



Modernizing operations in the AWS Cloud

AWS Prescriptive Guidance



AWS Prescriptive Guidance: Modernizing operations in the AWS Cloud

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Introduction

Intended audience

Objectives

Summary process

Attachments

Guidelines and steps

Discovery phase

Design phase

Implementation phase

Best practices and recommendations

AWS services for automation

Operations readiness

Operations automation

Tools integration

Operations testing

AIOps

Next steps

Resources

Contributors

Document history

1

1

1

2

2

3

3

3

4

6

6

12

15

16

18

20

22

23

24

25

Modernizing operations in the AWS Cloud

Libin Roy and Phani Lingamallu, Amazon Web Services

The process of modernizing operations in the cloud involves readiness, automation, and integration. In a migration project, these activities are commonly referred to as *operations integration (OI)*. This guide describes the OI workstream, and specifically how to incorporate tools, people, and process perspectives into various activities to build a modern cloud operating model.

Intended audience

This guide is designed for technology leaders, cloud architects, and operations teams that modernize enterprise IT on AWS. It primarily serves executives who plan cloud transformation strategies, architects who design operational models, and practitioners who implement cloud operations, including DevOps engineers, site reliability engineers (SREs), and IT service management (ITSM) professionals.

Objectives

Business objectives can be categorized as follows:

- **Operations readiness:** Understand your current IT operations and envision your future state on AWS. This involves defining a comprehensive cloud operating model that takes advantage of the latest AWS services and methodologies. For more information, see the [cloud operating model diagram](#) later in this guide.
- **Operations automation:** Make strategic investments in automation to implement an effective AWS operating model. This includes using services for automated governance, monitoring, and management, and incorporating security best practices and compliance requirements from the start. For more information, see the [Using AWS services for automation](#) section later in this guide.
- **Operations integration:** Maintain operational continuity by extending and integrating your existing IT tools with AWS services. This ensures a smooth transition while you gradually adopt cloud-native solutions. Integration should focus on creating a unified operational view across your hybrid environment. For more information, see the [Tools integration](#) section later in this guide.

Summary process

When you start the process, your operations begin in a hybrid state that balances existing systems with cloud implementations. Although full modernization in the cloud is the ultimate goal, the OI workstream ensures that you can effectively manage applications in a hybrid cloud environment by using both traditional and cloud-native tools and processes.

The primary objective of the OI workstream is to evaluate your current operational model and develop an approach to achieve a future-state operating model as you migrate to AWS by following best practices. This requires careful consideration of the interconnections between people, processes, and tools. As the workstream owner, you'll need to identify and document operational gaps in tools, processes, and people. Then you can create a prioritized implementation roadmap by comparing the current state with your desired future-state operational model.

Attachments

To access additional content that is associated with this document, download and unzip the following file:

[attachment.zip](#)

Guidelines and steps

The three primary phases during OI are discovery, design, and implementation. This section covers the inputs required from other workstreams and the outputs expected from each phase.

Discovery phase

Discovery is the first phase. It forms the basis of operations readiness. During discovery, you should:

- Hold workshop or kickoff meetings to come up with a prioritized list of operational domains that need to be modernized.
- Gather as much information as possible to get the big picture of your processes and procedures.
- Review documentation such as playbooks, runbooks, and organizational charts.
- Speak to application owners, support staff, and business owners to create a full picture of pain points.
- Review service-level agreements (SLAs), operational-level agreements (OLAs), and disaster recovery and backup strategies.
- Assess your current tooling and technology stack.
- Evaluate skill gaps and training needs.

Design phase

The design phase usually begins soon after discovery and before implementation. However, depending on your delivery methodology (for example, if you're using an agile approach), design and implementation can occur in the same sprint. During the design phase, you use insights from the discovery phase to address gaps and to refine, improve, or even eliminate existing processes and procedures. Key activities include:

- Creating specific deliverables (for example, architecture diagrams and process flows)
- Planning change management activities
- Determining risk assessment and mitigation strategies
- Planning the timeline and resource allocation

