Information Security Management ISO 27001 Training Course

Professional Development Training Course Outline

Category	Information Technology	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This crucial training course is meticulously designed for IT professionals, information security managers, compliance officers, risk managers, and anyone responsible for safeguarding organizational information assets. In an era defined by rampant cyber threats, data breaches, and stringent regulatory requirements (including Kenya's Data Protection Act 2019), establishing a robust and internationally recognized Information Security Management System (ISMS) is no longer an option but a strategic imperative. Training Course on Information Security Management ISO 27001 provides participants with the comprehensive knowledge and practical skills required to understand, implement, maintain, and continually improve an ISMS based on the globally acclaimed ISO/IEC 27001 standard, the benchmark for information security excellence.

The curriculum delves deeply into the core principles of confidentiality, integrity, and availability (CIA triad), guiding participants through the systematic process of information security risk assessment, risk treatment planning, and the selection and implementation of appropriate security controls (Annex A of ISO 27001:2022). Through interactive workshops, real-world case studies (with a focus on Kenyan organizational contexts), and practical exercises, attendees will gain hands-on experience in developing security policies, managing incidents, conducting internal audits, and ensuring compliance with relevant legal and regulatory obligations. This course empowers organizations to build a resilient information security posture, protect their most valuable assets, and foster trust with stakeholders by demonstrating a verifiable commitment to global best practices in information security management.

Programme Curriculum

Information Security Management ISO 27001 Training Course

Introduction

This crucial training course is meticulously designed for IT professionals, information security managers, compliance officers, risk managers, and anyone responsible for safeguarding organizational information assets. In an era defined by rampant cyber threats, data breaches, and stringent regulatory requirements (including Kenya's Data Protection Act 2019), establishing a robust and internationally recognized Information Security Management System (ISMS) is no longer an option but a strategic imperative. Information Security Management ISO 27001 Training Course provides participants with the comprehensive knowledge and practical skills required to understand, implement, maintain, and continually improve an ISMS based on the globally acclaimed ISO/IEC 27001 standard, the benchmark for information security excellence.

The curriculum delves deeply into the core principles of confidentiality, integrity, and availability (CIA triad), guiding participants through the systematic process of information security risk assessment, risk treatment planning, and the selection and implementation of appropriate security controls (Annex A of ISO 27001:2022). Through interactive workshops, real-world case studies (with a focus on Kenyan organizational contexts), and practical exercises, attendees will gain hands-on experience in developing security policies, managing incidents, conducting internal audits, and ensuring compliance with relevant legal and regulatory obligations. This course empowers organizations to build a resilient information security posture, protect their most valuable assets, and foster trust with stakeholders by demonstrating a verifiable commitment to global best practices in information security management.

Course Duration

5 Days

Course Objectives

1. Understand the structure, clauses, and principles of ISO/IEC 27001:2022 and its relationship with ISO/IEC 27002.
2. Identify and analyze information security risks specific to an organization's context, assets, and threats.
3. Develop and implement an effective information security risk treatment plan to mitigate identified risks.
4. Design and document an Information Security Management System (ISMS) compliant with ISO 27001 requirements.
5. Select and apply appropriate ISO 27001 Annex A controls (organizational, people, physical, technological) based on risk assessment.
6. Establish clear information security policies, procedures, and guidelines within an organization.
7. Understand the requirements for leadership commitment and involvement in ISMS implementation and maintenance.
8. Plan, conduct, and report on internal audits of an ISMS to ensure its effectiveness and compliance.
9. Manage information security incidents and nonconformities according to ISO 27001 guidelines.
10. Ensure continual improvement of the ISMS through performance monitoring, measurement, and management reviews.
11. Navigate the relationship between ISO 27001 and data privacy regulations, specifically Kenya's Data Protection Act 2019.
12. Prepare an organization for ISO 27001 certification audits.

13. Foster a security-aware culture within the organization to support ISMS objectives.

Organizational Benefits

1. Enhanced Information Security Posture: Systematically identifies and mitigates information security risks.
2. Increased Resilience to Cyber Threats: Reduces the likelihood and impact of data breaches and cyberattacks.
3. Improved Legal and Regulatory Compliance: Ensures adherence to data protection laws like Kenya's Data Protection Act 2019.
4. Strengthened Stakeholder Trust: Demonstrates a commitment to protecting sensitive information for customers, partners, and regulators.
5. Competitive Advantage: Differentiates the organization in the market, attracting new business and partnerships.
6. Optimized Resource Allocation: Directs security investments efficiently based on identified risks.
7. Reduced Financial Losses: Minimizes the costs associated with security incidents, fines, and reputational damage.
8. Better Business Continuity: Ensures the availability of critical information and systems during disruptions.
9. Clearer Roles and Responsibilities: Defines clear security roles, responsibilities, and accountability across the organization.
10. Culture of Security Awareness: Promotes a security-conscious mindset among all employees.

