AALBORG UNIVERSITET

STUDIEORDNING FOR KANDIDATUDDANNELSEN I CYBERSIKKERHED, 2020

CIVILINGENIØR
KØBENHAVN

MODULER SOM INDGÅR I STUDIEORDNINGEN

INDHOLDSFORTEGNELSE

DISTRIBUTED SYSTEMS SECURITY

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

All students must be introduced to proper use of scientific methods. This project module therefore separate learning objectives for scientific methods.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about the analysis of complex problems and the design of secure distributed solutions for such problems.
- Must have knowledge about the analysis implementation, with a focus on the security aspects.
- Must have knowledge about IoT and mobile devices, and how to securely integrate them in distributed solutions.
- Must have knowledge about open source and commercial tools and frameworks and how to select between them, considering the security aspects.
- Must have knowledge about privacy and security by design principles.

Scientific Methods:

- Must have knowledge about scientific methods and their applicability in ICT engineering.
- Must have knowledge about main scientific paradigms and their applicability for different problems.
- Must know methods for the iterative development and refining of project ideas and problem formulations .
- Must know methods for quantitative data gathering, data analysis and data presentation, e.g.interview techniques for expert interviews.
- Must know the consequences of plagiarism.

SKILLS

- Must be able to understand when to apply a distributed system solution to a problem.
- Must be able to develop such solution in a secure way.
- Must be able to understand the different problems and advantages related to distributed computing, such as synchonization, scalability, etc.
- Must be able to select the appropriate communication channels, considering security as one of the important deciding factors.

Scientific Methods:

- Must be able to extract scientific knowledge from academic publications, e.g. journal papers, conference procesdings and anthologies.
- Must be able to master good academic praxis for the use and presentation of sources.
- Must be able to discern between inductivism, models vs. reality, hypothesis, empirical data, assumptions and proofs for a given research problem within the scope of the study programme.
- Must be able to explain the applicability for qualitative methods for a given ICT engineering problem.
- Must be able to conduct a structured search for sources, e.g. peer-reviewed literature.
- Must be able to assess the quality and applicability of a given source (e.g. peer-reviewed / non peer-reviewed sources, industry whitepapers, interviews, marketing texts)

COMPETENCES

- Must have the competencies in identifying the privacy and security concerns in a distributed system
- Must have the competencies in identifying and combining a wide range of IoT, mobile devices, and technologies in order to analyse and implement advanced distributed solutions for complex problems.

Scientific Methods

- Must have the competency to identify and apply relevant scientific methods in relation to ICT engineering problems and projects

- Must have the competency to structure an academic presentation of project (e.g. semester project) in a report
- Must master the principles for correct academic citing.

TYPE OF INSTRUCTION

Project work

EXAM

EXAMS

Name of exam	Distributed Systems Security
Type of exam	Oral exam based on a project
ECTS	10
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Sikkerhed i distribuerede systemer
Module code	ESNCYSK1P1
Module type	Project
Duration	1 semester
Semester	Autumn
ECTS	10
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

FUNDAMENTALS OF SECURITY AND CRYPTOGRAPHY

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

OBJECTIVES

- To provide the students with the basics of network and application security
- To provide the students with basic knowledge about the fundamentals of cryptography
- To give students of the education a common theoretical ground for their further studies

LEARNING OBJECTIVES

KNOWLEDGE

- Must be able to understand the basic concepts, principles and practice of network and application security
- Must have knowledge about the fundamental concepts and theories of cryptography
- Must be able to understand the basic concepts, principles and practice of cryptography
- Must be able to understand professional articles and documentation concerning security issues
- Must be able to comprehend the various classes of cryptographic algorithms, explain their relative properties and the interplay of algorithms in network security applications and protocols
- Must be able to understand the different types of attacks that exist in network security and cryptograhy

SKILLS

- Must have the ability to consider cyber security issues when developing IT-systems
- Must be able to identify the basic cyber security principles and properties of an arbitrary security mechanism or network protocol
- Must have the ability to infer the security weaknesses of an IT-system by knowing the basics of its protocols and architecture

COMPETENCES

- Must have competencies in implementing basic security properties for IT-systems based on the current best practices

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; structure and contents of the programme

EXAM

EXAMS

Name of exam	Fundamentals of Security and Cryptography
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Grundlæggende sikkerhed og kryptografi
Module code	ESNCYSK1K1
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

NETWORK SECURITY

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The course requires a basic knowledge of computer network. It is recommended that students taking this course have some experience working with TCP/PI protocol stack.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

Objektives

The course gives the participants a thorough introduction to network monitoring and network security, including both passive methods for network monitoring and network analysis as well as active methods such as network scanning.