Implementation phase

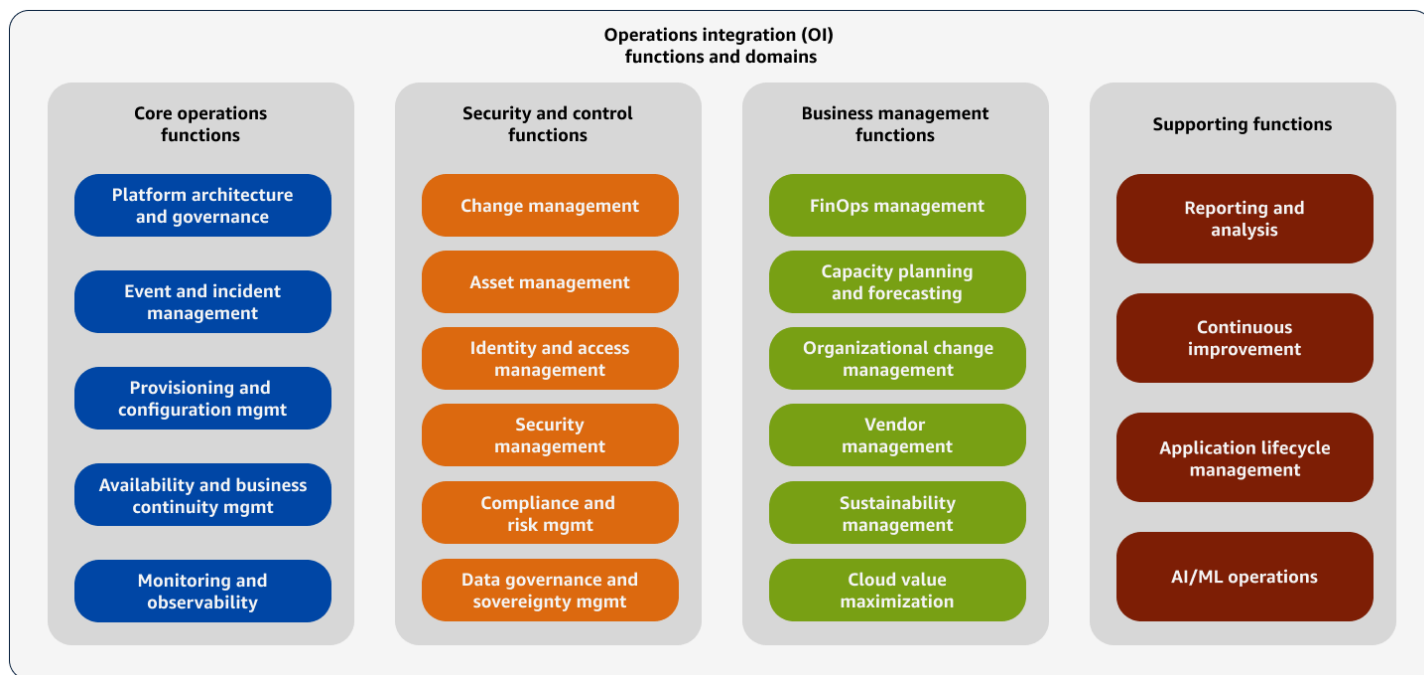
Implementation can begin in parallel with the design phase depending on your delivery methodology (for example, agile). During the implementation phase, focus shifts to executing the designed solutions and preparing the organization for adoption. Key activities include:

- Developing a phased rollout strategy
- Defining training and documentation requirements
- Establishing success metrics and key performance Indicators (KPIs)
- Defining a post-implementation review process
- Testing for operational readiness

The design and implementation phases are critical to operational automation and integration. For this reason, everything must be fully prepared and production-ready before the go-live date. For detailed guidance on what to consider during these phases, see the [Best practices and recommendations](#) section.

Perform these phases in a logical manner in one or more sprints. Deliver functions for core operations or other prioritized domains. You can capture the work for each phase in a cloud playbook. A playbook can take the form of scripts, automated runbooks, or even a summary of processes or steps required to operate your modernized environment.

The following diagram shows the 21 OI domains organized in 4 functions: core operations, security and control, business management, and supporting functions. These are described in detail in the [next section](#).



Best practices and recommendations

This section provides best practices related to automation, readiness, tools integration, and testing:

- [AWS services for automation](#)
- [Operations readiness](#)
- [Operations automation](#)
- [Tools integration](#)
- [Operations testing](#)
- [AIOps](#)

AWS services for automation

You can use a number of AWS services to automate your IT operations. The following table lists the 21 OI domains and provides information to help you select the right service for each operational need.

Function	Domain	Launch focus and tools
Core operations	Platform architecture and governance	Enterprise-wide governance, security baselines, multi-account strategy, and automated compliance. Usually covered by deploying the AWS Landing Zone solution, AWS Control Tower , or AWS Managed Services .
Core operations	Event and incident management	Logging, monitoring, automated incident response, and incident correlation using Amazon CloudWatch , Amazon Simple Notification Service (Amazon SNS) , and Amazon DevOps Guru .

Core operations	Provisioning and configuration management	Infrastructure as code (IaC), automated deployment, and configuration compliance by using AWS Service Catalog , AWS CloudFormation , AWS Cloud Development Kit (AWS CDK) , AWS Systems Manager , and AWS Config .
Core operations	Availability and business continuity management	High availability, resiliency, disaster recovery, and business continuity by using AWS Resilience Hub , AWS Elastic Disaster Recovery , and AWS Backup .
Core operations	Monitoring and observability	Operational visibility, proactive monitoring, and automated response to service health issues by using Amazon CloudWatch (metrics, logs, alarms), AWS Health , Service Quotas , AWS X-Ray , Amazon Managed Grafana , and Amazon Managed Service for Prometheus .
Security and control	Change management	Compliance controls, risk management, and tracking changes by using AWS Config , Change Manager , a capability of AWS Systems Manager, AWS Audit Manager , and AWS CloudTrail .

