AWS Organizational Change Acceleration (OCA) 6-Point Framework – 4. Engage the Organization

AWS Prescriptive Guidance

AWS Prescriptive Guidance: AWS Organizational Change Acceleration (OCA) 6-Point Framework – 4. Engage the Organization

Table of Contents

AWS Organizational Change Acceleration (OCA) 6-Point Framework – 4. Engage the Organization

Amazon Web Services ([contributors](#))

February 2025 ([document history](#))

The AWS Organizational Change Acceleration (OCA) 6-Point Framework is intended to cover the full scope of people-related issues and challenges throughout the lifecycle of a cloud transformation, which might include migration, modernization, generative AI scaling, and innovation. This framework guides customer adoption of AWS technologies, processes, and new ways of working by:

- Identifying, aligning, and mobilizing key leaders

- Assessing and mitigating the organizational impacts of cloud transformation

- Designing change acceleration, communications, and training plans

- Developing leadership, sponsorship, and culture strategies

The framework's six points align with an agile sprint cadence, from program initiation through sustainable long-term change. The following diagram shows these six points and their subpoints.
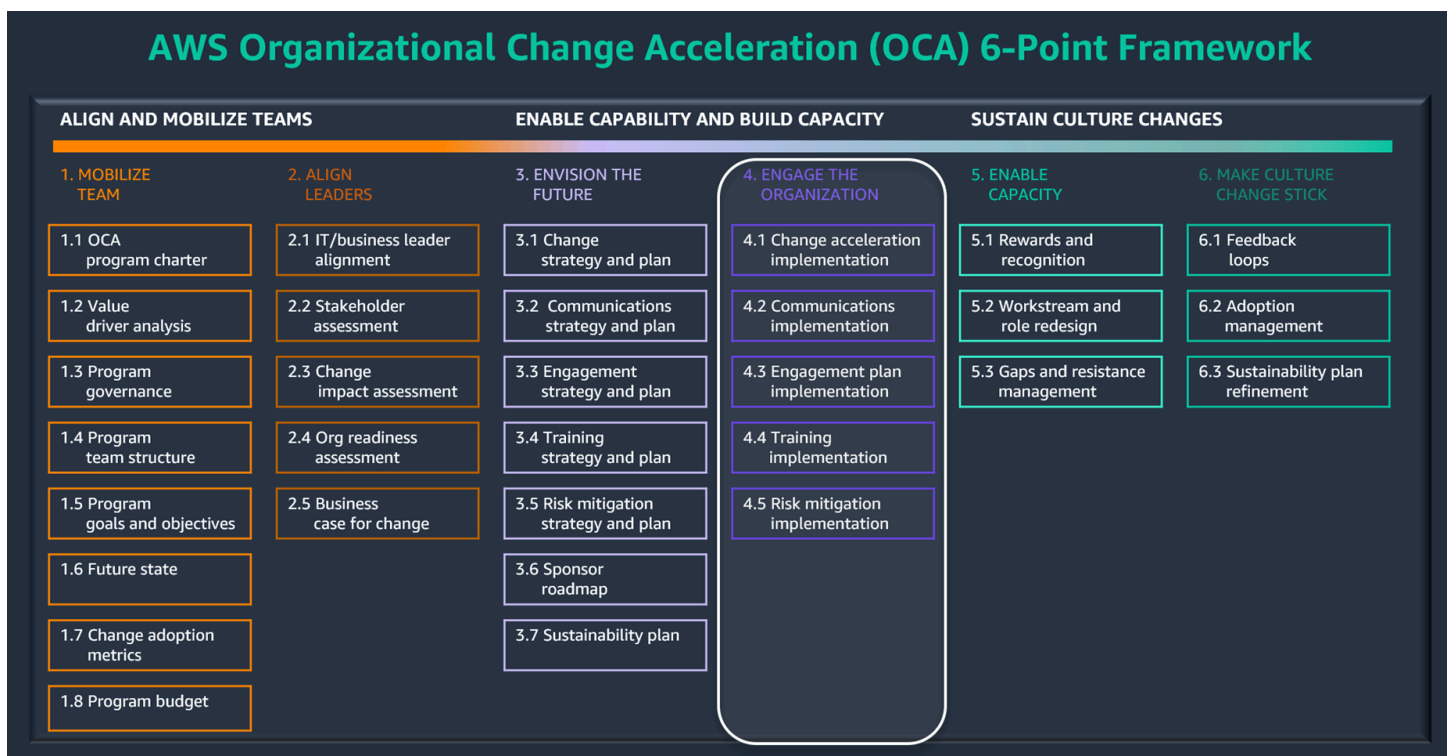
The fourth point, *Engage the Organization*, helps you activate the strategies and plans created in the previous three points and use the insights gained from various assessments to actively transform the organization to the desired future state. As the transformation starts to take place, the burden begins to shift from the cloud transformation team and cross-functional leaders to the employee base. *Engage the Organization* contains five subpoints:

4.1 Change acceleration implementation. Implement the change strategy and plan to enable cloud adoption and achieve desired business outcomes.

