EXPLORE | DIGITAL SKILLS

AWS Cloud Security

Train Overview

In this train we will cover the following:

1. AWS Shared Responsibility Model
2. Identity and Access Management
3. Securing a new AWS account
4. Securing multiple accounts
5. Securing data on AWS
6. Working to ensure compliance

EXPLORE | DIGITAL SKILLS

AWS Shared Responsibility Model

Identity and Access Management

Securing a new AWS account

Securing multiple accounts

Securing data on AWS

Working to ensure compliance

Conclusion

EXPLORE | DIGITAL SKILLS

AWS Shared Responsibility Model

Cloud security is a shared responsibility between AWS and its customers. Both parties have vested interests to make sure that all the components of the cloud solution are secured.

VS

Responsible for Security OF the cloud.

- AWS is responsible for the physical implementation of the cloud. This includes physical facilities and systems.
- AWS provides you with the tools to protect your applications and data.
- AWS manages the software virtualisation layer, the hardware, and global infrastructure components.
- AWS is responsible for protecting the infrastructure including the hardware, software, networking, and facilities that run the AWS cloud services.

Responsible for Security IN the cloud.

- Customers are responsible for all applications and data sets employed in the cloud.
- It is the customers' responsibility to use the AWS tools available to ensure that data is secure.
- The customer is responsible for the encryption of data at rest and in transit.
- The customer should ensure that the network is securely configured. Security credentials and logins should be managed safely.
- The customer should manage firewall configurations and the security of the operating systems and applications executing on any computer instances they launch.

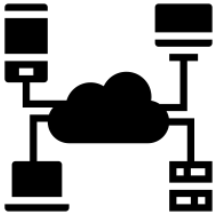
Categorising Cloud Services

Cloud services generally have three types of services: **Infrastructure**, **Platform,** and **Software**. Each of the service offerings are designed to give **specialised service for production requirements.**

Infrastructure as a service (IaaS)

With this service, the customer has more flexibility over configuring networking and storage settings and as a result, the customer will be responsible for securing these aspects.

Platform as a service (PaaS)



With this service, the customer does not need to manage the underlying infrastructure. The operating system, database patching, firewall configuration, and disaster recovery are managed for you.

Software as a service (SaaS)

Refers to services that provide a complete software solution. The software is centrally hosted and as the customer, you do not need to manage any of the infrastructure that supports the service.

EXPLORE DIGITAL SKILLS

AWS Shared Responsibility Model

Identity and Access Management

Securing a new AWS account

Securing multiple accounts

Securing data on AWS

Working to ensure compliance

Conclusion

EXPLORE | DIGITAL SKILLS

Identity and Access Management

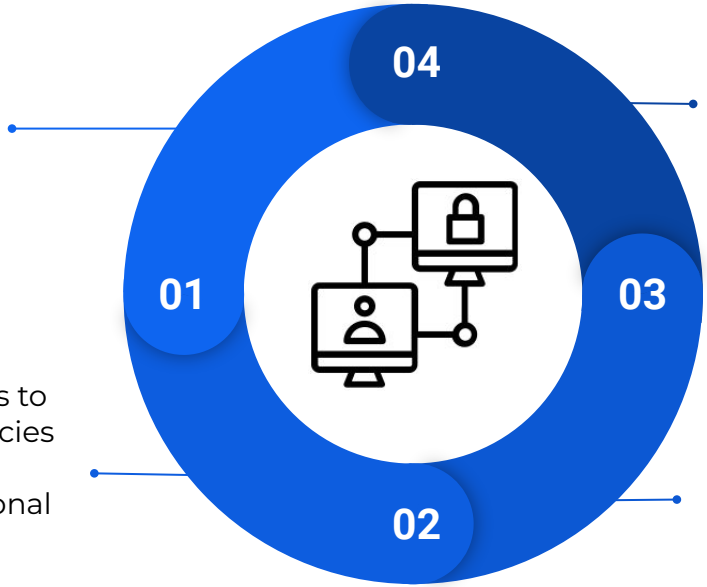
IAM is a no-cost AWS feature that allows you to control and manage access to AWS resources by defining roles, groups, and users. This means you have control over users and what they can access.