Security and control	Asset management	Transparency and resource lifecycle tracking by using AWS Resource Explorer , Inventory and Fleet Manager , capabilities of AWS Systems Manager, AWS Config , and automated tagging strategies.
Security and control	Identity and access management	Least privilege implementation through AWS Identity and Access Management (IAM) , single sign-on capabilities with AWS IAM Identity Center , federation with AWS Directory Service , usually implemented through the security workstream.
Security and control	Security management	Security controls and incident response by using AWS Security Hub CSPM , Amazon GuardDuty , Amazon Detective , Amazon Inspector , Amazon Macie , AWS WAF , AWS Shield , and AWS Network Firewall , specified by the security workstream with automated security assessments and remediation capabilities. For example, see the guide Automated patching for mutable instances in the hybrid cloud using AWS Systems Manager on the AWS Prescriptive Guidance website.

Security and control	Compliance and risk management	Regulatory compliance, automated auditing, and continuous risk assessment by using AWS Artifact , AWS Config , AWS Audit Manager , AWS Security Hub CSPM , and AWS Control Tower .
Security and control	Data governance and sovereignty management	Data classification, regional compliance requirements such as General Data Protection Regulation (GDPR), and data residency controls by using AWS GovCloud (US) for government workloads, AWS European Sovereign Cloud for EU data sovereignty, and AWS Region-specific deployments.
Business management	FinOps management	Cost optimization, governance, and billing reporting by using AWS Cost Explorer , AWS Budgets , AWS Cost Anomaly Detection , AWS Trusted Advisor , AWS Billing Conductor , and cost tagging strategies.
Business management	Capacity planning and forecasting	Capacity forecasting by using AWS Cost Explorer forecasting , resource optimization by using AWS Compute Optimizer , AWS Trusted Advisor , and AWS Budgets .

Business management	Organizational change management	Training, communications, transformation buy-in, adoption frameworks, and managing the people side of cloud transformation .
Business management	Vendor management	License and provider management through AWS Marketplace , AWS License Manager , AWS Partner Network , outsourced provider controls, and integration.
Business management	Sustainability management	Environmental impact monitoring and optimization by using AWS Customer Carbon Footprint Tool , AWS Graviton processors for better performance per watt, AWS Well-Architected Sustainability Pillar implementation, and sustainability-focused architecture decisions.

Business management	Cloud value maximization	Maximizing the business value with the AWS Cloud by optimizing costs, improving operational efficiency, and leveraging cloud capabilities effectively. This includes understanding cost drivers by using AWS Cost Explorer and implementing strategic purchasing (Savings Plans , Reserved Instances , Spot Instances), while using AWS Compute Optimizer for right-sizing and total cost of ownership (TCO) analysis. The goal is to balance cost optimization with performance and innovation to ensure that cloud investments drive business outcomes while supporting growth objectives.
Supporting functions	Reporting and analytics	Usage trends and service health monitoring by using Amazon OpenSearch Service , Amazon Quick , Amazon Athena , and CloudWatch analytics and monitoring .
Supporting functions	Continuous improvement	Process iterations by using AWS Trusted Advisor , Amazon DevOps Guru , AWS Well-Architected Tool , and OpsCenter , a capability of AWS Systems Manager, for operational excellence.

Supporting functions	Application lifecycle management	Software development lifecycle, people, process, and tools integrations, DevOps workstream with Amazon Q Developer , AWS CodeBuild , AWS CodeDeploy , and AWS CodePipeline .
Supporting functions	AI/ML operations	Enhanced operational capabilities with CloudWatch anomaly detection , CloudWatch investigations , and Amazon DevOps Guru for predictive monitoring and issue detection; AWS Security Hub CSPM , Amazon GuardDuty , and Amazon Detective for ML-powered threat detection and investigation; and AI-driven document processing and architecture visualization solutions to streamline operations and improve incident response.

Operations readiness

Workshops are an effective way to understand your current operating model and to define an AWS operating model.

