TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

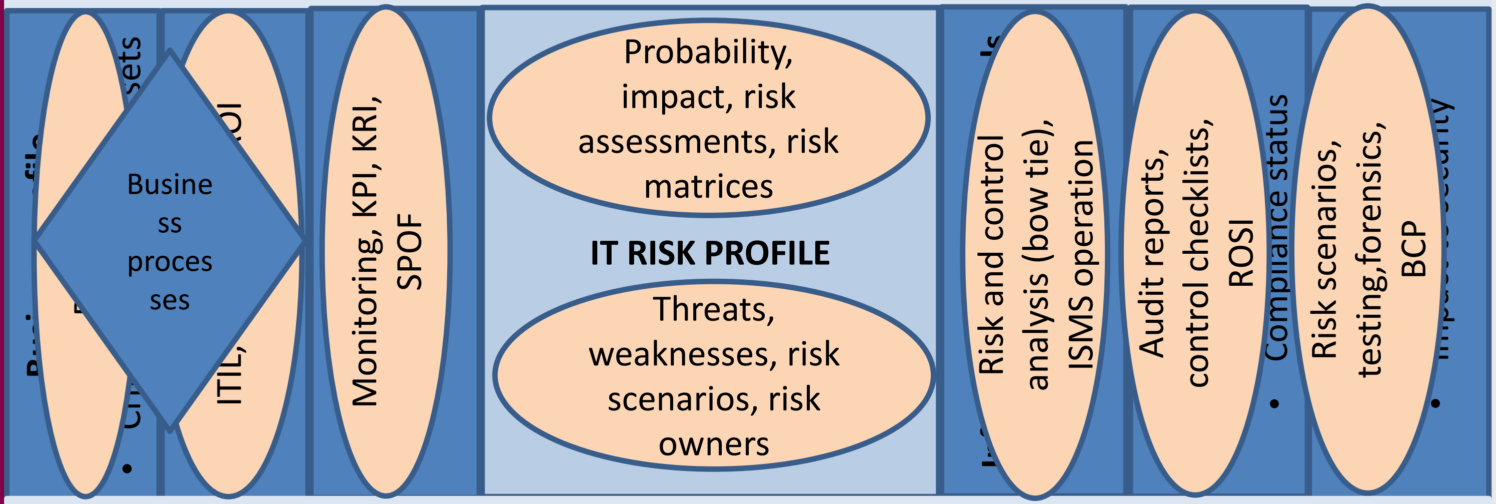
II

Formal issues

Everyone: please send e-mail to Andro.Kull@ttu.ee with subject ITX 8090

Concept developments

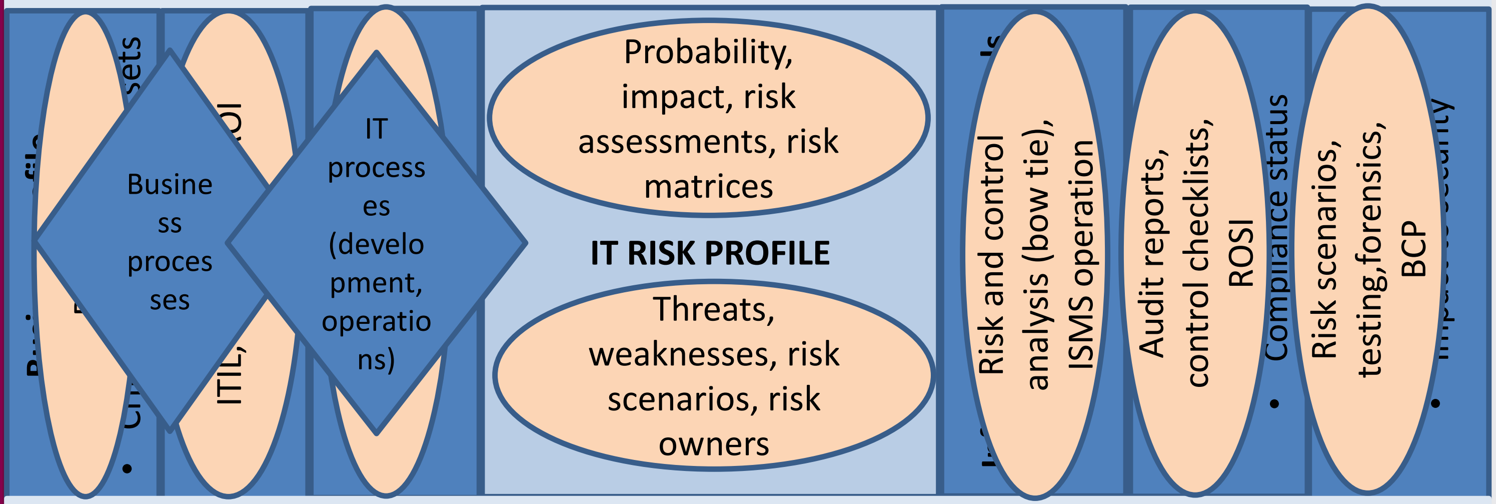
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.


sets
Busine
ss
proces
ses
ITIL,
Monitoring, KPI, KRI, SPOF
Probability, impact, risk assessments, risk matrices
IT RISK PROFILE
Threats, weaknesses, risk scenarios, risk owners
Risk and control analysis (bow tie), ISMS operation
Audit reports, control checklists, ROSI
• Compliance status
Risk scenarios, testing,forensics, BCP

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 …)

Concept developments

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



Busine
ss
proces
ses

IT
process
es
(develo
pment,
operatio
ns)

Probability, impact, risk assessments, risk matrices

IT RISK PROFILE

Threats, weaknesses, risk scenarios, risk owners

Risk and control analysis (bow tie), ISMS operation

Audit reports, control checklists, ROSI

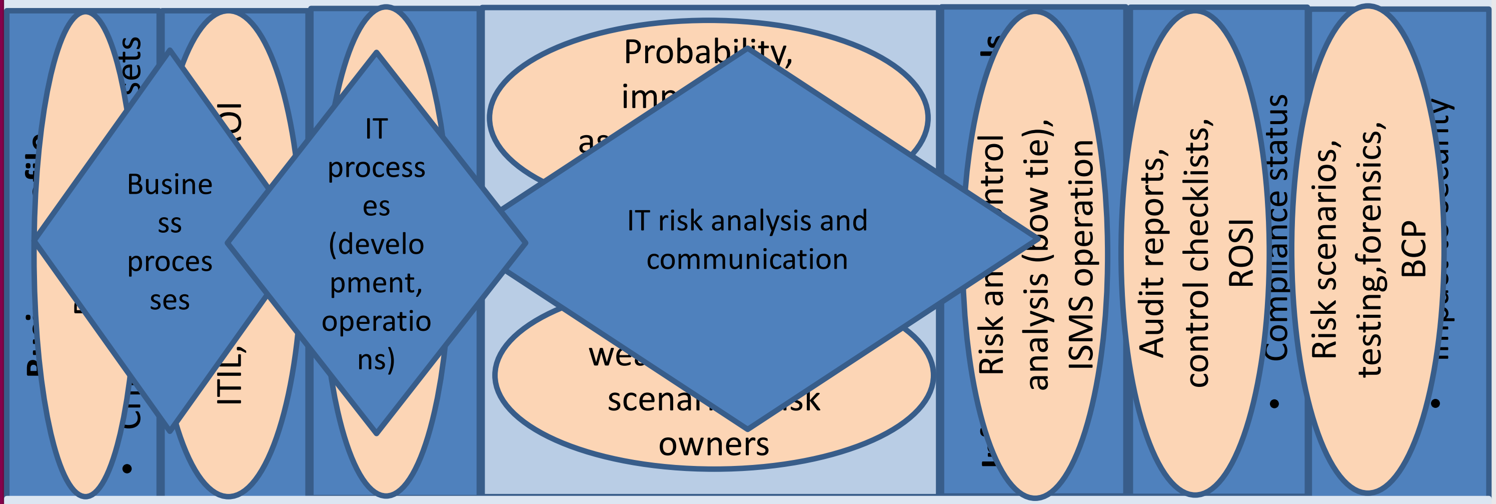
- Compliance status

Risk scenarios, testing,forensics, BCP

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 …)

Concept developments

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



Busine ss proces ses

ITIL,

IT process es (develo pment, operatio ns)

Probability,

IT risk analysis and communication

owners

Risk an ntrol analysis (bow tie), ISMS operation

Audit reports, control checklists, ROSI

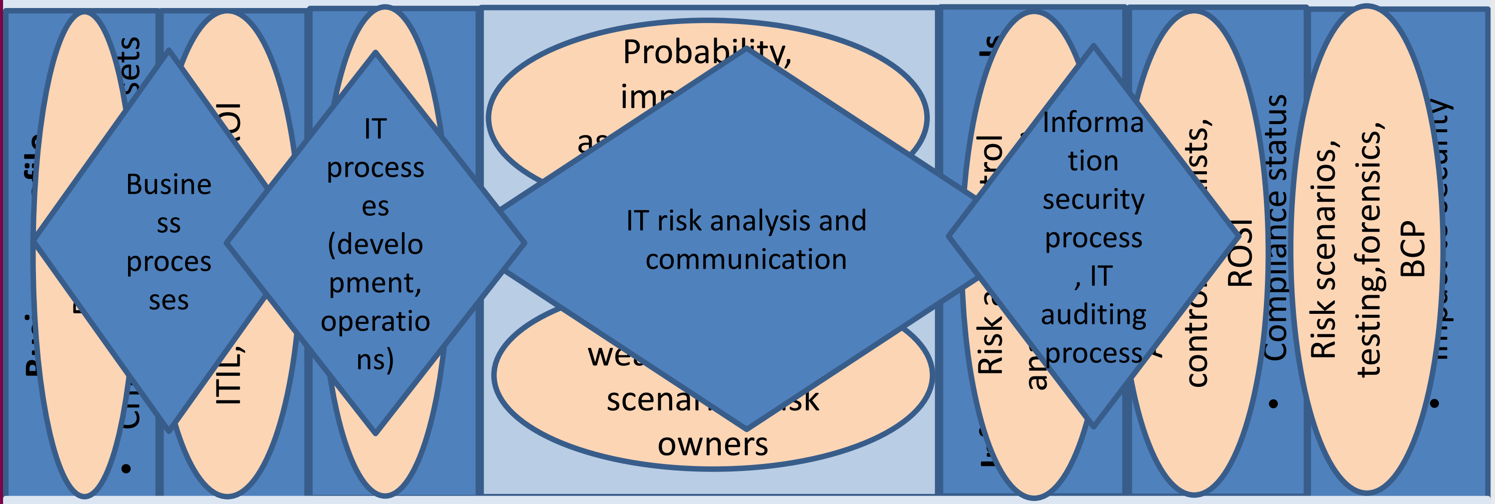
- Compliance status

Risk scenarios, testing,forensics, BCP

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 …)