Global Service

IAM is a global service - meaning that IAM resources are available to all regions of the AWS cloud.

Access Control

IAM allows you to control access to all your AWS services using policies and assigning them to specific users in order to define operational groups.



Granular control

IAM provides granular control over access to resources so you can centrally manage access to launching, configuring, managing, and terminating resources in your AWS account.

Authentication

IAM handles authentication and verification of access for a user, role, or to a specific resource.

EXPLORE DIGITAL SKILLS

Essential Components of IAM

The IAM service allows you to define **users, groups, policies,** and **roles**. All these components allow you to fine-tune your cloud security requirements.

IAM User

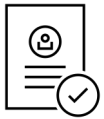
An IAM user is a person or application that has access to your AWS account

---

IAM Group

This a collection of **IAM users** who have the same access permissions. If specific cloud access roles and responsibilities are defined within a company, we can create associated IAM groups and attach policies to the group instead of attaching policies to users individually.

IAM Policy



This is a document that defines access to specific resources. These are created independently from users or groups and can be attached to a resource to control access and usage of the resource.

IAM Role

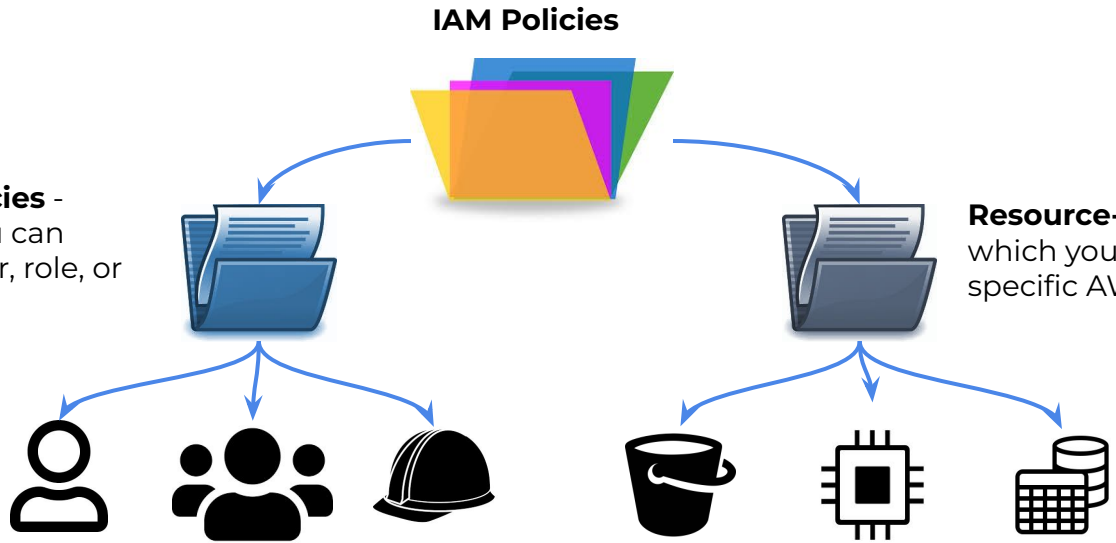
Roles are used for granting temporary access to AWS services. A role can be given to a user when they want to perform tasks outside the capabilities of their current IAM user or group access.

EXPLORE DIGITAL SKILLS

IAM Policies

This is a document that defines access to specific resources, it also defines the level of access for each specific resource. These are created independently from users or groups and can be attached to a resource to control access and usage of the resource.

The **IAM policies** are written in a **JSON (JavaScript Object Notation)** format, which lists the permissions that allow or deny access to services in AWS. IAM policies can be broken down into two subcategories.



