TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

VIII

Lectures

- 05.09.2017 at 12.00-15.15 ICT 312 (introduction)
- 12.09.2017 at 12.00-15.15 self study (roles)
- 19.09.2017 at 12.00-15.15 ICT 312 (business processes)
- 26.09.2017 at 12.00-15.15 ICT 312 (asset list, valuation)
- 03.10.2017 at 12.00-15.15 self study (OCTAVE)
- 10.10.2017 at 12.00-15.15 ICT 312 (risk assessment)
- 17.10.2017 at 12.00-15.15 ICT 312 (risk+control, bow tie)
- 24.10.2017 at 12.00-15.15 ICT 312 (infosecurity controls)
- 31.10.2017 at 12.00-15.15 self study (security metrics)
- 07.11.2017 at 12.00-15.15 ICT 312 (cybersecurity controls)
- 14.11.2017 at 12.00-15.15 self study (COBIT)
- 21.11.2017 at 12.00-15.15 ICT 312 (audit)
- 28.11.2017 at 12.00-15.15 ICT 312 (continuity)
- 05.12.2017 at 12.00-15.15 seminar
- 12.12.2017 at 12.00-15.15 seminar
- 19.12.2017 at 12.00-15.15 seminar
- 26.12.2017 at 12.00-15.15 seminar?

Practical info

Updates in course page

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

Practical info

Homework description

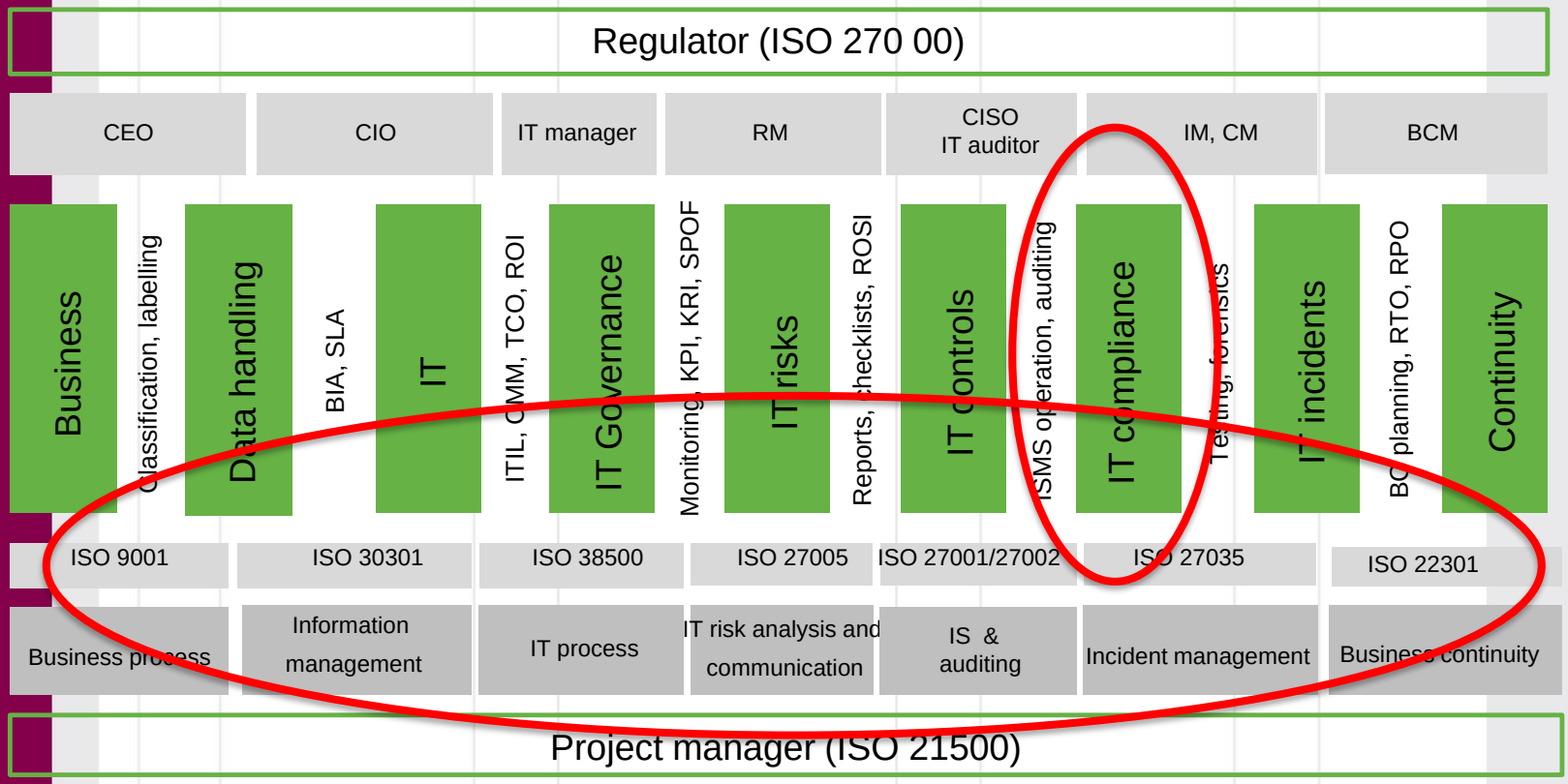
Deadline for submission - 30. November

Formal issues – around 10 pages +/-5

Presentation – during December in seminars.

