TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

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 < score ≤ 90 -- grade 4 (very good)

70 < score ≤ 80 -- grade 3 (good)

60 < score ≤ 70 -- grade 2 (satisfactory)

50 < score ≤ 60 -- grade 1 (pass)

score < 50 -- grade 0 (failed)

Course themes

- IT risk assessment and management;
- 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;
- International standards for information- and cybersecurity: ISO/IEC 27001 (ISMS), ISO/IEC 27002 (controls), ISO/IEC 27005 (risk), 22301 (continuity), 27032 (cybersecurity);
- information- and cybersecurity policy, planning the application of security measures;
- Applying baseline security (e.g. ISKE) in public sector in Estonia, discussing Cyber Essentials in UK;

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- and cybersecurity;
- Control and compliance issues of information- and cybersecurity;
- 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

Lectures

- 05.09.2017 at 12.00-15.15 ICT 315
- 12.09.2017 at 12.00-15.15 self study
- 19.09.2017 at 12.00-15.15 ICT 315
- 26.09.2017 at 12.00-15.15 ICT 315
- 03.10.2017 at 12.00-15.15 self study
- 10.10.2017 at 12.00-15.15 ICT 315
- 17.10.2017 at 12.00-15.15 ICT 315
- 24.10.2017 at 12.00-15.15 ICT 315?
- 31.10.2017 at 12.00-15.15 ICT 315
- 07.11.2017 at 12.00-15.15 ICT 315
- 14.11.2017 at 12.00-15.15 self study
- 21.11.2017 at 12.00-15.15 ICT 315
- 28.11.2017 at 12.00-15.15 ICT 315
- 05.12.2017 at 12.00-15.15 seminar
- 12.12.2017 at 12.00-15.15 seminar
- 19.12.2017 at 12.00-15.15 seminar
- 26.12.2017 at 12.00-15.15 seminar?

Course page

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

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

LINK

PhD Andro Kull
CISA, CISM, CRISC, ABCP
ISO 27001 Master, CCSM
E-mail: Andro.Kull@ttu.ee
Skype: andro.kull
Phone: +372 5093296