Identity-based policies - permissions that you can attach to an IAM user, role, or group.

Resource-based policies - which you can attach to specific AWS resources.

IAM Policy Example

This is a document that defines access to specific resources, it also defines the level of access for each specific resource. These are created independently from users or groups and can be attached to a resource to control access and usage of the resource.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "NotResource": "arn:aws:s3:::bucket-name/*"
        }
    ]
}
```

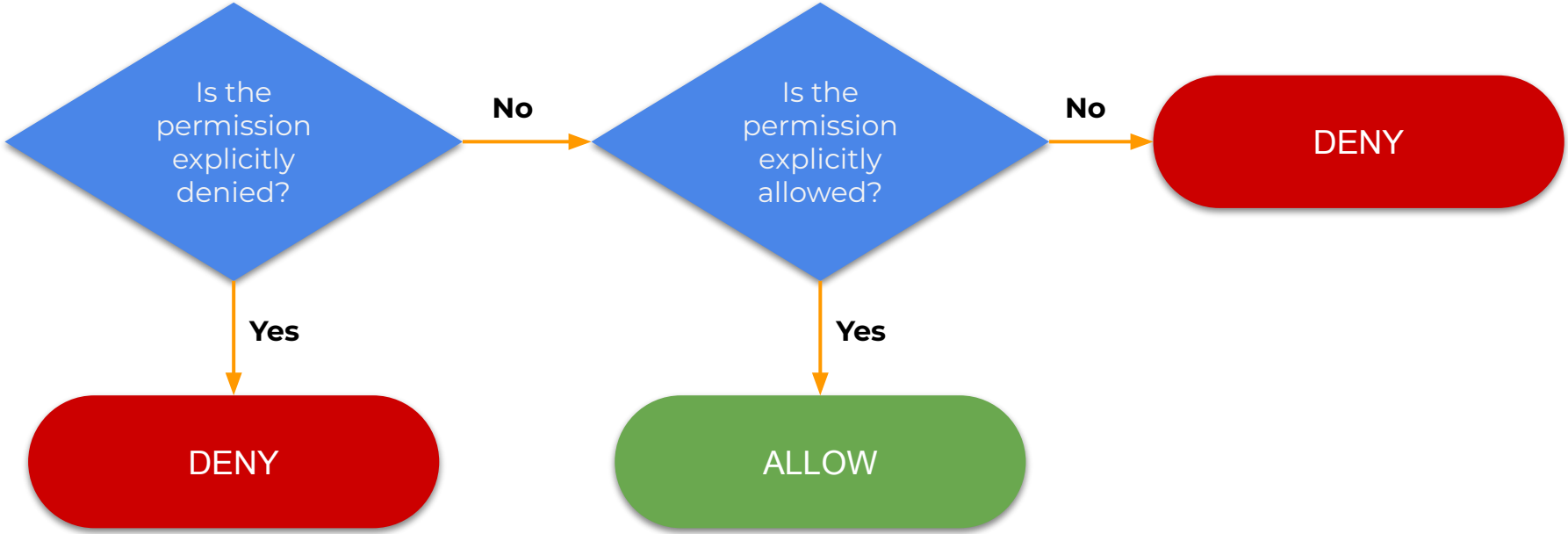
Explicit allow gives users access to the S3 bucket.

Explicit deny ensures that users cannot access any other resources except the listed bucket.

Deny Statements take precedence over **Allow Statements.** If there are any conflicting permissions, the **Deny Statement** will always take preference.

IAM Permissions

When **IAM** determines whether a permission is allowed, it first checks for all explicit **denial policies** before moving on to the explicit **allow policies.**



Authentication for IAM user

With any application, authentication is required to make sure that you are who you claim to be. This is not different with cloud security. We need authentication to give an IAM user access to AWS services.

Programmatic access

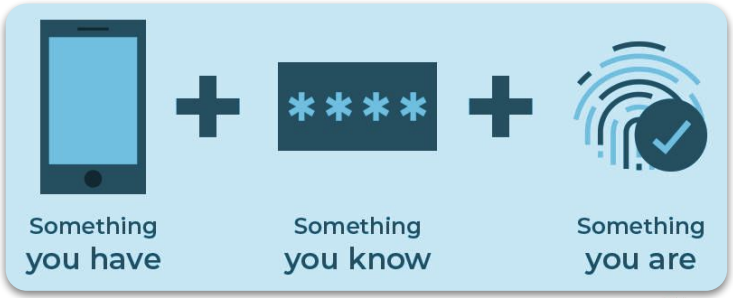
Key Pairs: Users of an EC2 will be required to present a key pair that consists of an **access key ID** and a **secret access key** when making AWS API calls by using the AWS CLI or AWS SDK.

Access Key: These keys give you full access to AWS, and in turn you can create key-pairs for users to access EC2 instances.

AWS Management Console access

At the minimum, you will be required to produce a **username and password**.

You can also add **Multi-Factor Authentication (MFA)** to the authentication process. This provides increased security, if your username and password combination were to be compromised they will still need to provide the **MFA key** to access your account.



EXPLORE DIGITAL SKILLS

Authorisation

Authorisation is the process of determining what permissions a user or service should be granted. By default IAM users do not have permission to access anything. You are required to **explicitly grant permissions** by creating a policy and attaching it to the user

Principle of least privilege (PoLP)

It is the principle of applying the **minimal set of permissions needed to accomplish a specific task**. Determine what users need to be able to do, and then create policies so that they can perform their duties.

In the AWS cloud, most resources are sealed shut when they are created, and you provide access to them using a policy attached to a user, a group, or a role.

AWS Shared Responsibility Model

