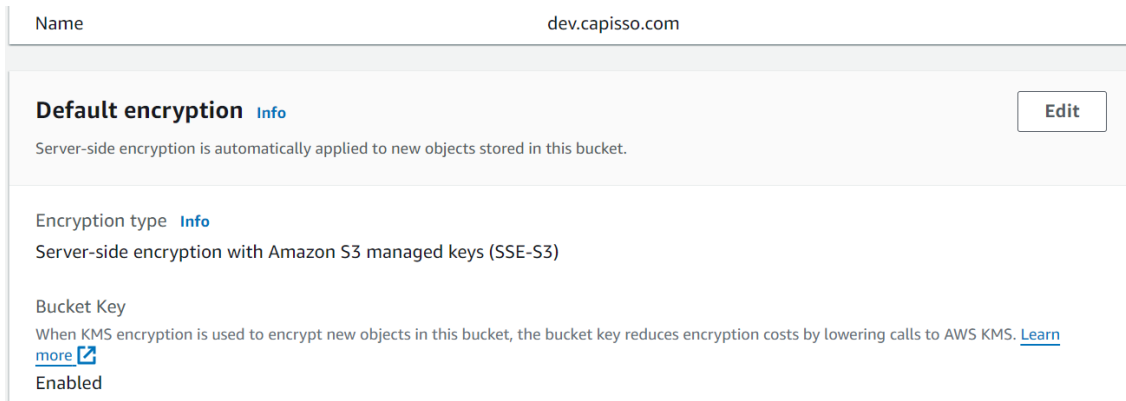
- **Objective:** Secure data at-rest through the use of AWS owned keys or through customers' keys where necessary [5].

#### Steps:

1. Go to the [S3 Console](#).
2. Go to the object list, choose the bucket you would like to encrypt and click on the Properties option.
3. Down scroll to Default encryption and click on 'Edit' section.
4. Select between AES-256 (AWS encrypted with AWS master keys) or AWS-KMS (Customer master keys).
5. If utilising the KMS namespace, choose from one of the keys available or create one using one of the methods provided.
6. If you have made changes then click on OK to apply the changes and enable encryption for the bucket.

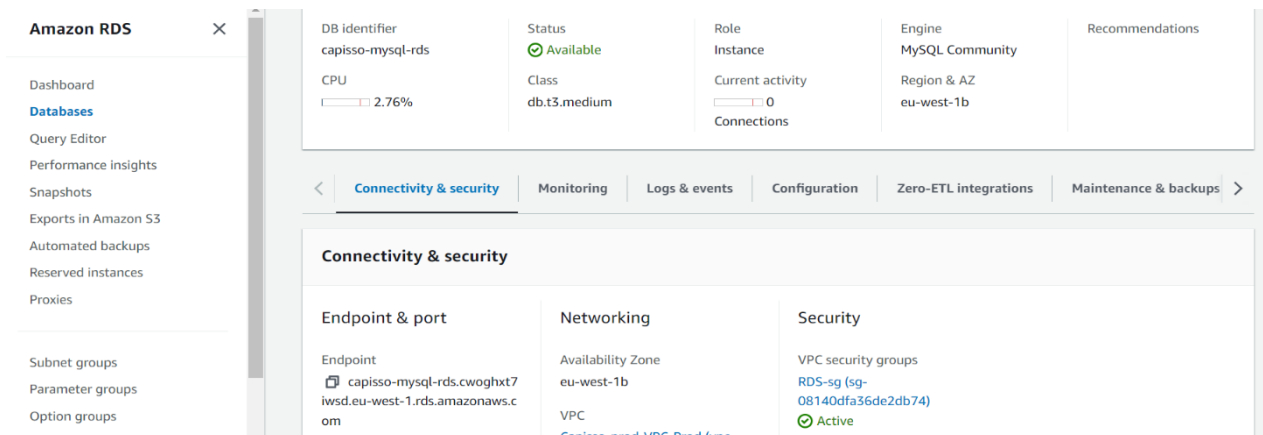
- **Compliance References:**

- **GDPR Compliance:** Article 32 (Security of Processing)
- **CIS Control:** Control 13 (Data Protection), IG1



