TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

VII

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)

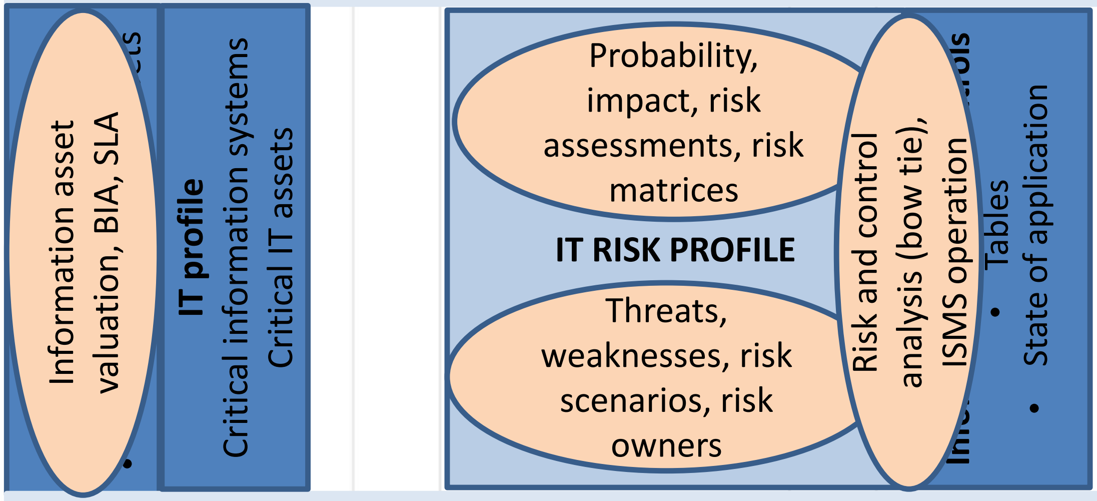
Practical info

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.



Information asset valuation, BIA, SLA

IT profile

Critical information systems

Critical IT assets

Probability, impact, risk assessments, risk matrices

IT RISK PROFILE

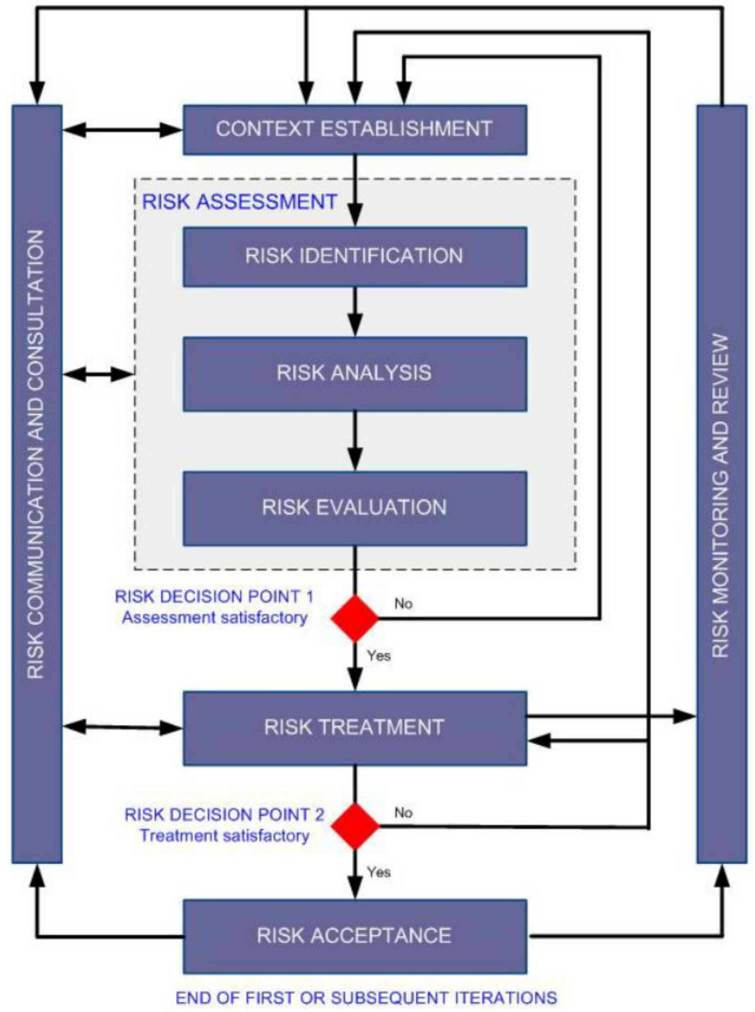
Threats, weaknesses, risk scenarios, risk owners

Risk and control analysis (bow tie), ISMS operation

- Tables
- State of application

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 …)

