



TALLINN UNIVERSITY OF
TECHNOLOGY



Information and Cyber Security Assurance in Organisations

ITX8090

X



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 – 1,5 h seminar; 1,5 h exam

~~22.12.15~~

~~29.12.15~~

05.01.16 – 1,5 h seminar; 1,5 h exam

12.01.16 – exam (if appropriate)

19.01.16 – exam (if appropriate)



Evaluation

Evaluation criteria

- 1) The course contains obligatory homework assignment. Maximum summary points for assignment: 20.
- 2) Homework assignment deadline 12.12 (via e-mail Andro@consultit.ee)
- 3) In order to pass the course, each student has to pass the written exam. Maximum points: 80.
- 4) Final evaluation The final grade for each student is calculated using a summary score of the homework assignments and the exam, ie. 20% for the homework, 80% for the exam.



Evaluation

The grades are assigned as follows:

score ≥ 90 -- grade 5 (excellent)

$80 < \text{score} \leq 90$ -- grade 4 (very good)

$70 < \text{score} \leq 80$ -- grade 3 (good)

$60 < \text{score} \leq 70$ -- grade 2 (satisfactory)

$50 < \text{score} \leq 60$ -- grade 1 (pass)

score < 50 -- grade 0 (failed)



Practical info

Course page

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



IT risk and control concept

Assurance service is an independent professional service with the goal of improving the information (security) or the context of the information (security) so that decision makers can make more informed, and presumably better, decisions. Assurance services provide independent and professional opinions that reduce the information (security) risk.



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.



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.

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 ...)



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 ...)



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 profile

Critical information systems
Critical IT 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 ...)



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 profile

Critical information systems
Critical IT assets

IT governance profile

- Policy
- Procedures

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 ...)



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 profile

Critical information systems
Critical IT assets

IT governance profile

- Policy
- Procedures

IT incidents

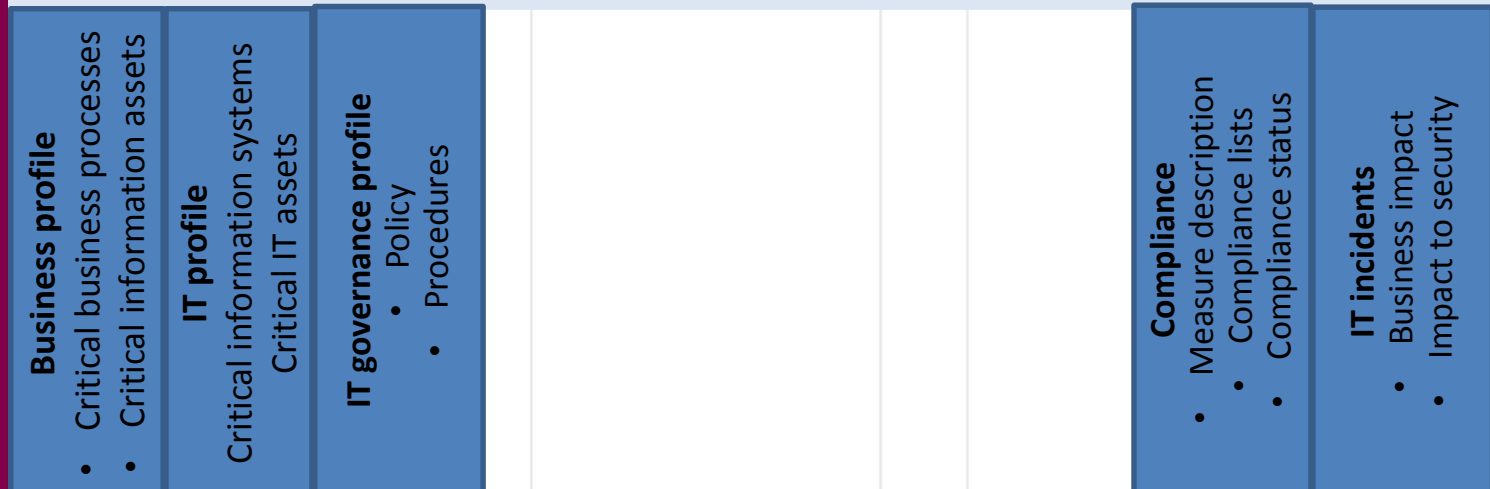
- Business impact
- Impact to security

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 ...)



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.



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 ...)



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.



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 ...)



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.

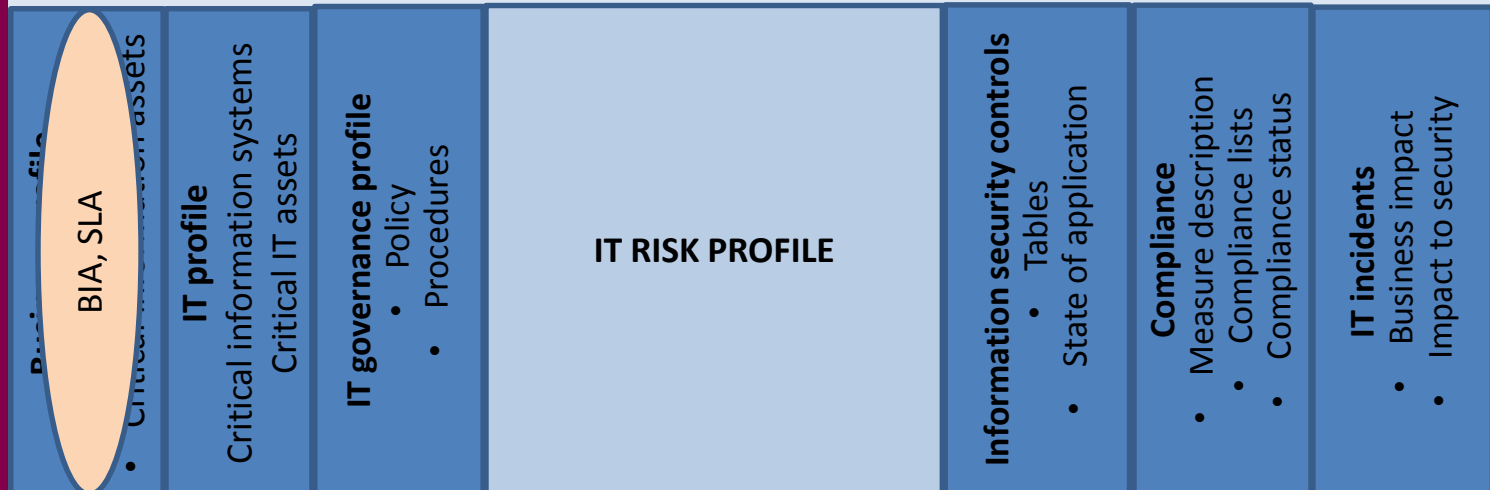


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.



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 ...)



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.



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 ...)



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.



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 ...)



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.



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 ...)



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.

