FUTUREVISIONAI · IAM ADVISORY · SUBSCRIBER RESOURCE

Azure & AWS Security — Advanced Guide — Steps 3–8

Steps 3–8 · Governance through operational excellence

Included with all IAM subscription tiers

Step 3	Cloud governance hierarchy
Step 4	Certification roadmap (AZ-104 · AZ-305 · AZ-500 · AWS Security)
Step 5	Azure vs AWS security service mapping
Step 6	Zero Trust implementation
Step 7	Saviynt IGA across Azure & AWS
Step 8	Operational best practices

STEP 3 — GOVERNANCE MODEL

Cloud governance: the hierarchy that protects everything

Governance without structure is chaos. Both Azure and AWS provide hierarchical constructs that let you enforce security policies at scale — from the root down to the individual resource. Understand the model before deploying a single VM.

01

Root / tenant level — the ultimate guardrail

On Azure, the Entra ID tenant is your root identity boundary. On AWS, the Organization's management account is the root. Policies set here cascade to everything below — no exception. Global MFA requirements, emergency access policies, and root credential restrictions live here.

`Azure Tenant` `AWS Root Account` `Break-glass accounts` `Global Admins locked down`

02

Management Groups / OUs — policy inheritance

Azure Management Groups and AWS Organizational Units (OUs) group subscriptions and accounts by business unit, environment, or geography. Azure Policy and Service Control Policies (SCPs) attach here and flow downward — enforce "deny public S3 buckets" or "require TLS 1.2" once, everywhere.

`Management Groups` `AWS OUs` `SCPs` `Azure Policy Initiative` `Policy inheritance`

03

Subscriptions / accounts — isolation boundaries

Each Azure Subscription or AWS Account is a hard isolation boundary for billing, quotas, and blast radius. Security teams should separate Production, Non-Production, and Security/Log Archive accounts. The "Security Tooling" account pattern prevents attackers from deleting their own audit trails.

`Azure Subscriptions` `AWS Accounts` `Blast radius isolation` `Log Archive account` `Prod / Non-Prod split`

04

Resource Groups / VPCs — workload segmentation

Azure Resource Groups and AWS VPCs segment workloads within a subscription/account. Network Security Groups (NSGs), Security Groups, and NACLs enforce micro-segmentation. Each workload has its own managed identity or IAM role — no shared credentials between applications.

`Resource Groups` `NSGs` `VPCs` `Security Groups` `Micro-segmentation`

05

Resources — the actual attack surface

VMs, containers, storage, databases, and functions. Each resource must have: a managed identity instead of stored secrets, encryption at rest and in transit, logging enabled, public network access disabled by default, and tags that tie it to a data owner and business unit for access review automation.

`Managed Identity` `IAM Instance Profiles` `KMS / Key Vault` `Tagging governance` `No public endpoints`

06

Audit & feedback loop — governance is continuous

Azure Monitor + Microsoft Sentinel and AWS CloudTrail + Security Hub close the governance loop. Every API call, every policy change, every login attempt is logged, correlated, and surfaced to your security operations team. Governance that isn't monitored is theater.

`Azure Monitor` `Sentinel SIEM` `CloudTrail` `Security Hub` `Continuous audit`

STEP 4 — CERTIFICATION ROADMAP

Target certifications — what each one demands

Each certification validates a different depth of cloud security expertise. This is your map: what to study, in which order, and what the exam actually tests beyond the surface-level objectives.

AZ-104

AZURE ADMINISTRATOR ASSOCIATE

The foundation. Covers identity management, storage, networking, and compute on Azure. Security concepts here are operational — how to configure, not just design. Required before AZ-305 or AZ-500 for most learning paths.

Entra ID | RBAC | VNet / NSG | Key Vault | Storage security | Monitor / Alerts

AZ-305

AZURE SOLUTIONS ARCHITECT EXPERT

Architecture-level thinking. You must design multi-region, multi-layered security architectures that balance security, cost, and resilience. Exam scenarios require justifying design decisions — not just describing services.

Landing Zones | Management Groups | Defender for Cloud | Zero Trust design | Hybrid connectivity | Governance at scale

AZ-500

AZURE SECURITY ENGINEER ASSOCIATE

The deepest Azure security certification. Focuses on identity protection, platform protection, data/app security, and security operations. Expect heavy Sentinel, PIM, Conditional Access, and Defender scenario questions.

PIM / Entra ID P2 | Sentinel / SIEM | Conditional Access | Defender suite | DDoS / WAF | App registrations

AWS Security Specialty

AWS CERTIFIED SECURITY — SPECIALTY

The most demanding AWS security certification. Tests incident response, logging & monitoring, infrastructure security, IAM, data protection, and compliance. Scenario-heavy; requires hands-on AWS experience to pass.