Reasons

Knowledge about network security and network monitoring is an important foundation for the rest of the education, and also important competencies for the students after graduation.

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge about:

- the most important network-based IT security threats
- botnets
- security protocols in general, and more specifically for wireless networks
- security challenges when setting up networks, including network equipment and configurations
- selected security threats including the use of covert channels and detection hereof

SKILLS

Must have skills in:

- gathering network traffic and network traffic data
- understanding basic stastistics based on network traffic/network traffic data using commonly available tools
- understanding fundamental techniques within network traffic monitoring, including active and passive monitoring techniques and the application within detection of malicious network activities.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Network Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale

Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Netværkssikkerhed
Module code	ESNCYSK1K2
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

SECURE SOFTWARE DEVELOPMENT

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

Objectives

- To familiarise the student with current best-practices and state-of-the-art in tools, techniques, and processes for secure software development
- To enable the student to perform a wide spectrum of security activities required for secure software development.

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge about:

- Relevant security goals for secure software development, including the "CIA triad": confidentiality, integrity, and availability
- Typical and commonly occurring software security bugs and vulnerabilities
- Theories, techniques, and tools for secure software development, including static analysis tools
- Evaluation and assessment of potential security vulnerabilities

SKILLS

Must have the skills to:

- Conduct basic threat -assessment for a small software project and based on this, propose relevant security goals
- Plan and conduct an assessment of security aspects for a small software project, including review of architecture and codem evaluate the implementation process and tools used
- Evaluate and implement security mechanisms against commonly known attack forms
- Use commonly known security information sources to learn about new threats, types of threats, and concomitant countermeasures

COMPETENCES

Must have the competences to:

- Assess and evaluate security relevance of different tools, methods, and processes used for developing small software project; in particular, be able to assess the security consequences of a given software development process as well as integrating relevant security best-practices in an existing process
- Understand new types of threats against software security and assess potential consequences and proposed countermeasures for existing projects.
- Understand and assess the effectiveness of new tools and techniques for secure software development

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme

EXAM

EXAMS

Name of exam	Secure Software Development
Type of exam	Written or oral exam

ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Sikker softwareudvikling
Module code	ESNCYSK1K3
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

SECURITY IN IOT AND CLOUD ARCHITECTURES

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

Objectives:

- To provide the student with knowledge about state-of-the-art Internet of Things (IoT) devices, their functionalities, and the privacy and security considerations related to those
- To provide the student with knowledge about virtualization, cloud computing, edge computing, and their security aspects.
- To provide the student with knowledge about recent trends of IoT and cloud integration, with a focus on the privacy and security aspects.
- To provide the student with skills to perform analysis, design, and implementation of systems that integrate IoT and cloud computing, with a focus on privacy and security.
- To provide the student with knowledge about recent developments in communication technologies, such as 5G, their usage, and their security aspects.

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge about:

- IoT devices and the usage of cloud computing in complex IoT architectures.
- open source and commercial state-of-the-art tools and frameworks for IoT and cloud integration.
- privacy and security considerations of such architectures.
- different virtualization techniques, how they are used to support the cloud and their security characteristics.
- privacy and security by design principles.
- programming for IoT devices.

SKILLS

Must be able to:

- design and implement secure solutions for IoT devices that make use of the cloud.
- use common frameworks for developing secure IoT solutions provided by the biggest cloud providers.
- analyse and discuss the security aspects of existing IoT platforms.
- understand the adoption of 5G in the context of IoT and edge computing.

COMPETENCES

Must have the competencies to:

- design and implement secure IoT solutions that integrate with the cloud.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme

EXAM

EXAMS

Name of exam	Security in IoT and Cloud Architectures
Type of exam	Written or oral exam

ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Sikkerhed i IoT- og cloud-arkitekturer
Module code	ESNCYSK1K4
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

SECURE SYSTEMS: ATTACK AND DEFENCE

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The project unit requires basic knowledge about network security, e.g. obtained by following the first semester of the education. The project unit makes use of elements from the other courses of the semester.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

OBJECTIVE

In this project unit, the students learn to protect a given system against cyber attacks and/or to test how a given system can be attacked. The system to be used can be based either on software alone, or it can be a cyber physical system consisting of both hardware and software elements. It can also be an embedded system, or a distributed system connected through one or more networks.

REASON

The students achieve both theoretical understanding and practical experience in protecting and security testing systems, which are important elements in the education, and important competencies for the candidates after graduation.

