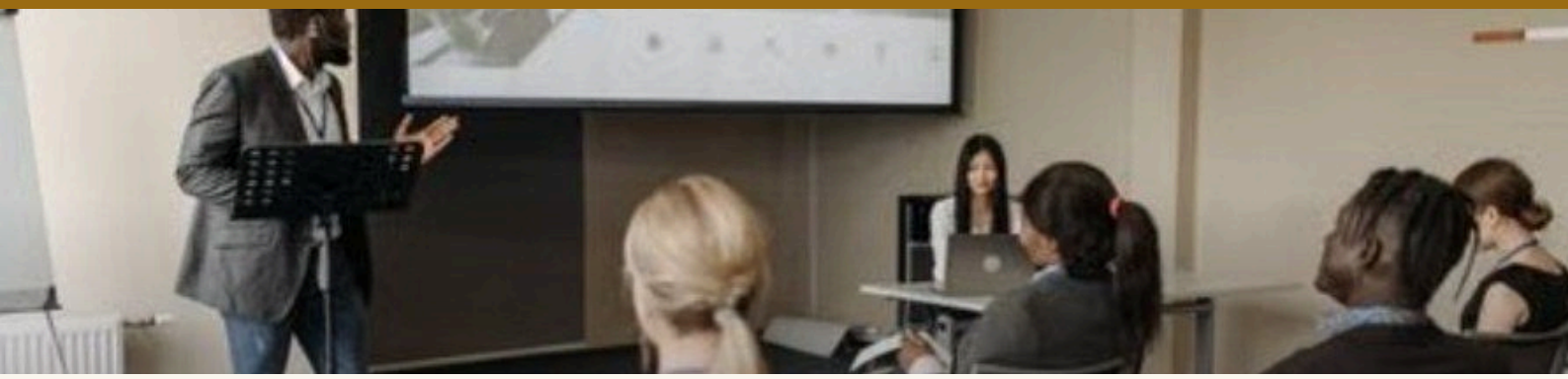


SEYA CAPITAL
INSIGHT.STRATEGY.GROWTH

INFORMATION & COMMUNICATION TECHNOLOGY

AI for ICT Risk and Security Management in the Public Sector Professional Certificate Programme

Strengthening ICT Risk Governance, Cyber Resilience and Intelligent Security Management Through Artificial Intelligence

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

OVERVIEW

About this course

As governments continue to digitise public services and modernise ICT infrastructure, managing technology risks and safeguarding information assets have become critical priorities. Public sector organisations face increasing threats from cyberattacks, data breaches, system failures, operational disruptions, regulatory compliance challenges, and emerging technology risks. Artificial Intelligence (AI) is transforming how organisations identify, assess, monitor, mitigate, and respond to these risks.

The Seya Capital AI for ICT Risk and Security Management in the Public Sector Professional Certificate Programme equips ICT professionals, risk managers, cybersecurity practitioners, auditors, compliance officers, and public sector leaders with the knowledge, frameworks, tools, and practical skills required to leverage AI in managing ICT risks and strengthening organisational security.

The programme covers AI-powered risk intelligence, cybersecurity risk management, ICT governance, threat analytics, security monitoring, compliance management, operational resilience, risk automation, data protection, business continuity, and emerging technologies in ICT risk and security management.

Participants will gain practical insights into how AI can enhance risk detection, strengthen security controls, improve governance oversight, and support resilient digital government operations.

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

- Fundamentals of ICT risk and security management
- Artificial Intelligence applications in risk management
- AI-powered cyber risk assessment and monitoring
- Intelligent threat intelligence and security analytics
- ICT governance, risk and compliance (GRC) frameworks
- AI-enabled security operations and incident response
- Data privacy and information protection strategies
- Business continuity and digital resilience planning
- Risk automation and predictive analytics
- AI-supported audit and compliance monitoring
- Security performance measurement and reporting
- Emerging trends in ICT security and risk management
- Participants will explore practical applications including:
- ICT Risk Assessments
- Cyber Risk Monitoring Programmes
- AI-Powered Threat Intelligence Platforms
- Security Analytics Dashboards
- Governance, Risk and Compliance Framework Development
- Security Control Assessments
- Vulnerability Management Programmes
- Digital Resilience Planning
- Incident Response Simulations
- Information Security Risk Registers
- Business Continuity Strategy Development
- Enterprise ICT Risk Transformation Roadmaps
- AI-Powered ICT Risk Management
- Predictive risk analytics
- Continuous risk monitoring
- Risk intelligence platforms
- Automated risk assessment frameworks
- Cybersecurity Risk and Resilience
- Cyber threat intelligence
- Security operations and monitoring
- Incident response planning
- Digital resilience management
- Governance, Risk and Compliance (GRC)
- ICT governance frameworks
- Compliance management systems
- AI-enabled audit and assurance
- Risk governance and reporting
- Public Sector Security Transformation
- Government risk management strategies
- Secure digital transformation initiatives
- Public sector cyber resilience frameworks
- Future-ready security governance models

