



TALLINN UNIVERSITY OF
TECHNOLOGY



Information and Cyber Security Assurance in Organisations

ITX8090

II



Formal issues

Everyone:

please send e-mail to

Andro.Kull@ttu.ee

with subject ITX 8090



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

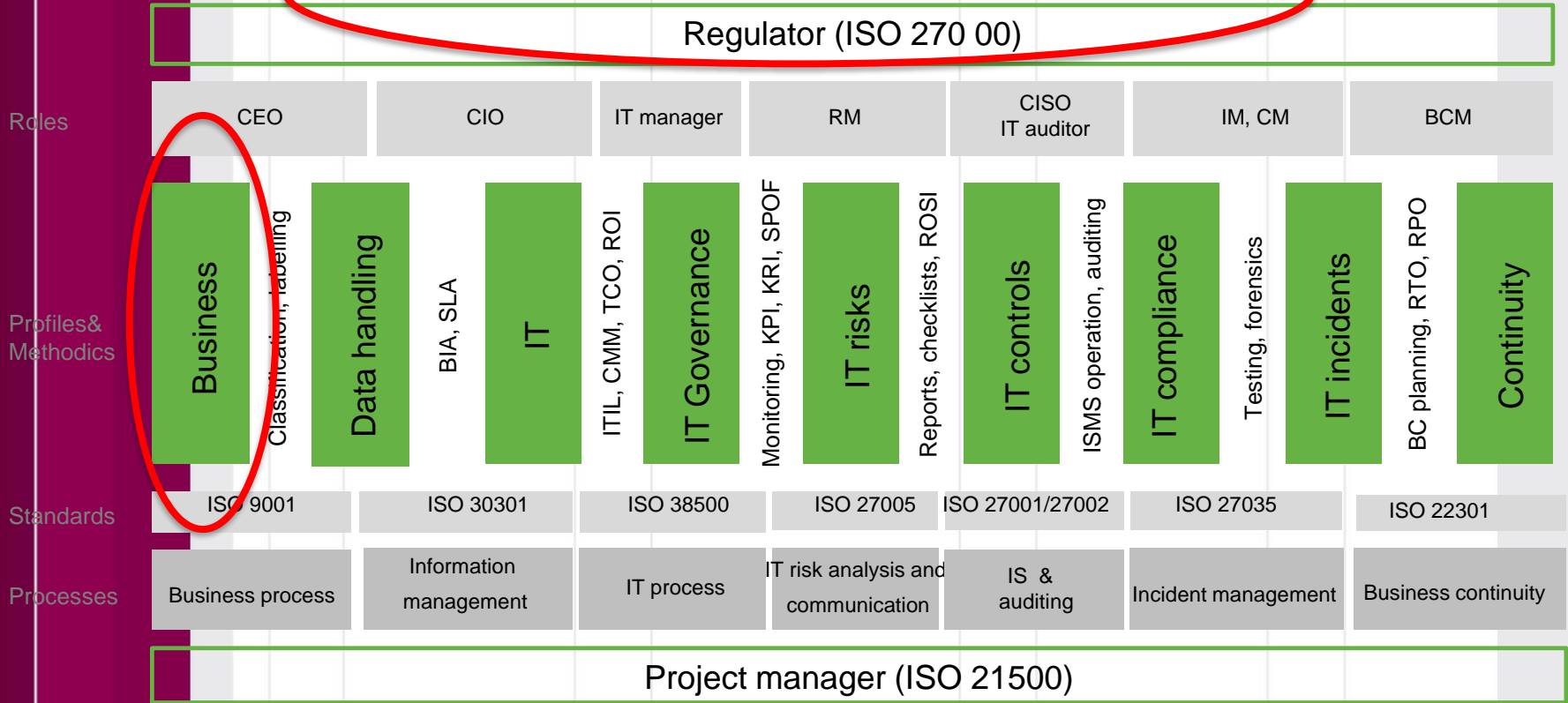
Updates in course page

<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



Requirements by law

[Link](#)