4.2 Communications implementation. Implement the communications strategy and plan to address ongoing communications needs as the cloud strategy is implemented.

4.3 Engagement plan implementation. Implement stakeholder-specific plans to address changes that are required to successfully apply the cloud strategy and realize business value from the cloud.

4.4 Training implementation. Implement the training strategy and plan to holistically prepare affected stakeholder groups to proficiently perform future-state cloud activities.

4.5 Risk mitigation implementation. Proactively identify and manage people-related risks that can impact timely business outcomes.

This guide discusses each subpoint of *Engage the Organization* in detail.

Intended audience

This guide targets leaders who are responsible for accelerating cloud transformation. Following these recommendations will help minimize risks and maximize value.

Targeted business outcomes

The *Engage the Organization* phase of the AWS OCA 6-Point Framework contributes to the following outcomes:

- **Value realization and return on investment (ROI)**: This OCA phase focuses on implementing strategies that speed up cloud adoption. These strategies align with both the overall cloud plan and business goals to ensure maximum value from cloud investments.
- **Transformational leadership**: Leadership is aligned and mobilized for accelerating cloud transformation.
- **Cloud acceleration**: The OCA workstream establishes the direction, metrics, governance, and program budget required to quickly mobilize resources to accelerate cloud transformation.
- **Organizational alignment**: The OCA workstream works with leaders to set clear business objectives and goals, and aligns organizational entities and performance levers.
- **Engaged workforce:** The OCA workstream creates strategies to actively involve employees in the cloud transformation process, and to develop their digital acumen and capabilities.
- **Future-ready workforce:** The OCA workstream modernizes roles and enables the workforce to work autonomously and drive key cloud-enabled capabilities.

By effectively implementing the *Engage the Organization* activities, organizations can realize tangible improvements in speed, agility, innovation, and business value from their cloud transformation.

About the OCA 6-Point Framework guides

This guide is part of a set of publications that cover the OCA 6-Point Framework, which is a programmatic and evidence-based organizational change adoption framework.

The content set includes a comprehensive set of templates, guidelines, supporting artifacts, assessments, accelerators, and tools that are designed to accelerate cloud transformation. We

recommend that you start with the overview to understand the framework and its six points, and then consult the following individual guides for detailed discussions of each point.

1. Mobilize Team
2. Align Leaders
3. Envision the Future
4. Engage the Organization (this guide)
5. Enable Capacity
6. Make Culture Change Stick

For a comprehensive set of cloud transformation strategies, guidance, and resources, see Accelerating cloud transformation.
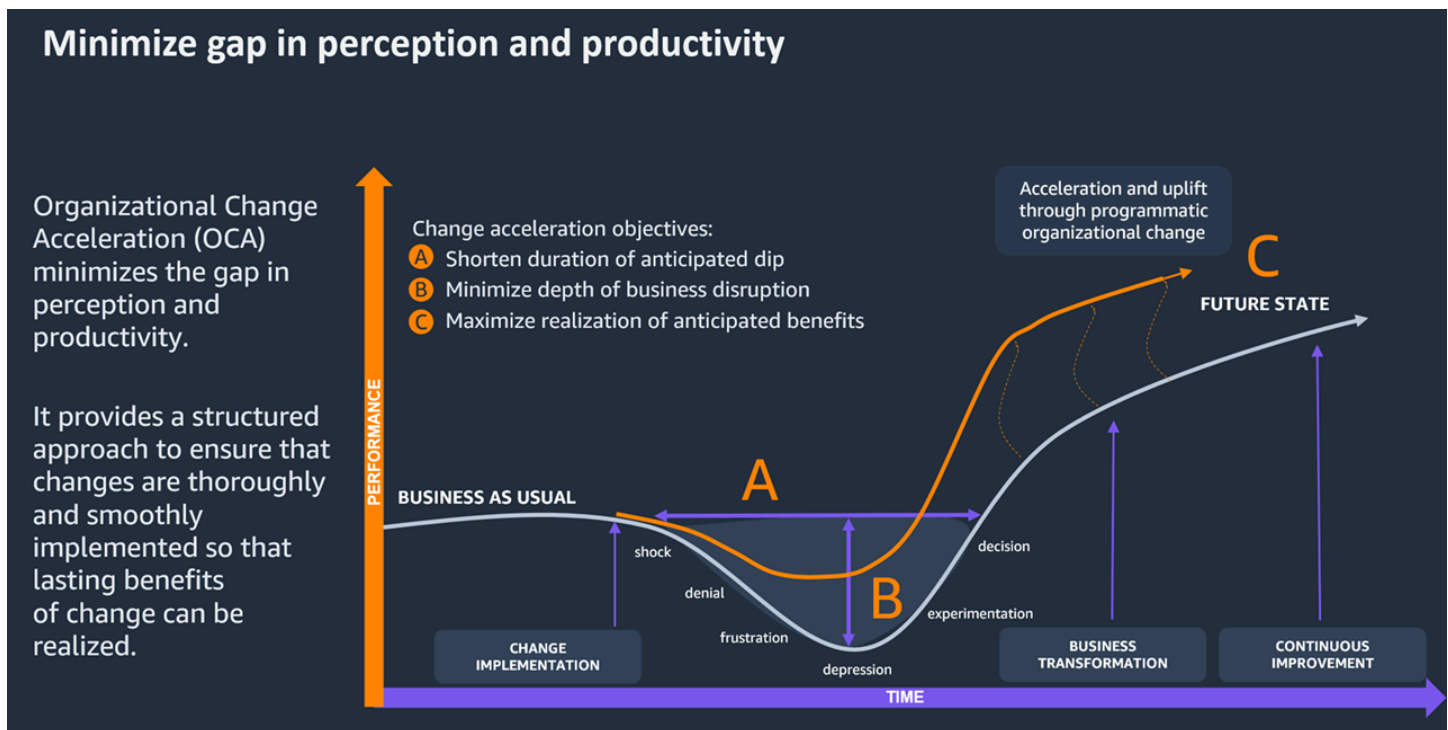
4.1 Change acceleration implementation

