TÜV NORD GROUP
Excellence for your Business

Information Security Management Systems (ISMS) Auditor/Lead Auditor Training Course
IRCA certified no. A17242

Course Introduction
(5 Days)

Date : January. 2014
Author: Joe Liu

Ref. No. ISMS-A17242-doc-01-v4-r0

Contents

Introduction

Course Description

Information is the basis on which governments and commercial organizations to conduct their business activities. Loss confidentiality, integrity, availability of information and services can have an adverse impact on organizations. Consequently, there is a critical need to protect information and to manage the security of information technology (IT) system within organizations. This requirement to protect information is particularity important in today's environment because many organizations are internally and externally connected by networks of IT systems.

TÜV Training services has designed a number of courses that will help you fully understand and implement effective information security and management.

This five day **- Information Security Management System (ISMS) Lead Auditor/Auditor training courses** is constructed in accordance with the international standard ISO 27001:2013 and ISO 27002:2013. It designed to provide an general introduction on the overall requirement of the standard itself.

By the end of this ISMS Auditor/Lead Auditor training courses, you will be able to:

- Explain the purpose and benefits of Information Security Management System (ISMS);
- Explain and apply the process (PDCA, Plan-Do-Check-Act) approach;
- Explain the processes in establishing, implementing, operating, monitoring, reviewing and improving an ISMS as defined in ISO/IEC 27001:2013;
- Explain the purpose, content and interrelationship of ISO/IEC 27001:2013, ISO/IEC 27002 and ISO 19011, ISO 31000: 2009 and legislative framework relevant to ISMS;
- Explain the roles of an auditor to plan, conduct, report and follow up an ISMS audit in accordance with ISO 19011;
- Interpret the requirements of ISO/IEC 27001:2013 in the context of an ISMS audit;
- Undertake the roles of an auditor to plan, conduct, report and follow-up an audit in accordance with ISO 19011.

Benefits

- Successful completion of an IRCA certified ISM Auditor/Lead Auditor training course will satisfy the training requirements for IRCA certification to all grades of Information Security Management Systems (ISMS) auditor. Detailed reference to http://www.irca.org ;
- Recognise your competence;
- Increase your credibility;
- International recognition;
- Increase earning potential;
- Improve your CV / resume.

Course structure and content

A combination of tutorials, workshop exercises and role-play, including the following topics:

- Relevant standards, ISO/IEC 27001: 2013, ISO/IEC 27002: 2013, ISO/IEC 27000: 2014, ISO 31000: 2009 , ISO 17021 and ISO 19011
- Information security
- The importance of information security
- Assessing security threats and vulnerabilities
- Management of information security risks
- Selecting security controls
- Information Security Management System (ISMS)
- Auditing to ISO/IEC 27001:2013
- ISO/IEC 27001:2013 auditing techniques
- Managing and leading a ISO/IEC 27001:2013 audit team
- Audit reporting
- Comprehensive course materials
- Formal written examination- ISO/IEC 27001:2013 Lead Auditor Qualification.

Who should attend?

- Those wishing to implement a formal Information Security Management System (ISMS) in accordance with ISO/IEC 27001: 2013
- Existing security auditors who wish to expand their auditing skills
- Consultants who wish to provide advice on ISO/IEC 27001: 2013 systems certification
- IT and Quality Professionals.

Prior knowledge

Before starting this course, you must inform students that they are expected to have the following prior knowledge:

a) Management systems

Understand the Plan-Do-Check-Act (PDCA) cycle

b) Information security management

Knowledge of the following information security management principles and concepts:

· 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 making of modifications as appropriate.

c) 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, which may be gained by completing an IRCA certified ISMS Foundation Training course or equivalent.

Organizational issues

- Delegates should note that there are evening works during the course
- **Minimum number of delegates is 4 (four). If the students less than 4, the course will be postpone.**

Continuous assessment process

Whilst participating on this course you will be subject to formal assessment as required by IRCA, which will involve two separate elements:-

1. **Complete/attend all elements of this course.**

2. Continuous assessment of each delegate undertaken by the course tutor(s) throughout the duration of the course whilst delegates are engaged in undertaking various case studies, collectively or individually, and during the simulated audit exercise.
3. A formal examination to be sat by each delegate on the final day of the five day course.

