MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

ISO/IEC 27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) LEAD AUDITOR TRAINING

Level: Professional | **Duration:** 5 days

Auditing is crucial to the success of any management system. As a result, it carries with it heavy responsibilities, tough challenges and complex problems. This five-day intensive course trains ISMS auditors to lead, plan, manage and implement an Audit Plan. It also empowers them to give practical help and information to those who are working towards certification and also provides the knowledge and skill required to carry out 2nd party auditing (suppliers and subcontractors).

Objectives

Effective auditing helps to ensure that the measures you put in place to protect your organization and your customers are properly managed and achieve the desired result.

Explain the purpose and business benefits of:

1. an ISMS and of ISMS standards;
2. of management system audit;
3. of third-party certification.
4. Explain the role of an auditor to plan, conduct, report and follow up an Information Security MS audit in accordance with ISO 19011 (and ISO 17021 where appropriate)

Have the skills to:

1. Plan;
2. Conduct;
3. Report;
4. And follow up an audit of an ISMS to establish conformity (or otherwise) with ISO/IEC 27001/2, ISO 19011 (and ISO 17021 where appropriate).

Target Participants

1. Management System (ISMS) in accordance with ISO 27001:2013 (either as a 2nd party, or 3rd party auditor), Those wishing to learn about effective audit practices
2. Existing information security auditors who wish to expand their auditing skills
3. Consultants who wish to provide advice on ISO 27001:2013 ISMS Auditing
4. Security and quality professionals

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

Modules

Day 1

1. What is an Information Security Management System?
   - Information security
   - Management systems
   - Purpose and benefits of ISO 27001
   - Related standards
2. Process Approach
   - PDCA model
   - Process model
3. Overview of ISO 27001 contents
4. ISO 27001 Mandatory clauses 4 – 8

Day 2

5. Controls
6. Overview of the audit process
7. Auditing the SOA
8. Audit and Auditors
   - Definitions
   - 1st, 2nd and 3rd party audits
   - Roles and responsibilities of auditors and lead auditors
   - Skills and characteristics of effective auditors
9. Audit Planning
   - Information needed to plan the audit, and things to consider
   - Preliminary visits
   - Preparation of an audit plan
10. Audit communications and meetings
    - Good practice for communication during the audit
    - Formal meetings
    - Opening meeting – what to cover and how
11. Checklists
    - Benefits and drawbacks
    - Content – what to include
    - Developing a checklist for a specific audit

Day 3

12. Process Audits
13. Case studies
14. Conducting the audit
    - interviewing
    - sampling
    - note taking
    - interacting with the auditee
    - who's involved and general points
15. Nonconformities
    - definition of nonconformity
    - linking to requirements of ISO 27001
    - grading nonconformity reports
    - structure and content of nonconformity reports

Day 4

16. Case studies
    - including interviewing.
    - developing and following audit trails
    - identifying non conformities
17. Specimen Examination
    - Review of answers
    - Layout and marking scheme of the papers
18. Closing Meeting
    - Outcomes
    - Content
    - Identifying possible issues and how to prevent or deal with these
19. Corrective Actions
    - Corrective action process
    - Evaluating corrective actions
20. Reporting the audit
    - Purpose and content of the written audit report
21. Next steps
    - action planning
    - further development
    - auditor registration

Day 5

22. Course Evaluations
23. Written Examination

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