CIIP Implementing ISO 27001

The course is designed to involve delegate participation, and there are many exercises of differing styles, based primarily on a detailed case study. Styles include lectures, discussions, individual exercises, group exercises and role-play.

The mysteries are explained of such areas as:

- information asset inventory
- risk assessment

Gain confidence that certification is within reach. An in-depth understanding of information security and how it applies to you and your organisation.

What you will learn

- The component parts of the Standard
- How to manage information security
- How the individual components of the process fit together
- How to treat implementation as a project
- Common pitfalls
- How to define and risk assess "information assets"

- How to manage risks in a way suitable to your organisation
- The essential requirements for obtaining auditor approval, i.e. certification

Who should attend

- Those with an interest / responsibility for information security
- IT, Financial and HR Management
- Computer Auditors
- IT Security Officers
- Information Security Professionals

To Book Call:

+353 1 685 4942

Duration: 3 days
Cost: €1600.00

CPE Credits: 24   MSc Credits: 15

3.0.1

Course content highlights

• Why do you need certification to ISO 27001?

• What the Information Security Management System (ISMS) is and what it is trying to achieve

CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND AUDIT

• Overview of the stages of the ISMS

• Defining an Information Security Policy

• Defining the scope of the ISMS

IDENTIFYING INFORMATION ASSETS

• What are information assets?

• Creating an asset classification system

UNDERTAKING A RISK ASSESSMENT

• Identifying asset values, threats and vulnerabilities

• Creating a usable and simple risk methodology

• Using risk tools

• Practical exercise – undertaking a risk assessment

• Results and conclusions resulting from an assessment

MANAGING RISK

• Risk measurement

• Risk reduction and acceptance techniques

• Practical exercise - determining control objectives

• Selecting control objectives and controls

• Security in depth

• ISO 27001 control objectives and controls

• The application of countermeasures

• Practical exercise – creating a workable countermeasure

• Additional controls not in ISO 27001

• Preparing a Statement of Applicability

• The need to review and audit the ISMS

AUDITING

• What does auditing achieve?

• How should auditing be conducted?

• Different types of audit

• The phase 1 and 2 ISO 27001 audits

• Certification – what is next?