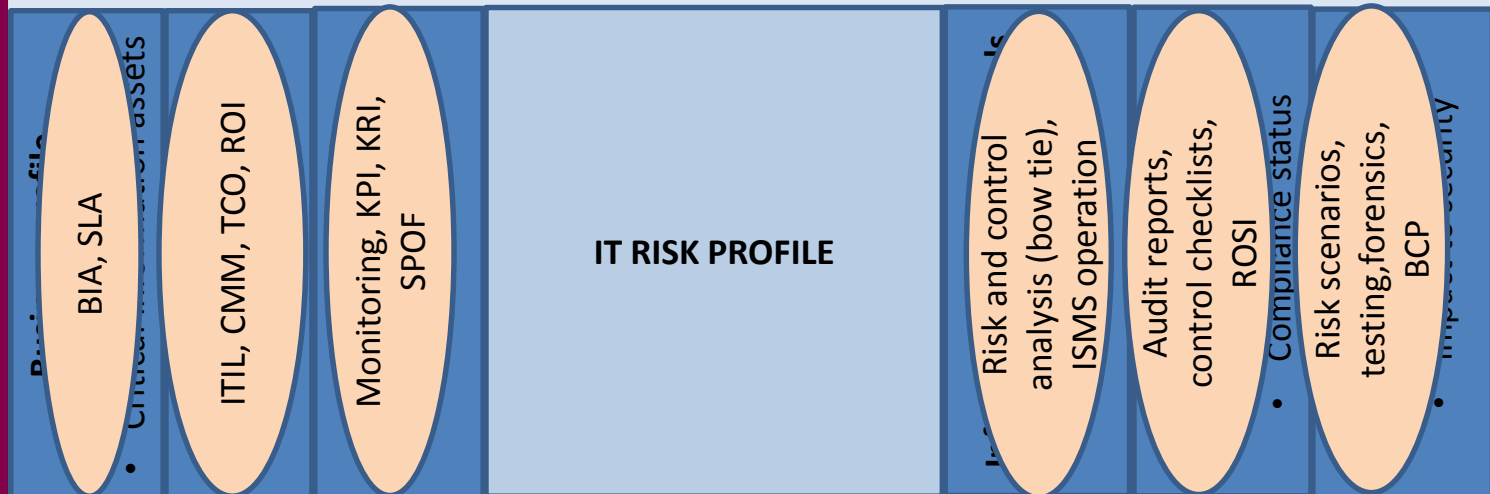


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

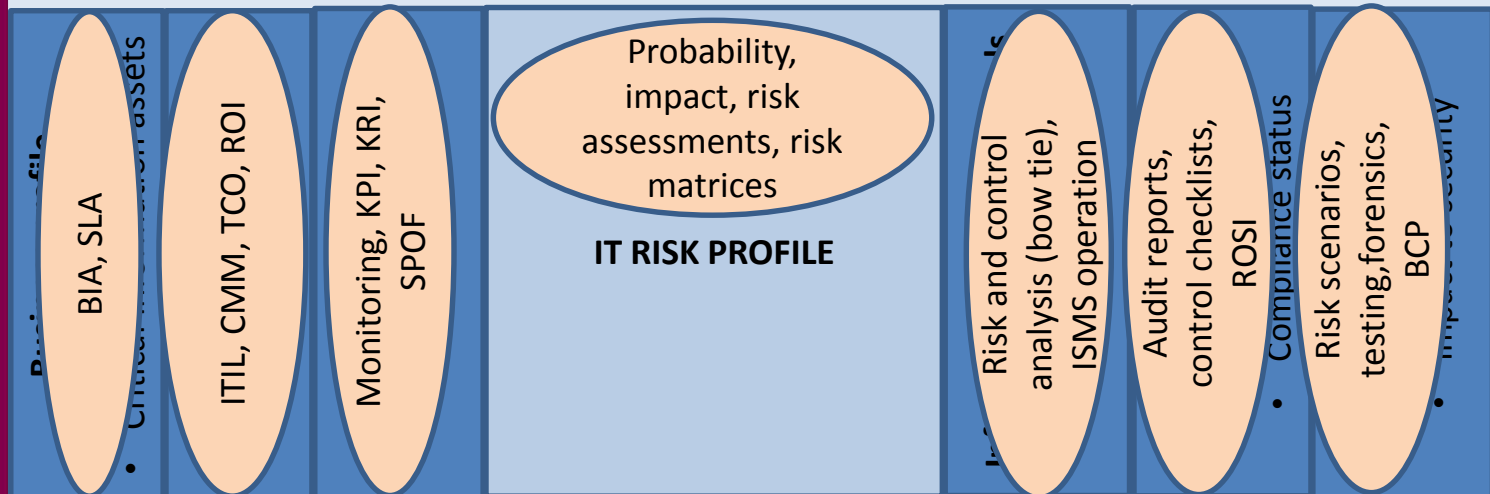


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

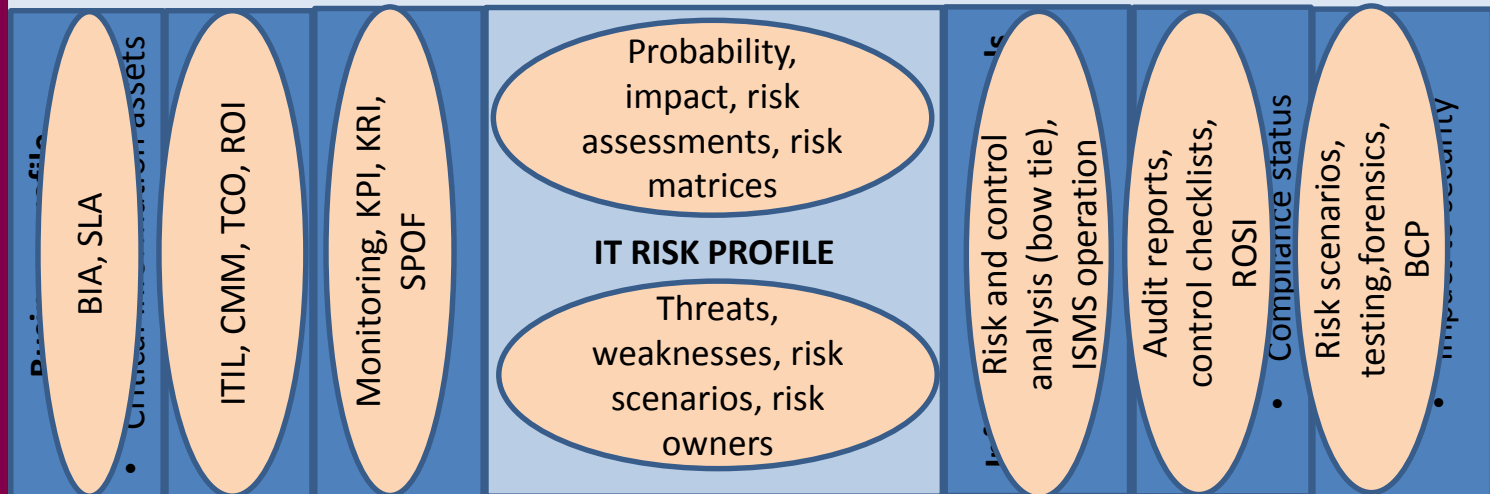


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

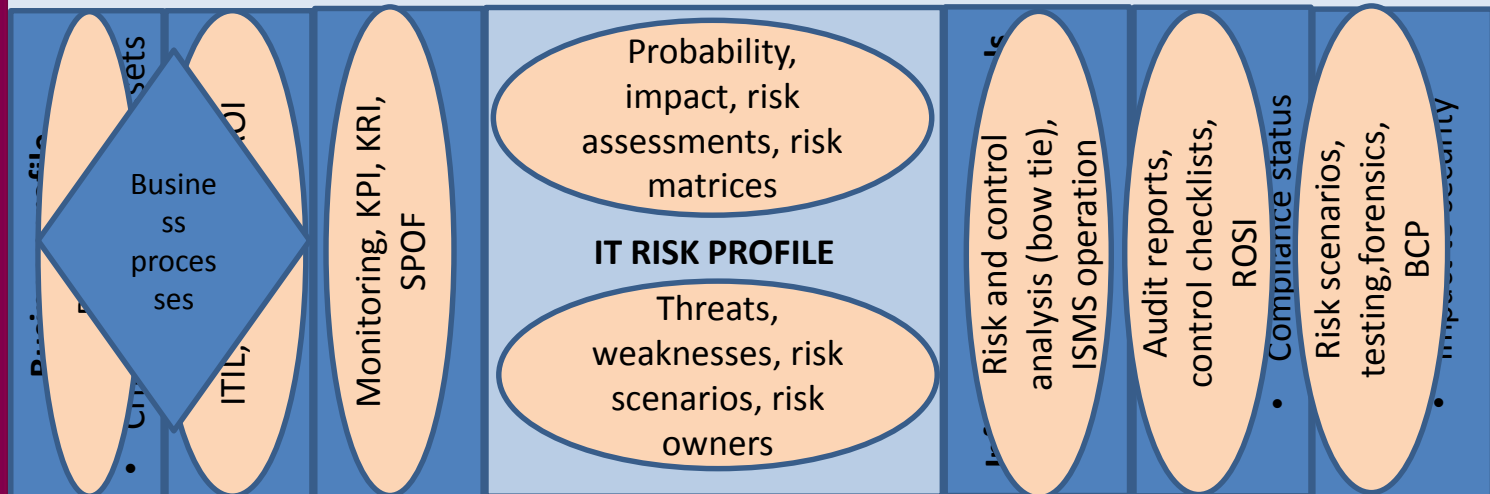


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

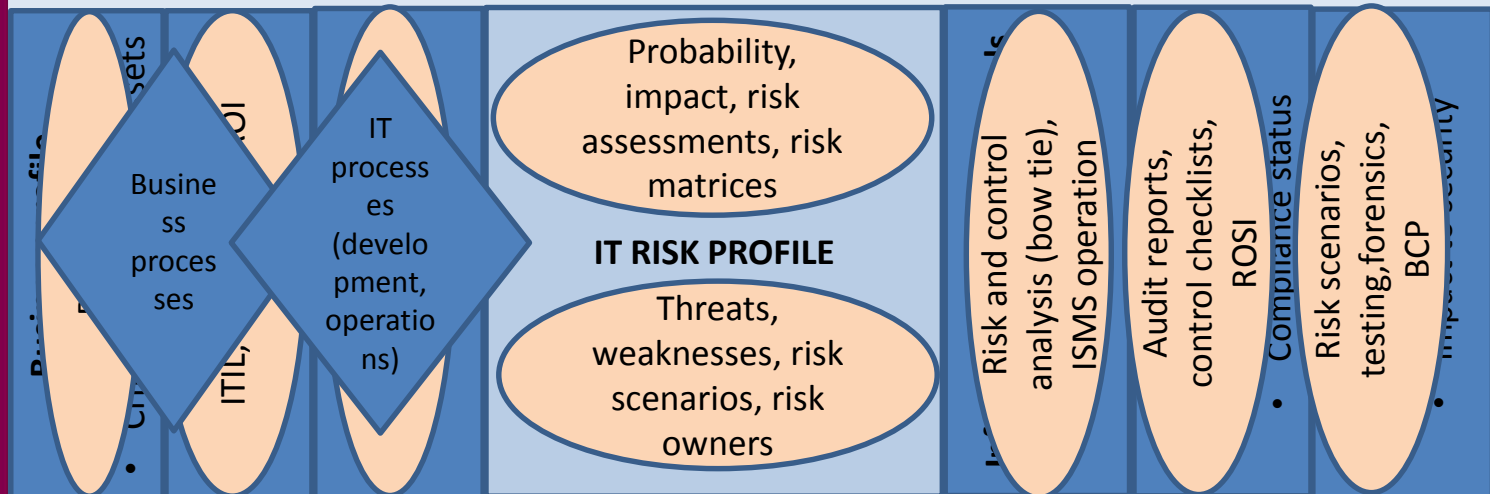


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

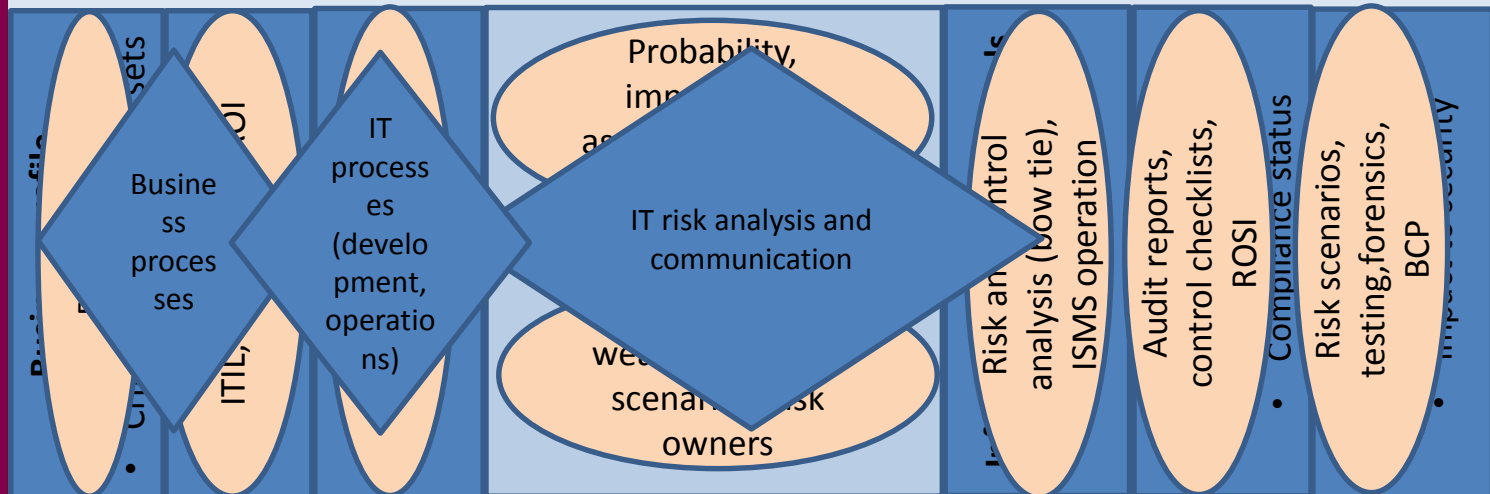


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