Concept developments

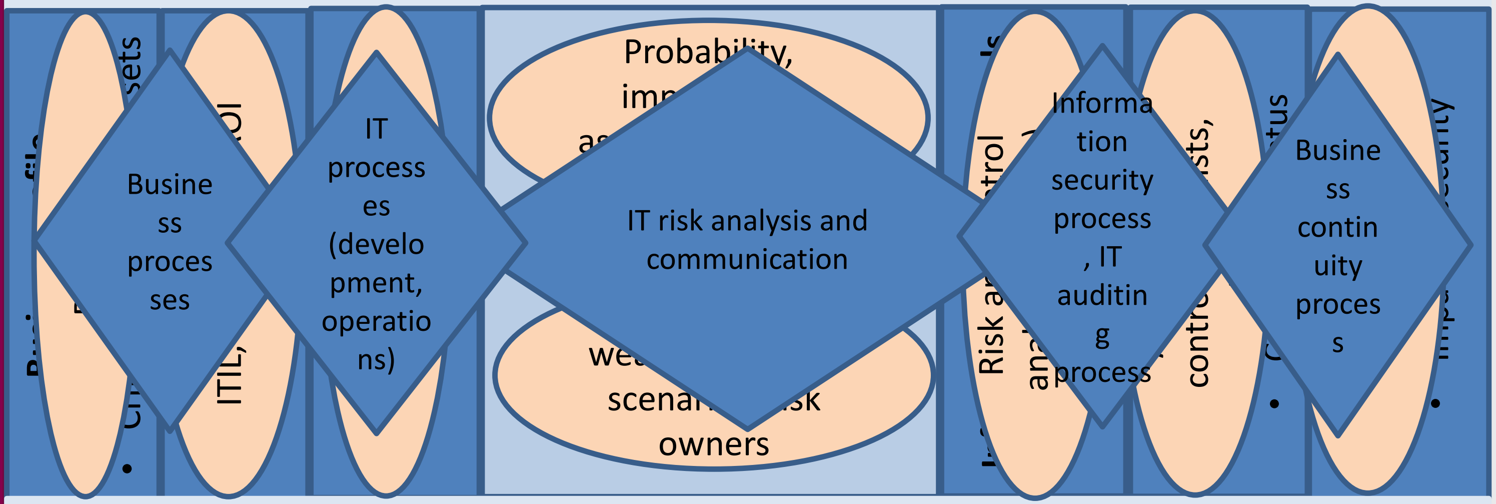
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.


Business processes
IT processes (development, operations)
Probability,
IT risk analysis and communication
owners
Information security process, IT auditing process
ITIL,
ROSI
Compliance status
Risk scenarios, testing,forensics, BCP

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 …)

Concept developments

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



Business processes

IT processes (development, operations)

IT risk analysis and communication

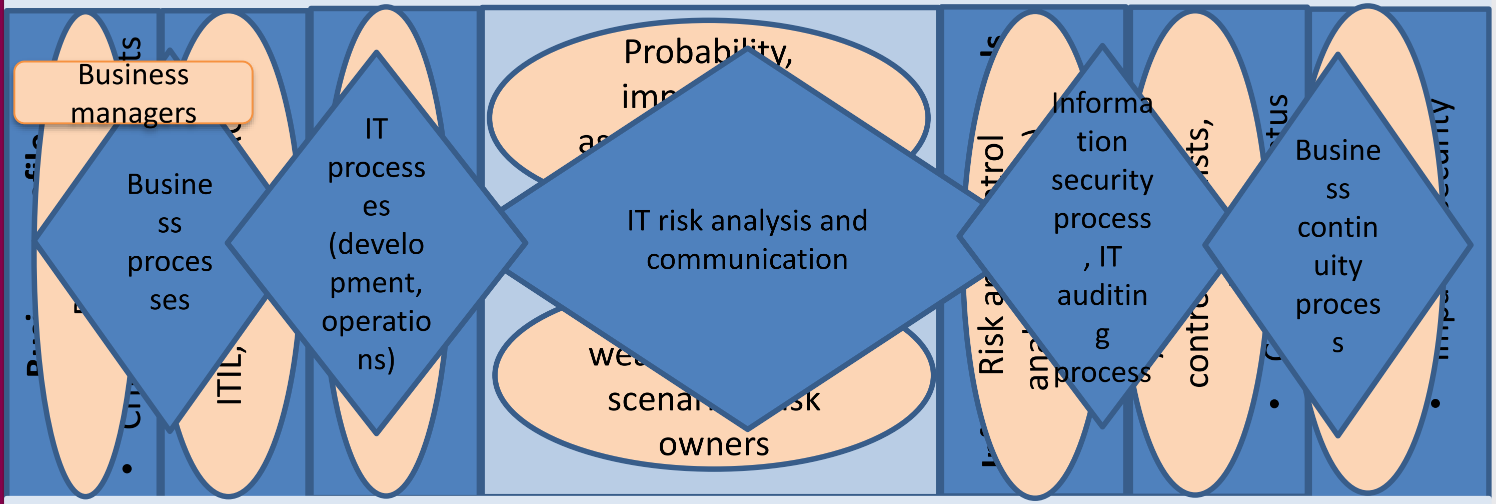
Information security process, IT auditing process

Business continuity process

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 …)

Concept developments

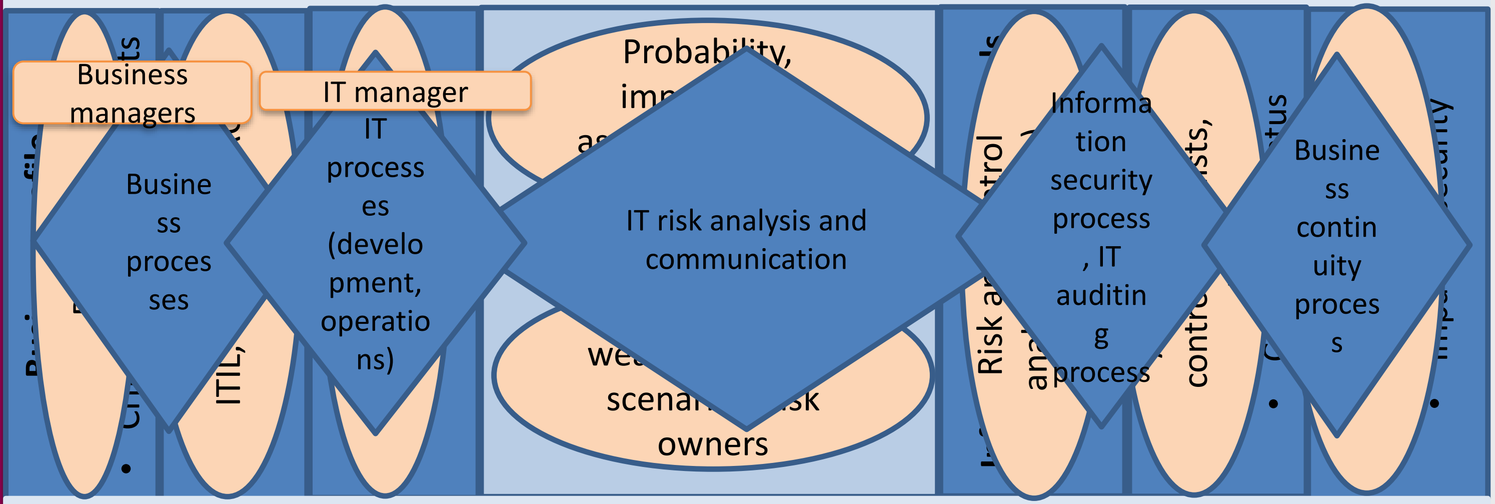
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.


Business managers
Business processes
IT processes (development, operations)
Probability,
IT risk analysis and communication
owners
Information security process, IT auditing process
Business continuity process
ITIL,
Risk a
conto

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 …)

Concept developments

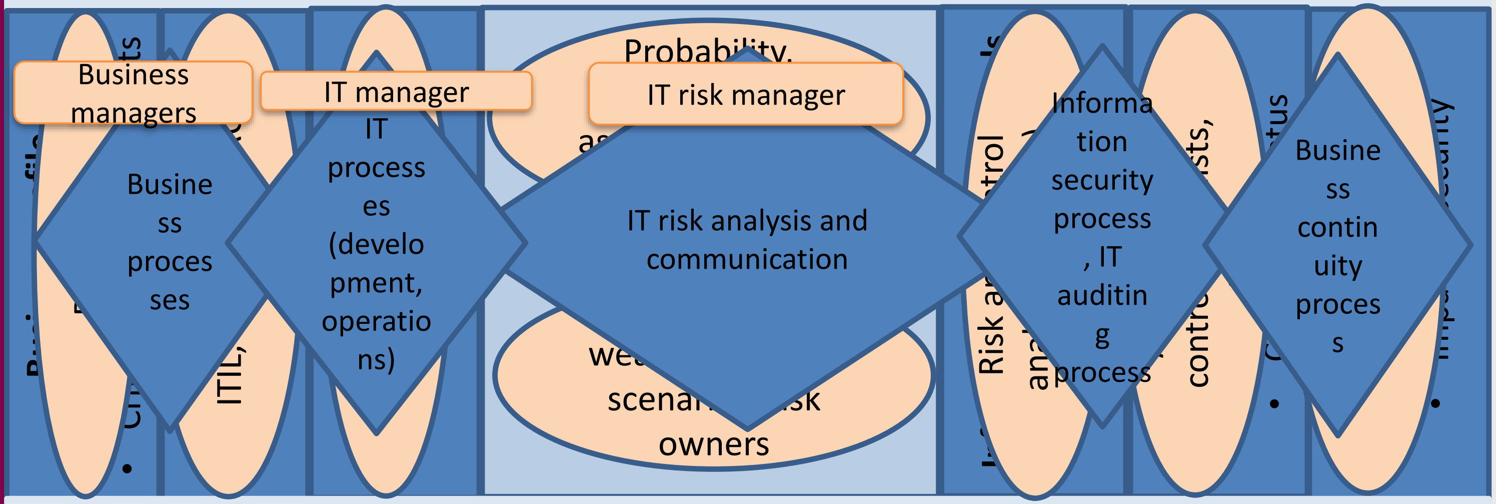
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.


