TALLINN UNIVERSITY OF TECHNOLOGY

# Information and Cyber Security Assurance in Organisations

**ITX8090**

# VI

# Practical info

01.09.15
08.09.15
15.09.15
22.09.15
~~29.09.15~~
06.10.15
13.10.15
20.10.15
~~27.10.15~~
03.11.15
~~10.11.15~~
17.11.15
24.11.15
01.12.15
08.12.15
15.12.15

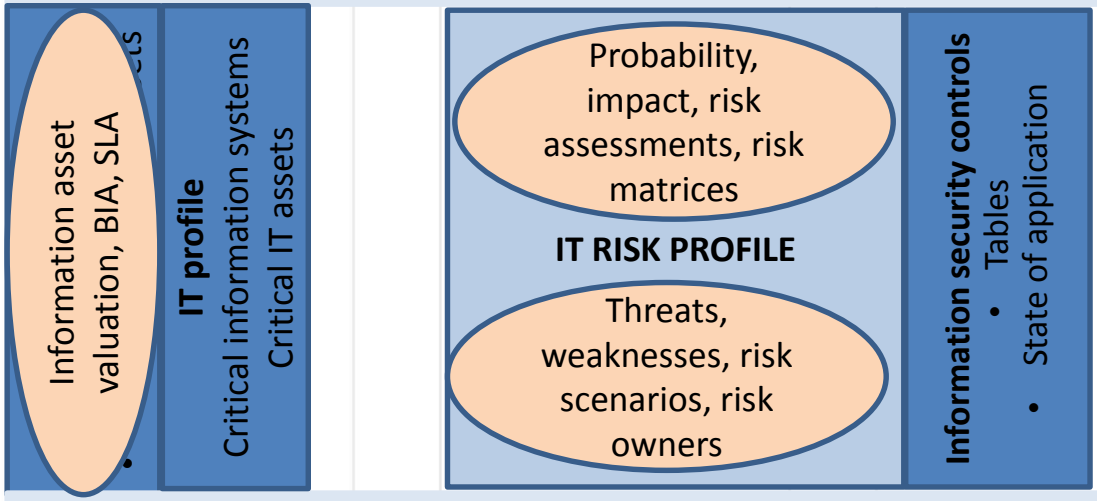
# Practical info

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 …)

# 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.

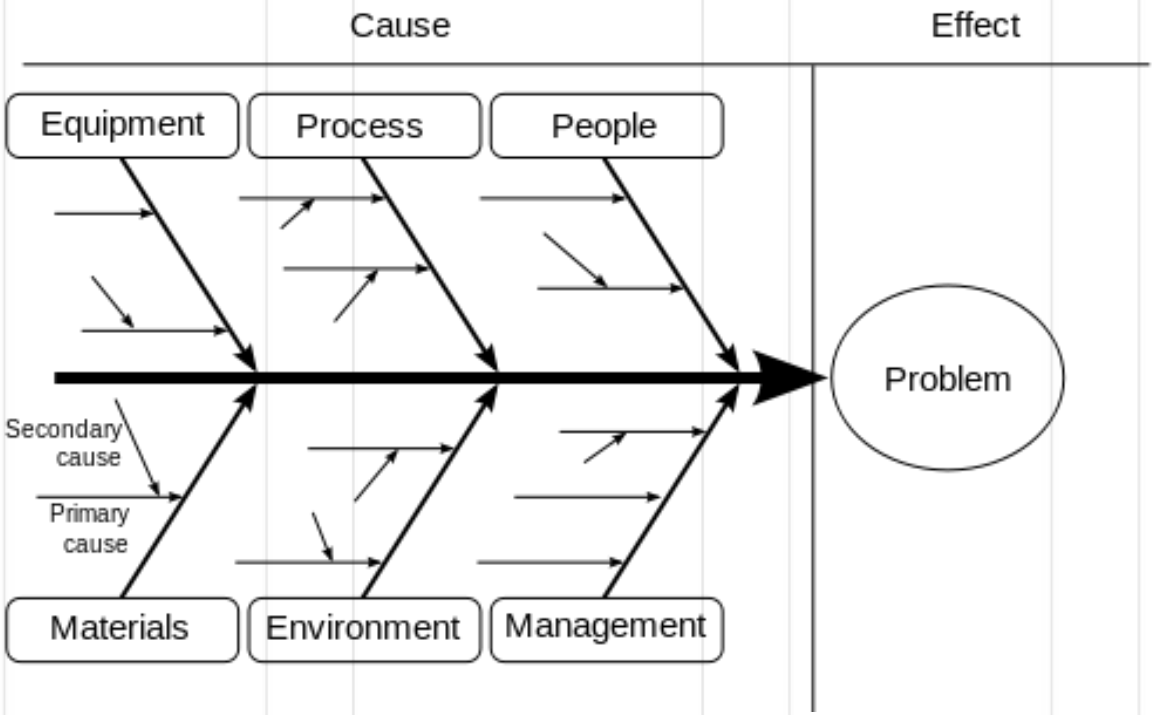
# Risk+control

| Risk /control | … | … | … | … |
|---|---|---|---|---|
| … | … | … | … | … |
| … | … | … | … | … |
| … | … | … | … | … |
| … | … | … | … | … |

# Causal analysis

- Ishikawa diagrams (fishbone diagrams, herringbone diagrams, cause-and-effect diagrams, or Fishikawa) are causal diagrams (by Kaoru Ishikawa);
- Causes are grouped into major categories to identify these sources of variation.

# Ishikawa diagrams



# Bow-tie method

- The outcome looks like men’s bow tie
- Analysing and demonstrating causal relationships
- Two main goals:
  - Gives a visual summary of all plausible accident scenarios that could exist around a certain hazard (risk event).
  - By identifying control measures displays what a company does to control those scenarios.

# Construction

- A hazard is something in the company which has the potential to cause damage.
- Once the hazard is chosen, the next step is to define the top event.

- Use indentified and assessed risks as „High“, „Critical“!

# Construction

- Threats are whatever will cause top event. There can be multiple threats.
- Consequences are the result from the top event. There can be more than one consequence for every top event.

# Construction

- Barriers (control and recovery measures) in the bow tie appear on both sides of the top event;
- Barriers interrupt the scenario so that the threats do not result in a loss of control (the top event) or do not escalate into an actual impact (the consequences).

# Construction

- There are different types of barriers, which are mainly a combination of human behaviour and/or hardware/technology.
- Once the barriers are identified, there is a basic understanding about how risks are managed (under control).

# Construction

- Anything that will make a barrier fail can be described in an escalation factor (for example, server does not have a power).
- The logical next step to manage escalation factors is to create barriers for escalation factors (in this case it could be a backup generator).

# Bow tie diagram

# Practice

**Exercise VII**

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