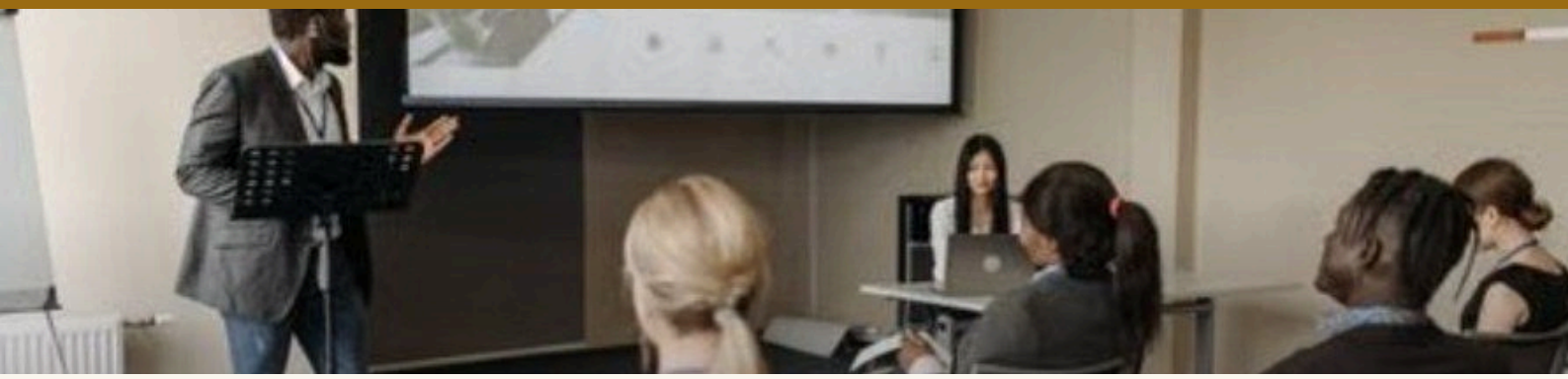


SEYA CAPITAL
INSIGHT.STRATEGY.GROWTH

INFORMATION & COMMUNICATION TECHNOLOGY

Cyber Security

Protecting Digital Assets, Managing Cyber Risks & Building Organisational Cyber Resilience

SECTOR	AVAILABILITY	DELIVERY
Information & Communication Technology	On request	Open or in-house

OVERVIEW

About this course

As organisations increasingly depend on digital technologies, cloud platforms, mobile applications, and interconnected systems, cybersecurity has become a strategic business priority. Cyber threats such as ransomware, phishing attacks, data breaches, insider threats, and cyber espionage continue to grow in sophistication, posing significant operational, financial, legal, and reputational risks.

The Seya Capital Cyber Security Training Course equips participants with the knowledge, skills, tools, and practical techniques required to identify, prevent, detect, respond to, and recover from cybersecurity threats. The programme provides a comprehensive understanding of cybersecurity fundamentals, security governance, threat management, network security, data protection, cloud security, incident response, and cyber resilience.

Participants will gain practical exposure to leading cybersecurity frameworks, technologies, and best practices required to effectively secure organisational information assets and digital environments.

SCHEDULE

Dates, venues & fees

Dates and fees for this programme are available on request. It can be scheduled as open enrolment or delivered in-house for your team. Contact info@seyacapital.com.

HIGHLIGHTS

What you will learn

- Cybersecurity fundamentals and threat landscape
- Cybersecurity governance and risk management
- Network and infrastructure security
- Security operations and threat monitoring
- Identity and Access Management (IAM)
- Endpoint and device security
- Data protection and cryptography
- Cloud security principles and controls
- Incident response and cyber crisis management
- Vulnerability management and threat intelligence
- Business continuity and cyber resilience
- Cybersecurity compliance and regulatory requirements

- Participants will explore practical applications including:
- Cybersecurity Risk Assessments
- Security Policy Development
- Network Security Reviews
- Vulnerability Assessments
- Threat Intelligence Analysis
- Incident Response Simulations
- Access Control Reviews
- Security Monitoring Exercises
- Data Protection Assessments
- Cyber Resilience Planning
- Cloud Security Evaluations
- Security Awareness Programme Development

OBJECTIVES

By the end of the course

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

- Understand the principles and foundations of cybersecurity.
- Identify and assess cybersecurity threats and vulnerabilities.
- Implement effective security controls and safeguards.
- Strengthen organisational cybersecurity governance and oversight.
- Protect networks, systems, applications, and data assets.
- Manage cybersecurity risks and security incidents effectively.
- Implement data protection and access control measures.
- Enhance threat detection, monitoring, and response capabilities.
- Improve organisational cyber resilience and business continuity.
- Support compliance with cybersecurity standards and regulations.