Overview

The objective of this activity is to launch the activities set forth in the change strategy and plan (see Envision the Future, 3.1). A change strategy and plan provide a thoughtful, structured, programmatic approach to delivering the right change tactics to the right people at the right time throughout the course of the cloud transformation. They outline a comprehensive approach to ensure that changes introduced to the organization as a result of the cloud are accepted by leaders, employees, and other stakeholders with minimal disruption and maximum results. They provide a systematic mechanism for adjusting the application of tools, technologies, processes, or skills during a project or initiative. They describe the specific ways in which the organization will address changes in the way it operates its business, technology, supply chain, organizational structure, or project scope. The change strategy provides direction and results in informed decision-making throughout the cloud transformation process.

In the change acceleration implementation activity, the focus of the OCA team is to work closely with all cloud workstreams and stakeholders to implement the elements of that strategy and plan in a programmatic, rhythmic timeline that lasts the life of the program, and accelerates and decelerates with the various milestones over time.

Change can be highly disruptive to an organization and will affect both the cloud transformation and the surrounding environment over time. For example, new leaders might emerge or join, and others might retire or leave. New business transactions such as mergers, acquisitions, and divestitures might take place that cause the cloud transformation to accelerate, pause, or change scope.

The following diagram illustrates how OCA can minimize the gap in perception and productivity during change acceleration.

Minimize gap in perception and productivity

Organizational Change Acceleration (OCA) minimizes the gap in perception and productivity.

It provides a structured approach to ensure that changes are thoroughly and smoothly implemented so that lasting benefits of change can be realized.

Change acceleration objectives:
- A Shorten duration of anticipated dip
- B Minimize depth of business disruption
- C Maximize realization of anticipated benefits

Best practices

Key best practices for the implementation of change acceleration include the following:

- For each major milestone, describe how the changes will impact the organization and who will be affected. These changes might include data center exits, deployments of new solutions and features, and establishing a Cloud Center of Excellence (CCOE).

- Create a plan for stakeholders to recognize when a change is needed, and how to mitigate impacts to their workforce.

- Follow the defined process or mechanism for implementing, approving, and monitoring changes to make sure that they have the desired effect.

- Regularly review and update both the strategic vision and business case for cloud transformation. This ensures that messaging remains consistent, relevant, and aligned with changing business conditions.

- Interview key leaders who join the organization, and identify impacted stakeholders for all key milestones early in the planning process. Periodically assess their alignment throughout the life of the program.

- Continuously integrate partners who join the broader cloud transformation program team to ensure consistent objectives and key results (OKRs), timelines, and motivations.

- Continuously partner with enabling functions that can prove helpful when they are engaged, and can cause timing and budgetary delays when they're not engaged. For example, these functions might include human resources, training, finance, cross-functional leaders, line of business leaders, and other partners or vendors who are directly or indirectly impacted. Plan to speak to these stakeholders at least quarterly. At the minimum, provide a program update and show them that you value their input. A few action items or insights will typically result that might derail plans if they aren't proactively addressed.