GuardDuty | Security Hub | KMS / CloudHSM | SCPs / IAM policies | CloudTrail / Config | Macie / Inspector

STEP 5 — SERVICE MAPPING

Azure vs AWS — security services mapped

Both clouds offer equivalent capabilities, but with different names, models, and maturity levels. This mapping lets you translate knowledge between platforms and identify gaps in your coverage.

SECURITY DOMAIN	AZURE	AWS	KEY DIFFERENCE
IDENTITY PROVIDER	Microsoft Entra ID (Azure AD)	IAM Identity Center + Cognito	Entra ID is richer for B2B/B2C; AWS splits workforce vs customer identity
PRIVILEGED ACCESS	Entra PIM (Privileged Identity Mgmt)	AWS IAM + Temporary Credentials (STS)	PIM has built-in JIT UI; AWS relies on IAM roles + STS assume-role patterns
THREAT DETECTION	Microsoft Defender for Cloud	Amazon GuardDuty	Defender covers workload protection too (CWPP); GuardDuty is DNS/flow/CloudTrail ML
SIEM / SOAR	Microsoft Sentinel	AWS Security Hub + EventBridge + Lambda	Sentinel is a full managed SIEM; AWS requires assembly of multiple services
POLICY ENFORCEMENT	Azure Policy + Blueprints	SCPs + AWS Config Rules	SCPs are hard deny guardrails; Azure Policy can also auto-remediate via DeployIfNotExists
SECRETS MANAGEMENT	Azure Key Vault	AWS Secrets Manager + KMS	AWS separates key management (KMS) from secrets (Secrets Manager); Azure unifies both
CSPM	Defender CSPM (Cloud Security Posture)	AWS Security Hub + Trusted Advisor	Defender CSPM includes attack path analysis; Security Hub aggregates findings from partners
AUDIT & LOGGING	Azure Monitor + Activity Log	CloudTrail + CloudWatch + Config	CloudTrail is immutable by default; Azure Activity Log requires explicit retention configuration
NETWORK SECURITY	NSG + Azure Firewall + DDoS Protection	Security Groups + Network Firewall + Shield	Both have stateful inspection; Azure Firewall is FQDN-aware; AWS Network Firewall is Suricata-based
COMPLIANCE DASHBOARD	Defender for Cloud — Compliance	AWS Security Hub — Standards	Both map to NIST, PCI DSS, HIPAA, ISO 27001 with real-time compliance scores

STEP 6 — ZERO TRUST IMPLEMENTATION

Zero Trust on Azure & AWS — principles into practice

Zero Trust is not a product you buy — it is an architecture you build. These principles translate “never trust, always verify” into concrete cloud security controls on both platforms.

Verify identity explicitly — every time

Enforce MFA for all users, including admins. Use Conditional Access (Azure) or identity-based policies (AWS) to evaluate risk signals at every login: device compliance, location, sign-in risk score, and time of access.

Grant least privilege access — always

No standing admin access. Use PIM (Azure) or IAM role assumption with STS (AWS) for just-in-time privilege. Audit effective permissions quarterly. Flag any role with AdministratorAccess or Owner that isn’t a break-glass account.

Assume breach — design for it

Segment every workload as if the perimeter is already compromised. No lateral movement paths between VNets/VPCs. Immutable logging to a separate Security account. Every service-to-service call authenticated with a managed identity or IAM role.

Monitor everything — continuously

Enable Defender for Cloud at Defender CSPM tier. Enable GuardDuty across all regions and all accounts in your organization. Set up SIEM alerts for privilege escalation, failed MFA, API calls from unusual geos, and root account usage.

Automate remediation — don’t rely on humans

Azure Policy DeployIfNotExists auto-remediates non-compliant resources. AWS Config Remediation Actions + Lambda close findings automatically. Human review should be reserved for high-severity, novel threats — not routine drift.

Encrypt everything — at rest and in transit

Customer-managed keys (CMK) in Key Vault or KMS for sensitive workloads. TLS 1.2 minimum enforced by policy. No HTTP endpoints — Azure Policy “deny” and SCP effect block non-TLS resource creation. Secrets in Key Vault / Secrets Manager only — never in code or environment variables.

STEP 7 — UNIFIED IAM WITH SAVIYNT

Saviynt — IGA across Azure & AWS at scale

Saviynt bridges the governance gap that native cloud tools leave open. With 500+ out-of-the-box controls, it provides a unified Identity Governance and Administration (IGA) layer across your entire Azure and AWS estate — enforcing consistency that no cloud-native tool does alone.

