TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

III

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)

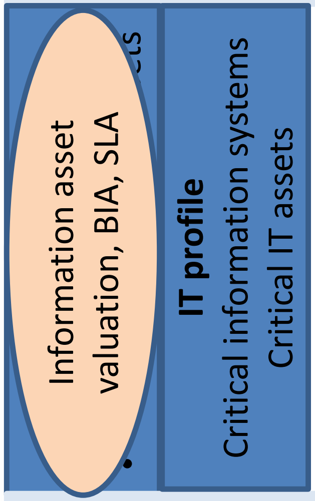
Practical info

Course page

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

Concept progress

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

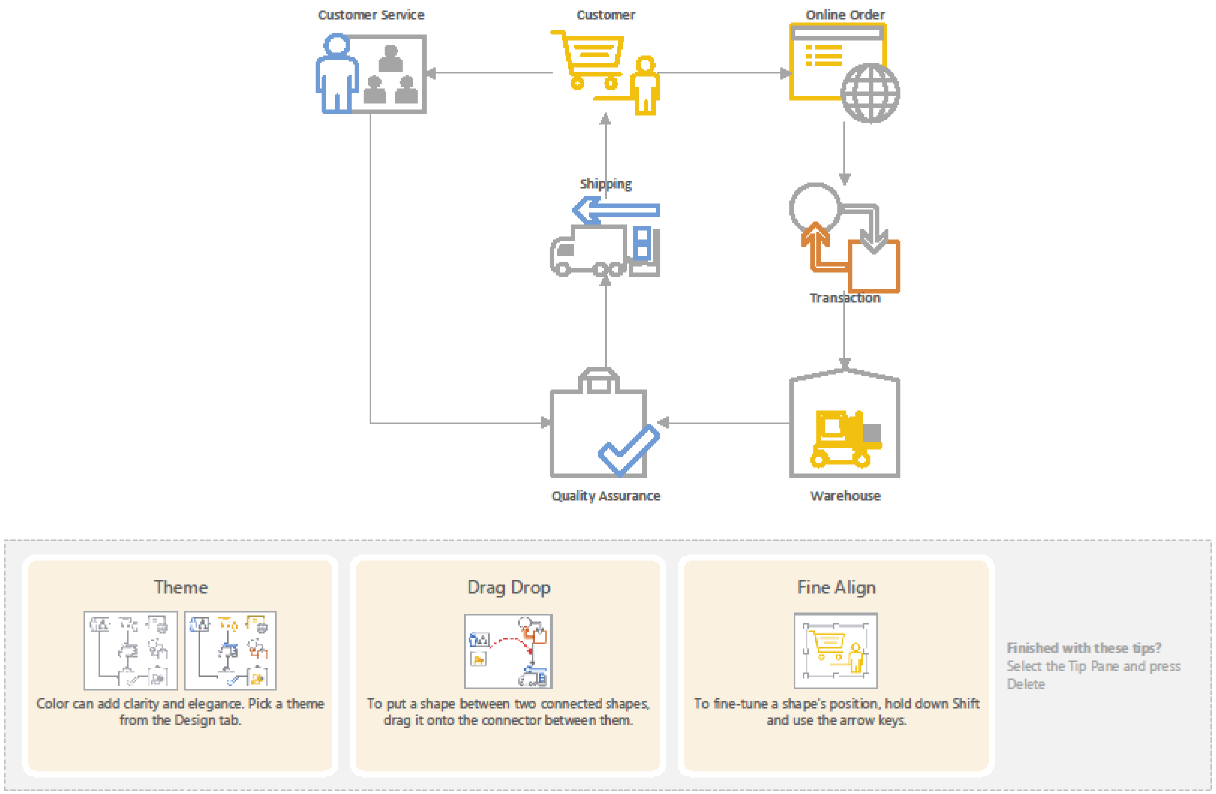


Information asset valuation, BIA, SLA

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 …)

BP model – Visio example



Theme

Color can add clarity and elegance. Pick a theme from the Design tab.

