Implementing security controls on AWS

AWS Prescriptive Guidance

AWS Prescriptive Guidance: Implementing security controls on AWS

Table of Contents

Implementing security controls on AWS

Iqbal Umair, Gurpreet Kaur Cheema, Wasim Hossain, Joseph Nguyen, San Brar, and Lucia Vanta, Amazon Web Services (AWS)

December 2023 (document history)

Security is critical to every company, and it is a key pillar in the AWS Well-Architected Framework. However, many do not know how to work through security considerations and create a holistic automated security testing and remediation strategy for their cloud environments. By using AWS services and tools, such as AWS Config, Amazon GuardDuty, and AWS CloudFormation, you can create a security testing strategy and build it into your AWS Cloud environments.

To help meet your company's security policy and standards, *security controls* are the technical or administrative guardrails that help prevent, detect, or reduce the ability of a threat actor to exploit a security vulnerability. They are designed to protect the confidentiality, integrity, and availability of resources and data. The following are examples of security controls:

- Implementing multi-factor authentication for users that need to sign in to an application
- Logging, monitoring, and querying actions for the purposes of performing real-time audits of account activity
- Making sure that sensitive data is encrypted
- Making sure logs are stored according to your company's retention policy

There are four types of security controls: preventative, proactive, detective, and responsive. This guide describes each type in more detail and focuses on how to implement and automate these controls in the AWS Cloud. This guide helps you implement security controls that are continuous and proactive.

Intended audience

This guide is intended for architects and security engineers who are responsible for implementing security controls in the AWS Cloud. If your company has not defined a security policy, control objectives, or standards, as described in Security controls in the governance framework, we recommend that you complete these governance tasks before proceeding with this guide.

Targeted business outcomes

Companies use security controls to mitigate or act as countermeasures against risks to its IT systems. Controls define the baseline of requirements to satisfy the main security objectives of an IT program and its security strategy. Having controls in place improves a company's security posture by protecting the confidentiality, integrity, and availability of its data and IT assets. Without controls, it would be difficult to know where you need to focus and invest to establish a security baseline.

Security controls can be used to address a variety of scenarios. Examples include meeting requirements that stem from risk assessments, achieving industry standards, or complying with regulations. Satisfying security controls demonstrates that you have measured the risk to a system, determined the level of protection needed, and proactively implemented solutions. Additional factors, such as business, industry, and geography, can all dictate the security controls that you need.

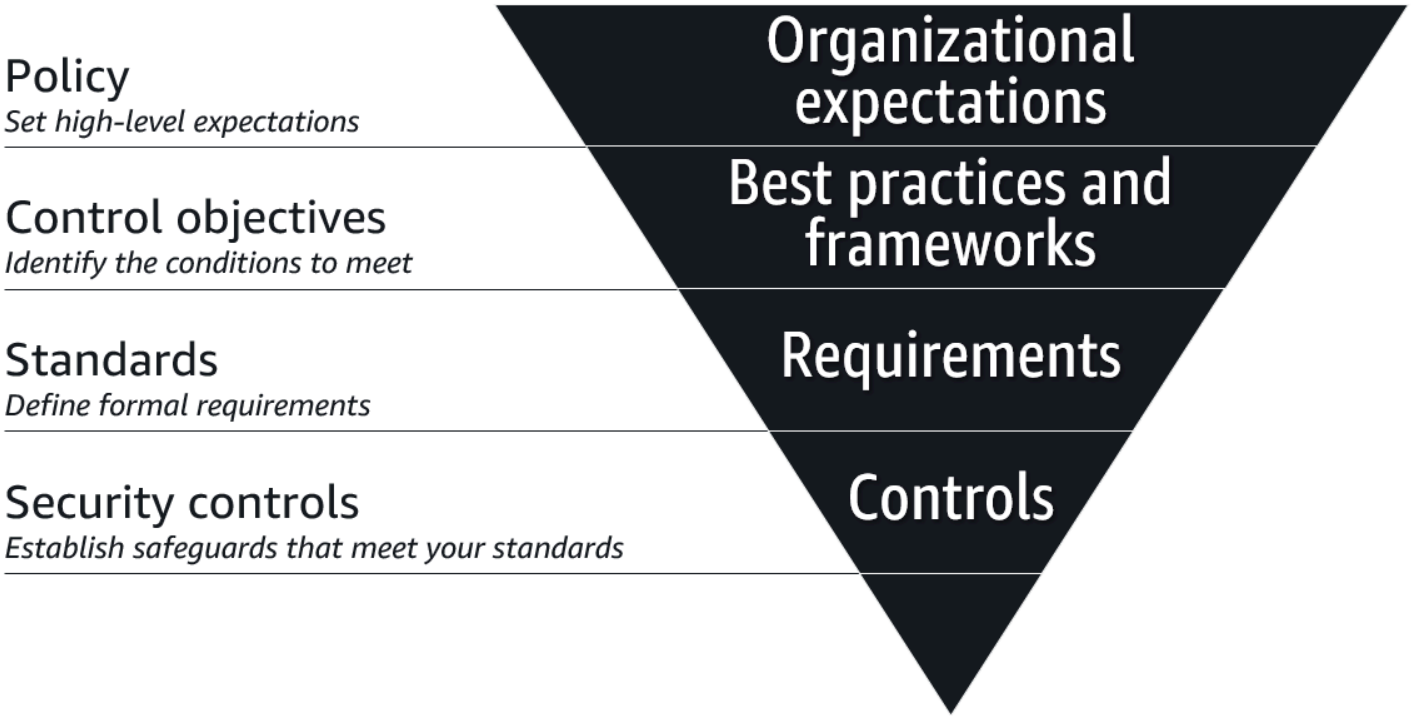
The following are common use cases for implementing security controls:

- A security assessment of an application has identified the need for access controls based on the sensitivity of data that is being processed.
- You must comply with security standards, such as Payment Card Industry Data Security Standard (PCI DSS), HIPAA (Health Insurance Portability and Accountability Act), or National Institute of Standards and Technology (NIST).
- You need to protect sensitive information for business transactions.
- Your company has expanded into a geographical region that requires security controls, such as a region that requires compliance with General Data Protection Regulation (GDPR).

After reading this guide, you should be familiar with the four types of security controls, understand how they are part of your security governance framework, and be prepared to start implementing and automating security controls in the AWS Cloud.

Security controls in the governance framework

It is important to plan from a foundational level. How does one start? The following figure shows how you can build a security governance strategy based on a policy, control objectives, standards, and security controls.



The following are the hierarchical components of a governance strategy for security:

- **Policy** – A *policy* is the foundation of any cybersecurity governance strategy. It is a document that states the expectations of the company, such as statutory, regulatory, or contractual obligations that it must meet. Policies can vary by industry and region.
- **Control objectives** – *Control objectives* are targets, such as industry-recognized best practices, that help you meet the intent of a policy. For cloud computing, many companies adopt the Cloud Controls Matrix (CCM) (Cloud Security Alliance website), which is a framework of cybersecurity control objectives.
- **Standards** – *Standards* are formally established requirements that satisfy a control objective. Standards might include processes, actions, or configurations, and they are quantifiable so that you can measure performance against the standard.
- **Security controls** – *Security controls* are the technical or administrative mechanisms you put in place to implement the standards. All security controls map to standards, but not all standards

map to security controls. Testing of security controls is designed to monitor and measure whether you are effectively meeting the defined standards.

This guide focuses on how to design and implement common types of security controls in the AWS Cloud.

Types of security controls

There are four main types of security controls:

- Preventative controls – These controls are designed to prevent an event from occurring.
- Proactive controls – These controls are designed to prevent the creation of noncompliant resources.
- Detective controls – These controls are designed to detect, log, and alert after an event has occurred.
- Responsive controls – These controls are designed to drive remediation of adverse events or deviations from your security baseline.

An effective security strategy includes all four types of security controls. While preventative controls are a first line of defense to help prevent unauthorized access or unwanted changes to your network, it is important to make sure that you establish detective and responsive controls so that you know when an event occurs and can take immediate and appropriate action to remediate it. Using proactive controls add another layer of security because it complements preventative controls, which are generally stricter in nature.

The following sections describe each type of control in more detail. They discuss the objectives, implementation process, use cases, technological considerations, and target outcomes of each control type.

Preventative controls

Preventative controls are security controls that are designed to prevent an event from occurring. These guardrails are a first line of defense to help prevent unauthorized access or unwanted changes to your network. An example of a preventative control is an AWS Identity and Access Management (IAM) role that has read-only access because it helps prevent unintended write actions from unauthorized users.

Review the following about this type of control:

- Objectives
- Process
- Use cases

- Technology
- Business outcomes

Objectives

The primary purpose of preventative controls is to minimize or avoid the likelihood of a threat event from occurring. The control should help prevent unauthorized access to the system and help prevent unintentional changes from affecting the system. The following are the objectives of preventative controls:

- **Segregation of duties** – Preventative controls can establish logical boundaries that limit privileges, allowing permissions to perform only specific tasks in designated accounts or environments. Examples include:
  - Segmenting workloads to different accounts for specific services
  - Separating and accounts into isolated production, development, and test environments
  - Delegating access and responsibilities to multiple entities to perform specific functions, such as using IAM roles or assumed roles to allow only specific job functions to perform certain actions
- **Access control** – Preventative controls can consistently grant or deny access to resources and data in the environment. Examples include:
  - Preventing users from exceeding their intended permissions, known as *privilege escalation*
  - Restricting access to applications and data to only authorized users and services
  - Keeping the administrator group small
  - Avoiding use of the root user credentials
- **Enforcement** – Preventative controls can help your company adhere to its policies, guidelines, and standards. Examples include:
  - Locking configurations that serve as the minimum security baseline
  - Implementing additional security measures, such as multi-factor authentication
  - Avoiding nonstandard tasks and actions that are performed by unapproved roles

Process

Preventative control mapping is the process of mapping controls to requirements and using policies to implement those controls by restricting, disabling, or blocking. When mapping controls, consider

the proactive effect they have on the environment, resources, and users. The following are best practices for mapping controls:

- Strict controls that disallow an activity should be mapped to production environments where the action requires review, approval, and change processes.
- Development or contained environments might have fewer preventative controls in order to provide the agility to build and test.
- The classification of data, risk level of an asset, and risk management policy dictate the preventative controls.
- Map to existing frameworks as evidence of compliance with standards and regulations.
- Implement preventative controls by geographical location, environment, accounts, networks, users, roles, or resources.

