TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

VII

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

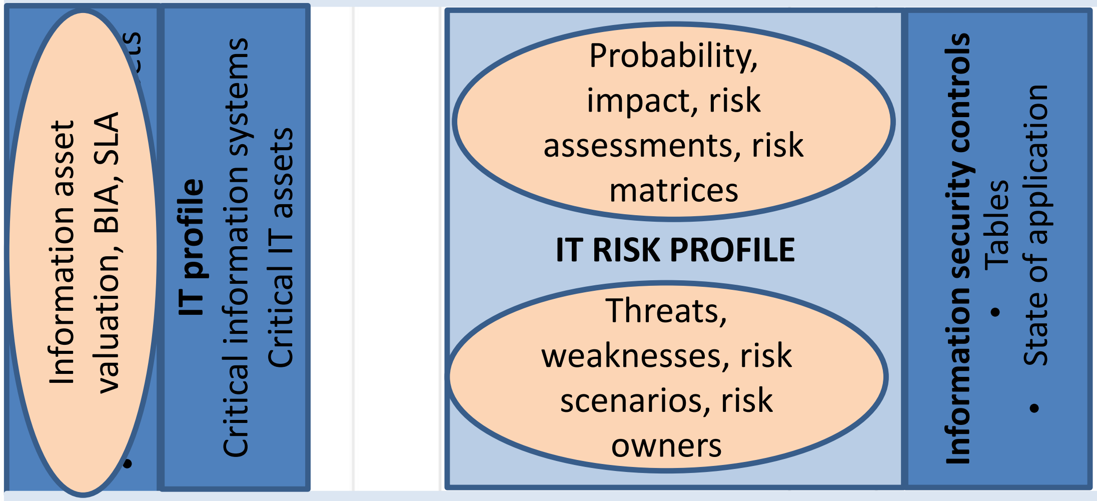
Practical info

Course page

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

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

Probability, impact, risk assessments, risk matrices

IT RISK PROFILE

Threats, weaknesses, risk scenarios, risk owners

Information security controls

- Tables
- State of application

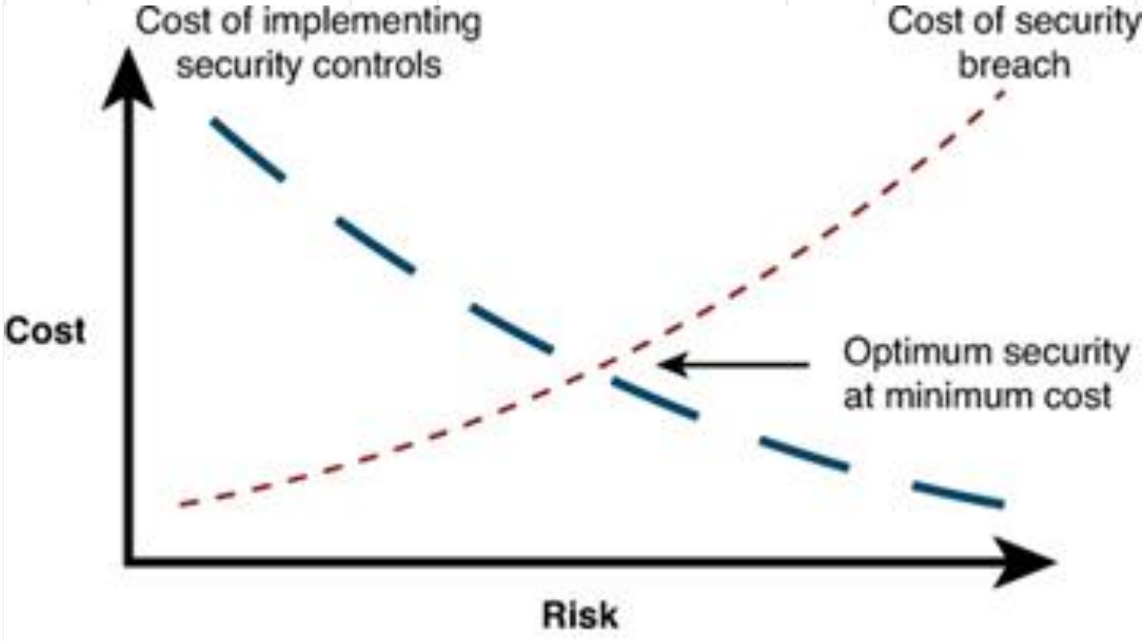
IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc …)

Risk management

Why do we assess risk?

