TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

V

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?

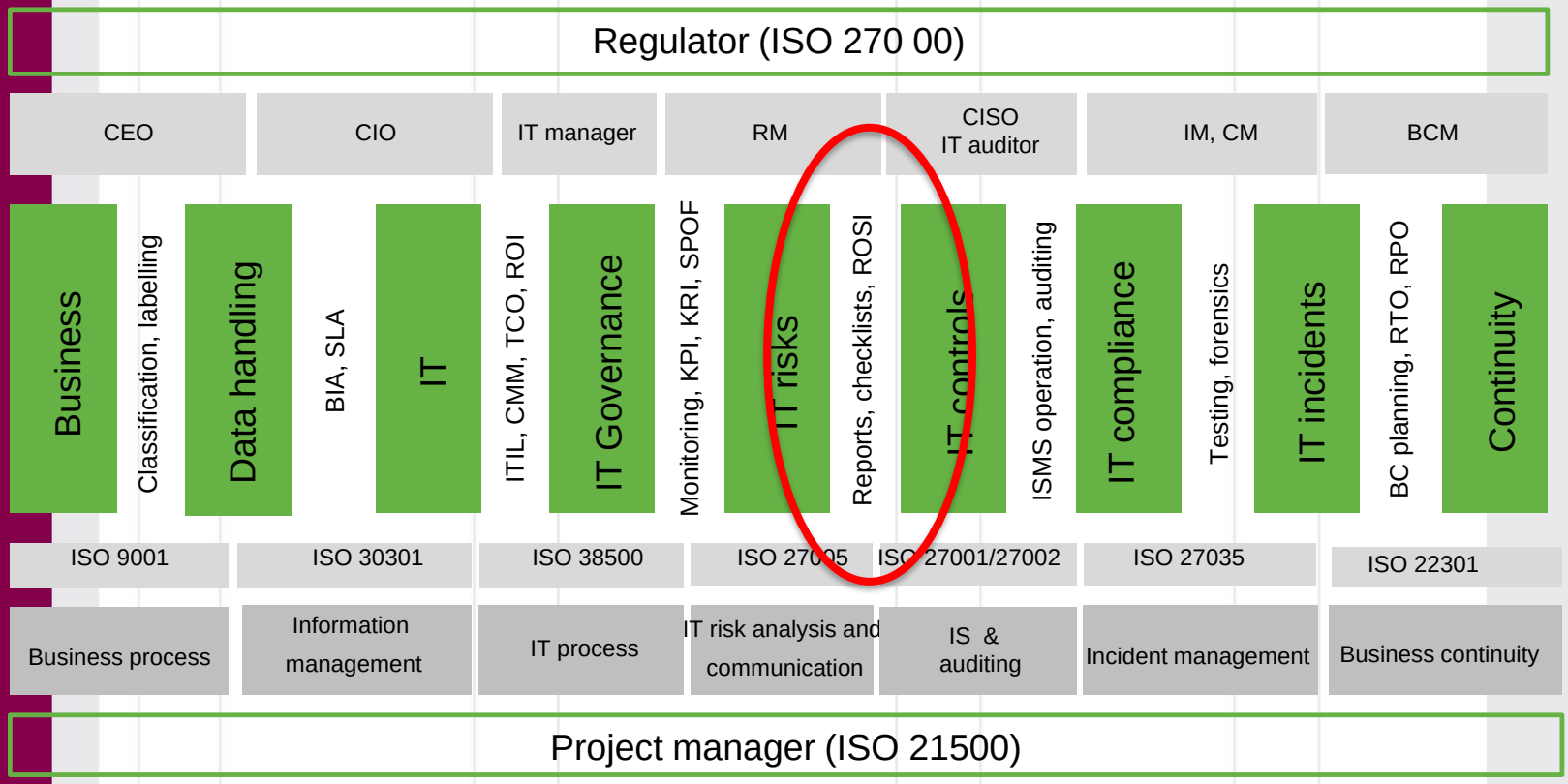
Practical info

Updates in course page

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

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

Risk+control

Critical	…
High	…
Medium	…
Low	…

No control	…
Unsufficient	…
Adequate	…
Strong	…

Risk+control

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

Risk treatment

- Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment.

