TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

V

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 (IS management metrics, IS economics)
~~22.11.2016 – Lecture 12 (self reading - IT auditing (ISACA))~~
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)

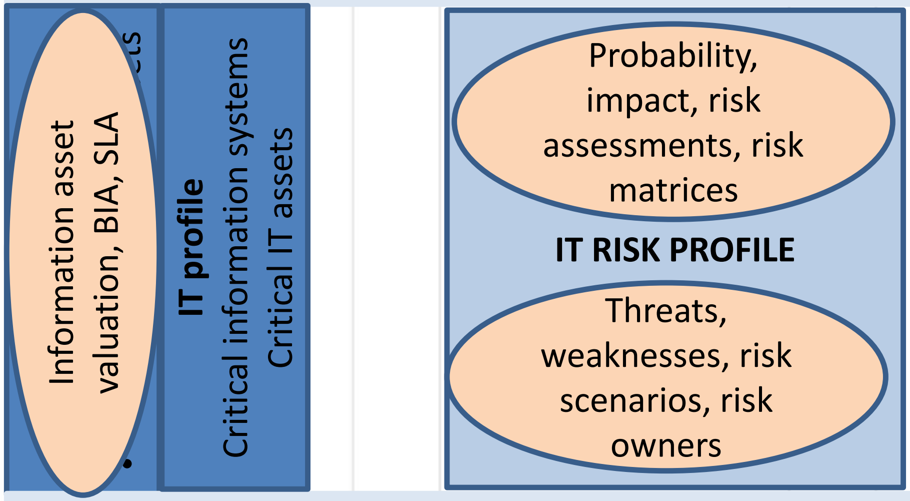
Practical info

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.



Information asset valuation, BIA, SLA

IT profile
Critical information systems
Critical IT assets

Probability, impact, risk assessments, risk matrices

IT RISK PROFILE

Threats, weaknesses, risk scenarios, risk owners

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 …)

ISO 27000 Terms and Definitions

Risk (information security)

- effect of uncertainty on (information security) objectives
- risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
- Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

ISO 27000 Terms and Definitions

Risk management:

- coordinated activities to direct and control an organization with regard to risk

Risk assessment

- overall process of risk identification, risk analysis and risk evaluation

Risk treatment

- process to modify risk

Risk analysis

Risk = probability x impact

Why?

Why do we assess risk?

- To inform a proper balance of safeguards against risk of failing to meet business objectives.

Why?

- To inform a position so that:
    - Removal of safeguards will increase the risk of loss to an unacceptable level
    - Adding any safeguards would make the security system too expensive/bureaucratic
    - ... and therefore it is a means by which expenditure on security and contingency can be justified

When?

- Organization must define a risk assessment process which includes criteria for performing risk assessments
- <u>What triggers the need for a risk assessment?</u>
- The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur
  - Risk owner proposal
  - Security event or incident

Event vs incident

Information security event

- identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.

Information security incident

- single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

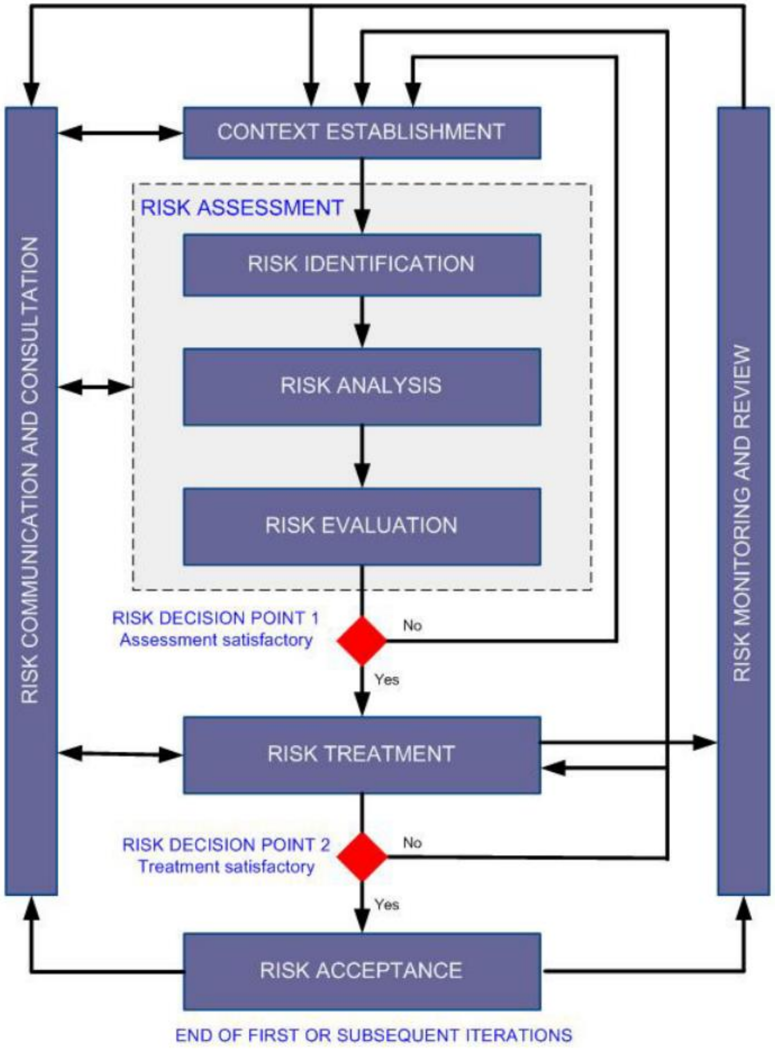
Financial terms

The annualized loss expectancy (ALE)

- is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).
- mathematically expressed as:

ALE = ARO x SLE

Place of risk assessment



Approach

The result of IT risk assessment should ensure that IT risks are:

Consistent

- constantly adhering to the same principles, course, form, etc.

