TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

VIII

Practical info

06.09.2016 – Lecture 1 (introduction, CSMS)
13.09.2016 – Lecture 2 (context, regulations, assets, BPM, BIA)
20.09.2016 – Lecture 3 (asset valuation, CIA, IT mapping, governance)
~~27.09.2016 – Lecture 4 (self reading - OCTAVE)~~
04.10.2016 – Lecture 5 (IT risk assessment, methodology, ISO 27005)
11.10.2016 – Lecture 6 (IT risk management, KRI, CE)
~~18.10.2016 – Lecture 7 (IS management, ISO 27001)~~
~~25.10.2016 – Lecture 8 (self reading – IS roles)~~
01.11.2016 – Lecture 9 (IS measures planning, ISO 27002, IEC 62443)
08.11.2016 – Lecture 10 (risk+countermeasures analysis, bowtie, CMM)
15.11.2016 – Lecture 11 (IT auditing)
~~22.11.2016 – Lecture 12 (IS management metrics, IS economics)~~
29.11.2016 – Lecture 13 (Business continuity, testing)
06.12.2016 – Seminar 1 (around 10 HW presentations)
13.12.2016 – Seminar 2 (around 10 HW presentations)
20.12.2016 – Seminar 3 (around 10 HW presentations)
27.12.2016 – Exam (need confirmation)

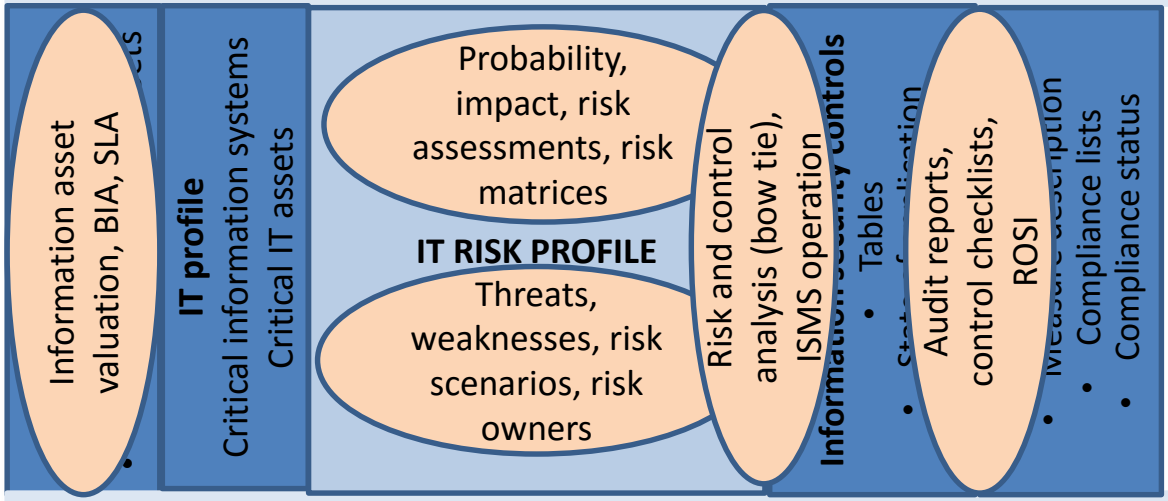
Practical info

Course page

https://courses.cs.ttu.ee/pages/ITX8090

Concept progress

Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.



IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc …)

Influence

<u>The events increase risk</u>

- Incident happened: the likelihood of its recurrence
- Key person leave: the loss of know-how
- Technological innovation: the interfaces to the existing infrastructure

Influence

The events mitigating risk

- Testing: successful
- **The audit's assessment: positive assessment**
- Apply additional measures: reduce the risk

Audit types

- Compliance audit - IT organization is in compliance with current legislation, standards, good practices etc;
- Information security audit - information security risks are adequately assessed and adequate measures have been implemented to manage risks;

Audit types

- Infrastructure audit - the infrastructure is built according to the needs and comprehensively, the administrative procedures have been implemented correctly;
- Process audit - for example, information systems development process has been developed and implemented, the development process will ensure adequate solutions to a reasonable use of resources.