Change acceleration checklist

Creating a change acceleration checklist of activities can be helpful to see if your change strategy and plan (and associated user stories) are comprehensive and robust. The following table provides a list to get you started.

Area	OCA 6-Point Framework reference	Actions
Project management	Engage the Organization, 1.5 Program goals and objectives	- Ensure close integration and participation in weekly meetings for the cloud transformation project (for example, sprint ceremonies, backlog planning meetings, and launch readiness planning sessions). - Update the risk management and mitigation log for change acceleration risks every week. - Update the change acceleration reporting scorecard and status reports every week (or for each sprint).

Area	OCA 6-Point Framework reference	Actions
Leadership alignment and stakeholder analysis	[Align Leaders, 2.1 IT and business leader alignment](#) [Align Leaders, 2.2 Stakeholder assessment](#)	- Prepare the stakeholder analysis approach. - Identify leaders to interview. - Conduct stakeholder interviews and analysis activities. - Present findings to the leadership team. - Insert risk findings into the risk management and mitigation log. - Update and maintain the stakeholder matrix. - Use the stakeholder matrix as an input to persona-based change impacts, communications, and training.
Change impact assessment	[Align Leaders, 2.3 Change impact assessment](#)	- Assess change impacts and document them. - Determine the appropriate interventions to manage and mitigate impacts to user groups, timelines, data center exits, product launches, and other important milestones.

Area	OCA 6-Point Framework reference	Actions
Risk management and mitigation	Envision the Future, 3.5 Risk mitigation strategy and plan Engage the Organization, 4.5 Risk mitigation implementation	- Prepare the change risk assessment approach. - Conduct risk assessment activities such as interviews, focus groups, and surveys. - Analyze and present findings to the leadership team. - Assign and mitigate risks and issues according to risk management guidelines. - Update the change acceleration plan and stakeholder engagement plans as needed.

Area	OCA 6-Point Framework reference	Actions
Sponsor roadmap	Envision the Future, 3.6 Sponsor roadmap	- Prepare the sponsor approach. - Prepare the materials for sponsors, such as key messages, FAQ, timelines, and roadshow presentations, according to the leadership action plan. - Identify sponsors and leaders. - Engage and onboard sponsors and leaders. - Monitor and measure the progress of leadership action plan activities according to the sponsor roadmap. - Support sponsors and leaders as needed. Update materials and FAQ as needed.
Change acceleration plan	Envision the Future, 3.1 Change strategy and plan	Continuously monitor and measure the implementation of the change plan.

Additional steps

To get started on change acceleration implementation, do the following:

1. Review the [change strategy and plan](#) in its entirety at key milestones, such as data center exits, migrations, new solutions, business transactions (mergers, acquisitions, divestitures), leadership changes, and at a minimum once per quarter.

2. Participate in all weekly status meetings and sprint ceremonies as part of the cloud transformation integrated team.

3. Meet with stakeholders regularly as part of their leadership action plans, and update key messages, FAQ, and communications as required, to stay relevant with the current IT and business strategy.

4. Manage people-related, cultural, organizational, and political risks by using the risk management and mitigation log. Be careful to document highly sensitive issues separately and share them only with a limited audience on a need-to-know basis.

5. Review and update the cloud business case as required, and create new change acceleration activities as necessary to realize the ROI of the cloud.

6. Document and share lessons learned with the cloud transformation team and other teams within the company to create a culture of evolution, iteration, and continuous improvement.

The effective implementation of change acceleration is critical for realizing the full value of cloud transformation. By following these steps and best practices, and systematically implementing the change strategy, organizations can minimize disruption, align stakeholders, and accelerate cloud adoption to achieve their desired business outcomes.

4.2 Communications implementation

Overview

Effective communication is crucial for driving cloud adoption and achieving business outcomes. This section focuses on implementing the communications strategy and plan ([Envision the Future, 3.2](#)). The objective of communications implementation is to launch the activities that were agreed upon in the communications strategy and plan. This ensures that all affected stakeholders understand the reasons, benefits, stakeholders, and timeline of the cloud transformation. Effective communication focuses on benefits and business value, and sustains overall stakeholder engagement throughout the transformation.

Best practices

Assumptions

- The [communications strategy and plan](#) has been validated and approved by the cloud leadership team, executive sponsor, HR team, and the internal communications team (if applicable).

- The stakeholder analysis step is complete, and the stakeholder metrics are current.