Business managers
IT manager
Busine ss proces ses
IT process es (develo pment, operatio ns)
ITIL,
Probability,
IT risk analysis and communication
scenar
owners
Risk a
Informa tion security process , IT auditin g process
contro
Busine ss contin uity proces s

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 …)

Concept developments

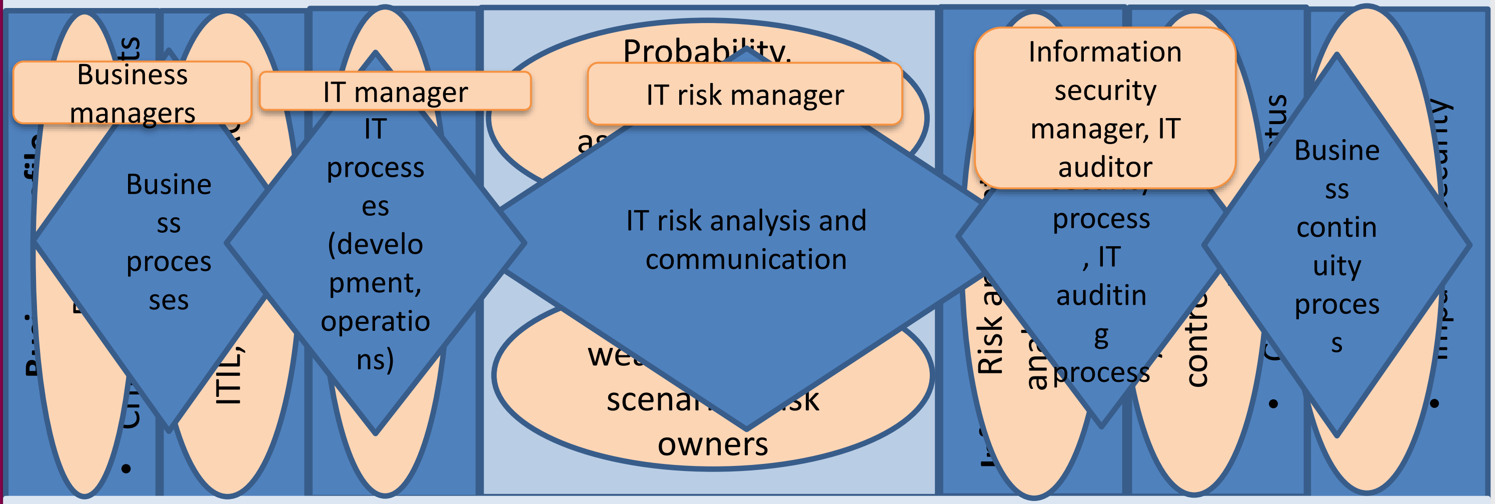
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.


Business managers
IT manager
IT risk manager
Business processes
IT processes (developments, operations)
IT risk analysis and communication
Information security process, IT auditing process
Business continuity process
Probability,
scenar
sk
owners
ITIL,
Risk a
ntrol
contro
sts,
tus

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 …)

Concept developments

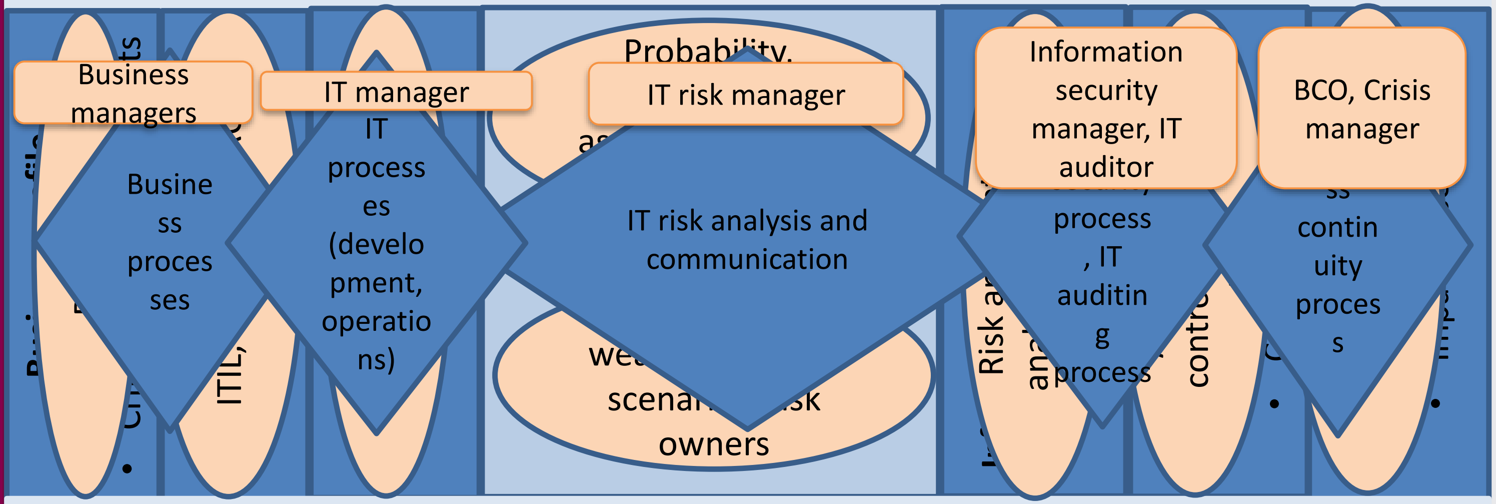
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.


Business managers
Business processes
IT manager
IT processes (developments, operations)
IT risk manager
Probability,
IT risk analysis and communication
owners
Information security manager, IT auditor
process, IT auditing process
Risk an
Business continuity process
ITIL,
contro

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 …)

Concept developments

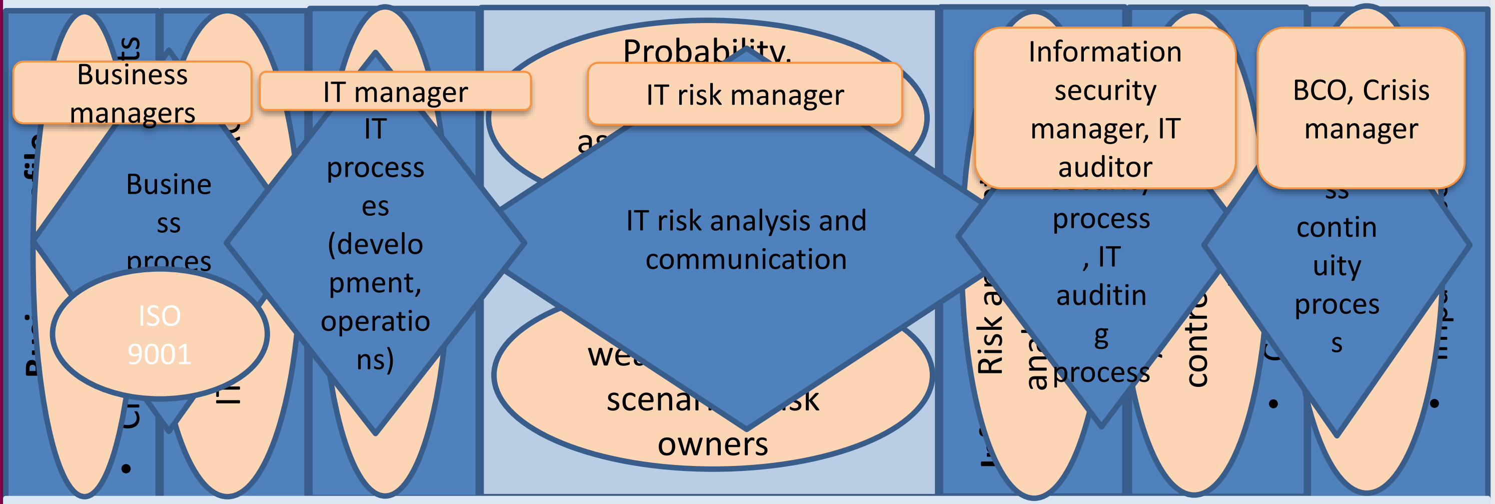
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.


Business managers
Business processes
ITIL,
IT manager
IT processes (development, operations)
Probability,
IT risk manager
IT risk analysis and communication
owners
Information security manager, IT auditor
process, IT auditing process
Risk a
BCO, Crisis manager
continuity process

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 …)

Concept developments

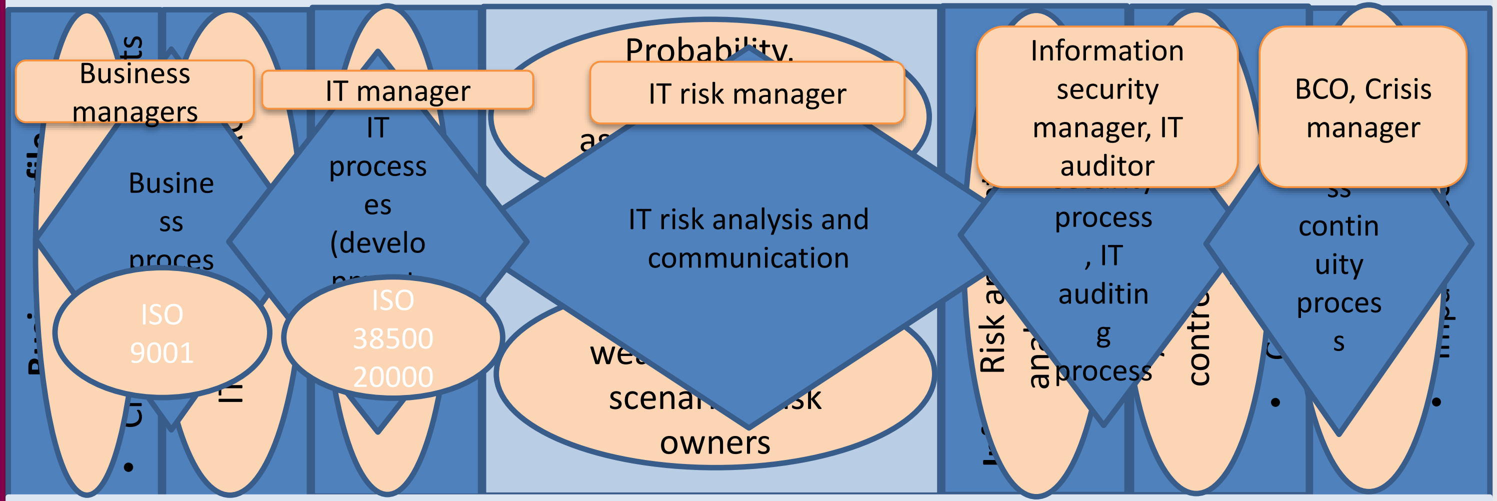
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.



