BLACKBIRD FOR TRAINING

Enterprise Cloud Infrastructure Security and Risk Management Course

15 – 19 February 2027
Kuala Lumpur (Malaysia)

UK Traininig
PARTNER



Enterprise Cloud Infrastructure Security and Risk Management Course

Ref: 104_363803 **Date:** 15 – 19 February 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction:

In this one-week Enterprise Cloud Infrastructure Security and Risk Management course, you learn to assess, secure and govern the platforms your organisation runs in the cloud, from identities and networks to workloads, data and suppliers. You build a cloud infrastructure security risk and governance plan that links every identified risk to a named control, an owner and a recovery target. You should already work with cloud services or infrastructure and understand basic networking, identity and security concepts. You practise through case studies, working on realistic architecture diagrams, configuration exports, supplier responses and incident timelines drawn from several sectors.

Course Objectives:

- Map your cloud estate against the CSA Shared Security Responsibility Model and score its risks in a likelihood-impact register.
- Draft identity lifecycle and privileged access rules for your cloud accounts using NIST SP 800-210 guidance.
- Build a network isolation and data protection control matrix for your workloads using ISO/IEC 27017 controls.
- Test your workload configurations against approved baselines using policy-as-code rules and posture scan results.
- Score your cloud suppliers with a CCM-based questionnaire and draft an incident runbook for your monitoring team.
- Present a resilience and compliance plan that maps your controls to recovery objectives and ISO/IEC 27001 evidence.

Target Audience:

- You build and operate cloud infrastructure, networks or landing zones and need security controls that hold up in production.
- You analyse security alerts, review architectures or design controls for cloud workloads and services.
- You assess IT risk, gather compliance evidence or answer audit requests about the cloud services your organisation uses.
- You run a cloud platform or operations team and decide which risks to treat, accept or escalate.
- You review cloud suppliers, contracts or integrations and need a structured way to judge their security.



Course Outline:

Day 1: Assess Enterprise Cloud Environments and Risk Requirements

- Mapping Cloud Service Models Against the Shared Responsibility Model
- Profiling Enterprise Cloud Threats Using a Threat Modelling Canvas
- Scoring Cloud Infrastructure Risks With a Likelihood-Impact Matrix
- Deriving Security Requirements From CSA Cloud Controls Matrix Domains
- Build: Cloud Asset Inventory and Initial Risk Register

Day 2: Design Identity Controls and Secure Cloud Connectivity

- Designing Identity Lifecycle Workflows for Joiners, Movers and Leavers
- Applying NIST SP 800-210 Access Control Guidance to Cloud Roles
- Controlling Privileged Access With Just-in-Time Elevation and Session Recording
- Segmenting Cloud Networks Using Private Endpoints and Security Groups
- Build: Identity and Network Isolation Control Matrix

Day 3: Protect Cloud Data and Harden Workloads

- Classifying Cloud Data With an Encryption and Key Management Matrix
- Applying ISO/IEC 27017 Controls to Data Retention and Deletion
- Hardening Virtual Machines and Containers Against Approved Configuration Baselines
- Detecting Configuration Drift With Policy-as-Code and Posture Scans
- Build: Data Protection and Workload Hardening Checklist

Day 4: Analyse Third-Party Risk and Coordinate Cloud Incidents

- Assessing Cloud Providers With a CCM-Based Supplier Security Questionnaire
- Tracing Supply Chain Risk Through Dependencies and Third-Party Integrations
- Centralising Cloud Audit Logs Into a Security Monitoring Pipeline
- Running Cloud Incident Triage With a Shared Escalation Playbook
- Build: Third-Party Risk Scorecard and Cloud Incident Runbook

Day 5: Case Study: Test Resilience and Finalise Cloud Governance

- Testing Recovery Time and Point Objectives Against Your Risk Register
- Rehearsing a Cloud Service Outage Using Your Incident Runbook
- Mapping Your Control Matrix to ISO/IEC 27001 Compliance Evidence
- Presenting Residual Risk and Governance Decisions to a Review Panel
- Build: Cloud Infrastructure Security Risk and Governance Plan



Skills You Will Gain:

- Shared Responsibility Mapping
- Cloud Risk Register Scoring
- Privileged Access Design
- Network Segmentation Planning
- Encryption Key Management
- Configuration Drift Detection
- Supplier Security Assessment
- Cloud Incident Escalation

Why Attend This Course:

- Score real cloud risks in a register you can reuse for your own estate the following week.
- Rehearse a cloud outage with your own incident runbook before you ever need it live.
- Compare supplier answers with a questionnaire you can send to your next cloud vendor.
- Leave with a cloud infrastructure security risk and governance plan ready to present to your platform owners.

Conclusion:

In your first week back, open your cloud infrastructure security risk and governance plan and replace the case data with your own accounts, workloads and suppliers, starting with the three risks you scored highest. Walk your platform owner, security lead and risk or compliance colleague through the control matrix, and agree an owner and a target date for each treatment. After the first change goes live, check that the related logs reach your monitoring pipeline, that the runbook escalation path still works and that the evidence you mapped is actually being produced.

Frequently Asked Questions FAQ:

What will you be able to do after the Enterprise Cloud Infrastructure Security and Risk Management course?

You will be able to score cloud infrastructure risks, design identity, network, data and workload controls, assess cloud suppliers, coordinate incident response and map your controls to recovery objectives and compliance evidence, all recorded in one risk and governance plan you can apply to your own platforms.

What do you need to know before starting cloud infrastructure security and risk management training?

You need working experience with at least one cloud platform or with infrastructure operations, plus a basic grasp of networking, identity and security terms. You do not need prior risk management training; the course shows you how to score and treat risks step by step.



What do you build during the cloud infrastructure security and risk management course?

You build a cloud infrastructure security risk and governance plan. Each day adds a part: an asset inventory and risk register, an identity and isolation matrix, a hardening checklist, a supplier scorecard and incident runbook, then recovery targets and compliance mapping.

How does this cloud infrastructure security and risk management course differ from general risk or certification courses?

General enterprise risk courses treat risk across the whole organisation, and certification courses follow an exam syllabus. This course stays on cloud infrastructure, joining hands-on controls with risk scoring and governance, so engineers, analysts and risk staff work on the same plan together.