Focus areas

The activities in this phase focus on the communications part of the change strategy during the cloud transformation process, specifically:

- Communications setup

- Media analysis

- Key messaging (case for change)

- Communications development

- Communications deployment

- Communications monitoring

Maintaining leadership sponsorship

It is critical to secure commitment from the executive sponsor and leaders throughout the implementation of communication activities to maintain focus on the benefits and business value and sustain overall stakeholder engagement.

Communications implementation checklist

If you're new to this process, you can use the following checklist as a reference guide throughout the cloud transformation process.

> **ⓘ Note**
>
> This is only a representative list of communications-related tasks and not exhaustive. A comprehensive list should be included in the communications plan.

Area	Actions
Setup	- Develop the theme and brand for the project or program. - Obtain approval for the final theme and brand. - Incorporate a visual identity into the project's standard templates.
Media analysis	- Conduct a communications audit or assessment. - Analyze results (for example, through a media analysis). - Update the communications assessment report.
Key messaging	- Determine the key organizational message set. - Organize messages by category (consider timing frequency and channels).

Area	Actions
	- Determine initial communication needs and key messages. This is tied to the case for change. - Determine the channel and sender for initial communications. - Use the stakeholder matrix. - Align sponsors and leadership with communication deployment activities.
Communications development	- Outline the drafting, review, approval, and distribution process for communicating key messages with target audiences. - Identify roles and responsibilities, including the reporting hierarchy for drafting, review, and final approval. - Establish an internal team communications process (such as weekly meetings). - Develop communications process flows. - Develop a communications production checklist. - Develop and obtain necessary approval of communications drafts. - Manage the communications production process.
Communications deployment	- Socialize the communications deployment timeline with the executive sponsor and key stakeholders. - Ensure awareness and alignment with leadership teams and communications champions. - Deliver final communications.

Area	Actions
Communications monitoring	- Implement a feedback mechanism. - Review information gathered from feedback mechanisms. - Update communications materials (such as presentations and FAQ) with revised information.

Additional steps

To begin implementing the communications plan:

1. Verify that the [communications strategy and plan](#) have been validated and approved.
2. Validate the communications checklist.
3. Establish monitoring mechanisms.

The effective implementation of the communications plan is critical for driving cloud adoption and achieving desired business outcomes. By following these best practices, using the provided checklist, and maintaining ongoing leadership support, organizations can ensure that stakeholders remain informed, engaged, and committed throughout the cloud transformation process.

4.3 Engagement plan implementation

Overview

An engagement plan describes specific ways in which an individual, stakeholder group, or organization will address changes brought forth by the cloud transformation. The implementation of the engagement plan is to keep all key stakeholders committed to, and focused on, the desired business results of the cloud transformation. Each stakeholder group should be addressed and engaged with relevant information according to their prioritization and mapping in the commitment model, as outlined in the engagement strategy and plan (Envision the Future, 3.3).

The OCA team's focus is to secure commitment from designated leaders and champions in the implementation of engagement tasks.

Best practices

Assumptions

- The engagement strategy and plan have been validated and approved by the cloud leadership team, the executive sponsor, the HR team, and the internal communications team.

- Leaders and champions have been involved in the planning phase. They have been adequately onboarded, they accept the plan, and they are committed to participating in its implementation.

Focus areas

The areas of focus in this workstream include:

- Engagement setup

- Engagement plan development

- Engagement plan deployment

- Monitoring and reporting

Engagement activities checklist

You can use the following engagement plan checklist as a reference guide throughout the cloud transformation process.

> ⓘ **Note**
>
> This isn't an exhaustive list of activities. It is only a sample of tasks that should be included in the engagement plan.

Area	Actions
Setup	• Validate stakeholder groups according to the engagement strategy and stakeholder assessment. • Align activities by stages of engagement (for example, focus groups, informal presentations, webinars, and town halls). • Identify and onboard owners and champions. • Assign owners and champions to stakeholder groups.
Plan development	• Develop a core presentation deck that provides key information about the cloud transformation for all audiences. • Submit the core presentation deck to the leadership team for their approval. • Sign off on the core presentation deck. • Develop specific materials (for example, overview, impact information, key benefits by stakeholder group, timing information, training information) for targeted audience groups.

Area	Actions
	• Review and approve materials with subject matter experts (SMEs) for each area. • Obtain signoff on these materials. • Upload the materials to the project library or knowledge repository.
Plan deployment	• Review materials with SMEs and champions. • Determine delivery formats (for example, face-to-face or virtual). • Review timing of activities with leaders and champions. • Schedule events and activities. • Notify participants. • Conduct engagement sessions such as focus groups, department meetings, informal gatherings, webinars, and demonstrations.
Monitoring and reporting	• Monitor the implementation of engagement activities. • Capture attendance and questions; conduct feedback evaluations. • Update the engagement materials with feedback as necessary. • Update the engagement report or scorecard.