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge about:

- ethical and legal aspects of security testing.
- handling of results from security tests, including responsible disclosure of newly found vulnerabilities.
- how to formulate own competences related to PBL.

SKILLS

Must have skills in:

- protecting a system against attacks, including one or more of the following elements:
  - Analysis of systems in order to uncover relevant cyber risks and attack vectors.
  - Prevention of cyber attacks by selecting and establishing relevant countermeasures.
  - Section and implementation of techniques to monitor systems in order to detect cyber attacks.
  - Selection and implementation of techniques for detecting cyber attacks based on relevant information, possibly including information from monitoring systems.
  - Mitigating and dealing with cyber attacks when they are discovered, and considering conditions related to forensics.

- security testing how a given system is protected and might be attacked, including one or more of the following elements:

- Analysis of attack vectors
- Conducting reconnaissance, including the selection of relevant methods and tools.
- Network scanning and vulnerability scanning, including the selection of relevant methods and tools.
- Conducting security tests.

- reflecting over own use of PBL methods and how these methods can be used in the future projects and work situations.

COMPETENCES

Must have competencies in:

- assessing, selecting and applying methods in order to secure and/or to conduct security testing of a given system, evaluate the specific results generated by using these methods, as well as reflecting over approach and results.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme

EXAM

PREREQUISITE FOR ENROLLMENT FOR THE EXAM

- An approved PBL competency profile is a prerequisite for participation in the project exam

EXAMS

Name of exam	Secure Systems: Attack and Defence
Type of exam	Oral exam based on a project
ECTS	15
Assessment	7-point grading scale
Type of grading	External examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Sikre systemer: Angreb og forsvar
Module code	ESNCYSK2P1
Module type	Project
Duration	1 semester
Semester	Spring
ECTS	15
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

HACKER SPACE

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The course requires a basic knowledge of network security, which can be obtained e.g. from the course “network security” from the first semester of the education.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

OBJECTIVES

The course gives the participants theoretical knowledge about as well as practical experience with testing and experimenting with network based cyber attacks and malware. It provides practical experience from both attack and defence points of view and allows the participants to test out different attack and defence strategies in a secure and contained testing environment.

REASON

Understanding of network based cyber attacks and how these can be defended against are central elements in the education. Training in how systems look from an attack point of view, and how attackers think, are crucial in order to develop good defence strategies and techniques.

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge about:

- systems for detecting, establishing and preventing intrusions (intrusion detection systems and intrusion prevention systems) - including knowledge about relevant monitoring and logging.
- malware analysis from a network perspective, in order to identify selected types of malicious activity and attacks.

SKILLS

Must have skills in:

- configuration and operation of secure test environments.
- applying selected tools for attacking and defending network devices and network infrastructure, including detection and establishing of attacks.

COMPETENCES

Must have competencies in:

- understanding Internet-based threats and attack techniques, including DoS (Denial of Service) attacks, DDOS (Distributed Denial of Service) attacks and information theft.
- understanding malicious network activity, including the malicious use of relevant Internet infrastructure such as DNS servers.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme

EXAM

EXAMS

Name of exam	Hacker Space
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Hacker space
Module code	ESNCYSK2K1
Module type	Course
Duration	1 semester
Semester	Spring
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

ADVANCED SOFTWARE SECURITY

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

OBJECTIVES

- To familiarise the student with state-of-the-art research within select areas of software security, e.g., language-based security, secure information flow, secure programming languages, verified programming.
- To enable the student to assess and evaluate proposed or novel tools and techniques for software security.
- To familiarise the student with the theoretical foundations underlying key areas of software security, e.g., fuzzing, static analysis, model checking etc.

LEARNING OBJECTIVES

KNOWLEDGE

- To know and be able to explain the difference(s) between the most common software security methodologies, e.g., fuzzing, static analysis, model checking, verified programming.
- To know and be able to explain common use cases and pitfalls for key software security tools, techniques, and theories, as well as discuss inherent advantages vs. disadvantages in such use cases.
- To know of the theoretical foundations for one or more of the studied tools and techniques, in particular static analysis, model checking, and fuzzing.
- To know and be able to explain the limitations of the studied theories, tools, and techniques.

SKILLS

- To be able to deploy and use one or more software security tools or techniques for security analysis of a small software project.
- To be able to evaluate potential (security related) benefits or drawbacks of using the studied tools and theories on a small software project.
- To be able to identify the best tool or technique to solve specific software security problems.