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 …)

Concept developments

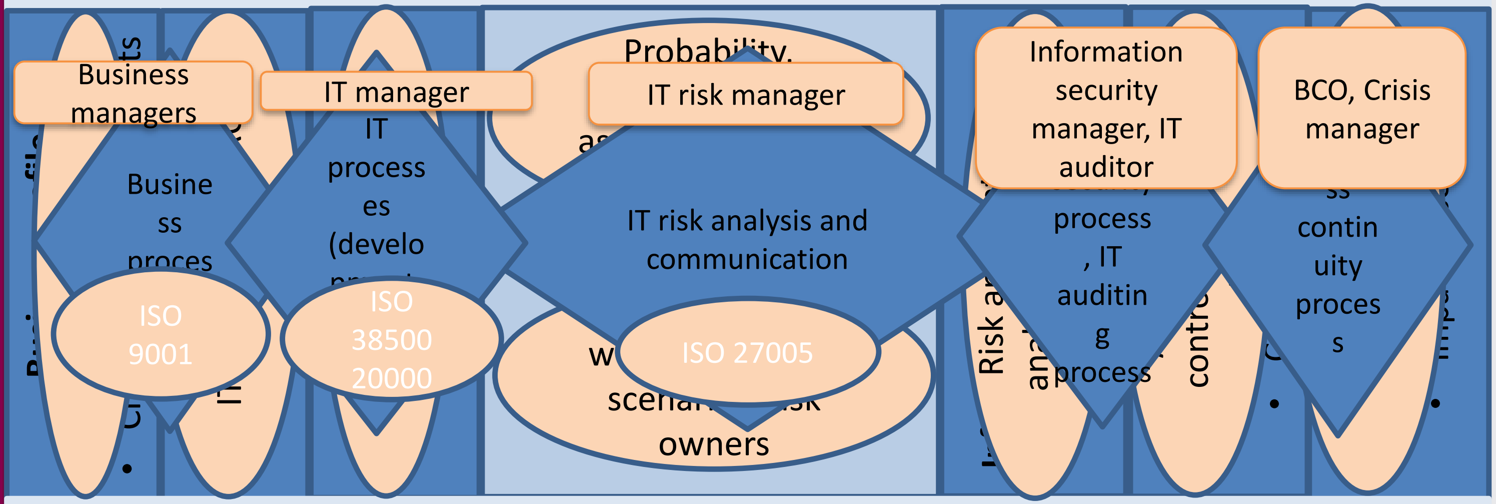
Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.



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 …)

Concept developments

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



Business managers

Busine ss proces

ISO 9001

IT manager

IT process es (develo

ISO 38500 20000

Probability,

IT risk manager

IT risk analysis and communication

ISO 27005

owners

Information security manager, IT auditor

process , IT auditin g process

Risk a

contro

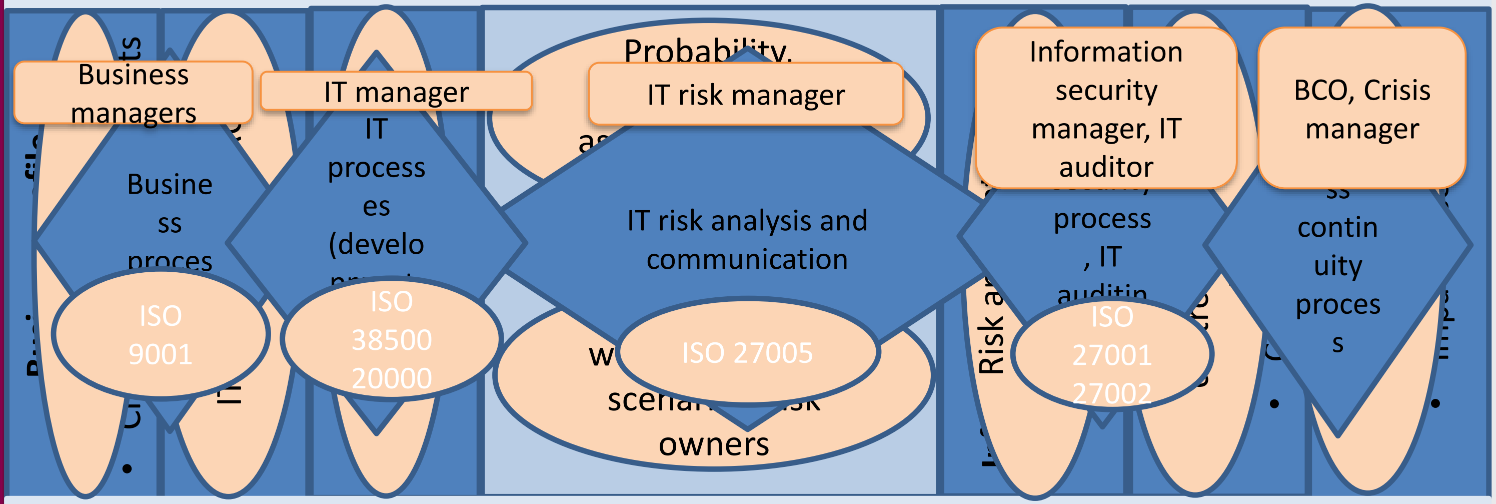
BCO, Crisis manager

ss contin uity proces s

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 …)

Concept developments

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



Business managers

Business process

ISO 9001

IT manager

IT processes (develo

ISO 38500 20000

Probability,

IT risk manager

IT risk analysis and communication

ISO 27005

owners

Information security manager, IT auditor

process , IT auditin

ISO 27001 27002

Risk a

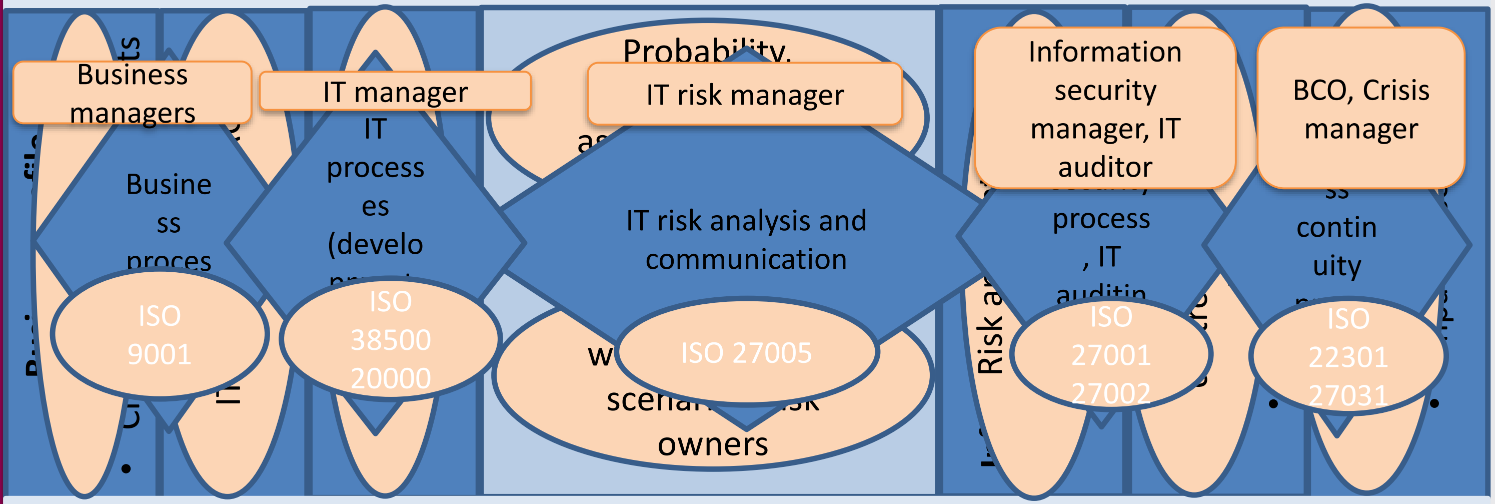
BCO, Crisis manager

continuity process

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 …)

Concept developments

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

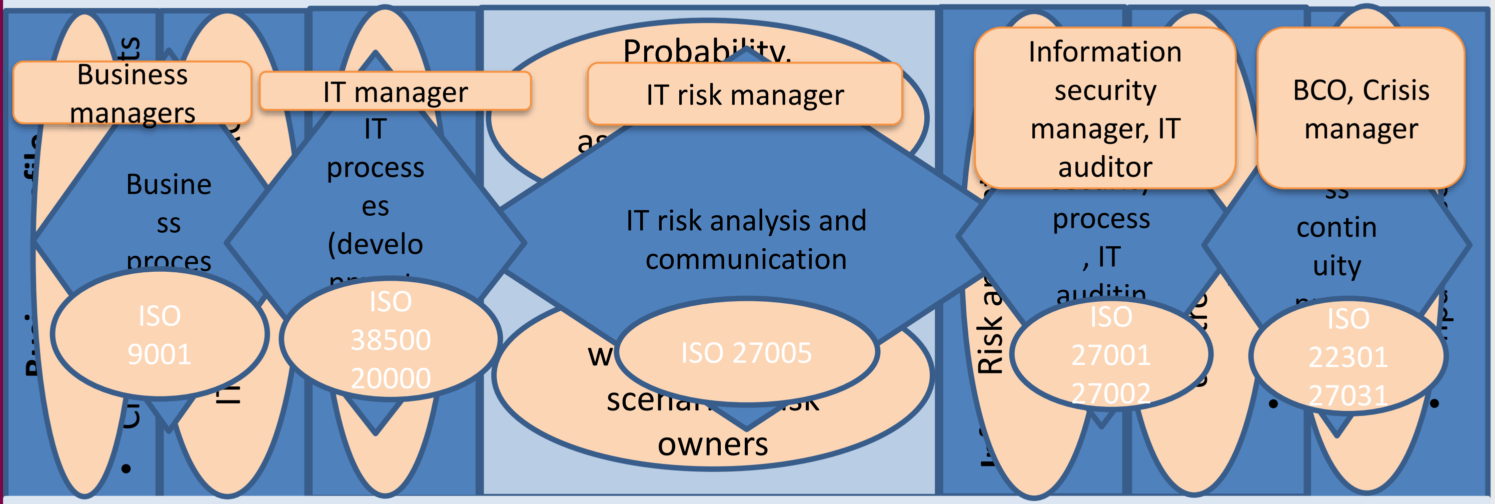


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc …)