Risk treatment

- Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks

Decision

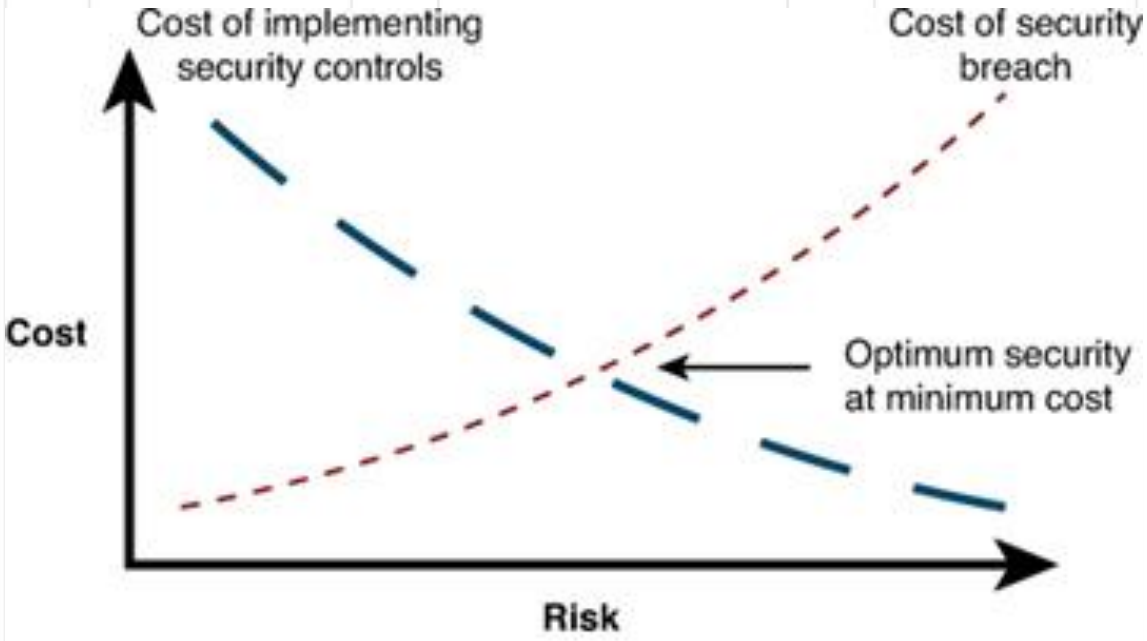
Options for risk decision

- Terminate the risk (eliminate, reject, avoid)
- Tolerate (accept, retention, retain)
- Treat (reduce)
- Transfer (share), for example insurance, outsourcing and SLA terms

Treatment

- Risk acceptance criteria should consider business, legal, operational, technological, financial and social requirements
- Other risks to be handled
- If treat, controls are either:
  - Already in place and need enhancing, ensuring consistent and measures aligned
  - Need to be introduced

Risk and security cost



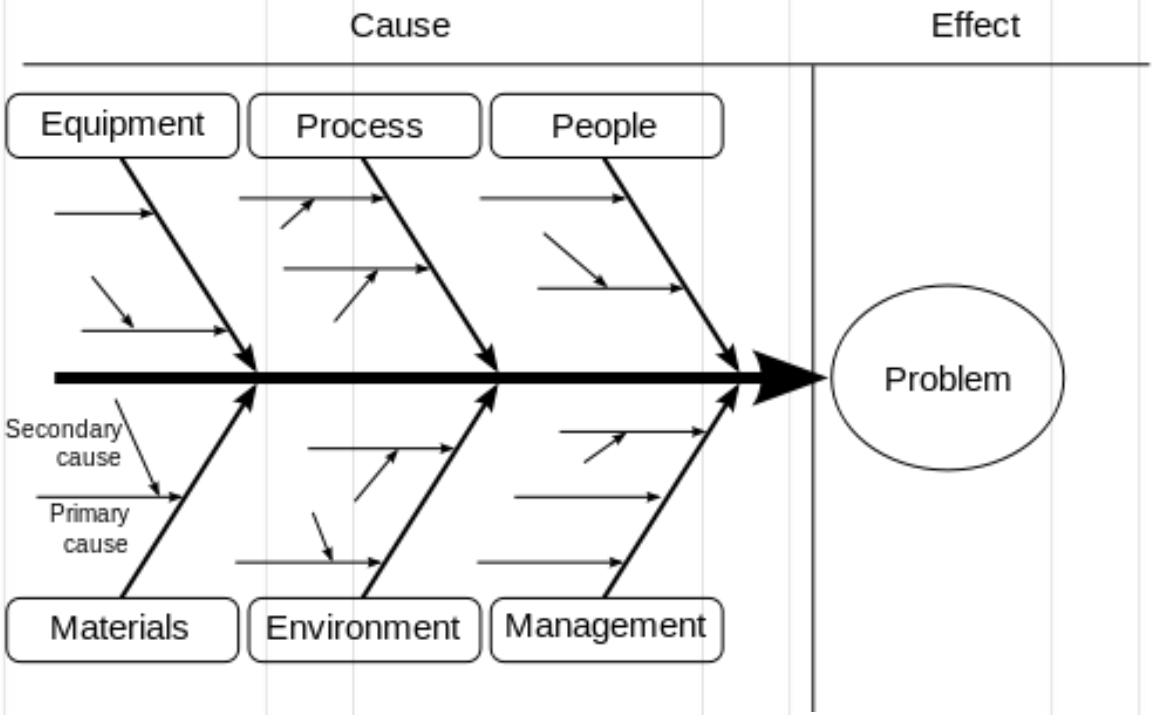
Analysis of cost vs. risk
Cost of implementing security vs. cost of security breach

