TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

II

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

IT risk and control concept

Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.

Business profile
- Critical business processes
- Critical information assets

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 …)

Information security goals

Direct monetary loss

Loss of reputation -> monetary loss

Breach of law

-> loss of reputation -> monetary loss

-> penalties -> monetary loss

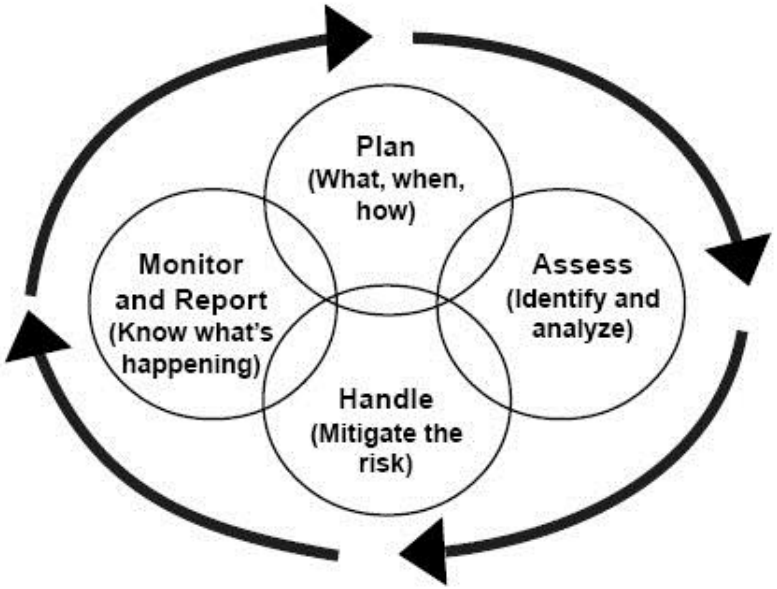
Violation of work -> additional work -> monetary loss

Interruption of core business

-> loss of income -> monetary loss

-> breach of contract -> monetary loss

Process



A Continuous Interlocked Process—Not an Event

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 taks advantage of the weakness and causes damage to information assets

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

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

Homework I description

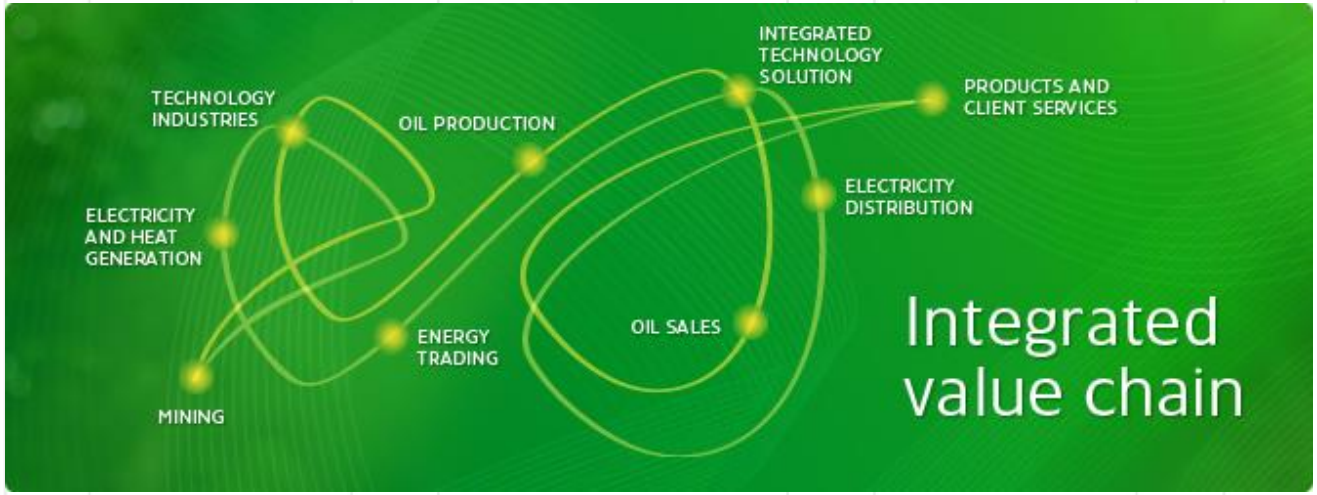
Link

BPM

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

Business process example



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.