Concept developments

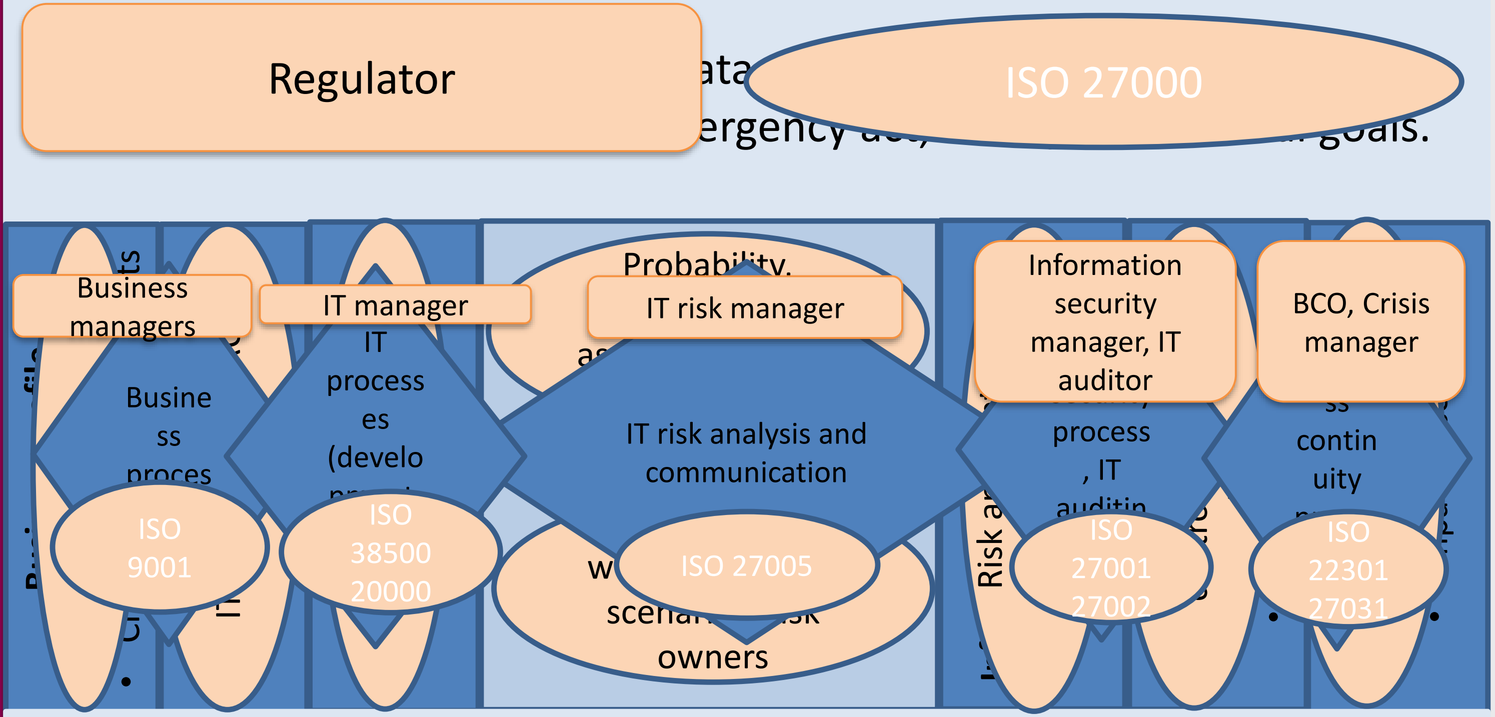
Regulator

ata protection, business continuity (for ergency act, etc …) and internal goals.



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 …)

Concept developments



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 …)

Concept developments

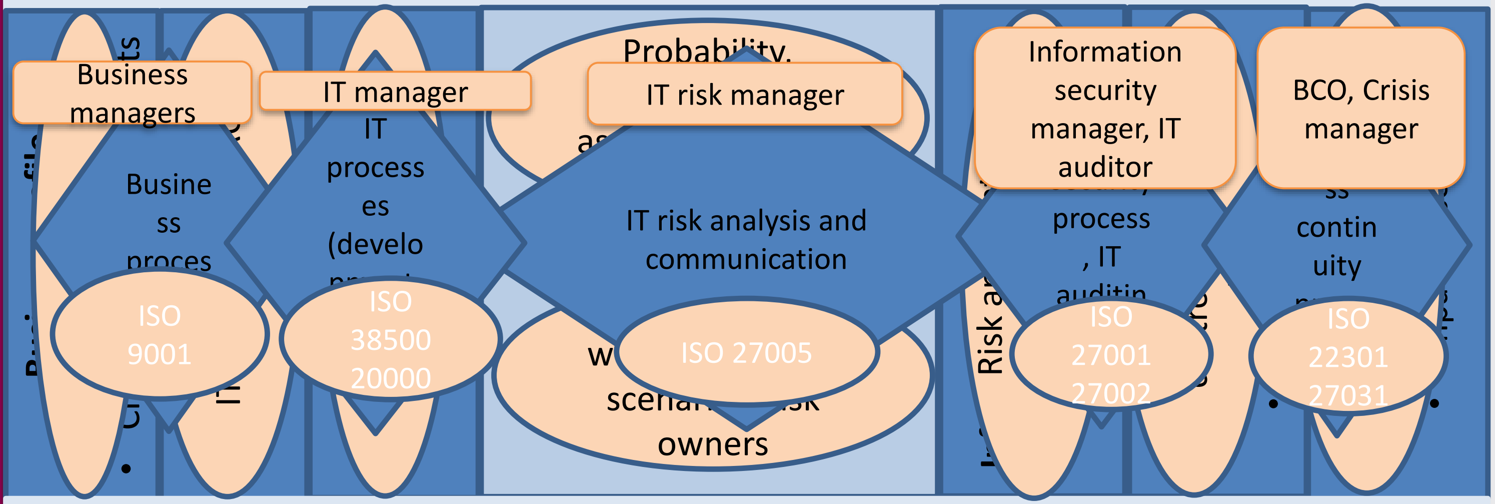
Regulator

ISO 27000

ata

ergency act,

goals.



Business managers

Busine ss proces

ISO 9001

IT manager

IT process es (develo

ISO 38500 20000

Probability,

IT risk manager

IT risk analysis and communication

ISO 27005

w

scenar

owners

Information security manager, IT auditor

process , IT auditin

ISO 27001 27002

Risk ar

BCO, Crisis manager

ss contin uity

ISO 22301 27031

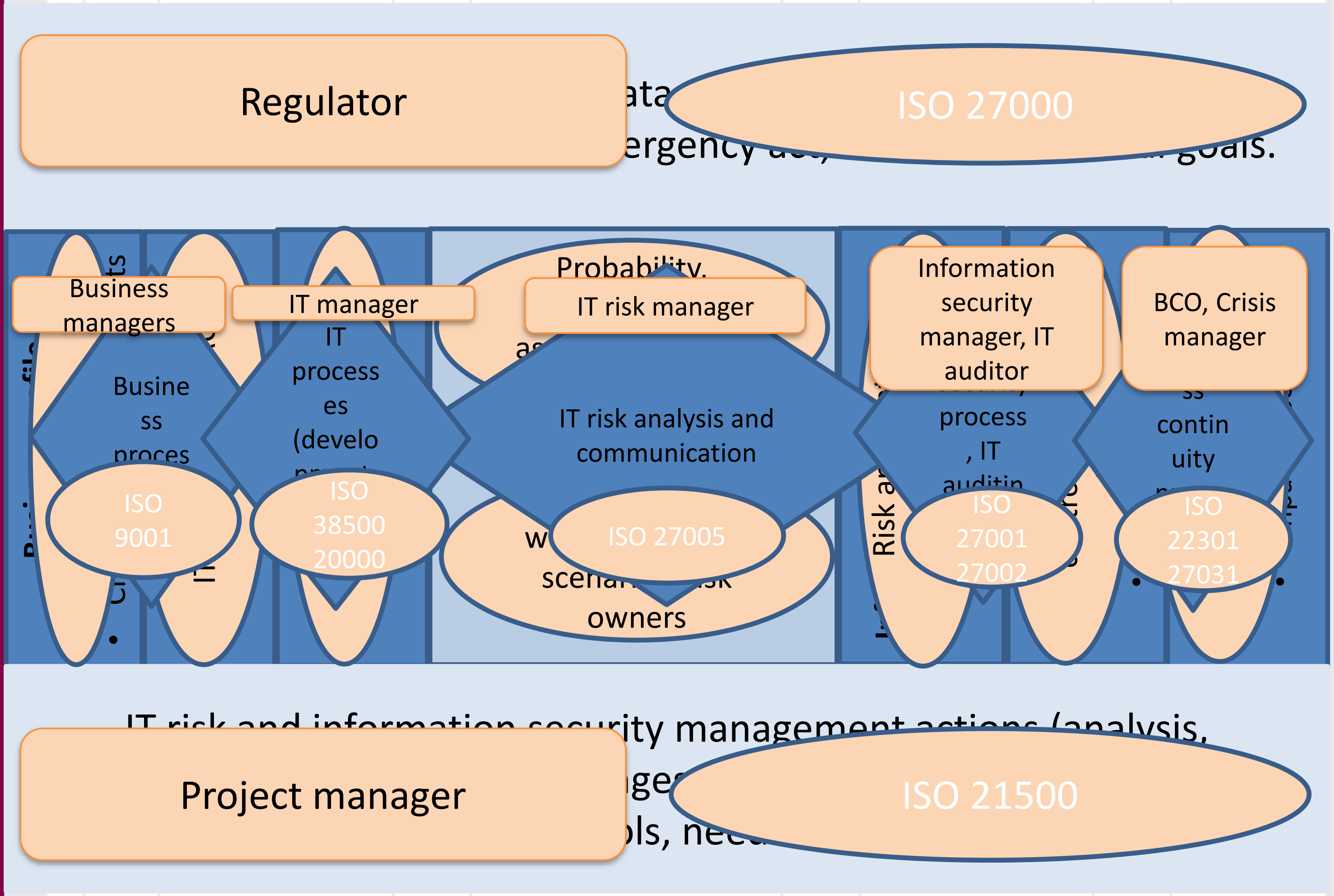
Project manager

IT risk and information security management actions (analysis,

ges in profiles and impact to risks,

ls, need to audit, test etc …)

Concept developments



Regulator

ISO 27000

…ata… …ergency act, … goals.