Drag Drop

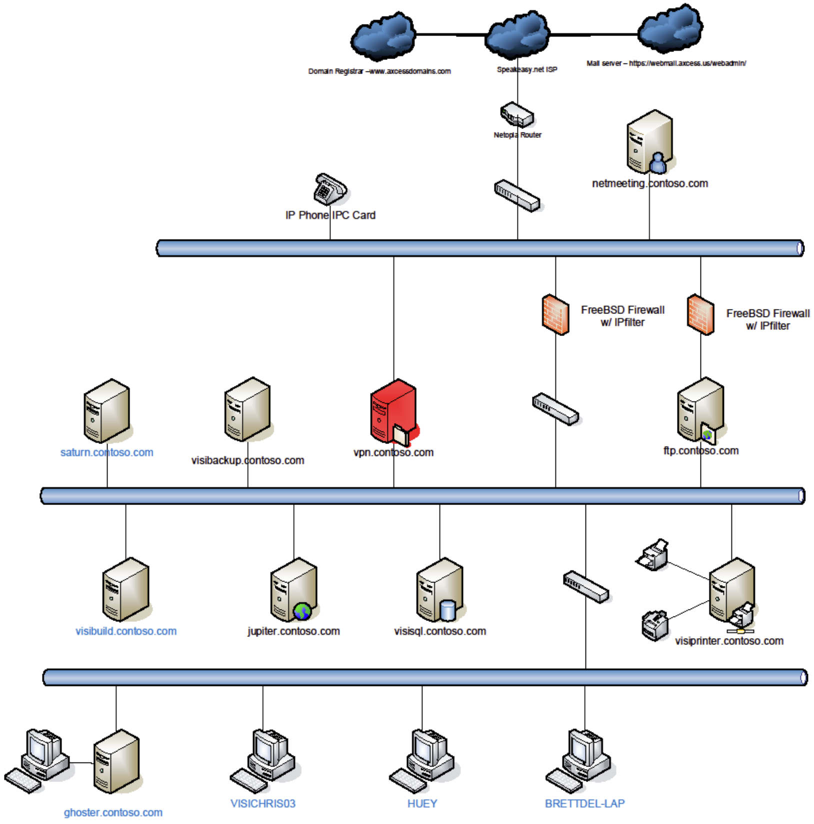
To put a shape between two connected shapes, drag it onto the connector between them.

Fine Align

To fine-tune a shape's position, hold down Shift and use the arrow keys.

Finished with these tips? Select the Tip Pane and press Delete

IT infra – Visio example



Protection requirements (BSI)

"Normal"	The impact of any loss or damage is limited and calculable.
"High"	The impact of any loss or damage may be considerable.
"Very High"	The impact of any loss or damage may be of catastrophic proportions which could threaten the very survival of the organisation.

Protection requirements (Normal)

1. Violations of laws, regulations, or contracts	Violations of regulations and laws with minor consequences Minor breaches of contract which result in at most minor contractual penalties
2. Impairment of the right to informational self-determination	This deals with personal data whose processing could adversely affect the social standing or financial wellbeing of those concerned.
3. Physical injury	Does not appear possible.
4. Impaired ability to perform tasks	Impairment was assessed to be tolerable by those concerned. The maximum acceptable downtime is greater than 24 hours.
5. Negative internal or external effects	Only minimal impairment or only internal impairment of the reputation / trustworthiness of the organisation is expected.
6. Financial consequences	The financial loss is acceptable to the organisation.

Protection requirements (High)

1. Violation of laws, regulations or contracts	Violations of regulations and laws with substantial consequences Major breaches of contract with high contractual penalties
2. Impairment of the right to informational self-determination	This aspect deals with personal data whose processing could have a seriously adverse affect on the social standing or financial well-being of those concerned.
3. Physical injury	Physical injury to an individual cannot be absolutely ruled out.
4. Impaired ability to perform tasks	Impairment of the ability to perform the tasks at hand was assessed as intolerable by some of the individuals concerned. The maximum acceptable down time is between one and 24 hours.
5. Negative internal or external effects	Considerable impairment of the reputation / trustworthiness can be expected.
6. Financial consequences	The financial loss is considerable, but does not threaten the existence of the organisation.

