JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Cloud Security Architecture for IT Managers Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Cloud Security Architecture for IT Managers Course

Cloud Security Architecture for IT Managers is a 2-week advanced training course for IT managers, cloud architects and infrastructure leads who decide how workloads are protected across public, private and hybrid cloud, and it ends with a cloud security architecture review of a live or reference estate. Most breaches in cloud environments now trace back to identity and configuration choices rather than provider failures. Jupiter Prime Training runs this course for the managers who own those choices.

Why Cloud Security Architecture for IT Managers Matters Now

Three forces shape cloud security decisions today: the speed of self-service provisioning, which lets teams create exposed storage or over-privileged roles in minutes; multi-cloud and SaaS sprawl, which scatters identities, keys and logs across consoles; and boards and clients who expect the same assurance in the cloud as on premises. An organisation with a sound architecture contains mistakes through guardrails and least privilege; one without it discovers public data buckets through a journalist or an extortion note. The course maps controls to the NIST Cybersecurity Framework 2.0 NIST CSF 2.0 and to the control themes of ISO/IEC 27001:2022.

Who Gains Most from Cloud Security Architecture for IT Managers

- IT managers who approve cloud adoption, budgets and provider contracts
- Cloud architects who design landing zones, networks and identity structures
- Infrastructure leads who run hybrid estates linking data centres and cloud tenants
- Platform owners who manage container and serverless environments
- Security liaisons who translate cloud findings into remediation for delivery teams

A cloud centre of excellence that sends its manager, lead architect and platform owner together gains most, because guardrails only work when design and operation agree on them.

Cloud Security Architecture for IT Managers Capabilities

Participants leave able to judge a cloud estate's design, close its biggest exposures and justify the choices to leadership.

- Specify shared responsibility boundaries for each service model — provider contracts and internal ownership
- Design identity and access structures built on least privilege and federation — cloud architects and auditors
- Weigh encryption and key management options, including customer-managed keys — data owners and legal counsel
- Apply cloud security posture management to detect misconfiguration — platform teams
- Assess container and serverless workload protections — DevOps leads

- Build cloud incident response playbooks across tenants and providers — security operations and service managers

Key Cloud Security Architecture for IT Managers Terms

- Shared responsibility model — The division of security duties between a cloud provider and its customer, which shifts with each service model.
- Landing zone — A pre-configured cloud environment with accounts, networking, identity and guardrails set up before workloads arrive.
- Cloud security posture management — Tooling that continuously checks cloud configurations against policy and flags risky settings such as public storage.
- Customer-managed key — An encryption key the customer controls, rotates and can revoke, rather than one held solely by the provider.
- Workload identity — A machine identity assigned to an application or service so it can access resources without stored passwords.
- Guardrail — A preventive or detective policy that stops or flags insecure cloud actions automatically, regardless of who attempts them.

Cloud Security Architecture for IT Managers Day by Day

Day 1: Cloud Risk from a Manager's Seat

- Cloud Breach Patterns — Identity and Configuration as Root Causes
- Service Models and Shared Responsibility — Ownership of Each Control
- NIST CSF 2.0 Functions in the Cloud — Coverage Gaps by Provider
- Multi-Cloud and SaaS Sprawl — Visibility Across Tenants
- Cloud Security Maturity Baseline — Starting Point for Investment

Day 2: Landing Zones and Reference Architecture

- Account and Subscription Hierarchy — Blast Radius Containment
- Landing Zone Guardrails — Preventive and Detective Policies
- Hub-and-Spoke Network Topology — Traffic Inspection Points
- Hybrid Connectivity Options — Private Links Versus Internet Paths
- Tagging and Resource Ownership Standards — Accountability for Spend and Risk

Day 3: Identity and Access in the Cloud

- Federation and Single Sign-On — One Identity Source for Staff
- Least Privilege Role Design — Permission Boundaries and Reviews
- Privileged Access and Break-Glass Accounts — Emergency Control Decisions
- Workload Identities and Secrets Handling — Removing Stored Credentials
- Conditional Access Policies — Device and Location Signals