Business managers

Business processes

ISO 9001

IT manager

IT processes (develo…

ISO 38500 20000

Probability,

IT risk manager

IT risk analysis and communication

ISO 27005

scenarios … risk owners

Information security manager, IT auditor

… process , IT auditin…

ISO 27001 27002

Risk a…

BCO, Crisis manager

…ss contin uity …

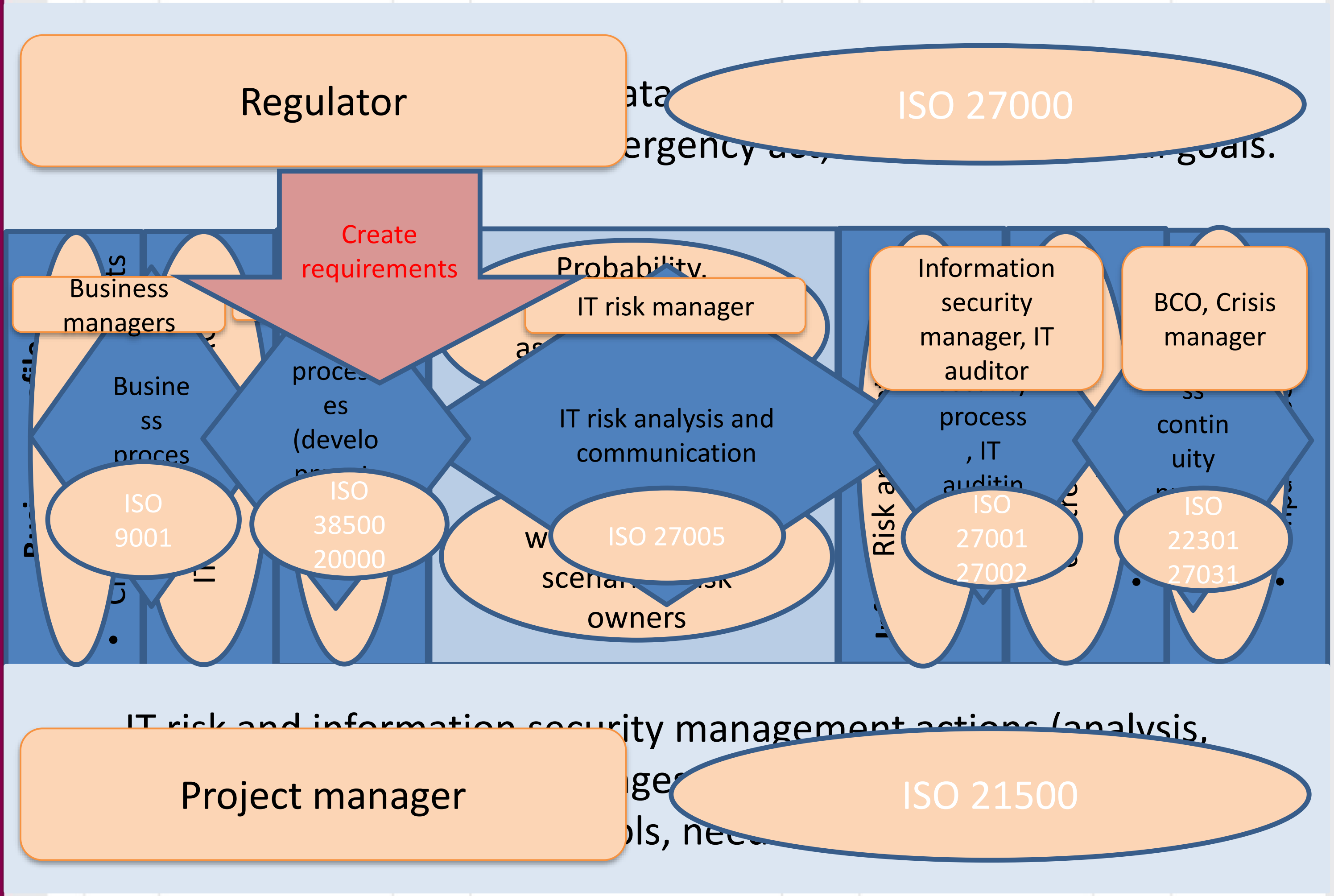
ISO 22301 27031

IT risk and information security management actions (analysis, …ges… …ols, nee…

Project manager

ISO 21500

Concept developments



Regulator

ata
ergency act,
goals.

ISO 27000

Create requirements

Business managers

Busine ss proces

ISO 9001

proce es (develo

ISO 38500 20000

Probability,

IT risk manager

IT risk analysis and communication

ISO 27005

w
scenar
owners

Information security manager, IT auditor

process , IT auditin

ISO 27001 27002

Risk a

BCO, Crisis manager

ss contin uity

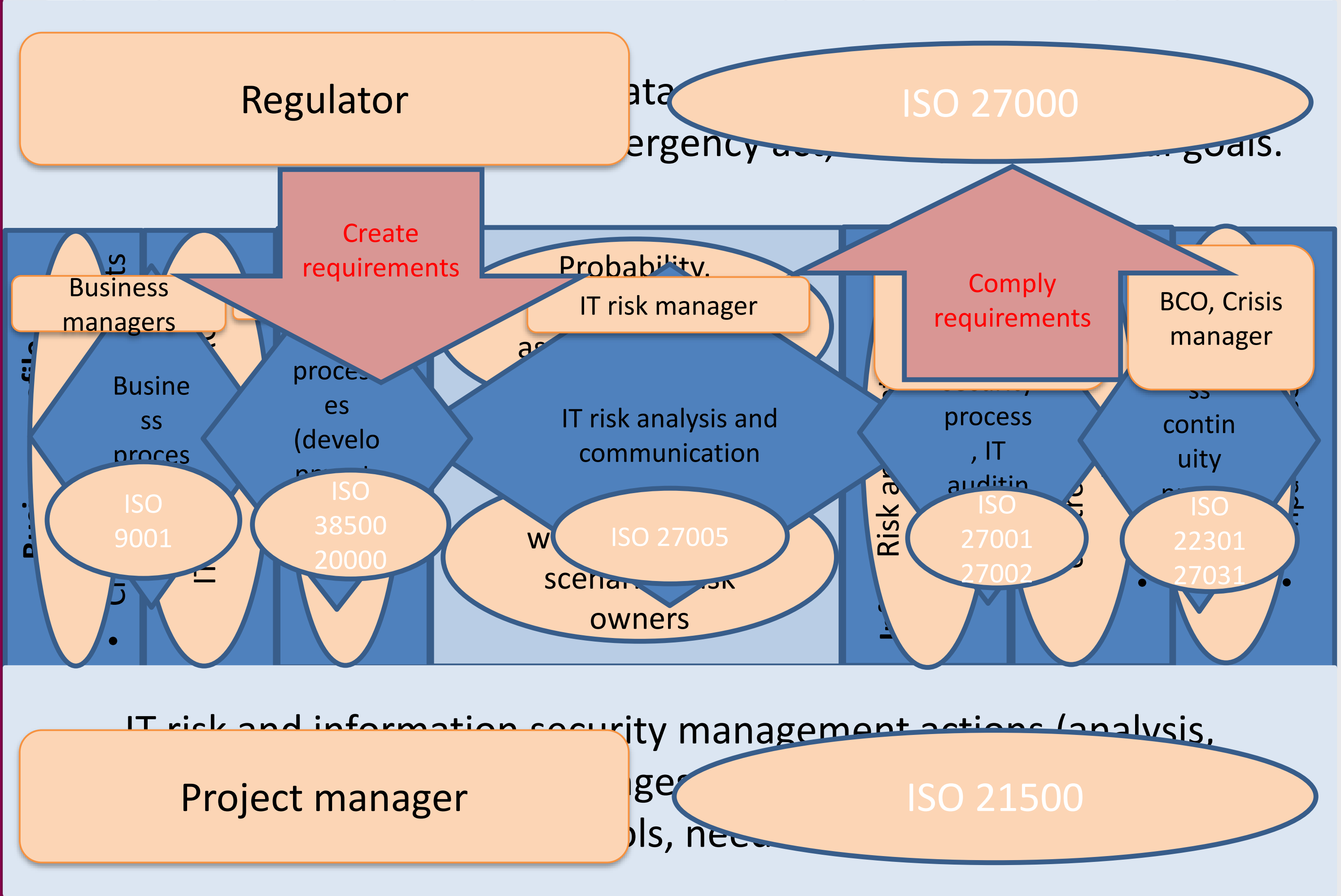
ISO 22301 27031

IT risk and information security management actions (analysis,
ges
ls, nee

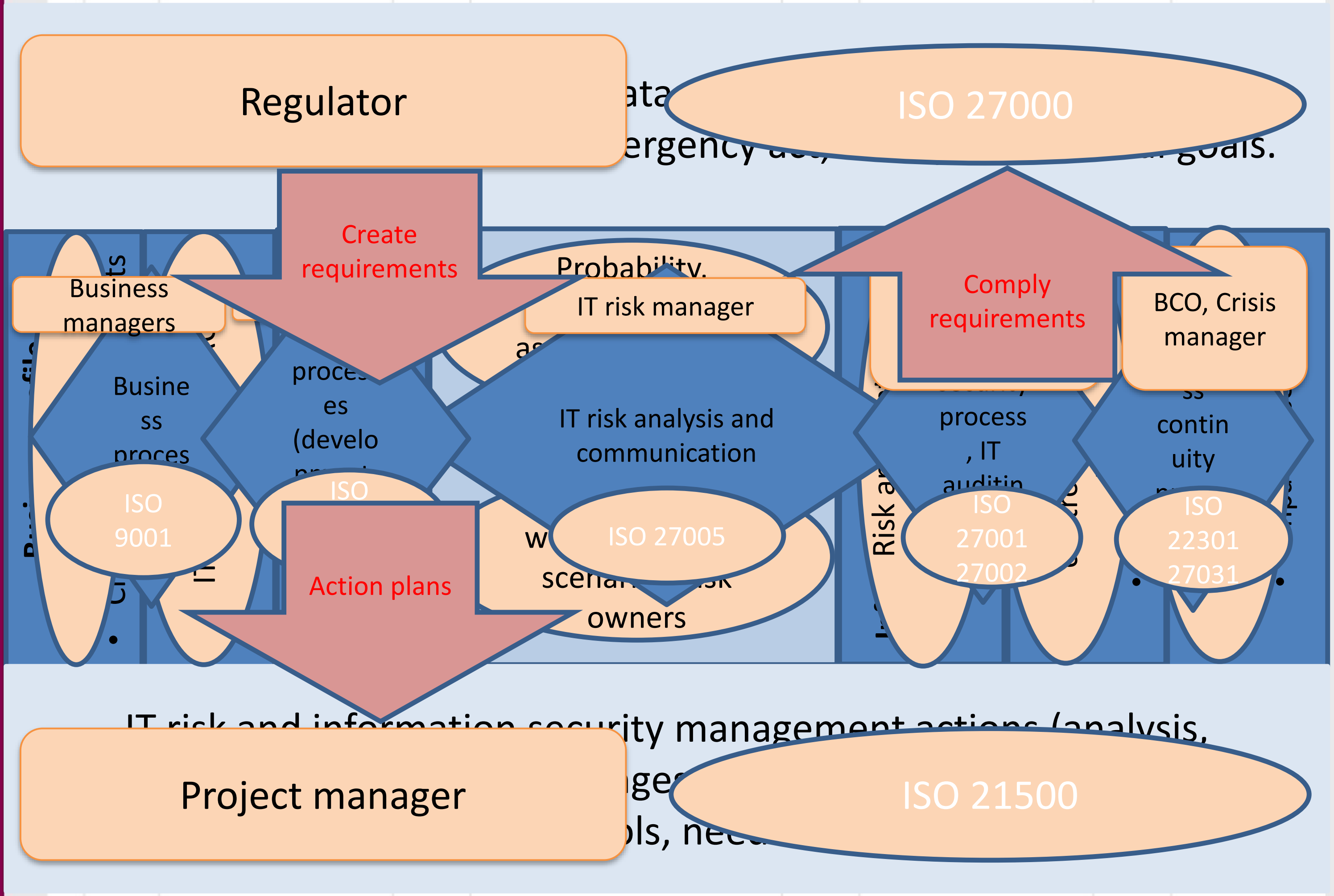
Project manager

ISO 21500

Concept developments



Concept developments



Regulator

ISO 27000

ata

ergency act,

goals.

