Nephology AWS Cloud Operations Checklist

Last updated: 2026-08-03

Framework reference: AWS Well-Architected Framework

Focus areas: Security, Cost Optimisation, Operational Excellence

Contents

How to Use This Checklist

This checklist is organised by cadence: Daily, Weekly, Monthly, and Annual. Each item includes:

- A brief description of the task
- The relevant AWS Well-Architected Framework (WAF) pillar and best-practice area
- A RACI assignment for large-enterprise roles
- A URL for further reading

It is recommended for each action that you collect evidence/confirmation of the results at that time, kept in an operations log/system of record. This could be a collection of screenshots, statistics, etc. You may want to script some of these checks, and populate CloudWatch metrics of the result, with alerts on failure. You may also wish to create a version of this filtered for each role, and each DevOps team where applicable. This checklist is not complete, and should be used as a guide, supplemented with specific checks to your workloads, compliance requirements, and risk assessments.

WAF Pillar Abbreviations

Code	Pillar
OE	Operational Excellence
SEC	Security
REL	Reliability
PERF	Performance Efficiency
COST	Cost Optimisation
SUS	Sustainability

RACI Role Definitions

Role	Description
R – Responsible	Does the work
A – Accountable	Owns the outcome; approves
C – Consulted	Provides input before/during
I – Informed	Notified when complete or when an event occurs

Enterprise Roles Used in This Checklist

Abbreviation	Role
CloudOps	Cloud Operations Engineer / SRE
SecEng	Security Engineer / Cloud Security Analyst
FinOps	FinOps Analyst / Cloud Cost Manager
Architect	Cloud / Solutions Architect
DevOps	DevOps / Platform Engineer
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
CIO	Chief Information Officer
DBA	Database Administrator
Compliance	Compliance & Risk Officer
AppOwner	Application / Service Owner
ChangeAdv	Change Advisory Board (CAB)

This checklist should be reviewed and updated at least annually, whenever significant architectural changes are made to the AWS environment, or significant AWS changes are available.

Daily Tasks

D-01 · Review CloudWatch Alarms and Dashboards

Check all active CloudWatch alarms, review operational dashboards, and confirm no critical metrics (CPU, memory, error rates, latency) are breached. Acknowledge or escalate any firing alarms.

Role	RACI
CloudOps	R
AppOwner	A
SecEng	I
DevOps	I

- WAF Pillar: OE – OPS 7: How do you understand the health of your workload?
- AWS Docs: Amazon CloudWatch Alarms

D-02 · Review AWS Security Hub Findings

Triage new and active Security Hub findings. Escalate CRITICAL and HIGH severity findings immediately. Update finding status (resolved/suppressed) where appropriate.

Role	RACI
SecEng	R
CISO	A
CloudOps	C
Compliance	I

- WAF Pillar: SEC – SEC 1: How do you securely operate your workload?
- AWS Docs: AWS Security Hub

D-03 · Review Amazon GuardDuty Findings

Check GuardDuty for new threat-intelligence findings (recon, credential compromise, unusual API calls). Confirm no unaddressed HIGH or CRITICAL detections are open.

Role	RACI
SecEng	R
CISO	A
CloudOps	C
Compliance	I

- WAF Pillar: SEC – SEC 5: How do you detect and investigate security events?
- AWS Docs: Amazon GuardDuty Findings

D-04 · Review AWS Cost Explorer / Daily Spend Anomalies

Check AWS Cost Anomaly Detection alerts and the daily spend trend in Cost Explorer. Investigate any spend spikes or unexpected charges against the prior 7-day baseline.

Role	RACI
FinOps	R
CTO / CIO	A
CloudOps	C
AppOwner	I

- WAF Pillar: COST – COST 3: How do you monitor your cost and usage?
- AWS Docs: AWS Cost Anomaly Detection

D-05 · Verify Backup Job Completion

Confirm that AWS Backup jobs (RDS, EBS, EFS, DynamoDB) completed successfully overnight. Investigate and remediate any failed or partial backup jobs. Tip: script this check into a CloudWatch Metric, looking at total number of completed backup jobs, and backup durations.

Role	RACI
CloudOps	R
AppOwner	A
DBA	C
Compliance	I

- WAF Pillar: REL – REL 9: How do you back up data?
- AWS Docs: AWS Backup

D-06 · Review CI/CD Pipeline Health

Role	RACI
DevOps	R
AppOwner	A

Confirm that deployment pipelines (CodePipeline, GitHub Actions, Jenkins, etc.) have no failed or stalled stages. Review recent deployments for rollbacks or error spikes post-deploy. Tip: script this check into a CloudWatch Metric.

CloudOps	C
Architect	I

- WAF Pillar: OE – OPS 5: How do you reduce defects, ease remediation, and improve flow?
- AWS Docs: AWS CodePipeline

D-07 · Check EC2 / Container Health (Auto Scaling Groups, ECS/EKS)

Verify that all Auto Scaling Groups are at desired capacity and no instances are in an unhealthy state. For ECS/EKS clusters, confirm that all services are running the desired task/pod count. Tip: script this check into a CloudWatch Metric.

Role	RACI
CloudOps	R
AppOwner	A
DevOps	C
Architect	I

- WAF Pillar: REL – REL 6: How do you monitor workload resources?
- AWS Docs: Amazon EC2 Auto Scaling Health Checks

D-08 · Review On-Call / Incident Log

Review the on-call handover log. Confirm any overnight incidents are documented, tickets are open, and owners are assigned. Clear resolved items.

Role	RACI
CloudOps	R
AppOwner	A
SecEng	C
CTO	I

- WAF Pillar: OE – OPS 11: How do you manage workload and operations events?
- AWS Docs: AWS Systems Manager OpsCenter

D-09 · Review AWS What's New

Look for new releases that may have an impact on your current workloads (including work about to be done). Look for services that are deprecated, or have new versions, security improvements, cost improvements, or performance improvements.

Role	RACI
CloudOps	R
AppOwner	A
SecEng	I
CTO	I

- AWS Docs: What's New

Weekly Tasks

W-01 · Run AWS Trusted Advisor Review

Review Trusted Advisor checks across all five categories: Cost Optimisation, Security, Fault Tolerance, Performance, and Service Limits. Create tickets for any RED (action recommended) items.

Role	RACI
CloudOps	R
FinOps	R
CTO	A
SecEng	C
AppOwner	I

- WAF Pillar: OE / COST / SEC – Trusted Advisor
- AWS Docs: AWS Trusted Advisor

W-02 · Review IAM Access Analyser Findings

Check IAM Access Analyzer for any new findings indicating unintended external access to S3 buckets, IAM roles, KMS keys, Lambda functions, or SQS queues. Remediate or archive findings with justification.

Role	RACI
SecEng	R
CISO	A
CloudOps	C
Compliance	I

- WAF Pillar: SEC – SEC 2: How do you manage identities for people and machines?
- AWS Docs: IAM Access Analyzer

W-03 · Audit Unused or Idle Resources

Use Cost Explorer, Compute Optimizer, or third-party tooling to identify idle EC2 instances, unattached EBS volumes, unused Elastic IPs, and empty S3 buckets. Schedule for rightsizing or termination. Look for new EC2 Instance Families or EBS volumes with a better price or price/performance (without compromising security or raw performance). Consider migrating workloads to ARM CPUs.

Role	RACI
FinOps	R
CloudOps	R
CTO	A
AppOwner	C
Architect	I

- WAF Pillar: COST – COST 6: How do you manage demand and supply resources?

- AWS Docs: AWS Compute Optimizer

W-04 · Review AWS Config Rule Compliance

Check AWS Config compliance dashboard. Identify non-compliant resources (e.g., unencrypted EBS volumes, publicly accessible S3 buckets, security groups open to 0.0.0.0/0). Raise remediation tasks.