Use cases

Data handling

A role is created that can access all data in an account. If there is sensitive and encrypted data, overly permissive privileges might present a risk, depending on the users or groups that can assume the role. By using a key policy in AWS Key Management Service (AWS KMS), you can control who has access to the key and can decrypt the data.

Privilege escalation

If administrative and write permissions are assigned too broadly, a user can circumvent the limits of their intended permissions and grant themselves additional privileges. The user who creates and manages a role can assign a *permissions boundary*, which defines the maximum allowable privileges for the role.

Workload lockdown

If your business does not have a foreseeable need to use specific services, enable a *service control policy* that limits which services can operate in an organization's member accounts or restricts services based on the AWS Region. This preventative control can reduce the scope of impact if a threat actor manages to compromise and access an account in your organization. For more information, see Service control policies in this guide.

Impact to other applications

Preventative controls can enforce the use of services and features, such as IAM, encryption, and logging, in order to meet the security requirements of your applications. You can also use these controls to help protect against vulnerabilities by limiting the actions that a threat actor can exploit due to unintentional errors or misconfiguration.

Technology

Service control policies

In AWS Organizations, service control policies (SCPs) define the maximum available permissions for member accounts in an organization. These policies help accounts stay within access control guidelines of the organization. Note the following when designing SCPs for your organization:

- SCPs are preventative controls because they define and enforce the maximum allowable permissions for IAM roles and users in the organization's member accounts.
- SCPs affect only the IAM roles and users in the member accounts of the organization. It does not affect users and roles in the management account of the organization.

You can make an SCP more granular by defining the maximum permissions for each AWS Region.

IAM permissions boundaries

In AWS Identity and Access Management (IAM), a permissions boundary is used to set the maximum permissions that an identity-based policy can grant to an IAM entity (users or roles). An entity's permission boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permission boundaries. Note the following when using permissions boundaries:

- You can use an AWS managed policy or a customer managed policy to set the boundary for an IAM entity.
- A permissions boundary does not grant permissions on its own. The permissions boundary policy limits the permissions that are granted to the IAM entity.

Business outcomes

Time savings

- By adding automation after you set up preventative controls, you can reduce the need for manual intervention and reduce the frequency of errors.
- Using permission boundaries as a preventative control helps security and IAM teams focus on critical tasks, such as governance and support.

Regulatory compliance

- Companies might need to comply with internal or industry regulations. These might be regional restrictions, user and role restrictions, or service restrictions. SCPs can help you stay compliant and avoid violation penalties.

Risk reduction

- With growth, the number of requests to create and manage new roles and policies increases. It becomes more challenging to understand the context of what is required to manually create the permissions for each application. Establishing preventative controls acts as a baseline and helps prevent users from performing unintended actions, even if they were accidentally given access.
- Applying preventative controls to access policies provides an additional layer to help protect data and assets.

Proactive controls

Proactive controls are security controls that are designed to prevent the creation of noncompliant resources. These controls can reduce the number of security events handled by responsive and detective controls. These controls make sure that deployed resources are compliant before they are deployed; therefore, there is no detection event that requires response or remediation.

For example, you might have a detective control in place that notifies you if an Amazon Simple Storage Service (Amazon S3) bucket becomes publicly accessible. You might also have a responsive control that remediates it. Although you already have these two controls in place, you can add another layer of protection by adding a proactive control. Through AWS CloudFormation, the proactive control can prevent the creation of update of any S3 bucket that has public access

enabled. Threat actors could still bypass this control and deploy or modify resources outside of CloudFormation. In this case, the detective and responsive controls would remediate the security event.

Review the following about this type of control:

- Objectives
- Process
- Use cases
- Technology
- Business outcomes

Objectives

- Proactive controls help you improve security operations and quality processes.
- Proactive controls can help you adhere to security policies, standards, and regulatory or compliance obligations.
- Proactive controls can prevent the creation of noncompliant resources.
- Proactive controls can reduce the number of security findings.
- Proactive controls provide another layer of protection against threat actors who bypass preventative controls and attempt to deploy noncompliant resources.
- In combination with preventative, detective, and responsive controls, proactive controls can help you address potential security incidents.

Process

Proactive controls complement preventative controls. Proactive controls reduce your organization's security risk and enforce the deployment of compliant resources. These controls evaluate resource compliance before the resource is created or updated. Proactive controls are generally implemented by using CloudFormation hooks. If the resource fails the proactive control validation, you can choose to either fail the resource deployment or present a warning message. The following are some tips and best practices for building proactive controls:

- Make sure that proactive controls are mapped to your organization’s compliance requirements.
- Make sure that proactive controls follow security best practices for the associated service.

- Use CloudFormation StackSets or another solution to deploy proactive controls across multiple AWS Regions or accounts.
- Make sure that the warning or failure message associated with a proactive control is explicit and clear. This helps developers understand the reason why the resource did not pass the evaluation.
- When building new proactive controls, start in observe mode. This means that you send a warning message instead of failing the resource deployment. This helps you understand the impact of the proactive control.
- Enable logging in Amazon CloudWatch Logs for proactive controls.
- If you need to monitor the invocation of a specific proactive control, use an Amazon EventBridge rule and subscribe to invocation events for the CloudFormation hook.

Use cases

- Prevent deployment of noncompliant resources
- Meet compliance requirements
- Improve code quality by enforcing remediation of a security issue before deployment
- Reduce operational downtime associated with remediating security issues after deployment

Technology

CloudFormation hooks

AWS CloudFormation helps you set up AWS resources, provision them quickly and consistently, and manage them throughout their lifecycle across AWS accounts and Regions. CloudFormation hooks proactively evaluate the configuration of your CloudFormation resources before they are deployed. If noncompliant resources are found, it returns a failure status. Based on the hook failure mode, CloudFormation can fail the operation or present a warning that allows the user to continue with the deployment. You can use available hooks, or you can develop your own.

AWS Control Tower

AWS Control Tower helps you set up and govern an AWS multi-account environment, following prescriptive best practices. AWS Control Tower offers preconfigured proactive controls that you can enable in your landing zone. If your landing zone is setup using AWS Control Tower, you can use these optional proactive controls as a starting point for your organization. You can build additional, custom proactive controls in CloudFormation as needed.

Business outcomes

Less human effort and error

Proactive controls reduce the risk of human error that leads to the deployment of noncompliant resources. They also reduce human effort later in the development cycle because they make developers consider resource security prior to deployment. This applies the *shift left* practice to building secure resources because it forces compliance earlier in the development lifecycle.

Reduced costs

It is generally more expensive to fix a security issue after deployment. Identifying and fixing issues earlier in the development cycle reduces the cost of development.

Time savings

Because proactive controls prevent the deployment of noncompliant resources, they reduce the amount of time you spend triaging and fixing security issues. They also the number of security findings, which detective controls would identify later in the development cycle.

Regulatory compliance

If your organization needs to comply with internal or industry regulations, proactive controls can help you stay compliant and avoid violation penalties.

Risk reduction

Proactive controls help developers deploy compliant and more securely built resources, so proactive controls reduce your organization's security risk.

Detective controls

Detective controls are security controls that are designed to detect, log, and alert after an event has occurred. Detective controls are a foundational part of governance frameworks. These guardrails are a second line of defense, notifying you of security issues that bypassed the preventative controls.

For example, you might apply a detective control that detects and notifies you if an Amazon Simple Storage Service (Amazon S3) bucket becomes publicly accessible. While you might have preventative controls in place that disable public access to S3 buckets at the account level and then disable access through SCPs, a threat actor can circumvent these preventative controls by

logging in as an administrative user. In these situations, a detective control can alert you to the misconfiguration and potential threat.

Review the following about this type of control:

- Objectives
- Process
- Use cases
- Technology
- Business outcomes

Objectives

- Detective controls help you improve security operations processes and quality processes.
- Detective controls help you meet regulatory, legal, or compliance obligations.
- Detective controls provide security operations teams with visibility to respond to security issues, including advanced threats that bypass the preventative controls.
- Detective controls can help you identify the appropriate response to security issues and potential threats.

Process

You implement detective controls implemented in two phases. First, you set up the system to log events and resource states to a centralized location, such as Amazon CloudWatch Logs. After centralized logging is in place, you analyze those logs to detect anomalies that might indicate a threat. Each analysis is a control that is mapped back to your original requirements and policies. For example, you can create a detective control that searches the logs for a specific pattern and generates an alert if it matches. Detective controls are used by security teams to improve their overall visibility into threats and risks that their system might be exposed to.

Use cases

Detection of suspicious behavior

Detective controls help identify any anomalous activity, such as compromised privileged user credentials or access to or exfiltration of sensitive data. These controls are important reactive factors that can help your company identify and understand the scope of anomalous activity.

Detection of fraud

These controls help detect and identify a threat inside your company, such as a user who is circumventing policies and performing unauthorized transactions.

Compliance

Detective controls help you meet compliance requirements, such as Payment Card Industry Data Security Standard (PCI DSS), and can help prevent identity theft. These controls can help you discover and protect sensitive information that is subject to regulatory compliance, such as personally identifiable information.

Automated analysis

Detective controls can automatically analyze logs to detect anomalies and other indicators of unauthorized activity.

You can automatically analyze logs from different sources such as AWS CloudTrail logs, VPC Flow Log, and Domain Name System (DNS) logs, for indications of potentially malicious activity. To help with organization, aggregate security alerts or findings from multiple AWS services to a centralized location.