   Note:

   A. If a delegate should pass the continuous assessment, but fail the examination, they may re-sit the examination at a later date.

   B. If a delegate fails the examination with a particularly low mark, they will be advised to re-take the entire course.

   C. If a delegate should fail the continuous assessment (less than 60 out of 100 marks) they will not be permitted to take the examination.

   Re-sit of the examination must be taken within 12 months of the original course, and with the original course provider.

Continuous Assessment will be undertaken by the course tutor(s) on a daily basis and will be recorded in a "Personal Continuous Assessment Record" document. Tutors will use this document to maintain a record of delegate performance throughout the duration of the course.

Guidance for Syndicate exercise & Syndicate group work

You will be arranged into suitably sized syndicate teams for the purpose of undertaking the various course exercises and role play activities.

Each member of a syndicate team will be expected to undertake the role of Team Leader in turn, and your tutor will advise how this will be done. You should remember that your tutor(s) will have had very little time to get to know you and so teams may not always be suitably selected at first and your tutor may need to make some changes after the first exercise.

Syndicate exercises will require a formal presentation to be made by the Team Leader.

Syndicate Group Working will be undertaken in support of the Simulated Role Play audit and may not always require a formal presentation to be made, however the documents produced by delegates as a result of the syndicate group working should be retained as they will be used for the audit role play activity.

Please remember that some of your fellow delegates may have had more or less experience than yourself, and there may be naturally strong leaders. Try to allow each member of the team to act as Team Leader when it is their turn and respect their role as leader.

We hope that you enjoy the role play activities, none of which should be too difficult for you to attempt.

Please note that you will be expected to undertake some of the syndicate exercises and group working in the evenings, and under the supervision of the course tutor(s).

For those delegates attending this course on a non-residential basis:

Please note that it is an IRCA requirement that you are in attendance at all published course times. You should therefore make appropriate travel arrangements to ensure that you arrive in good time each morning, and can fully participate in course work until the published finishing time.

A failure to comply with this requirement could result in your failure to successfully complete the course.

Timetable

Day 1

Time	Description / Objectives
08:30	Coffee/Registration/Welcome
09:00	Ice Breaker: Self introduction of Tutors and Delegates
09:30	**Presentation 1:** Day 1 1. Introduction /IRCA Auditor Certification Scheme 2. Course Overview 3. Course Learning Objectives and continuous assessment process 4. Course Methodology 5. Accelerated Learning
09:45	Module 1**:** An Overview of Information Security Management System 1. The purpose and business benefits of an ISMS 2. Plan-Do-Check-Act framework and its application to information security management processes 3. The intent of Annex SL Appendix 2 & ISO/IEC 27001: 2013 structure 4. Benefits of third-party accredited certification of ISMS
10:15	Break
10:30	Module 1: Audit the Scope, Policies and Objectives of the ISMS – (case study) 1. Verify the purpose and the intended outcome(s) of the ISMS and the relevant external and internal issues 2. Verify the relevant interested parties and any relevant requirements 3. Verify the scope of ISMS 4. Verify that the information security policy and objectives.
12:00	Lunch
13:00	Module 1: Intent of management system clauses of ISO/IEC 27001:2013
14:30	**Presentation 4:** ISMS controls 1. Annex A
14:45	Module 1: ISO/IEC 27001:2013 controls (include 15 minutes break)
16:30	Module 1: Documentary requirement
18:00	End of Day 1

Day 2

Time	Description / Objectives
08:30	Recap of Day 1 – student understanding - performance review
09:00	**Presentation 5:** Risk management. (due to ISO/IEC TR 13335 part 3 & 4) 1. Systematic approach to risk assessment 2. Risk management process ■ Risk assessment ■ Risk treatment ■ SOA
09:30	Workshop 5: Risk identification, assessment and management (include 15 minutes break)
11:40	**Presentation 6:** Audit Types and Levels 1. Certification industry 2. Different types of Audit 3. Philosophy of Audit 4. Typical audit activities 5. Competence of Auditors 6. Interactive discussion
12:00	Lunch
13:00	**Presentation 7:** Audit Planning and Stage one Audit 1. Audit Planning 2. Stage one audit 3. Interactive discussion
13:15	Workshop 6: Audit planning, team composition and document review
15:30	Break
15:45	**Presentation 8:** Audit Plan
16:00	Workshop 7: Audit plan
18:00	End of Day 2