Identity and Access Management

Securing a new AWS account

Securing multiple accounts

Securing data on AWS

Working to ensure compliance

Conclusion

EXPLORE DIGITAL SKILLS

Securing a new AWS account

It is not recommended to use the **AWS root account** except when absolutely necessary. This account has full access to all resources and privileges cannot be controlled.

AWS recommends that you make use of IAM services to create users and assign policies to these users by following the principle of least privilege.

To stop using the account root user:

1. While you are logged in as the account root user, **create an IAM user** for yourself. Save the access keys if needed.
2. **Create an IAM group**, give it full administrator permissions, and add the IAM user to the group.
3. **Disable and remove your account root user access keys**, if they exist
4. **Enable a password policy** for users.
5. Sign in with your new IAM user credentials.
6. Store your account root user credentials in a secure place.

Securing a new AWS account: MFA

A username together with a strong password provides good security, but we can add another layer by enabling Multi-Factor Authentication (MFA) for your root user as well as your IAM users.

There are 3 options available for retrieving the MFA token:

- Virtual MFA-compliant applications:
  - Google Authenticator
  - Authy Authenticator

- U2F security key devices:
  - YubiKey

- Hardware MFA Options:
  - Gemalto

gemalto
security to be free

EXPLORE | DIGITAL SKILLS

Securing a new AWS account: AWS CloudTrail

AWS Cloud Trail is a service that logs all API requests to resources in your account. Meaning you can enable operational auditing on your account.

AWS CloudTrail allows you to track all your API interactions.

The **CloudTrail** logs can be used for security and forensic investigations. The logs are also useful for documenting compliance when needed.

AWS CloudTrail is enabled on account creation by default, and it keeps a record of the last 90 days of account management event activity.

AWS Shared Responsibility Model

Identity and Access Management

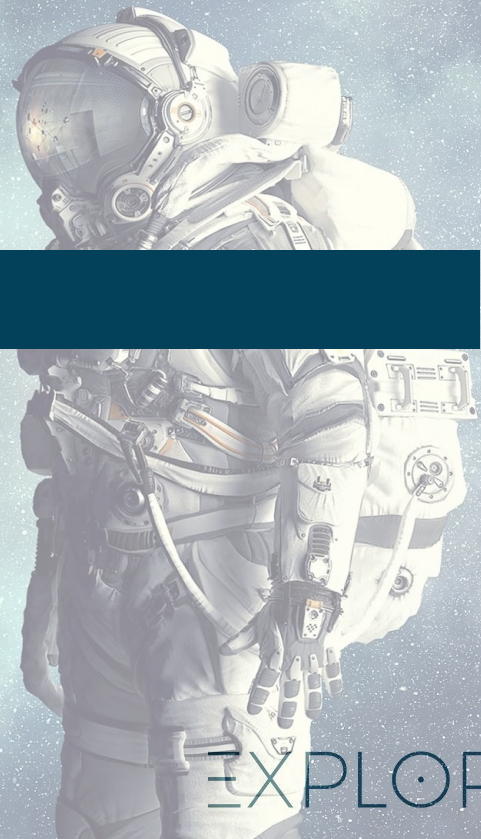
Securing a new AWS account

Securing multiple accounts

Securing data on AWS

Working to ensure compliance

Conclusion



EXPLORE DIGITAL SKILLS

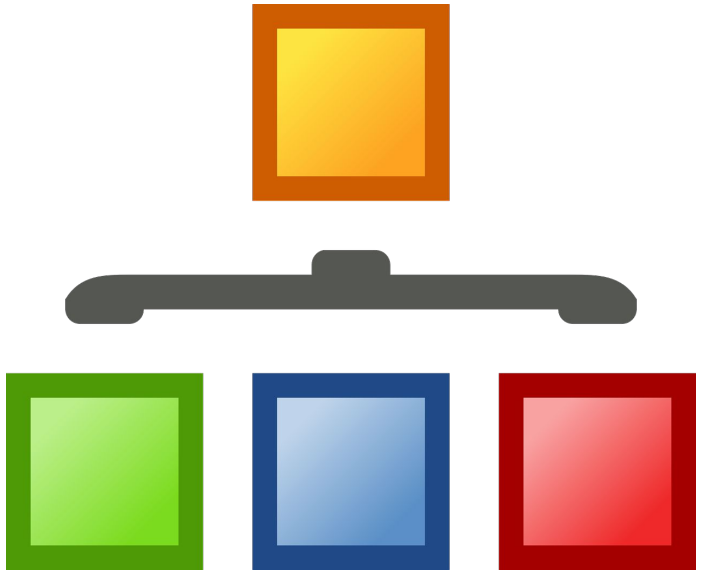
Securing Multiple Accounts

AWS Organisations is an accounts management service that enables you to consolidate multiple AWS accounts into an organisation that you create and centrally manage.

You can group multiple accounts into **Organisational Units (OUs)** and attach different access policies to each **OU**.

Policies in **AWS Organisations** are called **Service Control Policies**. These allow you to apply permissions to multiple AWS accounts at the same time. This enables you to have separate accounts for different departments in your organisation.