COMPETENCES

- To be able to assess and evaluate security relevance of different tools, methods, and processes used for developing small software projects.
- To be able to evaluate and propose or adapt existing techniques to perform specific security related analyses of software, e.g., extending a taint-analysis to cover new language features.
- To be able to identify and research novel theories, tools, and techniques for software security.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Advanced Software Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale

Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Avanceret software-sikkerhed
Module code	ESNCYSK2K2
Module type	Course
Duration	1 semester
Semester	Spring
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

ADVANCED TOPICS IN CYBER SECURITY

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

OBJECTIVES

- To provide students the opportunity to combine their knowledge from previous courses and projects.
- To give students the chance to improve their programming and software engineering competences.
- To enable students to develop approaches that are in the frontier of cyber security engineering and research.
- To provide the student with knowledge about the state of the art in a plethora of cutting-edge cyber security topics.
- To provide the student with knowledge about how research is conducted in cyber security.
- To provide the student with knowledge about recent developments in network and application security via the utilization of newly established technologies.

LEARNING OBJECTIVES

KNOWLEDGE

- Must be able to understand the fundamental pillars of cyber security research and evaluation.
- Must have knowledge on a broad spectrum of innovative technologies and on how they can be applied in the context of cyber security.
- Must be able to comprehend and analyse research articles from the top cyber security conferences and journals.
- Must be able to understand how sophisticated threats, vulnerabilities and attack methods function and how countermeasures can be developed and applied.
- Must be able to understand advanced concepts, principles and practice of network and application security.

SKILLS

- Must be able to identify research questions and challenges for a variety of topics in cyber security.
- Must be able to use various state of the art frameworks for analysing network traffic, identifying adversaries, as well as for developing/deploying attacks.
- Must have the ability to critically review, summarize and discuss scientific content in cyber security.

COMPETENCES

- Must have the competencies of identifying open challenges in different cyber security research areas and discussing them on a scientific basis.
- Must have the competence of connecting research challenges and questions with real world problems and products that will have an impact to the society.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Advanced Topics in Cyber Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale

Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Avancerede emner i cybersikkerhed
Module code	ESNCYSK3K1
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

PROJECT-ORIENTED STUDY IN AN EXTERNAL ORGANISATION

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

A project-oriented study in an external organisation agreement approved by the company, an AAU supervisor and the study board for Electronics and IT (ESN).

The project-oriented study in an external organisation must have a scope that corresponds to the ECTS load.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The student stays in a company with the purpose of learning and applying theories and methods to address engineering problems in an industrial context. In addition, the student will be introduced to business procedures and policies.

LEARNING OBJECTIVES

KNOWLEDGE

- Has knowledge about the organisation of the company and business procedures and policies.
- Has knowledge about performance measures in the company.
- Has developed a fundamental business sense.
- Has knowledge of the competence profile of the programme and how the academic internship contributes to the competence profile.
- Has gained deepened knowledge into engineering theories and methods within the programme.

SKILLS

- Can initiate and ensure the completion of an agreement for the academic internship, with learning objectives corresponding to the semester at the master's programme.
- Can apply analytic, methodological and/or theoretic skills to address advanced engineering problems in an industrial context.
- Can contribute in a professional manner to company objectives as an individual and in teams in accordance with the project management model applied in the company.
- Can collaborate and communicate with peers, managers and others.
- Can document the academic internship in a report and defend it orally.

COMPETENCES

- Can discuss and reflect on the learning outcomes of the academic internship.
- Can discuss the need for knowledge transfer between academia and industry.
- Has a deepened understanding of the academic interests to pursue in the master's thesis and possible job positions to aim at after graduation.

TYPE OF INSTRUCTION

Project work

EXAM

EXAMS

Name of exam	Project-Oriented Study in an External Organisation
Type of exam	Oral exam based on a project
ECTS	25
Assessment	Passed/Not Passed
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Projektorienteret forløb i en virksomhed
Module code	ESNCYSK3P3
Module type	Project
Duration	1 semester
Semester	Autumn
ECTS	25
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

MASTER'S THESIS

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The project builds on knowledge obtained during the previous semesters.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The master’s thesis can be conducted as a long master’s thesis. If choosing to do a long master’s thesis, it has to include experimental work and has to be approved by the study board. The amount of experimental work must reflect the allotted ECTS-credits.

LEARNING OBJECTIVES

KNOWLEDGE

Must have:

- knowledge, at the highest international level of research, of at least one of the core fields of the education.
- Must have comprehension of implications of research (research ethics).