Operating models on AWS can be structured across three main paradigms: traditional operations, CloudOps, and DevOps. Each model offers distinct approaches to managing cloud operations,

Traditional operations model

- Maintains conventional processes based on IT Infrastructure Library (ITIL)
- Operates with clear separation between development and operations teams

- Uses established change management procedures
- Relies on existing ITSM tools that are integrated with AWS services
- Suitable for organizations that are in the early stages of cloud adoption
- Works well with the [rehost](#) (lift and shift) and [relocate](#) migration strategies

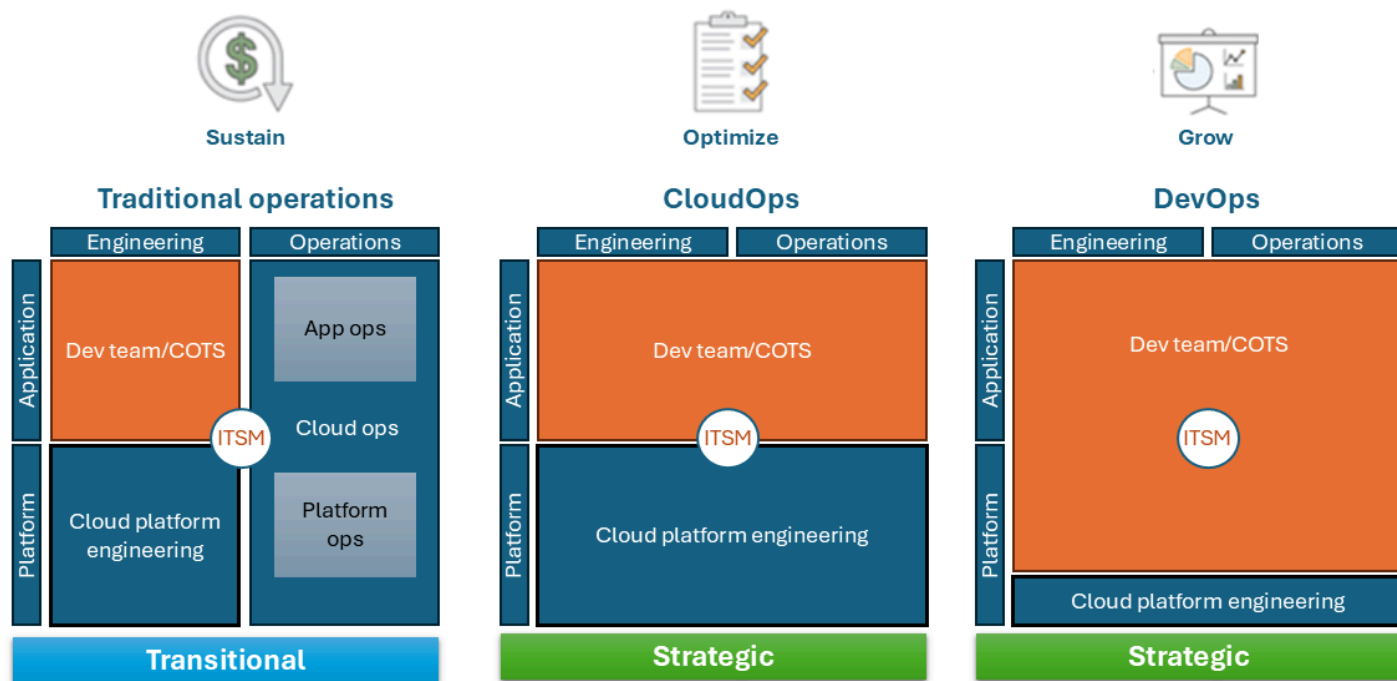
CloudOps model

- Represents a hybrid approach that combines traditional and cloud-native practices
- Takes advantage of AWS-specific operational capabilities
- Implements automated monitoring and management
- Maintains some traditional controls while adopting cloud practices
- Ideal for organizations during cloud transformation
- Aligns well with the [replatform](#) and [repurchase](#) migration strategies
- Serves as a transitional model during cloud maturity development