Permissions given to a user are the **intersection** of what is allowed by **AWS Organisation** and what is granted by **IAM** in that account.



EXPLORE DIGITAL SKILLS

Service Control Policies

Service Control Policies (SCPs) offer central control over the maximum available permissions for all accounts in your organisation.

Service control Policies are available only in an organisation that has all features enabled, including consolidated billing.

Service Control Policies are similar to IAM permission policies. However, they never grant permissions, instead, they specify the maximum permissions for an organisation

Attaching a **Service Control Policy** to an **Organisational Unit** defines a safeguard for the actions that accounts in that **OU** can actually do.

SCPs should not be used as a substitute for IAM configurations within each account.

EXPLORE | DIGITAL SKILLS

AWS Key Management Service

AWS Key Management Service (AWS KMS) enables you to create and manage encryption keys and to control the use of encryption across AWS services.

AWS KMS integrates with **AWS CloudTrail** to log all key usage to ensure you meet your regulation and compliance requirements.

Uses hardware security modules to protect your keys.

Customer master keys are used to control access to other keys that **encrypt and decrypt your data**. You can create new master keys as you wish and manage who has access to them and which services they can be used with.

You can also import keys from your own key management infrastructure into **AWS KMS**.

You can use **AWS KMS master keys** to control the encryption of data stored in most AWS services.

Amazon Cognito

Amazon Cognito provides solutions to control access to AWS resources from your application.

Amazon Cognito uses the **Security Assertion Markup Language (SAML)**, version 2.0

SAML is an open standard for exchanging identity security information with applications and identity service providers.

Applications and identity service providers that support **SAML** enable you to sign in using your corporate directory credential, such as your username and password from Microsoft Active Directory.

You can use single sign-on to access all your SAML-enabled applications by using a single set of credentials

Amazon Shield

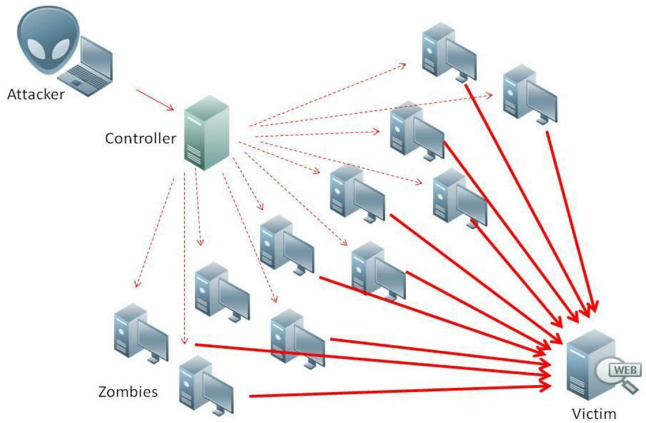
AWS Shield is a managed **Distributed Denial of Service (DDoS)** attack protection service for applications that run on your AWS account.

It provides protection and automatic mitigations that minimise application downtime and latency.

AWS Shield Standard is automatically enabled for you at no additional cost, so you do not need to contact AWS support to benefit from DDoS protection.