- To inform a proper balance of safeguards against risk of failing to meet business objectives.
- Inform a position so that:
  - Removal of safeguards will increase the risk of loss to an unacceptable level
  - Adding any safeguards would make the security system too expensive/bureaucratic
- ... and therefore it is a means by which expenditure on security and contingency can be justified

Risk and security cost



Analysis of cost vs. risk
Cost of implementing security vs. cost of security breach

www.ciscopress.com

IS risk assessment

Information Security Risk Assessment

- Organization must define a risk assessment process which includes criteria for performing risk assessments

What triggers the need for a risk assessment?

- The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria

Risk treatment

- Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment.
- Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks

Decision

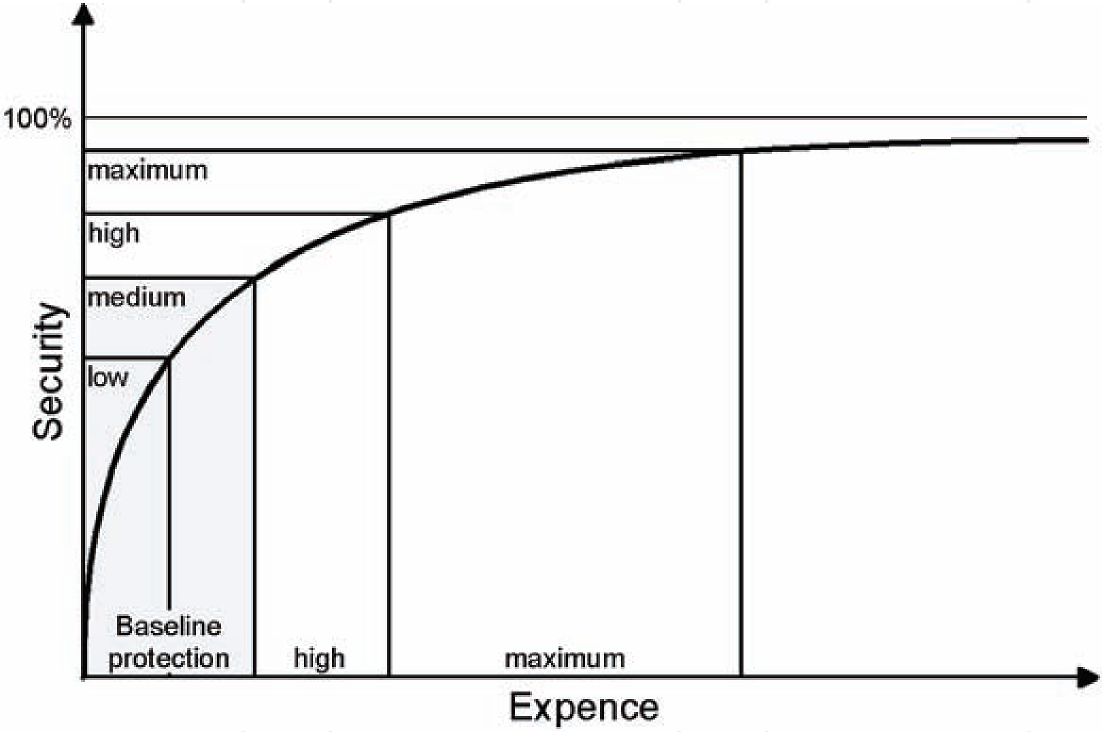
Options for risk decision

- Terminate the risk (eliminate, reject, avoid)
- Tolerate (accept, retention, retain)
- Treat (reduce)
- Transfer (share), for example insurance, outsourcing and SLA terms

Treatment

- Risk acceptance criteria should consider business, legal, operational, technological, financial and social requirements
- Other risks to be handled
- If treat, controls are either:
  - Already in place and need enhancing, ensuring consistent and measures aligned
  - Need to be introduced

Security expences



Risk assurance

- Agree approach to risk management
- Degree of assurance required
- Conduct risk assessment
- Ensure those involved understand the methodology to ensure comparable and reproducible results
- Manage risk to level of assurance required using controls

Need for ISMS

Some driving questions

- Do you have information you rely on or which needs to be kept confidential (business secrecy)?
- Do you collect personal information? (customers and/or employees)
- Does your business rely on IT for daily activities?
- Does anyone need confidence in your information handling measures?
- Can you afford reputation damage because of security incident?

ISMS

Management system for IS

- satisfy the information security requirements of customers and ohter stakeholders;
- improve an organization's plans and activities;
- meet the organization's information security objectives;
- comply with regulations, legislation and industry mandates; and
- manage information assets in an organized way that facilitates continual improvement and adjustment to current organisational goals.