Role	RACI
SecEng	R
Compliance	A
CloudOps	C
CISO	I

- WAF Pillar: SEC – SEC 1: How do you securely operate your workload?
- AWS Docs: AWS Config Rules

W-05 · Review VPC Flow Logs and Network Anomalies

Sample or query VPC Flow Logs (via Athena, CloudWatch Logs Insights, or a SIEM) for unusual traffic patterns: port scans, unexpected outbound connections, denied traffic spikes.

Role	RACI
SecEng	R
CloudOps	C
CISO	A
Compliance	I

- WAF Pillar: SEC – SEC 6: How do you protect your network resources?
- AWS Docs: VPC Flow Logs

W-06 · Review Patch Compliance Status (SSM Patch Manager)

Role	RACI

Check Systems Manager Patch Manager compliance report. Identify non-compliant EC2 instances or managed nodes. Schedule patching windows for any instances missing critical or important patches.

CloudOps	R
SecEng	C
AppOwner	A
Compliance	I

- WAF Pillar: SEC – SEC 6: How do you protect your compute resources?
- AWS Docs: AWS Systems Manager Patch Manager

W-07 · Validate SSL/TLS Certificate Expiry Alerts

Review ACM and any externally managed certificate expiry notifications. Ensure no external manually-deployed certificate expires within 30 days without a renewal in progress. Check ACM certificates are configured for automatic renewal and redeployment. Check CA Root CA expiry is well into the future (>12 months). Note: TLS Certificate lifetimes are progressively shrinking to 45 days, so only alarm if less than 2 days validity remains (if automated). Tip: script this check into a CloudWatch Metric.

Role	RACI
SecEng	R
CloudOps	R
CISO	A
AppOwner	I

- WAF Pillar: SEC – SEC 8: How do you protect your data in transit?
- AWS Docs: AWS Certificate Manager

W-08 · Confirm CloudTrail is Active and Logging

Verify that all CloudTrail trails are active, logs are being delivered to S3, and no delivery errors are reported. Confirm log file validation is enabled. Tip: script this check into a CloudWatch Metric. Ensure you are using an Organisational CloudTrail, that is enforced, and that you have an SCP to require CloudTrail.

Role	RACI
SecEng	R
CISO	A
CloudOps	C
Compliance	I

- WAF Pillar: SEC – SEC 4: How do you detect and investigate security events?
- AWS Docs: AWS CloudTrail

Monthly Tasks

M-01 · Test Restore from Backup (Spot-Check)

Randomly select one backup set (RDS snapshot, EBS snapshot, or S3 versioned object) and verify it can be restored successfully into a non-production account, then remove the restored version (keep the backup). Document restore duration to understand potential future RTO.

Role	RACI
CloudOps	R
DBA	C
AppOwner	A
Compliance	I

- WAF Pillar: REL – REL 9: How do you back up data?
- AWS Docs: AWS Backup Restore Testing

M-02 · IAM User and Role Access Review

Review all IAM users, roles, and policies. Remove or deactivate stale users (no console/API activity in 90+ days). Review roles for overly broad permissions and apply least-privilege corrections. Use IAM Credential Report and Access Advisor.

Role	RACI
SecEng	R
CISO	A
CloudOps	C
Compliance	I
CIO	I

- WAF Pillar: SEC – SEC 2: How do you manage identities for people and machines?
- AWS Docs: IAM Credential Report, IAM Access Advisor

M-03 · Review and Rotate Secrets and Access Keys

Use AWS Secrets Manager and IAM to identify any long-lived access keys (>90 days) or secrets approaching rotation schedules. Rotate keys, update dependent services, and revoke old credentials.