Technology

A common detective control is implementing one or more monitoring services, which can analyze data sources, such as logs, to identify security threats. In the AWS Cloud, you can analyze sources such as AWS CloudTrail logs, Amazon S3 access logs, and Amazon Virtual Private Cloud flow logs to help detect unusual activity. AWS security services, such as Amazon GuardDuty, Amazon Detective, AWS Security Hub, and Amazon Macie have built-in monitoring functionalities.

GuardDuty and Security Hub

Amazon GuardDuty uses threat intelligence, machine learning, and anomaly-detection techniques to continuously monitor your log sources for malicious or unauthorized activity. The dashboard provides insights into the real-time health of your AWS accounts and workloads. You can integrate GuardDuty with AWS Security Hub, a cloud security posture management service that checks for adherence to best practices, aggregates alerts, and enables automated remediation. GuardDuty sends findings to Security Hub as a way to centralize information. You can further integrate Security Hub with security information and event management (SIEM) solutions to extend monitoring and alerting capabilities for your organization.

Macie

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to help discover and protect sensitive data in AWS. The following are some of the detective controls and features available in Macie:

- Macie inspects bucket inventory and all objects stored in Amazon S3. This information can be presented in a single dashboard view, providing visibility and helping you evaluate bucket security.
- For discovering sensitive data, Macie uses built-in, managed data identifiers and also supports custom data identifiers.
- Macie integrates natively with other AWS services and tools. For example, Macie issues findings as Amazon EventBridge events, which are automatically sent to Security Hub.

The following are best practices for configuring detective controls in Macie:

- Enable Macie on all accounts. By using the delegated management feature, enable Macie on multiple accounts by using AWS Organizations.
- Use Macie to evaluate the security posture of the S3 buckets in your accounts. This helps prevent data loss by providing visibility into data location and access. For more information, see Analyzing your Amazon S3 security posture (Macie documentation).
- Automate discovery of sensitive data in your S3 buckets by running and scheduling automated processing and data discovery jobs. This inspects S3 buckets for sensitive data on a regular schedule.

AWS Config

AWS Config audits and records the compliance of AWS resources. AWS Config discovers existing AWS resources and generates a full inventory, along with the configuration details of each resource. If there are any configuration changes, it records those changes and provides notification. This can help you detect and roll back unauthorized infrastructure changes. You can use AWS managed rules and can create custom rules.

The following are best practices for configuring detective controls in AWS Config:

- Enable AWS Config for each member account in the organization and for each AWS Region that contains resources that you want to protect.

- Set up Amazon Simple Notification Service (Amazon SNS) alerts for any configuration changes.
- Store configuration data in an S3 bucket and use Amazon Athena to analyze it.
- Automate the remediation of noncompliant resources by using Automation, a capability of AWS Systems Manager.
- Use EventBridge or Amazon SNS to set up notifications about noncompliant AWS resources.

Trusted Advisor

AWS Trusted Advisor can be used as a service for detective controls. Through a set of checks, Trusted Advisor identifies areas where you can optimize your infrastructure, improve performance and security, or reduce costs. Trusted Advisor provides recommendations based on AWS best practices that you can follow to improve your services and resources. Business and Enterprise Support plans provide access to all available checks for the pillars of the AWS Well-Architected Framework.

The following are best practices for configuring detective controls in Trusted Advisor:

- Review the check level summary
- Implement resource-specific recommendations for warning and error states.
- Check Trusted Advisor frequently to actively review and implement its recommendations.

Amazon Inspector

Amazon Inspector is an automated vulnerability management service that, after being enabled, continuously scans your workloads for any unintended network exposure or software vulnerabilities. It contextualizes findings into a risk score that can help you determine next steps, such as remediating or confirming compliance status.

The following are best practices for configuring detective controls in Amazon Inspector:

- Enable Amazon Inspector on all accounts and integrate it into EventBridge and Security Hub to configure reporting and notifications for security vulnerabilities.
- Prioritize remediations and other actions based on the Amazon Inspector risk score.

Business outcomes

Less human effort and error

You can achieve automation by using infrastructure as code (IaC). Automating deployment, configuration of monitoring and remediation services and tools reduces the risk of manual errors and reduces the amount of time and effort required to scale these detective controls. Automation helps with the development of security runbooks and reduces manual operations for security analysts. Regular reviews help tune the automation tools and continuously iterate and improve the detective controls.

Appropriate actions against potential threats

Capturing and analyzing events from logs and metrics is crucial to gaining visibility. This helps analysts act on security events and potential threats to help secure your workloads. Being able to quickly identify which vulnerabilities exist helps analysts take appropriate actions to address and remediate them.

Better incident response and investigative handling

Automation of detective control tools can increase the speed of detection, investigation, and recovery. Automated alerting and notifications based on defined conditions enable security analysts to investigate and respond appropriately. These responsive factors can help you identify and understand the scope of anomalous activity.

Responsive controls

Responsive controls are security controls that are designed to drive remediation of adverse events or deviations from your security baseline. Examples of technical responsive controls include patching a system, quarantining a virus, shutting down a process, or rebooting a system.

Review the following about this type of control:

- Objectives
- Process
- Use cases
- Technology
- Business outcomes

Objectives

- Responsive controls can help you create runbooks for common types of attacks, such as phishing or brute force.
- Responsive controls can implement automated responses to potential security issues.
- Responsive controls can automatically remediate unintended or unapproved actions on AWS resources, such as deleting unencrypted S3 buckets.
- Responsive controls can be orchestrated to work with preventative and detective controls to create a holistic and proactive approach for addressing potential security incidents.

Process

Detective controls are a prerequisite for establishing responsive controls. You must be able to detect the security issue before you can remediate it. You can then establish a policy or response to the security issue. For example, in the event of a brute force attack, a remediation process would be implemented. After the remediation process exists, it can then be automated and run as a script by using a programming language, such as a shell script.

Consider whether the responsive control might break an existing production workload. For example, if the detective security control is *S3 buckets must not be publicly accessible* and the remediation is *turn off public access for Amazon S3*, this could have significant implications for your company and its customers. If the S3 bucket is serving a public website, turning off public access could create an outage. Databases are a similar example. If a database must not be publicly accessible through the internet, turning off public access could affect connectivity to the application.

Use cases

- Automatic response to detected security events
- Automatic remediation of detected security vulnerabilities
- Automated recovery control to reduce operational downtime

Technology

Security Hub

AWS Security Hub automatically sends all new findings and all updates of existing findings to EventBridge as events. You can also create custom actions that send selected findings and insight results to EventBridge. You can configure EventBridge to respond to each type of event. The event can initiate an AWS Lambda function that performs the remediation action.

AWS Config

AWS Config uses rules to evaluate your AWS resources and helps you remediate noncompliant resources. AWS Config applies remediation using AWS Systems Manager Automation. In Automation documents, you define the actions that you want to perform on resources that AWS Config determines to be noncompliant. After you create Automation documents, you can use them in Systems Manager through the AWS Management Console or by using APIs. You can choose to either manually or automatically remediate noncompliant resources.

Business outcomes

Minimize data loss

After a cybersecurity incident, using responsive security controls can help minimize data loss and damage to the system or network. Responsive controls can also help restore critical business systems and processes as quickly as possible, adding to the resilience of your workloads.

Reduce cost

Automation reduces costs associated with human resources because team members don't have to manually respond to incidents or otherwise manage them on a case-by-case basis.

Next steps

After reading this guide, you should be familiar with the four types of security controls, understand how they are part of your security governance framework, and be prepared to start implementing and automating security controls in the AWS Cloud. For more information and, we recommend that you review the references included in the Resources section.

We also recommend that you take the following next steps to assess the security of your cloud infrastructure and start implementing security controls:

1. Enable and configure AWS Security Hub. As a best practice, we recommend enabling the available standards controls. For more information, see Security standards and controls (Security Hub documentation).
2. Enable and configure AWS Config. For more information, see Getting started (AWS Config documentation).
3. Using AWS services such as Security Hub, Amazon Macie, AWS Config, AWS Trusted Advisor, and Amazon Inspector, assess your organization and account infrastructure , identify areas that need improvement, and review and recommendations in these services. Use the security check feature in Security Hub to generate a security score for a security standard. For more information, see Determining security scores (Security Hub documentation).
4. Implement preventative, proactive, detective, and responsive security controls based on the identified improvements.
5. Conduct a follow-up security assessment to evaluate the effectiveness of the implemented security controls. In Security Hub, determine whether the security score has improved. Iterate to improve or add new security controls.
6. Establish a regular cadence for performing security assessments, such as yearly.

FAQ

What should I focus on if I have limited time and resources and can't implement all of these control types?

We recommend implementing AWS Security Hub. Security Hub has a set of automated security controls called the AWS Foundational Security Best Practices standard (Security Hub documentation). This is a highly curated set of security best practices managed by AWS security experts. You can run these standard controls either continuously, whenever there are changes to the associated resources, or periodically, on a regular schedule. Each control has a specific severity score to help you prioritize your remediation efforts. For more information, see Running security checks (Security Hub documentation). If you are using AWS Control Tower, you can also review and choose to enable its preventative, detective, and proactive controls.

Resources

AWS documentation

- AWS Security Reference Architecture (AWS SRA)
- AWS CAF security perspective
- Best Practices for security, identity, and compliance
- Automated Security Response on AWS (AWS Solution)
  - Solution landing page
  - Implementation guide

AWS blog posts

- Identity Guide – Preventive controls with AWS Identity – SCPs
- How to implement a read-only service control policy (SCP) for accounts in AWS Organizations
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment
- Maintain compliance using Service Control Policies and ensure they are always applied
- When and where to use IAM permissions boundaries
- Proactively keep resources secure and compliant with AWS CloudFormation hooks

Other resources

- Cloud Controls Matrix (CCM) (Cloud Security Alliance)
- Example permissions boundaries (GitHub)

Document history

The following table describes significant changes to this guide. If you want to be notified about future updates, you can subscribe to an RSS feed.

