



ISMS (ISO/IEC 27001:2013) **IMPLEMENTER** **TRAINING COURSE**

COURSE DURATION: 3 DAYS

COURSE BENEFITS

- Your organization will have an internal resource and process to plan and establish an ISMS
- You will gain a professional qualification that certifies you have the knowledge and skills to plan and establish an ISMS for the organization
- Support the organization to protection the sensitive data, i.e. personal data, trade secret, to compliance with legal, legislation and governance requirements
- Understand the gaps between existing ISMS and international standards

COURSE INTRODUCTION

The successful completion of this course is essential for ISMS (ISO/IEC 27001, Information Security Management Systems) implementation, can reduce the cost on try and error and speed-up the implementation.

To participate this training course, the following prior knowledge were expected:

1) Knowledge of Management System Compliance (ISO 19600)

- Process approach (Plan-Do-Check-Act)
- Business overall compliance risk management (ISO 31000), includes legal, legislation, contractual obligations, standards, policies and procedures.
- Top management leadership, other roles and responsibilities to support management system
- Consideration of planning a management system - identify the organisational and technical measures to manage the identified risk
- Supporting required by the management system
- Management system operation consideration - monitoring, reporting and communicating
- Performance evaluation of a management - objectives evaluation, Internal Audits and Management Review
- Continual improve the effectiveness of a management system

2) Knowledge of Information security management principles and concepts, includes but not limited to:

- Awareness of the need for information security;
- The assignment of responsibility for information security;
- Incorporating management commitment and the interests of stakeholders;
- Enhancing societal values;
- Using the results of risk assessments to determine appropriate controls to reach acceptable levels of risk;
- Incorporating security as an essential element of information networks and systems;
- The active prevention and detection of information security incidents;
- Ensuring a comprehensive approach to information security management;
- Eontinual reassessment of information security and make of modifications as appropriate.



COURSE DURATION

- 3 Days

FURTHER INFO

- This is an International Register of Certificated Auditors (IRCA) Certified Course (A17533) and meets training requirements for those seeking registration as a lead auditor under this scheme.
- Evening session is available for participants to discuss with the trainer on their issues or case studies (optional)
- Refreshments, lunch, course notes & training certificate will be provided.



3) ISO/IEC 27001: Knowledge of the requirements of ISO/IEC 27001 (with ISO/IEC 27002) and the commonly used information security management terms and definitions, as given in ISO/IEC 27000.

Note. You are advised that course examination questions can relate to any requirement of ISO/IEC 27001 and the expected prior knowledge. For delegates who do not have these, we recommend attending our foundation training course.

LEARNING OBJECTIVES

- Understand the ISMS documentation requirements
- Understand how to develop the ISMS policies, procedures, includes:
 - * ISMS operation and certification scope
 - * ISMS policy and objectives
 - * ISMS organization security
 - * Information asset management
 - * Information security risk management process
 - * Information security risk control on human resource security (employee, outsource and supplier)
 - * Information security risk control on encryption, mobile devices, redundancy
 - * Information security risk control on physical and environmental
 - * Information security risk control on communication and network
 - * Information security risk control on information system and application
 - * Information security risk control on legal and technical compliance
 - * Information security risk control on incident and change management
 - * Information security risk control on business continuity



WHO SHOULD ATTEND?

This is intended for those who will be involved in implementation an ISMS that conforms to ISO/IEC 27001:2013 in any organization. Suggested job functions and their teams include:

- Information security managers
- IT and corporate security managers
- Corporate governance managers
- Risk and compliance managers
- Information security consultants

COURSE OUTLINE

DAY 1: RISK MANAGEMENT PRINCIPLES (ISO 31000), MANAGEMENT SYSTEM COMPLIANCE (ISO 19600), ISMS (ISO/IEC 27001)

- Understand the compliance risk (ISO 31000) - Legal, Legislation, Contractual Obligations, Standards, Policy and Procedures
- Information security risk control on legal and technical compliance
- Select and define ISMS operation and certification scope
- ISMS policy and objectives
- ISMS documented information
- ISMS Organizational Security



DAY 2: ASSET MANAGEMENT PRINCIPLES AND INFORMATION SECURITY RISK MANAGEMENT PROCESS (ISO/IEC 27005) AND INFORMATION SECURITY RISK CONTROL OBJECTIVES AND CONTROLS (ISO/IEC 27002)