DevOps model

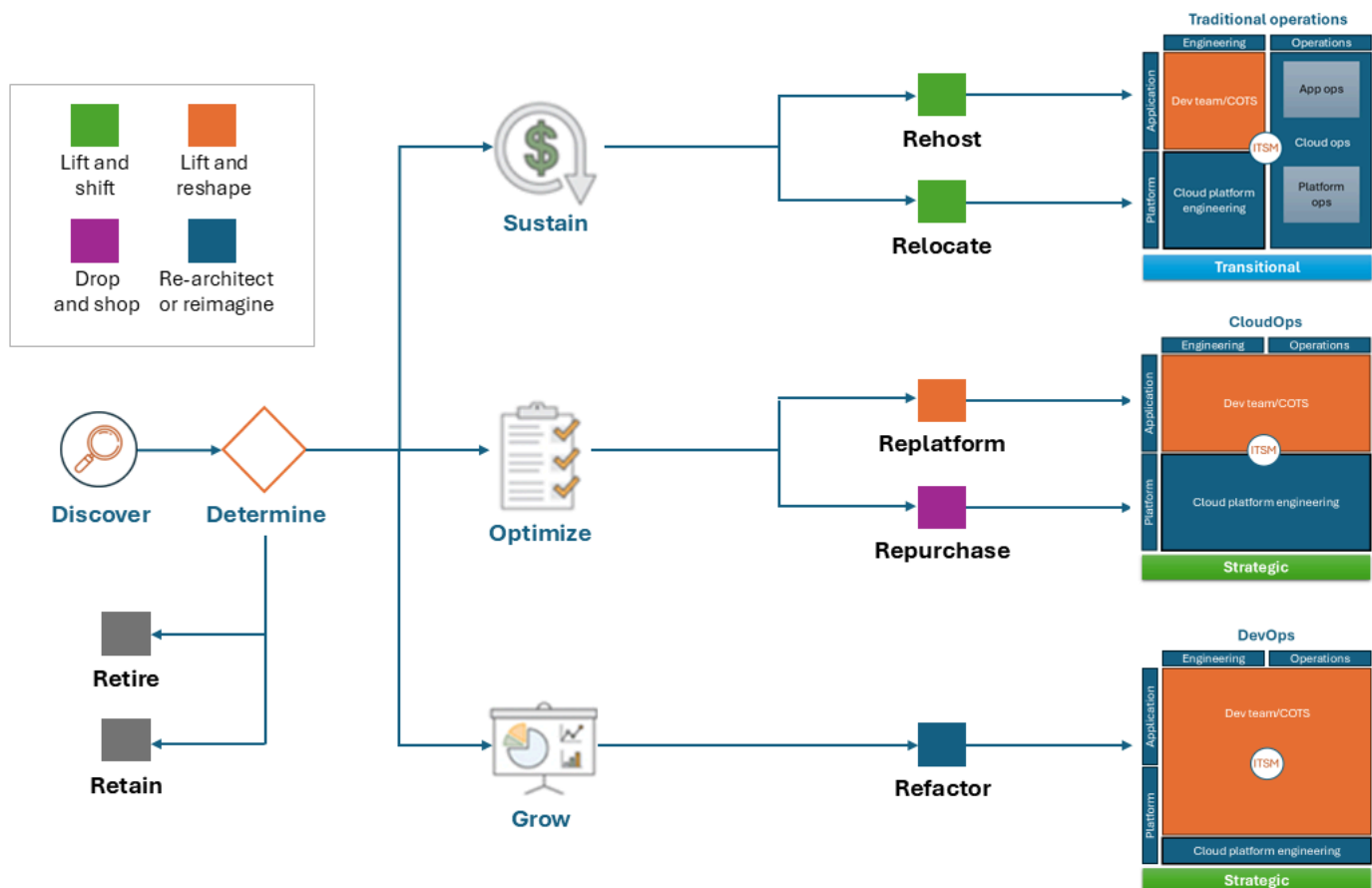
- Represents a fully integrated development and operations approach
- Emphasizes automation and continuous delivery
- Implements cloud-native practices and tools
- Features cross-functional teams and collaborative workflows
- Focuses on rapid iteration and deployment
- Best suited for the [refactor](#) (reimagine) migration strategy
- Represents the most mature cloud operating model

The following diagram illustrates these three models.



The choice of operating model should align with your organization's cloud maturity, migration strategy, and business objectives. Organizations often evolve through these models as they progress in their cloud journey—starting with traditional operations and gradually moving toward DevOps as their cloud capabilities mature.

The following diagram shows suggested operating models based on the [7Rs migration strategies](#) and approach to AWS.



Operations automation

You are not expected to have all your IT operations fully automated on day 1. Take a phased approach instead. Start by carefully prioritizing the core operations functions that are listed in the following table. Use the AWS services listed in the [AWS services for automation](#) section to streamline the modernization process.

Core operations functions

Platform architecture and governance

Event and incident management

Capabilities and considerations

[Account strategy](#), [virtual private cloud \(VPC\) strategy](#), [multi-Region and Multi-AZ strategy](#), [tagging strategy](#), IP addressing and connectivity, [security strategy](#), audit and compliance

Alerting and alarming, incident management process, AWS Support engagement, service

desk, [observability toolsets and integrations](#), cloud runbooks

Provisioning and configuration management

Provisioning, continuous integration and continuous delivery (CI/CD) pipeline and toolset, release management, testing framework and toolset, code repository, branching strategy, blue/green deployments, configuration management database (CMDB), configuration items

Availability and continuity management

High availability architecture, automatic scaling, [backup and restore](#), replication, recovery time objective (RTO) and recovery point objective (RPO), data storage and retention policy, [disaster recovery](#), automation and bots, hybrid options, storage gateways

Monitoring and observability

Metrics, logging, application performance, user experience, network monitoring, unified dashboards

Tools integration

Most enterprises rely on ITSM tools to automate their on-premises operations. When these organizations move to the cloud, they need to maintain their existing ITSM tools and processes. Attempting to completely replace existing ITSM tools and retrain staff on new operational processes would be costly and time-consuming, and could significantly delay migration initiatives.

To address this need, AWS provides several integration patterns that enable enterprises to connect their existing ITSM tools with AWS services. These integration patterns allow organizations to maintain operational continuity while progressively adopting cloud capabilities. The following table outlines the common integration patterns between ITSM tools and AWS services. These patterns provide a practical approach to cloud adoption without disrupting existing operational processes.