/ISO 27000:2014, section 3.2.5/

IS controls

Controls implementation

- requirements and constraints of national and international legislation and regulations;
- organizational objectives;
- operational requirements and constraints;
- their cost of implementation and operation in relation to the risks being reduced, and remaining proportional to the organization’s requirements and constraints;

/ISO 27000:2014, section 3.5.5/

IS controls

- they should be implemented to monitor, evaluate and improve the efficiency and effectiveness of information security controls to support the organization’s aims
- the selection and implementation of controls should be documented within a statement of applicability to assist with compliance requirements
- the need to balance the investment in implementation and operation of controls against the loss likely to result from information security incidents

/ISO 27000:2014, section 3.5.5/

Terms

Control

- measure that is modifying risk (controls include any process, policy, device, practice, or other actions which modify risk)

Control objective

- statement describing what is to be achieved as a result of implementing controls

Standards

ISO/IEC 27000:2014

- Information Security Management Systems (ISMS) Overview and Vocabulary

ISO/IEC 27001:2013

Specification for ISMS

ISO/IEC 27002:2013

code of practice for information security controls

27001

…

4. Context of organisation
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Continual improvement

…

ISMS success

- awareness of the need for information security;
- assignment of responsibility for information security;
- incorporating management commitment and the interests of stakeholders;
- enhancing societal values;
- risk assessments determining appropriate controls to reach acceptable levels of risk;

/ISO 27000:2014, section 3.2.1/

ISMS success

- security incorporated as an essential element of information networks and systems;
- active prevention and detection of information security incidents;
- ensuring a comprehensive approach to information security management; and
- continual reassessment of information security and making of modifications as appropriate

/ISO 27000:2014, section 3.2.1/

Organization

- Management owns information security, approves the policy
- Departments are responsible for their own processes, risks and countermeasures
- Everyone has a role with respect to the Organisation’s information security stance
- Project team coordinate tasks to deliver project
- Risk assessors and project team identify and evaluate risks
- Risk owners coordinate controls to mitigate risks and accept residual risk

Roles

RASCI:

- Responsible
- Accountable
- Supportive
- Consulted
- Informed

RASCI

Section of ISO/IEC 27002:2013 R = Responsible A = Accountable S = Supportive C = Consulted I = Informed		Asset Owners	Staff	CEO	Executive	Steering	IS manager	OP	HR	Proc	Compliance	Fin	Facilities	CIO	R&D
5	Information security policies														
5.1.1	Policies for information security	C	I	C	A	S	R	S	C	S	C	C	C	S	C
5.1.2	Review of the policies for information security	C		S	A	R	S	C	S	S	S	S	C	S	S
6	Organizing information security														
6.1.1	Information security roles and responsibilities	A	I		R	S	C		C		C			C	C
6.1.2	Segregation of duties	A	I		C	R	C							C	
6.1.3	Contact with authorities	A			C	S	S				R				
6.1.4	Contact with special interest groups	A			C	C	R				S			S	
6.1.5	Information security in project management	A			C	R	S							S	
6.2.1	Mobile device policy	A	I		C	R	S	C						C	
6.2.2	Teleworking	A	I		R	S	C	C						C	

Documentation

Documents Required by ISO27001

Scope, Information security policy, Information security risk assessment process, Information security risk treatment Process, Statement of Applicability, Information security objectives, Evidence of competence, That ‘determined by the organization as being necessary for the effectiveness of the information security management system’, The extent necessary to have confidence that the processes required for operational planning and control have been carried out as planned.

Documentation

Results of information security risk Assessments, Results of information security risk treatment, Evidence of the information security performance monitoring and measurement results, Internal audit programme(s) and the audit results, *Internal audit procedure,* Evidence of the results of management reviews, Evidence of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective actions.

Hierarchy

Policy (why and aim)
Manual, statement of applicability
Procedures (who, what, where and when)
Work instructions and training documents (how)
forms, records forms, records forms, records, forms

Scope

Who requires what assurance?

- Processes involved;
- Assets used in those processes;
- Where else are those assets used/accessed from?
- Include in considerations:
  - All sites;
  - All staff;
  - All time.

Leadership

Top management leadership and commitment

1. Ensuring information security policy and objectives are established and are compatible with strategic direction;
2. Ensuring integration of ISMS into organization’s processes;
3. Ensuring resources needed for ISMS are available;
4. Communicating importance of effective information security management and of conforming to ISMS;
5. Ensuring the ISMS achieves its intended outcome(s);
6. Directing and supporting persons to contribute to the effectiveness of the ISMS;
7. Promoting continual improvement;
8. Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Practice

Exercise VIII

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