## 4.2. Enable Encryption in Transit for RDS Databases

- **Objective:** Secure data during transmission between your application and RDS [6].
- **Steps:**
  1. Navigate to the RDS Console.
  2. Select your database instance.
  3. Under the "Connectivity & security" section, verify that "Use SSL connection" is enabled.
  4. Download the appropriate SSL/TLS certificate from the AWS Documentation.
  5. Configure your application to use this certificate for encrypted connections.
- **Compliance References:**
  - **GDPR Compliance:** Article 32 (Security of Processing)
  - **CIS Control:** Control 13 (Data Protection), IG2



## 5. Networking

### 5.1. Configure Security Groups to Restrict Access

- **Objective:** Security groups can help to regulate incoming and outgoing communications to resources in AWS [7].
- **Steps:**
  1. Navigate to the [VPC Console](#) and under services find Security Groups on the left side of the Window.
  2. Go to create new security group and as the security group name and security group description.
  3. In case of Inbound rules, one need to add rules to permit specific traffic only (e.g. permit SSH from particular IP addresses only).
  4. Under Outbound rules define allowed outbound traffic for instance, all outbound traffic to other TCP ports are prohibited apart from ports 80 and 443 for HTTPs connection.
  5. Attach the security group to your EC2 instances or other resources.
- **Compliance References:**
  - **GDPR Compliance:** Article 32 (Security of Processing)

- **CIS Control:** Control 9(Limitation and Control of Network Ports, Protocols, and Services), IG1

**Create security group** [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, you must specify a VPC.

**Basic details**

Security group name [Info](#)  
  
Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Security group name: Capisco-sg  
 Security group ID: sg-01c5472dcdade5241  
 Owner: 983812815872  
 Inbound rules count: 3 Permission entries  
 Description: Allow 80 inbound traffic  
 Outbound rules count: 1 Permission entry  
 VPC ID: vpc-02779e695

**Inbound rules (3)**

Security group rule...	IP version	Type	Protocol	Port range
sg-09db789eEb1689...	-	HTTP	TCP	80
sg-0b7c3f7c73c23fa7	-	SSH	TCP	22

**Outbound rules (1)**

Name	Security group rule...	IP version	Type	Protocol
-	sg-0a46753dd90b37c...	IPv4	All traffic	All

## 5.2. Set Up VPC Flow Logs for Network Traffic Monitoring

- **Objective:** Capture and monitor network traffic within your VPC [8].
- **Steps:**
  1. Navigate to the VPC Console.
  2. Select your VPC, then click "Create Flow Log".
  3. Choose the traffic to capture (All, Accept, or Reject).
  4. Specify the destination (CloudWatch Logs or S3).
  5. Create the flow log and monitor it through the chosen destination.
- **Compliance References:**
  - **GDPR Compliance:** Article 32 (Security of Processing)
  - **CIS Control:** Control 9 (Limitation and Control of Network Ports, Protocols, and Services), IG2

**Create VPC** [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

**VPC settings**

Resources to create [Info](#)  
 Create only the VPC resource or the VPC and other networking resources.  
☒ VPC only ☐ VPC and more

Name tag - optional [Info](#)  
 Creates a tag with a key of 'Name' and a value that you specify.

IPv4 CIDR block [Info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR  
  
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)  
☒ No IPv6 CIDR block  
☐ IPAM-allocated IPv6 CIDR block  
☐ Amazon-provided IPv6 CIDR block  
☐ IPv6 CIDR owned by me

Tenancy [Info](#)

## 6. Data Backup and Recovery

### 6.1. Automate Backups for RDS Databases

- **Objective:** Always plan for the disaster recovery and makes sure you are backing up data frequently [9].
- **Steps:**
  1. Go to the [RDS Console](#).
  2. Choose the database instance that you'd like to resize, and then click on 'Modify'.
  3. Under the **Backup** section, set the backup retention period (e.g., 7 days).
  4. Enable **Automated backups** and specify the backup window.
  5. Hit Continue then Apply immediately to make a current change.
- **Compliance References:**



- **GDPR Compliance:** Article 32 (Security of Processing)
- **CIS Control:** Control 11 (Data Recovery Capabilities), IG1

6.2. Enable S3 Bucket

## Versioning for Data Redundancy

- **Objective:** Protect against accidental deletions by keeping previous versions of objects [10].