Additional steps

To begin implementing the engagement plan, follow these steps:

1. Confirm that the engagement strategy and plan have been validated and approved.

2. Verify that the engagement activities checklist has been validated and approved.

3. Make sure that monitoring and reporting mechanisms (such as status reports, dashboard of success metrics, and OKRs) are in place.

The effective implementation of the engagement plan is critical for driving cloud adoption and achieving desired business outcomes. By following these best practices, using the provided checklist, and maintaining ongoing stakeholder engagement, organizations can ensure that all key stakeholders remain committed and focused on the cloud transformation process. This ultimately leads to the successful adoption and realization of your business outcomes.

4.4 Training implementation

Overview

Training implementation is about launching the activities set forth in the training strategy and plan (Envision the Future, 3.4), which provide the structure and focus for identifying training that needs to be delivered, and the process for developing and delivering the training program. When you implement the training strategy and plan, consider delivering a training effort that is consistent with the training your organization typically conducts. Meaningful training that is not disruptive to an employee's accustomed workflow decreases resistance and helps employees respond readily to change. Additionally, using a data-driven approach to gather training preferences from the AWS Learning Needs Analysis (LNA) tool and applying those preferences to the training plan help you obtain the buy-in and desire to complete training from employees.

Best practices

The change acceleration team should focus on quickly assessing developmental and training needs, identifying training gaps, aligning with existing training practices, and delivering training to support the future state model.

Assumptions

- The training strategy and plan have been validated and approved by the cloud leadership team, the executive sponsor, the learning and development (L&D) team, the HR team, and the internal communications team.

- Leaders and champions have been involved in the training planning phase and are committed to participating in training activities according to the plan.

- The training strategy and plan take the full cloud transformation plan and roadmap into account, and mitigate any SME bandwidth.

- Any courses that are not part of the AWS Training and Certification course curriculum will be assigned to stakeholders and customized for each stakeholder group.

Focus areas

This workstream focuses on the following areas:

- AWS Learning Needs Analysis (LNA)

- Training setup

- Training development (for custom needs and non-AWS learning curriculum)

- Training deployment

- Monitoring and reporting

Training plan checklist

Use the following checklist as a reference guide throughout your organization's cloud transformation process.

> (i) **Note**
>
> The following checklist is not an exhaustive list, but it represents the activities that you would typically find in a training plan. Your validated and approved training strategy and plan should include the full list of training activities.

Area	Actions
AWS Learning Needs Analysis (LNA)	- Identify the executive sponsor and provide the team structure. - Create a survey and provide the preview URL. - Review the survey with the executive sponsor and get their approval. - Confirm survey distribution logistics. - Distribute the survey to employees. - Provide survey response numbers. - Send reminder email to complete the survey. - Close the survey on the planned date.

Area	Actions
	• Create a report and provide training recommendations.
Training setup	• Validate the training strategy and plan, and ensure alignment with key cloud milestones such as migration wave plans. • Create a training materials template (if needed) for non-AWS training courses. Validate AWS training courses based on the AWS LNA report. • Sign off on training materials and non-AWS training courses (if applicable). • Identify training needs by stakeholder group or cloud role (for example, engineers, developers, solutions architects, operations). • Onboard stakeholder groups to training plan. • Create the training curriculum. • Obtain approval and signoff on the training curriculum. • Develop the training production checklist. • Identify and onboard training developers (instructional designers) for non-AWS training courses. • Identify training material reviewers.
Training development	• Assign stakeholder groups to training courses. • Develop draft training materials. • Review and approve training materials. • Upload materials to a library or knowledge repository.

Area	Actions
Training deployment	- Draft the training calendar. - Obtain approval and signoff on the training calendar. - Schedule training events, including specific AWS instructor-led trainings (ILTs). - Identify training participants based on the migration wave plan. - Enroll and notify training participants. - Conduct and support training activities.
Monitoring and reporting	- Monitor the implementation of training development and deployment activities. - Capture attendance, questions, and feedback evaluations. - Update training materials based on feedback as necessary. - Update the training development and deployment report or scorecard.

For more information, see AWS Learning Needs Analysis.

Additional steps

To begin the implementation of the training plan, make sure that:

1. The AWS LNA has been conducted and insights have been included in the training strategy and plan.

2. The training strategy and plan have been validated and approved.

3. The training activities checklist has been validated and approved.

4. Monitoring and reporting mechanisms are in place.

The effective implementation of the training plan is critical for driving cloud adoption and achieving desired business outcomes. By following these best practices, using the AWS LNA, and implementing a comprehensive training plan, organizations can ensure that their workforce is properly skilled and prepared for the cloud transformation. This accelerates adoption and also maximizes the value realized from the cloud investment.

