

## **BS 7799 - The Essentials of Information Security Management**

Duration: 2 Days

### **Course Content**

This course examines the business needs for a management system for information security and the current thinking reflected by the British Standard BS 7799-1:2000, (ISO 17799). The course looks at the requirements for a formal management system as specified in BS 7799-2:2002.

The course examines specific issues for information security, methods of control and countermeasures for threats, but is not intended to be of a particularly technical nature; the emphasis is on the management of information security.

### **Course Objective**

- To make participants aware of information security.
- To enable participants to understand the purpose of the standard.
- To make participants aware of the control objectives and controls.
- To emphasise the importance of the most significant controls.
- To enable participants to understand the implications of implementing BS 7799 in an organization.
- To make participants aware of the implications of certification and commercial pressures and possible penalties for non-compliance.

Information security is not limited to Information Technology arenas, although with ever-increasing use of electronic commerce, we all need to develop new skills as technology advances.

### **Who Should Attend**

The course is aimed at Senior Managers, IT Managers, Systems Managers, IT Security Officers and any auditors who will be involved in introducing BS 7799 into an organization.

### **Course Outline**

Module 1 Introduction and course outline About BS 7799

- History
- Development
- Current situation
- The future
- Other documents

Module 2 The basics

- What is information?

Module 3 Risks to information (Exercise 1)

- Myth and reality

Module 4 Information security management and business needs

- Commercial requirements
- Legal requirements
- Basic components

#### Module 5 Overview of controls from BS 7799 (Exercises 2,3 & 4 )

- Controls with legislative implications
- Controls for common best practice
- The 10 detailed control clauses

#### Module 6 Design and implementation of an information security management system

- PDCA
- ISMS framework
- Policy
- Scope

#### Module 7 Assets and risk management (Exercise 5,6,7 )

- Assets
- Asset values and potential impacts
- Risk assessment
- Threats
- Vulnerabilities
- Risk treatment
- Statement of applicability
- Critical success factors

#### Module 8 Maintenance of information security

- Documentation requirements
- Management responsibilities
- Improvements
- Re-evaluation

#### Module 9 Assessment and Certification

- The process
- Maintenance

#### Module 10 Exercises

- Task list for BS 7799 implementation
- Policy statement
- Analysis of controls
- Business continuity planning
- Security - risk assessment
- Asset identification
- Security - risk treatment