BLACKBIRD FOR TRAINING

Information Security & Cyber Security Fundamentals Course

22 – 26 February 2027
Cape Town (South Africa)



Information Security & Cyber Security Fundamentals Course

Ref: 321492_140392 **Date:** 22 – 26 February 2027 **Location:** Cape Town (South Africa) **Fees:** 4900 GBP

Why This Course

In today's digital era, organizations face an ever-growing landscape of cyber threats, data breaches, and security vulnerabilities. Protecting critical information and IT infrastructure is no longer optional—it is essential for business continuity, regulatory compliance, and stakeholder trust.

Professionals responsible for safeguarding information must understand both the technical and strategic aspects of cyber security. They need the skills to assess threats, manage risks, implement controls, and respond effectively to incidents.

This intensive 1-week program equips participants with the knowledge, tools, and practical strategies required to strengthen an organization's information security posture and respond confidently to evolving cyber challenges.

What You'll Learn and Practice

By joining this course, you will:

- Understand the core principles and frameworks of information security and cyber security
- Identify, assess, and mitigate common cyber threats and vulnerabilities
- Implement effective security controls across networks, applications, and data systems
- Develop incident response plans and business continuity strategies
- Apply best practices to protect organizational assets and sensitive information
- Navigate the legal, ethical, and regulatory aspects of information security

The Program Flow

Day 1: Introduction to Information Security

- Fundamentals of information security and key terminology
- The CIA triad: confidentiality, integrity, and availability
- Threat landscape and common attack vectors
- Risk management frameworks and methodologies



Day 2: Network and Infrastructure Security

- Network security architecture and protocols
- Firewalls, IDS/IPS, and VPN implementation
- Cloud security and virtualization considerations
- Securing wireless networks and remote access

Day 3: Application and Data Security

- Secure software development lifecycle SDLC
- Web application security best practices
- Cryptography, encryption, and key management
- Database protection and data privacy measures

Day 4: Identity and Access Management

- Authentication methods, including multi-factor authentication
- Access control models and implementation strategies
- Privileged access management PAM
- Identity governance and compliance frameworks

Day 5: Security Operations and Incident Response

- Security information and event management SIEM tools
- Incident detection, response, and reporting processes
- Digital forensics and investigative techniques
- Business continuity and disaster recovery planning

Individual Impact

Participants will leave the program with:

- Practical skills to conduct security assessments and risk analysis
- Ability to implement fundamental security controls in diverse IT environments
- Knowledge to develop and execute incident response and continuity plans
- Enhanced understanding of cybersecurity best practices to protect organizational assets

Organizational Impact

Organizations will benefit through:

- Strengthened information security posture and reduced risk exposure
- Improved preparedness for cyber incidents and operational disruptions
- Enhanced compliance with legal, regulatory, and ethical standards
- Greater confidence in managing and protecting critical IT assets



Training Methodology

This course emphasizes practical, hands-on learning through:

- Real-world cybersecurity scenarios and simulations
- Exercises in risk assessment and security control implementation
- Incident response and digital forensics workshops
- Group discussions on ethical, legal, and regulatory challenges

Beyond the Course

Upon completion, participants will be able to:

- Identify and mitigate cyber threats proactively
- Implement effective security controls across the organization
- Develop and maintain incident response and business continuity plans
- Contribute to building a culture of cyber awareness and resilience

This program provides a practical pathway for IT professionals and managers to enhance cyber security capabilities, safeguard organizational assets, and respond confidently to the challenges of today's digital landscape.