Target Participants

- Information Security Managers
- IT Managers and Directors
- Compliance Officers
- Risk Managers
- Cybersecurity Analysts
- Internal Auditors
- Data Protection Officers (DPOs)
- System Administrators
- Business Continuity Managers
- Consultants (IT, Security, Management Systems)

Course Outline

Module 1: Introduction to Information Security & ISO 27001 (ISMS Fundamentals)

?? The Importance of Information Security in the Digital Age

?? Understanding the CIA Triad (Confidentiality, Integrity, Availability)

?? Overview of ISO/IEC 27001:2022 and the ISO 27000 Family of Standards

?? Benefits of Implementing an ISO 27001 Compliant ISMS

?? **Case Study**: Analyzing a recent data breach scenario and discussing how an ISMS could have prevented or mitigated it in a Kenyan context.

Module 2: Context of the Organization & Scope of ISMS (Strategic Planning)

?? Understanding Internal and External Issues Affecting Information Security

?? Identifying Interested Parties and Their Requirements

?? Defining the Scope and Boundaries of the Information Security Management System (ISMS)

?? Establishing the Information Security Policy and Objectives

?? **Case Study**: Developing an ISMS scope for a Kenyan FinTech company, considering their specific business model and regulatory landscape.

Module 3: Leadership, Planning & Support (ISMS Implementation)

?? The Role of Top Management in ISMS Implementation and Governance

?? Risk Assessment Methodology and Criteria (Identification, Analysis, Evaluation)

?? Information Security Risk Treatment Planning and Options

?? Resource Management: Competence, Awareness, Communication, and Documented Information

?? **Case Study**: Conducting a simplified risk assessment for a common threat (e.g., phishing) and outlining a risk treatment plan.

Module 4: Operations: Controls & Incident Management (Operational Security)

?? Implementing Information Security Controls from Annex A of ISO 27001:2022

?? Managing Information Security Incidents: Identification, Response, Analysis, and Improvement

?? Change Management for the ISMS

?? Performance Monitoring, Measurement, Analysis, and Evaluation of the ISMS

?? **Case Study**: Developing an incident response plan for a simulated cyberattack on an organization's critical systems.

Module 5: Performance Evaluation & Internal Audit (Audit & Review)

?? Objectives and Planning of an Internal Audit Programme

?? Conducting Internal Audits: Gathering Evidence, Interviewing, Documentation Review

?? Reporting Audit Findings and Nonconformities

?? Management Review of the ISMS: Inputs, Outputs, and Decisions

?? **Case Study**: Participating in a mock internal audit of a specific ISO 27001 control area (e.g., Access Control).

Module 6: Continual Improvement & Certification (Optimization & Compliance)

?? Addressing Nonconformities and Implementing Corrective Actions

?? Continual Improvement Mechanisms for the ISMS

?? Preparing for External Certification Audits

?? Maintaining ISO 27001 Certification

?? **Case Study**: Developing a plan for continual improvement based on simulated audit findings.

Module 7: Legal, Regulatory & Compliance in Kenya (Local Compliance)

?? **Kenya Data Protection Act 2019 (DPA)**: Principles, Rights, Obligations of Data Controllers/Processors

?? How ISO 27001 Supports DPA Compliance (e.g., security measures, risk assessment)

?? Other Relevant Kenyan Laws and Regulations (e.g., Computer Misuse and Cybercrimes Act)

?? Legal and Ethical Considerations in Information Security

?? **Case Study**: Mapping specific ISO 27001 controls to requirements of the Kenya Data Protection Act 2019 for a hypothetical organization.

Module 8: Advanced Topics & Emerging Trends (Future of ISMS)

?? Cloud Security and ISO 27001 Considerations

?? Integrating ISO 27001 with other Management Systems (e.g., ISO 9001, ISO 22301)

?? Emerging Threats and Technologies (AI, IoT, Quantum Computing) and their Impact on ISMS

?? The Future of Information Security Management

?? **Case Study**: Discussing how an organization can adapt its ISMS to address the security challenges of adopting cloud services.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com