ISO 27000 Foundation Certification Course

Course#:ITSM-18
Duration:3 Days
Price:0.00

Course Description

Every organization, whether it is a commercial enterprise, government agency, or a not-for profit organization, must have established guidelines that will protect it from business risks. The ISO/IEC 27000 suite of standards define exactly these requirements and form a formal specification that help organizations establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management System. As an ISO 27000 certified professional, you can help an organization demonstrate achievement of excellence and compliance with global best practices for quality in Information Security Management.

KnowledgeHut helps you prepare for the ISO 27000 Foundation certification provided by Peoplecert where candidates will be introduced to the principles and core elements of the ISO 27000, specifically for ISO/IEC 27001 and ISO/IEC 27000. With comprehensive courseware, in-depth exercises, and training from experienced professionals, participants can aim for a first time clearance of the examination and apply the ISO 27000 standard to ensure continuity and effectiveness of the organization.

Objectives

As this is the Foundation level course, candidates will be introduced to the principles and core elements of the ISO/IEC 27001 and ISO/IEC 27002 standards for Information Security Management, and more specifically:

ISO/IEC 27000: which provides an overview of information security management systems, which form the subject of the ISMS family of standards, and defines related terms.
ISO/IEC 27001: the formal specification which defines the requirements that must be achieved for an information security management system (ISMS).
ISO/IEC 27002: which describes a code of practice for information security management and details hundreds of specific controls which may be applied to secure information and related assets

Holders of Peoplecerts ISO 27000: Information Security Management Foundation Certification will be able to demonstrate their knowledge, ability, competence and understanding in:

Definitions and principles of quality management services in accordance with ISO/IEC 27001.
Positioning of ISO/IEC 20000 in the Information security management including its relationship with other standards and best practices.
Objectives and requirements in each section of the specification.
Scope, aims and use of the ISO/IEC 27001 and ISO/IEC 27002 Specification and Code of Practice.
Processes and objectives of ISO/IEC 27001 and ISO/IEC 27002 and Information security management (ISMS).
Fundamental requirements for an Information Security Management System (ISMS).
Requirements of the Information Security Management System and the Plan, Do, Check, Act cycle.
How assessments, reviews and internal audits of Information Security Management systems against the requirements of the standard are used.

Audience

This qualification is the first level of the ISO/IEC 27000 certification scheme provided by Peoplecert, and is aimed at anyone working within an organization (internally or externally) who may require to have and demonstrate a solid knowledge and understanding of the ISO/IEC 27001 and ISO/IEC 27002 standards and their content. The certification can also cater for candidates seeking personal certification, also in regards to their knowledge and understanding of the requirements and the content of the standard.

Prerequisites

There are no prerequisites for attending this workshop or the exam. It is recommended that participants have at least a basic knowledge of Information security management concepts and terminology and have undergone some formal training on the subject with a proposed duration of 24 hours.

Content

Category

Ref

Knowledge Set

ISMS-7.1 Introduction

ISMS-7.1.1

Scope of ISO/IEC 27000 series of standards

ISMS-7.1.2

Recognize industry standards/best practices in Service Management and Quality management systems, such as: ITIL, SixSigma, CobiT, ISO/IEC 9000, ISO/IEC 20000

ISMS-7.1.3

Recognize the content and correlation between ISO/IEC 27001:2005 and ISO/IEC 27002:2005

ISMS-7.1.4

Definition and need for Information Security and Information Security Management System (ISMS)

ISMS-7.1.5

Importance of an Information Security Management System (ISMS)

ISMS-7.1.6

Value and Reliability of Information

ISMS-7.1.7

Benefits and Critical Success factors of an Information Security Management System (ISMS)

ISMS-7.2 Organization of Information Securityl

ISMS-7.2.1

Management responsibility:

Management commitment

Resource management

ISMS-7.2.2

Confidentiality agreements

ISMS-7.2.3

Contact with authorities and with special interest parties

ISMS-7.2.4

Independent review of information security

Addressing security when dealing with external parties

Addressing security when dealing with external parties

ISMS-7.3 Information Security Management System

ISMS-7.3.1

Information Security Policy

ISMS-7.3.2

General ISMS requirements

ISMS-7.3.3

Structure of policies

ISMS-7.3.4

Establishing and managing the ISMS:

Establish the ISMS

Implement and operate the ISMS

Monitor and review the ISMS Maintain and improve the ISMS

ISMS-7.3.5

Documentation requirements

General

Control of documents

Control of records

ISMS-7.3.6

Management review of the ISMS

General
Review input
Review output

ISMS-7.3.7
ISMS improvement:
Continual improvement
Corrective action
Preventive action

ISMS-7.4 ISMS Implementation
ISMS-7.4.1
Defining ISMS scope, boundaries and ISMS policy

ISMS-7.4.2
Asset Management:
Responsibility for assets
Information classification

ISMS-7.4.3

Risk Assessment and Treatment:

Assessing security risks

Treating security risks

ISMS-7.4.4

Information security aspects of business continuity management

ISMS-7.5 Human resources, physical and environmental security

ISMS-7.5.1

Human Resources Security: Prior to employment

ISMS-7.5.2

Human Resources Security: During employment

ISMS-7.5.3

Human Resources Security: Termination or change of employment

ISMS-7.5.4

Physical and Environmental Security: Secure areas

ISMS-7.5.5

Physical and Environmental Security: Equipment security

ISMS-7.6 Communications and operations management

ISMS-7.6.1

Operational procedures and responsibilities

ISMS-7.6.2

Third party service delivery management

ISMS-7.6.3

System Planning and acceptance:

Capacity management

System acceptance

ISMS-7.6.4

Protection against malicious and mobile code

ISMS-7.6.5

Back-up

ISMS-7.6.6

Network security management

ISMS-7.6.7

Media handling

ISMS-7.6.8

Exchange of information

ISMS-7.6.9

Electronic commerce services

ISMS-7.6.10

Monitoring

ISMS-7.7 Access Control

ISMS-7.7.1

Access control policy

ISMS-7.7.2

User access management

ISMS-7.7.3

User responsibilities

ISMS-7.7.4

Network access control

ISMS-7.7.5

Operating system access control

ISMS-7.7.6

Application and information access control

ISMS-7.7.7

Mobile computing and teleworking

ISMS-7.8 Information systems acquisition, development and maintenance

ISMS-7.8.1

Security requirements of information systems

ISMS-7.8.2

Correct processing in applications

ISMS-7.8.3

Cryptographic controls

ISMS-7.8.4

Security of system files

ISMS-7.8.5

Security in development and support processes

ISMS-7.8.6

Technical vulnerability management

ISMS-7.9 Compliance

ISMS-7.9.1

Compliance with legal requirements

ISMS-7.9.2

Compliance with security policies and standards, and technical compliance

ISMS-7.9.3

Internal ISMS audits:

Define criteria, scope, frequency, method and audit procedures

Define roles and responsibilities of internal auditors

Ensure objective and impartial documentation

Plan audit activities

Follow up activities

Record keeping procedures

ISMS 7.10 Information Security Incident Management

ISMS-7.10.1

Reporting information security events

ISMS-7.10.2

Management of information security incidents and improvements

Total Proposed Training Time: 24 hours