Information security management 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

In an increasingly digital world, protecting sensitive information has become a critical priority for organizations across industries. Cyber threats and data breaches pose significant risks, making robust information security management essential for safeguarding business operations, customer trust, and regulatory compliance. This Information Security Management training course is designed to equip professionals with the skills and knowledge to protect their organizations from evolving security challenges.

The course focuses on the principles and practices of managing information security within organizational contexts. Participants will learn how to identify vulnerabilities, implement protective measures, and respond effectively to incidents. Drawing from international standards such as ISO/IEC 27001, this program provides a comprehensive framework for building and maintaining an effective information security management system (ISMS).

Through interactive sessions and real-world case studies, participants will explore strategies to mitigate cyber risks, ensure data integrity, and foster a culture of security awareness. By combining theoretical knowledge with practical applications, the training empowers organizations to remain resilient in the face of complex threats.
Whether you are an IT professional, a compliance officer, or a business leader, this course offers invaluable insights to strengthen your organization’s security posture. From mitigating risks to responding to breaches, participants will leave the course equipped to implement and sustain robust information security strategies.

Programme Curriculum

Information security management Training Course

Introduction

In an increasingly digital world, protecting sensitive information has become a critical priority for organizations across industries. Cyber threats and data breaches pose significant risks, making

robust information security management essential for safeguarding business operations, customer trust, and regulatory compliance. Information Security Management training course is designed to equip professionals with the skills and knowledge to protect their organizations from evolving security challenges.

The course focuses on the principles and practices of managing information security within organizational contexts. Participants will learn how to identify vulnerabilities, implement protective measures, and respond effectively to incidents. Drawing from international standards such as ISO/IEC 27001, this program provides a comprehensive framework for building and maintaining an effective information security management system (ISMS).

Through interactive sessions and real-world case studies, participants will explore strategies to mitigate cyber risks, ensure data integrity, and foster a culture of security awareness. By combining theoretical knowledge with practical applications, the training empowers organizations to remain resilient in the face of complex threats.

Whether you are an IT professional, a compliance officer, or a business leader, this course offers invaluable insights to strengthen your organization's security posture. From mitigating risks to responding to breaches, participants will leave the course equipped to implement and sustain robust information security strategies.

Course duration

5 Days

Course Objectives

1. Understand the fundamentals of information security management.
2. Develop and implement an Information Security Management System (ISMS).
3. Identify and assess security risks in organizational operations.
4. Align security policies with international standards (e.g., ISO/IEC 27001).
5. Establish controls to protect sensitive data and systems.
6. Develop strategies for incident response and recovery.
7. Enhance employee awareness of information security practices.
8. Evaluate the effectiveness of security measures through audits.
9. Ensure compliance with legal and regulatory requirements.
10. Foster a culture of proactive information security within the organization.

Organizational Benefits

1. Improved protection of sensitive data and systems.
2. Reduced risk of cyberattacks and data breaches.
3. Enhanced compliance with industry standards and regulations.
4. Increased stakeholder trust and customer confidence.
5. Better alignment of security practices with organizational goals.

6. Strengthened incident response and recovery capabilities.
7. Cost savings through effective risk management.
8. Cultivation of a security-conscious workforce.
9. Competitive advantage through robust security measures.
10. Long-term sustainability through continuous security improvement.

Target Participants

- IT managers and system administrators.
- Information security officers and analysts.
- Risk managers and compliance officers.
- Business leaders and decision-makers.
- Auditors and consultants in cybersecurity.
- Data protection officers (DPOs).
- Professionals involved in IT governance.
- Human resource managers seeking to enhance organizational security awareness.
- Small business owners managing digital assets.
- Students and aspiring professionals in cybersecurity fields.

Course Outline

Module 1: Introduction to Information Security Management

- Key concepts and principles of information security.
- Overview of ISO/IEC 27001 standards.
- Understanding the threat landscape.
- Importance of an Information Security Management System (ISMS).
- Case studies: Organizations benefiting from strong ISMS practices.

Module 2: Risk Assessment and Management

- Identifying information security risks.
- Conducting vulnerability assessments.
- Implementing risk mitigation strategies.
- Developing risk management plans.
- Case studies: Effective risk management in high-stakes industries.

Module 3: Developing and Implementing Security Policies

- Writing comprehensive security policies and procedures.
- Aligning policies with business objectives.
- Communicating policies to employees and stakeholders.
- Monitoring and enforcing compliance.
- Case studies: Successful policy implementation examples.

Module 4: Incident Response and Recovery

- Developing incident response plans.

- Identifying and containing security breaches.
- Reporting incidents to relevant authorities.
- Implementing recovery measures to minimize impact.
- Case studies: Lessons learned from major cybersecurity incidents.

Module 5: Security Awareness and Training

- Building a culture of security consciousness.
- Training employees on security best practices.
- Using simulations to test security readiness.
- Promoting secure use of technology in the workplace.
- Case studies: Enhancing employee security awareness in organizations.

Module 6: Continuous Improvement and Compliance

- Conducting internal and external audits of the ISMS.
- Leveraging feedback for system improvements.
- Staying updated on evolving threats and standards.
- Ensuring compliance with data protection regulations (e.g., GDPR).
- Case studies: Organizations achieving sustained security excellence.

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