" EXIN Information Security Foundation based on ISO/IEC 27001"

Course Introduction:

The "EXIN Information Security Foundation based on ISO/IEC 27001" course offers a comprehensive introduction to information security, emphasizing the global standard ISO/IEC 27001. This course is ideal for individuals aiming to grasp the fundamentals of information security management systems and the principles guiding the safeguarding of sensitive information within organizations. By the end of this course, participants will have a foundational understanding of how to implement, maintain, and improve an information security management system (ISMS) in accordance with ISO/IEC 27001 standards.

Day 1: Foundational Concepts and Organizational Security

Section 1: Information and Security Fundamentals

- Concepts Relating to Information: Delve into the core principles of information security.
- Data vs. Information: Understand the distinction and the relationship between data and information.
- Information Security Management Concepts: Overview of ISMS essentials.
- Reliability Aspects: The CIA Triangle (Confidentiality, Integrity, and Availability) and their significance.
- Accountability and Auditability: Define and understand their importance in information security.

Section 2: Securing Information in the Organization

- Information Security Policy: Objectives and content for creating robust policies.
- Supplier Security: Ensuring information security when collaborating with suppliers.
- Roles and Responsibilities: Outlining key roles and responsibilities in information security.

Section 3: Threats, Risks, and Management

• Threats and Risks: Examine the landscape of potential threats and risks.

• Threat, Risk, and Risk Management: Definitions and interrelationships.

• Types of Damage: Understanding potential impacts of security incidents.

• Risk Strategies: Approaches to managing risks such as avoid, mitigate, accept, and transfer.

• Risk Analysis: Methods and processes for identifying and evaluating risks.

Day 2: Security Controls, Legislation, and Standards

Section 4: Security Controls - Implementation

• Outlining Security Controls: Explore the array of security controls available.

• Examples of Security Control Types: Administrative, technical, and physical controls.

• Organizational Controls: Information asset classification and access management.

• Threat and Vulnerability Management, Project Management, and Incident Management: Their roles in information security.

• Business Continuity: Explaining its value in maintaining operations.

• Audits and Reviews: The value of regular assessments.

Section 5: Physical and Technical Controls

• Physical Controls: Safeguarding physical access points and secure areas.

• Protection Rings: Understanding layered security.

• Technical Controls: Managing and controlling information assets technically.

• Secure System Development: Integrating security into the system development lifecycle.

• Network Security Controls: Examples of controls for network protection.

• Technical Access Management Controls: Implementing access controls using technology.

• Protection Against Malware, Phishing, and Spam: Technical measures to combat these threats.

• Recording and Monitoring: Contribution to information security through logging and analysis.

Section 6: Legislation, Regulations, and Standards

• Legislation and Regulations: Examples of key laws and regulations impacting information security.

• Standards: Overview of ISO/IEC 27000, ISO/IEC 27001, and ISO/IEC 27002, along with other relevant standards.

Conclusion and Next Steps:

• Review of Key Concepts: Recap the key concepts and takeaways from the course.

• Pathways for Further Learning: Identify advanced courses and certifications to further enhance information security expertise.

• Building a Career in Information Security: Explore career opportunities and professional development paths in the field of information security.