AWS Shield protects your websites from all types of DDoS attacks:

- Infrastructure layer attacks - UDP floods
- State exhaustion attacks - TCP SYN floods
- Application-Layer attacks - HTTP GET or POST floods



AWS Shield Advanced

This is a paid version that provides additional detection and mitigation against sophisticated DDoS attacks and near real-time visibility into attacks. It also gives you full access to the AWS DDoS Response Team (DRT).

AWS Shared Responsibility Model

Identity and Access Management

Securing a new AWS account

Securing multiple accounts

Securing data on AWS

Working to ensure compliance

Conclusion

EXPLORE DIGITAL SKILLS

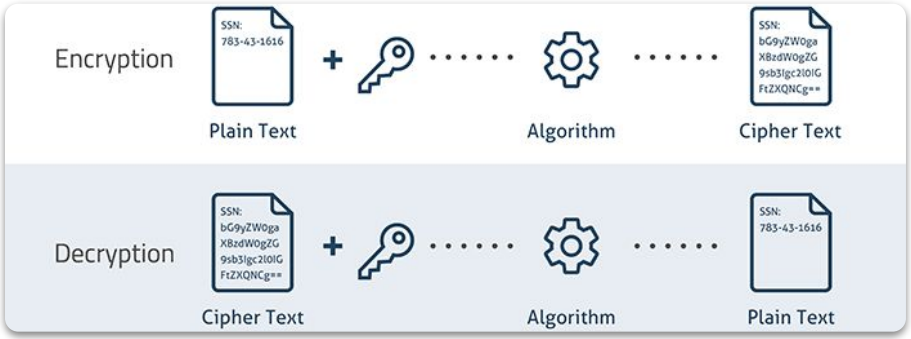
Securing Data on AWS

Data encryption plays a key role when protecting your data at rest and in transit. Data encryption is used when we want to keep data private and confidential.

Encryption takes data and encodes it such that it is an unreadable format. It can only be decrypted by a secret key that was used to encode it. So even if an attacker gains access to your data, they'll be unable to make sense of the contents.

Data at rest refers to data that is physically stored on a disk. You can create encrypted file systems on AWS so that all your data is encrypted at rest.

When using **AWS KMS, encryption** and **decryption** are handled automatically so that you do not need to modify your applications.



EXPLORE DIGITAL SKILLS

Securing Data on AWS

Data encryption plays a key role when protecting your data at rest and in transit. Data encryption is used when we want to keep data private and confidential.

Data in transit refers to data that is moving across a network. Encryption of moving data is accomplished by using **Transport Layer Security (TLS)**.

TLS certificates are used to secure network communications and establish the identity of websites over the internet. You can also establish the identity of resources on private networks.

AWS Certificate Manager is a service that enables you to provision and manage the deployment of **TLS certificates** for use with your AWS services. AWS Certificate Manager also handles certificate renewals.

Traffic that runs over HTTPS is encrypted using TLS and is protected from eavesdropping because of the bi-directional encryption of the communication.

AWS Shared Responsibility Model

Identity and Access Management

Securing a new AWS account

Securing multiple accounts

Securing data on AWS

Working to ensure compliance

Conclusion

EXPLORE DIGITAL SKILLS

Working to ensure compliance

AWS continuously interacts with certifying bodies and independent auditors to provide customers with detailed information about the policies, processes, and controls that are established and operated by AWS.

Certifications and attestations

Certifications and attestations are assessed by a third-party, independent auditor.