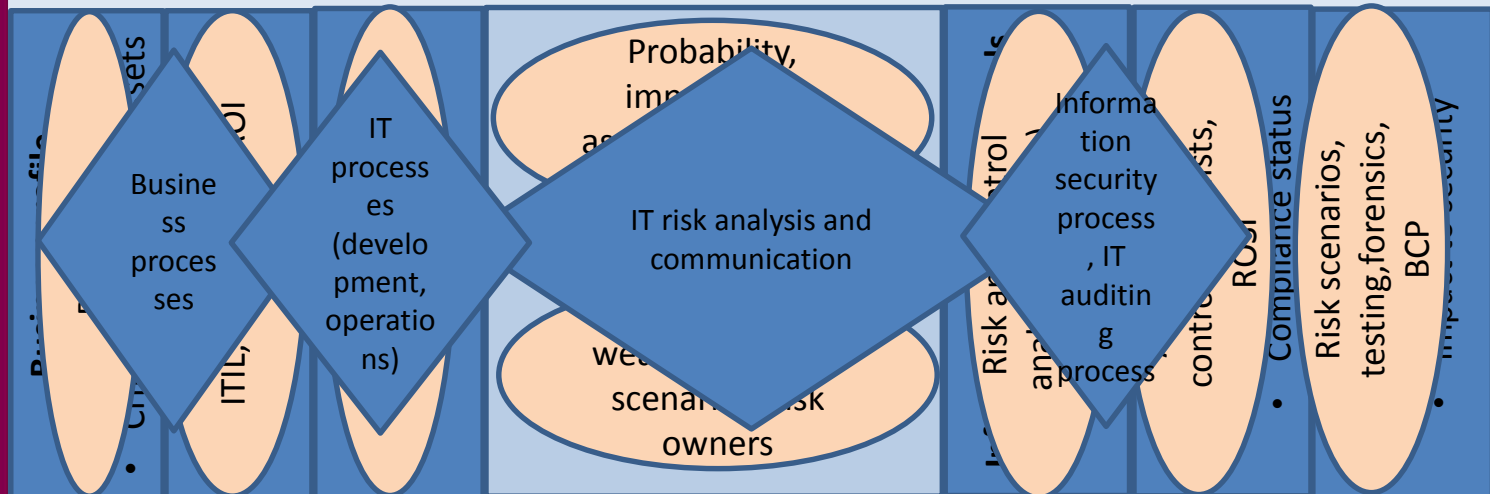


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

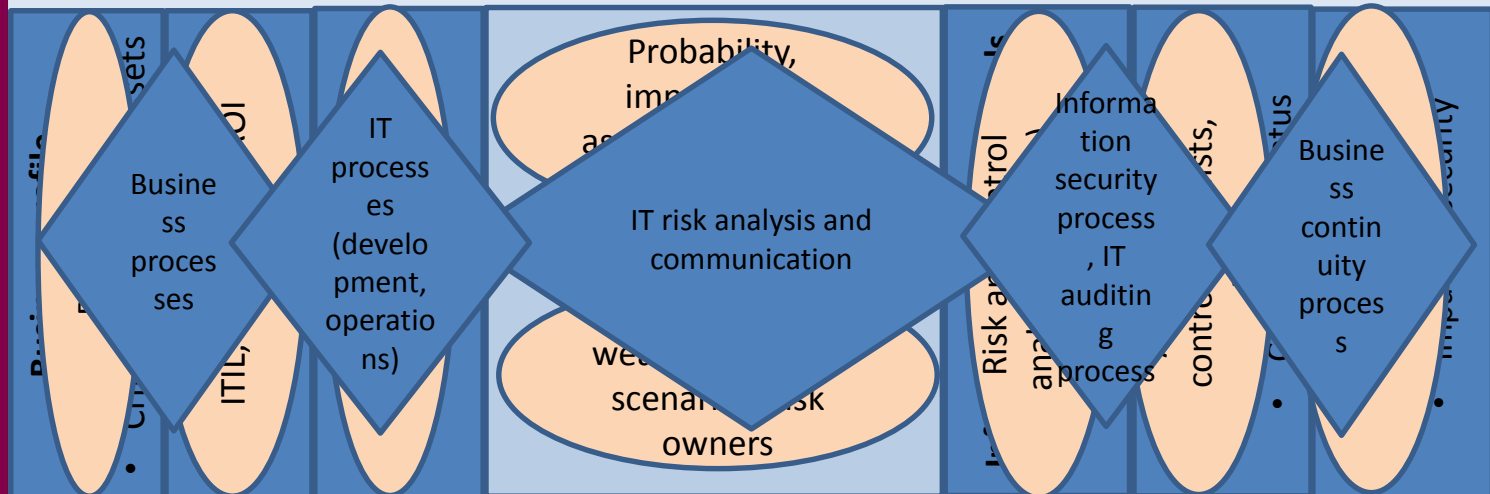


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

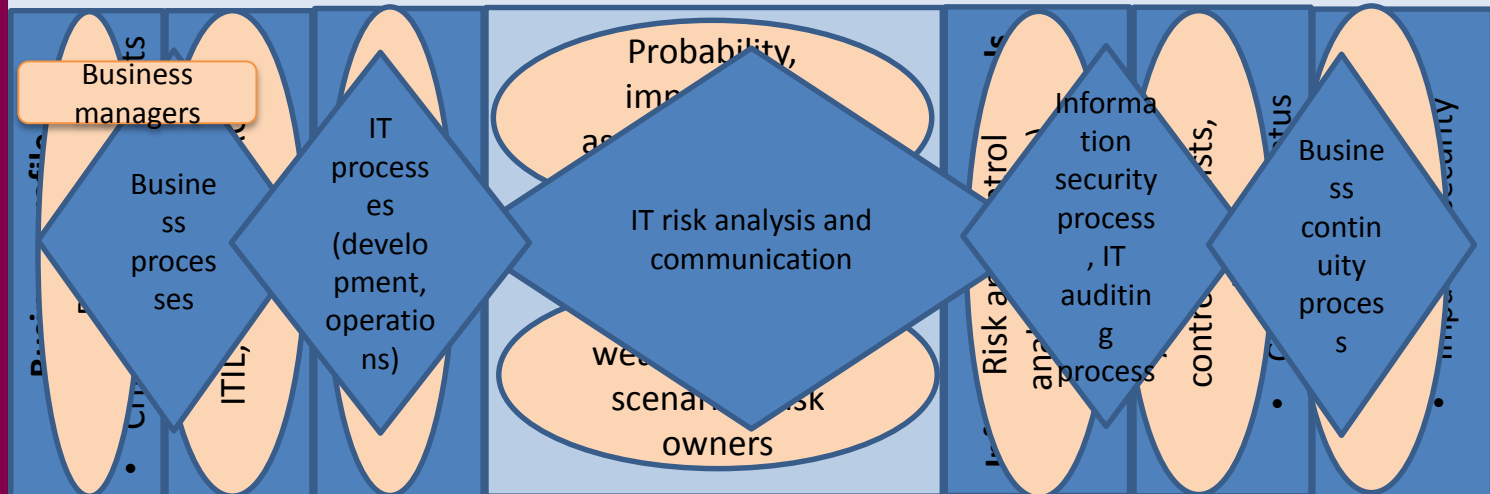


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

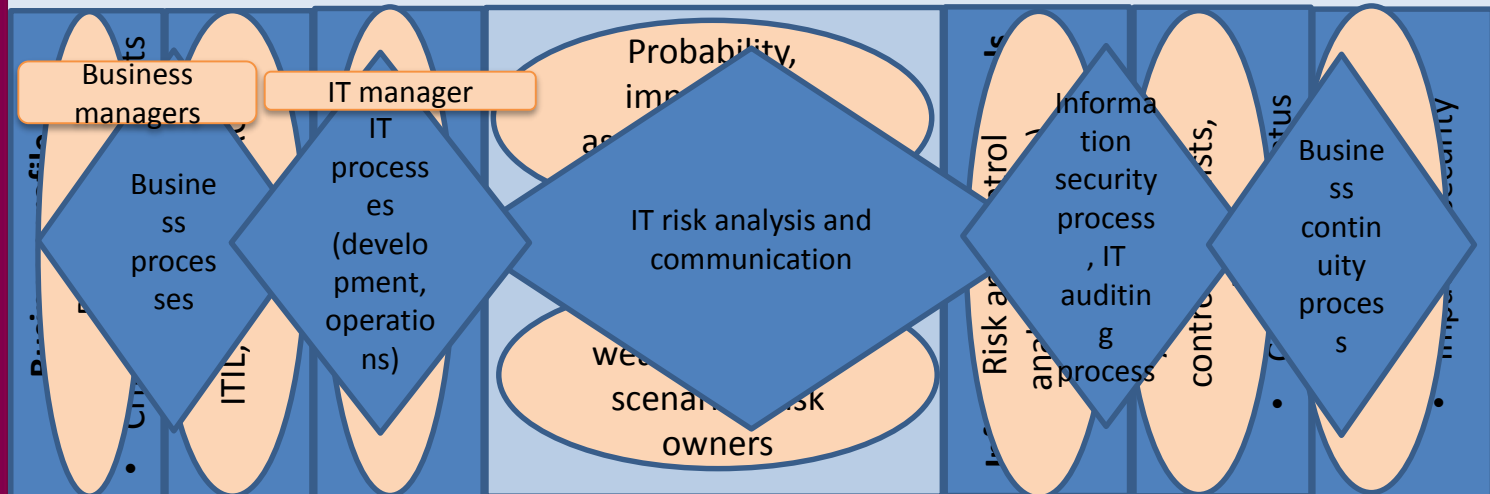


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

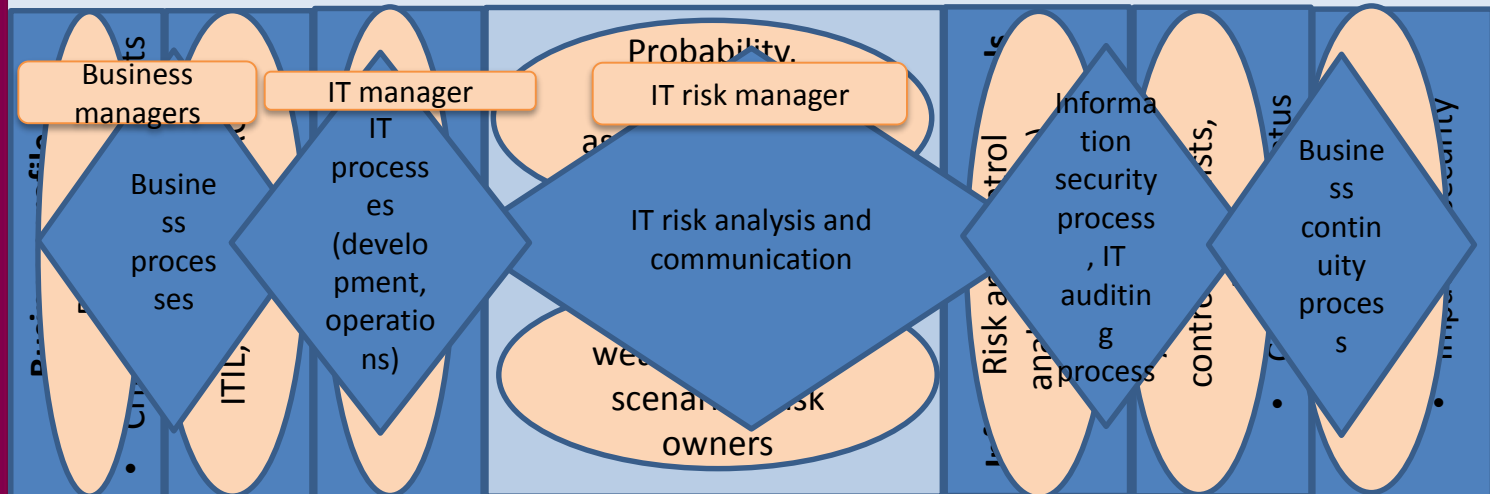


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

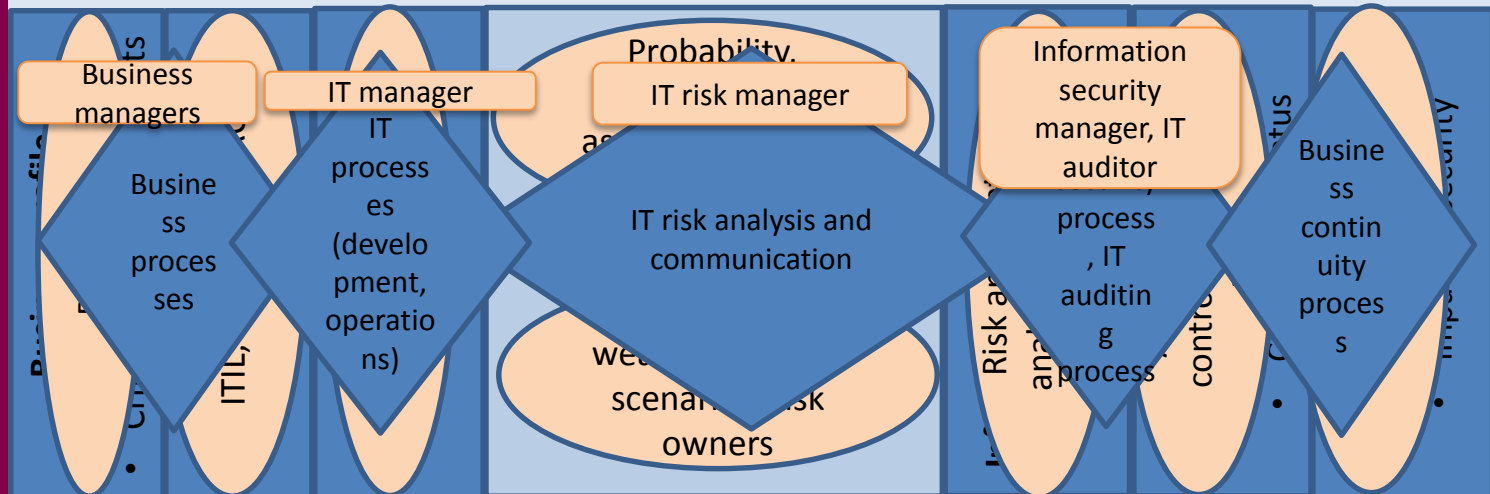


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