Role	RACI
SecEng	R
DevOps	C
CISO	A
AppOwner	I

- WAF Pillar: SEC – SEC 3: How do you manage permissions for people and machines?
- AWS Docs: AWS Secrets Manager Rotation, Rotating IAM Access Keys

M-04 · Monthly Cost Optimisation Review

Produce a monthly cost report per account/business unit. Identify top 5 cost drivers. Review rightsizing recommendations from Compute Optimizer. Evaluate new Savings Plan or RI purchase opportunities. Present findings to stakeholders.

Role	RACI
FinOps	R
CTO / CIO	A
CloudOps	C
Architect	C
AppOwner	I

- WAF Pillar: COST – COST 2: How do you govern usage?
- AWS Docs: AWS Cost Explorer, AWS Compute Optimizer

M-05 · Review AWS Service Quotas and Limits

Check Service Quotas for accounts with high growth. Submit limit increase requests where usage exceeds 75% of a quota. Prioritise limits for EC2, Lambda concurrency, VPC, and API Gateway.

Role	RACI
CloudOps	R
Architect	C
AppOwner	A
CTO	I

- WAF Pillar: REL – REL 2: How do you plan your network topology? / REL 3: How do you manage service quotas and constraints?
- AWS Docs: AWS Service Quotas

M-06 · Review and Test Disaster Recovery (DR) Plan

Execute a tabletop or partial failover test of the DR plan for at least one Tier-1 application. Measure RTO and RPO against agreed targets. Document results and update the DR runbook.

- WAF Pillar: REL – REL 13: How do you plan for disaster recovery?
- AWS Docs: Disaster Recovery on AWS, AWS Elastic Disaster Recovery

Role	RACI
CloudOps	R
Architect	C
AppOwner	A
Compliance	C
CTO	I

M-07 · Vulnerability and Penetration Testing Review

Review Amazon Inspector findings across EC2, Lambda, and ECR for new CVEs. Prioritise CRITICAL and HIGH findings for patching. Confirm any authorised penetration test results are tracked to remediation.

- WAF Pillar: SEC – SEC 6: How do you protect your compute resources?
- AWS Docs: Amazon Inspector, Penetration Testing on AWS

Role	RACI
SecEng	R
CISO	A
CloudOps	C
Compliance	I
AppOwner	I

M-08 · Review CloudTrail and Audit Log Integrity

Validate CloudTrail log file integrity using the validation feature. Confirm logs are retained per policy (typically 12 months online, 7 years archived). Review for any gaps in logging coverage across regions and accounts.

- WAF Pillar: SEC – SEC 4: How do you detect and investigate security events?
- AWS Docs: Validating CloudTrail Log File Integrity

Role	RACI
SecEng	R
Compliance	A
CloudOps	C
CISO	I

M-09 · Review Multi-Account / AWS Organizations Policy Compliance

Review Service Control Policies (SCPs) in AWS Organizations. Confirm no accounts have drifted from approved guardrails (e.g., allowed regions, prohibited services). Review AWS Control Tower drift reports if applicable.

- WAF Pillar: SEC / OE – SEC 1: How do you securely operate your workload?
- AWS Docs: AWS Organizations SCPs, AWS Control Tower

Role	RACI
SecEng	R
CloudOps	C
Compliance	A
CISO	I
CIO	I

M-10 · Review Reserved Instance / Savings Plans Utilisation

Check utilisation of active Reserved Instances and Savings Plans in Cost Explorer. If utilisation falls below 80%, investigate underused commitments and re-evaluate coverage.

- WAF Pillar: COST – COST 4: How do you decommission resources? / COST 7: How do you use pricing models to reduce cost?
- AWS Docs: Savings Plans Utilization

Role	RACI
FinOps	R
CTO / CIO	A
CloudOps	C
Architect	I

M-11 · Conduct Operational Runbook Review

Role	RACI
CloudOps	R
Architect	C

Verify that runbooks for top-5 highest-risk operational procedures are up to date. Update steps where services, ARNs, or account structures have changed during the week.

