

|                               |  |
|-------------------------------|--|
| <b>Course Name:</b>           | Building Information Security Governance by implementing ISO 27001 |
| <b>Duration:</b>              | 2 Day  |
| <b>Medium of Instruction:</b> | Cantonese (with handout in English)                                |
| <b>Award of Certificate:</b>  | Certificate of Attendance  |

### **Nature and Objectives:**

Information security governance consists of leadership, organizational structures and processes that safeguard information and information processing facilities of corporations. Critical to the success of these structures and processes is effective communication within an organization based on constructive relationships, a common language and shared commitment to addressing the issues. It focuses on alignment of information security with business strategy to support organizational objectives; risk management by executing appropriate measures to manage and mitigate risks to an acceptable level; resource management by utilizing information security knowledge and infrastructure efficiently and effectively; performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved; value delivery by optimizing information security investments in support of organizational objectives. This course provides participants with practical knowledge to establish information security governance within their organizations by implementing ISO 27001 international standard. This is an interactive training program consisting of integrated exercises, case studies and examples to illustrate the concept taught. Upon completion of the course, participants will be able to grasp full working knowledge of how to build information security governance and implement ISO 27001 information security management standard.

### **Who Should Attend:**

IT Manager, Security Officers, Auditors and anyone who need to have a comprehensive understanding of information security governance and management.

### **Course Outline:**

#### **Introduction**

- Information Security and Information Security Gov.
- Managing Information Security
- Introduction to ISO 27001 standard

#### **Plan your Information Security Governance Project**

- Understand the current situation of your org.
- Define Scopes and Boundaries for implementation
- Get management buy-in
- Build your implementation team
- Typical implementation plan and approach

#### **Defining Policy Steer for Information Security**

- Identifying Security Requirement – Strategic Alignment
- Setting the Overall Direction for Information Security
- How to Measure the Performance of Information Security Effort

#### **Establishing an Information Security Management System Framework**

- The executive management's roles and resp.
- Security Organization
- Allocation of Security Responsibilities
- Defining the Continue Improvement Management Framework

#### **Risk Management**

- Know what you need to protect and what are at risk
- Risk assessment
  - Introduction to risk assessment model (AS 4360, OCTAVE)
  - Asset, Threat and Vulnerability Mapping
  - The risk formula

- Practical ways to identify risks

- Risk Treatment – handling the risks

#### **Reducing risk – Info.Sec Controls**

- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance
- Others that outside ISO 27001

#### **Information Security Performance Measurement – Metrics**

#### **Documenting your Information Security Management System**

- Principle of documentation
  - Documentation – a formality?
  - What & Why documents?
- A Proposed Documentation Structure
- Documentation Control
- Documentation Requirements

#### **Auditing**

- Types of Audit
- Objective of Audit
- The Audit Process

➤ The Audit Risk

**Management review Maintaining the information security management system Certification**

➤ Go for certification?

➤ The pros and cons of certification

➤ The certification process

➤ Maintaining the certificate