SKILLS

Must be able to:

- reflect on a scientific basis on their knowledge,
- argue for the relevance of the chosen problem to the education including specifically account for the core of the problem and the technical connections in which it appears
- account for possible methods to solve the problem statements of the project, describe and assess the applicability of the chosen method including account for the chosen delimitation and the way these will influence the results of the product
- analyse and describe the chosen problem applying relevant theories, methods and experimental data
- describe the relevant theories and methods in a way that highlights the characteristics and hereby document knowledge of the applied theories, methods, possibilities and delimitations within the relevant problem area
- analyse and/or implement solutions to problems related to one or more of the core fields of the education.

COMPETENCES

Must have competencies:

- in one or more areas of cyber security
- to identify and delimit relevant problems within cyber security with an engineering approach and apply relevant theories, methods and experimental data
- to contribute to the secure use of technologies to resolve user needs and improve organizational processes.

TYPE OF INSTRUCTION

Project work. The project is carried out individually or in a small group of maximum three members. At least one internal supervisor is assigned, who works with the primary subject within his/her research. Moreover, additional supervisors e.g. from industry can be involved in the project.

EXAM

EXAMS

Name of exam	Master's Thesis
Type of exam	Master's thesis/final project
ECTS	45
Assessment	7-point grading scale
Type of grading	External examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Kandidatspeciale
Module code	ESNCYSK4P2
Module type	Project
Duration	2 semesters
Semester	Autumn
ECTS	45
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

MASTER'S THESIS

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The project builds on knowledge obtained during the previous semesters.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The master’s thesis can be conducted as a long master’s thesis. If choosing to do a long master’s thesis, it has to include experimental work and has to be approved by the study board. The amount of experimental work must reflect the allotted ECTS-credits.

LEARNING OBJECTIVES

KNOWLEDGE

Must have:

- knowledge, at the highest international level of research, of at least one of the core fields of the education.
- Must have comprehension of implications of research (research ethics).

SKILLS

Must be able to:

- reflect on a scientific basis on their knowledge,
- argue for the relevance of the chosen problem to the education including specifically account for the core of the problem and the technical connections in which it appears
- account for possible methods to solve the problem statements of the project, describe and assess the applicability of the chosen method including account for the chosen delimitation and the way these will influence the results of the product
- analyse and describe the chosen problem applying relevant theories, methods and experimental data
- describe the relevant theories and methods in a way that highlights the characteristics and hereby document knowledge of the applied theories, methods, possibilities and delimitations within the relevant problem area
- analyse and/or implement solutions to problems related to one or more of the core fields of the education.

COMPETENCES

Must have competencies:

- in one or more areas of cyber security
- to identify and delimit relevant problems within cyber security with an engineering approach and apply relevant theories, methods and experimental data
- to contribute to the secure use of technologies to resolve user needs and improve organizational processes.

TYPE OF INSTRUCTION

Project work. The project is carried out individually or in a small group of maximum three members. At least one internal supervisor is assigned, who works with the primary subject within his/her research. Moreover, additional supervisors e.g. from industry can be involved in the project.

EXAM

EXAMS

Name of exam	Master's Thesis
Type of exam	Master's thesis/final project
ECTS	50
Assessment	7-point grading scale
Type of grading	External examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Kandidatspeciale
Module code	ESNCYSK4P3
Module type	Project
Duration	2 semesters
Semester	Autumn
ECTS	50
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

MASTER'S THESIS

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The project builds on knowledge obtained during the previous semesters.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

LEARNING OBJECTIVES

KNOWLEDGE

Must have:

- knowledge, at the highest international level of research, of at least one of the core fields of the education.
- Must have comprehension of implications of research (research ethics).

SKILLS

Must be able to:

- reflect on a scientific basis on their knowledge,
- argue for the relevance of the chosen problem to the education including specifically account for the core of the problem and the technical connections in which it appears
- account for possible methods to solve the problem statements of the project, describe and assess the applicability of the chosen method including account for the chosen delimitation and the way these will influence the results of the product
- analyse and describe the chosen problem applying relevant theories, methods and experimental data
- describe the relevant theories and methods in a way that highlights the characteristics and hereby document knowledge of the applied theories, methods, possibilities and delimitations within the relevant problem area
- analyse and/or implement solutions to problems related to one or more of the core fields of the education.

COMPETENCES

Must have competencies:

- in one or more areas of cyber security
- to identify and delimit relevant problems within cyber security with an engineering approach and apply relevant theories, methods and experimental data
- to contribute to the secure use of technologies to resolve user needs and improve organizational processes

TYPE OF INSTRUCTION

Project work. The project is carried out individually or in a small group of maximum three members. At least one internal supervisor is assigned, who works with the primary subject within his/her research. Moreover, additional supervisors e.g. from industry can be involved in the project.