Risk-based IT Audit

- Identification of high-risk areas (audit resource planning);
- Identification of confidentiality, integrity and availability needs;
- Assess the adequacy of processes and controls;
- Determine compliance with IT regulations;
- Require implementation of the improvements.

ISACA

Control development and implementation

- Based on business needs;
- The optimal level of clarification;
- Testing (effectiveness and efficiency);
- Implementation;
- Check measurement criteria;
- If possible automation;
- Necessary documentation, training;
- Enforcers confirmations.

ISACA

Control monitoring

- Testing;
- Documentation review;
- Detection of corrections;
- Implementation of corrections;
- Reporting.

Control object

- Whole organization, IT, business process;
- What is evaluated? Effectiveness, safety, compliance;
- What metrics / scale is used? Renewal of the systems, the number of regulations to be developed;
- Sufficient, insufficient - on the basis of what?
- The criteria for the test.

Test

Compliance testing/test of controls

An audit procedure designed to evaluate the operating effectiveness of controls in preventing or detecting and correcting material weaknesses. Examples of compliance testing of controls, where sampling could be considered, include user access rights, program change control procedures, procedure documentation, program documentation, follow-up on exceptions, review of logs and software licences audits.

Sampling

Audit sampling

The application of audit procedures to less than 100 percent of the items within a population to obtain audit evidence about a particular characteristic of the population.

Auditor

What should be?

- Independent;
- Competent;
- Correct;
- Ethical;
- …

Auditor (CISA)

What should know?

- Domain 1—The Process of Auditing Information Systems (14%)
- Domain 2—Governance and Management of IT (14%)
- Domain 3—Information Systems Acquisition, Development and Implementation (19%)
- Domain 4—Information Systems Operations, Maintenance and Support (23%)
- Domain 5—Protection of Information Assets (30%)

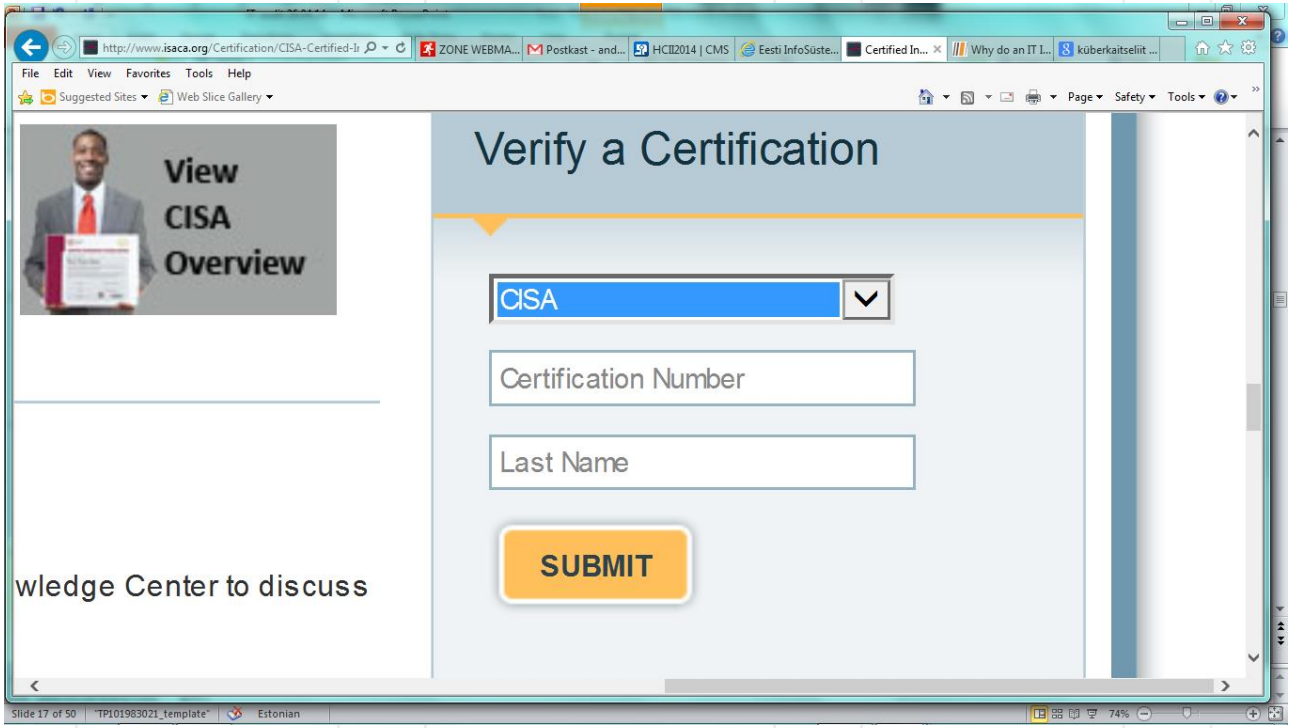
Auditor (CISA)

