TALLINN UNIVERSITY OF TECHNOLOGY

# Information and Cyber Security Assurance in Organisations

**ITX8090**

# IV

# Lectures

- 05.09.2017 at 12.00-15.15 ICT 312
- 12.09.2017 at 12.00-15.15 self study
- 19.09.2017 at 12.00-15.15 ICT 312
- 26.09.2017 at 12.00-15.15 ICT 312
- 03.10.2017 at 12.00-15.15 self study
- 10.10.2017 at 12.00-15.15 ICT 312
- 17.10.2017 at 12.00-15.15 ICT 312
- 24.10.2017 at 12.00-15.15 ICT 312?
- 31.10.2017 at 12.00-15.15 ICT 312
- 07.11.2017 at 12.00-15.15 ICT 312
- 14.11.2017 at 12.00-15.15 self study
- 21.11.2017 at 12.00-15.15 ICT 312
- 28.11.2017 at 12.00-15.15 ICT 312
- 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?

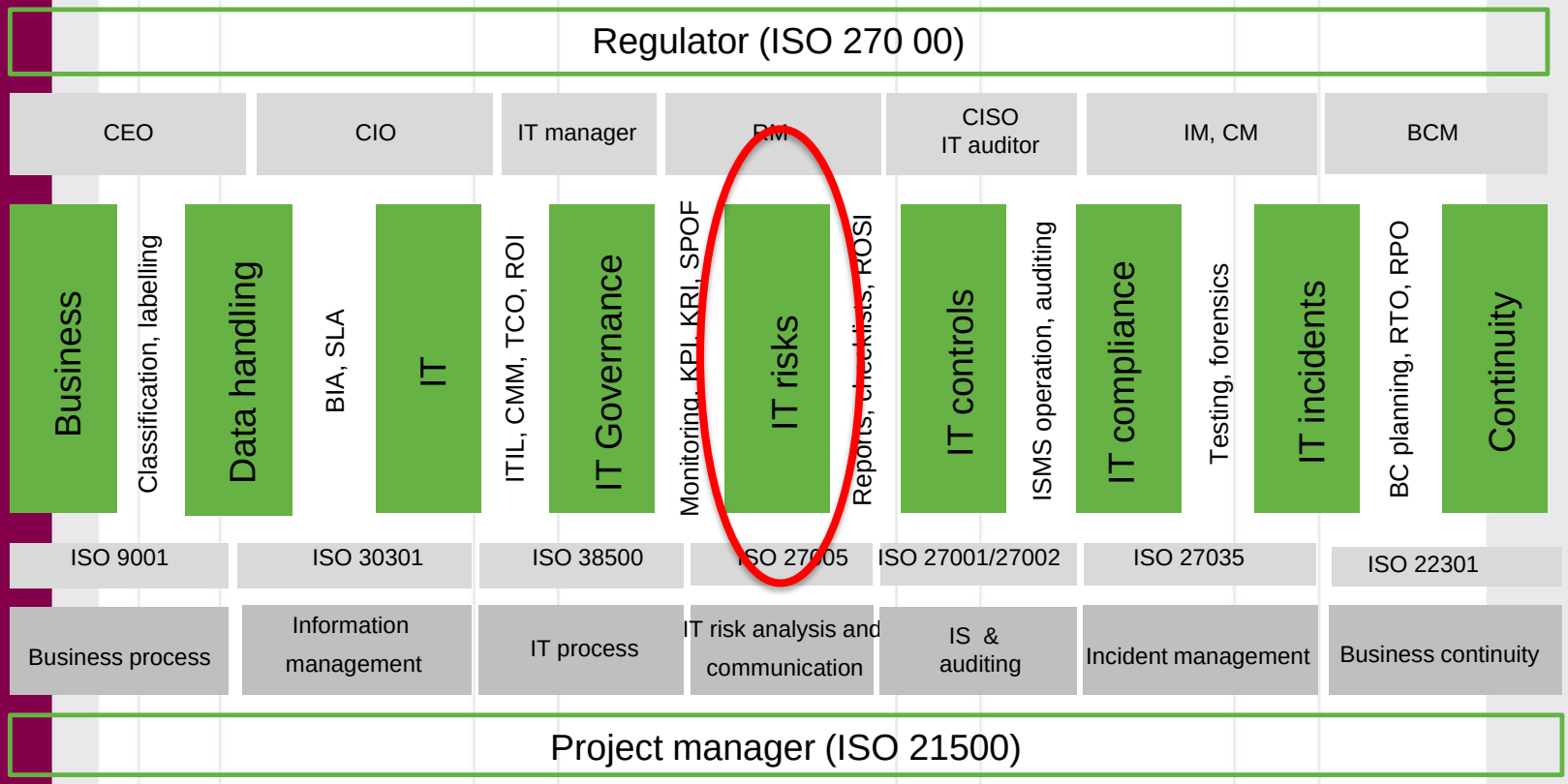
# Practical info

Updates in course page

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

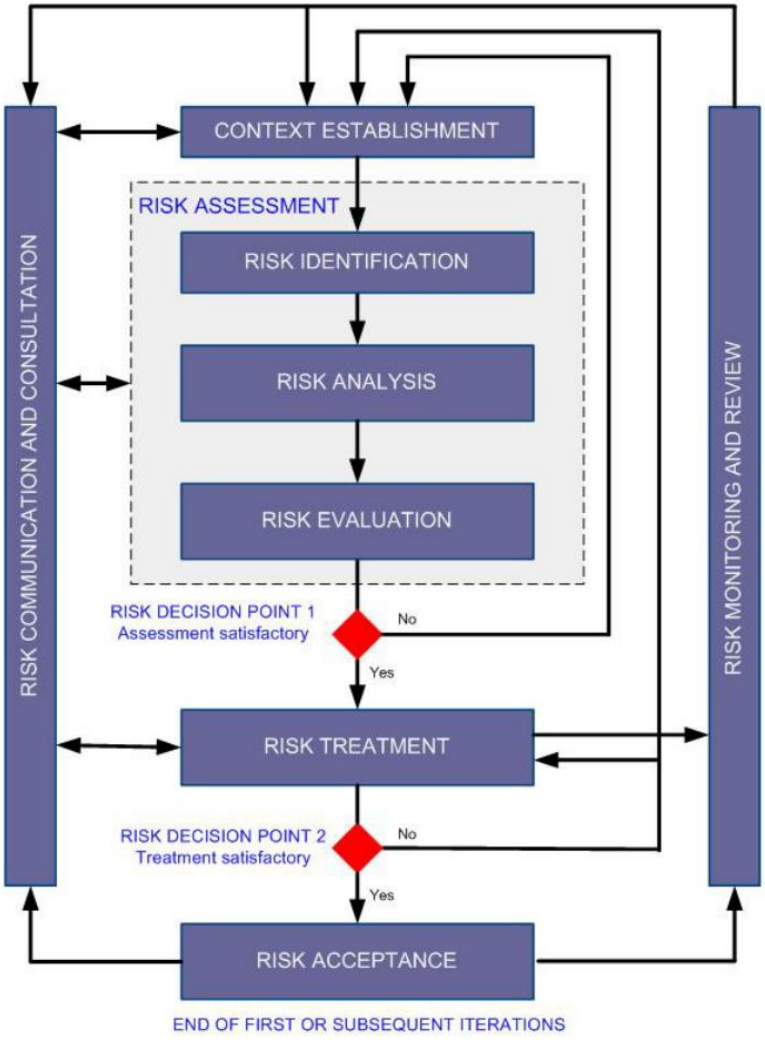
# IT risk and control concept

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




IT, risk, information security and business continuity management actions

# Process 27005



# Definitions (threat)

ISO 27005

A potential cause of an incident, that may result in harm of systems and organization