Scenario	Description and AWS tools
Self-service and self-provisioning	Enterprise users self-provision resources on AWS by using the AWS Service Catalog connector in ITSM without the need to sign into the AWS Management Console.
CMDB integration	AWS Config and AWS Systems Manager provide native discovery services that monitor continuous integrations (CIs) on AWS. Resource configurations, compliance states, and changes can be automatically logged into a CMDB.
AMS–ITSM integration	AWS Managed Services (AMS) integration by using AWS Service Management Connector App version 2 provides flexibility to customize integrations for various needs.
Ticketing	Bi-directional integration between the AWS Support API and ITSM enables tickets to seamlessly flow between AWS Enterprise Support and ITSM incidents. Integration with OpsCenter .
Monitoring	Amazon CloudWatch alarms trigger incidents in ITSM for remediation or workflow initiation.
Migration acceleration using ITSM (MAUS)	You can use ITSM discovery modules or CMDB data to define your on-premises landscape for mass migration projects. Data mapping can be imported into AWS Migration Portfolio Assessment to automate migration portfolio analysis and business case validation.

Operations testing

Like products, IT operations should be tested, end to end, on a regular cadence. Although enterprise customers have adopted operational testing for activities such as disaster recovery, operational testing should be extended to other operations domains such as incident and event management. Game-day scenarios, like fire drills, are activities that test how your processes, tools, and people react when an operations event occurs.

Here are some prescriptive game-day scenarios used to test incident and event management on AWS:

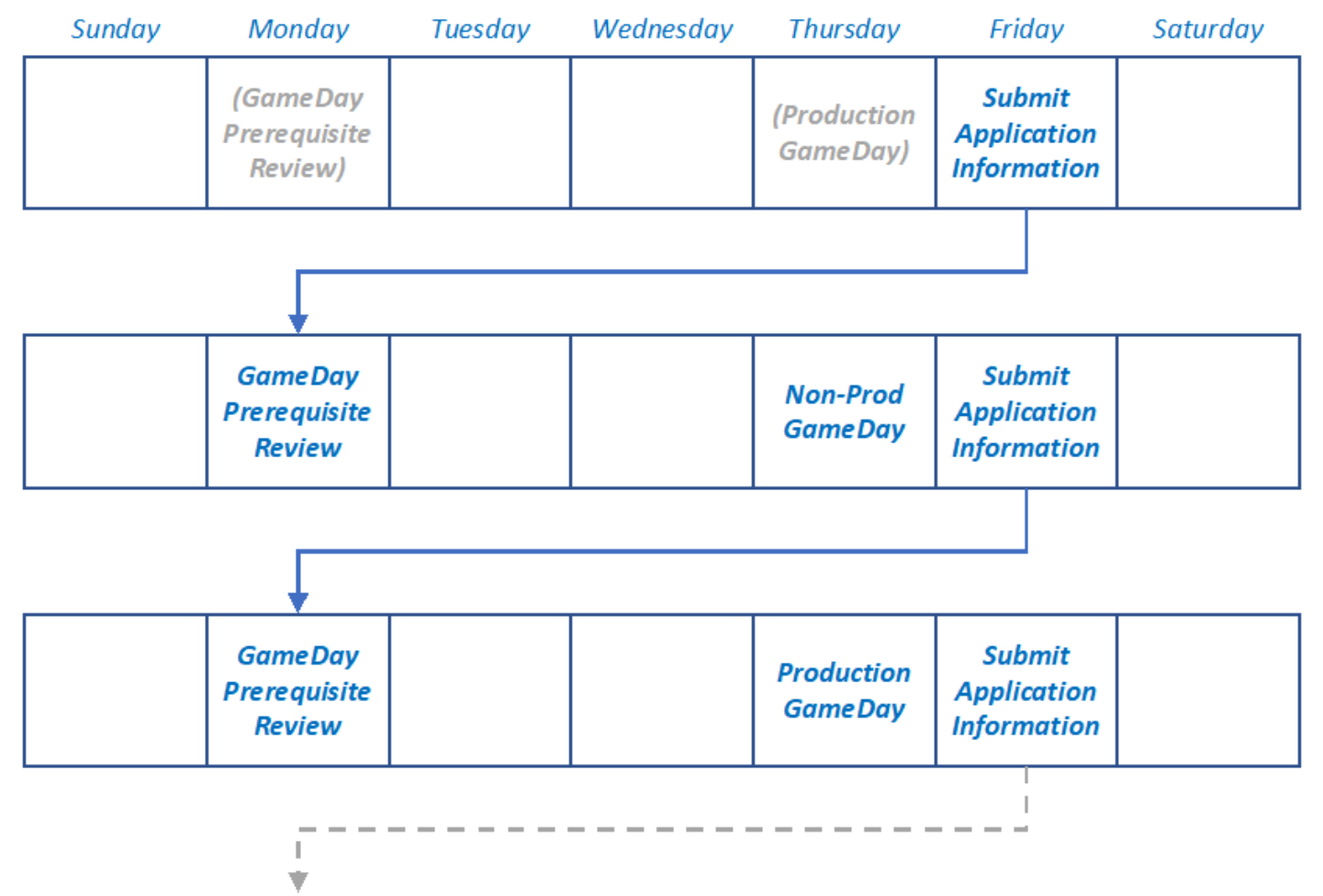
- Amazon Elastic Compute Cloud (Amazon EC2) CPU utilization stress test
- Amazon EC2 network stress test
- Amazon EC2 memory stress test
- Amazon Elastic Container Service (Amazon ECS) task failure scenarios
- AWS Lambda concurrency limits and cold start impact
- Amazon API Gateway throttling and latency injection
- Amazon Relational Database Service (Amazon RDS) memory stress test
- Amazon RDS failover testing
- Amazon RDS storage stress
- Amazon DynamoDB throttling and hot partition testing
- Availability Zone failure simulation