- Establish the information asset management process
- Establish information security risk management process
- Risk assessment report
- Risk treatment plan
- SoA, Statement of Applicability
- Information security risk control on human resource security (employee, outsource and supplier)
- Information security risk control on encryption, mobile devices, redundancy

DAY 3: INFORMATION SECURITY RISK CONTROL OBJECTIVES AND CONTROLS (ISO/IEC 27002)

- Information security risk control on physical and environmental
- Information security risk control on communication and network
- Information security risk control on information system and application
- Information security risk control on incident and change management
- Information security risk control on business continuity
- Q & A / Course examination



TRAINER'S PROFILE

PHILIP KU

EDUCATION QUALIFICATIONS

- ✓ **Doctoral Candidate, Master of Advanced Business Practice**, University of South Australia
- ✓ **Master of Business Administration (MBA)**, Leicester University, United Kingdom (UK)
- ✓ **Degree in Electronic Engineer and Computer Science**, Kuang-Wu College, Taiwan

CLIENTS SERVICED

- Ministry of Health Malaysia
- Universiti Putra Malaysia
- MAMPU (Malaysia Administrative Modernisation And Management Planning Unit)
- BKPP (Cabinet, Constitution and Government Relation Division)
- SMPKE Division, Prime Minister's Office, Putrajaya Malaysia
- Securities Commission Malaysia
- Ministry of Foreign Affairs, Malaysia
- ISM Insurance Services Malaysia Berhad,
- Measat Broadcast Network System Sdn Bhd
- Malaysia Airlines, MEPS, Sime Darby, TUV Nord, HSBC Bank,

Mr. Philip Ku has more than 22 years of hands-on experience in Information Technology. In his years of experience, he has achieved various achievements and references in organizations worldwide such as: Indonesia, Thailand, Vietnam, Taiwan, China, Malaysia, Singapore, Germany, Greece, India, Iran, Turkey, Bosnia, and Czech Republic.

The achievements and references include accreditation of IRCA Training Organization, development of site security inspection scheme, ISMS Lead auditor training course, establishing the Common Criteria (ISO/IEC 15408) ITSEF and etc.

Furthermore, Philip has attended numerous networks and business related seminars, workshops, and conferences since 1992. These can be categorized into different categories such as: management and security related system, data communication, database, software and business management.

This gave him a special edge to share his knowledge in the areas of IRCA registered ISMS (ISO/IEC 27001) Lead Auditor and CISCO.

COURSES & I.T. SERVICES

- Business Continuity Management Systems (BCMS: ISO 22301)
- Data Protection and Privacy service
- Data Center Design and Security Management
- Information Security Management & Technical services
- Information Security Management Systems (ISMS: ISO 27001)
- Personal Information Management System (PIMS: BS 10012)



TRAINER'S PROFILE

PHILIP KU

TECHNICAL QUALIFICATIONS AND EXPERIENCE

- IRCA certified Information Security Management Systems (ISMS, ISO/IEC 27001) Principle Auditor
- IRCA Auditor/Lead Auditor Training Courses; Programme Designer and Lead Tutor on
 - * ISMS (ISO/IEC 27001)
 - * ITSMS (ISO/IEC 20000-1)
 - * BCMS (ISO 22301)
- Other Training Courses; Programme Designer & Lead Tutor on
 - * PIMS (BS 10012) Foundation, Auditor/Lead Auditor Training Course
 - * EnMS (ISO 50001) Foundation, Auditor/Lead Auditor Training Course
- European Union certified "EuroPriSe" Seal Evaluation according to European Union directive - Data Protection Directives 95/46/EC (Certificate No. ULD-EuroPriSe-153-2011e) - the first EuroPriSe technical expert in Asia Pacific Region since 2010
- German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) licensed Common Criteria (ISO/IEC 15408) Evaluator
- ITIL Expert
- ISACA CRISC (Certified in Risk and Information Systems Control)
- Associate Member of Business Continuity Institute (BCI)
- BICSI DC 110 - Data Center Design Certified
- TSI Data Center Auditing (TUViT)
- Supervisor of National Accredited IT Security Evaluation Laboratory (ISO 17025 and ISO/IEC 15408 / ISO 18405), Taiwan