Saviynt connects directly to Microsoft Entra ID, Azure resources, AWS IAM, and AWS Organizations — pulling access data, running analytics, enforcing Separation of Duties (SoD), and automating the Joiner-Mover-Leaver lifecycle. It transforms scattered access permissions into a governed, auditable, and reviewable inventory that satisfies regulators and security teams alike.

CAPABILITY 01

Access request & approval

Business users request Azure role assignments or AWS permission sets through a self-service portal. Multi-level approval workflows route to the right approver — manager, data owner, security team — based on risk level and classification.

`JML lifecycle`

CAPABILITY 02

Access certifications

Quarterly or annual access reviews pushed to line managers. Each reviewer certifies or revokes Azure / AWS access directly from the Saviynt interface. Non-certified access is automatically revoked. Full audit trail for SOC 2 and ISO 27001.

`Audit-ready`

CAPABILITY 03

Separation of Duties (SoD)

Real-time SoD conflict detection across Azure RBAC and AWS IAM. Prevent a single identity from holding both “create payment” and “approve payment” rights. Policy violations are flagged before access is granted — not discovered in a year-end audit.

`Risk prevention`

CAPABILITY 04

500+ cloud security controls

Pre-built controls mapped to PCI DSS, HIPAA, SOC 2, ISO 27001, and NIST frameworks. Continuous monitoring of your Azure and AWS posture against these controls — with dashboards that show compliance percentage by regulation, by account, and by business unit.

`500+ controls`

CAPABILITY 05

Privileged access management

Just-in-time privileged access to Azure subscriptions and AWS accounts. Time-boxed sessions with full session recording. Automatic expiration of elevated access. PAM for cloud complements PIM and STS but adds cross-cloud visibility and a unified audit trail.

`Just-in-time PAM`

CAPABILITY 06

Analytics & risk scoring

Machine learning-based peer group analysis identifies outlier access — an engineer with permissions 3x broader than their peers is flagged automatically. Risk scores surface the riskiest identities across your Azure and AWS estate for targeted remediation.

`ML-powered`

STEP 8 — OPERATIONAL BEST PRACTICES

What high-maturity cloud security teams do differently

These are the controls and habits that separate organizations that get breached and spend six months recovering from those that detect, contain, and recover in hours. Implement them in this order.

Lock down root / Global Admin immediately

AWS root account: disable programmatic access, enable MFA hardware token, store credentials in a physical safe. Azure Global Admin: max 5 accounts, all with FIDO2 keys, all monitored. PIM-activate for all privileged operations — no standing access.

Enable logging across every region — day one

CloudTrail organization trail to a dedicated Log Archive account with S3 Object Lock. Azure Activity Log to a Log Analytics Workspace retained 90 days minimum. GuardDuty and Defender for Cloud enabled in every region — threats do not respect your "primary" region.

Use managed identities — never store secrets in code

Every Azure resource that calls another Azure service uses a Managed Identity. Every AWS workload uses an IAM Instance Profile or Task Role. Zero static credentials in environment variables, app settings, or source code. Rotate any key that has ever been committed to a repo.

Tag everything — governance requires metadata

Enforce tagging policy on all resources: data-classification, owner, cost-center, environment. Azure Policy deny creation without required tags. AWS Config rule flags untagged resources. Saviynt uses these tags to route access reviews to the correct data owner automatically.

Block public endpoints by default

Azure Policy deny effect: block creation of Storage Accounts with public blob access, SQL Servers without firewall rules, VMs with public IPs. AWS SCP: deny creation of public S3 buckets, internet-facing load balancers without WAF, security groups with 0.0.0.0/0 inbound on 22/3389.

Run access reviews quarterly — without exception

Saviynt or Entra ID Access Reviews for all Azure RBAC assignments. AWS IAM Access Analyzer for unused roles and policies. Any access uncertified for 90+ days is revoked automatically. No exceptions for VIPs — they review their own access like everyone else.

Test your incident response — before you need it

Run a quarterly tabletop: “Our management account root credentials were compromised. What do we do in the first 15 minutes?” Documented runbooks for: credential compromise, ransomware in a VNet, public S3 bucket containing PII, GuardDuty finding severity HIGH. Practice makes the real event survivable.

Implement Infrastructure as Code from day one

Terraform or Bicep for every resource. Security policies as code — not manual console clicks. IaC enables drift detection: anything that exists in the cloud but not in your repo is unauthorized. Pair with Azure DevOps or AWS CodePipeline with security scanning gates (Checkov, tfsec, Semgrep) in every pipeline.