



Well-Architected: Operational Excellence and Security

AWS Well-Architected Operational Excellence and Security pillar whitepapers (as of 2026) | design principles, best-practice areas, what the OPS and SEC questions ask, AWS services per practice, metrics, anti-patterns

Well-Architected

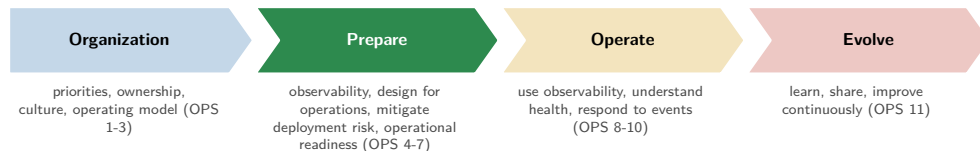
Operational excellence

Security

☀ Operational excellence: principles

- 1 Organize teams around business outcomes** team ownership aligned with business KPIs; leadership sets vision and investment
- 2 Implement observability for actionable insights** CloudWatch metrics, logs, alarms, dashboards, X-Ray / Application Signals traces, KPIs tied to customer outcomes
- 3 Safely automate where possible** infrastructure and operations as code (CloudFormation, CDK, SSM Automation), guardrails such as rate limits and approvals
- 4 Make frequent, small, reversible changes** CI/CD, canary and blue/green deployments, feature flags (AppConfig), automatic rollback on alarms
- 5 Refine operations procedures frequently** review runbooks and playbooks after each event and game day
- 6 Anticipate failure** pre-mortems, FIS experiments, test runbooks before you need them
- 7 Learn from all operational events and metrics** blameless post-incident analysis (COE), share lessons across teams
- 8 Use managed services** reduce operational burden: RDS, Fargate, Lambda, managed observability

Design principles



Practice	AWS services
Operations as code	CloudFormation, CDK, Terraform, Systems Manager (Automation, Run Command, State Manager, Parameter Store)
Safe deployments	CodePipeline, CodeDeploy (canary, linear, blue/green), AppConfig feature flags, Lambda aliases with traffic shifting
Observability	CloudWatch (metrics, Logs Insights, Synthetics, RUM, Application Signals), X-Ray, Managed Grafana and Prometheus
Event management	EventBridge, SNS, Systems Manager OpsCenter, AWS Health events, Chatbot / Amazon Q in chat apps
Insight and improvement	DevOps Guru (ML anomalies), Trusted Advisor, Well-Architected Tool milestones

📊 Measuring operations

Deployment frequency

22/week

▲ +6

Lead time for changes

1.5 d

▼ -2 d

Change failure rate

4.8 %

▼ -3.2 pt

Time to restore

38 min

▼ -22 min

PROBLEM

Last quarter a team deployed 125 times; 6 deployments caused a production incident; restoring service took 20, 45, 30, 90, 25 and 18 minutes. Compute the change failure rate and the mean time to restore.

1. Change failure rate

$$\Rightarrow \text{CFR} = F / D \times 100 = 6 / 125 \times 100 = 4.8 \%$$

why: share of deployments that needed remediation

2. Total restore time

$$\Rightarrow 20 + 45 + 30 + 90 + 25 + 18 = 228 \text{ min}$$

why: sum over the failed deployments

3. Mean time to restore

$$\Rightarrow \text{MTTR} = 228 / 6 = 38 \text{ min}$$

why: average per incident

4. Read it

$\Rightarrow$ one 90-min outlier: was rollback automated?