NIST

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

# Definitions (threat)

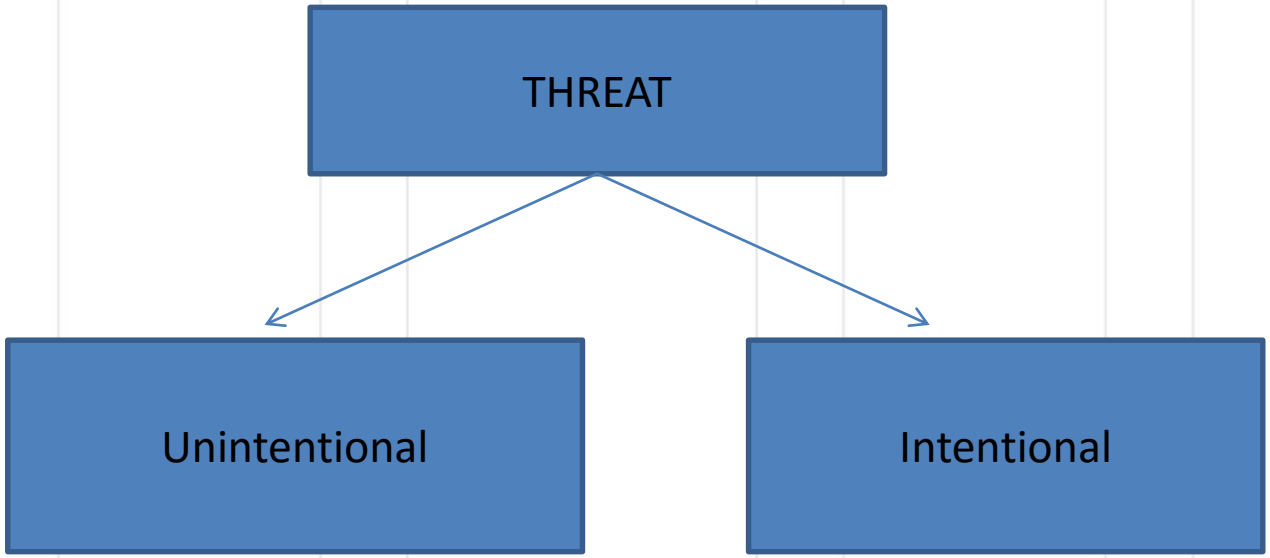
National Information Assurance Glossary

Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

ENISA gives a similar definition

Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

# Threats



# Threats

Unintentional (elemental)

- Environmental - lightning, flood, too low or high temperatures, fire and the like;
- Technical faults - a power failure, computer failure and the like;
- Human threats - errors, mistakes, illness, exits and the like;

One threat can lead to another, such as lightning - > computer failure, flood - > power failure.

# Threats

Intentional (attacks)

- Physical attacks;
- Misuse of resources;
- Resource blocking;
- Information fishing;
- Data forgery;
- Manipulation with systems;
- …