Examples:

- ISO 27001, 27017, 27018
- ISO/IEC 9000

Laws, regulations, and privacy

AWS provides security features and legal agreements to support compliance.

Examples:

- EU General Data Protection Regulation (GDPR).
- Health Insurance Portability and Accountability Act (HIPAA)

Alignments and frameworks

AWS aligns on industry or function-specific security or compliance requirements.

Examples:

- Center for Internet Security
- EU-US Privacy Shield certified.

Working to ensure compliance: AWS Config

AWS Config is a service you can use to assess, audit, and evaluate the configurations of your AWS resources.

AWS Config maintains a history of your AWS configurations and allows you to define the parameters of who can make changes to your configuration. This is achieved by continuously monitoring your AWS resource configurations.

You can automate the evaluation of recorded configurations against a set of rules.

You can review changes in your configurations and relationships between AWS resources and **determine your overall compliance** against the appropriate guidelines. This simplifies compliance, auditing, and security analysis.

AWS Config is a **regional resource**, to activate it you need to enable it in all regions where you want it to be active.

Working to ensure compliance: AWS Artifact

AWS Artifacts centralises all AWS security and compliance documents and makes them available for download.

Through this facility you can easily submit your security and compliance documents to your auditors to demonstrate **compliance** of your **AWS Infrastructure and services.**

The documents can also be used as guidelines to ensure that you build a compliant AWS cloud environment and assess the efficacy of your company's internal controls.

You can use **AWS Artifact** to electronically review and sign agreements. It also enables you to assign AWS accounts that can legally process restricted information.

AWS Artifact only contains information relating to **AWS infrastructure and services**. It is the customers responsibility to produce compliance documents about application running of the AWS cloud services.

AWS Shared Responsibility Model

Identity and Access Management

Securing a new AWS account

Securing multiple accounts

Securing data on AWS

Working to ensure compliance

Conclusion

EXPLORE | DIGITAL SKILLS

Conclusion

What we've learnt

- Introduced to key concepts that are involved when dealing with security in general.
- AWS ensures access to multiple tools that secure the data and applications we deploy to the cloud.
- Understand that keeping our cloud environment secure is a joint effort between the service provider and the customer.
- Our responsibility to observe best practices and make sure we're compliant with security standards.