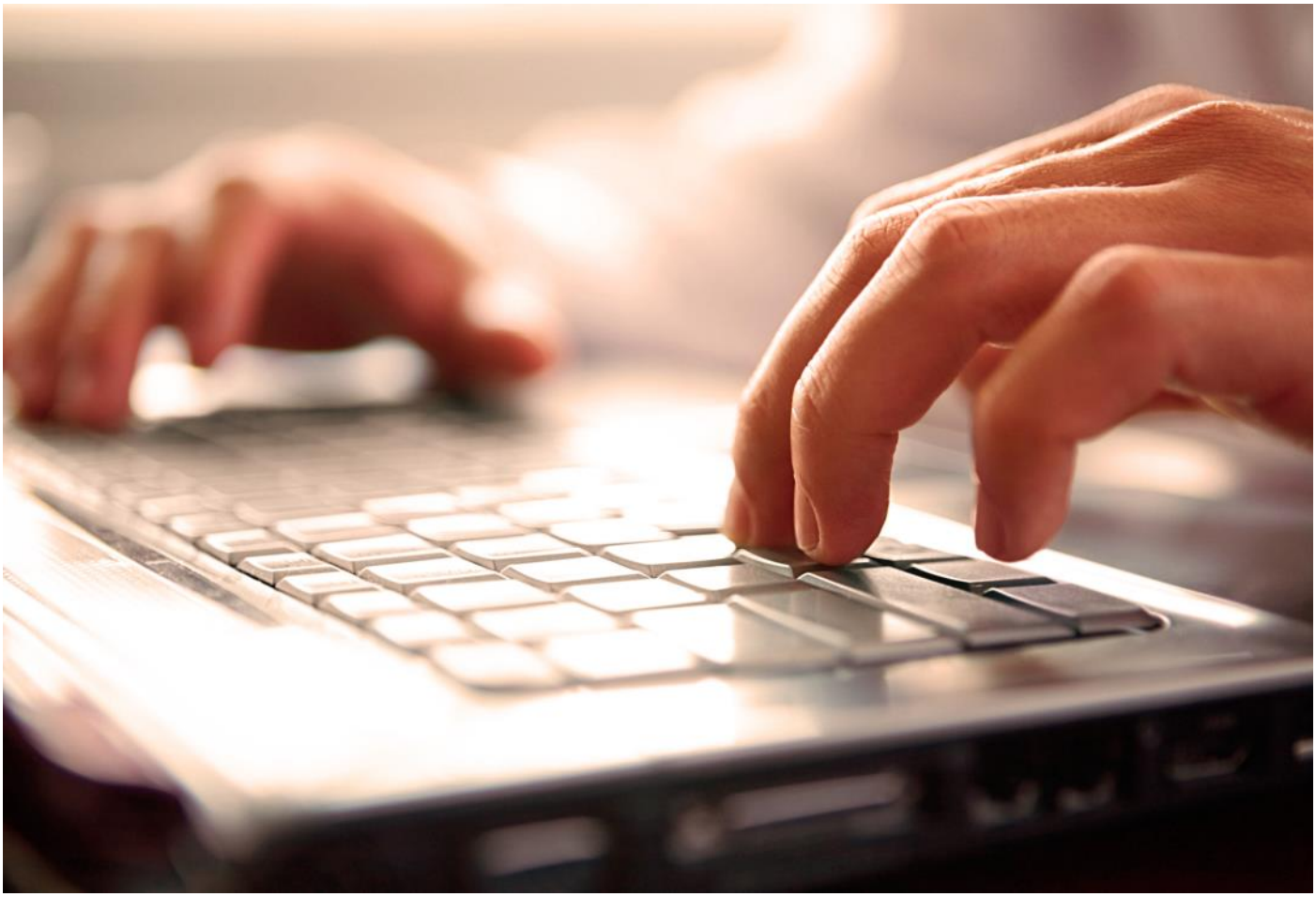
IDC Training House Sdn Bhd

LAST UPDATED 03-01-2018



# ISMS (ISO/IEC 27001:2013) AUDITOR / LEAD AUDITOR

## TRAINING COURSE (A17533)

**COURSE DURATION: 5 DAYS**

## LEARNING OBJECTIVES

- Learn how to explain the purpose and business benefits of an ISMS, of ISMS standards, of management system audit and of third-party certification
- Learn how to explain the role of an auditor to plan, conduct, report and follow-up an ISMS audit in accordance with ISO 19011 (and ISO 17021) where appropriate
- Learn how to plan, conduct, report and follow-up an audit of an ISMS to establish conformity (or otherwise) with ISO/IEC 27001 (with ISO/IEC 27002) in accordance with ISO 19011 (and ISO 17021 where appropriate)

# COURSE INTRODUCTION

This **CQI** (Chartered Quality Institute) /**IRCA** (International Register of Certificated Auditors) certified Information Security Management Systems (**ISMS**) Auditor / Lead Auditor Training Course (Registered Course Nr. A17533) is part of International recognized CQI/IRCA ISMS Auditor Certification programme.

The successful completion of this course is pre-requisite and essential to become an IRCA ISMS (ISO/IEC 27001, Information Security Management Systems) Auditor.

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 organizational 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;
- continual reassessment of information security and make of modifications as appropriate.

## COURSE DURATION

- 5 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) Management system audit (ISO 19011)**

- Audit programme management
- Initial the audit
- Document review
- Preparing for on-site audit
- Audit skills
- Conducting on-site audit
- Preparation of Audit evidences and findings
- Audit report
- Audit follow-up

**4) 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.

## COURSE BENEFITS

- Your organization will have an internal resource and process to be able to conduct its own audit of its ISMS to assess and improve conformance with ISO/IEC 27001:2013