Change	Description	Date
Proactive controls	We added information about proactive controls to this guide, including the Proactive controls section.	December 4, 2023
Initial publication	—	December 12, 2022

AWS Prescriptive Guidance glossary

The following are commonly used terms in strategies, guides, and patterns provided by AWS Prescriptive Guidance. To suggest entries, please use the **Provide feedback** link at the end of the glossary.

Numbers

7 Rs

Seven common migration strategies for moving applications to the cloud. These strategies build upon the 5 Rs that Gartner identified in 2011 and consist of the following:

- Refactor/re-architect – Move an application and modify its architecture by taking full advantage of cloud-native features to improve agility, performance, and scalability. This typically involves porting the operating system and database. Example: Migrate your on-premises Oracle database to the Amazon Aurora PostgreSQL-Compatible Edition.
- Replatform (lift and reshape) – Move an application to the cloud, and introduce some level of optimization to take advantage of cloud capabilities. Example: Migrate your on-premises Oracle database to Amazon Relational Database Service (Amazon RDS) for Oracle in the AWS Cloud.
- Repurchase (drop and shop) – Switch to a different product, typically by moving from a traditional license to a SaaS model. Example: Migrate your customer relationship management (CRM) system to Salesforce.com.
- Rehost (lift and shift) – Move an application to the cloud without making any changes to take advantage of cloud capabilities. Example: Migrate your on-premises Oracle database to Oracle on an EC2 instance in the AWS Cloud.
- Relocate (hypervisor-level lift and shift) – Move infrastructure to the cloud without purchasing new hardware, rewriting applications, or modifying your existing operations. You migrate servers from an on-premises platform to a cloud service for the same platform. Example: Migrate a Microsoft Hyper-V application to AWS.
- Retain (revisit) – Keep applications in your source environment. These might include applications that require major refactoring, and you want to postpone that work until a later time, and legacy applications that you want to retain, because there's no business justification for migrating them.

- Retire – Decommission or remove applications that are no longer needed in your source environment.

A

ABAC

See attribute-based access control.

abstracted services

See managed services.

ACID

See atomicity, consistency, isolation, durability.

active-active migration

A database migration method in which the source and target databases are kept in sync (by using a bidirectional replication tool or dual write operations), and both databases handle transactions from connecting applications during migration. This method supports migration in small, controlled batches instead of requiring a one-time cutover. It's more flexible but requires more work than active-passive migration.

active-passive migration

A database migration method in which in which the source and target databases are kept in sync, but only the source database handles transactions from connecting applications while data is replicated to the target database. The target database doesn't accept any transactions during migration.

aggregate function

A SQL function that operates on a group of rows and calculates a single return value for the group. Examples of aggregate functions include `SUM` and `MAX`.

AI

See artificial intelligence.

AIOps

See artificial intelligence operations.

anonymization

The process of permanently deleting personal information in a dataset. Anonymization can help protect personal privacy. Anonymized data is no longer considered to be personal data.

anti-pattern

A frequently used solution for a recurring issue where the solution is counter-productive, ineffective, or less effective than an alternative.

application control

A security approach that allows the use of only approved applications in order to help protect a system from malware.

application portfolio

A collection of detailed information about each application used by an organization, including the cost to build and maintain the application, and its business value. This information is key to the portfolio discovery and analysis process and helps identify and prioritize the applications to be migrated, modernized, and optimized.

artificial intelligence (AI)

The field of computer science that is dedicated to using computing technologies to perform cognitive functions that are typically associated with humans, such as learning, solving problems, and recognizing patterns. For more information, see What is Artificial Intelligence?

artificial intelligence operations (AIOps)

The process of using machine learning techniques to solve operational problems, reduce operational incidents and human intervention, and increase service quality. For more information about how AIOps is used in the AWS migration strategy, see the operations integration guide.

asymmetric encryption

An encryption algorithm that uses a pair of keys, a public key for encryption and a private key for decryption. You can share the public key because it isn't used for decryption, but access to the private key should be highly restricted.

atomicity, consistency, isolation, durability (ACID)

A set of software properties that guarantee the data validity and operational reliability of a database, even in the case of errors, power failures, or other problems.

attribute-based access control (ABAC)

The practice of creating fine-grained permissions based on user attributes, such as department, job role, and team name. For more information, see ABAC for AWS in the AWS Identity and Access Management (IAM) documentation.

authoritative data source

A location where you store the primary version of data, which is considered to be the most reliable source of information. You can copy data from the authoritative data source to other locations for the purposes of processing or modifying the data, such as anonymizing, redacting, or pseudonymizing it.

Availability Zone

A distinct location within an AWS Region that is insulated from failures in other Availability Zones and provides inexpensive, low-latency network connectivity to other Availability Zones in the same Region.

AWS Cloud Adoption Framework (AWS CAF)

A framework of guidelines and best practices from AWS to help organizations develop an efficient and effective plan to move successfully to the cloud. AWS CAF organizes guidance into six focus areas called perspectives: business, people, governance, platform, security, and operations. The business, people, and governance perspectives focus on business skills and processes; the platform, security, and operations perspectives focus on technical skills and processes. For example, the people perspective targets stakeholders who handle human resources (HR), staffing functions, and people management. For this perspective, AWS CAF provides guidance for people development, training, and communications to help ready the organization for successful cloud adoption. For more information, see the AWS CAF website and the AWS CAF whitepaper.

AWS Workload Qualification Framework (AWS WQF)

A tool that evaluates database migration workloads, recommends migration strategies, and provides work estimates. AWS WQF is included with AWS Schema Conversion Tool (AWS SCT). It analyzes database schemas and code objects, application code, dependencies, and performance characteristics, and provides assessment reports.

B

bad bot

A bot that is intended to disrupt or cause harm to individuals or organizations.

BCP

See business continuity planning.

behavior graph

A unified, interactive view of resource behavior and interactions over time. You can use a behavior graph with Amazon Detective to examine failed logon attempts, suspicious API calls, and similar actions. For more information, see Data in a behavior graph in the Detective documentation.

big-endian system

A system that stores the most significant byte first. See also endianness.

binary classification

A process that predicts a binary outcome (one of two possible classes). For example, your ML model might need to predict problems such as “Is this email spam or not spam?" or "Is this product a book or a car?"

bloom filter

A probabilistic, memory-efficient data structure that is used to test whether an element is a member of a set.

blue/green deployment

A deployment strategy where you create two separate but identical environments. You run the current application version in one environment (blue) and the new application version in the other environment (green). This strategy helps you quickly roll back with minimal impact.

bot

A software application that runs automated tasks over the internet and simulates human activity or interaction. Some bots are useful or beneficial, such as web crawlers that index information on the internet. Some other bots, known as *bad bots*, are intended to disrupt or cause harm to individuals or organizations.

botnet

Networks of bots that are infected by malware and are under the control of a single party, known as a *bot herder* or *bot operator*. Botnets are the best-known mechanism to scale bots and their impact.

branch

A contained area of a code repository. The first branch created in a repository is the *main branch*. You can create a new branch from an existing branch, and you can then develop features or fix bugs in the new branch. A branch you create to build a feature is commonly referred to as a *feature branch*. When the feature is ready for release, you merge the feature branch back into the main branch. For more information, see About branches (GitHub documentation).

break-glass access

In exceptional circumstances and through an approved process, a quick means for a user to gain access to an AWS account that they don't typically have permissions to access. For more information, see the Implement break-glass procedures indicator in the AWS Well-Architected guidance.

brownfield strategy

The existing infrastructure in your environment. When adopting a brownfield strategy for a system architecture, you design the architecture around the constraints of the current systems and infrastructure. If you are expanding the existing infrastructure, you might blend brownfield and greenfield strategies.

buffer cache

The memory area where the most frequently accessed data is stored.

business capability

What a business does to generate value (for example, sales, customer service, or marketing). Microservices architectures and development decisions can be driven by business capabilities. For more information, see the Organized around business capabilities section of the Running containerized microservices on AWS whitepaper.

business continuity planning (BCP)

A plan that addresses the potential impact of a disruptive event, such as a large-scale migration, on operations and enables a business to resume operations quickly.

C

CAF

See AWS Cloud Adoption Framework.

canary deployment

The slow and incremental release of a version to end users. When you are confident, you deploy the new version and replace the current version in its entirety.

CCoE

See Cloud Center of Excellence.

CDC

See change data capture.

change data capture (CDC)

The process of tracking changes to a data source, such as a database table, and recording metadata about the change. You can use CDC for various purposes, such as auditing or replicating changes in a target system to maintain synchronization.

chaos engineering

Intentionally introducing failures or disruptive events to test a system's resilience. You can use AWS Fault Injection Service (AWS FIS) to perform experiments that stress your AWS workloads and evaluate their response.

CI/CD

See continuous integration and continuous delivery.

classification

A categorization process that helps generate predictions. ML models for classification problems predict a discrete value. Discrete values are always distinct from one another. For example, a model might need to evaluate whether or not there is a car in an image.

client-side encryption

Encryption of data locally, before the target AWS service receives it.

Cloud Center of Excellence (CCoE)

A multi-disciplinary team that drives cloud adoption efforts across an organization, including developing cloud best practices, mobilizing resources, establishing migration timelines, and leading the organization through large-scale transformations. For more information, see the CCoE posts on the AWS Cloud Enterprise Strategy Blog.

cloud computing

The cloud technology that is typically used for remote data storage and IoT device management. Cloud computing is commonly connected to edge computing technology.

cloud operating model

In an IT organization, the operating model that is used to build, mature, and optimize one or more cloud environments. For more information, see Building your Cloud Operating Model.

cloud stages of adoption

The four phases that organizations typically go through when they migrate to the AWS Cloud:

- Project – Running a few cloud-related projects for proof of concept and learning purposes
- Foundation – Making foundational investments to scale your cloud adoption (e.g., creating a landing zone, defining a CCoE, establishing an operations model)
- Migration – Migrating individual applications
- Re-invention – Optimizing products and services, and innovating in the cloud

These stages were defined by Stephen Orban in the blog post The Journey Toward Cloud-First & the Stages of Adoption on the AWS Cloud Enterprise Strategy blog. For information about how they relate to the AWS migration strategy, see the migration readiness guide.