AppOwner	A
ChangeAdv	I

- WAF Pillar: OE – OPS 6: How do you mitigate deployment risks?
- AWS Docs: AWS Systems Manager Documents (Runbooks)

M-12 · Security Group Rule Audit

Review Security Group changes made in the past 7 days (via CloudTrail or AWS Config). Confirm no overly permissive inbound rules (port 22/3389/0.0.0.0/0) were introduced without approval. Tip: script this check.

Role	RACI
SecEng	R
CloudOps	C
CISO	A
Compliance	I

- WAF Pillar: SEC – SEC 6: How do you protect your network resources?

- AWS Docs: Security Groups for your VPC

Annual Tasks

A-01 · AWS Well-Architected Review(s)

Conduct a comprehensive Well-Architected Review for one production workload. Engage AWS or an AWS Partner for an independent review where applicable. Produce a prioritised remediation roadmap for the coming year. Take learnings for the in-scope workload(s) and review in context of other applications.

- WAF Pillar: OE – OPS 1: How do you determine what your priorities are?

- AWS Docs: AWS Well-Architected Tool, AWS Well-Architected Partner Program

Role	RACI
Architect	R
CTO	A
CloudOps	C
SecEng	C
FinOps	C
Compliance	C
CIO	I

A-02 · Annual Security Penetration Test

Commission a formal third-party penetration test of all internet-facing and critical internal AWS workloads. Review findings, assign remediation owners, and track closure within agreed SLAs. Notify AWS before testing per their penetration testing policy.

- WAF Pillar: SEC – SEC 6: How do you protect your compute resources?
- AWS Docs: AWS Penetration Testing Policy

Role	RACI
SecEng	R
CISO	A
CloudOps	C
Compliance	C
CTO	I
AppOwner	I

A-03 · Annual IAM Deep-Dive and Privilege Audit

Perform a full inventory and audit of all IAM entities (users, groups, roles, policies). Re-certify every privileged role and service account. Remove unused permissions, enforce MFA on all human identities, and validate that break-glass accounts are secured and credentials are valid.

- WAF Pillar: SEC – SEC 2: How do you manage identities for people and machines?, SEC 3: How do you manage permissions?
- AWS Docs: IAM Best Practices, AWS Identity Center

Role	RACI
SecEng	**R**
CISO	**A**
Compliance	C
CloudOps	C
CIO	I

A-04 · Review and Renew AWS Support Plan and Enterprise Agreements

Review the current AWS Support plan level (Developer, Business, Enterprise On-Ramp, or Enterprise). Evaluate whether TAM engagement, AWS IQ credits, or EDP (Enterprise Discount Program) commitments should be renegotiated for the coming year.

- WAF Pillar: COST – COST 1: How do you implement cloud financial management?
- AWS Docs: AWS Support Plans, AWS Enterprise Discount Program

Role	RACI
FinOps	R
CTO / CIO	A
CloudOps	C
Architect	C
Compliance	I

A-05 · Reserved Instance and Savings Plans Annual Strategy

Role	RACI
FinOps	**R**
CTO	**A**
Architect	C

Conduct a full review of RI and Savings Plan portfolio. Analyse 12-month usage patterns. Plan new 1-year or 3-year commitments. Get updated estimates for all workloads for their 1-year and 3-year future usage patterns and plans. Look at the coverage strategy date-of-acquisition plan as well, and reduce long term regret spend.

CloudOps	C
AppOwner	I

- WAF Pillar: COST – COST 7: How do you use pricing models to reduce cost?
- AWS Docs: AWS Savings Plans, EC2 Reserved Instances

A-06 · Annual Disaster Recovery Full-Scale Test

Execute a full failover test of all Tier-1 production workloads to the DR region or environment. Validate RTO and RPO against business requirements. Update the Business Continuity Plan (BCP) and DR documentation based on results.