Create requirements

Comply requirements

Business managers

IT risk manager

BCO, Crisis manager

Probability,

Busine ss proces

proces es (develo

IT risk analysis and communication

process , IT auditin

ss contin uity

ISO 9001

ISO

ISO 27005

ISO 27001 27002

ISO 22301 27031

Risk ar

scenar risk owners

Action plans

IT risk and information security management actions (analysis,

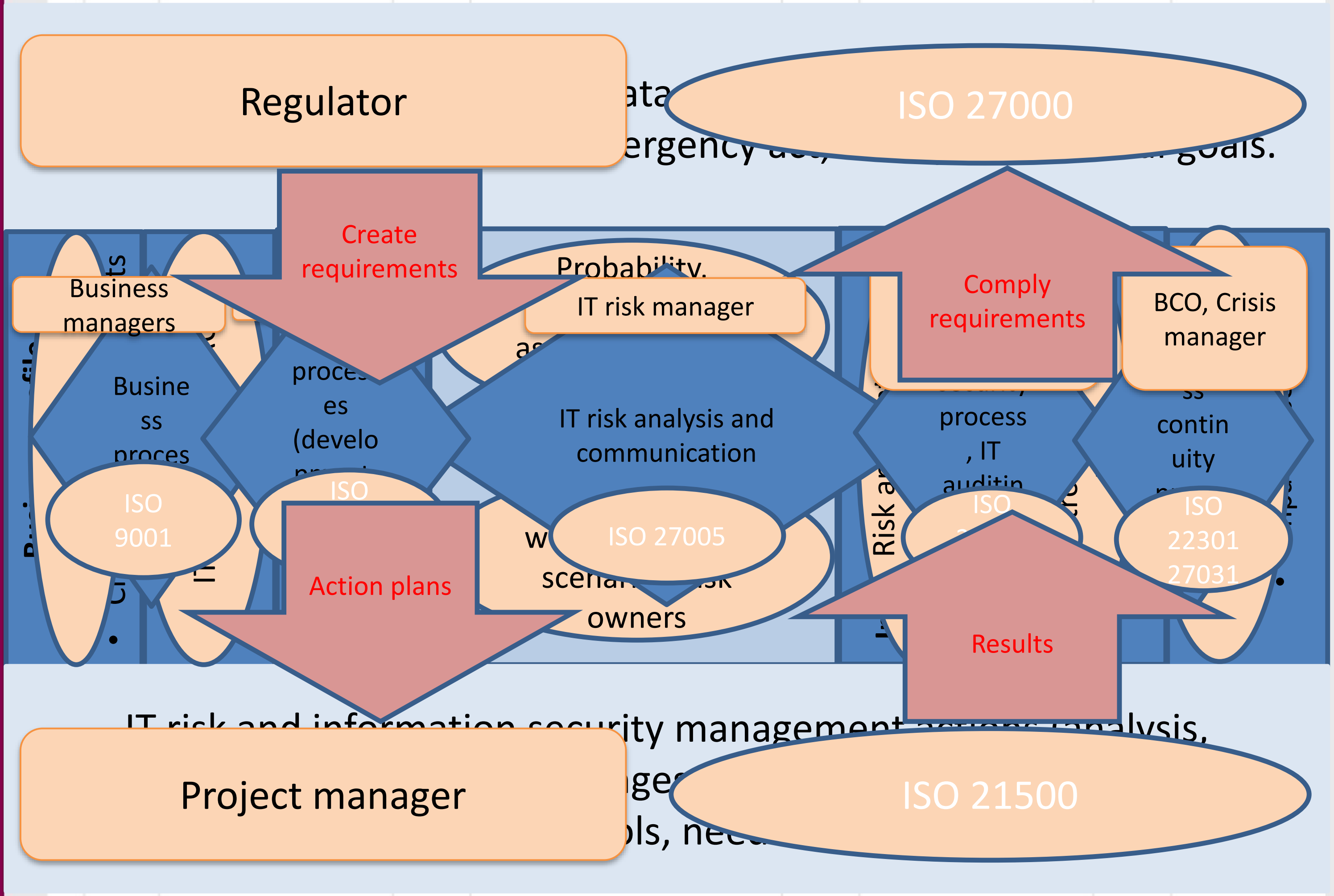
ges

ols, nee

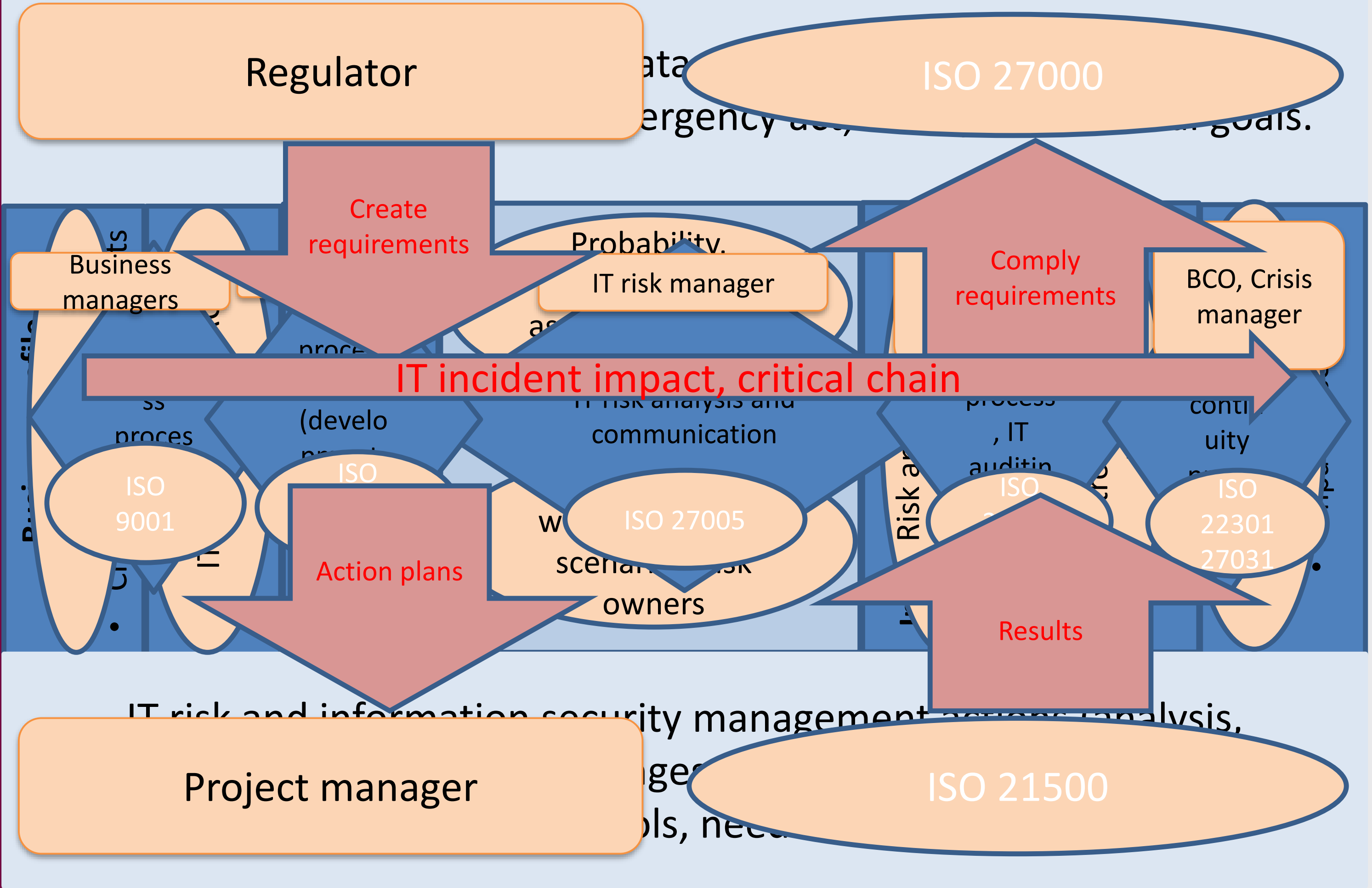
Project manager

ISO 21500

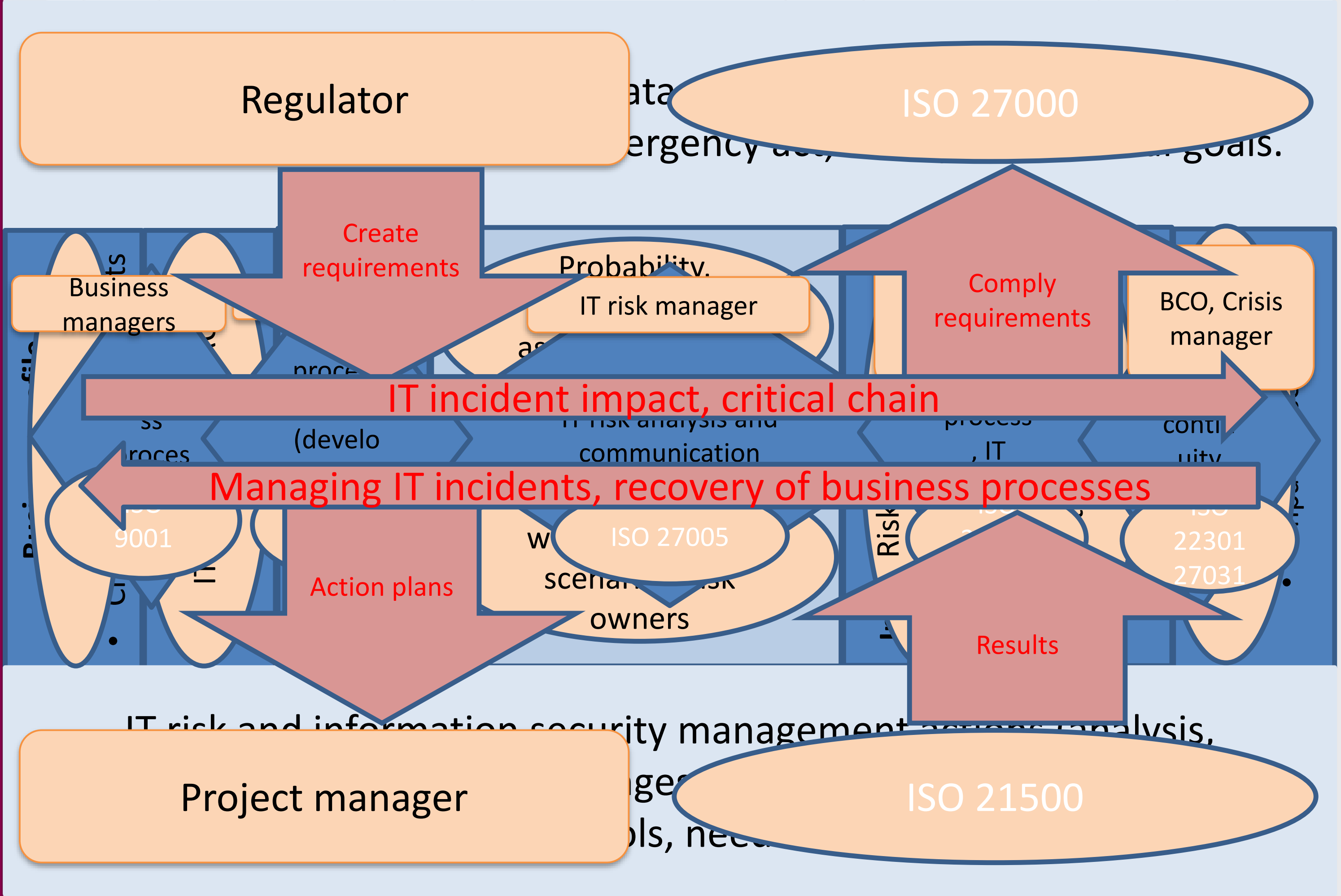
Concept developments



Concept developments



Concept developments



Regulator

ISO 27000

Create requirements

Comply requirements

Business managers

IT risk manager

BCO, Crisis manager

Probability,

IT incident impact, critical chain

Managing IT incidents, recovery of business processes

(develo

communication

ISO 9001

ISO 27005

ISO 22301 27031

owners

Action plans

Results

Project manager

ISO 21500

...ata

...ergency act, ... goals.

IT risk and information security management actions, analysis,

...ges

...ols, nee...

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 (IS management metrics, IS economics)
~~22.11.2016 – Lecture 12 (self reading - IT auditing (ISACA))~~
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

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

Requirements by law

Link

Requirements by regulators

Link

Requirements by standard

Link

Information security goals