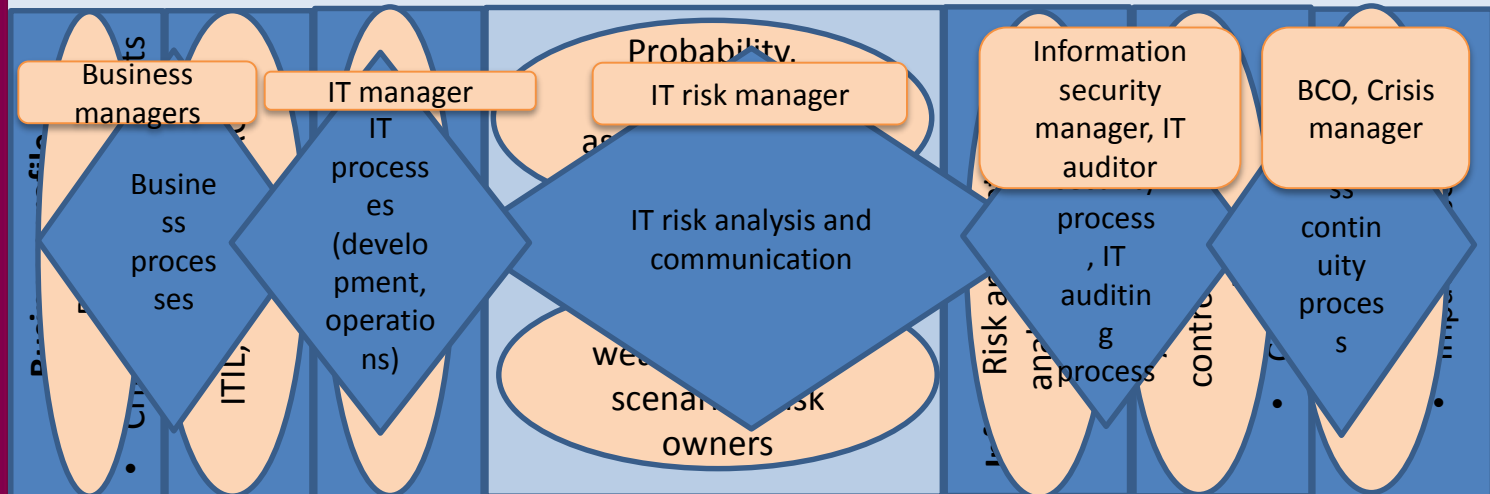


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

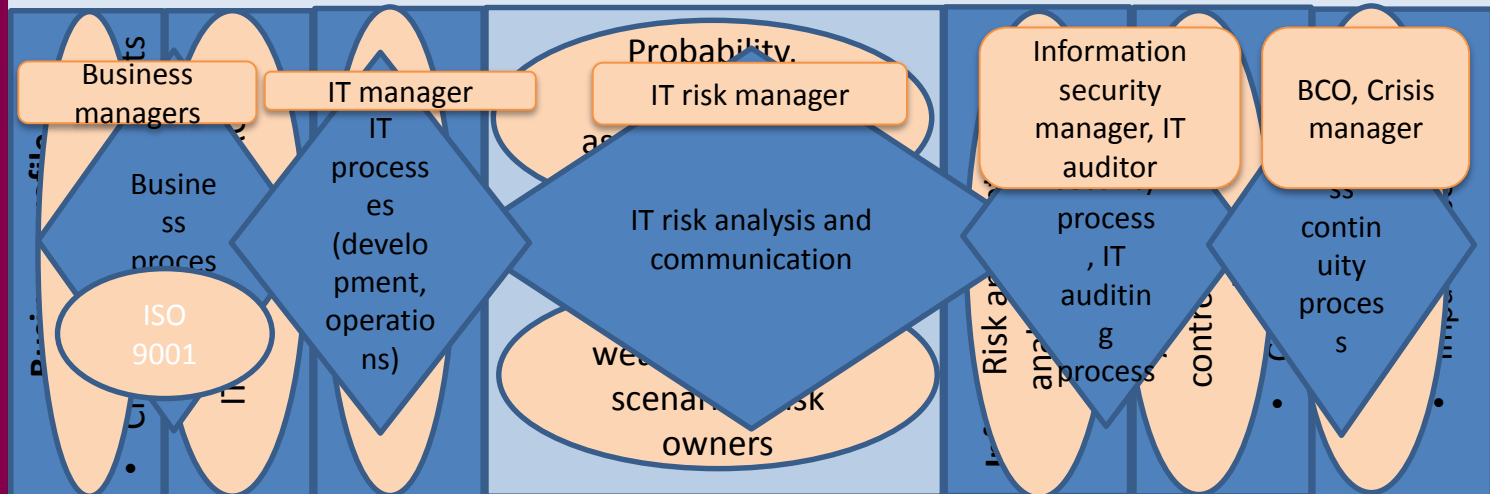


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

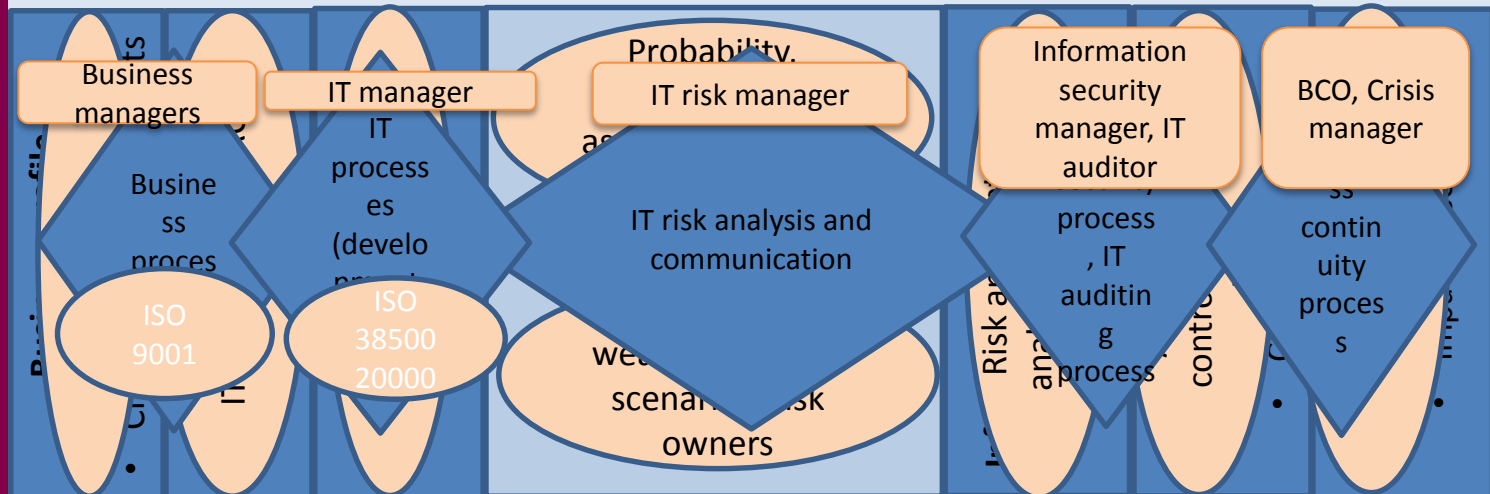


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

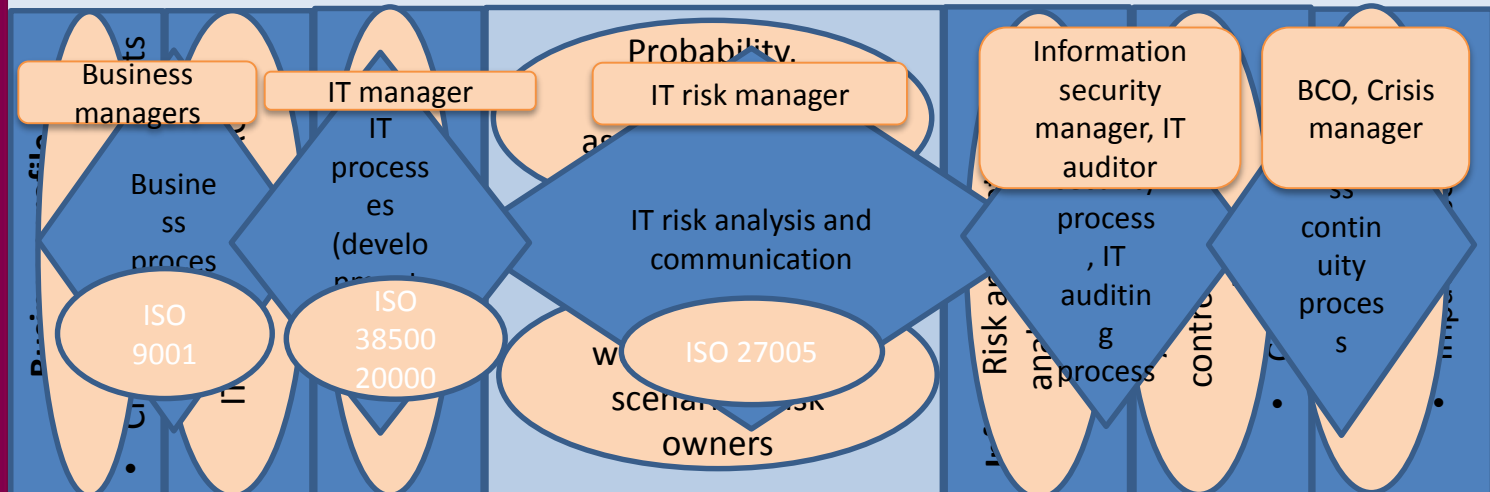


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

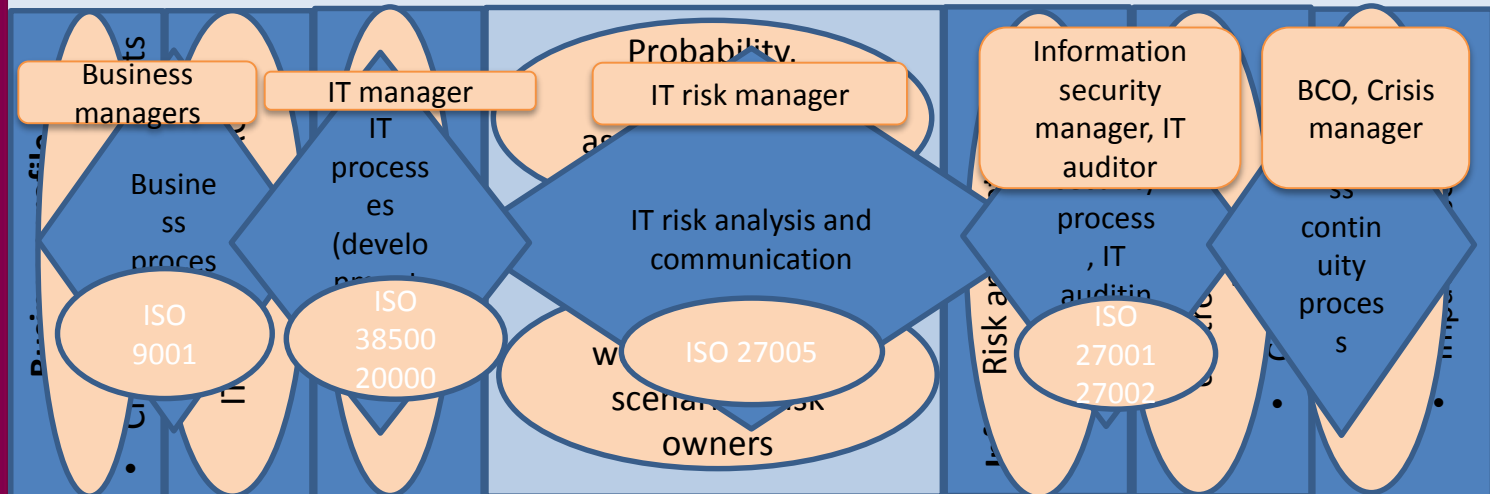


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

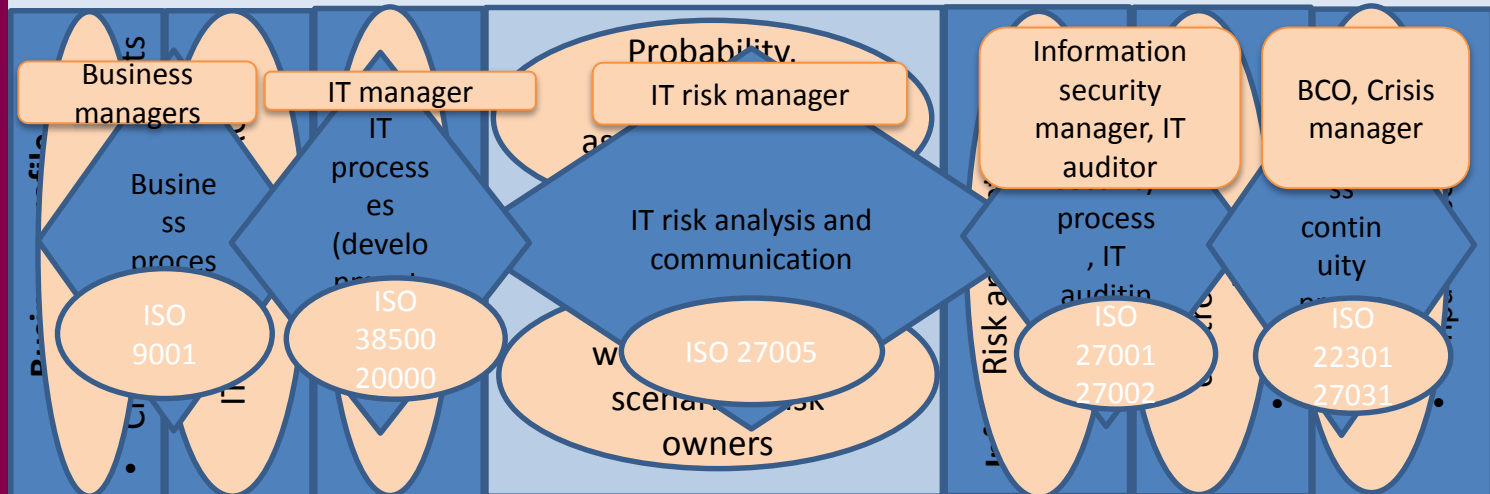


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.