www.ciscopress.com

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

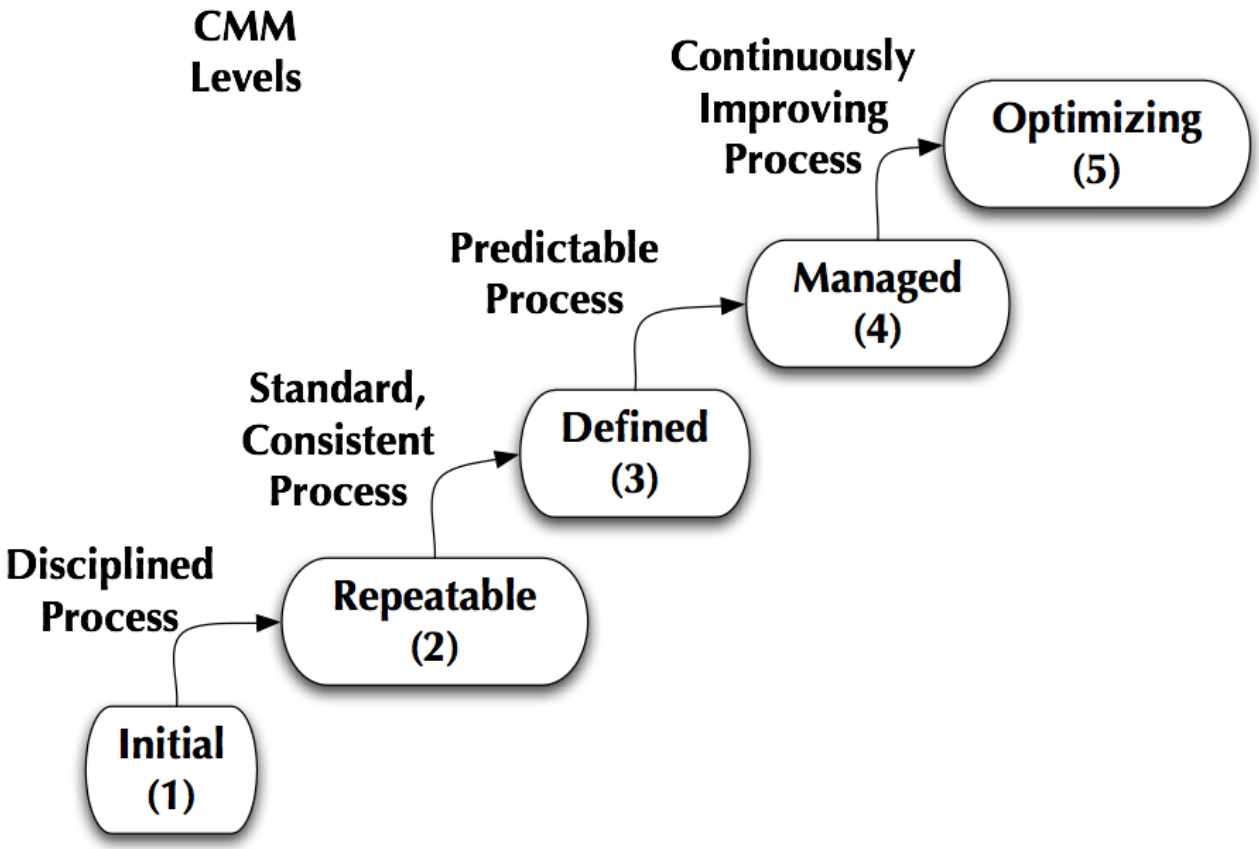
- Anything that will make a barrier fail can be described in an escalation factor (for example, server does not have a power).
- The logical next step to manage escalation factors is to create barriers for escalation factors (in this case it could be a backup generator).

Bow tie diagram

Practice

https://www.youtube.com/watch?v=P7Z6L7fjsi0

CMM


CMM
Levels
Continuously
Improving
Process
Optimizing
(5)
Predictable
Process
Managed
(4)
Standard,
Consistent
Process
Defined
(3)
Disciplined
Process
Repeatable
(2)
Initial
(1)

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