WHO SHOULD ATTEND

Designed for

- Information Security Officers
- Cybersecurity Professionals
- IT Managers
- Systems Administrators
- Network Administrators
- Risk Management Professionals
- Compliance Officers
- IT Auditors
- ICT Managers and Directors
- Security Operations Centre (SOC) Personnel
- Digital Transformation Leaders
- Technology Consultants
- Business Continuity Professionals
- Professionals seeking careers in cybersecurity

PROGRAMME

Course outline

Day 1: Cybersecurity Fundamentals and Threat Landscape

- Introduction to Cybersecurity
- Cyber Threat Landscape
- Common Types of Cyber Attacks
- Cybersecurity Principles and Concepts
- Cybersecurity Frameworks and Standards
- Cybersecurity Governance Fundamentals
- Roles and Responsibilities in Cybersecurity

Day 2: Cybersecurity Risk Management and Governance

- Cyber Risk Management Frameworks
- Risk Identification and Assessment
- Security Risk Analysis Techniques
- Security Policies and Procedures
- Security Governance Structures
- Regulatory and Compliance Requirements
- Cybersecurity Programme Management

Day 3: Network Security and Infrastructure Protection

- Network Security Architecture
- Firewalls and Security Appliances
- Intrusion Detection and Prevention Systems
- Secure Remote Access
- Wireless Security
- Network Monitoring and Protection
- Zero Trust Security Concepts

Day 4: Information Security Operations and Incident Response

- Security Operations Centres (SOC)
- Threat Intelligence
- Security Monitoring and Logging
- Incident Detection and Investigation
- Incident Response Methodology
- Cyber Crisis Management
- Post-Incident Analysis and Reporting

Day 5: Cloud Security, Data Protection and Cyber Resilience

- Cloud Security Fundamentals
- Identity and Access Management (IAM)
- Data Protection and Encryption
- Business Continuity and Disaster Recovery
- Cyber Resilience Strategies
- Emerging Cybersecurity Trends
- Capstone Cybersecurity Case Study and Action Planning

METHODOLOGY

How you will learn

This highly interactive programme combines:

- Expert-led presentations
- Hands-on cybersecurity workshops
- Cyber attack simulations
- Real-world cybersecurity case studies
- Security assessment exercises
- Group discussions and collaborative learning
- Threat modelling workshops
- Incident response simulations
- Security tool demonstrations
- Capstone cyber resilience project

Participants will gain practical experience in identifying cybersecurity threats, evaluating risks, implementing controls, and responding to incidents.

IMPACT

The return on learning

For your organisation

- Strengthen overall cybersecurity posture
- Reduce exposure to cyber threats and attacks
- Improve cybersecurity governance and accountability
- Enhance incident response and recovery capabilities
- Improve protection of critical information assets
- Strengthen employee cybersecurity awareness
- Improve regulatory compliance and security readiness
- Enhance operational resilience
- Support secure digital transformation programmes
- Increase stakeholder confidence in cybersecurity practices

For you

- Develop comprehensive cybersecurity knowledge and skills
- Improve cyber risk assessment capabilities
- Strengthen incident response and security management expertise
- Enhance technical and analytical capabilities
- Gain practical knowledge of security technologies and frameworks
- Improve decision-making regarding cybersecurity risks
- Enhance professional credibility and career opportunities
- Develop competencies required for cybersecurity leadership roles

CERTIFICATION

Seya Capital certificate

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

Seya Capital Certificate in Cyber Security

Recognising professional competence in cybersecurity governance, cyber risk management, network security, threat management, incident response, cloud security, data protection, cyber resilience, security operations, and enterprise cybersecurity programme management.

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