EXAM

EXAMS

Name of exam	Master's Thesis
Type of exam	Master's thesis/final project

ECTS	30
Assessment	7-point grading scale
Type of grading	External examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Kandidatspeciale
Module code	ESNCYSK4P1
Module type	Project
Duration	1 semester
Semester	Spring
ECTS	30
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

IDENTITY AND ACCESS MANAGEMENT

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The module is offered jointly with the MSc programme in Innovative Communication Technologies and Entrepreneurship (ICTE). It builds on knowledge obtained in the ICTE module “Internet technologies and service architectures” or similar.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge about:

- physical identities, digital identities and credentials
- key identity concepts such as linkability, personally identifiable information, personal data, attributes, claims, and assertions
- state-of-the-art principles, laws, guidelines and frameworks for protecting users’ privacy, including fine-grained management of personal attributes
- security objectives and methods to achieve them
- principles and methods for identification, authentication, and authorisation, including assurance levels and methods for strong authentication
- policies, policy architectures, and access control schemes
- identity management systems, identity federation and single sign-on systems
- state-of-the-art technologies and frameworks for managing access to protected resources, including identity and access management (IAM) in enterprises

SKILLS

Must be able to:

- identify the personal attributes that are needed to perform a given task
- apply methods and technologies for privacy protection as a part of service development, including “privacy by design” principles
- identify resource sets and protect them with secure interfaces
- apply state-of-the-art technologies for realising advanced services with authentication, authorisation and access control
- design applications and services incorporating authenticators, different assurance levels, and management of user identities (authentication, authorisation, privacy protection)
- analyse and design information flows and architectures for ICT services and solutions

COMPETENCES

Must have the competences to:

- design secure services and policy architectures with controlled exchange of attributes between stakeholders and minimal disclosure of personal information
- discuss and reflect on management of personal information for access to resources and for personalisation of services

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Identity and Access Management
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Identitets- og adgangshåndtering
Module code	ESNCYSK2K3
Module type	Course
Duration	1 semester
Semester	Spring
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

MACHINE LEARNING

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The module is offered jointly with the MSc programme in Innovative Communication Technologies and Entrepreneurship (ICTE). It builds on mathematical knowledge obtained in the bachelor courses “Linear Algebra” and “Introduction to Probability and Applied Statistics“ (bachelor in IT, Communication and New Media), or similar.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge about:

- data modelling in form of preparing data, modelling data, and evaluating and disseminating the results.
- key machine learning concepts such as feature extraction, cross-validation, generalization and over-fitting, prediction and curse of dimensionality.
- different machine learning principles, algorithms, techniques and be able to define and describe fundamental problems and consequences within machine learning.
- basic recommender system principles, techniques, algorithms and be able to define and describe fundamental problems and consequences within these.

SKILLS

Must be able to:

- discuss how the data modelling methods work and describe their assumptions and limitations.
- map practical problems to standard data models such as regression, classification, density estimation, clustering and association mining.
- select and apply a range of different machine learning algorithms and techniques on specific problems.
- select and apply the basic recommender system algorithms and techniques on specific problems

OR

- select and apply relevant machine learning algorithms and techniques for detection of cyber attacks or anomalous behaviour in cyber systems

COMPETENCES

Must have the competency to:

- solve machine learning related problems in a practical context.
- apply machine learning algorithms and analyse the results

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Machine Learning

Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Maskinlæring
Module code	ESNCYSK2K4
Module type	Course
Duration	1 semester
Semester	Spring
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

SECURE SYSTEMS DEVELOPMENT

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

- To provide students the opportunity to combine their knowledge from previous courses and projects.
- To give students the chance to improve their programming and software engineering competences.
- To enable students to develop approaches that are in the frontier of cyber security engineering and research

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge about the relation between security risks and business processes, including indentification and protection of business-critical Assets.
- Must have knowledge on identifying security properties and requirements of a system (including e.g. software systems, cyber physical systems, distributed systems and embedded system).
- Must have knowledge of secure software development and scripting.
- Must be able to combine the knowledge of the previous semester's projects and courses
- Must have deep knowledge of security concepts, both from the defender's and the attacker's perspectives.

