Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0973-2022

COURSE SYLLABUS

Sårbarhetsanalys och riskhantering

Security Metrics and Risk Management

2 credits (2 högskolepoäng)

Course code: DV2625
Main field of study: Computer Science, Software Engineering
Disciplinary domain: Technology
Education level: Second cycle
Specialization: A1N - Second cycle, has only first cycle course/s as entry requirements

Language of instruction: English
Applies from: 2023-01-16
Approved: 2022-09-01

1. Decision

This course is established by Dean 2022-03-25. The course syllabus is approved by Head of Department of Computer Science 2022-09-01 and applies from 2023-01-16.

2. Entry requirements

Admission to the course require at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

3. Objective and content

3.1 Objective

The goal of the course is to provide attendees with an understanding of how security metrics should talk about the state or degree of safety relative to a reference point. Students should be able to clarify the distinction between managing the technical IT security infrastructure at the operational level and the overall management of an information security program.

3.2 Content

- Efficiency and effectiveness of the security metrics
- Information security governance metrics
- Risk assessment and management
- Incident management metrics and indicators
- Security program metrics and monitoring

4. Learning outcomes

The following learning outcomes are examined in the course:

4.1 Knowledge and understanding

On completion of the course, the student will be able to:
- explain the importance of evaluation of security strategy and program
- understand the evaluation principles
- know the risk definition, criteria, and management process

4.2 Competence and skills

On completion of the course, the student will be able to:
- assess and evaluate the efficiency of the information security program
- evaluate the strategy milestones
- analyze and assess the risks and make a conclusions

4.3 Judgement and approach

On completion of the course, the student will be able to:

- analyze and use the security metrics: KPI. KRI, etc., for decision-making
- identify the gaps in information security processes with metrics

5. Learning activities

The teaching is organized around online lectures, recorded videos, assignments, and presentations. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through the course's online learning platform, and online messengers.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2305	Laboratory Session 1	1 credits	GU
2315	Laboratory Session 2	1 credits	GU

The course will be graded G Pass, UX Fail, supplementation required, U Fail.

The information before a course occasion states the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

An examiner can, after consulting the Disability Advisor at BTH, decide on a customized examination form for a student with a long-term disability to be provided with an examination equivalent to one given to a student who is not disabled.

7. Course evaluation

The course evaluation should be carried out in line with BTH:s course evaluation template and process.

8. Restrictions regarding degree

The course can form part of a degree but not together with another course the content of which completely or partly corresponds with the contents of this course.

9. Course literature and other materials of instruction

CISM Review Manual.15th Edition – ISACA, 2016. – ISBN 978-1-60420-508-4.