# Definitions (vulnerability)

ISO 27005

A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission

National Information Assurance Glossary

Vulnerability — Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited

# Definitions (vulnerability)

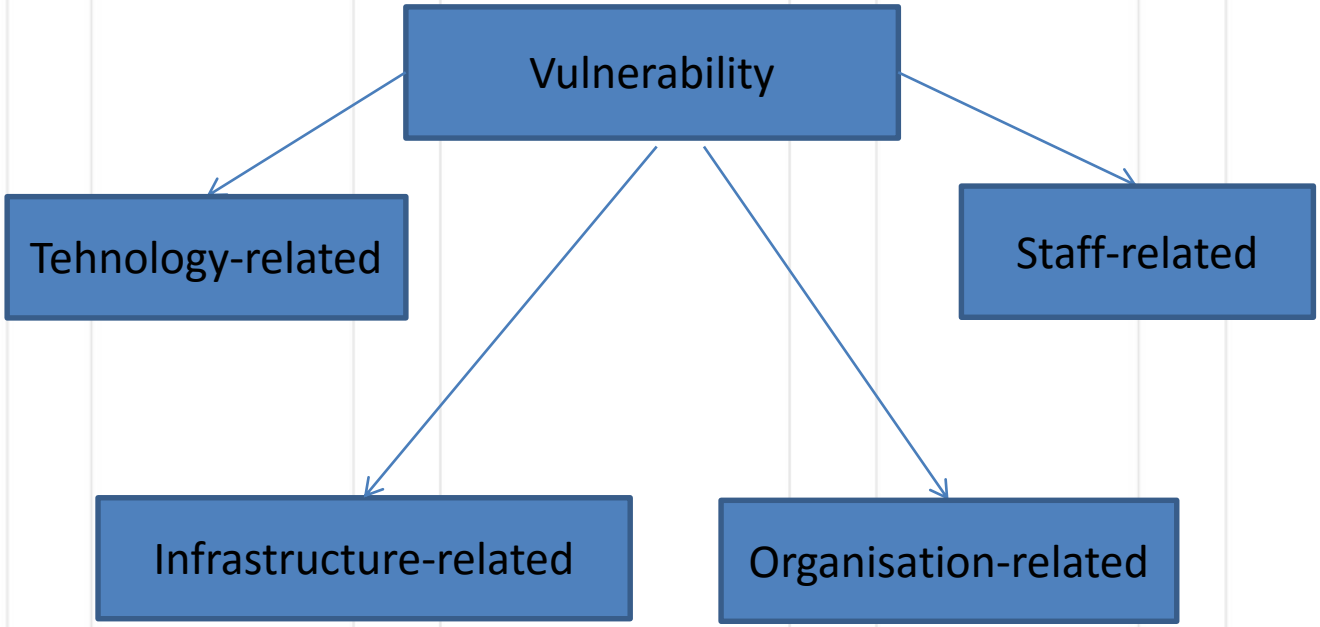
NIST

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

ENISA

The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

# Vulnerability



# Vulnerability

Technology-related

- Obsolete technology, „legacy“;
- Improper placement;
- Errors in programs, operating systems;
- Weaknesses in technology management;
- ...

# Vulnerability

Infrastructure-related

- Unfavorable location;
- Natural conditions;
- Decaying infrastructure;
- Communication system installation deficiencies;
- Malicious neighbor;
- ...

# Vulnerability

Staff-related

Lack of experience;

Excessive trust;

Incorrect procedures;

Ignorance and low motivation level;

Failure to comply with security requirements;

Self-interest;

...

# Vulnerability

Organisation-related

- Lack of security organisation;
- Shortcomings in the organisation of work;
- Resource management deficiencies;
- Documenting drawbacks;
- Deficiencies in selection of security measures;
- Deficiencies in control of security measures;
- ...

# Listing sources

Internal possibilities

- Predefined forms;
- Interviews;
- Questionnaires;
- Debates;
- Analysis of the documents;
- Observations;
- Incidents occurred;
- Audit reports.

External possibilities

- Standards;
- Statistics;
- How is the in other similar businesses?
- How is the country as a whole?
- How is Europe?
- What are the trends in the world?
- Agencies.

# Pairing (NIST)

**Table 3-2. Vulnerability/Threat Pairs**

| Vulnerability | Threat-Source | Threat Action |
|---|---|---|
| Terminated employees' system identifiers (ID) are not removed from the system | Terminated employees | Dialing into the company's network and accessing company proprietary data |
| Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server | Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists) | Using telnet to XYZ server and browsing system files with the *guest* ID |
| The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system | Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists) | Obtaining unauthorized access to sensitive system files based on known system vulnerabilities |

# Risk scenario

| Component | Description |
|---|---|
| Participant | Internal (employee, temporary employee)<br>External (competitor, external business partner, regulator, market operator) |
| Threat | Malicious<br>Accidental<br>Malfunction<br>Natural error<br>External requirement |
| Event | Disclosure<br>Disruption<br>Modification<br>Theft |

# Risk scenario

| Component | Description |
|---|---|
| Event | Destruction<br>Structure change<br>Ineffective Use<br>Regulations violation<br>Misuse |
| Information asset/IT asset | Organisation<br>Processes<br>Infrastructure<br>IT infrastructure<br>Information<br>Applications |
| Time | Time period<br>The critical/non- critical time<br>Detection speed |

# Advising questions

1. Asset - **what** should be protected?
2. Threat - **who** or **what** uses the advantage of the weakness?
3. Weakness - **why** is asset vulnerable?
4. Risk - **what** may happen if weakness exploited and **how** likely is it?

# 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.

# Practice

## Creating risk register

# 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
- What triggers the need for a risk assessment?
- 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

# 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

**Filling risk register**

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