Consider using the following AWS services to run testing scenarios:

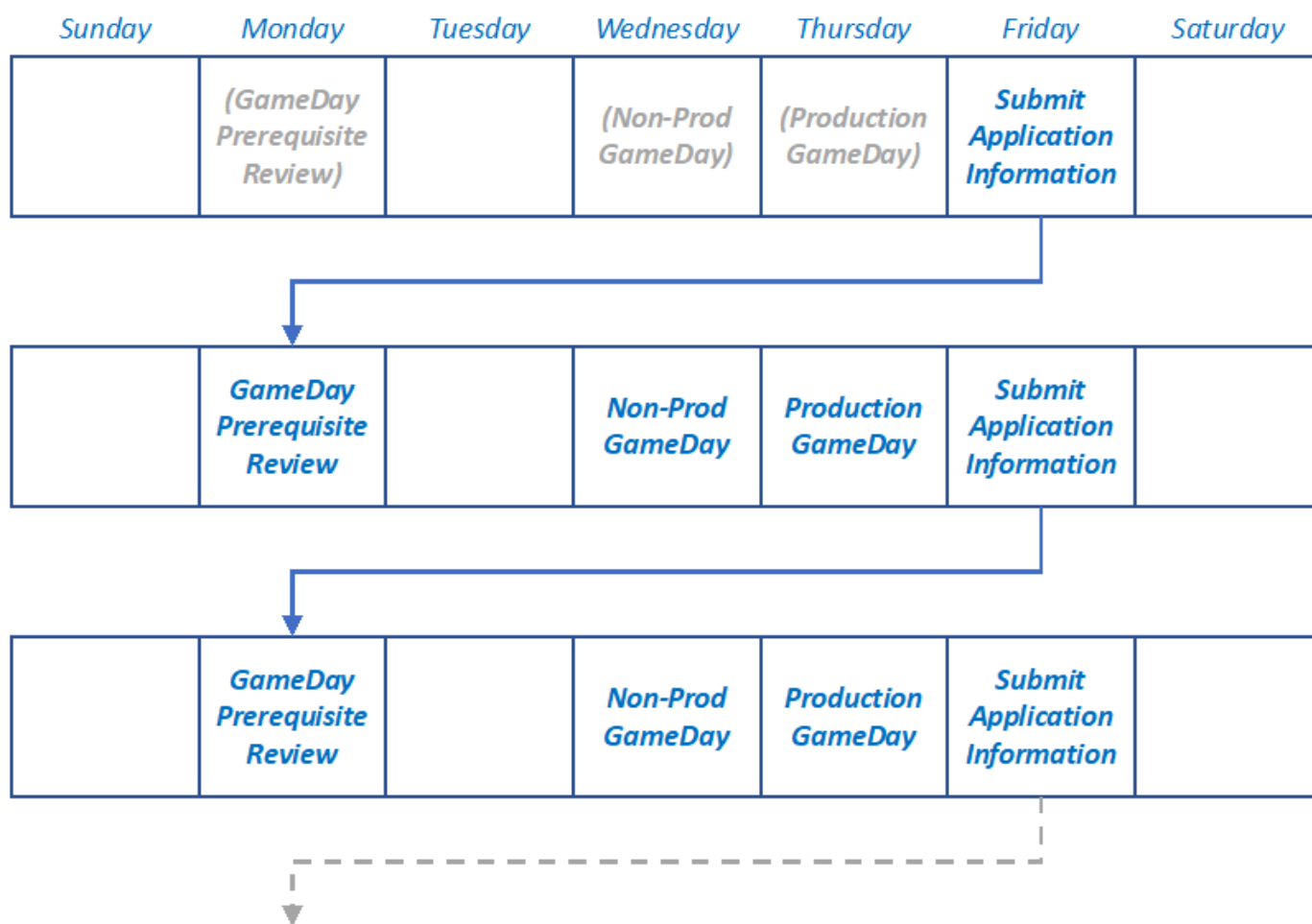
- [AWS Fault Injection Service \(AWS FIS\)](#) for controlled chaos engineering experiments
- [Amazon CloudWatch Synthetics](#) for application endpoint testing
- [Automation](#), a capability of AWS Systems Manager, for orchestrating complex scenarios
- [AWS Resilience Hub](#) for assessing and improving application resiliency