### Steps:

1. Navigate to the S3 Console.
2. Select your bucket and click on the "Properties" tab.
3. Scroll to "Bucket Versioning" and click "Enable Versioning".
4. Confirm the changes.

- **Compliance Reference:**

- **GDPR Compliance:** Article 32 (Security of Processing)
- **CIS Control:** Control 11 (Data Recovery Capabilities), IG1, IG2

## 7. Incident Response

### 7.1. Set Up AWS Config Rules for Continuous Compliance

- **Objective:** Automatically check and enforce compliance with security policies [11].

### Steps:

1. Go to the [AWS Config Console](#).
2. Click **Rules** in the left-hand menu, then **Add Rule**.
3. Select a predefined rule (e.g., **s3-bucket-encrypted**) or create a custom rule.
4. Define the scope and parameters for the rule (e.g., check all S3 buckets for encryption).
5. Set up notifications for rule violations using SNS.
6. Click **Save** to enable the rule.

- **Compliance References:**

- **GDPR Compliance:** Article 32 (Security of Processing)

- **CIS Control:** Control 4 (Continuous Vulnerability Management), IG2

The screenshot shows the 'Set up AWS Config' wizard in the AWS Config console. The 'Settings' tab is selected, showing the following configuration options:

- Recording method:**
  - Recording strategy:**
    - ☒ **All resource types with customizable overrides:** AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.
    - ☐ **Specific resource types:** AWS Config will only record the resource types that you specify.
  - Default settings:**
    - Recording frequency:**
      - ☒ **Continuous recording:** Record configuration changes continuously whenever a change occurs.
      - ☐ **Daily recording:** Record configuration changes daily.
- Data governance:**
  - IAM role for AWS Config:**
    - ☒ **Create AWS Config service-linked role:** Choose an IAM role from one of your pre-existing roles and permission policies.
    - ☐ **Choose a role from your account:** Choose an IAM role from one of your pre-existing roles and permission policies.
- Delivery method:**
  - Amazon S3 bucket:**
    - ☒ **Create a bucket**
    - ☐ **Choose a bucket from your account**
    - ☐ **Choose a bucket from another account**

## 7.2. Enable AWS Security Hub for Centralized Security Monitoring

- **Objective:** Collect and rank security issues for all of your AWS accounts [12].  
**Steps:**
  1. Go to Security Hub Console.
  2. Go to the configure tab and click 'Get started', then enable Security Hub.
  3. Select the compliance framework for you wish to meet (for example CIS AWS Foundations).
  4. Classification and prioritization of security findings from Security Hub dashboard.
- **Compliance Reference:**
  - **GDPR Compliance:** Article 24 (Responsibility of the Controller)
  - **CIS Control:** Control 19 (Incident Response and Management), IG1

The screenshot shows the 'Enable AWS Security Hub' wizard in the AWS Security Hub console. The 'Enable AWS Config' section is highlighted, showing the following information:

- Enable AWS Config:** Before you can enable Security Hub standards and controls, you must first enable resource recording in AWS Config. You must enable resource recording for all of the accounts and in all of the Regions where you plan to enable Security Hub standards and controls. If you do not first enable resource recording, you might experience problems when you enable Security Hub standards and controls. AWS Config bills separately for resource recording. For details, see the [AWS Config pricing page](#).
- Security standards:** Enabling AWS Security Hub grants it permissions to conduct security checks. Service Linked Roles (SLRs) with the following services are used to conduct security checks: Amazon CloudWatch, Amazon SNS, AWS Config, and AWS CloudTrail.
  - ☒ Enable AWS Foundational Security Best Practices v1.0.0
  - ☐ Enable AWS Resource Tagging Standard v1.0.0
  - ☒ Enable CIS AWS Foundations Benchmark v1.2.0
  - ☐ Enable CIS AWS Foundations Benchmark v1.4.0
  - ☐ Enable CIS AWS Foundations Benchmark v3.0.0
  - ☐ Enable NIST Special Publication 800-53 Revision 5
  - ☐ Enable PCI DSS v3.2.1
- AWS Integrations:** Enabling Security Hub grants it permissions to import findings from AWS services that you have enabled. [Learn more](#)

At the bottom, there are 'Cancel' and 'Enable Security Hub' buttons.