CMDB

See configuration management database.

code repository

A location where source code and other assets, such as documentation, samples, and scripts, are stored and updated through version control processes. Common cloud repositories include GitHub or AWS CodeCommit. Each version of the code is called a *branch*. In a microservice structure, each repository is devoted to a single piece of functionality. A single CI/CD pipeline can use multiple repositories.

cold cache

A buffer cache that is empty, not well populated, or contains stale or irrelevant data. This affects performance because the database instance must read from the main memory or disk, which is slower than reading from the buffer cache.

cold data

Data that is rarely accessed and is typically historical. When querying this kind of data, slow queries are typically acceptable. Moving this data to lower-performing and less expensive storage tiers or classes can reduce costs.

computer vision (CV)

A field of AI that uses machine learning to analyze and extract information from visual formats such as digital images and videos. For example, AWS Panorama offers devices that add CV to on-premises camera networks, and Amazon SageMaker provides image processing algorithms for CV.

configuration drift

For a workload, a configuration change from the expected state. It might cause the workload to become noncompliant, and it's typically gradual and unintentional.

configuration management database (CMDB)

A repository that stores and manages information about a database and its IT environment, including both hardware and software components and their configurations. You typically use data from a CMDB in the portfolio discovery and analysis stage of migration.

conformance pack

A collection of AWS Config rules and remediation actions that you can assemble to customize your compliance and security checks. You can deploy a conformance pack as a single entity in an AWS account and Region, or across an organization, by using a YAML template. For more information, see Conformance packs in the AWS Config documentation.

continuous integration and continuous delivery (CI/CD)

The process of automating the source, build, test, staging, and production stages of the software release process. CI/CD is commonly described as a pipeline. CI/CD can help you automate processes, improve productivity, improve code quality, and deliver faster. For more information, see Benefits of continuous delivery. CD can also stand for *continuous deployment*. For more information, see Continuous Delivery vs. Continuous Deployment.

CV

See computer vision.

D

data at rest

Data that is stationary in your network, such as data that is in storage.

data classification

A process for identifying and categorizing the data in your network based on its criticality and sensitivity. It is a critical component of any cybersecurity risk management strategy because it helps you determine the appropriate protection and retention controls for the data. Data classification is a component of the security pillar in the AWS Well-Architected Framework. For more information, see Data classification.

data drift

A meaningful variation between the production data and the data that was used to train an ML model, or a meaningful change in the input data over time. Data drift can reduce the overall quality, accuracy, and fairness in ML model predictions.

data in transit

Data that is actively moving through your network, such as between network resources.

data mesh

An architectural framework that provides distributed, decentralized data ownership with centralized management and governance.

data minimization

The principle of collecting and processing only the data that is strictly necessary. Practicing data minimization in the AWS Cloud can reduce privacy risks, costs, and your analytics carbon footprint.

data perimeter

A set of preventive guardrails in your AWS environment that help make sure that only trusted identities are accessing trusted resources from expected networks. For more information, see Building a data perimeter on AWS.

data preprocessing

To transform raw data into a format that is easily parsed by your ML model. Preprocessing data can mean removing certain columns or rows and addressing missing, inconsistent, or duplicate values.

data provenance

The process of tracking the origin and history of data throughout its lifecycle, such as how the data was generated, transmitted, and stored.

data subject

An individual whose data is being collected and processed.

data warehouse

A data management system that supports business intelligence, such as analytics. Data warehouses commonly contain large amounts of historical data, and they are typically used for queries and analysis.

database definition language (DDL)

Statements or commands for creating or modifying the structure of tables and objects in a database.

database manipulation language (DML)

Statements or commands for modifying (inserting, updating, and deleting) information in a database.

DDL

See database definition language.

deep ensemble

To combine multiple deep learning models for prediction. You can use deep ensembles to obtain a more accurate prediction or for estimating uncertainty in predictions.

deep learning

An ML subfield that uses multiple layers of artificial neural networks to identify mapping between input data and target variables of interest.

defense-in-depth

An information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within. When you adopt this strategy on AWS, you add multiple controls at different layers of the AWS Organizations structure to help secure resources. For example, a defense-in-depth approach might combine multi-factor authentication, network segmentation, and encryption.

delegated administrator

In AWS Organizations, a compatible service can register an AWS member account to administer the organization's accounts and manage permissions for that service. This account is called the *delegated administrator* for that service. For more information and a list of compatible services, see Services that work with AWS Organizations in the AWS Organizations documentation.

deployment

The process of making an application, new features, or code fixes available in the target environment. Deployment involves implementing changes in a code base and then building and running that code base in the application's environments.

development environment

See environment.

detective control

A security control that is designed to detect, log, and alert after an event has occurred. These controls are a second line of defense, alerting you to security events that bypassed the preventative controls in place. For more information, see Detective controls in *Implementing security controls on AWS*.

development value stream mapping (DVSM)

A process used to identify and prioritize constraints that adversely affect speed and quality in a software development lifecycle. DVSM extends the value stream mapping process originally designed for lean manufacturing practices. It focuses on the steps and teams required to create and move value through the software development process.

digital twin

A virtual representation of a real-world system, such as a building, factory, industrial equipment, or production line. Digital twins support predictive maintenance, remote monitoring, and production optimization.

dimension table

In a star schema, a smaller table that contains data attributes about quantitative data in a fact table. Dimension table attributes are typically text fields or discrete numbers that behave like text. These attributes are commonly used for query constraining, filtering, and result set labeling.

disaster

An event that prevents a workload or system from fulfilling its business objectives in its primary deployed location. These events can be natural disasters, technical failures, or the result of human actions, such as unintentional misconfiguration or a malware attack.

disaster recovery (DR)

The strategy and process you use to minimize downtime and data loss caused by a disaster. For more information, see Disaster Recovery of Workloads on AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

See database manipulation language.

domain-driven design

An approach to developing a complex software system by connecting its components to evolving domains, or core business goals, that each component serves. This concept was introduced by Eric Evans in his book, *Domain-Driven Design: Tackling Complexity in the Heart of Software* (Boston: Addison-Wesley Professional, 2003). For information about how you can use domain-driven design with the strangler fig pattern, see Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

DR

See disaster recovery.

drift detection

Tracking deviations from a baselined configuration. For example, you can use AWS CloudFormation to detect drift in system resources, or you can use AWS Control Tower to detect changes in your landing zone that might affect compliance with governance requirements.

DVSM

See development value stream mapping.

E

EDA

See exploratory data analysis.

edge computing

The technology that increases the computing power for smart devices at the edges of an IoT network. When compared with cloud computing, edge computing can reduce communication latency and improve response time.

encryption

A computing process that transforms plaintext data, which is human-readable, into ciphertext.

encryption key

A cryptographic string of randomized bits that is generated by an encryption algorithm. Keys can vary in length, and each key is designed to be unpredictable and unique.

endianness

The order in which bytes are stored in computer memory. Big-endian systems store the most significant byte first. Little-endian systems store the least significant byte first.

endpoint

See service endpoint.

endpoint service

A service that you can host in a virtual private cloud (VPC) to share with other users. You can create an endpoint service with AWS PrivateLink and grant permissions to other AWS accounts or to AWS Identity and Access Management (IAM) principals. These accounts or principals can connect to your endpoint service privately by creating interface VPC endpoints. For more information, see Create an endpoint service in the Amazon Virtual Private Cloud (Amazon VPC) documentation.

enterprise resource planning (ERP)

A system that automates and manages key business processes (such as accounting, MES, and project management) for an enterprise.

envelope encryption

The process of encrypting an encryption key with another encryption key. For more information, see Envelope encryption in the AWS Key Management Service (AWS KMS) documentation.

environment

An instance of a running application. The following are common types of environments in cloud computing:

- development environment – An instance of a running application that is available only to the core team responsible for maintaining the application. Development environments are used to test changes before promoting them to upper environments. This type of environment is sometimes referred to as a *test environment*.
- lower environments – All development environments for an application, such as those used for initial builds and tests.
- production environment – An instance of a running application that end users can access. In a CI/CD pipeline, the production environment is the last deployment environment.
- upper environments – All environments that can be accessed by users other than the core development team. This can include a production environment, preproduction environments, and environments for user acceptance testing.

epic

In agile methodologies, functional categories that help organize and prioritize your work. Epics provide a high-level description of requirements and implementation tasks. For example, AWS CAF security epics include identity and access management, detective controls, infrastructure security, data protection, and incident response. For more information about epics in the AWS migration strategy, see the program implementation guide.

ERP

See enterprise resource planning.

exploratory data analysis (EDA)

The process of analyzing a dataset to understand its main characteristics. You collect or aggregate data and then perform initial investigations to find patterns, detect anomalies, and check assumptions. EDA is performed by calculating summary statistics and creating data visualizations.

F

fact table

The central table in a star schema. It stores quantitative data about business operations. Typically, a fact table contains two types of columns: those that contain measures and those that contain a foreign key to a dimension table.

fail fast

A philosophy that uses frequent and incremental testing to reduce the development lifecycle. It is a critical part of an agile approach.

fault isolation boundary

In the AWS Cloud, a boundary such as an Availability Zone, AWS Region, control plane, or data plane that limits the effect of a failure and helps improve the resilience of workloads. For more information, see AWS Fault Isolation Boundaries.

feature branch

See branch.

features

The input data that you use to make a prediction. For example, in a manufacturing context, features could be images that are periodically captured from the manufacturing line.

feature importance

How significant a feature is for a model's predictions. This is usually expressed as a numerical score that can be calculated through various techniques, such as Shapley Additive Explanations (SHAP) and integrated gradients. For more information, see Machine learning model interpretability with :AWS.

feature transformation

To optimize data for the ML process, including enriching data with additional sources, scaling values, or extracting multiple sets of information from a single data field. This enables the ML model to benefit from the data. For example, if you break down the "2021-05-27 00:15:37" date into "2021", "May", "Thu", and "15", you can help the learning algorithm learn nuanced patterns associated with different data components.