Protection requirements (Very high)

1. Violation of laws, regulations or Contracts	Fundamental violations of regulations and laws Breaches of contract with ruinous damage liabilities
2. Impairment of the right to informational self-determination	This aspect deals with personal data whose processing could result in the injury or death of the persons concerned or that could endanger the personal freedom of the persons concerned.
3. Physical injury Serious injury to an individual is possible	There is a danger to life and limb.
4. Impaired ability to perform tasks	Impairment of the ability to perform tasks was assessed as intolerable by all individuals concerned. The maximum acceptable down time is less than one hour.
5. Negative internal or external effects	A nation-wide or state-wide loss of reputation / trustworthiness is conceivable, possibly even endangering the existence of the organisation.
6. Financial consequences	The financial loss threatens the existence of the organisation.

Classification

K0 - Availability - less than 80% per year; the length of a single failure may be greater than 24 hours;

K1 - Availability - greater than or equal to 80% and less than 99% per year; single outage may have a length 4-24 hours;

K2 - Availability - equal to or higher than 99% and less than 99.9% per year; single outage may have a length 1-4 hours;

K3 - Availability - more and equal to 99.9% per year; single outage may have a length 0-1 hours.

Classification

T0 - Integrity – detectability of a source of information, modification or destruction is not important; controls about information accuracy, completeness and timeliness are not necessary;

T1 - Integrity - the information source, modification and destruction shall be detectable; information accuracy, completeness, timeliness, appropriateness controls in specific cases;

T2 - Integrity - the information source, modification and destruction shall be detectable; periodic inspections about information accuracy, completeness and timeliness needed;

T3 - Integrity – the information source, modification and destruction shall have evidential value; real time control about information accuracy, completeness and timeliness needed.

Classification

S0 - Confidentiality - public information: access to information is not restricted (ie, read all interested parties, the right to change comes from integrity requirement);

S1 - Confidentiality - information for internal use: access to information is permitted, access to the person needs legitimate interest;

S2 - Confidentiality - secret information: the use permitted only to certain groups of users, access to the person needs legitimate interest;

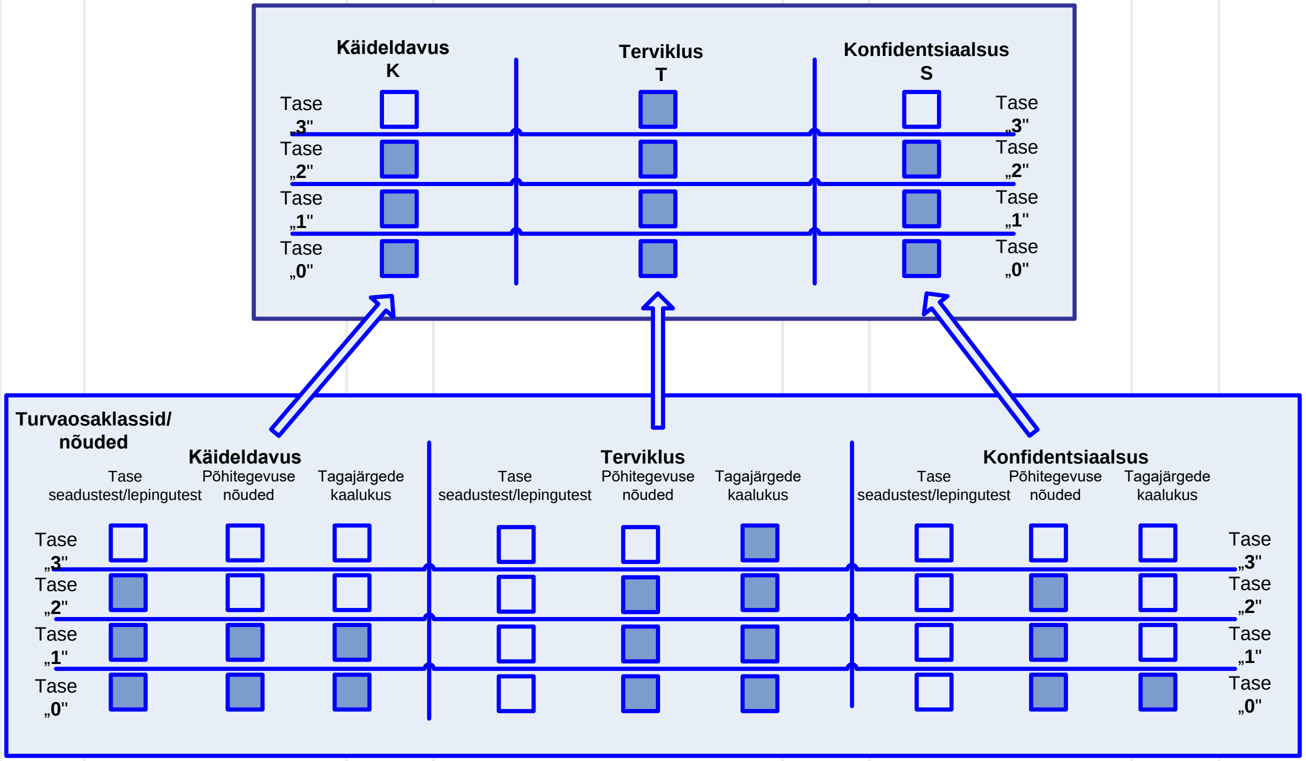
S3 - Confidentiality - top secret information: the use permitted only to certain users, access to the person needs legitimate interest.