What should do?

- Successful completion of the CISA examination;
- Submit an Application for CISA Certification;
- Adherence to the Code of Professional Ethics;
- Adherence to the Continuing Professional Education Program;
- Compliance with the Information Systems Auditing Standards.

Auditor (CISA)

How to make shore?



Audit task

An IT Infrastructure audit should cover for example the following:

1. Asset listing of your hardware to support budgeting, planning and management;
2. A list of software installed on each machine;
3. Appropriateness of hardware in each machine and how this impacts upon performance;
4. The version of operating system, security, and patching done;

Audit task

An IT Infrastructure audit should cover for example the following:

5. Analysis of the network design;
6. Server hardware: appropriateness, performance, and levels of redundancy;
7. Analysis of the security environment (software, policies and procedures); and
8. Back-up systems: hardware, software, data management, and disaster recovery planning.

Infrastructure audit example

Compliance frameworks

ISO standards

Baseline Security

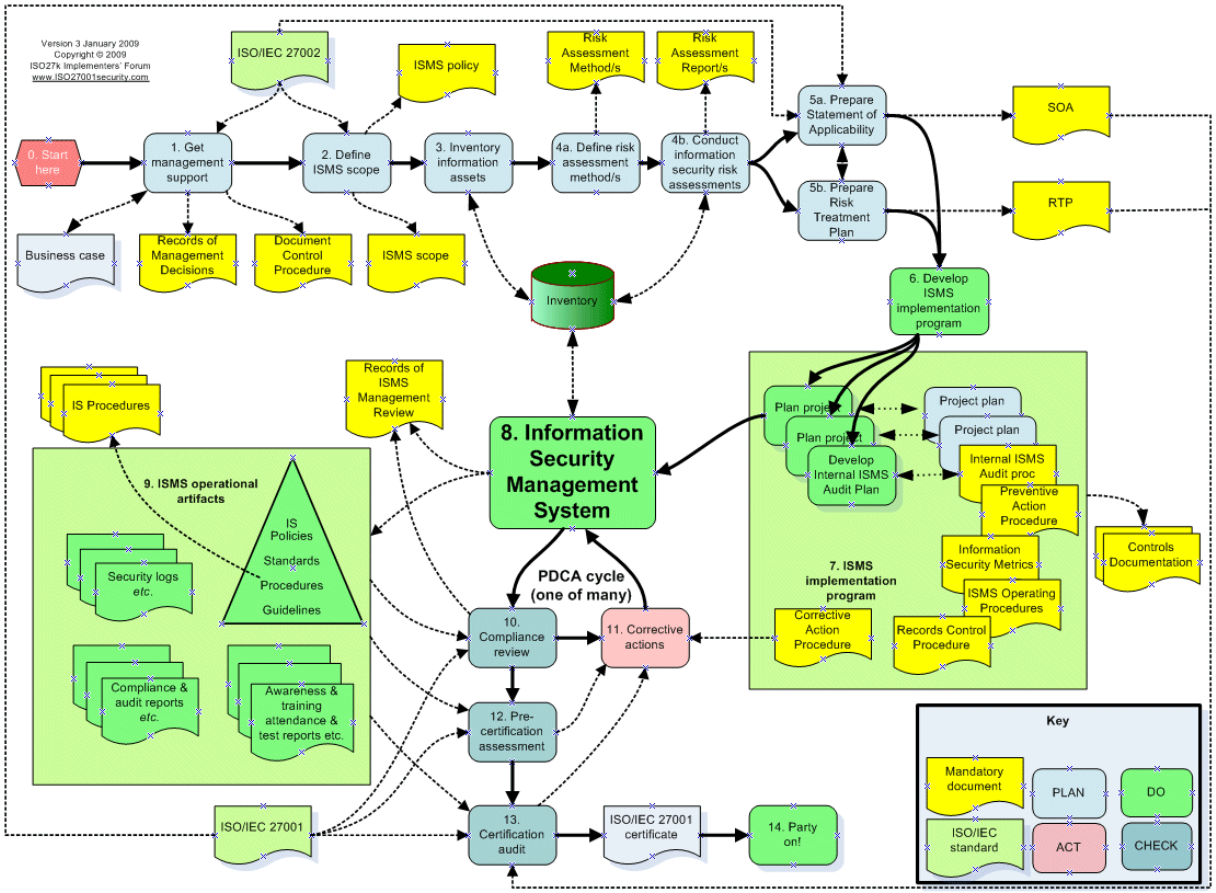