Requirements by regulators

[Link](#)



Requirements by new regulation

[Link](#)



Information security goals for business

Direct monetary loss

Loss of reputation -> monetary loss

Breach of law

-> loss of reputation -> monetary loss

-> penalties -> monetary loss

Violation of work -> additional work -> monetary loss

Interruption of core business

-> loss of income -> monetary loss

-> breach of contract -> monetary loss



Business objective example

The primary objective of Eesti Pank is to contribute to **price stability** within the euro area. A stable price level is maintained with the help of the single monetary policy, which is formulated by all the Eurosystem members, including Eesti Pank. The latter is also responsible for the implementation of the euro area single monetary policy in Estonia.

Eesti Pank





Business mission example

The mission of Tallinn University of Technology is to be a promoter of **science, technology** and **innovation** and a leading provider of engineering and economic **education** in Estonia.



TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY



Understand the business

Business process modeling (BPM) in systems engineering is the activity of representing processes of an enterprise, so that the current process may be analyzed or improved. BPM is typically performed by business analysts, who provide expertise in the modeling discipline; by subject matter experts, who have specialized knowledge of the processes being modeled; or more commonly by a team comprising both.

www.wikipedia.org



BPM processes

- **Management** processes: corporate governance and strategic management.
- **Operational** processes: purchasing, manufacturing, marketing, and sales.
- **Supporting** processes: IT, HR, bookkeeping.



BPM tools

Pen and paper;

LucidChart;

MS Word;

MS Visio;

Aris

...



Practice

[Simple diagram example](#)



Definitions

Information assets – information with value;

Threats – something that can harm information assets;

Weaknesses – a feature which lets the threats materialize;

Risks – the probability that threat takes advantage of the weakness and causes damage to information assets

Residual risk – the risk that remains after the application of controls;

Measures – actions to mitigate risk (acceptable level, risk appetite).



Information assets

Information assets - information, data, business secrecy, organization knowledge;

Specifications of the data in digital form:

- physical dimensions,
- simplicity of copying;
- transmission speed;
- access over the network.



Information assets valuation

- **Availability** - Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.
- **Integrity** - Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
- **Confidentiality** – Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

SANS (<http://www.sans.org/security-resources/glossary-of-terms/>)



Information assets valuation

- **Authenticity** - is the validity and conformance of the original information.
- **Non-repudiation** - is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

SANS

(<http://www.sans.org/security-resources/glossary-of-terms/>)



Information assets valuation

- **Accountability** - the state of being answerable for the actions and decisions that have been assigned.
(<http://www.praxiom.com/iso-27000-definitions.htm>)
- **Reliability** - the ability of a system to consistently perform its intended or required function or mission, on demand and without degradation or failure.
(<http://www.businessdictionary.com/>)
- **Privacy** - the state of being concealed; secrecy (<http://dictionary.reference.com/>)



Data modelling

Is a process used to define and analyze data requirements needed to support the business processes within the scope of corresponding information systems in organizations.



