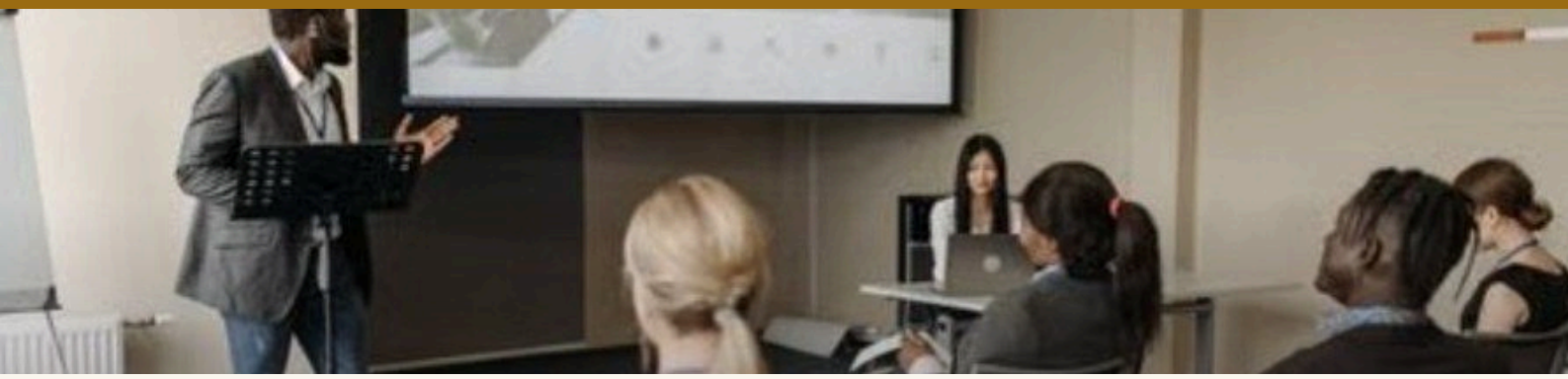


SEYA CAPITAL
INSIGHT.STRATEGY.GROWTH

INFORMATION & COMMUNICATION TECHNOLOGY

Cloud Management and Security, Principles and Best Practice

Securing Cloud Environments, Optimising Cloud Operations & Enabling Digital Transformation

SECTOR	FORMATS	FEE FROM	2027 SESSIONS
Information & Communication Technology	5 days & 2 weeks	US$ 2,100	3

OVERVIEW

About this course

Cloud computing has become the foundation of modern digital transformation, enabling organisations to achieve greater agility, scalability, innovation, and operational efficiency. However, cloud adoption also introduces significant challenges relating to governance, security, compliance, risk management, data protection, service availability, and operational control.

The Seya Capital Cloud Management and Security: Principles and Best Practice Certificate Course equips participants with the knowledge, frameworks, methodologies, and practical skills required to effectively manage, secure, govern, and optimise cloud environments. The programme combines cloud management best practices with cloud security principles to ensure organisations can maximise the benefits of cloud technologies while effectively managing risks.

Participants will gain practical insights into cloud governance, cloud security architecture, risk management, compliance requirements, cloud service management, identity and access management, business continuity, and cloud optimisation strategies.

2027 SCHEDULE

Dates, venues & fees

DATES	VENUE	FORMAT	FEE PER DELEGATE
15 – 19 Nov 2027	Zanzibar, Tanzania	5 days	**US$ 2,100**
22 Nov – 3 Dec 2027	Singapore	2 weeks	**US$ 6,660**
29 Nov – 3 Dec 2027	Singapore	5 days	**US$ 3,700**

Fees exclude travel and accommodation. This course is also available in-house, on dates and at a venue of your choice.

HIGHLIGHTS

What you will learn

- Cloud computing principles and service models
- Cloud governance and management frameworks
- Cloud security architecture and design
- Cloud risk management and compliance
- Identity and Access Management (IAM) in cloud environments
- Cloud data protection and encryption
- Hybrid, multi-cloud, and cloud-native security
- Business continuity and disaster recovery in the cloud
- Cloud monitoring and performance optimisation
- Cloud service management and operational excellence
- Security incident management in cloud environments
- Cloud security best practices and governance
- Participants will explore practical applications including:
- Cloud Readiness Assessments
- Cloud Risk Assessments
- Cloud Security Architecture Reviews
- IAM Configuration and Review
- Data Protection and Encryption Planning
- Compliance and Governance Assessments
- Disaster Recovery Planning
- Cloud Monitoring and Performance Analysis
- Cloud Cost Optimisation Projects
- Cloud Incident Response Simulations
- Vendor Risk Reviews
- Enterprise Cloud Strategy Development

OBJECTIVES

By the end of the course

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

- Understand cloud computing concepts, technologies, and deployment models.
- Develop and implement effective cloud governance frameworks.
- Design and manage secure cloud architectures.
- Identify and manage cloud-related risks and vulnerabilities.
- Implement cloud security controls and protection mechanisms.
- Secure cloud identities, applications, and data assets.