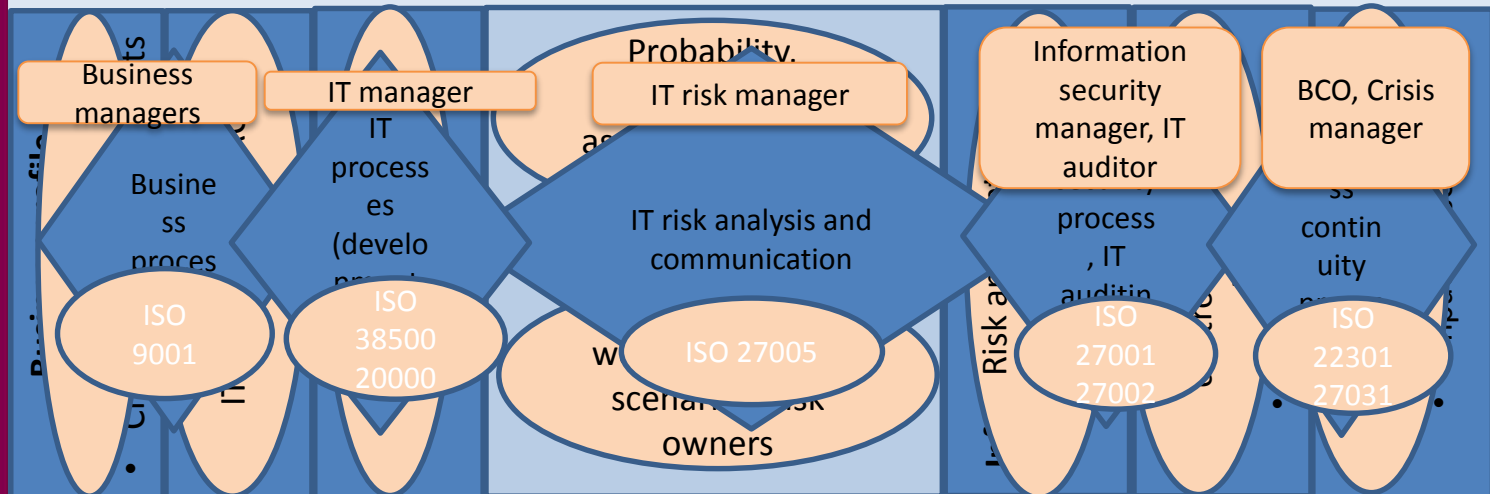
IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



IT risk and control concept

Regulator

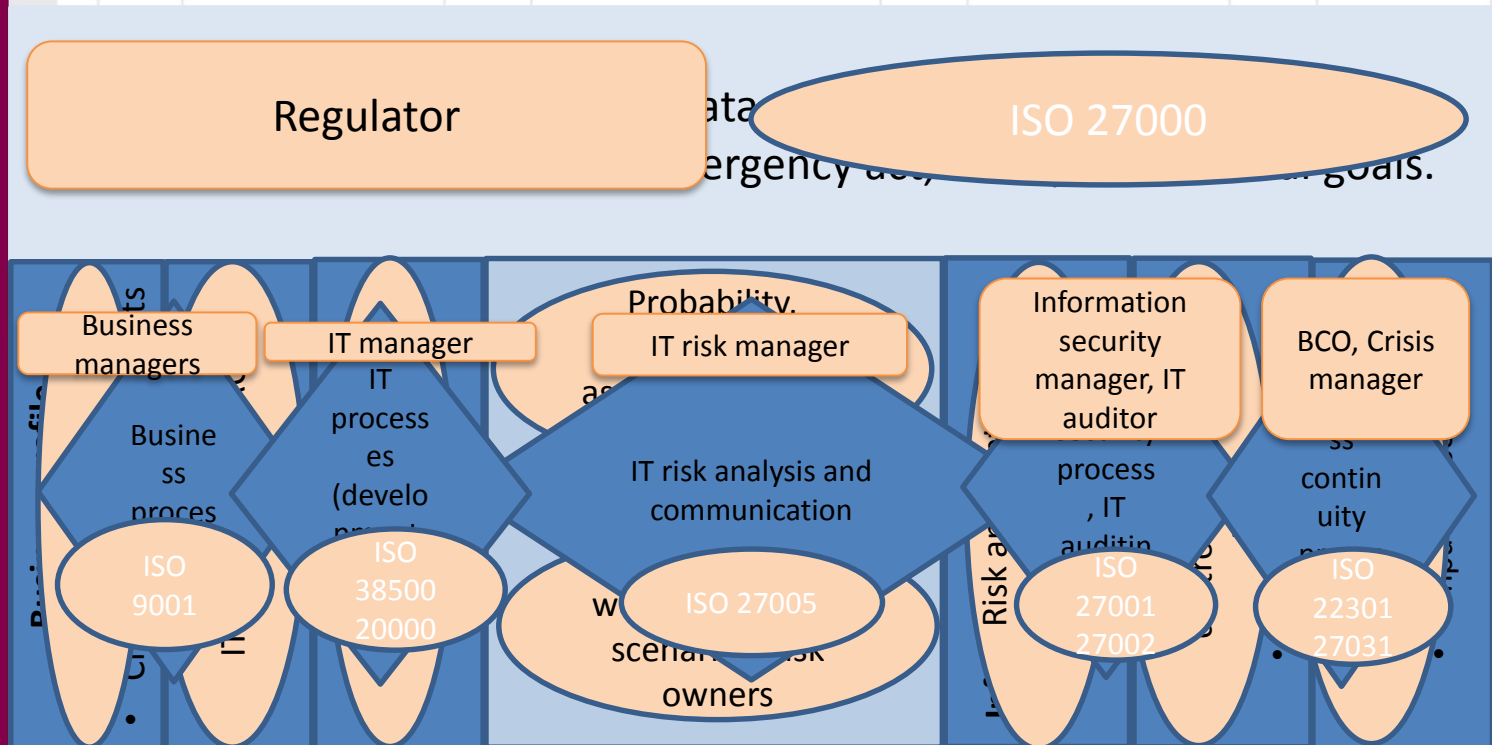
data protection, business continuity (for emergency act, etc ...) and internal goals.



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 ...)



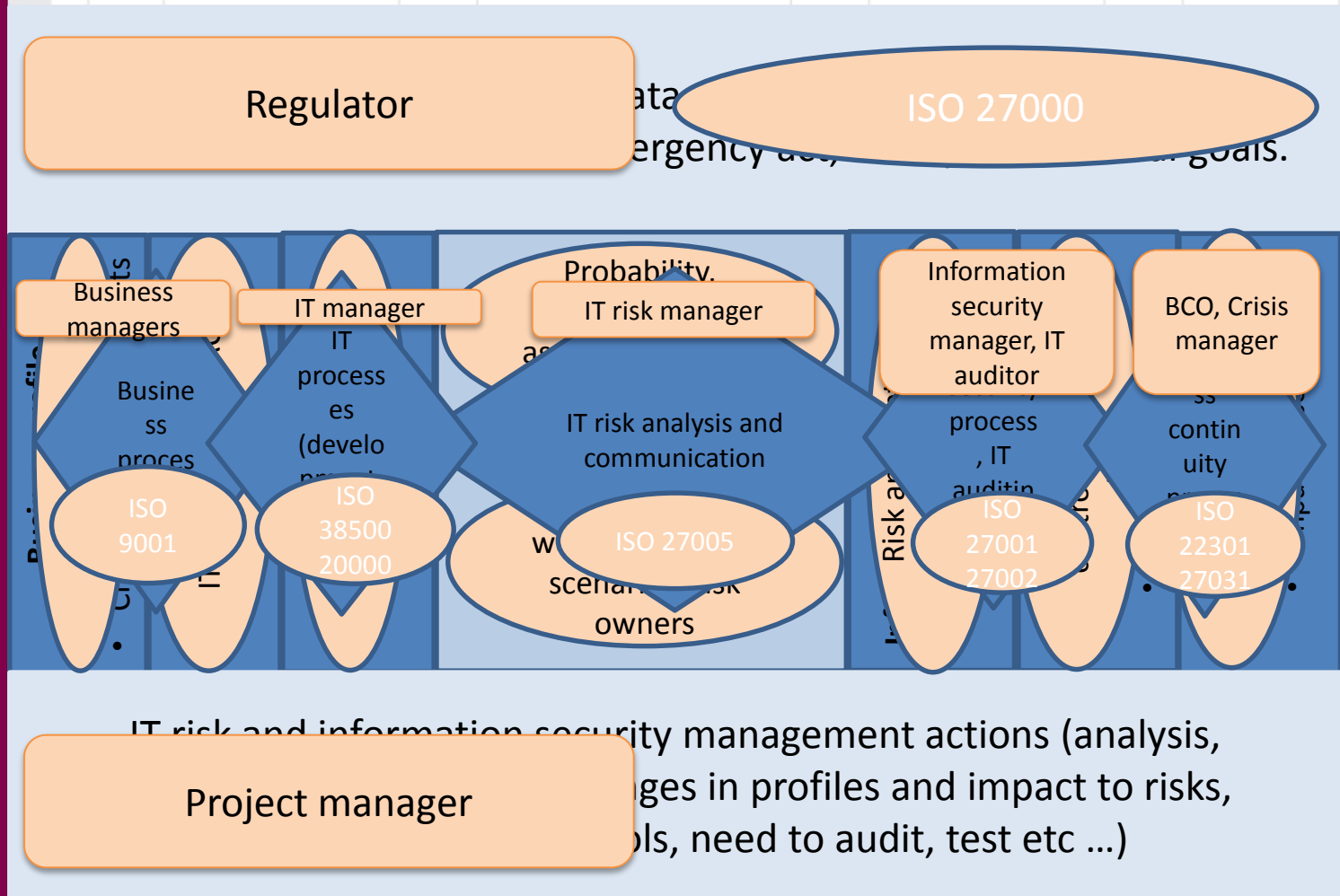
IT risk and control concept



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 ...)