IT assets

Applications

Servers

Databases

PS's, laptops, smartphones

Development systems

Web server, e-mail server

Firewalls

Operating systems

Routers and switches

Testing systems

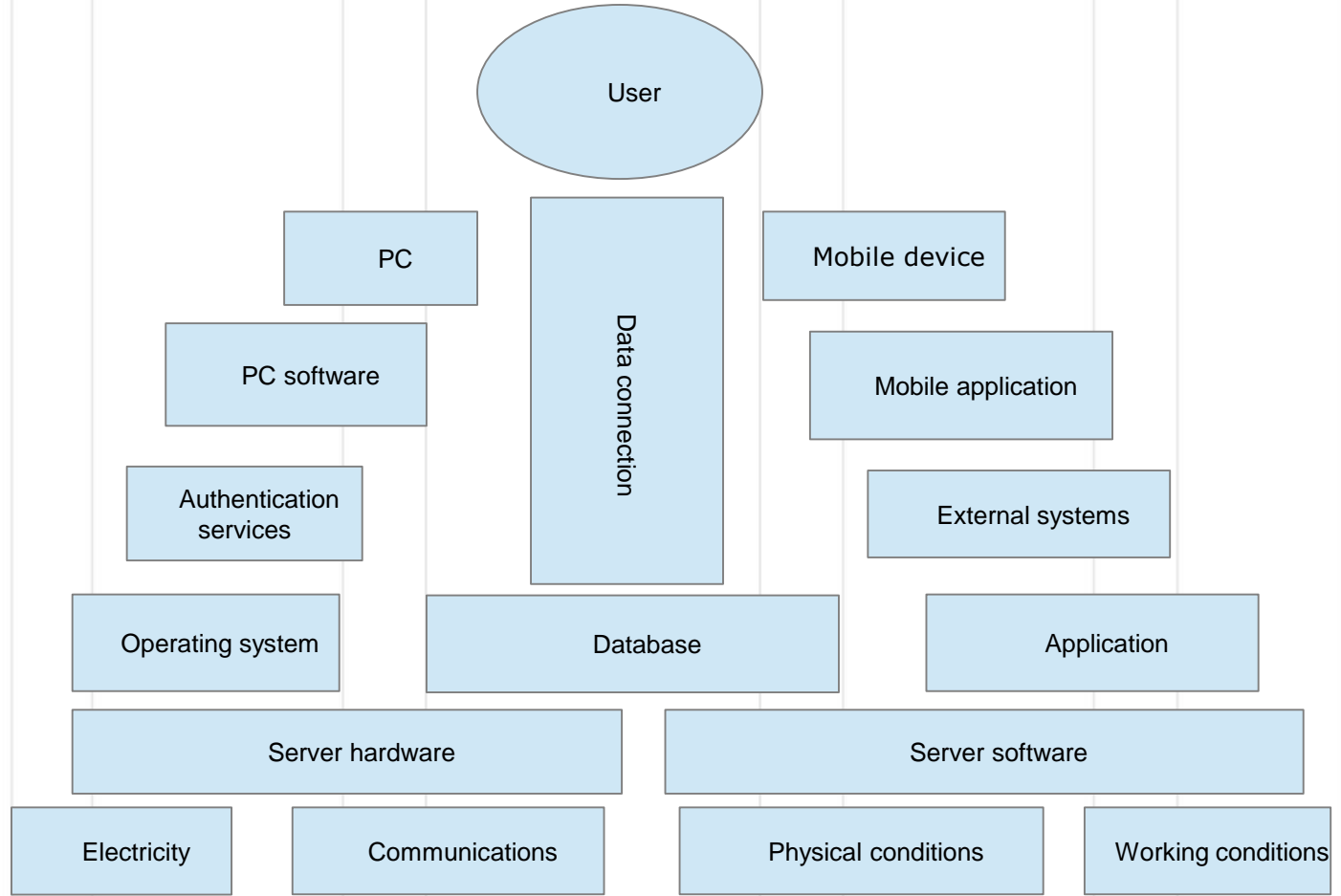
Third party systems

Wired and wireless networks

...



Information system





ITAM

IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.



Practice

[Worksheet](#)



Criticality assessment

Business critical IT solutions – solutions critical to run business process, i.e. production, cash system, etc.

Supporting IT solutions – solutions needed for some functions, i.e. bookkeeping, etc.

Necessary IT solutions – i.e. company home page for contacts, etc.



Dependency assessment

Critical activity dependency on IT solutions (easy scale):

1. Critical dependency;
2. Important dependency, but there exist alternative way to run critical activity;
3. Weak dependency.



BIA

Business Impact Analysis

- IT risk realization has some impact to business process;
- BIA enables us to prioritize IT risks;
- Great IT risks which cause business disruptions is a case of business continuity planning.



Practice

[BIA template](#)

PhD Andro Kull
CISA, CISM, CRISC, ABCP
ISO 27001 Master, CCSM
E-mail: Andro.Kull@ttu.ee
Skype: andro.kull
Phone: +372 5093296