Day 3

Time	Description / Objectives
08:30	Recap of Day 2 – student understanding - performance review
09:00	**Presentation 9:** Audit Checklist and Questionnaire
09:20	Workshop 8: Audit Checklist (include 15 minutes break)
11:35	**Presentation 10:** Process and Process Audit 1. Process 2. Process Approach 3. Skill of Process audit
12:00	Lunch
13:00	Workshop 9: Process and process audit
14:45	**Presentation 11:** Overview of On-Site Audit Process (Stage two audit)
15:00	**Presentation 12:** Meeting 1. Opening meeting 2. Daily review meeting 3. Team meeting 4. Interactive discussion
15:15	Break
15:30	Workshop 10: Preparation of Opening Meeting
16:00	Workshop 11: Conduct Opening Meetings
18:00	End of Day 3

Day 4

Time	Description / Objectives
08:30	Recap of Day 3 – student understanding – performance review
09:00	**Presentation 13:** Collection information and Audit Skills 1. Collection information/objective evidence 2. Audit Skills ■ Sampling ■ Conducting interviews ■ Questioning ■ Note taking ■ Generic 3. Interactive discussion
09:30	Workshop 12: Preparation of On-site Auditing
10:30	Break
10:45	Workshop 13: Conduct Auditing
12:00	Lunch
13:00	(Audit activity continued)
14:00	**Presentation 14:** Audit findings and Nonconformity 1. Audit Findings 2. Nonconformity 3. Classification of nonconformity 4. Interactive discussion
14:20	Workshop 14: Classification of Finding
15:30	Break
15:45	**Presentation 15:** Writing Nonconformity report (NCR)
16:00	Workshop 15: Writing nonconformity reports
18:00	End of Day 4

Day 5

Time	Description / Objectives
08:30	Recap of Day 4 – student understanding – performance review
09:00	**Presentation 16:** Preparing Audit Conclusion and Closing Meeting 1. Preparing Audit Conclusion 2. Draft Audit Report(summery report) 3. Closing meeting
09:15	Workshop 16: Auditing review, preparing audit conclusion and Closing Meeting 1. Preparing audit conclusion 2. Writing Draft Audit Report (summery report) 3. Preparing Closing Meeting
10:30	Break
10:45	Briefing for Closing Meeting & Role Play
11:00	Workshop 17: Conduct Closing Meeting
12:00	Lunch
13:00	(Closing Meeting activity continued)
14:00	**Presentation 17:** Audit Report and Corrective/Preventive process 1. Audit Report 2. Corrective/Preventive process
14:15	**Presentation 18:** ISMS certification audit 1. Certification audit 2. Surveillance audit 3. Repeat audit 4. Interactive discussion
14:30	Final discussion and Course review ■ Student course feedback forms – Response ■ Course evaluation form ■ Examination Briefing
14:45	Break
15:00	***Examination:*** **ISMS Lead Auditor Examination**
17:00	End of Course

Contact information

Course information:

Web: http://www.tuv-nord.com or http://www.irca.org

Regional office: TÜV Asia Pacific Ltd. – Taiwan

Contact:	Ms. Cindy Lin
e-Mail:	cilin@tuv-nord.com
Tel:	+886-2-2378-0578 #32
Fax:	+886-2-2378-0587
Address:	Room A1, 9th Fl., No. 333, Tun-Hua S. Rd., Sec. 2, Taipei 106, Taiwan, R.O.C.

Control of this document:

This introduction has been designed and developed by TÜV Asia Pacific Ltd. Any changes or amendments that need to be made or are recommended need to be communicated to:

Joe Liu

TÜV Asia Pacific Ltd.

Tel: +886-2-2378-0578

Fax: +886-2-2378-0587

e-Mail: michael.chen@tuv-nord.com

Address: Room A1, 9th Fl., No. 333, Tun-Hua S. Rd., Sec. 2, Taipei 106, Taiwan, R.O.C.