OBJECTIVES

By the end of the course

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

- Understand ICT risk management principles within public sector environments.
- Apply AI technologies to enhance risk identification and assessment processes.
- Strengthen cybersecurity risk management and security governance practices.
- Improve risk monitoring through intelligent analytics and automation.
- Develop ICT risk treatment and mitigation strategies.
- Implement AI-powered security monitoring and threat detection mechanisms.
- Support regulatory compliance and governance requirements.
- Improve organisational resilience and business continuity capabilities.
- Build integrated ICT risk and security management frameworks.
- Lead secure digital transformation initiatives within government institutions.

WHO SHOULD ATTEND

Designed for

ICT Risk Managers | Cybersecurity Managers | Information Security Officers | ICT Directors and Managers | Chief Information Security Officers (CISOs) | Internal Auditors | Risk and Compliance Officers | Systems and Network Administrators | Data Protection Officers | Enterprise Risk Management Professionals | Government ICT Professionals | Technology Consultants | Digital Transformation Teams | Public Sector Governance Professionals

PROGRAMME

Course outline

Day 1: Foundations of ICT Risk and Security Management

- Introduction to ICT Risk Management
- ICT Security and Information Assurance Principles
- Public Sector Risk and Security Challenges
- Risk Governance and Oversight Frameworks
- Risk Management Life Cycle
- Introduction to AI in Risk and Security Management
- Emerging Risk Landscape in Digital Government

Day 2: AI-Powered Risk Assessment and Intelligence

- AI-Driven Risk Identification Techniques
- Predictive Risk Analytics
- Risk Quantification and Prioritisation
- AI-Based Threat Intelligence
- Continuous Risk Monitoring Approaches
- Intelligent Risk Dashboards and Reporting
- Risk Data Management and Analytics

Day 3: Cybersecurity Risk Management and Security Operations

- Cyber Risk Management Frameworks
- AI-Powered Threat Detection Systems
- Security Analytics and Monitoring
- Security Operations Centre (SOC) Concepts
- Incident Response and Recovery Planning
- Vulnerability Management and Security Testing
- Critical Infrastructure Protection

Day 4: Governance, Compliance and Digital Resilience

- ICT Governance Frameworks
- Governance, Risk and Compliance (GRC) Integration
- Regulatory and Policy Compliance Requirements
- Data Privacy and Information Protection
- Business Continuity and Disaster Recovery Planning
- Operational Resilience Strategies
- AI-Supported Compliance Monitoring

Day 5: Enterprise Risk Transformation, Innovation and Capstone Project

- Developing ICT Risk Management Strategies
- AI Adoption for Enterprise Security Management
- Risk Automation and Intelligent Controls
- Security Performance Measurement and Metrics
- Future Trends in ICT Risk and Security Management
- Building Risk-Aware Digital Organisations
- Capstone AI-Powered ICT Risk Management Project

METHODOLOGY

How you will learn

This highly interactive programme combines:

- Expert-led presentations
- ICT risk management workshops
- AI security demonstrations
- Cybersecurity risk simulations

- Governance and compliance case studies
- Security analytics practical sessions
- Risk assessment and control evaluation exercises
- Public sector security scenarios
- Group discussions and collaborative learning
- Capstone ICT risk and security transformation project

Participants will gain practical exposure to AI-driven risk management tools and intelligent security frameworks.

IMPACT

The return on learning

For your organisation

- Strengthen ICT risk governance and oversight
- Improve cybersecurity preparedness and resilience
- Enhance threat detection and response capabilities
- Improve regulatory compliance and audit readiness
- Reduce operational and technology-related risks
- Strengthen business continuity and disaster recovery capabilities
- Improve protection of critical information assets
- Support secure and resilient digital transformation
- Improve decision-making through intelligent risk analytics
- Build a culture of proactive risk management

For you

- Develop expertise in AI-enabled ICT risk management
- Strengthen cybersecurity governance and security management skills
- Improve risk analysis and decision-making capabilities
- Gain practical understanding of intelligent security technologies
- Enhance compliance and governance competencies
- Strengthen professional credibility and career opportunities
- Improve strategic thinking in technology risk management
- Build competencies required for modern ICT governance environments

CERTIFICATION

Seya Capital certificate

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

Seya Capital Professional Certificate in AI for ICT Risk and Security Management in the Public Sector

Recognising professional competence in ICT risk management, AI-powered risk analytics, cybersecurity governance, intelligent threat detection, security operations, compliance management, digital resilience,

business continuity planning, governance, risk and compliance (GRC) frameworks, and the implementation of AI-enabled ICT risk and security management systems within public sector organisations.

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