Sector-specific standards

Cyber Essentials

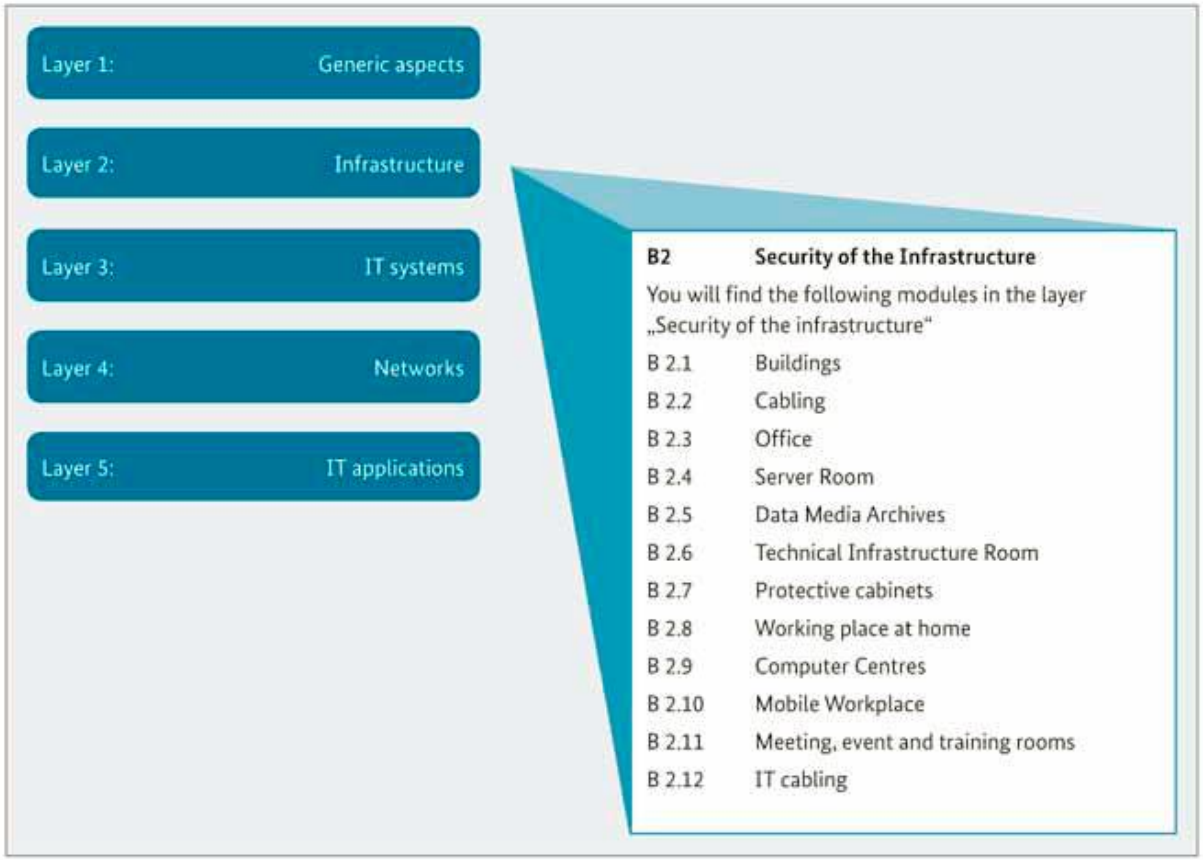
Critical controls

…

ISO ISMS


Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com
ISO/IEC 27002
ISMS policy
Risk Assessment Method/s
Risk Assessment Report/s
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4a. Define risk assessment method/s
4b. Conduct information security risk assessments
5a. Prepare Statement of Applicability
SOA
5b. Prepare Risk Treatment Plan
RTP
Business case
Records of Management Decisions
Document Control Procedure
ISMS scope
Inventory
6. Develop ISMS implementation program
IS Procedures
Records of ISMS Management Review
8. Information Security Management System
9. ISMS operational artifacts
IS Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO/IEC 27001
ISO/IEC 27001 certificate
14. Party on!
Plan project
Plan project
Develop Internal ISMS Audit Plan
Project plan
Project plan
Internal ISMS Audit proc
Preventive Action Procedure
Information Security Metrics
ISMS Operating Procedures
Records Control Procedure
Corrective Action Procedure
7. ISMS implementation program
Controls Documentation
Key
Mandatory document
PLAN
DO
ISO/IEC standard
ACT
CHECK