As a best practice, you should test your IT operations starting with incident and event management, and extend testing to other operational domains. It's also crucial to have a predetermined game-day schedule. Here are some example schedules:

Prod or non-prod schedule



Prod and non-prod schedule



AIOps

When you migrate your workloads to AWS, you can take advantage of various AWS monitoring services that are enhanced with AI and machine learning (ML) capabilities. Although traditional monitoring through Amazon CloudWatch events, alarms, and AWS Config Rules provides foundational insights, the integration of ML techniques elevates operational intelligence to new levels.

[Amazon CloudWatch investigations](#) represents the convergence of AI and IT operations, designed to minimize human intervention in operational processes. [Amazon DevOps Guru](#) provides proactive incident detection and recommendations to help prevent potential issues before they impact your systems. [Amazon CloudWatch anomaly detection](#) uses ML algorithms to analyze historical metric patterns to detect unusual behavior in your AWS resources.

AI operations (AIOps) services enhance operational capabilities through three key dimensions: service quality improvements, proactive operations, and enhanced operational insights.

Service quality improvements

- Advanced metric correlation and pattern analysis
- Automated alerting and notification system implementation
- Seamless integration with incident management systems

Proactive operations

- ML-driven anomaly detection
- Continuous performance metric tracking and trending
- Real-time monitoring and alerting

Enhanced operational insights

- Resource performance analysis
- Application behavior tracking
- Automated issue detection and classification

By implementing AIOps on AWS, organizations can achieve more efficient operations, reduced mean time to resolution (MTTR), and improved overall service reliability through data-driven, AI-enhanced operational practices. This modernized approach helps organizations move from reactive to proactive operations management while taking advantage of the robust AI/ML capabilities provided by AWS.

Next steps

If you are in the process of modernizing your operations, use this guide and the [associated resources](#) to start your journey. Many organizations that are considering a large-scale migration to the cloud invest significant time and resources in planning and assessment, but it may be helpful to start with a targeted application to use as a minimal viable product (MVP). You'll find it faster and more valuable to establish the foundation services, and then use the technical foundations, business learnings, and deployment processes developed in that project as the basis for larger-scale activities.

Modernizing operations is an iterative process. It evolves over time as you integrate other operations tooling with your cloud initiatives. As the following diagram illustrates, the process includes alignment, launch (cycle 1), scaling, and optimization.



Align



Launch



Scale



Optimize

- **Align.** In this phase, you conduct discovery activities to agree on the desired business outcome, educate the team, address blockers, and align technical and business stakeholders on the initiative. This is part of operational readiness and discovery described earlier in this guide.
- **Launch (cycle 1).** In this phase, you launch something small but fully functional into a production-like environment. The goal is to deliver MVP capabilities. For example, you can migrate an existing workload or create new functionality.
- **Scale.** In this phase, you expand the limited-scope work from the launch phase and expand it to full scale. For innovation, this means rolling out all functionality to all users. For migration, this means migrating all workloads to AWS.
- **Optimize.** In this phase, you revisit workloads on AWS to identify areas for improvement and implement them. It's during this phase that you might consider AIOps, for example.

The process of modernizing operations in the cloud involves readiness, automation, and integration. This guide described how to achieve readiness by defining a cloud operating model, how to automate your operations by using AWS services, and how to integrate your tools by using best practices. It also showed you how to use a migration project with a targeted application to start the process of modernizing operations.

Resources

AWS Prescriptive Guidance publications:

- [Strategies for overcoming common cloud transformation challenges](#)
- [Building your Cloud Operating Model](#)
- [AWS Change Acceleration 6-Point Framework and Organizational Change Management Toolkit](#)
- [Accelerating observability outcomes](#)

Other AWS content:

- [AWS Well-Architected Framework documentation](#)
- [AWS observability best practices](#)
- [How organizations are modernizing for cloud operations](#)
- [Transitioning from migration to modernization on the cloud](#)

Contributors

The following individuals contributed to this guide.

Authors

- Itai Njanji, Global Practice Lead, AWS Cloud Management Tools Partner Network
- Libin Roy, Solutions Architect, AWS
- Phani Lingamallu, Sr. Partner Solutions Architect, AWS

Reviewer

- Moises Ulloa, Sr. Solutions Architect, AWS

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
Revision	Updated with the 7Rs approach and the latest AWS services and approaches for cloud operations	August 8, 2025
Initial publication	—	August 5, 2019