Classification

Sources

- Laws and contractual claims
- Main activity/business processes requirements
- Assessment of the consequences

Grading



	Käideldavus K	Terviklus T	Konfidentsiaalsus S	
Tase „3"	□	■	□	Tase „3"
Tase „2"	■	■	■	Tase „2"
Tase „1"	■	■	■	Tase „1"
Tase „0"	■	■	■	Tase „0"

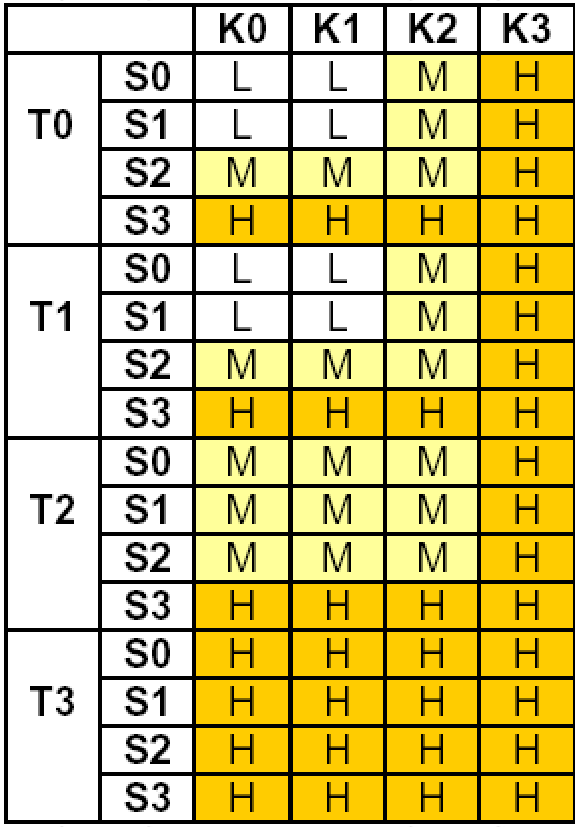
Turvaosaklassid/ nõuded	Käideldavus			Terviklus			Konfidentsiaalsus			
	Tase seadustest/lepingutest	Põhitegevuse nõuded	Tagajärgede kaalukus	Tase seadustest/lepingutest	Põhitegevuse nõuded	Tagajärgede kaalukus	Tase seadustest/lepingutest	Põhitegevuse nõuded	Tagajärgede kaalukus	
Tase „3"	□	□	□	□	□	■	□	□	□	Tase „3"
Tase „2"	■	□	□	□	■	■	□	■	□	Tase „2"
Tase „1"	■	■	■	□	■	■	□	■	□	Tase „1"
Tase „0"	■	■	■	□	■	■	□	■	■	Tase „0"

Grading

Security class is a combination of security levels.