Baseline Security

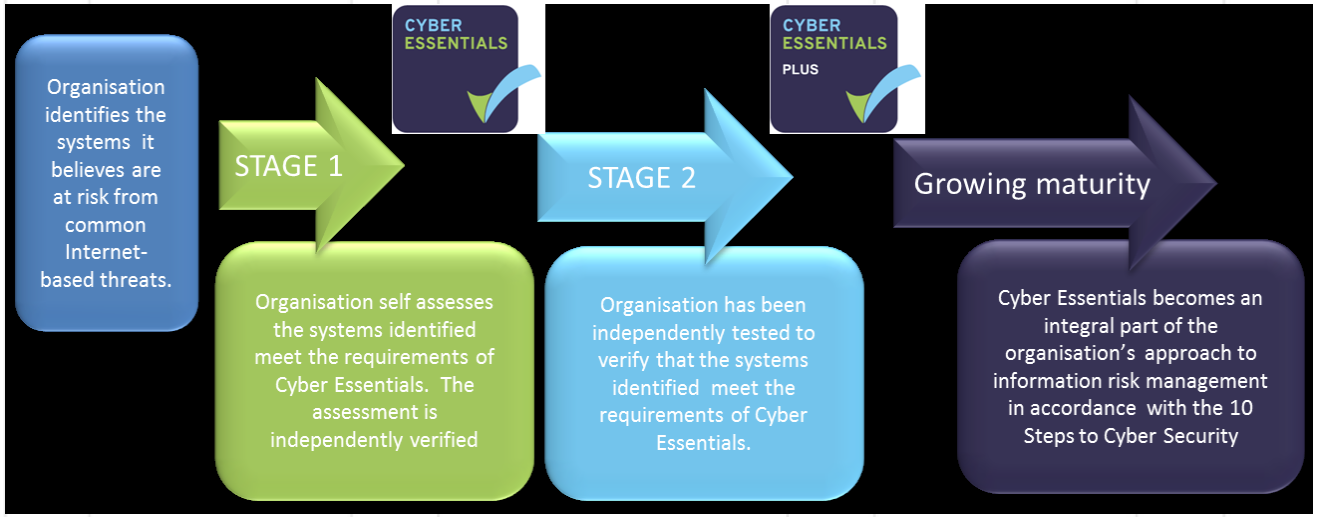


Sector-standards

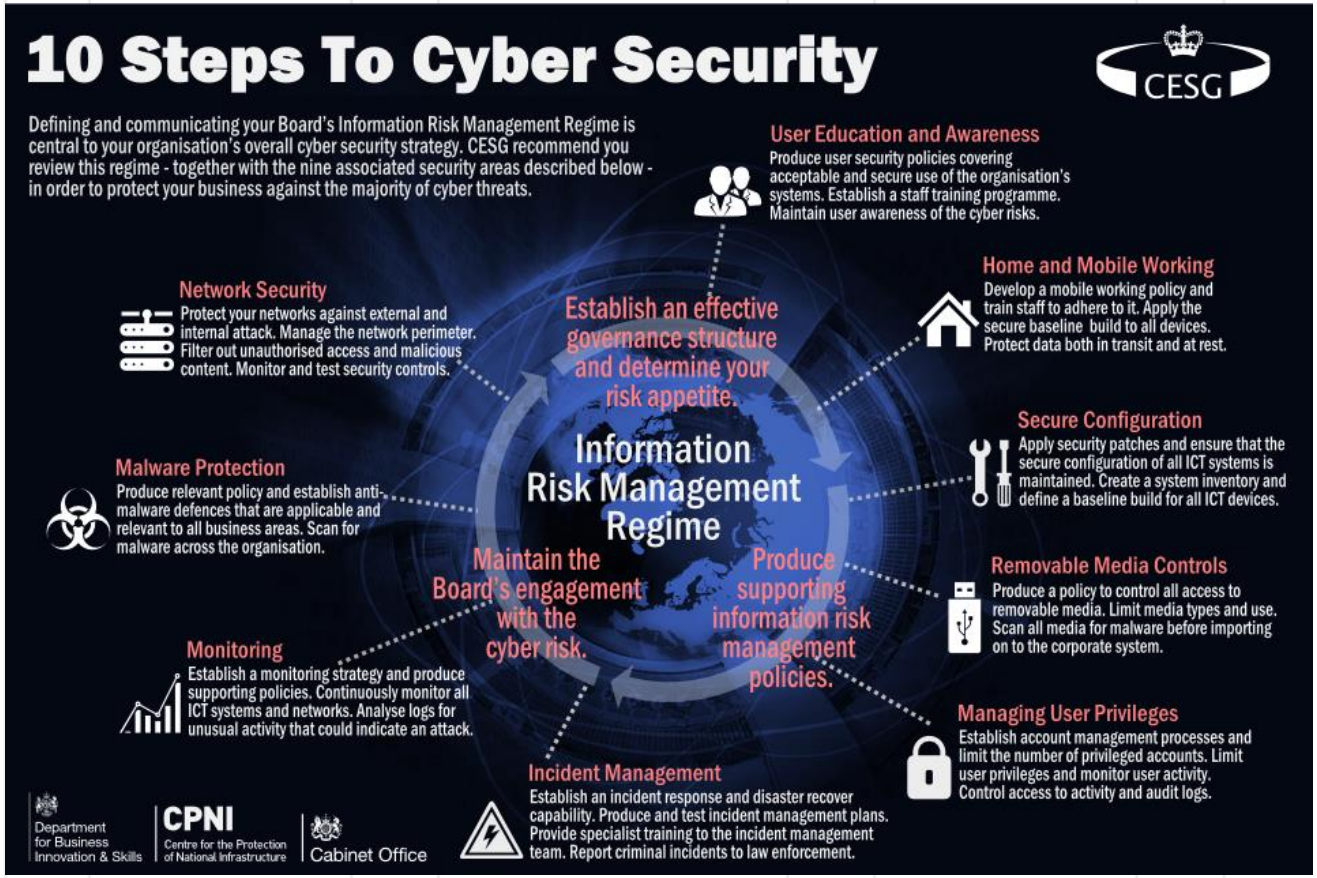
Financial sector

- Requirements for the organisation of the field of information technology
- Requirements for the organization of the field of information security
- Requirements for Organising the Business Continuity Process of Supervised Entities

