Course Introduction

Implementing the Information Security Management System (ISMS) based on ISO/IEC 27001 for certification requirements and code of practices based on ISO/IEC 27002 become the essential approach for enterprises on managing information security. Also, the legislative and regulations are increasingly developed based on this standard. This requires the essential process to be established, so-call Information Security Risk Management.

ISO/IEC 27005 is the specific standard for Information Security Risk Management in implementing ISMS and information security controls. This standard is differential from the other standards using in IT risk and other enterprise risks. However, the main concepts and framework of ISRM are similarly to the other IT risk standards, but some more specific detail like identification of assets, vulnerabilities, threats, and selection of controls are more specific and particularized for information security controls.

Course Objectives

- Understand the principles and concepts of information security risk management
- Understand how to develop the information security risk approach, including methodology, criteria of accepting risks and acceptable levels of risk
- Understand the framework on information security risk assessment and risk treatment
- Understand the processes and activities needed by the Standard in conducting information security risk assessment and risk treatment

Learning Level

- Advance

Course Duration

- 2 Days

Target Group

- IT Manager/Director
- Information Security Officer/Manager
- IT Risk/Operational Risk Officer

Course Outline

Module 1: Introduction to ISMS Requirements and Risk Management

Overview of ISMS Standards

Overview of ISO/IEC 27001 (ISMS)

Overview of ISO/IEC 27002 (Code of practices)

Overview of other related IT risk standards

Module 2: Information Security Risk Management (ISRM)

- Concepts of information security risk management
- Terms and definitions of information security risk management
- Structure of the ISRM standard
- Overview of the ISRM process

Module 3: Context Establishment

- General considerations
- Basic criteria
- The scope and boundaries
- Organization for ISRM

Module 4: Information security risk assessment

- General description of risk assessment
- Risk analysis
- Risk identification
- Asset
- Vulnerabilities
- Threats
- Risk estimation
- Risk evaluation

Module 5: Information security risk treatment

- General description of risk treatment
- Risk reduction
- Risk retention
- Risk avoidance
- Risk transfer

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

Module 6: ISRM in implementation

- Information security risk acceptance
- Information security risk communication
- Information security risk monitoring and review

Official Training Partner