why: automatic rollback on CloudWatch alarms shortens the tail

GIVEN

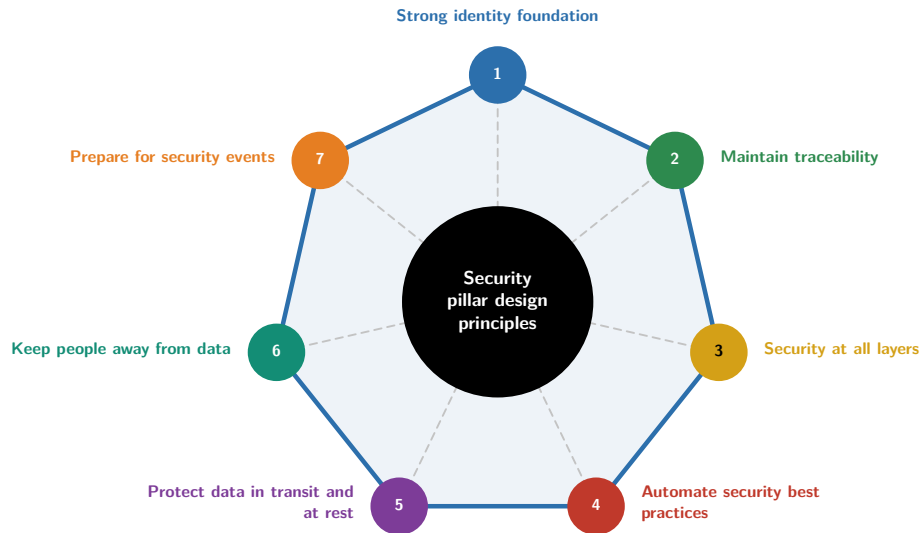
- deployments $D = 125$
- failed deployments $F = 6$
- restore times: 20, 45, 30, 90, 25, 18 min

ANSWER

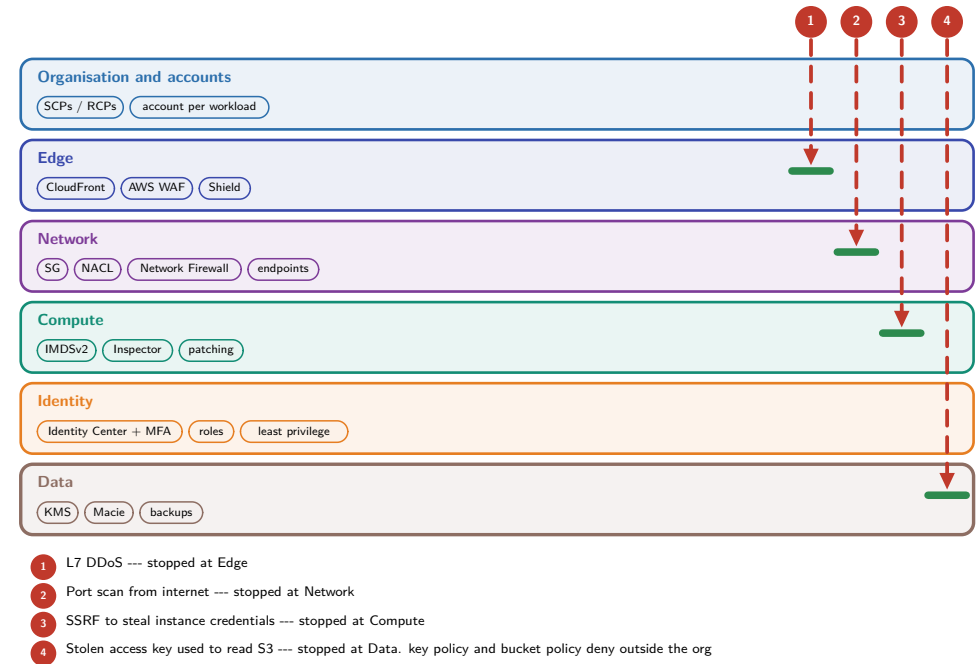
CFR 4.8 %, MTTR 38 minutes

Check: Elite DORA performers keep change failure rate low and restore in under an hour; track per milestone