Cyber essentials



Cyber essentials



Critical controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability

Critical Controls

11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Audit procedure

- Roles
- Planning
- Execution
- Reporting
- Closure

Roles

Lead auditor

- Prepares an Audit Plan/Notification as a basis for planning the audit and for disseminating information about the audit.
- Leads the ISMS internal audit activities
- Co-ordinates the audit schedule with concerned department/section heads
- Plans the audit, prepares the working documents and briefs the audit team.
- Consolidates all audit findings and observations and prepares internal audit report.
- Reports critical non-conformities to the auditee immediately.
- Report to the auditee the audit results clearly and without delay.
- Conducts the opening and closing meeting.

Roles

Auditor

- Supports the Lead Auditor’s activities.
- Performs the audit using the consolidated audit checklist.
- Reports the non-conformities and recommends suggestions for improvement
- Retains the confidentiality of audit findings.
- Acts in an ethical manner at all times.

Roles

Auditee

- Receives, considers and discusses the audit report.
- Determines, resources, drives and completes corrective actions as necessary.
- Is and remains accountable for protecting information assets.

Planning

The plan shall include:

- Audit objective and scope
- Department/Section and responsible individuals in charge.
- Audit team members. The number of auditors depends on the audit area size.
- Type of management system to be audited
- Date, place, time of the audit and distribution date of the audit report

Meetings

Pre-audit meeting

- To ensure the availability of all the resources needed and other logistics that may be required by the auditor.
- The scope of the audit is verified from the Audit Plan

Meetings

Opening meeting

- The purpose and scope of the audit.
- Confirmation of the audit plan
- Clarification of other matters must be settled before the audit takes place.

Execution

The auditors will perform several checklists:

- Audit Checklist/Observation Form – contains specific items that are particular to the organizational unit to be audited. The assigned auditors are responsible for generating questions using this form.
- Systemic Requirements Checklist– contain items relating to the requirements of ISO/IEC 27001
- Control Requirements Checklist– contain items pertaining to controls outlined in Appendix A of ISO/IEC 27001 and described more fully in ISO/IEC 27002.

Findings

Audit findings are collected through interviews, examination of documents and observation of activities and conditions in the areas of concern and will be written on the above-mentioned checklists.

Evidence

Evidence suggesting other non-conformities should be noted if they seem significant, even though not covered by the checklist. Other objective evidence and/or observations that may reflect positively or negatively on the information security management system shall also be listed on the space provided for on the above-mentioned checklists.

Reporting

Classification of findings shall be:

Major non-conformity – This pertains to a major deficiency in the ISMS. A non-conformity also pertains to one or more element of the ISO 27001 is not implemented. Non-conformities have a direct affect on information security specifically on the preservation of confidentiality, integrity and availability of information assets.

Minor non-conformity – A minor deficiency. One or more elements of the ISMS is/are only partially complied. Minor non- conformity has an indirect effect on information security.

Report

- Audit Reference Number
- Date of Audit
- Department/Section Audited/Process Name
- Name of Auditee and auditors
- Statement of findings (all non conformities found)
- Reference to the information security management system and standard
- Corrective and Preventive Actions with completion date
- Follow-up actions for non conformities
- Verification of follow-up actions

Closure

- Whereas the auditors are responsible for identifying non-conformities, auditees are responsible for resolving non-conformities
- Approved corrective actions shall be based on time scales agreed with the auditors.
- The Lead Auditor shall follow-up to check the implementation of corrective action
- An audit will not be considered complete and closed until all corrective actions or measures have been successfully implemented to the satisfaction of the Lead Auditor.

Records

ISMS internal audits generate the following formal records:

- Audit programme
- Audit plan/Notification
- Audit checklist/Observation sheet
- Systemic requirements checklist
- Control requirements checklist
- Internal audit Report
- Non-conformity/Corrective and Preventive Action report

Compliance audit exercising based on ISO 27001/002

PhD Andro Kull
CISA, CISM, CRISC, ABCP
E-mail: Andro@consultit.ee
Skype: andro.kull