INFORMATION SECURITY MANAGEMENT AND ISO/IEC 27001 IMPLEMENTATION COURSE

Introduction

The Information Security Management and ISO/IEC 27001 Implementation programme is designed to equip information security professionals, ICT managers, compliance officers, auditors and organisational leaders with the knowledge required to establish, implement, maintain and continually improve an Information Security Management System (ISMS). Organisations process sensitive business information, personal data, financial records, intellectual property and operational information that must be protected against unauthorized access, alteration, disclosure, loss and disruption. Ad hoc technical controls alone may not provide sufficient assurance. A structured management system is needed to identify information security risks, establish appropriate controls, assign responsibilities, monitor performance and demonstrate that security arrangements are integrated into normal organisational operations. The programme introduces the principles and requirements of ISO/IEC 27001, with emphasis on the 2022 edition and the practical implementation of an ISMS. Participants examine organisational context, leadership commitment, scope definition, risk assessment, risk treatment, security objectives, documented information, internal audit, management review and continual improvement. The course also explains how Annex A controls can be considered in relation to identified risks and applicable requirements, rather than being treated as a generic checklist. Participants explore asset management, access control, supplier security, incident management, business continuity, awareness and performance evaluation. Practical exercises guide them through ISMS scoping, risk register preparation, control selection and implementation planning. The programme is appropriate for organisations preparing for certification, improving an existing information security management system or strengthening internal security governance. It is a training programme and does not itself confer ISO certification or make an organisation certified.

Course Objectives

- Explain the purpose, structure and key requirements of ISO/IEC 27001.
- Define the scope and context of an organisational ISMS.
- Identify information assets, threats, vulnerabilities and security risks.
- Conduct and document information security risk assessments.
- Develop risk treatment plans and select appropriate controls.
- Establish information security policies, objectives and documented procedures.
- Implement relevant organisational, people, physical and technological controls.
- Plan internal audits and management reviews of the ISMS.
- Monitor nonconformities, corrective actions and continual improvement.
- Develop a practical ISMS implementation roadmap.

Course Modules

> Module 1: Foundations of Information Security Management

- Confidentiality, integrity and availability of information.
- Information security risks in modern organisations.
- Introduction to information security management systems.
- Overview of ISO/IEC 27001:2022 and its relationship with ISO/IEC 27002.

> Module 2: Organisational Context and ISMS Scope

- Understanding organisational context and interested parties.
- Identifying internal and external information security requirements.
- Defining ISMS boundaries, locations, systems and processes.
- Determining responsibilities, dependencies and scope exclusions.

> Module 3: Leadership, Policy and ISMS Planning

- Leadership commitment and information security accountability.
- Developing an information security policy and objectives.
- Assigning roles, resources and implementation responsibilities.
- Integrating information security with business objectives and governance

> Module 4: Information Security Risk Assessment

- Identifying and classifying information assets.
- Analysing threats, vulnerabilities and potential consequences.
- Establishing risk evaluation criteria and prioritisation methods.

- Documenting risk assessments and maintaining a risk register.

> Module 5: Risk Treatment and Statement of Applicability
- Selecting risk treatment options and appropriate controls.
- Understanding the role of Annex A controls.
- Preparing a Statement of Applicability and documenting justifications.
- Developing risk treatment plans, owners and completion timelines.

> Module 6: Implementing Information Security Controls
- Asset management, access control and identity management.
- Human resource security, awareness and acceptable use.
- Physical security, operational controls and system protection.
- Supplier security, incident management and relevant continuity controls.

> Module 7: ISMS Documentation and Operational Control
- Developing procedures, policies, registers and supporting records.
- Document control, version management and evidence retention.
- Integrating security requirements into business processes.
- Monitoring operational controls and handling implementation exceptions.

> Module 8: Performance Evaluation and Internal Audit
- Establishing information security performance indicators.
- Monitoring control effectiveness and achievement of objectives.
- Planning and conducting internal ISMS audits.
- Recording audit findings, nonconformities and opportunities for improvement.

> Module 9: Management Review and Continual Improvement
- Preparing management review inputs and performance reports.
- Reviewing risk changes, audit findings and corrective actions.
- Investigating root causes and verifying corrective action effectiveness.
- Maintaining the ISMS through organisational and technology changes.

> Module 10: ISMS Implementation Capstone
- Defining the ISMS scope for a sample organisation.
- Preparing a preliminary information security risk register.
- Developing a control selection matrix and Statement of Applicability outline.
- Presenting an ISMS implementation roadmap with responsibilities and milestones.

P.O Box 7254- 01000
www.trustgatecorporateskills.co.ke
Location Thika & Nairobi