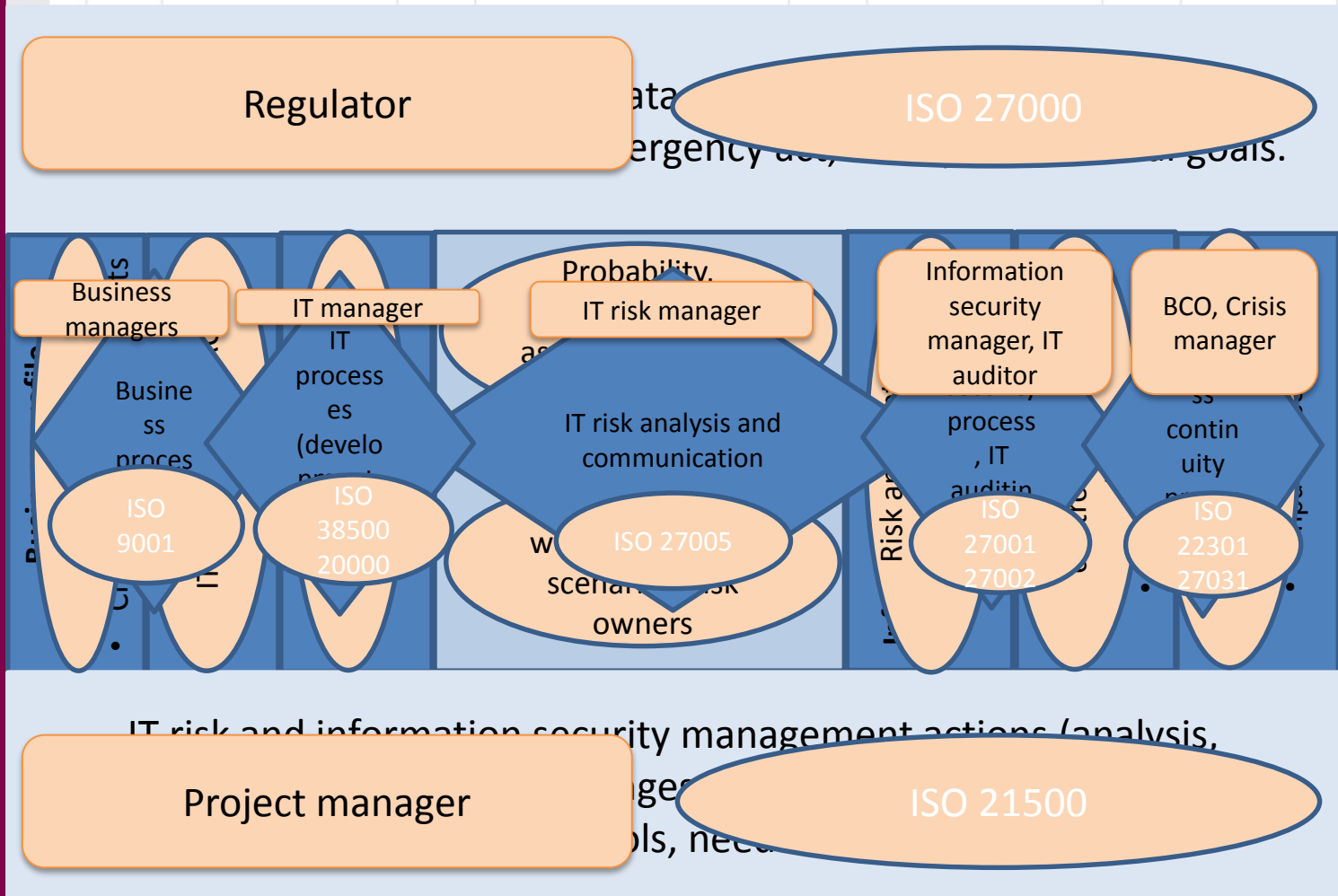


IT risk and control concept



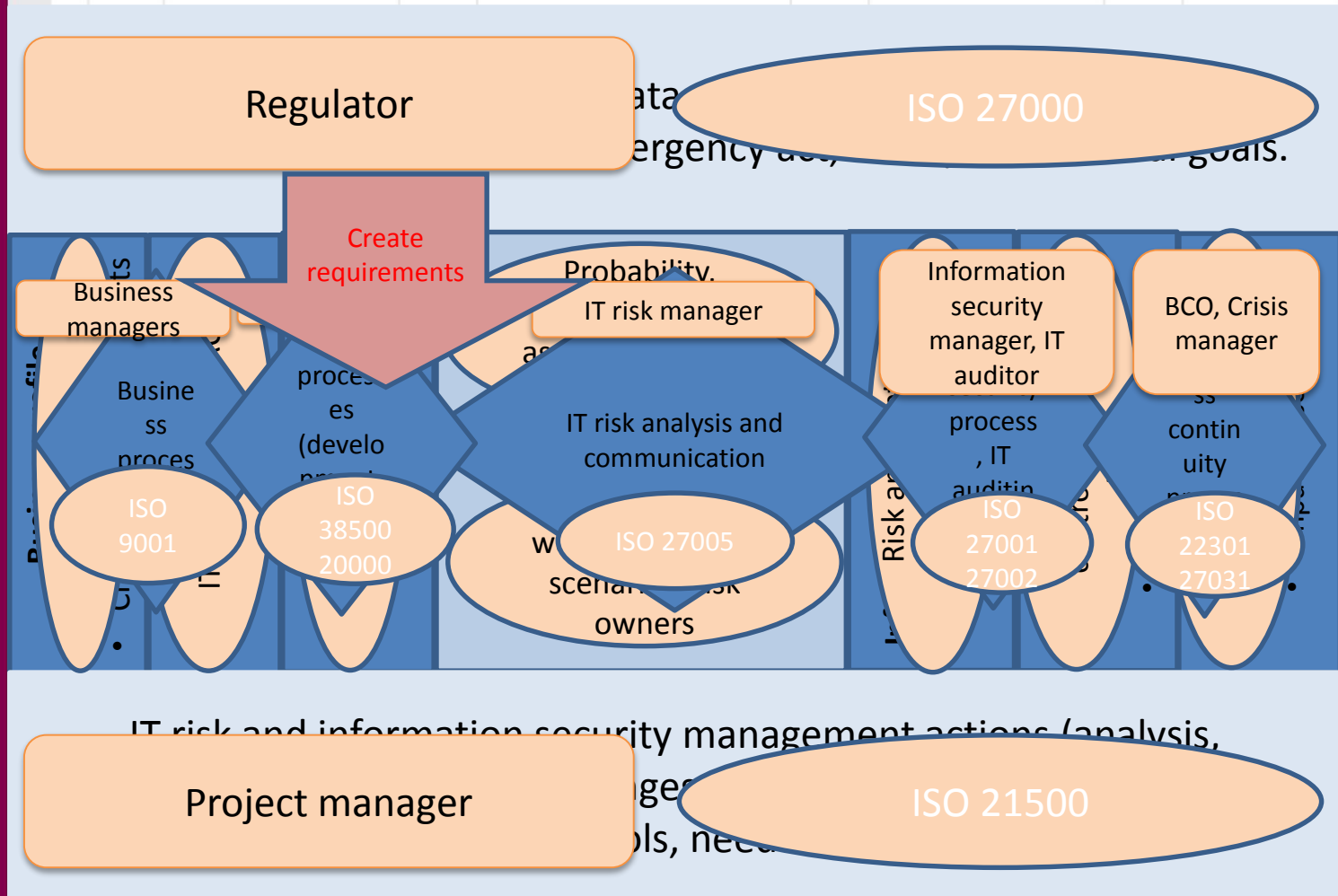


IT risk and control concept



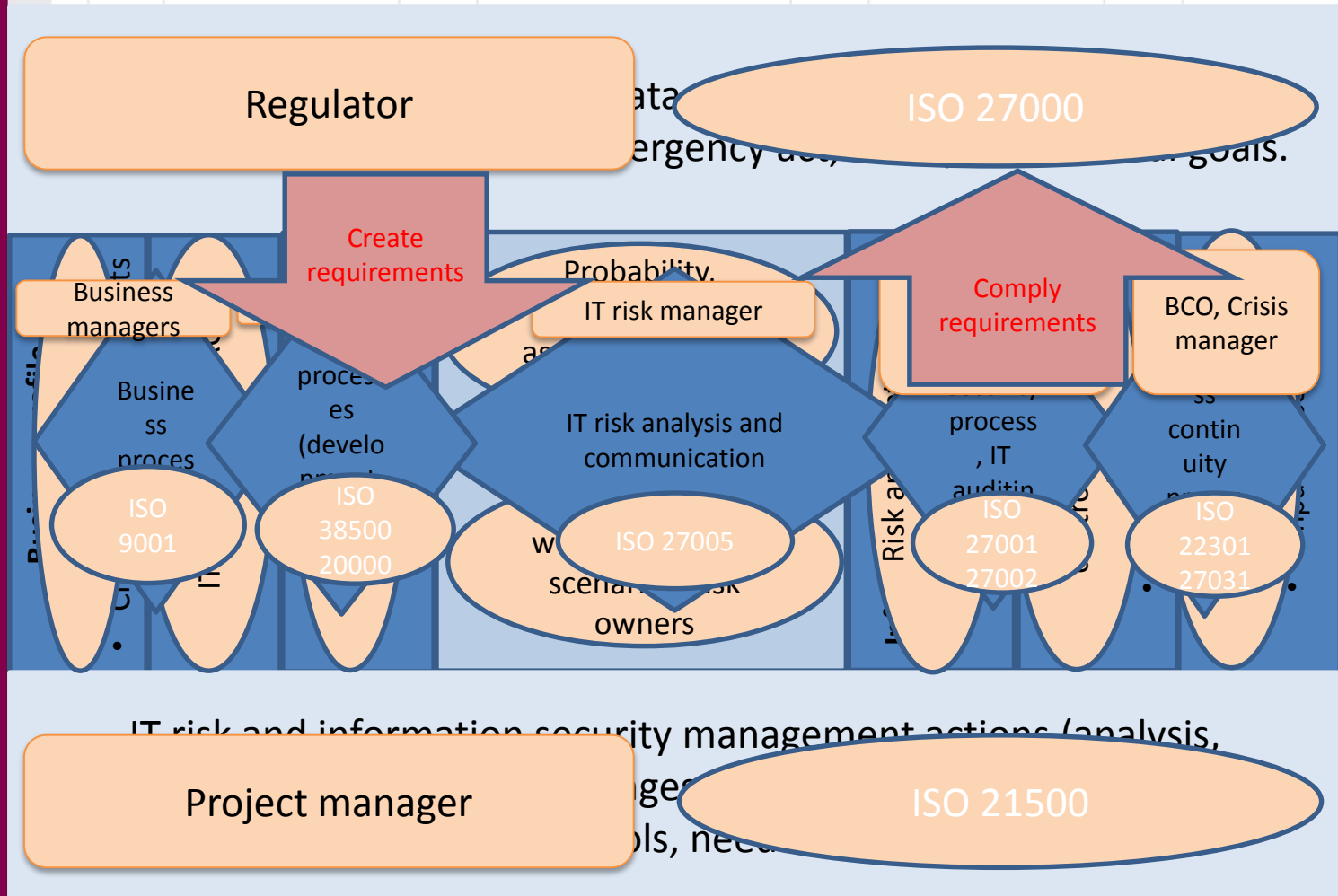


IT risk and control concept



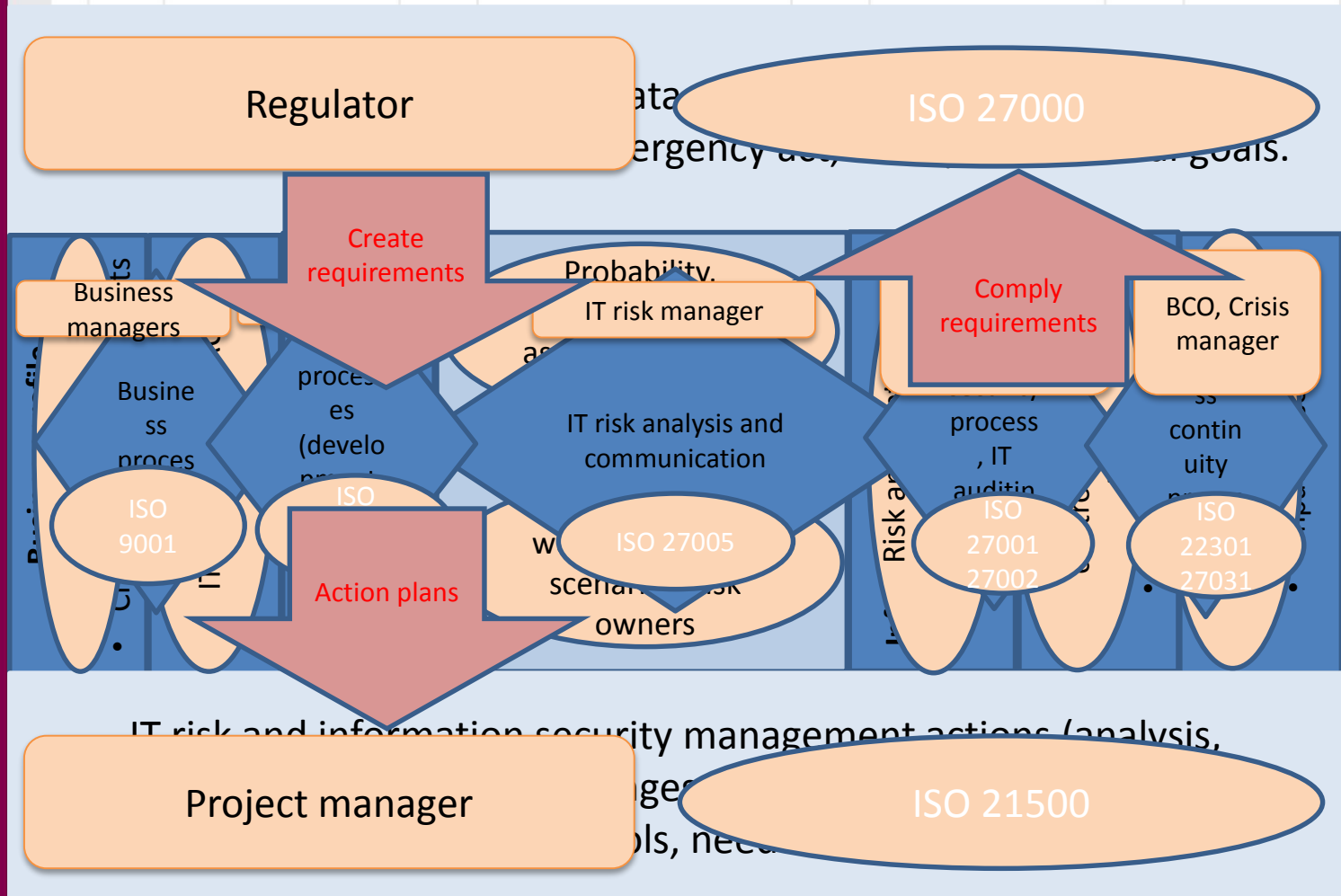


IT risk and control concept



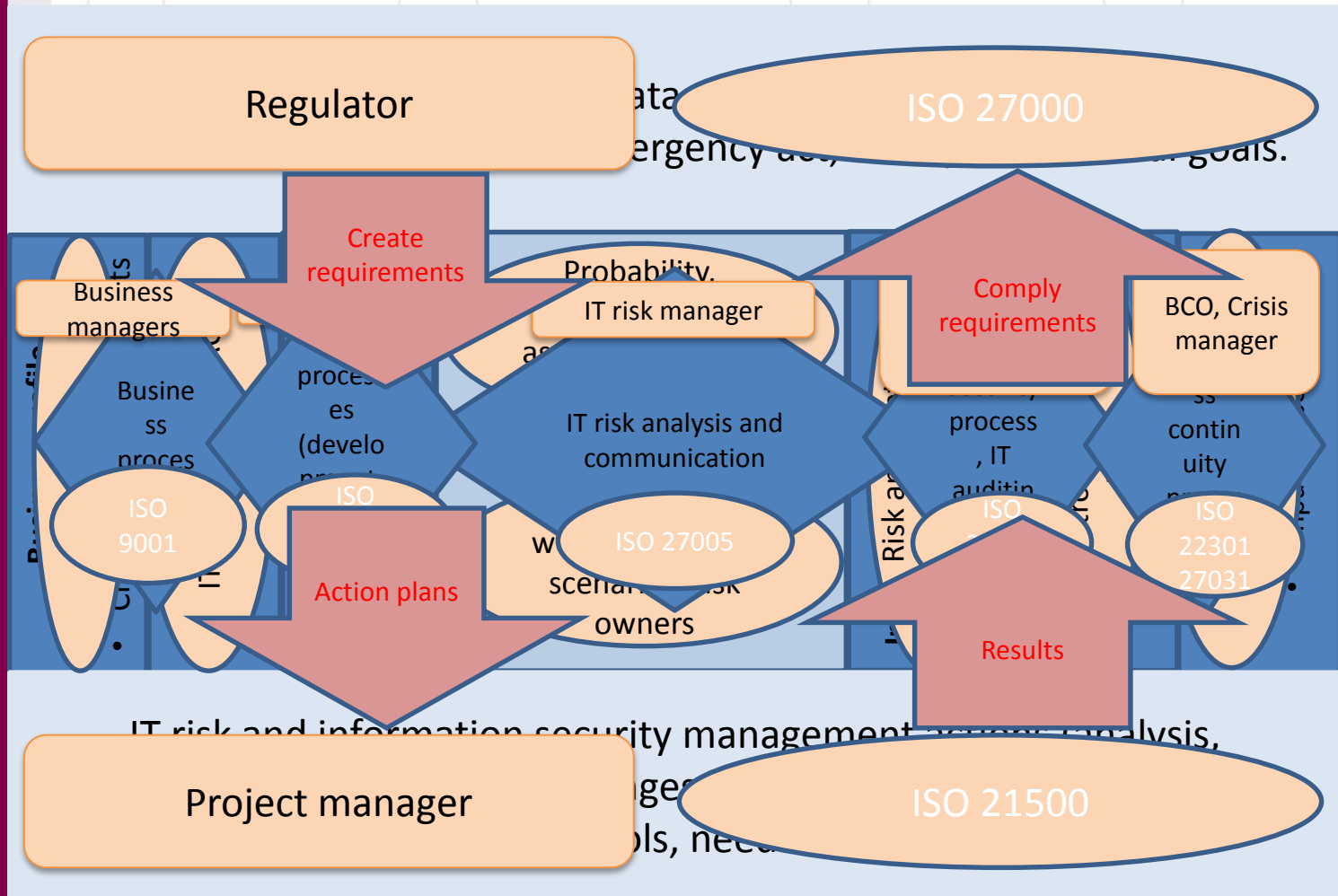


IT risk and control concept



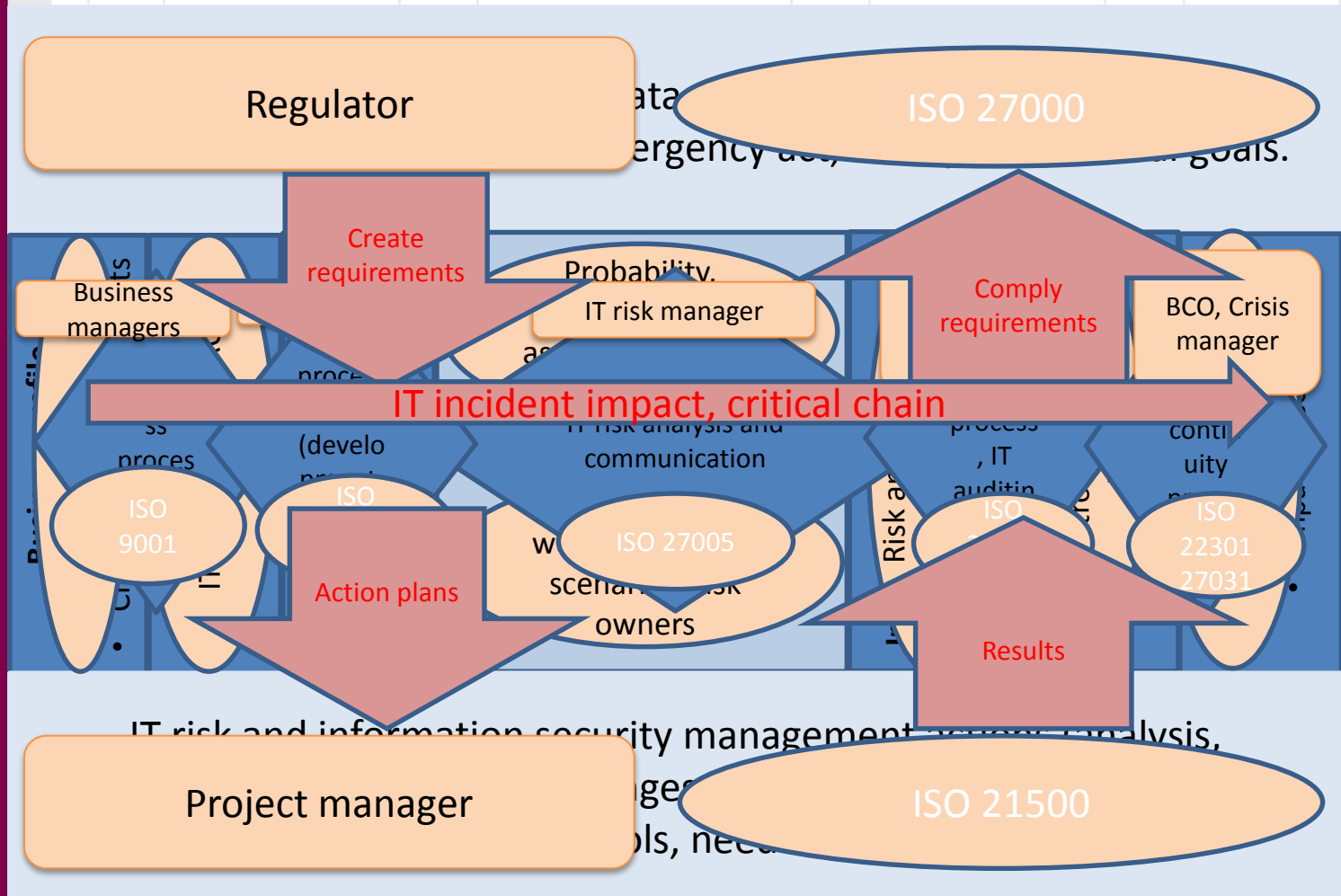


IT risk and control concept



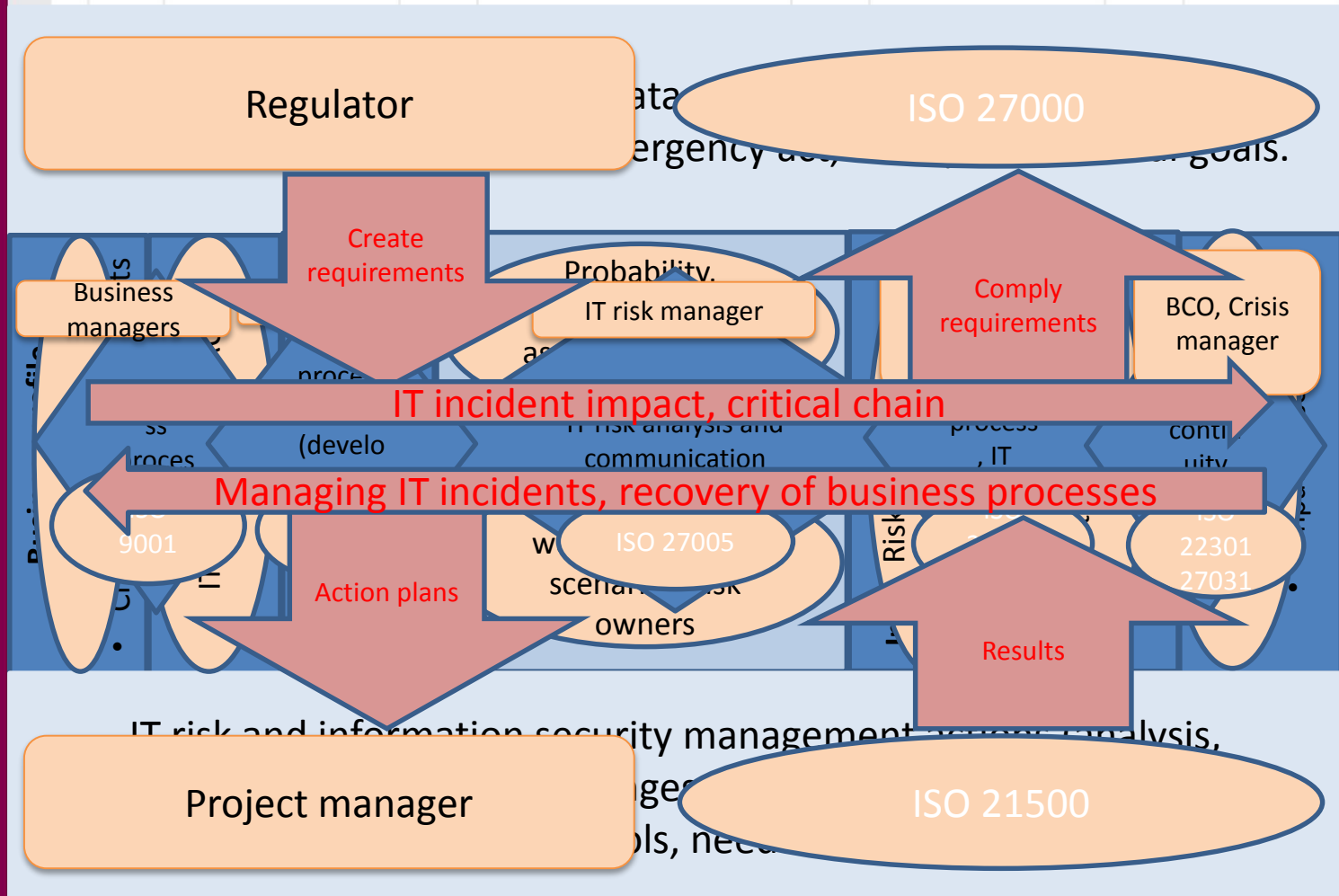


IT risk and control concept





IT risk and control concept





Business continuity

Normal management

- Strategically-driven
- Long analyzed and planned activities
- Company manager
- Organization structure
- Main location and ordinary solutions
- Formal communication

Crisis management

- Driven by current situation
- Fast and tactical decisions
- Crisis manager
- Crisis teams
- Spare parts and office solutions
- Crisis communication



Business continuity

Business Continuity (BC) is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

/ISO 22301:2012/



Disaster recovery

Disaster Recovery (DR) is the ability of an organization to provide critical Information Technology (IT) and telecommunications capabilities and services, after it is disrupted by an incident, emergency or disaster.

/BCM Institute/



BC terms

Maximum Acceptable Outage (MAO)

The duration after which an organization's viability will be threatened if an IT system or service cannot be resumed.

Recovery Time Objective (RTO)

The target time for resuming the delivery of a product or service to an acceptable level following its disruption.