- You will gain a professional qualification that certifies that you have the knowledge and skills to be able to lead a team to conduct an audit of an ISMS in any organization
- Successful auditing will improve the protection of any organization's private data to meet market assurance and corporate governance needs
- Understand how to identify gaps in an ISMS system
- Accurately audit will be able to provide continuous improvement to a management system
- Meet training requirements for IRCA auditor certification

## COURSE OUTLINE

### DAY 1: MANAGEMENT SYSTEM KNOWLEDGE (ISO 27001)

- The benefits of ISMS
- Process approach, Plan-Do-Check-Act (PDCA) and ISMS
- ISMS terms and definitions
- The ISMS processes and meaning for ISMS auditor
- Documented information for ISMS

### WHO SHOULD ATTEND?

This is intended for those who will be involved in leading audits of 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

## DAY 2: GUIDELINES FOR AUDITING MANAGEMENT SYSTEMS (ISO 19011 AND ISO 17021)

- Purpose of audit
- ISMS certification audit
- Audit processes
- Auditor responsibilities

## DAY 3: SIMULATE THE PROCESS OF PLANNING, PREPARATION FOR AN AUDIT

- Planning an audit
- Preparation of audit work documents includes checklist
- Conduct a Stage 1 audit (document review)
- Prepare a Stage 2 (on-site) audit plan

## DAY 4: SIMULATE THE OPENING MEETING, ON-SITE AUDIT ACTIVITIES, AND ROLE-PLAY

- Opening meeting
- Role play for audit scenarios
- Practice audit skills of collecting audit evidence
- Prepare audit findings, includes conformance, non-conformity, and opportunity for improvement (OFI)
- Prepare audit report

## DAY 5: SIMULATE THE CLOSING OF ON-SITE AUDIT - CLOSE MEETING AND FOLLOW-UP

- Closing meeting
- Audit follow-up
- Management system certification
- 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

www.facebook.com/IDCTrainingHouse www.idc-training.com info@idc-training.com +603-8061 5126 / 8061 8720
No.7, Unit 8, Jalan Industri PBP 3, Taman Industri Pusat Bandar Puchong, 47100 Puchong, Selangor, Malaysia.