Management decision



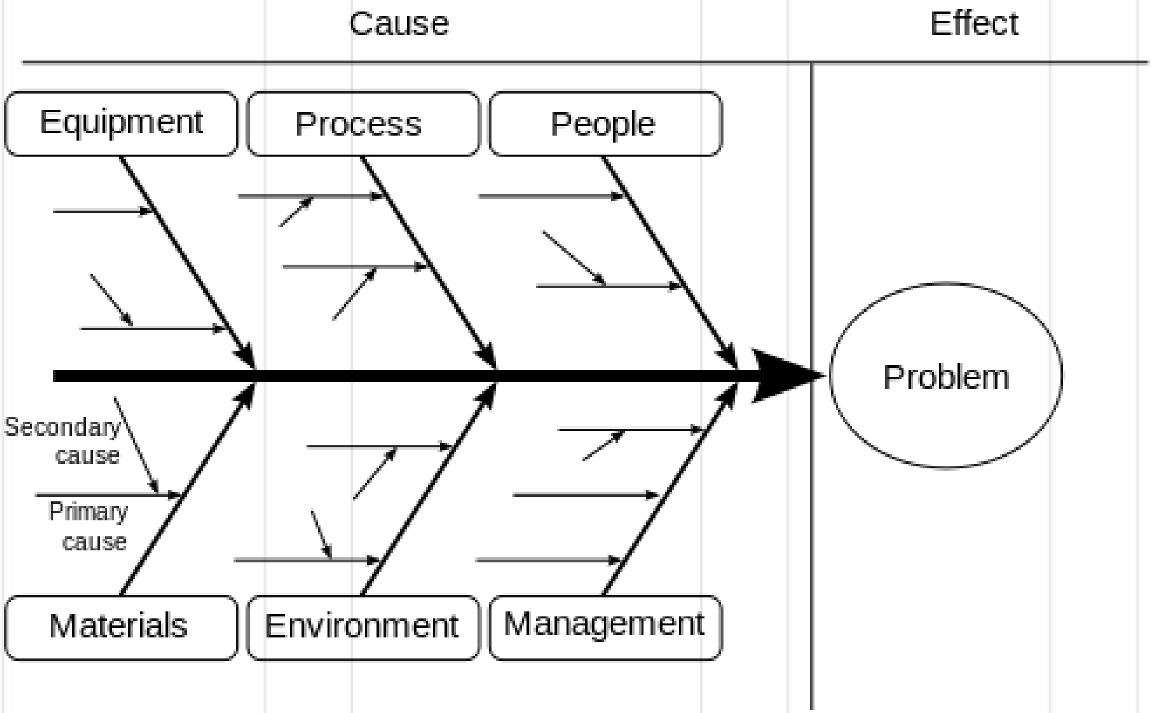
Risk+control

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

Causal analysis

- Ishikawa diagrams (fishbone diagrams, herringbone diagrams, cause-and-effect diagrams, or Fishikawa) are causal diagrams;
- 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).

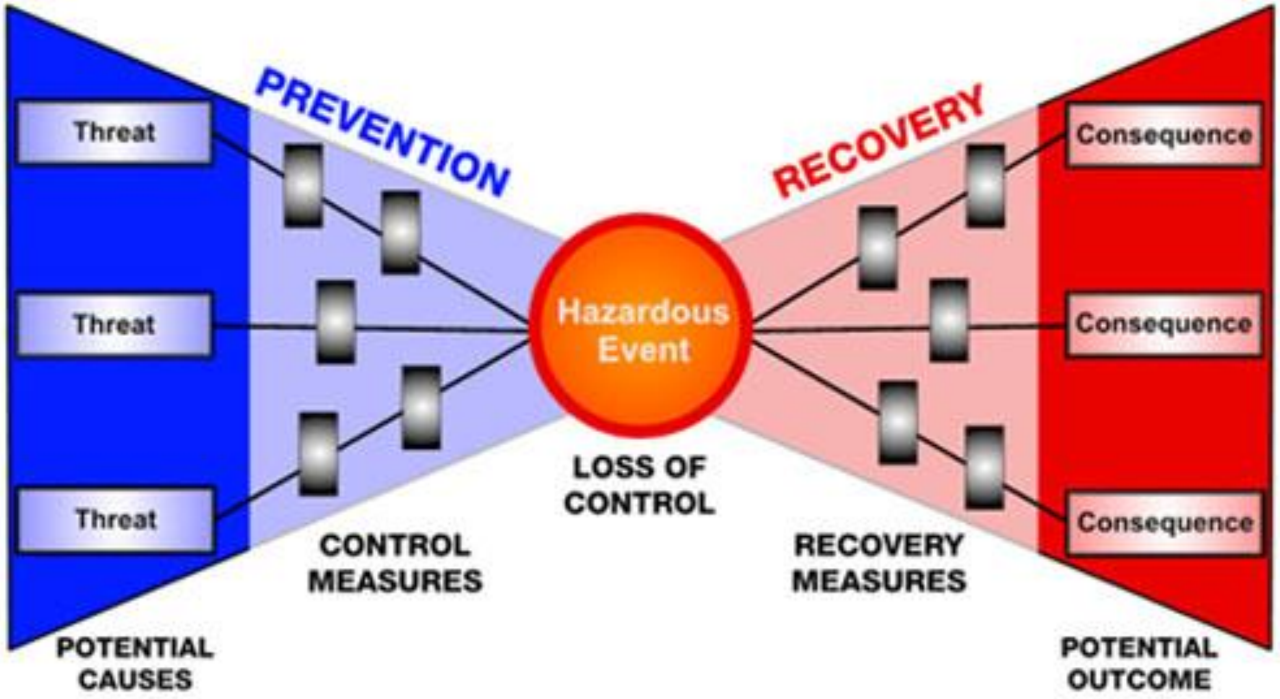
Construction

- 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).