The number of combinations - 4x4x4 = 64.

Example: K2T3S2=H.



		K0	K1	K2	K3
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

Terms

Service Level Agreement (SLA)

A service-level agreement is simply a document describing the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved.

www.cio.com

Terms

Business Impact Analysis (BIA) on an information system

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable.

csrc.nist.gov

Terms

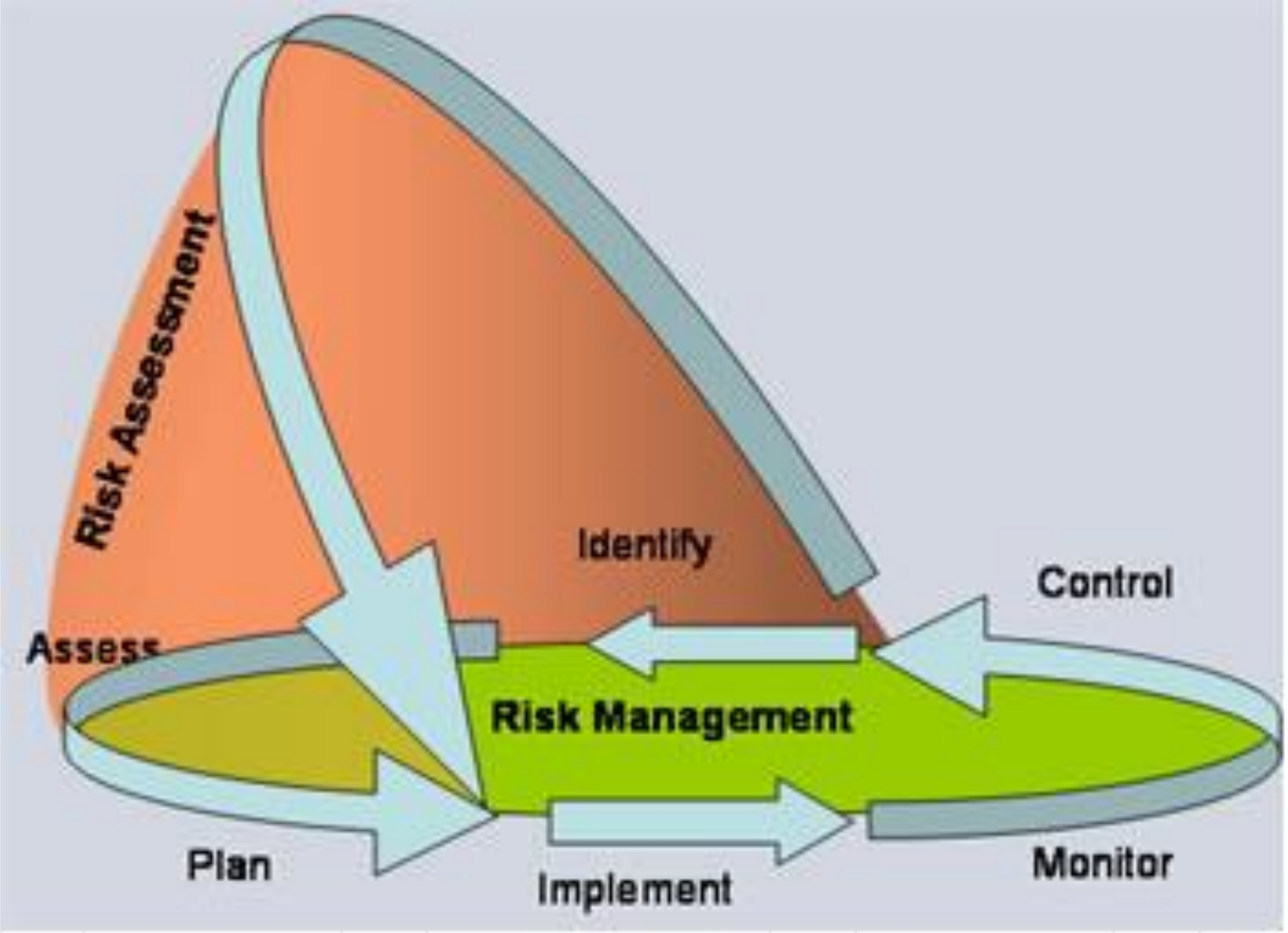
Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations.

Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.

Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

csrc.nist.gov

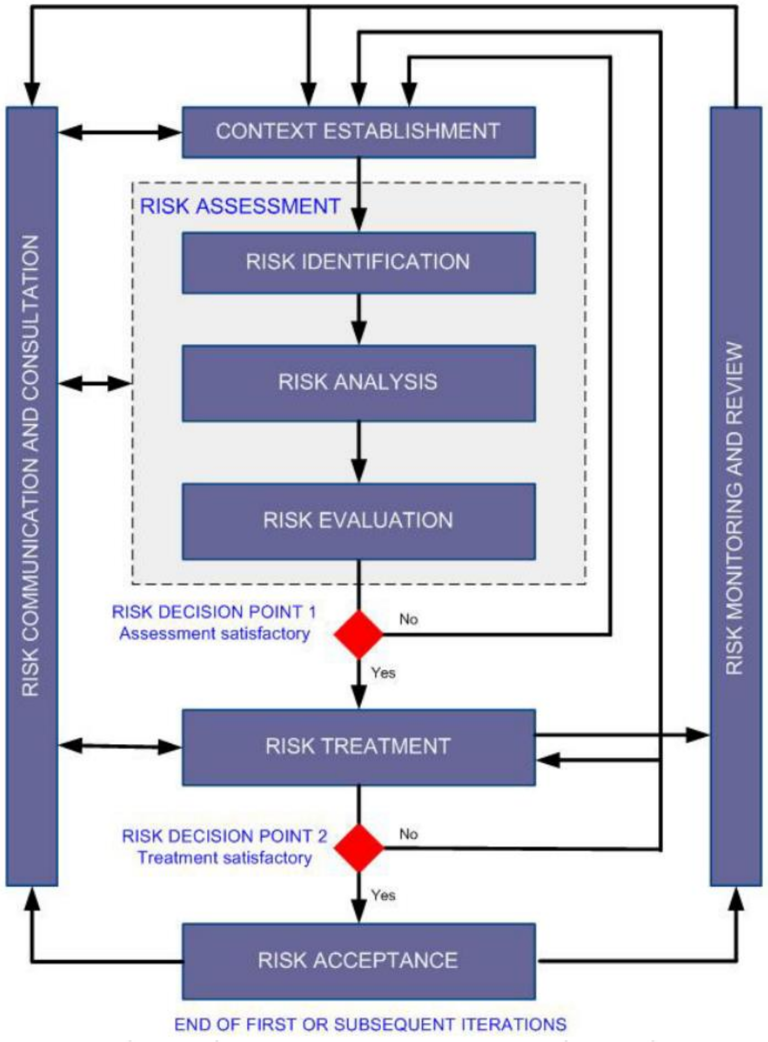
Process (SANS)



ISO standards

- ISO/IEC 27005:2011 provides guidelines for information security risk management.
- It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
- Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2011.
- ISO/IEC 27005:2011 is applicable to all types of organizations which intend to manage risks that could compromise the organization's information security.

Process 27005



Context establishment

Criteria include the risk evaluation, risk acceptance and impact evaluation criteria:

- legal and regulatory requirements
- the strategic value for the business of information processes
- stakeholder expectations
- negative consequences for the reputation of the organization

Risk identification

Risk identification states what could cause a potential loss; the following are to be identified:

- assets, primary (i.e. Business processes and related information) and supporting (i.e. hardware, software, personnel, site, organization structure)
- threats
- existing and planned security measures
- vulnerabilities
- consequences
- related business processes

Risk analysis

Risk analysis (estimation) has as input the output of risk analysis and can be split in the following steps:

- assessment of the consequences through the valuation of assets
- assessment of the likelihood of the incident (through threat and vulnerability valuation)
- assign values to the likelihood and consequence of the risks

Risk evaluation

The risk evaluation process receives as input the output of risk analysis process. It compares each risk level against the risk acceptance criteria and prioritize the risk list with risk treatment indications.