## 8. Broader GDPR Compliance Considerations

### 8.1. Data Processing Agreements (DPAs)

- **Objective:** Ensure all data processors must have DPAs in their companies that meet the requirement of GDPR [13].  
**Steps:**
  1. Please find a list of all Third-party processors in your AWS environment under AWS Artifact View Reports.
  2. Download DPA templates from AWS Artifact to ensure they are GDPR-compliant.
  3. Look at the existing DPAs to fit the GDPR requirements and when necessary, redesign the DPAs to meet the indicated GDPR specifications for your organisation.

4. All DPAs are to be documented in AWS Artifact.

- **Compliance Reference:**
  - **GDPR Compliance:** Article 28 (Processor)
  - **CIS Control:** Control 13 (Data Protection), IG2

Security, Identity, Compliance

# AWS Artifact

## Compliance and security in the AWS Cloud

No cost, self-service portal for on-demand access to compliance reports and for entering into select online agreements.

[AWS Artifact](#) > [AWS reports](#)

### Reports Info

[AWS reports](#) | [Third-party reports](#)

③ You are opted into the new infrastructure with fine-grained access control for Artifact reports. [Learn more about fine-grained access.](#)

If you have incorrect access to Artifact reports, contact your AWS administrator to update your [account's IAM permissions](#). To allow time for updating IAM permissions, you can temporarily [opt-out of the fine-grained permissions for AWS Artifact reports](#) and opt back in by January 2, 2025.

[AWS Artifact](#) > [Agreements](#)

### Agreements Info

[Account agreements](#) | [Organization agreements](#)

③ You are signed in to a member account in an organization in [AWS Organizations](#). When accepted, the following agreements apply only to your member account. To view agreements that apply to your account through your organization, choose the **Organization agreements** tab. [Learn more](#)

#### Account agreements (5)

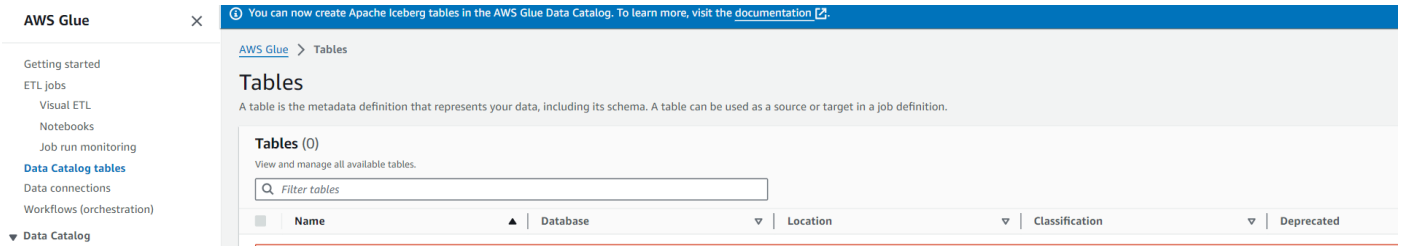
[Download agreement](#) [Terminate agreement](#) [Accept agreement](#)