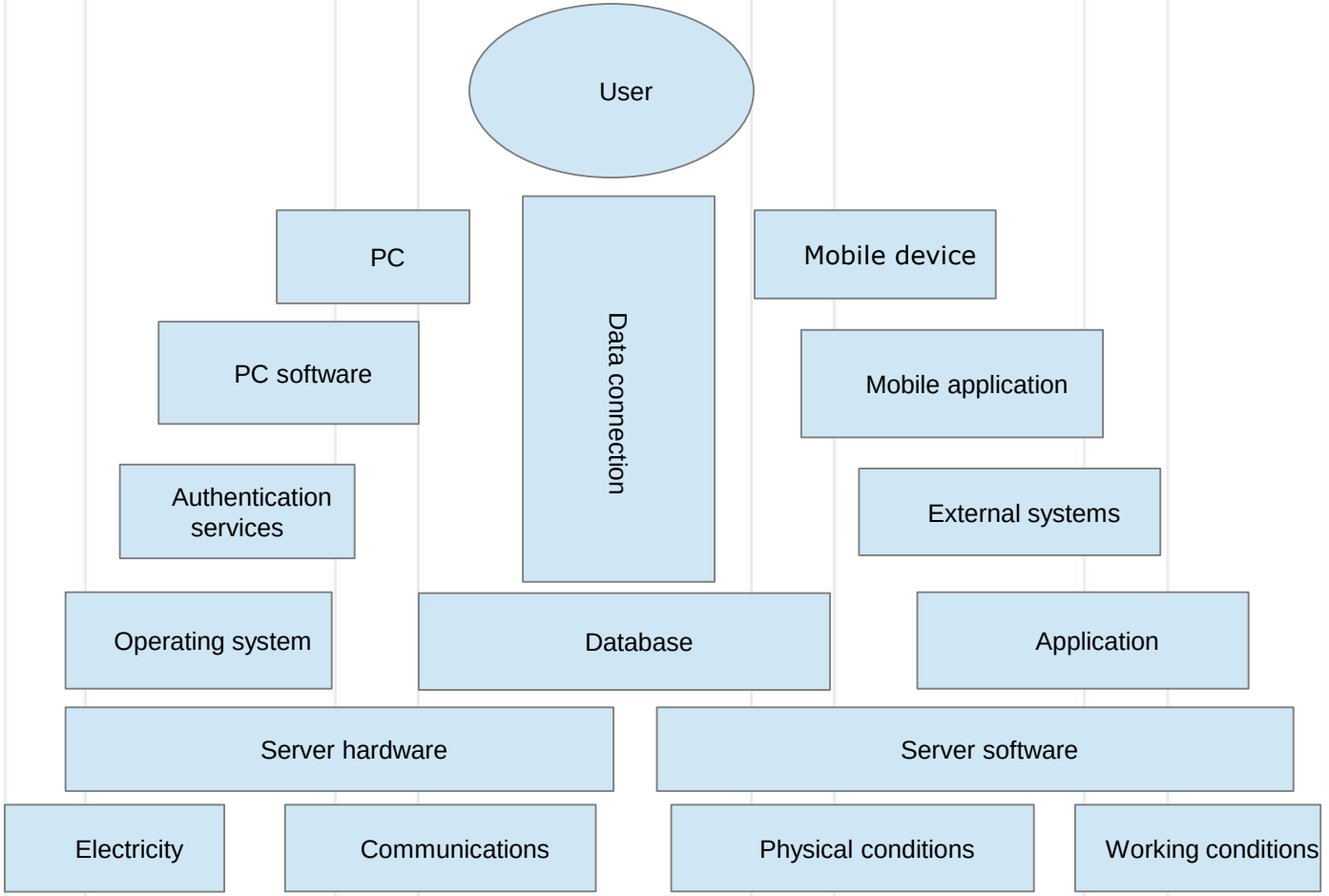
BPM and data modelling

Simple example

IT assets

Applications
Servers
Databases
PS’s, laptops, smartphones
Development systems
Web server, e-mail server
Firewalls
Operating systems
Routers and swiches
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.

Criticality assessment

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

Supporting IT solutions – solutions neede 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

Business process modelling (BPM)
Information assets
IT assets
Business Impact Analysis (BIA)

Exercise 2 reading 1
Exercise 2 reading 2

Exercise 2 worksheet 1
Exercise 2 worksheet 2

PhD Andro Kull
CISA, CISM, CRISC, ABCP
Andro@consultit.ee
andro.kull