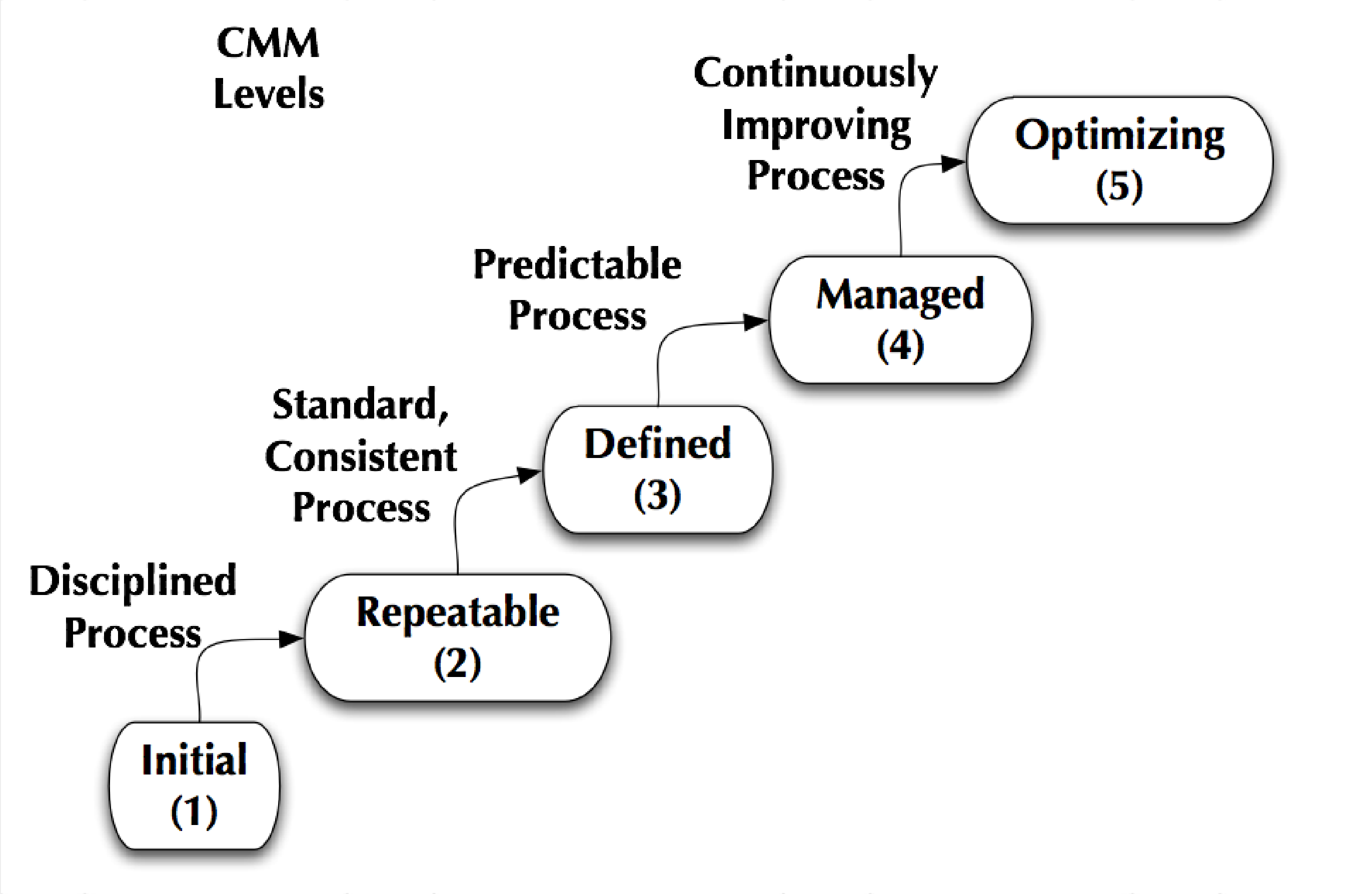
Construction

- 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



CMM



CMM Levels

Initial (1)

Disciplined Process

Repeatable (2)

Standard, Consistent Process

Defined (3)

Predictable Process

Managed (4)

Continuously Improving Process

Optimizing (5)

Process meaning

Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.

Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted.

Defined - the process is defined/confirmed as a standard business process.

Managed - the process is quantitatively managed in accordance with agreed-upon metrics.

Optimizing - process management includes deliberate process optimization/improvement.

Level 1 - Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 - Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process. In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5 - Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

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