Security: principles and practice areas



Practice area (questions)	Best practices you must recognise	AWS services
Security foundations (SEC 1)	separate workloads with accounts, secure the root user, keep up to date with threats, automate testing of controls, threat model	Organizations, Control Tower, SCPs
Identity and access management (SEC 2-3)	strong sign-in, temporary credentials, central IdP, least privilege, emergency access, ABAC, review access	IAM Identity Center, IAM, Access Analyzer
Detection (SEC 4)	configure service and application logging, analyse centrally, automate response to events	CloudTrail, GuardDuty, Security Hub, Config, Security Lake
Infrastructure protection (SEC 5-6)	network layers, control traffic at every layer, inspection; harden compute, vulnerability management, automate	VPC, SG, NACL, WAF, Shield, Network Firewall, Inspector, SSM
Data protection (SEC 7-9)	classify, encrypt at rest and in transit, enforce access control, key management	KMS, CloudHSM, Macie, ACM, S3 Object Lock
Incident response (SEC 10)	plans, pre-provisioned access and tools, simulations (game days)	Detective, SSM, Step Functions, AWS Security Incident Response
Application security (SEC 11)	train for security, automate testing in the pipeline, code reviews, centralised packages, deploy programmatically	Inspector code scanning, CodeArtifact, Q Developer



INFO

The Security Specialty chapter (security-specialty-scs) teaches these services in depth; here the point is the review question: for each SEC question, which best practices are in place, which are missing, and is the gap a high or medium risk?

⚠️ Anti-patterns the review looks for

Pillar	Anti-pattern	Better practice
OE	manual console changes in production	all changes through IaC and pipelines, drift detection
OE	alarms on CPU only, nobody owns them	alarms on customer KPIs with an owner and a runbook
OE	large quarterly releases	small, frequent, reversible changes with automatic rollback
OE	blame after incidents	blameless post-incident analysis with tracked actions
SEC	IAM users with long-term keys for humans	federation through Identity Center, temporary credentials
SEC	one account for everything	multi-account strategy with OUs and guardrails
SEC	logs only in the workload account	central, immutable log archive
SEC	engineers query production data directly	dashboards, automation, break-glass with approval

Check, recap, self-test

Statement	True	False
1. 'Use managed services' is an operational excellence design principle → Added in the 2023 revision; it also appears in sustainability.	☒	☐
2. The security pillar recommends one AWS account per company → SEC01-BP01: separate workloads using accounts.	☐	☒
3. Operational excellence measures success with business and customer outcomes, not only system metrics → KPIs tied to outcomes drive priorities.	☒	☐
4. 'Keep people away from data' means encrypting everything → It means reducing direct human access through tools and automation.	☐	☒
5. Game days belong to both OE and security practices → Simulate operational events and security incidents to test readiness.	☒	☐

OE: Organize, Prepare, Operate, Evolve
 11 questions

Small reversible changes
 canaries, flags, automatic rollback

Observe outcomes
 customer KPIs, not just CPU

SEC: seven principles
 identity, traceability, layers, automation, data, people away, prepare

Seven security areas
 foundations to application security, 11 questions

Q1 Name the four OE best-practice areas.

A Organization, Prepare, Operate, Evolve.

Q2 Which AWS service gives feature flags to make changes reversible?

A AWS AppConfig (feature flags and dynamic configuration).

Q3 Runbook vs playbook?

A Runbook: steps to reach an outcome (often automated). Playbook: steps to investigate an issue and decide; it calls runbooks.

Q4 Which security design principle covers CloudTrail, alerts and automated responses?

A Maintain traceability.

Q5 First best practice of the security foundations area?

A Separate workloads using accounts (SEC01-BP01).

Q6 Which DORA metric measures the share of deployments that fail?

A Change failure rate.

Q7 How many security practice areas, and which was added in 2023?

A Seven; application security was added.

Q8 Tool to detect operational anomalies with ML without writing alarms?

A Amazon DevOps Guru.

Q9 Which OE practice reduces deployment risk most for a Lambda API?

A Traffic shifting with aliases (canary or linear via CodeDeploy) and rollback on CloudWatch alarms.