Direct monetary loss

Loss of reputation -> monetary loss

Breach of law

-> loss of reputation -> monetary loss

-> penalties -> monetary loss

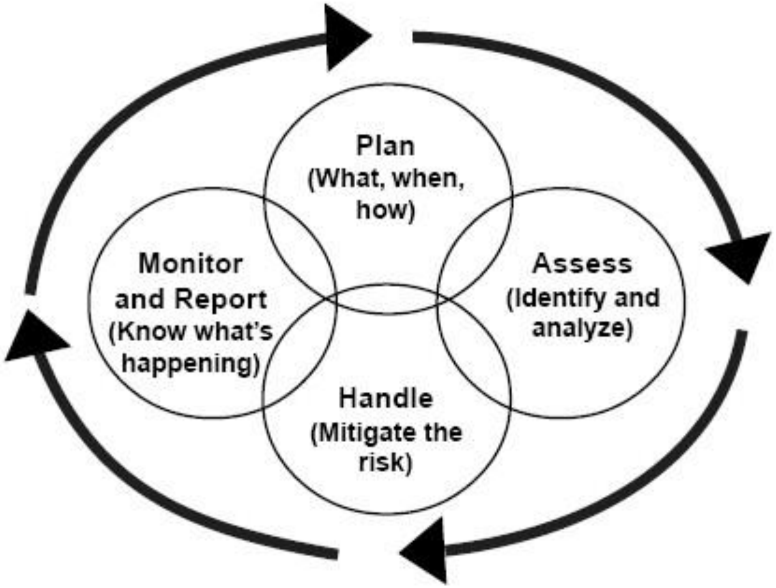
Violation of work -> additional work -> monetary loss

Interruption of core business

-> loss of income -> monetary loss

-> breach of contract -> monetary loss

Process



A Continuous Interlocked Process—Not an Event

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

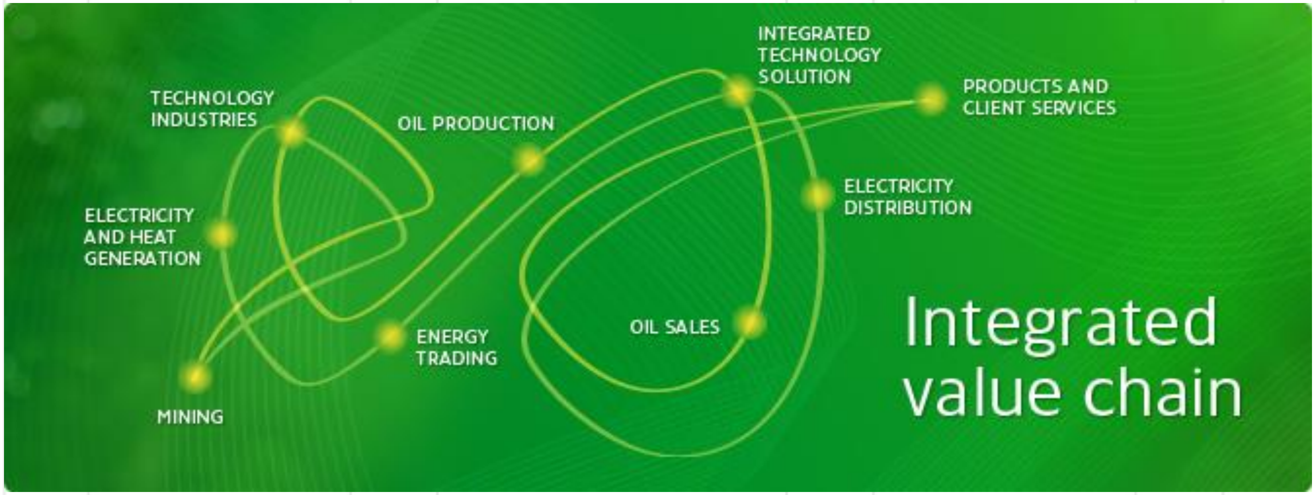
Business process example

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

EUROSÜSTEEM

Business process example



Business process 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.

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
…

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).

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/)

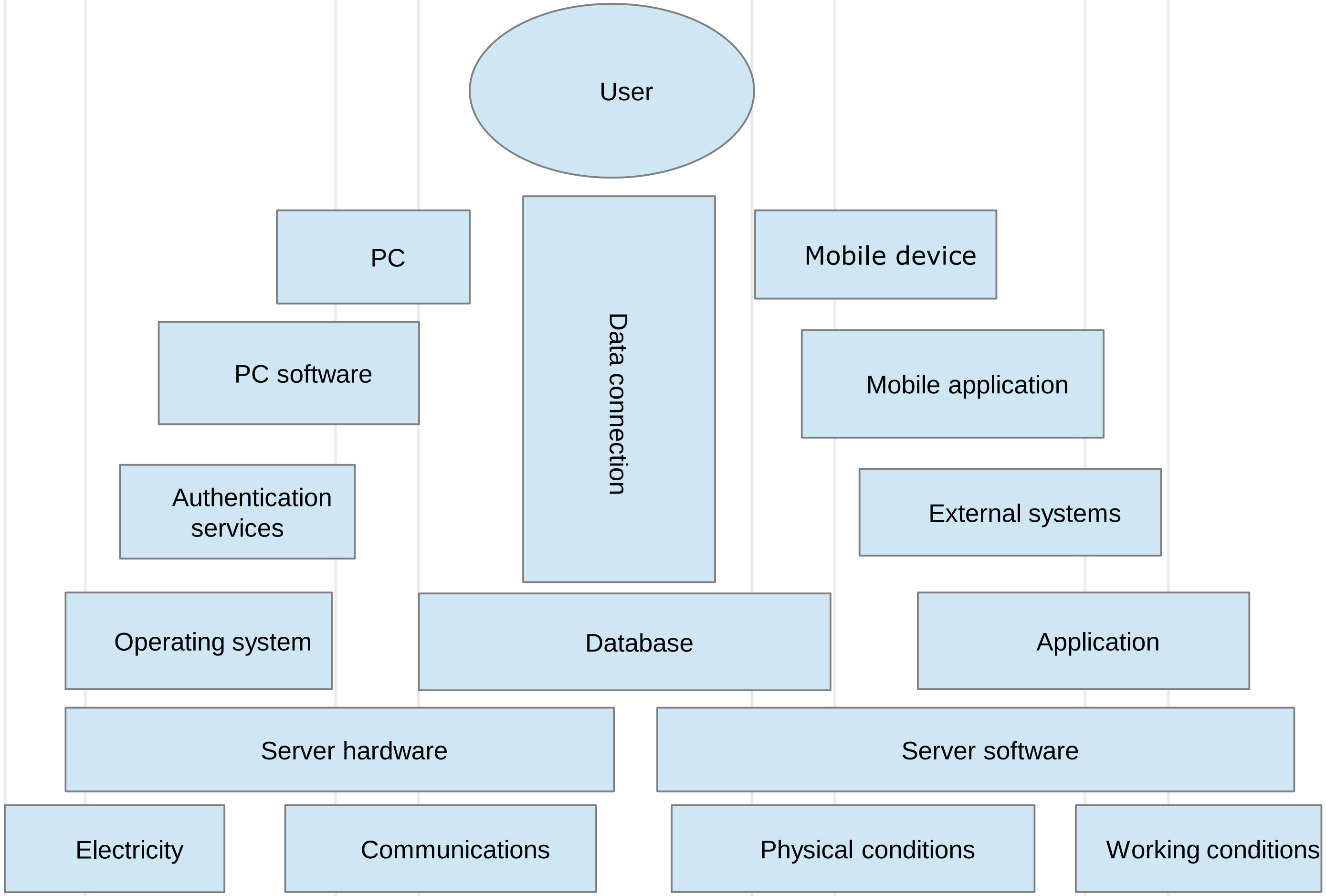
Data modelling

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 swiches
Testing systems
Third party systems
Wired and wireless networks
…

Information system


User

PC

Data connection

Mobile device

PC software

Mobile application

Authentication services

External systems

Operating system

Database

Application

Server hardware

Server software

Electricity

Communications

Physical conditions

Working conditions

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

Simple diagram example

BIA template

Worksheet

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