



TALLINN UNIVERSITY OF
TECHNOLOGY



Information and Cyber Security Assurance in Organisations

ITX8090

IVCM13



Self-introduction

- Education
- Work experience
- Training
- Teaching



Audience and expectations

Expectations for the course?

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.



Course

Outline

- Cyber security as a process;
- IS life cycle;
- Choosing security measures based on security model/standard/best practice;
- Graded security model;
- Security expences and optimization;
- Cooperation at organization/state/international level.

ois.ttu.ee



Course

Knowledge

- Terminology, security problem description
- Understand security as a process
- What may work for security governance
- Security economic aspects and cost optimization

ois.ttu.ee



Evaluation

Evaluation criteria

- 1) Homework assignments** The course contains several obligatory homework assignments. Assignments are supervised and graded during practice times. Maximum summary points for all assignments: 20.
- 2) Exam** In order to pass the course, each student has to pass the written exam. Maximum points: 80.
- 3) 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)



Introduction

Information and Cyber Security Assurance in Organisations

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

www.wikipedia.org



IT risk and control concept



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

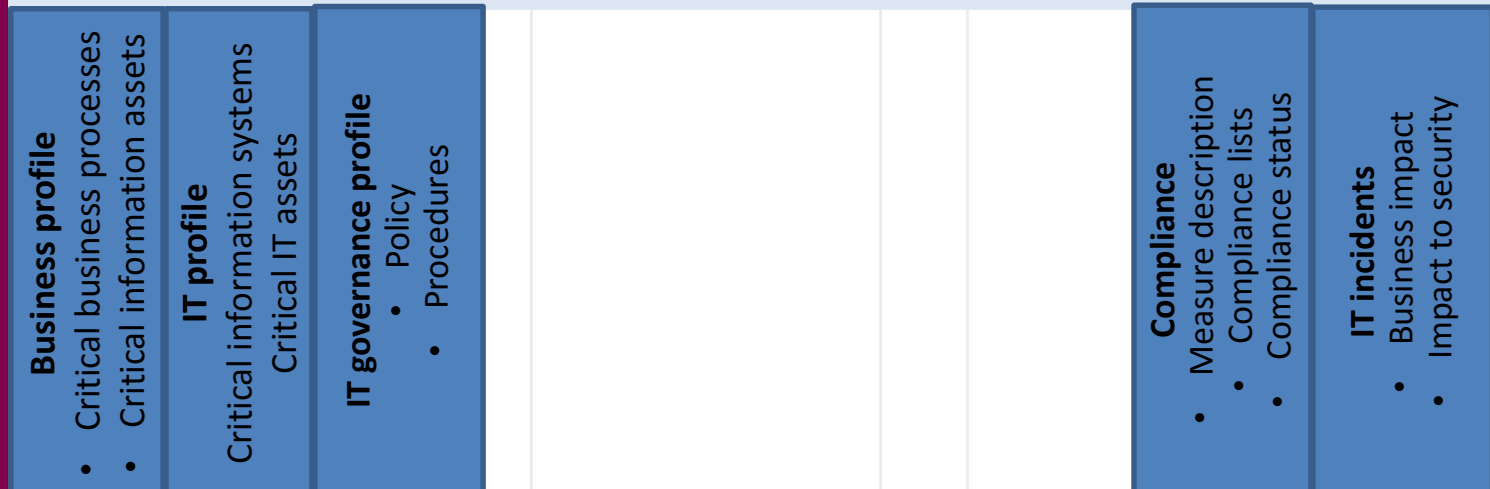
- Business impact
- Impact to security

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.

