MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

ISO/IEC 27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) – IMPLEMENTATION

Level: Intermediate | **Duration:** 3 days

Organizations are increasingly aware of the value of their business-critical information and the need to protect their information related assets. An Information Security Management System (ISMS) is based on risk management approach to maintain the confidentiality, integrity and availability of the organization's information.

ISO/IEC 27001:2013 Information Security Management System (ISMS) - Requirements - specifies requirements for the establishment, implementation, monitoring, review, maintenance and improvement of a management system for managing an organization's information security risks.

This three-day course leads you through the requirements specified in ISO/IEC 27001:2013 for implementing ISMS. These include modules from understanding your organization, scoping your ISMS, assessing and evaluating risks and building security awareness program for your organization. You will also learn practical risk assessment guided by case study example in conducting a risk assessment.

Objectives

1. This program defines the requirements to implement the ISO/IEC 27001:2013 Information Security Management System (ISMS). The course is designed to ensure information security management within your organization and the right way to review, monitor, operate, and improve information security. This helps you to protect organization's information and give confidence to any interested parties, especially your customers.

Target Participants

1. ISMS Implementors
2. ISMS Consultants
3. IT Managers/Personnel
4. Information Security Practicioners
5. Individual who needs to acquire and develop specific knowledge and skills in implementing the ISMS based on ISO/IEC 27001:2013

Modules

1. Introduction to ISMS
- What is Information Security
- What is Information Security Management Systems (ISMS)
- ISMS Family of Standards
- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- Critical Success Factor

2. ISMS Establishment
- Standards Relevant to ISMS
- Trainings Relevant to ISMS
- Gap Analysis
- Context of the organization
- ISMS Scope
- Information Security Objectives

3. Leadership
- Management Commitment
- Information Security Policy
- Roles and Responsibilities

4. ISMS Risk Assessment
- Introduction to Information Security Risk Management
- Standards Relevant for Risk Management
- Risk Assessment Process
- Risk Treatment Process
- Controls Determination
- Risk Treatment Plan (RTP)
- Residual Risk

5. Support
- Resources
- Competence
- Awareness
- Communication

6. Documented Information
- What is Documented Information
- Control of Documented Information
- Mandatory Documented Information
- Other Required Documented Information

7. Performance Evaluation
- Monitoring, Measurement, Analysis and Evaluation
- Internal Audit
- Management review

8. ISMS Improvement
- Nonconformity
- Corrective Action
- Continual Improvement

9. Group Activities and Case Studies

For additional information, please visit www.cyberguru.my. You can also contact us at training@cybersecurity.my or call at 03 8800 7999

Corporate Office:
CyberSecurity Malaysia, Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia | Tel: +603 8800 7999 | Fax: +603 8008 7000
Email: info@cybersecurity.my | Customer Service Hotline: +61 300 88 2999 | www.cybersecurity.my