Day 4: Data Protection and Key Management

- Data Classification for Cloud Storage — Placement and Residency Choices
- Encryption at Rest and in Transit — Default Versus Enforced Settings
- Key Management Services and Customer-Managed Keys — Control Versus Complexity
- Hardware Security Modules — High-Assurance Key Protection
- Backup Immutability and Cross-Region Copies — Ransomware Recovery Options

Day 5: Network Security and Segmentation

- Virtual Network Segmentation — Isolating Workloads by Sensitivity
- Cloud Firewalls and Security Groups — Rule Hygiene and Review
- Web Application Firewall and DDoS Protection — Internet-Facing Exposure
- Private Endpoints for Platform Services — Removing Public Access
- Zero Trust Network Access — Replacing Broad VPN Access

Day 6: Posture Management and Continuous Assurance

- Cloud Security Posture Management Tools — Misconfiguration Detection at Scale
- Policy as Code — Enforcing Standards in Deployment Pipelines
- Infrastructure as Code Scanning — Catching Errors Before Release
- Mapping Findings to ISO/IEC 27001:2022 Controls — Audit Evidence
- Remediation Prioritisation and Ownership — Closing Findings Fast

Day 7: Containers, Kubernetes and Serverless

- Container Image Provenance and Scanning — Trusted Build Supply Chain
- Kubernetes Role-Based Access and Network Policies — Cluster Hardening
- Runtime Protection for Containers — Detecting Malicious Behaviour
- Serverless Function Permissions — Event-Driven Attack Surface
- DevSecOps Pipeline Gates — Security Without Slowing Releases

Day 8: Logging, Monitoring and Cloud Incident Response

- Cloud Audit Logs and Centralised Collection — Evidence Across Tenants
- Threat Detection Services — Alert Tuning and Ownership
- Cloud Incident Response Playbooks — Compromised Keys and Exposed Storage
- Forensic Snapshots and Isolation — Preserving Evidence in the Cloud
- Provider Support and Escalation Paths — Coordinating During an Incident

Day 9: Governance, Contracts and Cost of Control

- Cloud Provider Due Diligence — Assurance Reports and Contract Terms
- SaaS Security Reviews — Third-Party Application Approval
- Security Cost Optimisation — Native Versus Third-Party Tooling
- Exit and Portability Planning — Avoiding Lock-In Risk
- Banking and Healthcare Cloud Cases — Sector Design Lessons

Day 10: Practising the Cloud Security Architecture Review

- Reference Estate Walkthrough — Applying Shared Responsibility Boundaries
- Identity and Data Protection Assessment — Gaps Against Target Design
- Posture and Container Findings Prioritisation — Remediation Sequence
- Leadership Briefing Rehearsal — Investment Case and Residual Exposure
- Cloud Security Architecture Review Completion — Findings, Target State and Roadmap

Applying Cloud Security Architecture for IT Managers After the Course

- Run a posture management scan across all cloud accounts and assign owners to the ten highest-risk misconfigurations
- Review privileged cloud roles against least privilege principles and remove standing administrator access where break-glass accounts can replace it

Cloud Security Architecture for IT Managers Questions FAQ

What is cloud security architecture for IT managers and why does it matter now?

Cloud security architecture for IT managers is the design of identity, data, network and monitoring controls that protect cloud workloads. It matters now because self-service provisioning and multi-cloud sprawl make misconfiguration the leading cause of cloud breaches.

Which roles gain most from cloud security architecture training for IT managers?

IT managers, cloud architects, infrastructure leads and platform owners gain most. You benefit if you approve cloud designs, own landing zones or must explain cloud exposure and investment needs to leadership.

How does cloud security architecture training for IT managers differ from a cloud engineering course?

It focuses on design decisions, guardrails and governance rather than configuring individual services by hand. You assess architectures, weigh control options and build a review, while specialist engineering courses go deeper into one provider's tools.

What do you bring back from cloud security architecture training for IT managers?

You bring back a structured review of a cloud estate's security design. It records findings, a target architecture, remediation priorities and a roadmap you can present to leadership and hand to delivery teams.

Cloud Security Architecture for IT Managers: The Way Forward

The cloud security architecture review first informs which guardrails and identity changes the platform team implements next. IT managers own it, architects maintain its target design and delivery teams work through its remediation list. After the first quarter, revisit the shared responsibility boundaries, because new SaaS and platform services often shift duties without anyone noticing.