< 1 > ⚙

	Title ▲	Status ▼	Effective start ▼	Description ▼
<input type="radio"/>	AWS Australian Notifiable Data Breach Addendum	Inactive	-	The AWS Australian Notifiable Data Breach Addendum (AWS ANDB Addendum) is an agreement between you and AWS regarding your use of AWS Services to process personal information of Australian individuals. It is an addendum to the AWS Customer Agreement, or other agreement between you and AWS governing your use of AWS Services under this AWS account. The terms of the AWS ANDB Addendum are confidential and subject to the terms of the AWS Artifact NDA. IMPORTANT: This AWS ANDB Addendum is specific to this AWS account, and upon acceptance will apply only to this AWS account. If you have multiple AWS accounts and intend to include personal information in any other AWS accounts, you MUST log in to AWS Artifact under each of those AWS accounts individually and accept a separate AWS ANDB Addendum before using them in connection with personal information.
<input type="radio"/>	AWS Business Associate Addendum	Inactive	-	The AWS Business Associate Addendum (AWS BAA) is an agreement between you and AWS regarding the use of AWS Services in connection with personal health information (PHI), as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Subtitle D of the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, and their implementing regulations. It is an addendum to the AWS Customer Agreement, or other agreement between you and AWS governing your use of AWS Services under this AWS account. The terms of the AWS BAA are confidential and subject to the terms of the AWS Artifact NDA. IMPORTANT: This AWS BAA is specific to this AWS account, and upon acceptance will apply only to PHI in this AWS account. If you have multiple AWS accounts and intend to

## 8.2. Data Inventory and Mapping

- **Objective:** Ensure that record is kept of all categories of personal data processed [14].  
**Steps:**
  1. Go to the AWS Glue Console and start a data catalog to document data sources.
  2. Identify where and how personal data is stored, processed, and transferred within your AWS infrastructure using AWS Glue Data Catalogs.
  3. Data could be categorized also using Amazon Macie for mapping sensitive data.
  4. Another subtle, yet important piece of advice: do not forget to update the data inventory periodically.
- **Compliance Reference:**
  - **GDPR Compliance:** Article 30 (Records of Processing Activities)
  - **CIS Control:** Control 3 (Data Protection), IG2



## References:

- [1] “Enable a virtual MFA device for the root user (console) - AWS Identity and Access Management.” Accessed: Aug. 19, 2024. [Online]. Available: <https://docs.aws.amazon.com/IAM/latest/UserGuide/enable-virt-mfa-for-root.html>
- [2] “Security best practices in IAM - AWS Identity and Access Management.” Accessed: Aug. 19, 2024. [Online]. Available: <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#bp-use-aws-defined-policies>
- [3] “IAM - Multi-Factor Authentication,” Amazon Web Services, Inc. Accessed: Aug. 19, 2024. [Online]. Available: <https://aws.amazon.com/iam/features/mfa/>
- [4] “Application logging and monitoring using AWS CloudTrail - AWS Prescriptive Guidance.” Accessed: Aug. 19, 2024. [Online]. Available: <https://docs.aws.amazon.com/prescriptive-guidance/latest/logging-monitoring-for-application-owners/cloudtrail.html>
- [5] “Protecting data with server-side encryption - Amazon Simple Storage Service.” Accessed: Aug. 19, 2024. [Online]. Available: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html>
- [6] “Encrypting Amazon RDS resources - Amazon Relational Database Service.” Accessed: Aug. 19, 2024. [Online]. Available: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>
- [7] “Control traffic to your AWS resources using security groups - Amazon Virtual Private Cloud.” Accessed: Aug. 19, 2024. [Online]. Available: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html>
- [8] “Logging IP traffic using VPC Flow Logs - Amazon Virtual Private Cloud.” Accessed: Aug. 21, 2024. [Online]. Available: <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>
- [9] “Backup and recovery using AWS Backup - AWS Prescriptive Guidance.” Accessed: Aug. 19, 2024. [Online]. Available: <https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/aws-backup.html>
- [10] “How S3 Versioning works - Amazon Simple Storage Service.” Accessed: Aug. 21, 2024. [Online]. Available: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/versioning-workflows.html>
- [11] “Incident Response in AWS Config - AWS Config.” Accessed: Aug. 19, 2024. [Online]. Available: <https://docs.aws.amazon.com/config/latest/developerguide/incident-response.html>
- [12] “Enabling Security Hub - AWS Security Hub.” Accessed: Aug. 21, 2024. [Online]. Available: <https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-settingup.html>
- [13] “AWS Data Processing Addendum (DPA) - Navigating GDPR Compliance on AWS.” Accessed: Aug. 21, 2024. [Online]. Available: <https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html>

[14] “Data discovery and cataloging in AWS Glue - AWS Glue.” Accessed: Aug. 21, 2024. [Online]. Available: <https://docs.aws.amazon.com/glue/latest/dg/catalog-and-crawler.html>