4.5 Risk mitigation implementation

Overview

The objective of this activity is to launch the activities set forth in the risk mitigation strategy and plan (Envision the Future, 3.5). The focus of the OCA team is to work closely with all cloud workstreams to assess and analyze risks, formulate a solution or mitigation plan, assign ownership, and address the risk for closure. The resolution of risks requires commitment and close alignment with executive sponsors, leaders, and champions, as well as a disciplined approach to managing, mitigating, and monitoring people-related risks throughout the program lifecycle, and integrating this process with all other workstreams in the cloud transformation program.

Best practices

The risks that you track across your cloud transformation program should be logged in a risk tracking tool, as discussed in *Envision the Future*, 3.5 Risk mitigation strategy and plan. The following table provides an example of such a tool.

Risk category	Severity	Probability	Risk description	Mitigation actions	Owner	Status	Due date
Resourcing	Medium	High	Security SME is taking a leave of absence that overlaps with our testing and cutover phase.	Onboard and train backup security SME on specific tests and cutover planning.	Martha Rivera	In progress	31 March 2025

Focus areas

Risk mitigation implementation can be organized into the following five phases:

- Planning and setup

- Identification and analysis

- Assignment and resolution

- Monitoring and reporting

- Continuous improvement

Risk mitigation plan checklist

Use the following checklist as a reference guide throughout your organization's cloud
transformation process.

> ⓘ **Note**
>
> The following checklist is not an exhaustive list, but it represents the activities that you
> would typically find in a risk mitigation plan. Your validated and approved risk mitigation
> strategy and plan should include the full list of training activities.

Area	Actions
Planning and setup	- Review the cloud strategy and plan for desired outcomes and timelines. - Align with the cloud project manager on the overall issue and risk mitigation process. - Create a template for the risk management tracking tool. - Obtain signoff on the risk management tracking tool template. - Identify SMEs or champions for risk management activities.

Area	Actions
	• Onboard SMEs or champions on OCA solution tactics and communications. • Secure OCA team participation in weekly project status meetings.
Identification and analysis	• Determine if the identified risk is a people-related issue. • If yes, identify the groups and stakeholders who are impacted. • Categorize each risk into an area such as change leadership, vision and clarity, organizational impact, retention and engagement, skills and capability, and commitment. • Identify the appropriate OCA solution tactics (for example, more information and communications, additional training, scenario and hands-on demonstrations).
Assignment and resolution	• Make a specific OCA team member responsible for addressing and resolving each identified risk. • Coordinate the timeframe for the solution or mitigation event. • Schedule the solution or mitigation event.

Area	Actions
Monitoring and reporting	• Monitor the implementation of solution or mitigation activities. • Evaluate the risk management tracker for common root causes. • When reviewing the risk management tracker, capture attendance, questions, and feedback evaluations. • Update presentation materials with feedback as necessary. • Update the risk mitigation tracker.
Track best practices and lessons learned for continuous improvement	• Analyze the risk tracking tool for insights and make improvements to your organization's ongoing transformation initiatives. • Establish and share the repository of lessons learned and best practices for ongoing development, training, and growth. • Determine any patterns within the list of risks, and help accelerate other transformation initiatives. If your organization has a transformation management office (TMO) or project management office (PMO), this might be a topic of interest to those offices. • Evolve your culture by sharing best practices and lessons learned. Timely feedback and adjustments can help your organization stay agile, and ultimately save valuable time, money, and effort.

Additional steps

To ensure effective risk mitigation:

1. Make sure that the people-related risk management process is integrated with program processes such as risk, action, issue, dependency (RAID) logs.

2. As you explore people-related risks, look across the program to see how other technical, budgetary, and timing risks will impact people.

3. Implement clear monitoring and measurement processes to ensure that any and all risk mitigation efforts are working and effective.

4. Track the mitigation and closure of people-related risks over the course of the cloud program to evaluate the impact of risk mitigation on your organization's ability to achieve desired cloud outcomes.

The effective implementation of the risk mitigation plan is critical for driving cloud adoption and achieving desired business outcomes. By following these best practices, using a comprehensive risk tracking tool, and maintaining a structured approach to risk management, organizations can proactively address potential obstacles in their cloud transformation journey. This not only minimizes disruptions but also accelerates adoption and maximizes the value realized from the cloud investment.