IT risk and control concept

Legal obligations for IT security, data protection, business continuity, and internal goals



IT, risk, information security and business continuity management actions

Continuous monitoring

The events increase risk

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

The events mitigating risk

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

Risk-based IT Audit

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

Risk-based approach

I Risk Identification

1. Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.
2. Collect and review information, including existing documentation, regarding the organization’s internal and external business and IT environments to identify potential or realized impacts of IT risk to the organization’s business objectives and operations.
3. Identify potential threats and vulnerabilities to the organization’s people, processes and technology to enable IT risk analysis.

I Risk Identification

4. Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.
5. Identify key stakeholders for IT risk scenarios to help establish accountability.
6. Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide risk profile.
7. Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.
8. Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.

II IT Risk Assessment

9. Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.
10. Analyze risk scenarios based on organizational criteria (e.g., organizational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk.
11. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.

II IT Risk Assessment

12. Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.
13. Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.
14. Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.
15. Update the risk register with the results of the risk assessment.

III Risk Response and Mitigation

16. Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.
17. Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.
18. Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date).
19. Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.

III Risk Response and Mitigation

20. Ensure that control ownership is assigned to establish clear lines of accountability.
21. Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.
22. Update the risk register to reflect changes in risk and management’s risk response.
23. Validate that risk responses have been executed according to the risk action plans.

IV Risk and Control Monitoring and Reporting

24. Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.
25. Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.
26. Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.
27. Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.

IV Risk and Control Monitoring and Reporting

28. Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.
29. Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.
30. Review the results of control assessments to determine the effectiveness of the control environment.
31. Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.

Terms

- **Key Risk Indicator**, also known as a KRI, is a measure used in management to indicate how risky an activity is. It differs from a
- **Key Performance Indicator** (KPI) in that the latter is meant as a measure of how well something is being done while the former is an indicator of the possibility of future adverse impact. KRI give us an early warning to identify potential event that may harm continuity of the activity/project.

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;
- 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.

Example 1

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;
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.

IT infrastructure audit example

Audit types

Internal

- Independent of the activities audited, dependent on organization
- Takes into account effectiveness and efficiency
- Advisory role for improvement
- Continuous audit

External

- Independent of the activities audited and the organization audited
- Only takes into account the effectiveness
- No advisory role
- Audit planned specifically

Controls 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.

Controls monitoring

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

Audit 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 audit test.

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:

- user access rights
- program change control procedures
- procedure documentation
- program documentation
- follow-up on exceptions
- review of logs.

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.

Audit procedure

- Audit object - the area where ...
- Audit objective - to establish whether ...
- Audit Scope - systems ...
- Procedures - collect data …
- Procedures - validate the results …
- Treatments - communicate the results …
- The audit report – findings …

Audit planning

- Purpose - why is it necessary to organize an audit and what it seeks to achieve?
- The resource needs - especially the time, people, including the audited resources?
- Milestones - what steps are carried out in the course of the audit in order to achieve the desired objectives?

Audit communication

Its purpose is to communicate plans and share information.

The presentation of the audit team and workflow.

It is not intended to provide time to make improvements!

Conduct audit

Audit activities are carried out according to the plan:

- Collect materials (documentation, records);
- Carry out interviews with relevant staff,
- Carry out observations;
- Conduct surveys;
- Initiate tests.

Audit reporting

- The results of the audit are usually formulated as report;
- The results shall be announced (auditee comments and propose how to solve problems);
- If necessary, follow-up (problematic areas).

Auditor

What should be?

- Independent;
- Competent;
- Correct;
- Ethical;
- ...

Auditor certification

Possibilities:

ISACA – Certified Information Systems Auditor (CISA)

ISO auditor – ISO 27001 ISMS Lead Auditor (LA)

…

In both, knowledge, experience and continual training is obligatory!

Personal behaviours

1. Integrity
2. Open minded
3. Diplomatic
4. Observant
5. Perceptive
6. Versatile
7. Tenacious
8. Decisive
9. Self-reliant
10. Responsible
11. Open to improvement
12. Culturally sensitiive
13. Collaborative

ISMS
audit example

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