



Implementing Information Security Based on ISO 27001 and ISO 27002

This interactive 2 day course provides an introduction to the ISO/IEC 27001:2005 and ISO/IEC 27002:2007 (formerly ISO/IEC 17799 / BS 7799) international standards for information security. The course presents a straightforward and logical approach to developing, implementing and maintaining your Information Security Management Process and Systems.

The course guides its participants through the Information Security Process and provides detailed guidance on how to effectively design, plan and implement this process and the related Information Security Management Systems (ISMS). Additionally it provides practical direction to prepare for a security audit and to enforcing compliance.

Who should attend?

This course will be beneficial for anyone who is looking for the details of the ISO/IEC 27001:2005 and 27002:2007 standards, including:

- Staff responsible for Information Security Management or implementation of ISO/IEC 27001 and/or ISO 27002
- Information Security Managers
- IT managers responsible for delivering or running critical business information systems
- IT consultants advising clients on security matters
- Information Service Provider (ISP) staff responsible for security issues.
- Security Managers, Auditors, Project Managers, Operations Managers and Business Managers

What You Will Learn

This course will enable delegates to:

- Understand the requirements of the ISO/IEC 27001:2005 and ISO/IEC 27002 standards
- Practical techniques for designing and implementing an ISMS
- Detail explanations of the ISO/IEC 27001:2005 ISMS components and the improvement cycle
- Understand the necessary skills to design, implement, maintain and audit an effective ISMS
- Assess an organisation's information security needs against ISO/IEC 27002:2007 and ISO/IEC 27001:2005

In addition the course will have hands-on activities in which delegates will have the opportunity to undertake practical exercises with the intention of formulating practical documents that can be used in their business, including:

- Information Security policy
- Identification of information assets and their value
- Determination of risk and impacts
- Identification of control objective and controls
- Risk Analysis and Risk Treatment Plan
- Statement of Applicability (SOA)
- Completion of ISMS documentation requirements
- Production of a ISMS Project Implementation Plan



Implementing Information Security Based on ISO 27001 and ISO 27002

Learning Method

This course is conducted as an instructor-led workshop and includes a combination of lectures and exercises. Each delegate will receive the book *Implementing Information Security based on ISO 27001 & ISO 17799* (ISBN: 9789077212783), the course notes, and a certificate of attendance.

Prerequisite

A basic knowledge of information systems, security and management processes

Course Fee

\$1,250 + gst

In-House Training

This course is available for private presentation, either on your own premises or 'off-site'. There are many advantages to in-house training. Please contact ALC for a quotation and to discuss your requirements. Telephone 1300 767 592 or email learn@alc-group.com.au

Course Structure

The course will cover the following topics:

1. Information Security Introduction
 - Introduction to Information Security Management (ISM)
 - Information Security Focus
 - ISM Benefits
2. Security Standards and Best Practices
 - Introduction to Security Standards and Best Practices and their purpose:
 - ASCII 33 – Ensures minimum standard for government ICT security
 - ISO 27001:2005 - Defines the ISMS requirements
 - ISO 27002 (ISO 17799:2005) - Defines a code of best practices for the management of information security
 - AS 8001:2003 - Control of fraud and corruption
 - AS/NZS 4360:2004 - Risk Management
 - SABSA – "best practice" method for delivering information security solutions to enterprises
 - CobiT - Control Objectives for Information and related Technology
 - ITIL - The IT Infrastructure Library
 - SOX - Sarbanes-Oxley
 - PRINCE2 - PRojects IN Controlled Environments, V2



Implementing Information Security Based on ISO 27001 and ISO 27002

3. The ISO 27001 and 27002 Standards
 - ISO 27000 series
 - Overview ISO/IEC 27001
 - Overview ISO/IEC 27002 (ISO 17799:2005)
 - Control Objectives and Controls
 - Technology
4. Information Security Process
 - Process approach
 - Implementation of an ISMS
 - The 'Plan – Do – Check – Act Model'
5. The 6 Steps of the Plan Phase:
 - Scope
 - Policy
 - Assess Risk
 - Treat Risk
 - Control Objectives
 - Statement of Applicability
6. Audit Readiness & Preparation
 - The Security Audit Process
 - Strategic, Tactical and Operational documents
 - Reasons for Non-Implementation
 - Audit Process
7. Enforcing Compliance
 - Reasons for Enforcing Compliance
 - Policy Compliance Reviews
 - Policy Compliance Vs Vulnerability Assessments
 - Survival Tactics
8. Organisational Change Challenge
 - Service Culture Barriers
 - Management Effort
9. Realising the Benefits
 - IT Security Management Benefits
 - Advantages of implementing ISO 27001 and 27002
 - Critical Success Factors