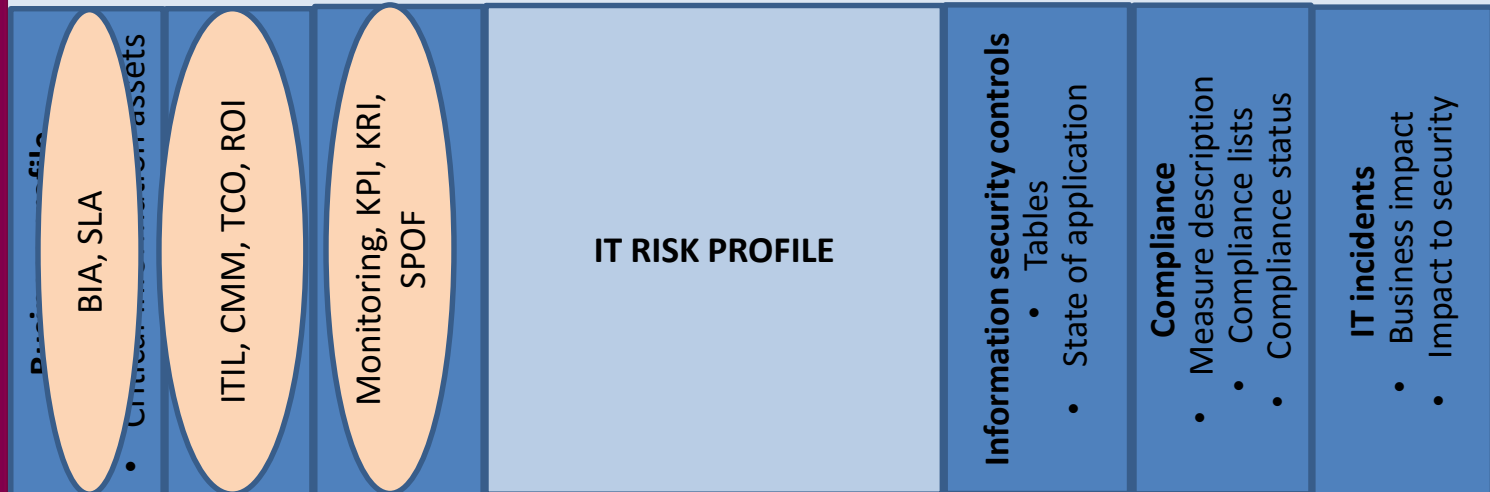


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

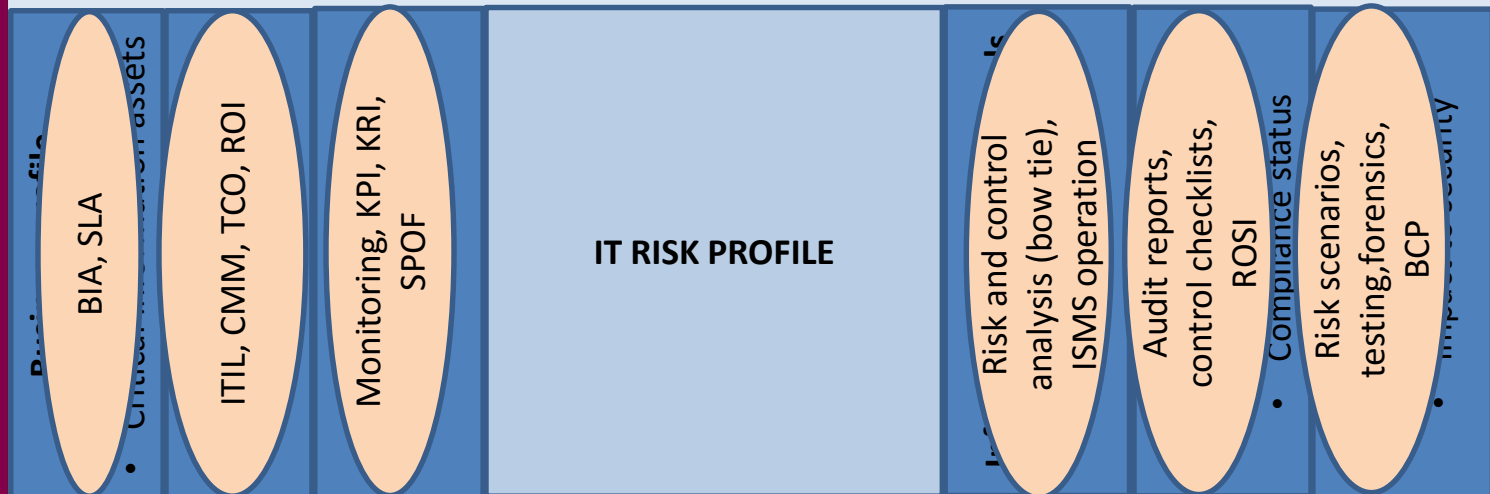


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

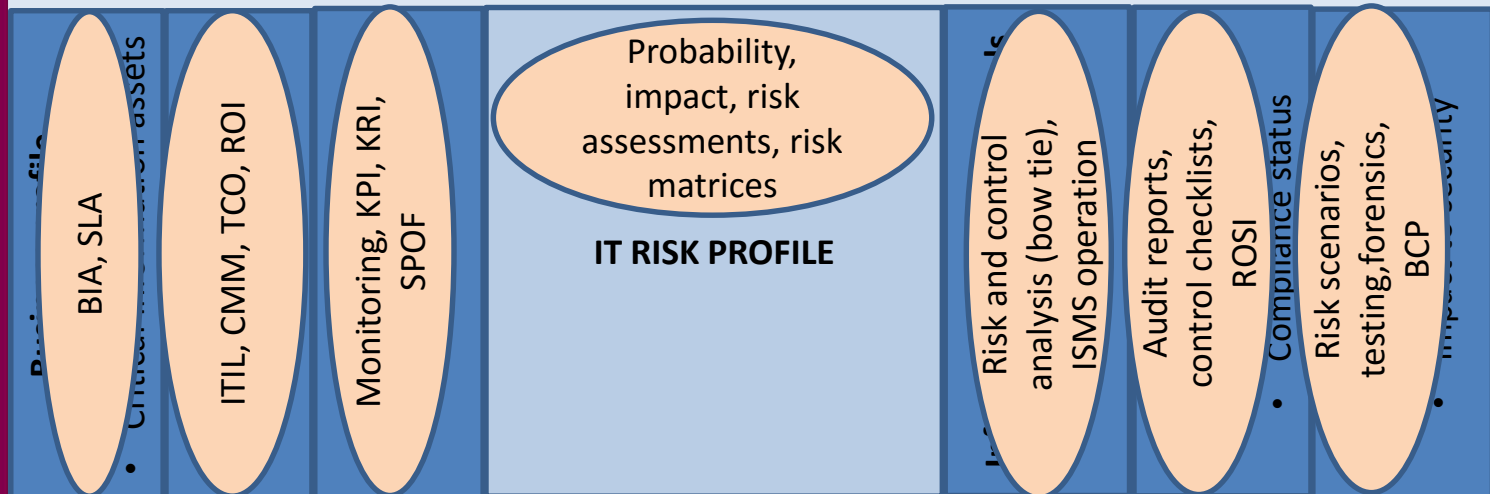


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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.

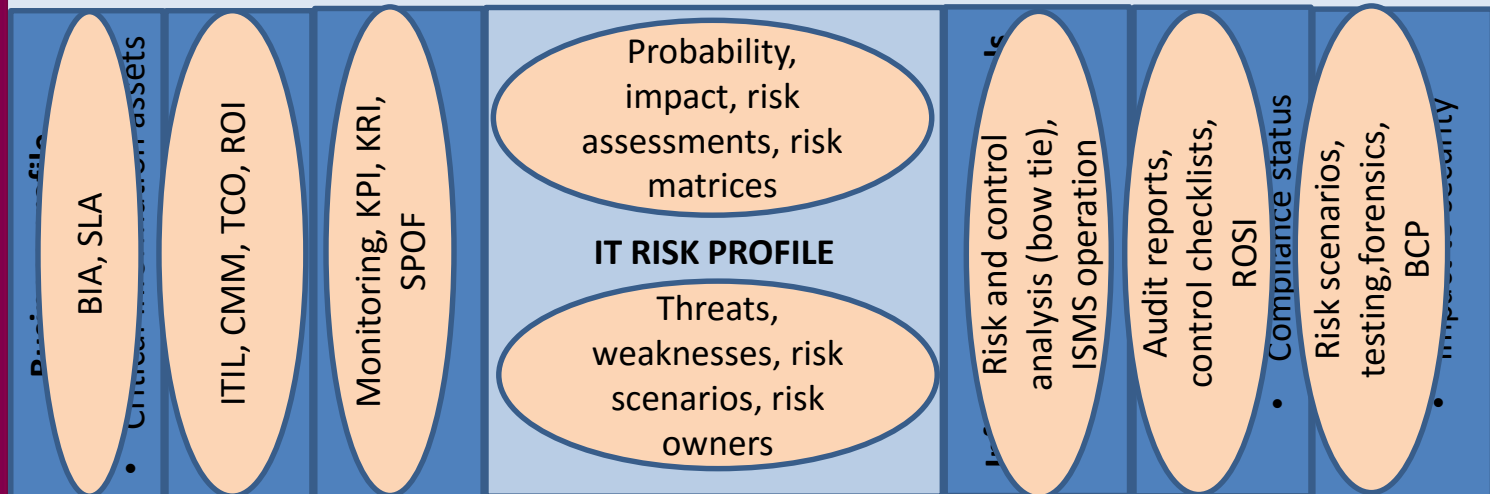


IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc ...)



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 ...)



Course themes

- IT risk assessment and management, standard ISO/IEC 27005, OCTAVE;
- IT risk assessment concepts and methods;
- Identifying and mapping the information assets and IT assets;
- Analysis of threats and vulnerabilities;
- Risk assessment and risk scales, risk matrix, residual risk;
- Information security standards ISO/IEC 27001 and ISO/IEC 27002, but also Cyber Essentials (CE), IEC 62443;
- Information security policy, planning the application of information security measures;
- Applying baseline security (e.g. ISKE) in public sector;



Course themes

- IT risk management methods, best practices;
- IT risk management organization and activities;
- Using the bow tie method (root-cause) to analyse risks with controls;
- Preventive, detective and corrective measures to achieve information security;
- Control and compliance issues of information security;
- Planning IT continuity and recovery (based on testing);
- Business continuity (BC) concept and terms;
- Business impact (BI) analysis and business continuity planning;
- Recovery objectives and recovery plans;
- Business continuity testing.



Practice

[Homework description and explanation](#)

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