FGAC

See fine-grained access control.

fine-grained access control (FGAC)

The use of multiple conditions to allow or deny an access request.

flash-cut migration

A database migration method that uses continuous data replication through change data capture to migrate data in the shortest time possible, instead of using a phased approach. The objective is to keep downtime to a minimum.

G

geo blocking

See geographic restrictions.

geographic restrictions (geo blocking)

In Amazon CloudFront, an option to prevent users in specific countries from accessing content distributions. You can use an allow list or block list to specify approved and banned countries. For more information, see Restricting the geographic distribution of your content in the CloudFront documentation.

Gitflow workflow

An approach in which lower and upper environments use different branches in a source code repository. The Gitflow workflow is considered legacy, and the trunk-based workflow is the modern, preferred approach.

greenfield strategy

The absence of existing infrastructure in a new environment. When adopting a greenfield strategy for a system architecture, you can select all new technologies without the restriction of compatibility with existing infrastructure, also known as brownfield. If you are expanding the existing infrastructure, you might blend brownfield and greenfield strategies.

guardrail

A high-level rule that helps govern resources, policies, and compliance across organizational units (OUs). *Preventive guardrails* enforce policies to ensure alignment to compliance standards. They are implemented by using service control policies and IAM permissions boundaries. *Detective guardrails* detect policy violations and compliance issues, and generate alerts

for remediation. They are implemented by using AWS Config, AWS Security Hub, Amazon GuardDuty, AWS Trusted Advisor, Amazon Inspector, and custom AWS Lambda checks.

H

HA

See high availability.

heterogeneous database migration

Migrating your source database to a target database that uses a different database engine (for example, Oracle to Amazon Aurora). Heterogeneous migration is typically part of a re-architecting effort, and converting the schema can be a complex task. AWS provides AWS SCT that helps with schema conversions.

high availability (HA)

The ability of a workload to operate continuously, without intervention, in the event of challenges or disasters. HA systems are designed to automatically fail over, consistently deliver high-quality performance, and handle different loads and failures with minimal performance impact.

historian modernization

An approach used to modernize and upgrade operational technology (OT) systems to better serve the needs of the manufacturing industry. A *historian* is a type of database that is used to collect and store data from various sources in a factory.

homogeneous database migration

Migrating your source database to a target database that shares the same database engine (for example, Microsoft SQL Server to Amazon RDS for SQL Server). Homogeneous migration is typically part of a rehosting or replatforming effort. You can use native database utilities to migrate the schema.

hot data

Data that is frequently accessed, such as real-time data or recent translational data. This data typically requires a high-performance storage tier or class to provide fast query responses.

hotfix

An urgent fix for a critical issue in a production environment. Due to its urgency, a hotfix is usually made outside of the typical DevOps release workflow.

hypercare period

Immediately following cutover, the period of time when a migration team manages and monitors the migrated applications in the cloud in order to address any issues. Typically, this period is 1–4 days in length. At the end of the hypercare period, the migration team typically transfers responsibility for the applications to the cloud operations team.

I

IaC

See infrastructure as code.

identity-based policy

A policy attached to one or more IAM principals that defines their permissions within the AWS Cloud environment.

idle application

An application that has an average CPU and memory usage between 5 and 20 percent over a period of 90 days. In a migration project, it is common to retire these applications or retain them on premises.

IIoT

See industrial Internet of Things.

immutable infrastructure

A model that deploys new infrastructure for production workloads instead of updating, patching, or modifying the existing infrastructure. Immutable infrastructures are inherently more consistent, reliable, and predictable than mutable infrastructure. For more information, see the Deploy using immutable infrastructure best practice in the AWS Well-Architected Framework.

inbound (ingress) VPC

In an AWS multi-account architecture, a VPC that accepts, inspects, and routes network connections from outside an application. The AWS Security Reference Architecture recommends

setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

incremental migration

A cutover strategy in which you migrate your application in small parts instead of performing a single, full cutover. For example, you might move only a few microservices or users to the new system initially. After you verify that everything is working properly, you can incrementally move additional microservices or users until you can decommission your legacy system. This strategy reduces the risks associated with large migrations.

Industry 4.0

A term that was introduced by Klaus Schwab in 2016 to refer to the modernization of manufacturing processes through advances in connectivity, real-time data, automation, analytics, and AI/ML.

infrastructure

All of the resources and assets contained within an application's environment.

infrastructure as code (IaC)

The process of provisioning and managing an application's infrastructure through a set of configuration files. IaC is designed to help you centralize infrastructure management, standardize resources, and scale quickly so that new environments are repeatable, reliable, and consistent.

industrial Internet of Things (IIoT)

The use of internet-connected sensors and devices in the industrial sectors, such as manufacturing, energy, automotive, healthcare, life sciences, and agriculture. For more information, see Building an industrial Internet of Things (IIoT) digital transformation strategy.

inspection VPC

In an AWS multi-account architecture, a centralized VPC that manages inspections of network traffic between VPCs (in the same or different AWS Regions), the internet, and on-premises networks. The AWS Security Reference Architecture recommends setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

Internet of Things (IoT)

The network of connected physical objects with embedded sensors or processors that communicate with other devices and systems through the internet or over a local communication network. For more information, see What is IoT?

interpretability

A characteristic of a machine learning model that describes the degree to which a human can understand how the model's predictions depend on its inputs. For more information, see Machine learning model interpretability with AWS.

IoT

See Internet of Things.

IT information library (ITIL)

A set of best practices for delivering IT services and aligning these services with business requirements. ITIL provides the foundation for ITSM.

IT service management (ITSM)

Activities associated with designing, implementing, managing, and supporting IT services for an organization. For information about integrating cloud operations with ITSM tools, see the operations integration guide.

ITIL

See IT information library.

ITSM

See IT service management.

L

label-based access control (LBAC)

An implementation of mandatory access control (MAC) where the users and the data itself are each explicitly assigned a security label value. The intersection between the user security label and data security label determines which rows and columns can be seen by the user.

landing zone

A landing zone is a well-architected, multi-account AWS environment that is scalable and secure. This is a starting point from which your organizations can quickly launch and deploy workloads and applications with confidence in their security and infrastructure environment. For more information about landing zones, see Setting up a secure and scalable multi-account AWS environment.

large migration

A migration of 300 or more servers.

LBAC

See label-based access control.

least privilege

The security best practice of granting the minimum permissions required to perform a task. For more information, see Apply least-privilege permissions in the IAM documentation.

lift and shift

See 7 Rs.

little-endian system

A system that stores the least significant byte first. See also endianness.

lower environments

See environment.

M

machine learning (ML)

A type of artificial intelligence that uses algorithms and techniques for pattern recognition and learning. ML analyzes and learns from recorded data, such as Internet of Things (IoT) data, to generate a statistical model based on patterns. For more information, see Machine Learning.

main branch

See branch.

malware

Software that is designed to compromise computer security or privacy. Malware might disrupt computer systems, leak sensitive information, or gain unauthorized access. Examples of malware include viruses, worms, ransomware, Trojan horses, spyware, and keyloggers.

managed services

AWS services for which AWS operates the infrastructure layer, the operating system, and platforms, and you access the endpoints to store and retrieve data. Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB are examples of managed services. These are also known as *abstracted services*.

manufacturing execution system (MES)

A software system for tracking, monitoring, documenting, and controlling production processes that convert raw materials to finished products on the shop floor.

MAP

See Migration Acceleration Program.

mechanism

A complete process in which you create a tool, drive adoption of the tool, and then inspect the results in order to make adjustments. A mechanism is a cycle that reinforces and improves itself as it operates. For more information, see Building mechanisms in the AWS Well-Architected Framework.

member account

All AWS accounts other than the management account that are part of an organization in AWS Organizations. An account can be a member of only one organization at a time.

MES

See manufacturing execution system.

Message Queuing Telemetry Transport (MQTT)

A lightweight, machine-to-machine (M2M) communication protocol, based on the publish/subscribe pattern, for resource-constrained IoT devices.

microservice

A small, independent service that communicates over well-defined APIs and is typically owned by small, self-contained teams. For example, an insurance system might include

microservices that map to business capabilities, such as sales or marketing, or subdomains, such as purchasing, claims, or analytics. The benefits of microservices include agility, flexible scaling, easy deployment, reusable code, and resilience. For more information, see Integrating microservices by using AWS serverless services.

microservices architecture

An approach to building an application with independent components that run each application process as a microservice. These microservices communicate through a well-defined interface by using lightweight APIs. Each microservice in this architecture can be updated, deployed, and scaled to meet demand for specific functions of an application. For more information, see Implementing microservices on AWS.

Migration Acceleration Program (MAP)

An AWS program that provides consulting support, training, and services to help organizations build a strong operational foundation for moving to the cloud, and to help offset the initial cost of migrations. MAP includes a migration methodology for executing legacy migrations in a methodical way and a set of tools to automate and accelerate common migration scenarios.

migration at scale

The process of moving the majority of the application portfolio to the cloud in waves, with more applications moved at a faster rate in each wave. This phase uses the best practices and lessons learned from the earlier phases to implement a *migration factory* of teams, tools, and processes to streamline the migration of workloads through automation and agile delivery. This is the third phase of the AWS migration strategy.

migration factory

Cross-functional teams that streamline the migration of workloads through automated, agile approaches. Migration factory teams typically include operations, business analysts and owners, migration engineers, developers, and DevOps professionals working in sprints. Between 20 and 50 percent of an enterprise application portfolio consists of repeated patterns that can be optimized by a factory approach. For more information, see the discussion of migration factories and the Cloud Migration Factory guide in this content set.

migration metadata

The information about the application and server that is needed to complete the migration. Each migration pattern requires a different set of migration metadata. Examples of migration metadata include the target subnet, security group, and AWS account.

migration pattern

A repeatable migration task that details the migration strategy, the migration destination, and the migration application or service used. Example: Rehost migration to Amazon EC2 with AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

An online tool that provides information for validating the business case for migrating to the AWS Cloud. MPA provides detailed portfolio assessment (server right-sizing, pricing, TCO comparisons, migration cost analysis) as well as migration planning (application data analysis and data collection, application grouping, migration prioritization, and wave planning). The MPA tool (requires login) is available free of charge to all AWS consultants and APN Partner consultants.