Role	RACI
CloudOps	**R**
Architect	**R**
AppOwner	**A**
Compliance	C
ChangeAdv	C
CTO	I
CISO	I

- WAF Pillar: REL – REL 13: How do you plan for disaster recovery?
- AWS Docs: AWS Disaster Recovery, Disaster Recovery Whitepaper

A-07 · Compliance and Regulatory Audit (SOC 2 / ISO 27001 / PCI DSS / HIPAA)

Facilitate the annual compliance audit. Provide AWS Artifact reports (SOC 1/2/3, PCI DSS AOC, ISO certifications) as evidence. Review shared-responsibility model documentation. Engage internal or external auditors for in-scope AWS services.

Role	RACI
Compliance	**R**
CISO	**A**
SecEng	C
CloudOps	C
CIO	I
CTO	I

- WAF Pillar: SEC – SEC 1: How do you securely operate your workload?
- AWS Docs: AWS Artifact, AWS Compliance Programs

A-08 · Annual Capacity and Architecture Review

Review current architecture against projected growth for the next 12–24 months. Identify architectural bottlenecks, single points of failure, and services approaching scaling limits. Produce an Architecture Decision Record (ADR; see Appendix for template) with recommended changes.

Role	RACI
Architect	**R**
CTO	**A**
CloudOps	C
AppOwner	C
FinOps	C
CIO	I

- WAF Pillar: PERF – PERF 1: How do you select appropriate cloud resources and architecture patterns? / REL
- AWS Docs: AWS Architecture Center, AWS Compute Optimizer

A-09 · Review Data Lifecycle and Retention Policies

Audit S3 lifecycle policies, Glacier vaults, RDS automated snapshot retention, and CloudWatch Logs retention settings. Confirm they align with data classification policies and regulatory requirements. Remove data that has exceeded its retention period (set up automation for this).

Role	RACI
CloudOps	R
DBA	C
Compliance	A
SecEng	C
FinOps	I

- WAF Pillar: COST / SEC – COST 5: How do you manage demand and supply resources?, SEC 8: How do you protect your data at rest?
- AWS Docs: S3 Lifecycle Policies, CloudWatch Logs Retention

A-10 · Annual Security Awareness and Cloud Training Review

Ensure all cloud operations, development, and security team members have completed AWS security and compliance training. Review certifications held vs. target. Schedule training for emerging services introduced during the year.

Role	RACI
CloudOps	C
SecEng	C
CISO	A
CTO	R
CIO	I

- WAF Pillar: OE – OPS 2: How do you structure your organisation to support your business outcomes?
- AWS Docs: AWS Training and Certification, AWS Skill Builder

A-11 · Tag Compliance and Governance Audit

Run a tagging audit across all accounts using AWS Resource Groups Tag Editor or a custom Config rule. Identify untagged or incorrectly tagged resources. Enforce mandatory tags (e.g., *Environment*, *CostCentre*, *Owner*, *Project*).

Role	RACI
FinOps	R
CloudOps	C
CTO	A
AppOwner	I

- WAF Pillar: COST – COST 1: How do you implement cloud financial management? / OE
- AWS Docs: AWS Tag Editor, AWS Organizations Tag Policy

Appendix: Architecture Decision Record template

Use the following headings (and description) to create a document that is immutable after each phase (proposed, accepted, superseded).

- ID: An identifier for this document. Perhaps something like yyyymmdd-nn.
- Title: A short phrase stating the decision.
- Workload: Name of the digital system or solution being considered.
- Status: proposed, accepted, superseded.
- Proposal Date: The date of this proposal.
- Accepted Date: The date this was accepted.
- Superseded Date: The date this is no longer valid.
- Technical stack: Programming language, OS and/or runtime environment and versions, database system(s) and versions.
- Present: People involved in this discussion at this time.
- Context: The problem, forces, and constraints leading to the choice.
- Options: Alternative solutions that were considered.
- Decision: The chosen path and the clear rationale behind it.
- Consequences: The resulting trade-offs, positive impacts, and side effects.