Resources

References

- [Accelerating your return on cloud investment by adopting a strategic transformation and change methodology](#)
- [AWS Change Acceleration 6-Point Framework and Organizational Change Management Toolkit](#)
- [AWS Organizational Change Acceleration (OCA) 6-Point Framework – 1. Mobilize Team](#)
- [AWS Organizational Change Acceleration (OCA) 6-Point Framework – 2. Align Leaders](#)
- [AWS Organizational Change Acceleration (OCA) 6-Point Framework – 3. Envision the Future](#)
- [AWS Organizational Change Acceleration (OCA) 6-Point Framework – 5. Enable Capacity](#)
- [AWS Organizational Change Acceleration (OCA) 6-Point Framework – 6. Make Culture Change Stick](#)
- [AWS Cloud Adoption Framework (CAF)](#)
- [AWS Cloud Adoption Framework: People Perspective](#)
- [AWS Learning Needs Analysis (LNA)](#)

Partners

- **Accenture**
  - [Contact Partner](#)
  - [Contact the Accenture AWS Business Group](#)
  - [Future Talent Platform](#)
  - [Accenture and AWS take you further faster](#)
- **Deloitte**
  - [Contact Partner](#)
  - [AWS and Deloitte](#)
  - [Where Innovation Meets Impact](#)
- **PwC**
  - [Contact Partner](#)

- [PwC and AWS](#)

- **Slalom**

  - [Contact Partner](#)

  - [AWS and Slalom Launch Centers](#)

- **Roberts Group Consulting**

  - [Contact Partner](#)

Contributors

- Melanie Gladwell, AWS Senior Practice Manager

- Scott Watson, AWS People Transformation Lead

- Tierra Jennings-Hill, AWS People Transformation Lead

- Nicole Lenz, AWS Sales Transformation Lead

- Jermel Moody, AWS Change Acceleration Lead

- Travis McNeal, AWS Change Acceleration Lead

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
Initial publication	—	February 7, 2025

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 Bitbucket Cloud. 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, Amazon SageMaker AI 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](#).

EDI

See [electronic data interchange](#).

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.

electronic data interchange (EDI)

The automated exchange of business documents between organizations. For more information, see [What is Electronic Data Interchange](#).

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](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.

few-shot prompting

Providing an LLM with a small number of examples that demonstrate the task and desired output before asking it to perform a similar task. This technique is an application of in-context learning, where models learn from examples (*shots*) that are embedded in prompts. Few-shot prompting can be effective for tasks that require specific formatting, reasoning, or domain knowledge. See also zero-shot prompting.

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.

FM

See foundation model.

foundation model (FM)

A large deep-learning neural network that has been training on massive datasets of generalized and unlabeled data. FMs are capable of performing a wide variety of general tasks, such as understanding language, generating text and images, and conversing in natural language. For more information, see What are Foundation Models.

G

generative AI

A subset of AI models that have been trained on large amounts of data and that can use a simple text prompt to create new content and artifacts, such as images, videos, text, and audio. For more information, see What is Generative AI.

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.

golden image

A snapshot of a system or software that is used as a template to deploy new instances of that system or software. For example, in manufacturing, a golden image can be used to provision software on multiple devices and helps improve speed, scalability, and productivity in device manufacturing operations.

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.

holdout data

A portion of historical, labeled data that is withheld from a dataset that is used to train a
[machine learning](#) model. You can use holdout data to evaluate the model performance by
comparing the model predictions against the holdout data.

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 language model (LLM)

A deep learning AI model that is pretrained on a vast amount of data. An LLM can perform
multiple tasks, such as answering questions, summarizing documents, translating text into
other languages, and completing sentences. For more information, see What are LLMs.

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.

LLM

See large language model.

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

A system engineering approach that takes privacy into account through the whole development 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.

prompt chaining

Using the output of one LLM prompt as the input for the next prompt to generate better responses. This technique is used to break down a complex task into subtasks, or to iteratively refine or expand a preliminary response. It helps improve the accuracy and relevance of a model's responses and allows for more granular, personalized results.

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).

RAG

See Retrieval Augmented Generation.

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.

Retrieval Augmented Generation (RAG)

A generative AI technology in which an LLM references an authoritative data source that is outside of its training data sources before generating a response. For example, a RAG model might perform a semantic search of an organization's knowledge base or custom data. For more information, see What is RAG.

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 by design

A system engineering approach that takes security into account through the whole development process.

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.

system prompt

A technique for providing context, instructions, or guidelines to an LLM to direct its behavior. System prompts help set context and establish rules for interactions with users.

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.

zero-shot prompting

Providing an LLM with instructions for performing a task but no examples (*shots*) that can help
guide it. The LLM must use its pre-trained knowledge to handle the task. The effectiveness of
zero-shot prompting depends on the complexity of the task and the quality of the prompt. See
also few-shot prompting.

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.