Migration Readiness Assessment (MRA)

The process of gaining insights about an organization's cloud readiness status, identifying strengths and weaknesses, and building an action plan to close identified gaps, using the AWS CAF. For more information, see the migration readiness guide. MRA is the first phase of the AWS migration strategy.

migration strategy

The approach used to migrate a workload to the AWS Cloud. For more information, see the 7 Rs entry in this glossary and see Mobilize your organization to accelerate large-scale migrations.

ML

See machine learning.

modernization

Transforming an outdated (legacy or monolithic) application and its infrastructure into an agile, elastic, and highly available system in the cloud to reduce costs, gain efficiencies, and take advantage of innovations. For more information, see Strategy for modernizing applications in the AWS Cloud.

modernization readiness assessment

An evaluation that helps determine the modernization readiness of an organization's applications; identifies benefits, risks, and dependencies; and determines how well the organization can support the future state of those applications. The outcome of the assessment is a blueprint of the target architecture, a roadmap that details development phases and

milestones for the modernization process, and an action plan for addressing identified gaps. For more information, see Evaluating modernization readiness for applications in the AWS Cloud.

monolithic applications (monoliths)

Applications that run as a single service with tightly coupled processes. Monolithic applications have several drawbacks. If one application feature experiences a spike in demand, the entire architecture must be scaled. Adding or improving a monolithic application's features also becomes more complex when the code base grows. To address these issues, you can use a microservices architecture. For more information, see Decomposing monoliths into microservices.

MPA

See Migration Portfolio Assessment.

MQTT

See Message Queuing Telemetry Transport.

multiclass classification

A process that helps generate predictions for multiple classes (predicting one of more than two outcomes). For example, an ML model might ask "Is this product a book, car, or phone?" or "Which product category is most interesting to this customer?"

mutable infrastructure

A model that updates and modifies the existing infrastructure for production workloads. For improved consistency, reliability, and predictability, the AWS Well-Architected Framework recommends the use of immutable infrastructure as a best practice.

O

OAC

See origin access control.

OAI

See origin access identity.

OCM

See organizational change management.

offline migration

A migration method in which the source workload is taken down during the migration process. This method involves extended downtime and is typically used for small, non-critical workloads.

OI

See operations integration.

OLA

See operational-level agreement.

online migration

A migration method in which the source workload is copied to the target system without being taken offline. Applications that are connected to the workload can continue to function during the migration. This method involves zero to minimal downtime and is typically used for critical production workloads.

OPC-UA

See Open Process Communications - Unified Architecture.

Open Process Communications - Unified Architecture (OPC-UA)

A machine-to-machine (M2M) communication protocol for industrial automation. OPC-UA provides an interoperability standard with data encryption, authentication, and authorization schemes.

operational-level agreement (OLA)

An agreement that clarifies what functional IT groups promise to deliver to each other, to support a service-level agreement (SLA).

operational readiness review (ORR)

A checklist of questions and associated best practices that help you understand, evaluate, prevent, or reduce the scope of incidents and possible failures. For more information, see Operational Readiness Reviews (ORR) in the AWS Well-Architected Framework.

operational technology (OT)

Hardware and software systems that work with the physical environment to control industrial operations, equipment, and infrastructure. In manufacturing, the integration of OT and information technology (IT) systems is a key focus for Industry 4.0 transformations.

operations integration (OI)

The process of modernizing operations in the cloud, which involves readiness planning, automation, and integration. For more information, see the operations integration guide.

organization trail

A trail that's created by AWS CloudTrail that logs all events for all AWS accounts in an organization in AWS Organizations. This trail is created in each AWS account that's part of the organization and tracks the activity in each account. For more information, see Creating a trail for an organization in the CloudTrail documentation.

organizational change management (OCM)

A framework for managing major, disruptive business transformations from a people, culture, and leadership perspective. OCM helps organizations prepare for, and transition to, new systems and strategies by accelerating change adoption, addressing transitional issues, and driving cultural and organizational changes. In the AWS migration strategy, this framework is called *people acceleration*, because of the speed of change required in cloud adoption projects. For more information, see the OCM guide.

origin access control (OAC)

In CloudFront, an enhanced option for restricting access to secure your Amazon Simple Storage Service (Amazon S3) content. OAC supports all S3 buckets in all AWS Regions, server-side encryption with AWS KMS (SSE-KMS), and dynamic `PUT` and `DELETE` requests to the S3 bucket.

origin access identity (OAI)

In CloudFront, an option for restricting access to secure your Amazon S3 content. When you use OAI, CloudFront creates a principal that Amazon S3 can authenticate with. Authenticated principals can access content in an S3 bucket only through a specific CloudFront distribution. See also OAC, which provides more granular and enhanced access control.

ORR

See operational readiness review.

OT

See operational technology.

outbound (egress) VPC

In an AWS multi-account architecture, a VPC that handles network connections that are initiated from within an application. The AWS Security Reference Architecture recommends

setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

P

permissions boundary

An IAM management policy that is attached to IAM principals to set the maximum permissions that the user or role can have. For more information, see Permissions boundaries in the IAM documentation.

personally identifiable information (PII)

Information that, when viewed directly or paired with other related data, can be used to reasonably infer the identity of an individual. Examples of PII include names, addresses, and contact information.

PII

See personally identifiable information.

playbook

A set of predefined steps that capture the work associated with migrations, such as delivering core operations functions in the cloud. A playbook can take the form of scripts, automated runbooks, or a summary of processes or steps required to operate your modernized environment.

PLC

See programmable logic controller.

PLM

See product lifecycle management.

policy

An object that can define permissions (see identity-based policy), specify access conditions (see resource-based policy), or define the maximum permissions for all accounts in an organization in AWS Organizations (see service control policy).

polyglot persistence

Independently choosing a microservice's data storage technology based on data access patterns and other requirements. If your microservices have the same data storage technology, they can encounter implementation challenges or experience poor performance. Microservices are more easily implemented and achieve better performance and scalability if they use the data store best adapted to their requirements. For more information, see Enabling data persistence in microservices.

portfolio assessment

A process of discovering, analyzing, and prioritizing the application portfolio in order to plan the migration. For more information, see Evaluating migration readiness.

predicate

A query condition that returns `true` or `false`, commonly located in a `WHERE` clause.

predicate pushdown

A database query optimization technique that filters the data in the query before transfer. This reduces the amount of data that must be retrieved and processed from the relational database, and it improves query performance.

preventative control

A security control that is designed to prevent an event from occurring. These controls are a first line of defense to help prevent unauthorized access or unwanted changes to your network. For more information, see Preventative controls in *Implementing security controls on AWS*.

principal

An entity in AWS that can perform actions and access resources. This entity is typically a root user for an AWS account, an IAM role, or a user. For more information, see *Principal* in Roles terms and concepts in the IAM documentation.

Privacy by Design

An approach in system engineering that takes privacy into account throughout the whole engineering process.

private hosted zones

A container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains within one or more VPCs. For more information, see Working with private hosted zones in the Route 53 documentation.

proactive control

A security control designed to prevent the deployment of noncompliant resources. These controls scan resources before they are provisioned. If the resource is not compliant with the control, then it isn't provisioned. For more information, see the Controls reference guide in the AWS Control Tower documentation and see Proactive controls in *Implementing security controls on AWS*.

product lifecycle management (PLM)

The management of data and processes for a product throughout its entire lifecycle, from design, development, and launch, through growth and maturity, to decline and removal.

production environment

See environment.

programmable logic controller (PLC)

In manufacturing, a highly reliable, adaptable computer that monitors machines and automates manufacturing processes.

pseudonymization

The process of replacing personal identifiers in a dataset with placeholder values. Pseudonymization can help protect personal privacy. Pseudonymized data is still considered to be personal data.

publish/subscribe (pub/sub)

A pattern that enables asynchronous communications among microservices to improve scalability and responsiveness. For example, in a microservices-based MES, a microservice can publish event messages to a channel that other microservices can subscribe to. The system can add new microservices without changing the publishing service.

Q

query plan

A series of steps, like instructions, that are used to access the data in a SQL relational database system.

query plan regression

When a database service optimizer chooses a less optimal plan than it did before a given change to the database environment. This can be caused by changes to statistics, constraints, environment settings, query parameter bindings, and updates to the database engine.

R

RACI matrix

See responsible, accountable, consulted, informed (RACI).

ransomware

A malicious software that is designed to block access to a computer system or data until a payment is made.

RASCI matrix

See responsible, accountable, consulted, informed (RACI).

RCAC

See row and column access control.

read replica

A copy of a database that's used for read-only purposes. You can route queries to the read replica to reduce the load on your primary database.

re-architect

See 7 Rs.

recovery point objective (RPO)

The maximum acceptable amount of time since the last data recovery point. This determines what is considered an acceptable loss of data between the last recovery point and the interruption of service.

recovery time objective (RTO)

The maximum acceptable delay between the interruption of service and restoration of service.

refactor

See 7 Rs.