Valid

- producing the desired result, effective:

Comparable

- having features in common with something else to permit or suggest compar ison

Possibilities - quantitative

Numerical example:

- Risk of power surge destroying server
- Cost of server 5000 (including impact on reputation, lost business, etc.)
- Power surge once every 2 years
- Annual Loss Expectancy 5000 x ½ = 2500

Possibilities - qualitative

Categories

- Low, Medium, High
- 1 to 10
- Critical, Essential, Important, Useful, Irrelevant
- …

Rate likelihood and impact, risk is factor of both!

Probability scale (example)

(Almost) certain	We are *bound* to experience further incidents of this nature - in fact they are probably occuring right now!	100%
Probable	We are likely to experience incidents of this nature before long	80%
Possible	It is distinctly possible that we will experience incidents of this nature	62%
Unlikely	Incidents of this nature are uncommon but there is a genuine chance that we may experience them at some future point	25%
Rare	Although they are conceivable, we will probably never experience incidents of this nature	1%

Impact scale (example)

Determining the impact value

- What if (confidentiality, integrity, availability (CIA)) is compromised?

Impact scale (example)

Extreme	Major	Moderate	Minor	Insignificant
Complete operational failure, "bet the farm" impact, unsurvivable	Severe loss of operational capability, highly damaging and extremely costly but survivable	Substantial operational impact, very costly	Noticeable but limited operational impact, some costs	Minimal if any operational impact, negligible costs
100%	**80%**	**62%**	**25%**	**1%**

Risk matrix (example)

100%	80%	62%	25%	1%
80%	64%	50%	20%	1%
62%	50%	38%	16%	1%
25%	20%	16%	6%	0%
1%	1%	1%	0%	0%

Risk appetite

Risk appetite

- The level of risk that an organization is prepared to accept, before action is deemed necessary to reduce it.
- It represents a balance between the potential benefits of innovation and the threats that change inevitably brings.

High-level

Advantages

- Less resource required
- Quick to do
- Easily repeatable

Disadvantages

- May not identify all significant threats
- May not be aware of all possible controls
- Managing relevant changes difficult
- Resulting ISMS not as “value for money”

Detailed

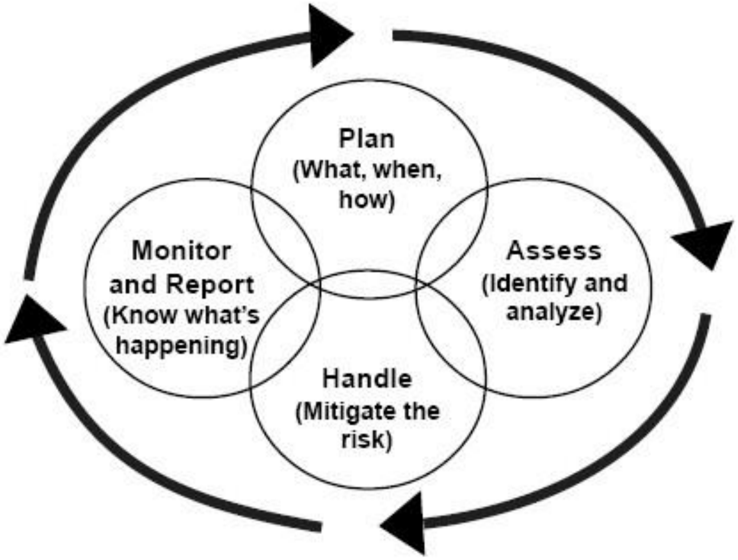
Advantages

- More accurate view obtained
- Allocation of controls more accurate
- More economical and efficient
- ISMS Handling of changes more manageable

Disadvantages

- Considerable
  - Time
  - Effort
  - Expertise

Risk management process



A Continuous Interlocked Process—Not an Event

Risk management process

- The Plan phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.
- The Do phase involves implementing and operating the controls.
- The Check phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.
- In the Act phase, changes are made where necessary to bring the ISMS back to peak performance.

Risk+control

Critical	🟥 …
High	🟧 …
Medium	🟨 …
Low	🟩 …

No control	🟥 …
Unsufficient	🟧 …
Adequate	🟨 …
Strong	🟩 …

Risk+control

Risk /control	…	…	…	…
…	…	…	…	…
…	…	…	…	…
…	…	…	…	…
…	…	…	…	…

Residual risk

Residual risk

- A residual risk is a portion of the risk that is left after a risk assessment has been conducted.
- The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats × vulnerability).

Practice

Risk register

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