BC terms

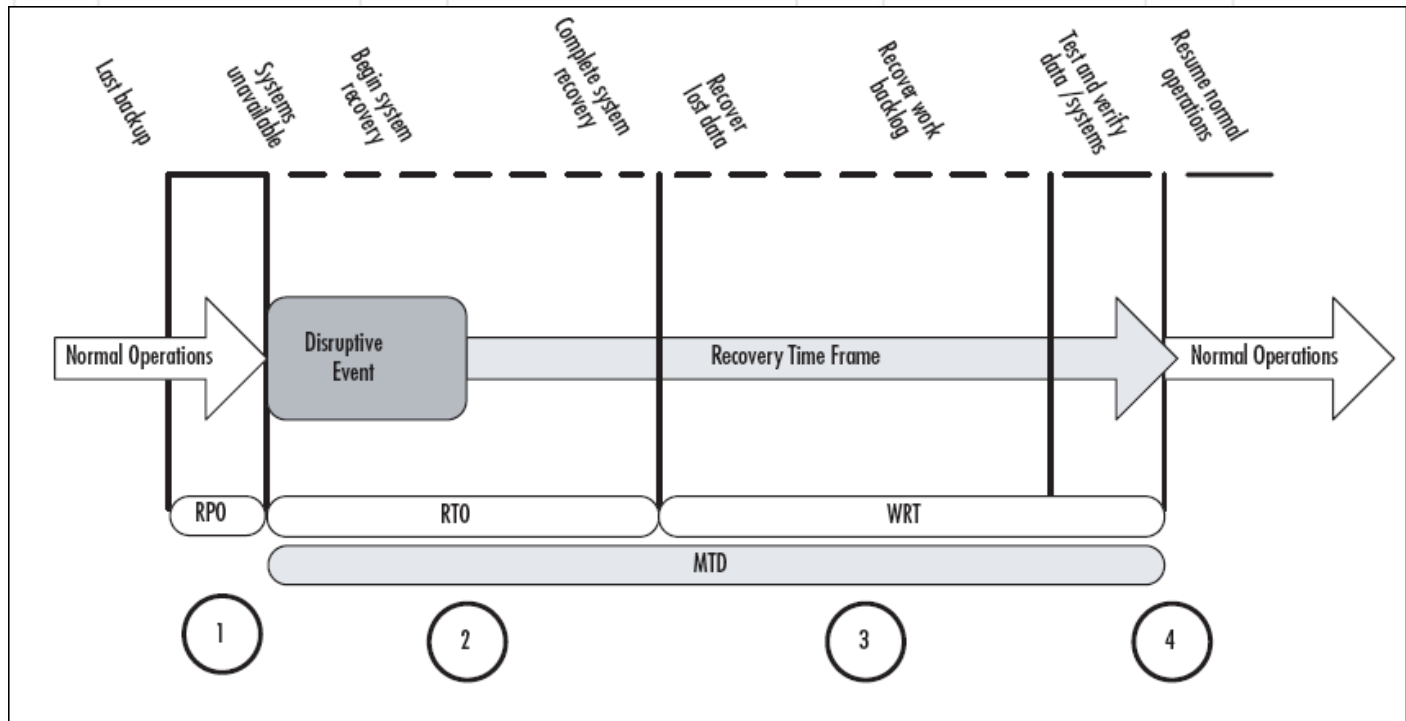
Recovery Point Objective (RPO)

The target set for the status and availability of data (electronic and paper) at the start of a recovery process.

It is a point in time at which data or capacity of a process is in a known, valid state and can safely be restored from.



BC terms





Standards

ISO 22301:2012

Societal security -- Business continuity management systems --- Requirements

ISO/IEC 27031:2011

Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity

ISO/IEC 24762:2008

Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services



BCP (DRII)

Preplanning

1. Program Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis

Planning

4. Developing Business Continuity Strategies
5. Emergency Preparedness and Response
6. Developing and Implementing Business Continuity Plans

Postplanning

7. Awareness and Training Programs
8. Business Continuity Plan Exercise, Audit, and Maintenance
9. Crisis Communications
10. Coordination with External Agencies



Practice 1

Program Initiation and Management: Summary

Establish the need for a Business Continuity Management (BCM) Program including resilience strategies, recovery objectives, business continuity, operational risk management considerations and crisis management plans. The prerequisites within this effort include obtaining management support and organizing and managing the formulation of the functions or processes required to construct the BCM framework.



Process

[Link](#)



Practice 2

Risk Evaluation and Control

Determine the risks (events or surroundings) that can adversely affect the organization and its resources (people, facilities, technologies) due to business interruption. Determine the potential loss the risks can cause and the controls needed to avoid or mitigate the effects of those risks. Complete a cost benefit analysis to justify the investment in the controls necessary to mitigate the effect of the risks.



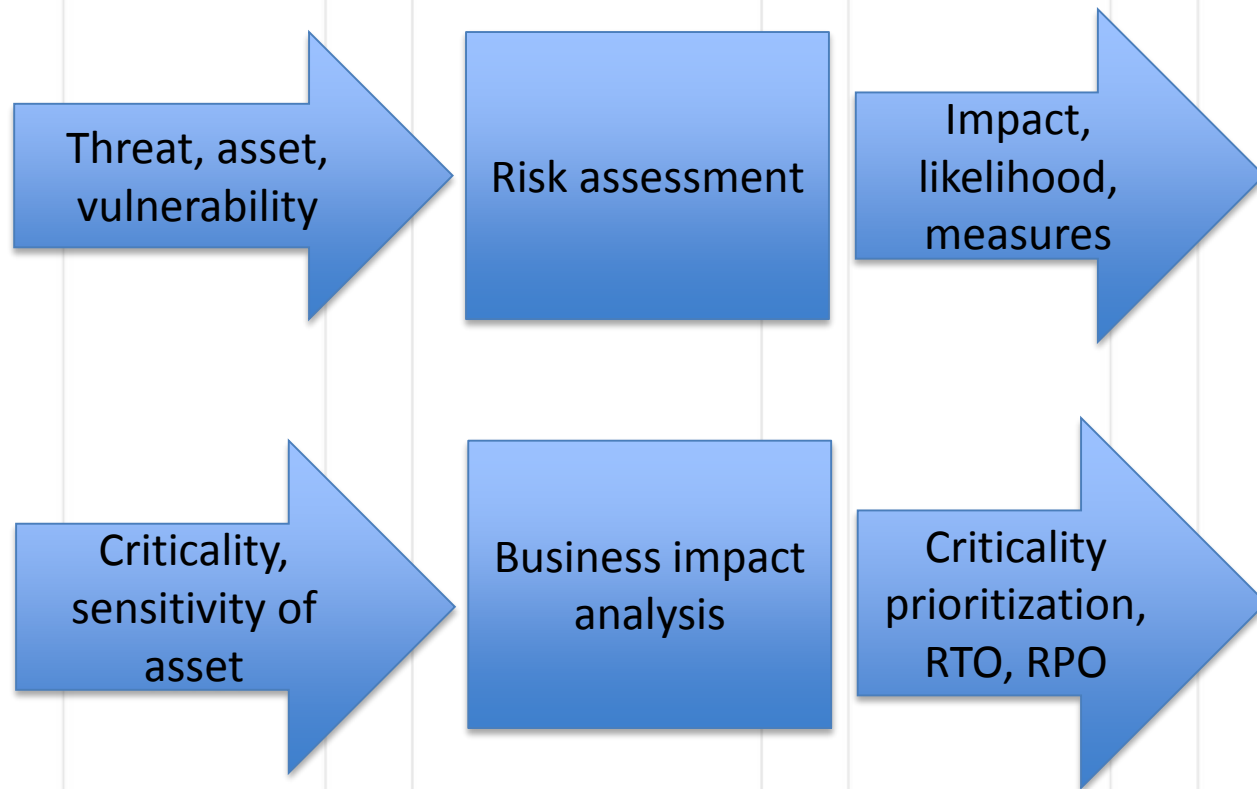
Practice 3

Business Impact Analysis

Identify the impacts resulting from business interruptions that can affect the organization and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and interdependencies so that recovery time objectives can be established and approved.



BIA





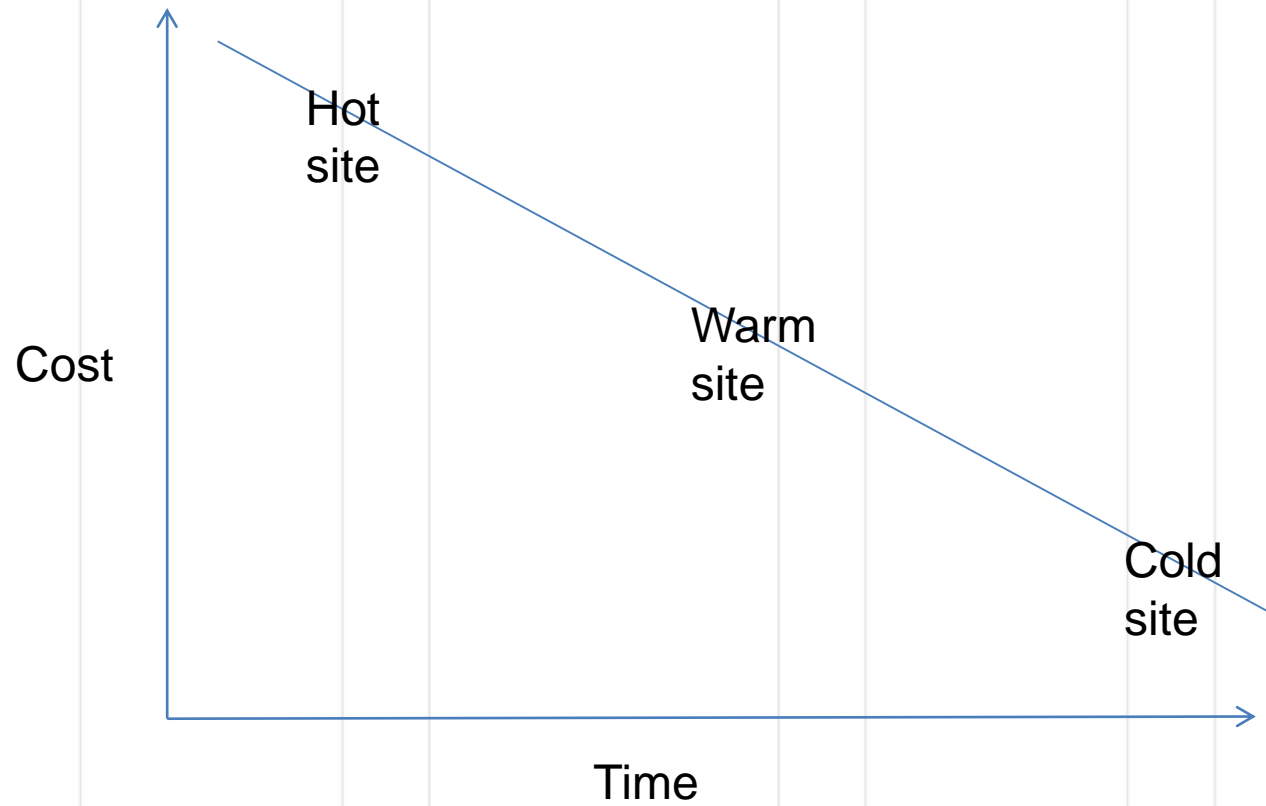
Practice 4

Business Recovery Strategies

Leverage the outcome of the BIA and Risk Evaluation to develop and recommend effective business continuity strategies. The basis for these strategies includes the consideration of both the recovery time objectives and the recovery point objectives. This will assist you in assessing and planning for the support of the organization's critical functions.



Strategy





Practice 5

Emergency Preparedness and Response

Identify the organization's readiness to respond to an emergency in a coordinated, timely and effective manner. Develop and implement the procedures for the initial response and stabilization of a situation until the arrival of the authorities which have jurisdiction (if/when).



Practice 6

Developing and Implementing Business Continuity Plans

Design, develop, and implement Business Continuity Plans that will provide continuity and/or recovery as identified by the organization's requirements.



Documentation

[Link](#)



Practice 7

Awareness and Training Programs

Prepare a program to establish and maintain corporate awareness that Business Continuity Management (BCM) is a part of normal business management, and to develop and enhance the skills required to create and implement Business Continuity Management.



Practice 8

Business Continuity Plan Exercise, Audit, and Maintenance

Establish an exercise/testing program which documents plan exercise requirements including the planning, scheduling, facilitation, communications, auditing and post review documentation. Establish a maintenance program to keep the plans current and relevant. Establish an audit process which will validate compliance with standards, review solutions, verify appropriate levels of maintenance and exercise activities, and validate the plans are correct, accurate and complete.



Testing

Test types

- Checklist Test
- Paper Test
- Tabletop Test
- Partial Walkthrough Test
- Walkthrough Test



Practice 9

Crisis Communication

Establish applicable procedures and policies for coordinating the continuity and restoration activities with external agencies (local, regional, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes and regulations.



Practice 10

Coordination with External Agencies

Establish applicable procedures and policies for coordinating the continuity and restoration activities with external agencies (local, regional, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes and regulations.



Practice

Exercise XI

PhD Andro Kull

CISA, CISM, CRISC, ABCP

E-mail: Andro@consultit.ee

Skype: andro.kull