SKILLS

- Must be able to identify the research and development challenges for a cyber security engineering project and propose/develop relevant solutions
- Must be able to use various state of the art frameworks for analysing network traffic, identifying adversaties, as well as for developing/deploying attacks.
- Must be able to understand security requirements for an organisation
- Must be able to include strong security, cryptography and acess control elements in mobile and web-based applications.
- Must be skills in communicating cyber security challenges and solutions to non-experts

COMPETENCES

- Must have competencies in identifying cyber security needs in an organisation
- Must have competencies in combining a wide range of networks, technologies and devices to relize advanced and non-trivial applications and solutions
- Must have competencies in comparing and assessing the potential of different technologies, methods and appoaches to make proper security design choices
- Must have competences to independently define and analyze, scientific and engineering problems in the area defined by the project theme, also in cooperation with external/internal partners or as a part of a multidosplinary projects.
- Must have competences to control the workning and development process within the project theme.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Secure Systems Development
Type of exam	Oral exam based on a project
ECTS	15

Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Udvikling af sikre systemer
Module code	ESNCYSK3P1
Module type	Project
Duration	1 semester
Semester	Autumn
ECTS	15
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

IT SECURITY GOVERNANCE

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

In this project unit, the students must work with the relationships between technical, economic- political-, regulatory and cultural aspects of cyber security threats for individuals, companies, organizations and nations. The aim is that the students must understand the interplay between these aspects of cyber security and how precautions require solutions that include technical as well as political-regulatory and normative initiatives. Furthermore, the students must be able to operationalize knowledge on complex cyber security problems in managerial initiatives at strategic and tactical levels.

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge:

- on problems within cyber security, that individuals, companies, organizations, public institutions and nations can encounter
- on the interrelationships between technical, economic, political-regulatory and cultural aspects of threats against cyber security
- on how the interplay between technical, political-regulatory and normative precautions can limit threats against cyber security
- on legal requirements, standards and certification arrangements concerning cyber security at national and EU level respectively
- on strategic and tactical management of cyber security within organizations, including norms for strengthening of the protection of personal data and cyber security
- about the relation between security risks and business processes including the identification and protection of business-critical assets

SKILLS

Must have skills:

- in detecting new risks and threats concerning cyber security within companies and other organizations
- in being able to contribute to the development of methods to protect cyber security
- in management of the prevention and control of threats against cyber security
- in developing security strategies that include technical as well as normative aspects

COMPETENCES

Must have competences:

- in being able to reflect on the ethical issues which the processing of sensitive personal data can involve
- in understanding complex security problems
- in communicating cyber security challenges and solutions to non-experts

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	IT Security Governance

Type of exam	Oral exam based on a project
ECTS	15
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Governance af it-sikkerhed
Module code	ESNCYSK3P2
Module type	Project
Duration	1 semester
Semester	Autumn
ECTS	15
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

PRIVACY ENGINEERING

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

Informational privacy is today an integrated element of digital services. Businesses and organisations that store or process personal information must protect users' privacy. The privacy engineering course examines privacy as a concept and its practical implications. Furthermore, the relation to cyber security and trust is discussed. Specifically, the course addresses GDPR and its implications for software developers and organizations. The course discusses technical solutions to provide privacy, the integration of privacy into the design process and privacy as expressed in interface design.

LEARNING OBJECTIVES

KNOWLEDGE

The student must have knowledge of:

- The concept "privacy", as understood in application contexts such as: service development, finance, legislation, etc.
- The concept of "privacy" from a moral-ethical perspective
- The concept of "privacy" in technical solutions
- System development-relevant principles for “privacy by design” and “privacy by default”
- Principles for privacy assessments (risk assessments)
- Privacy controlling / privacy protective technologies
- The relationship between privacy and the concepts of cyber-security, trust and risk
- User profiling and privacy
- Conflicts of interest related to the development of privacy protection solutions
- Communicating privacy issues and choices to users via interfaces

SKILLS

The student should be able to:

- Analyse cases from both technical, business and user perspectives
- Apply the different understandings of privacy in analyses of technologies
- Explain the principles of "privacy by design" and "privacy by default"
- Evaluate different privacy principles in selected cases
- Classify various privacy control / protective technologies
- Use different methods to investigate and assess privacy

COMPETENCES

The student must have competences to:

- Assess different privacy understandings in various examples
- Apply different privacy principles to selected examples
- Understand the difference between different privacy principles and security principles
- Apply privacy assessment principles in selected cases and assess their suitability

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Privacy Engineering
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Privacy Engineering
Module code	ESNCYSK3K2
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

MODELS OF SECURITY

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

Objectives

- To familiarise the student with the theoretical foundations of security, in the form of (a selection of) models for security, e.g., access control models, secure information flow, calculi of (secure) computation.
- To enable a deeper understanding of the theoretical (mathematical and computer science) foundations underlying state-of-the-art security tools and techniques.