Risk treatment and acceptance

The risk treatment process aim at selecting security measures to:

- reduce
- retain
- avoid
- transfer

risk and produce a risk treatment plan, that is the output of the process with the residual risks subject to the acceptance of management.

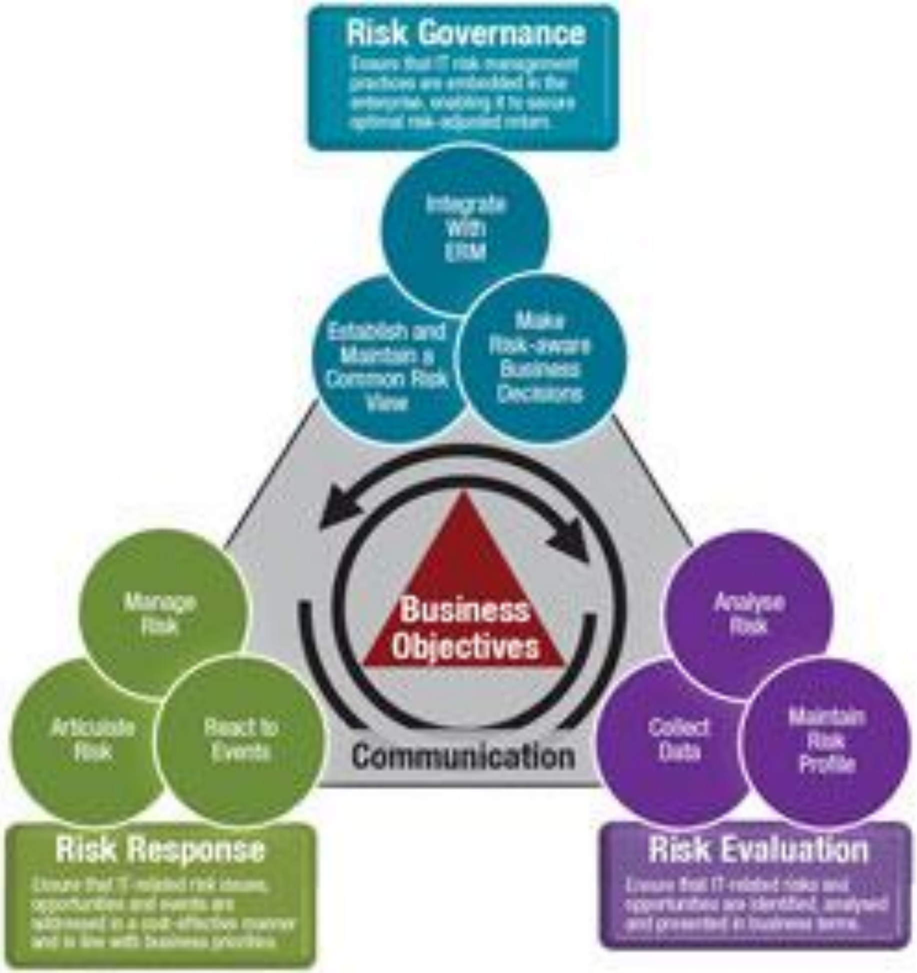
Risk communication

Risk communication is a horizontal process that interacts bidirectionally with all other processes of risk management. Its purpose is to establish a common understanding of all aspect of risk among all the organization's stakeholder.

Risk monitoring and review

Risk management is an ongoing, never ending process. Within this process implemented security measures are regularly monitored and reviewed to ensure that they work as planned and that changes in the environment rendered them ineffective. Business requirements, vulnerabilities and threats can change over the time.