- Support compliance with regulatory and security requirements.
- Develop cloud resilience and disaster recovery strategies.
- Optimise cloud operations, performance, and costs.
- Apply cloud management and security best practices across enterprise environments.

WHO SHOULD ATTEND

Designed for

Cloud Administrators | Cloud Architects | ICT Managers | Information Security Managers | Cybersecurity Professionals | IT Infrastructure Managers | Systems Administrators | Network Engineers | Risk Management Professionals | Compliance Officers | Enterprise Architects | Technology Consultants | Digital Transformation Leaders | ICT Directors and Technology Executives

PROGRAMME

Course outline

Day 1: Foundations of Cloud Computing and Cloud Management

- Introduction to Cloud Computing
- Cloud Service Models (IaaS, PaaS, SaaS)
- Cloud Deployment Models
- Cloud Adoption Drivers and Challenges
- Cloud Governance Fundamentals
- Cloud Operating Models
- Best Practices for Cloud Management

Day 2: Cloud Security Principles and Architecture

- Cloud Security Fundamentals
- Shared Responsibility Model
- Secure Cloud Architecture Design
- Security Controls in Cloud Environments
- Threats and Vulnerabilities in Cloud Platforms
- Cloud Security Frameworks
- Security-by-Design Principles

Day 3: Identity, Access Management and Data Protection

- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Privileged Access Management
- Cloud Data Classification and Protection
- Encryption Technologies
- Key Management Strategies
- Data Privacy and Compliance Requirements

Day 4: Cloud Risk Management, Compliance and Resilience

- Cloud Risk Assessment Methodologies
- Regulatory Compliance in Cloud Environments
- Security Monitoring and Logging
- Cloud Incident Response
- Business Continuity and Disaster Recovery
- Cyber Resilience Strategies
- Vendor and Third-Party Risk Management

Day 5: Cloud Optimisation, Governance and Capstone Project

- Cloud Cost Management and Optimisation
- Cloud Performance Monitoring
- Multi-Cloud and Hybrid Cloud Governance
- Cloud Service Management Best Practices
- Emerging Trends in Cloud Computing
- Developing a Cloud Governance Roadmap
- Capstone Cloud Security and Management Case Study

METHODOLOGY

How you will learn

This highly interactive programme combines:

- Expert-led presentations
- Cloud security workshops
- Cloud governance and management exercises
- Cloud risk assessment simulations
- Security architecture design activities
- Cloud deployment case studies
- Compliance and governance reviews
- Group discussions and collaborative learning
- Cloud optimisation exercises
- Capstone cloud management and security project

Participants will gain practical experience in cloud governance, cloud security management, cloud risk assessment, and cloud operations optimisation.

IMPACT

The return on learning

For your organisation

- Strengthen cloud governance and oversight
- Improve cloud security and resilience
- Reduce cloud-related operational and security risks
- Improve regulatory compliance and audit readiness
- Enhance business continuity and disaster recovery capabilities
- Improve utilisation and management of cloud resources
- Optimise cloud performance and operational efficiency
- Strengthen data protection and privacy controls
- Support digital transformation and innovation initiatives
- Improve organisational agility and scalability

For you

- Develop advanced cloud management and security expertise
- Strengthen cloud governance and compliance skills
- Improve cloud architecture and security design capabilities
- Gain practical experience in cloud operations and risk management
- Enhance cybersecurity and cloud resilience competencies
- Improve strategic decision-making regarding cloud technologies
- Enhance professional credibility in cloud computing and security
- Increase career opportunities in cloud management and cybersecurity

CERTIFICATION

Seya Capital certificate

Upon successful completion of the programme, participants will be awarded the prestigious:

Seya Capital Certificate in Cloud Management and Security: Principles and Best Practice

Recognising professional competence in cloud management, cloud governance, cloud security architecture, identity and access management, cloud risk management, compliance management, data protection, cyber resilience, disaster recovery, cloud optimisation, and enterprise cloud transformation.

SEYA CAPITAL
INSIGHT · STRATEGY · GROWTH

Register or enquire

info@seyacapital.com
www.seyacapital.com

The Kenya Police Sacco Plaza, 2nd Floor, Wing B
Ngara Road, off Muranga Road
P.O. Box 63978 – 00619, Nairobi, Kenya