

# Implementing an Information Security Management System using ISO 27001



The growing strategic importance of risk management, coupled with the vulnerability of IT, has highlighted the need for an organisation to protect its most valuable asset – **information**.

## ISO/IEC 17799: 2005 - Code of practice for Information Security Management

ISO 17799, the International Standard for information security management, which has been newly enhanced and updated in June 2005, provides a framework for businesses to review, and improve, the overall effectiveness of their information security.

## ISO 27001 - A Specification for an Information Security Management System

This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organisation's overall business risks.

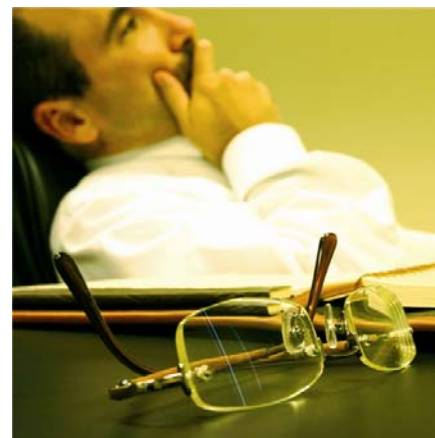
### Course Objectives

This two day practical course introduces delegates to the de-facto Information Security Standard and describes how to perform each step towards developing an Information Security Management System (ISMS), and obtaining ISO 27001 certification.

The course is designed for Information Security Professionals, Internal Auditors and management that deal with the complexities on Information Security requirements within the organisation.

The objective is to provide delegates with the necessary skills to develop an information security framework for their organisation. Attendees will learn how to assess their information assets and protect these assets against threats seeking to exploit potential vulnerabilities. Delegates will furthermore learn how to benchmark their existing security practices against the standard and implement a cost-effective security strategy that is compliant with international best practices.

This course also covers preparing for formal certification and offers clear explanations and practical solutions. Importance is placed on explaining not only how to comply with the Standard, but also how to demonstrate compliance to external auditors. Most importantly, it explains how to realise the true business benefits of implementing ISO 17799 / 27001.



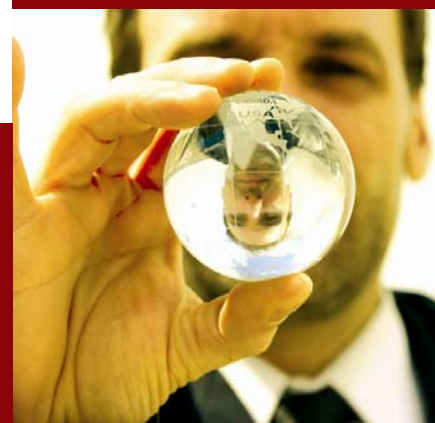
### What you will learn

On completion of the course, you will be able to:

- Define the scope of an ISMS
- Develop an ISMS
- Ask the pertinent questions required for an ISO 17799 Gap Analysis
- Prepare an effective security improvement plan
- Demonstrate compliance to an auditor
- Achieve the maximum benefit from your ISO 17799 & 27001 compliance.

### Who will benefit?

- CIO's / IT Directors / IT Managers
- Information Security Managers/Officers/Professionals
- Project Managers / Operations Managers / Business Managers
- Auditors involved in Information Security



## Course Content



### Day 1 – ISO 17799

#### **Introduction to ISO 17799**

- Individual introductions and learning objectives.
- Background to IT Governance & need for IT controls
- Background to ISO 17799 and ISO 27001
- What ISO 17799 means to your organisation
- What is Information Security, why is it needed?
- How to establish security requirements
- Assessing security risks
- Selecting Information Security controls

#### **Application of ISO 17799**

- Starting point - Identifying your Information Security objectives and Critical Success Factors
- Setting the scope and boundaries of the programme and developing your own guidelines
- Effective gap analysis
- Handling complex programmes
- Risk Assessment and treatment for ISO 17799

#### **Planning for ISO 17799**

- Planning and estimating your programme
- Identifying timescales, resources, key end products

#### **Implementation guidance**

- ISO17799 documentation requirements
- Developing audit checklists & internal auditing approach
- Presenting the documentation set
- Formal risk acceptance

### Day 2 – ISO 27001

#### **Introduction to ISO 27001**

- Background to ISO 27001
- Description of a process approach to the adoption of an (ISMS)
- The application of the Plan, Do, Check, Act (PDCA) to the ISMS process
- Understanding the ISMS concept

#### **Understanding the ISMS**

- Understanding the ISMS concept
- How to establish, manage, implement, an ISMS
- How to monitor and review an ISMS

#### **Implementing the ISMS**

- ISMS documentation requirements
- ISMS- Management responsibilities
- ISMS training and awareness campaigns

#### **Certification**

- Creating a Security Improvement Programme
- The certification process

#### **Approach, Deliverables and Method**

- Fully aligned to ISO 17799 / ISO 27001 and COBIT®'s DS 5, Ensuring System Security
- Instruction from trainers with extensive operational experience across a broad range of public and private sector organisations.
- Comprehensive course notes and advice on further sources of information.
- Classroom style lecturing - combining lecture, discussion and exercises utilising course materials, digital projector and flipchart.

#### **In-house Training**

All Analytix Courses are available in-house, should your organisation have a number of people or multiple sets to train. The cost advantages and the ability to discuss and resolve organisational issues are two major attractions of such training.

#### **Consulting Services**

Analytix also offers consulting services to support the design and implementation of Information Security Management Systems using ISO 17799 and ISO 27001.

Other services include, among others, Corporate and IT Governance, IT Management, IT maturity assessments, security certification assistance and performance management.

#### **CISA/CISM CPE Credits**

This training is directly applicable to the assessment of information systems or the improvement of audit, control, security or managerial skills to ensure a proper balance of professional development is attained. As such, this training falls under ISACA definition "workshops, and professional meetings and related activities not sponsored by ISACA." Fourteen (14) Continuing professional education (CPE) hours are earned attending this course. Delegates are responsible for applying for the CPE credits from ISACA.

## **Register Today**

To register, or for more information, please contact us:

**Tel: 0861 ANALYTIX or 0861 262 598**

**Fax: +27 (011) 447 4192**

**Email: [info@analytix.co.za](mailto:info@analytix.co.za)**

**Web site: [www.analytix.co.za](http://www.analytix.co.za)**

**ANALYTIX CONSULTING (PTY) LTD**

MLC House • 1st Floor • 50 Sixth Road • Hyde Park • 2196

PO Box 413988 • Craighall • 2024

[www.analytix.co.za](http://www.analytix.co.za) • [info@analytix.co.za](mailto:info@analytix.co.za)