

Cloud Security: Shared Responsibility and Control Implementation

Professional Training Course

Skillslab Training Provider

Skills for Tomorrow's World 



Course Description

Introduction

Cloud security has become a strategic priority for government entities, ministries, public sector organizations, and large enterprises that rely on cloud services to modernize operations, protect sensitive data, and maintain digital trust. As cloud adoption expands across infrastructure, platforms, applications, and data environments, organizations must clearly understand the shared responsibility model, define security ownership, and implement effective cloud security controls across every layer of the cloud ecosystem. This professional training course provides a practical and executive-level approach to cloud security governance, cloud risk management, compliance alignment, identity and access control, data protection, monitoring, and operational resilience. The course is designed to help organizations reduce cloud security gaps, strengthen accountability between cloud providers and customers, and implement controls that support secure cloud transformation. Its executive-level value proposition lies in enabling decision-makers and technical leaders to translate cloud security strategy into measurable protection, stronger governance, regulatory readiness, and sustainable operational confidence.

Course Objectives

- Understand the cloud shared responsibility model across public, private, hybrid, and multi-cloud environments.
- Identify security responsibilities owned by the cloud provider, the customer, and third-party service partners.
- Evaluate cloud security risks related to identity, access, data, applications, infrastructure, configuration, and operations.
- Implement practical cloud security controls aligned with governance, risk, compliance, and cybersecurity frameworks.
- Strengthen identity and access management through privileged access control, role-based permissions, and zero trust principles.
- Apply cloud data protection measures including encryption, key management, classification, backup, and retention.
- Improve cloud compliance readiness for government entities, regulated sectors, and enterprise environments.

- Build a practical roadmap for cloud security control implementation and continuous improvement.

Course Content

Day 1: Cloud Security Foundations and Shared Responsibility

- Overview of cloud computing models: infrastructure services, platform services, software services, hybrid cloud, and multi-cloud.
- Key cloud security challenges facing government entities, ministries, and large corporations.
- Understanding the shared responsibility model and its impact on accountability.
- Differences between provider-managed and customer-managed security responsibilities.
- Cloud security governance roles, ownership models, and decision-making structures.
- Common cloud security failures caused by unclear responsibility boundaries.
- Mapping business risk to cloud security responsibilities.
- Practical exercise: identifying responsibility ownership across cloud service scenarios.

Day 2: Cloud Governance, Risk Management, and Compliance Controls

- Establishing cloud security governance for enterprise and public sector environments.
- Cloud risk assessment methods for sensitive workloads and critical services.
- Regulatory compliance considerations for government cloud adoption.
- Control implementation planning for cloud security programs.
- Policy management, cloud standards, security baselines, and control libraries.
- Vendor risk management and cloud service provider assurance.
- Cloud audit readiness and evidence collection.
- Practical exercise: building a cloud security responsibility and control matrix.

Day 3: Identity, Access, Data Protection, and Secure Configuration

- Identity and access management as a core cloud security control.
- Role-based access control, privileged access management, and least privilege principles.
- Multi-factor authentication and conditional access strategies.
- Zero trust security concepts in cloud environments.
- Data classification, encryption, tokenization, and key management.

Day 4: Cloud Infrastructure, Application Security, Monitoring, and Incident Response

- Securing cloud networks, workloads, containers, virtual machines, and serverless environments.
- Secure cloud architecture principles for critical systems.
- Application security and secure software deployment in cloud environments.
- Logging, monitoring, threat detection, and cloud security analytics.
- Security information and event management integration for cloud operations.
- Cloud incident response planning and escalation procedures.
- Evidence handling and forensic readiness in cloud environments.
- Practical exercise: developing a cloud incident response and monitoring checklist.

Day 5: Control Implementation Roadmap and Continuous Improvement

- Designing a cloud security control implementation roadmap.
- Prioritizing controls based on risk, compliance, business impact, and operational maturity.
- Continuous control monitoring and security posture management.
- Cloud security metrics, reporting dashboards, and executive visibility.
- Building cross-functional collaboration between security, compliance, operations, procurement, and business teams.
- Cloud security maturity assessment and improvement planning.
- Final workshop: developing an actionable cloud security implementation plan.
- Course review, practical recommendations, and implementation guidance.

Target Audience

- Government executives and public sector decision-makers responsible for digital transformation and cloud adoption.
- Chief information security officers, cybersecurity managers, and information security professionals.
- Cloud architects, cloud engineers, infrastructure managers, and information technology leaders.
- Risk, governance, compliance, and internal audit professionals.
- Data protection officers and privacy professionals working with cloud-based systems.
- Procurement and vendor management teams involved in cloud service evaluation.
- Business continuity, resilience, and incident response teams.
- Project managers and transformation leaders responsible for secure cloud implementation.

- No advanced technical cloud engineering background is required.
- Participants are encouraged to bring examples of cloud security challenges, compliance requirements, or implementation concerns from their organizations.

Training Methodology

This course uses a practical, interactive, and results-oriented training methodology designed for executive professionals and enterprise teams. The program combines expert-led instruction, real-world case discussions, cloud security control examples, guided analysis, group exercises, practical templates, and implementation workshops. Participants will examine realistic cloud security scenarios, assess shared responsibility gaps, review control implementation priorities, and develop practical action plans that can be adapted to government entities, ministries, public sector organizations, and large corporations. The methodology focuses on translating cloud security concepts into operational decisions, governance improvements, and measurable risk reduction.

Learning Outcomes

By the end of this course, participants will be able to:

- Explain the cloud shared responsibility model and apply it to different cloud service models.
- Identify security responsibilities across provider, customer, and third-party environments.
- Assess cloud security risks and prioritize controls based on business and regulatory impact.
- Implement cloud security controls for identity, access, data protection, monitoring, configuration, and incident response.
- Strengthen cloud governance structures and improve accountability across teams.
- Develop cloud security policies, control matrices, and implementation roadmaps.
- Improve compliance readiness and audit evidence management for cloud environments.
- Reduce exposure to cloud misconfiguration, unauthorized access, data leakage, and operational disruption.
- Support secure cloud transformation through practical governance and control implementation.
- Communicate cloud security priorities clearly to executive stakeholders and operational teams.

Instructor Profile

The training will be delivered by an internationally certified expert with extensive practical and consulting experience. The instructor brings deep expertise in cloud security, cybersecurity governance, risk management, compliance implementation, cloud control frameworks, secure cloud architecture, incident response, and

Contact Us

For registration inquiries, upcoming dates, or group pricing, please contact us:

Websitewww.skillslab-training.com**Email**info@skillslab-training.com**WhatsApp**

+966 559 653 447

Generated by Skillslab Traininginfo@skillslab-training.com | WhatsApp: +966 559 653 447www.skillslab-training.com