LEARNING OBJECTIVES

KNOWLEDGE

- To know and be able to explain key points of a selection of access control models, e.g., Bell/LaPadula, Biba, Decentralised Label Model, as well as for a selection of other models of security, e.g., secure information flow or approaches based on calculi of computation.
- To know and be able to explain key theoretical results concerning the models, e.g., undecidability results.

SKILLS

- To be able to use one or more of the studied theories/models to perform security analyses and evaluations of a small system.
- To be able to use the studied theories/models to formally prove security properties of (a model of a) system.
- To be able to understand a formal reasoning and argument for security, e.g., for compliance with high-assurance standards.

COMPETENCES

- To be able to identify and research both classical and novel theories and models for security.
- To be able to use a model of security to model security relevant aspects of a system and identify and formally prove relevant security properties of the system (through the model).

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Models of Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Sikkerhedsmodeller
Module code	ESNCYSK3K3
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

REGULATION OF IT SECURITY

2020/2021

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

The aim of the course is to provide the students with an overview of the legal and institutional framework conditions for cyber security and how they are applied. The course includes relevant national and international legislation and regulation within the area including EU directives and regulations. Focus is on cybercrime, privacy, logging, and problems within digital media, the financial sector and national security.

LEARNING OBJECTIVES

KNOWLEDGE

- Must have knowledge on the various kinds of legislation and regulation
- Must have specific knowledge on legislation concerning cyber security in Denmark and the EU
- Must have knowledge on legislation and regulation regarding digital media
- Must have knowledge on the most important organizations within the development of standards and certification regarding cyber security and digital signature

SKILLS

- Must have skills with respect to detecting problems in cyber security in the financial sector
- Must have skills in correctly handling sensitive data including personal data taking current legislation into account
- Must have skills in being able to identify security requirements and solutions with implications for national security
- Must have skills in being able to include techno-economic considerations in an analysis of technical and organizational solutions in cyber security

COMPETENCES

- Must have competences to assess technical solutions in cyber security in light of the specific organizational conditions and legal frameworks
- Must have competences to include ethical issues in relation to the analysis of a concrete security solution

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Regulation of IT Security
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale
Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Regulering af it-sikkerhed
Module code	ESNCYSK3K4
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design

ENTERPRISE SECURITY AND COMPLIANCE

2020/2021

PREREQUISITE/RECOMMENDED PREREQUISITE FOR PARTICIPATION IN THE MODULE

The module is offered jointly with the MSc programme in Innovative Communication Technologies and Entrepreneurship (ICTE). It requires a basic understanding of network security.

CONTENT, PROGRESS AND PEDAGOGY OF THE MODULE

LEARNING OBJECTIVES

KNOWLEDGE

Must have knowledge of:

- standards addressing information security and cyber security challenges
- technologies already embedded in enterprise endpoints
- security services and policies within public and private cloud networks

SKILLS

Must be able to:

- identify and manage risks in combination with security requirements
- design, implement and verify enterprise security solutions
- identify and illustrate an IT system landscape end-to-end and pinpoint risks to be considered
- carry out an information security review and an IT audit

COMPETENCES

Must have the competency to:

- design requirements and controls for an enterprise security solution based on a risk assessment
- discuss end-to-end standards to create trust and controls in a large enterprise IT solution.
- discuss the business needs and willingness to accept risks based on an Enterprise Risk Management solution
- discuss risks, security and compliance in a cloud environment.

TYPE OF INSTRUCTION

Types of instruction are listed at the start of §17; Structure and contents of the programme.

EXAM

EXAMS

Name of exam	Enterprise Security and Compliance
Type of exam	Written or oral exam
ECTS	5
Assessment	7-point grading scale

Type of grading	Internal examination
Criteria of assessment	The criteria of assessment are stated in the Examination Policies and Procedures

FACTS ABOUT THE MODULE

Danish title	Sikkerhed og compliance i virksomheder
Module code	ESNCYSK3K5
Module type	Course
Duration	1 semester
Semester	Autumn
ECTS	5
Language of instruction	English
Empty-place Scheme	Yes
Location of the lecture	Campus Copenhagen
Responsible for the module	Tatiana Kozlova Madsen

ORGANISATION

Study Board	Study Board of Electronics and IT
Department	Department of Electronic Systems
Faculty	Technical Faculty of IT and Design