Best practice (RiskIT)


Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
Integrate With ERM
Establish and Maintain a Common Risk View
Make Risk-aware Business Decisions
Business Objectives
Communication
Manage Risk
Articulate Risk
React to Events
Risk Response
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Analyse Risk
Collect Data
Maintain Risk Profile
Risk Evaluation
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

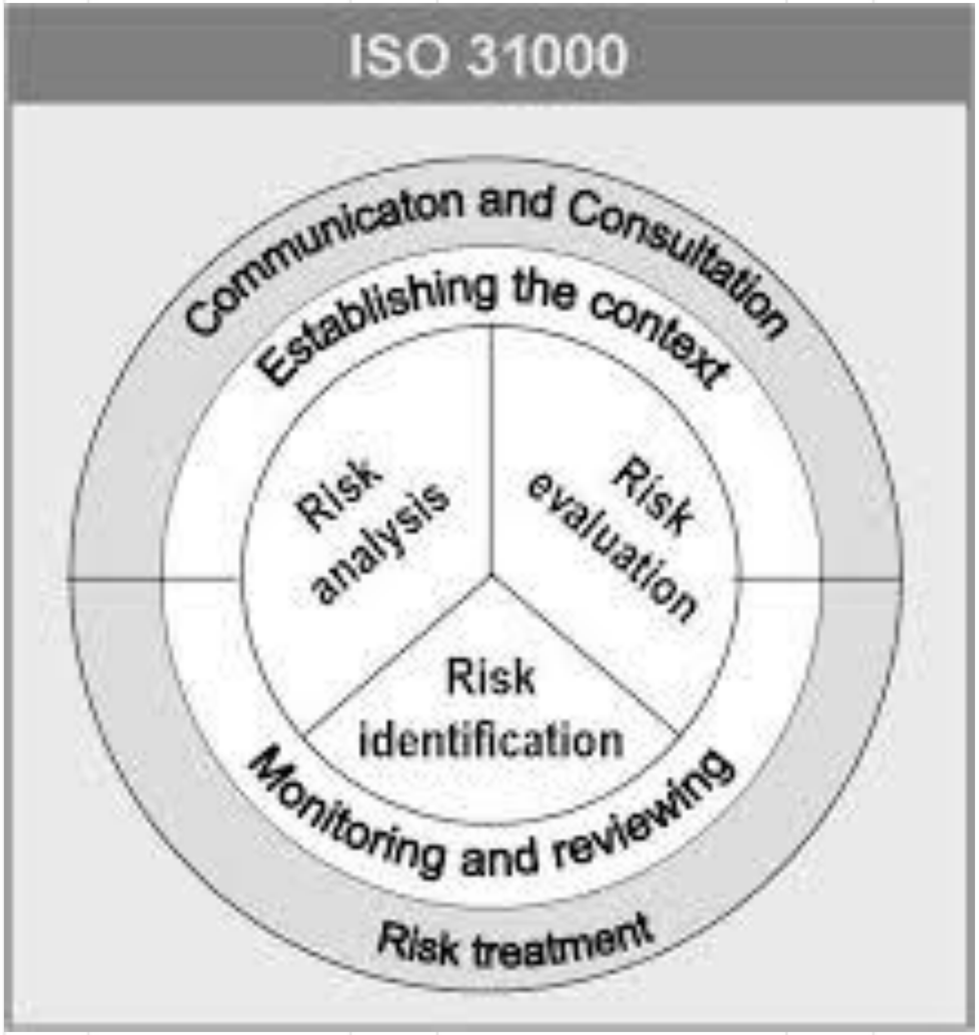
Best practice (RiskIT)

Risk IT provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues.

Best practice (RiskIT)

Risk IT was published in 2009 by ISACA. It is the result of a work group composed by industry experts and some academics of different nations, coming from organizations such as IBM, PricewaterhouseCoopers, Risk Management Insight, Swiss Life, and KPMG.

Standard (ISO 31000)



Standard (ISO 31000)

ISO 31000 is intended to be a family of standards relating to risk management codified by the International Organization for Standardization. The purpose of ISO 31000:2009 is to provide principles and generic guidelines on risk management.

Standard (ISO 31000)

ISO 31000 seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies and paradigms that differed between industries, subject matters and regions.

Self reading

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) – methodology

Practice

Asset inventory

HW example

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