Region

A collection of AWS resources in a geographic area. Each AWS Region is isolated and independent of the others to provide fault tolerance, stability, and resilience. For more information, see Specify which AWS Regions your account can use.

regression

An ML technique that predicts a numeric value. For example, to solve the problem of "What price will this house sell for?" an ML model could use a linear regression model to predict a house's sale price based on known facts about the house (for example, the square footage).

rehost

See 7 Rs.

release

In a deployment process, the act of promoting changes to a production environment.

relocate

See 7 Rs.

replatform

See 7 Rs.

repurchase

See 7 Rs.

resiliency

An application's ability to resist or recover from disruptions. High availability and disaster recovery are common considerations when planning for resiliency in the AWS Cloud. For more information, see AWS Cloud Resilience.

resource-based policy

A policy attached to a resource, such as an Amazon S3 bucket, an endpoint, or an encryption key. This type of policy specifies which principals are allowed access, supported actions, and any other conditions that must be met.

responsible, accountable, consulted, informed (RACI) matrix

A matrix that defines the roles and responsibilities for all parties involved in migration activities and cloud operations. The matrix name is derived from the responsibility types defined in the

matrix: responsible (R), accountable (A), consulted (C), and informed (I). The support (S) type is optional. If you include support, the matrix is called a *RASCI matrix*, and if you exclude it, it's called a *RACI matrix*.

responsive control

A security control that is designed to drive remediation of adverse events or deviations from your security baseline. For more information, see Responsive controls in *Implementing security controls on AWS*.

retain

See 7 Rs.

retire

See 7 Rs.

rotation

The process of periodically updating a secret to make it more difficult for an attacker to access the credentials.

row and column access control (RCAC)

The use of basic, flexible SQL expressions that have defined access rules. RCAC consists of row permissions and column masks.

RPO

See recovery point objective.

RTO

See recovery time objective.

runbook

A set of manual or automated procedures required to perform a specific task. These are typically built to streamline repetitive operations or procedures with high error rates.

S

SAML 2.0

An open standard that many identity providers (IdPs) use. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS API

operations without you having to create user in IAM for everyone in your organization. For more information about SAML 2.0-based federation, see About SAML 2.0-based federation in the IAM documentation.

SCADA

See supervisory control and data acquisition.

SCP

See service control policy.

secret

In AWS Secrets Manager, confidential or restricted information, such as a password or user credentials, that you store in encrypted form. It consists of the secret value and its metadata. The secret value can be binary, a single string, or multiple strings. For more information, see What's in a Secrets Manager secret? in the Secrets Manager documentation.

security control

A technical or administrative guardrail that prevents, detects, or reduces the ability of a threat actor to exploit a security vulnerability. There are four primary types of security controls: preventative, detective, responsive, and proactive.

security hardening

The process of reducing the attack surface to make it more resistant to attacks. This can include actions such as removing resources that are no longer needed, implementing the security best practice of granting least privilege, or deactivating unnecessary features in configuration files.

security information and event management (SIEM) system

Tools and services that combine security information management (SIM) and security event management (SEM) systems. A SIEM system collects, monitors, and analyzes data from servers, networks, devices, and other sources to detect threats and security breaches, and to generate alerts.

security response automation

A predefined and programmed action that is designed to automatically respond to or remediate a security event. These automations serve as detective or responsive security controls that help you implement AWS security best practices. Examples of automated response actions include modifying a VPC security group, patching an Amazon EC2 instance, or rotating credentials.

server-side encryption

Encryption of data at its destination, by the AWS service that receives it.

service control policy (SCP)

A policy that provides centralized control over permissions for all accounts in an organization in AWS Organizations. SCPs define guardrails or set limits on actions that an administrator can delegate to users or roles. You can use SCPs as allow lists or deny lists, to specify which services or actions are permitted or prohibited. For more information, see Service control policies in the AWS Organizations documentation.

service endpoint

The URL of the entry point for an AWS service. You can use the endpoint to connect programmatically to the target service. For more information, see AWS service endpoints in *AWS General Reference*.

service-level agreement (SLA)

An agreement that clarifies what an IT team promises to deliver to their customers, such as service uptime and performance.

service-level indicator (SLI)

A measurement of a performance aspect of a service, such as its error rate, availability, or throughput.

service-level objective (SLO)

A target metric that represents the health of a service, as measured by a service-level indicator.

shared responsibility model

A model describing the responsibility you share with AWS for cloud security and compliance. AWS is responsible for security *of* the cloud, whereas you are responsible for security *in* the cloud. For more information, see Shared responsibility model.

SIEM

See security information and event management system.

single point of failure (SPOF)

A failure in a single, critical component of an application that can disrupt the system.

SLA

See service-level agreement.

SLI

See service-level indicator.

SLO

See service-level objective.

split-and-seed model

A pattern for scaling and accelerating modernization projects. As new features and product releases are defined, the core team splits up to create new product teams. This helps scale your organization's capabilities and services, improves developer productivity, and supports rapid innovation. For more information, see Phased approach to modernizing applications in the AWS Cloud.

SPOF

See single point of failure.

star schema

A database organizational structure that uses one large fact table to store transactional or measured data and uses one or more smaller dimensional tables to store data attributes. This structure is designed for use in a data warehouse or for business intelligence purposes.

strangler fig pattern

An approach to modernizing monolithic systems by incrementally rewriting and replacing system functionality until the legacy system can be decommissioned. This pattern uses the analogy of a fig vine that grows into an established tree and eventually overcomes and replaces its host. The pattern was introduced by Martin Fowler as a way to manage risk when rewriting monolithic systems. For an example of how to apply this pattern, see Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

subnet

A range of IP addresses in your VPC. A subnet must reside in a single Availability Zone.

supervisory control and data acquisition (SCADA)

In manufacturing, a system that uses hardware and software to monitor physical assets and production operations.

symmetric encryption

An encryption algorithm that uses the same key to encrypt and decrypt the data.

synthetic testing

Testing a system in a way that simulates user interactions to detect potential issues or to monitor performance. You can use Amazon CloudWatch Synthetics to create these tests.

T

tags

Key-value pairs that act as metadata for organizing your AWS resources. Tags can help you manage, identify, organize, search for, and filter resources. For more information, see Tagging your AWS resources.

target variable

The value that you are trying to predict in supervised ML. This is also referred to as an *outcome variable*. For example, in a manufacturing setting the target variable could be a product defect.

task list

A tool that is used to track progress through a runbook. A task list contains an overview of the runbook and a list of general tasks to be completed. For each general task, it includes the estimated amount of time required, the owner, and the progress.

test environment

See environment.

training

To provide data for your ML model to learn from. The training data must contain the correct answer. The learning algorithm finds patterns in the training data that map the input data attributes to the target (the answer that you want to predict). It outputs an ML model that captures these patterns. You can then use the ML model to make predictions on new data for which you don't know the target.

transit gateway

A network transit hub that you can use to interconnect your VPCs and on-premises networks. For more information, see What is a transit gateway in the AWS Transit Gateway documentation.

trunk-based workflow

An approach in which developers build and test features locally in a feature branch and then merge those changes into the main branch. The main branch is then built to the development, preproduction, and production environments, sequentially.

trusted access

Granting permissions to a service that you specify to perform tasks in your organization in AWS Organizations and in its accounts on your behalf. The trusted service creates a service-linked role in each account, when that role is needed, to perform management tasks for you. For more information, see Using AWS Organizations with other AWS services in the AWS Organizations documentation.

tuning

To change aspects of your training process to improve the ML model's accuracy. For example, you can train the ML model by generating a labeling set, adding labels, and then repeating these steps several times under different settings to optimize the model.

two-pizza team

A small DevOps team that you can feed with two pizzas. A two-pizza team size ensures the best possible opportunity for collaboration in software development.

U

uncertainty

A concept that refers to imprecise, incomplete, or unknown information that can undermine the reliability of predictive ML models. There are two types of uncertainty: *Epistemic uncertainty* is caused by limited, incomplete data, whereas *aleatoric uncertainty* is caused by the noise and randomness inherent in the data. For more information, see the Quantifying uncertainty in deep learning systems guide.

undifferentiated tasks

Also known as *heavy lifting*, work that is necessary to create and operate an application but that doesn't provide direct value to the end user or provide competitive advantage. Examples of undifferentiated tasks include procurement, maintenance, and capacity planning.

upper environments

See environment.

V

vacuuming

A database maintenance operation that involves cleaning up after incremental updates to reclaim storage and improve performance.

version control

Processes and tools that track changes, such as changes to source code in a repository.

VPC peering

A connection between two VPCs that allows you to route traffic by using private IP addresses. For more information, see What is VPC peering in the Amazon VPC documentation.

vulnerability

A software or hardware flaw that compromises the security of the system.

W

warm cache

A buffer cache that contains current, relevant data that is frequently accessed. The database instance can read from the buffer cache, which is faster than reading from the main memory or disk.

warm data

Data that is infrequently accessed. When querying this kind of data, moderately slow queries are typically acceptable.

window function

A SQL function that performs a calculation on a group of rows that relate in some way to the current record. Window functions are useful for processing tasks, such as calculating a moving average or accessing the value of rows based on the relative position of the current row.

workload

A collection of resources and code that delivers business value, such as a customer-facing application or backend process.

workstream

Functional groups in a migration project that are responsible for a specific set of tasks. Each workstream is independent but supports the other workstreams in the project. For example, the portfolio workstream is responsible for prioritizing applications, wave planning, and collecting migration metadata. The portfolio workstream delivers these assets to the migration workstream, which then migrates the servers and applications.

WORM

See write once, read many.

WQF

See AWS Workload Qualification Framework.

write once, read many (WORM)

A storage model that writes data a single time and prevents the data from being deleted or modified. Authorized users can read the data as many times as needed, but they cannot change it. This data storage infrastructure is considered immutable.

Z

zero-day exploit

An attack, typically malware, that takes advantage of a zero-day vulnerability.

zero-day vulnerability

An unmitigated flaw or vulnerability in a production system. Threat actors can use this type of vulnerability to attack the system. Developers frequently become aware of the vulnerability as a result of the attack.

zombie application

An application that has an average CPU and memory usage below 5 percent. In a migration project, it is common to retire these applications.