ISO/IEC 27001 Lead Implementer

Course Summary

Description

This course enables the participants to develop the expertise to support an organization in implementing and managing an Information Security Management System (ISMS) as specified in ISO/IEC 27001:2005. Participants will also master the best practices for implementing information security controls from the eleven areas of ISO/IEC 27002:2005.

This training is consistent with the good practices of project management established by the Project Management Institute (PMI) and ISO 10006:2003 (Quality Management Systems - Guidelines for Quality Management in Projects). This training is fully compatible with ISO/IEC 27003:2009 (Guidelines for the Implementation of ISMS), ISO/IEC 27004:2009 (Measurement of Information Security) and ISO/IEC 27005:2008 (Risk Management in Information Security).

Objectives
At the end of this course, students will be able to:

- Understand the application of an Information Security Management System in the ISO/IEC 27001:2005 context
- Master the concepts, approaches, standards, methods and techniques allowing effective management of an Information Security Management System
- Understand the relationship between an Information Security Management System, including risk management and controls and compliance with the requirements of different stakeholders of the organization
- Acquire expertise to support an organization in implementing, managing and maintaining an ISMS as specified in ISO/IEC 27001:2005
- Acquire the expertise necessary to manage a team in implementing the ISO/IEC 27001:2005 standard
- Develop personal skills and knowledge required to advise organizations on best practices in management of information security
- Improve the capacity for analysis and decision making in a context of information security management

Topics

- Introduction to the management of an Information Security Management System (ISMS) based on ISO 27001 and launching an ISMS
- Planning an ISMS based on ISO27001
- Launching and implementing an ISMS based on ISO27001
- Control, act and the certification audit of the ISMS according ISO/IEC 27001
- Exam

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

ISO/IEC 27001 Lead Implementer

Course Summary (cont'd)

Audience

Project manager or consultant wanting to prepare for and support an organization in the implementation of an Information Security Management System (ISMS)

- ISO 27001 Auditor who wants to master the Information Security Management System implementation process
- Person responsible for the information security or conformity in an organization
- Member of the information security team
- Expert advisor in information technology
- Technical expert wanting to prepare for an information security function or for an ISMS project management function

Prerequisites

- ISMS Foundation training or a basic knowledge of ISO/IEC 27001:2005 and ISO/IEC 27002:2005 is recommended
- Participants are required to purchase a copy of the ISO/IEC 27001:2005 Standard from www.iso.org

Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

ISO/IEC 27001 Lead Implementer

Course Outline

I. Introduction to the management of an Information Security Management System (ISMS) based on ISO 27001 and launching an ISMS

A. Introduction to management systems and the process approach
B. Detailed presentation of the standards ISO/IEC 27001:2005, ISO/IEC 27002:2005 and ISO/IEC 27003:2009
C. Fundamental principles of Information Security
D. Preliminary analysis and determining the level of maturity of the existing management of the Information Security based upon ISO/IEC 21827:2008
E. Writing the business case and preliminary design of the ISMS
F. Developing a project plan of compliance to ISO/IEC 27001:2005

II. Planning an ISMS based on ISO27001

A. Establishment of the Governance Framework
B. Definition of roles & responsibilities
C. Drafting of the ISMS policy
D. Defining the scope of the ISMS
E. Risk management according to ISO/IEC 27005:2008: identification, analysis and treatment of risk
F. Drafting the Statement of Applicability
G. Launching and implementing an ISMS based on ISO27001
H. Implementation of a document management framework
I. Design of controls and writing procedures
J. Implementation of controls
K. Development of a training & awareness program and communication around the information security
L. Incident Management according to ISO/IEC TR 18044:2004
M. Operations management of ISMS

III. Control, act and the certification audit of the ISMS according ISO/IEC 27001

A. Monitoring controls and the management of records
B. Development of metrics, performance indicators and the dashboard in accordance with ISO/IEC 27004:2009
C. Internal ISMS Audit
D. Management review of the ISMS
E. Implementation of a continuous improvement program
F. Preparing for the ISO/IEC 27001:2005 audit

IV. Exam

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically