MODULE HANDBOOK

Master of Science

Master Cyber Security (CSE-MACSE-120)

120 CP

Campus Studies

As of April 1st, 2026

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

Classification: Consecutive

Contents

Module MMTHE: Master Thesis

Corporate Governance of IT, Compliance, and Law

Module Code: CSEMIGCR-01_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Johannes Kent Walter (Corporate Governance of IT, Compliance, and Law)

Contributing Courses to Module

- Corporate Governance of IT, Compliance, and Law (CSEMIGCR01-01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- IT Governance: Motivation and Challenges
- COBIT Framework
- IT Compliance
- IT basic protection according to BSI IT law

Learning Outcomes

Corporate Governance of IT, Compliance, and Law

On successful completion, students will be able to

- explain the terms IT governance and IT compliance.
- categorize typical processes and activities from the area of IT governance and IT compliance.
- give an overview of the COBIT framework and its elements.
- give an overview of IT-Governance and explain its structure.
- reproduce important laws and regulations in the field of IT law and explain their areas of application.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Computer Science & Software Development	All Master Programs in the IT & Technology field

Corporate Governance of IT, Compliance, and Law

Course Code: CSEMIGCR01-01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

In this course, students learn terms and frameworks related to IT governance and IT compliance. First, a short introduction and an overview of the different aspects of IT governance and IT compliance are given; then, COBIT and IT basic protection are explained as two frameworks that are used in industrial practice. In addition, this course will introduce and discuss important legal frameworks and standards related to IT law.

Course Outcomes

On successful completion, students will be able to

- explain the terms IT governance and IT compliance.
- categorize typical processes and activities from the area of IT governance and IT compliance.
- give an overview of the COBIT framework and its elements.
- give an overview of IT-Governance and explain its structure.
- reproduce important laws and regulations in the field of IT law and explain their areas of application.

Contents

1. IT Governance: Motivation and Challenges
   - 1.1 Governance and IT Governance
   - 1.2 Frameworks for IT Governance
   - 1.3 Typical IT Governance, Service Management, and Security Frameworks and Standards
2. COBIT Framework
   - 2.1 Overview of the Elements of COBIT
   - 2.2 Governance and Management Objectives
   - 2.3 Use of COBIT and COBIT Design Factors
   - 2.4 The Target Cascade of COBIT
3. IT Compliance
   - 3.1 Introduction to IT Compliance
   - 3.2 Examples of National and International Guidelines: Risk Management Standards and Frameworks

3.3 IT Compliance: Typical Measures

4. Basic IT Protection According to BSI
   - 4.1 Overview and Structure
   - 4.2 Approach to IT Security Governance
   - 4.3 Usage Example of IT Security Governance

5. Introduction to IT Service Management
   - 5.1 What is Information Technology Service Management?
   - 5.2 What is ITIL® V4?
   - 5.3 What is ISO/IEC 20000-1:2018?
   - 5.4 Other ITSM Frameworks and Standards

6. IT Law
   - 6.1 Overview of Relevant Laws
   - 6.2 Protection of Intellectual Property
   - 6.3 IT Contracts
   - 6.4 Privacy

Literature

Compulsory Reading

Further Reading

- Cervone, H. F. (2017). Implementing IT governance: A primer for informaticians. Digital Library Perspectives, 33(4), 282—287.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Course Book	☑ Practice Exam
☑ Video	☑ Online Tests
☑ Slides	

Advanced Mathematics

Module Code: CSEMDSAM-01

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Robert Graf (Advanced Mathematics)

Contributing Courses to Module

- Advanced Mathematics (CSEMDSAM01-01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Calculus
- Integral Transformations
- Vector Algebra
- Vector Calculus
- Matrices and Vector Spaces
- Information Theory

Learning Outcomes

Advanced Mathematics

On successful completion, students will be able to

- remember the fundamental rules of differentiation and integration.
- apply integration and differentiation techniques to vectors and vector fields.
- analyze matrix equations.
- understand the generalization of vectors to tensors.
- evaluate different metrics from information theoretical perspectives.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Methods	All Master Programmes in the Business field

Advanced Mathematics

Course Code: CSEMDSAM01-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Modern techniques to analyze data and derive predictions for future events are deeply rooted in mathematical techniques.The course builds a solid base to understand the concepts behind advanced algorithms used to process, analyze, and predict data and observations and enables students to follow future research, especially in the fields of data-intensive sciences.The course reviews differentiation and integration and then discusses partial differentiation, differentiation, vector algebra and vector calculus. Matrix calculation and vector spaces are fundamental to many modern data processing algorithms and are discussed in detail. Calculations based on Tensors are introduced.Common metrics are discussed from an informational, theoretical point of view.

Course Outcomes

On successful completion, students will be able to

- remember the fundamental rules of differentiation and integration.
- apply integration and differentiation techniques to vectors and vector fields.
- analyze matrix equations.
- understand the generalization of vectors to tensors.
- evaluate different metrics from information theoretical perspectives.

Contents

1. Calculus
   - 1.1 Differentiation
   - 1.2 Integration
   - 1.3 Partial Differentiation
   - 1.4 Vector Analysis
2. Integral Transformations
   - 2.1 Convolution
   - 2.2 Complex Numbers
   - 2.3 Fourier Series
   - 2.4 Fourier Transformation
3. Vector Algebra

- 3.1 Scalars and Vectors
- 3.2 Addition and Subtraction of Vectors
- 3.3 Multiplication of Vectors, Vector Product, Scalar Product

4. Vector Calculus
   - 4.1 Differentiation of Vectors
   - 4.2 Integration of Vectors
   - 4.3 Scalar and Vector Fields
   - 4.4 Vector Operators

5. Matrices and Vector Spaces
   - 5.1 Basic Matrix Algebra and Systems of Linear Equations
   - 5.2 Transpose, Trace, Determinant, and Inverse of a Matrix
   - 5.3 Eigenvalues, Eigenvectors, and Diagonalization
   - 5.4 Tensors

6. Information Theory
   - 6.1 Mean Squared Error (MSE) and Simple Linear Regression
   - 6.2 Area Under the ROC Curve and Gini Index
   - 6.3 Entropy
   - 6.4 Cross Entropy

Literature

Compulsory Reading

Further Reading

- Mathai, A. M., & Haubold, H. J. (2017). Linear algebra, a course for physicists and engineers (1st ed.) De Gruyter.
- Riley, K. F., Hobson, M. P, & Bence, S. J. (2006). Mathematical methods for physics and engineering (2nd ed.). Cambridge University Press.
- Yang, X.-S. (2018). Mathematics for Civil Engineers: An Introduction. Dunedin Academic Press.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	Mandatory attendance of at least 60% of the lectures
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Cyber Security and Data Protection

Module Code: CSEMCSITSDP-01

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ralf Kneuper (Cyber Security and Data Protection)

Contributing Courses to Module

- Cyber Security and Data Protection (CSEMCSITSDP01-01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Case Study	

Weight of Module

see curriculum

Module Contents

- Data protection and privacy
- Cyber security building blocks
- Cyber security management
- Cryptography concepts
- Cryptography applications

Learning Outcomes

Cyber Security and Data Protection

On successful completion, students will be able to

- explain the core concepts of cyber security, data protection, and cryptography including their differences and relationships.
- compare the approaches to data protection within in different legal systems.
- apply data protection concepts to data science and other application scenarios.
- analyze application scenarios to identify the adequate cyber security management measures that should be implemented.
- explain the different approaches to data protection in different cultures.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Master Programmes in the IT & Technology field

Cyber Security and Data Protection

Course Code: CSEMCSITSDP01-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

With the increasing digitization and networking of IT systems, the need for safeguarding systems and the data processed by these systems has grown. The aim of this module is to provide an understanding of security measures needed, cyber security including cryptography, and data protection. While the need for cyber security is similar around the world, different cultures have different expectations regarding data protection and privacy. Nevertheless, personal data are often processed outside the country where the affected individuals live. Hence, the cultural aspects of data protection need to be taken into account wherever the data are processed. This course provides an overview of the main cyber security measures in different application scenarios, as well as their integration into an Information Security Management System, with particular focus on the relevant ISO/IEC 270xx family of standards. Cryptography provides an important tool set for cyber security and is used in many different application scenarios such as secure Internet protocols and block chain.

Course Outcomes

On successful completion, students will be able to

- explain the core concepts of cyber security, data protection, and cryptography including their differences and relationships.
- compare the approaches to data protection within in different legal systems.
- apply data protection concepts to data science and other application scenarios.
- analyze application scenarios to identify the adequate cyber security management measures that should be implemented.
- explain the different approaches to data protection in different cultures.

Contents

1. Foundations of Data Protection and Cyber Security
    - 1.1 Terminology and Risk Management
    - 1.2 Core Concepts of Cyber Security
    - 1.3 Core Concepts of Data Protection and Privacy
    - 1.4 Core Concepts of Cryptography
    - 1.5 Legal Aspects
2. Data Protection

- 2.1 Basic Concepts of Data Protection (ISO/IEC 29100, Privacy by Design)
- 2.2 Data Protection in Europe: the GDPR
- 2.3 Data Protection in the USA
- 2.4 Data Protection in Asia

3. Applying Data Protection
   - 3.1 Anonymity and Pseudonyms (k-Anonymity, i-Diversity, Differential Privacy)
   - 3.2 Data Protection in Data Science and Big Data
   - 3.3 User Tracking in Online Marketing
   - 3.4 Cloud Computing

4. Building Blocks of Cyber Security
   - 4.1 Authentication, Access Management and Control
   - 4.2 Cyber Security in Networks
   - 4.3 Developing Secure IT Systems (OWASP, etc.)

5. Cyber Security Management
   - 5.1 Security Policy
   - 5.2 Security and Risk Analysis
   - 5.3 The ISO 270xx Series
   - 5.4 IT Security and IT Governance
   - 5.5 Example: Cyber Security for Credit Cards (PCI DSS)

6. Cryptography
   - 6.1 Symmetric Cryptography
   - 6.2 Asymmetric Cryptography
   - 6.3 Hash Functions
   - 6.4 Secure Data Exchange (Diffie-Hellman, Perfect Forward Secrecy, etc.)

7. Cryptographic Applications
   - 7.1 Digital Signatures
   - 7.2 Electronic Money
   - 7.3 Secure Internet Protocols (TLS, IPSec, etc.)
   - 7.4 Block Chain

Literature
Compulsory Reading
Further Reading ▪ Amoroso, E., & Amoroso, M. (2017). From CIA to APT: An introduction to cyber security. Independently published. ▪ National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. ▪ Paar, C., & Pelzl, J. (2011). Understanding cryptography: A textbook for students and practitioners. Springer. ▪ Walker, B. (2019). Cyber security comprehensive beginners guide to learn the basics and effective methods of cyber security. Independently published.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	Mandatory attendance of at least 60% of the lectures
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Advanced Research Methods

Module Code: CSEMARM-01

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Markus C. Hemmer (Advanced Research Methods)

Contributing Courses to Module

- Advanced Research Methods (CSEMARM01-01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Written Assignment	

Weight of Module

see curriculum

Module Contents

- Principles of Research
- Research Approaches
- The Research Project
- Selected Formal Techniques
- Selected Interpretative Topics
- Scientific Reporting

Learning Outcomes

Advanced Research Methods

On successful completion, students will be able to

- demonstrate an understanding of principles of scientific inquiry and logical reasoning.
- apply formal techniques to modeling and theory generation.
- apply interpretative techniques to intercultural case studies.
- propose, plan, and conduct research projects under ethical constraints.
- evaluate study results to arrive at valuable and ethical conclusions.
- report study results responsibly in an objective and comprehensible form.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Methods	All Master Programmes in the Business field

Advanced Research Methods

Course Code: CSEMARM01-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Advanced research methods, specifically business research, is scientific inquiry that attempts to uncover new information which helps a business improve performance, maximizing shareholder value while adhering to ethical and moral compliance standards.Managers seeking to conduct empirical research must maintain validity, reliability, and trustworthiness when utilizing scientific methodologies in order to produce meaningful and actionable results. Research proposals are typically written prior to conducting research, which have a certain structure, enabling the researcher to properly plan, conduct, and analyze case studies and surveys. Different data collection strategies are used to collect both qualitative and quantitative data, depending on the research proposal goals. Managers utilize their understanding of research methodologies to accurately assess the quality of research.

Course Outcomes

On successful completion, students will be able to

- demonstrate an understanding of principles of scientific inquiry and logical reasoning.
- apply formal techniques to modeling and theory generation.
- apply interpretative techniques to intercultural case studies.
- propose, plan, and conduct research projects under ethical constraints.
- evaluate study results to arrive at valuable and ethical conclusions.
- report study results responsibly in an objective and comprehensible form.

Contents

1. Principles of Research
   - 1.1 Scientific Inquiry
   - 1.2 Principles of Reasoning
   - 1.3 From Data to Knowledge
   - 1.4 Models & Theories
   - 1.5 The Research Cycle

2. Research Approaches
   - 2.1 Experimental Design
   - 2.2 Engineering & Development
   - 2.3 Empirical Research & Case Studies

- 2.4 Interpretative Studies

3. The Research Project
   - 3.1 Topic Generation
   - 3.2 Types of Literature Reviews
   - 3.3 Developing a Research Design
   - 3.4 The Research Proposal

4. Selected Formal Techniques
   - 4.1 Foundations of Probability Theory & Inferential Statistics
   - 4.2 Data Acquisition
   - 4.3 Pattern Recognition & Classification
   - 4.4 Modelling & Theory Generation
   - 4.5 Artificial Intelligence in Research

5. Selected Interpretative Topics
   - 5.1 Phenomenology
   - 5.2 Hermeneutics & Discourse Analysis
   - 5.3 Ethnography & Ethnomethodology
   - 5.4 Critical Management Theory

6. Scientific Reporting
   - 6.1 Results Presentation & Visualization
   - 6.2 Interpretation
   - 6.3 Argumentation & Discussion
   - 6.4 Conclusions
   - 6.5 Ethical Considerations

Literature

Compulsory Reading

Further Reading

- Babbie, E. R. (2021). The practice of social research (15th ed.). Cengage Learning.
- Babbie, E. R. (2016). The practice of social research (14th ed.). Cengage Learning.
- Crossman, A. (2019). How to conduct an index for research. https://www.thoughtco.com/index-for-research-3026543
- Eurostat. (n.d.). Beginners: Statistical concept - Index and base year. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Beginners:Statistical_concept_-_Index_and_base_year
- Giles, D. (2004). Advanced research methods in psychology (Reprint). Psychology Press.
- Rea, L.M., & Parker, R.A. (2014). Designing and conducting survey research: A comprehensive guide, (4th ed). Jossey-Bass.
- Saunders, M., Thornhill, A., & Lewis, P. (2019). Research methods for business students (8th ed). Pearson.
- Takahashi, A. R. W., & Araujo, L. (2019). Case study research: Opening up research opportunities. RAUSP Management Journal, 55(1), 100–111.
- Widner, J., Woolcock, M., & Ortega Nieto, D. (Eds.). (2022). The case for case studies: Methods and applications in international development (strategies for social inquiry). Cambridge University Press.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	Mandatory attendance of at least 60% of the lectures
Type of Exam	Written Assessment: Written Assignment

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
94 h	36 h	0 h	20 h	0 h	150 h

Seminar: Advanced Cyber Security

Module Code: CSEMCSSAITS

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	CSEMCSITSDP01-01	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Seminar: Advanced Cyber Security)

Contributing Courses to Module

- Seminar: Advanced Cyber Security (CSEMCSEAITSC01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Research Essay	

Weight of Module

see curriculum

Module Contents

- This course covers selected advanced topics in cyber security, including the closely related topics of data protection and cryptology, and discusses them in detail. Based on a list of topics updated regularly, students select or are assigned a specific topic about which they write a scientific research essay.

Learning Outcomes

Seminar: Advanced Cyber Security

On successful completion, students will be able to

- analyze and describe one aspect of cyber security in detail.
- independently analyze selected topics in cyber security and link them with well-known concepts, as well as critically question and discuss them.
- transfer theoretically-acquired knowledge to a specific context.
- write and edit a scientific essay on a relevant select topic.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development.	All Master Programmes in the IT & Technology field.

Seminar: Advanced Cyber Security

Course Code: CSEMCSEAITSC01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	CSEMCSITSDP01-01

Course Description

This seminar covers advanced topics in cyber security. With the growth of the internet and digitization, cyber security has become an increasingly important topic and needs to be taken into account in the development and setup of software and IT systems. Typical topics that may be addressed include the analysis of selected aspects of information security management systems according to the ISO 27000 series; the use of cyber security to support data protection; and the detailed analysis and description of certain algorithms or cryptosystems.

Course Outcomes

On successful completion, students will be able to

- analyze and describe one aspect of cyber security in detail.
- independently analyze selected topics in cyber security and link them with well-known concepts, as well as critically question and discuss them.
- transfer theoretically-acquired knowledge to a specific context.
- write and edit a scientific essay on a relevant select topic.

Contents

- The seminar covers different advanced topics regarding cyber security. Each participant must prepare a research essay on a topic assigned to him/her.

Literature

Compulsory Reading

Further Reading

- Turabian, K. L. (2013). A manual for writers of research papers, theses, and dissertations. Chicago: University of Chicago Press.
- Swales, J. M., & Feak, C. R. (2012). Academic writing for graduate students, essential tasks and skills. Michigan: University of Michigan Press.
- Bailey, S. (2011). Academic writing for international students of business. New York, NY: Routledge.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
114 h	36 h	0 h	0 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Slides	☑ Guideline

Cryptology

Module Code: CSEMCSC-01

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	CSEMCSITSDP01-01	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Björn Kaidel (Cryptology)

Contributing Courses to Module

- Cryptology (CSEMCSEAITSC02-01)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Basic Concepts of Cryptology
- Symmetric Cryptosystems
- Asymmetric Cryptosystems
- Authentication
- Cryptanalysis
- Cryptology and the Internet
- Practical Aspects of Cryptology
- Applications

Learning Outcomes

Cryptology

On successful completion, students will be able to

- discuss the main cryptographic systems and algorithms and their relevance in IT today.
- discuss the security of internet-based applications.
- evaluate different cryptographic systems and algorithms to select an appropriate solution for real-world problems in IT.
- apply standard cryptographic systems and algorithms to solve real-world problems in IT.
- appraise existing cryptographic solutions to real-world problems and identify major weaknesses where relevant.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development	All Master Programmes in the IT & Technology field

Cryptology

Course Code: CSEMCSEAITSC02-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	CSEMCSITSDP01-01

Course Description

The focus of this course is to provide a thorough introduction to cryptology and its main sub-disciplines cryptography and cryptanalysis. Particular emphasis is put on the use of cryptology to support the security of IT systems. In the first part of the courses, students gain a solid understanding of the basic concepts of cryptology, in particular symmetric and asymmetric cryptosystems, authentication, and common approaches to break these cryptosystems using cryptanalysis. Based on this foundational understanding, the course goes on to cover the practical use of cryptology, starting with an introduction to the standard protocols and techniques used to ensure the security of communication via the internet. Next, practical aspects of applying cryptographic techniques and algorithms are covered, such as their long-term security. Finally, some application examples show how the concepts of cryptology are commonly used and can be used to solve challenges such as online banking.

Course Outcomes

On successful completion, students will be able to

- discuss the main cryptographic systems and algorithms and their relevance in IT today.
- discuss the security of internet-based applications.
- evaluate different cryptographic systems and algorithms to select an appropriate solution for real-world problems in IT.
- apply standard cryptographic systems and algorithms to solve real-world problems in IT.
- appraise existing cryptographic solutions to real-world problems and identify major weaknesses where relevant.

Contents

1. Basic Concepts of Cryptology
    - 1.1 Introduction and Terminology
    - 1.2 IT Security, Threats and Common Attacks
    - 1.3 Historical Overview
    - 1.4 Security Criteria
    - 1.5 Hash Functions
2. Symmetric Cryptosystems

- 2.1 Substitution and Transposition
- 2.2 Stream and Block Ciphers
- 2.3 Digital Encryption Standard (DES)
- 2.4 Advanced Encryption Standard (AES)
- 2.5 Cryptographic Hash Functions
- 2.6 Message Authentication Codes

3. Asymmetric Cryptosystems
   - 3.1 The RSA Schemes
   - 3.2 Elliptic Curves
   - 3.3 Digital Signatures
   - 3.4 The Diffie-Hellman Key Exchange
   - 3.5 Key Exchange and Public Key Infrastructures

4. Authentication
   - 4.1 Passwords
   - 4.2 Challenge-Response and Zero-Knowledge
   - 4.3 Biometrics-Based Authentication
   - 4.4 Authentication in Distributed Systems
   - 4.5 Smartcards
   - 4.6 Identity and Anonymity

5. Cryptanalysis
   - 5.1 Frequency Analysis
   - 5.2 Brute-Force Attacks
   - 5.3 Rainbow Tables
   - 5.4 Security Models
   - 5.5 Side-Channel Attacks
   - 5.6 Modern Cryptanalytic Algorithms

6. Cryptology and the Internet
   - 6.1 Internet Protocols
   - 6.2 IPSec
   - 6.3 Transport Layer Security
   - 6.4 Secure E-Mail
   - 6.5 Secure DNS

7. Practical Aspects of Cryptology

7.1 Random Number Generation
7.2 Long-Term Security
7.3 Incorporating Cryptography into Application Development
7.4 Legal and Regulatory Aspects

8. Applications
8.1 Online Banking
8.2 Blockchain
8.3 Voting
8.4 Steganography and Watermarks
8.5 The Tor Project

Literature
Compulsory Reading
Further Reading ▪ Esslinger, B. (2010). The CrypTool script: Cryptography, mathematics, and more (10th ed.). CrypTool Development Team. ▪ Katz, J., & Lindell, Y. (2014). Introduction to modern cryptography (2nd ed.). Chapman and Hall/CRC. ▪ Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2015). Handbook of applied cryptography. CRC Press.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	Mandatory attendance of at least 60% of the lectures
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Cyber Risk Assessment and Management

Module Code: CSEMCSECRAM_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Carsten Skerra (Cyber Risk Assessment and Management)

Contributing Courses to Module

- Cyber Risk Assessment and Management (CSEMCSECRAM01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Organizational IT Risk Management
- Measuring the Cyber Threat
- Threat Modeling
- Standardization and Compliance
- Risk Assessment
- The Cyber-Resilient Organization

Learning Outcomes

Cyber Risk Assessment and Management

On successful completion, students will be able to

- understand the process of attack modeling.
- associate a cost with attack outcomes.
- understand black swan events.
- evaluate the impact that legislation has on risks and costs.
- understand how an organization needs to make decisions based on risk.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Cyber Risk Assessment and Management

Course Code: CSEMCSECRAM01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Decisions on making changes or not should be informed by the risk of that action or inaction. This is dictated by the cost a potentially successful attack would have. But how to model attacks and associate costs with them? We will explore the discipline of attack modeling and risk evaluation in this course.

Course Outcomes

On successful completion, students will be able to

- understand the process of attack modeling.
- associate a cost with attack outcomes.
- understand black swan events.
- evaluate the impact that legislation has on risks and costs.
- understand how an organization needs to make decisions based on risk.

Contents

1. Organizational IT Risk Management
   - 1.1 Business Need of Risk Management
   - 1.2 Anatomy of a Data Exfiltration Attack
   - 1.3 Cyber Catastrophes
   - 1.4 Cyber Risk
2. Measuring the Cyber Threat
   - 2.1 Measurement and Management
   - 2.2 Cyber Threat Metrics
   - 2.3 Measuring the Threat for an Organization
   - 2.4 The Likelihood of Major Cyber Attacks
   - 2.5 Black Swan Events
3. Threat Modeling
   - 3.1 Attack Tree Methodology
   - 3.2 STRIDE
   - 3.3 DREAD

3.4 LINDDUN

4. Standardization and Compliance
   - 4.1 NIST Risk Management Framework
   - 4.2 ISO 27005
   - 4.3 BSI 100-3

5. Risk Assessment
   - 5.1 Methodologies
   - 5.2 Factoring in Black Swan Events
   - 5.3 Continuous Reevaluation

6. The Cyber-Resilient Organization
   - 6.1 Changing Approaches to Risk Management
   - 6.2 Incident Response and Crisis Management
   - 6.3 Resilience Engineering, Security Solutions and Finances
   - 6.4 Cyber Insurance

Literature

Compulsory Reading

Further Reading

- Antonucci, D. (2017). The cyber risk handbook: Creating and measuring effective cybersecurity capabilities. Wiley.
- Refsdal, A., Solhaug, B., & Stolen, K. (2015). Cyber-risk management. Springer.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Practice Exam
- ☑ Online Tests

IT Systems: Software

Module Code: CSEMIMITSS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Carsten Skerra (IT Systems: Software)

Contributing Courses to Module

- IT Systems: Software (CSEMIMITSS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Basics of software development
- Data formats and coding
- Firmware and operating systems
- Classification and application areas of desktop applications
- Databases
- Application-specific software systems in the company
- Ergonomic aspects of computer workstation design and human-machine interaction

Learning Outcomes

IT Systems: Software

On successful completion, students will be able to

- understand the basics of software development.
- evaluate data formats and their application in different scenarios.
- understand the storage and processing of complex data and information.
- evaluate operating systems and their conceptual differences for application and security.
- understand the application areas of typical desktop applications and assess their limitations.
- differentiate database-based enterprise solutions and evaluate their usefulness for business applications.
- identify requirements for computer workstations and implement suitable solutions.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

IT Systems: Software

Course Code: CSEMIMITSS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The course introduces the function and application areas of typical software systems used in companies. Concepts of software development and programming languages form the basis for this. The course provides the necessary knowledge about data formats, their conversion, compression and transformation in order to apply them to the representation of complex data. It describes operating systems for local and mobile computers and their conceptual differences and areas of application. Based on this, typical desktop applications from text to graphics processing are introduced and their field of application is explained. After an introduction to the concept of databases, typical server-based solutions for information management are discussed. The course concludes with an examination of ergonomic software aspects and human-machine interaction.

Course Outcomes

On successful completion, students will be able to

- understand the basics of software development.
- evaluate data formats and their application in different scenarios.
- understand the storage and processing of complex data and information.
- evaluate operating systems and their conceptual differences for application and security.
- understand the application areas of typical desktop applications and assess their limitations.
- differentiate database-based enterprise solutions and evaluate their usefulness for business applications.
- identify requirements for computer workstations and implement suitable solutions.

Contents

1. Basics of software development
   - 1.1 Fundamentals of programming and programming languages
   - 1.2 Software lifecycle
   - 1.3 Software licensing models and patenting
2. Data formats
   - 2.1 ASCII code, Unicode and markup languages
   - 2.2 Page description languages (HTML, XHTML, HTML5)
   - 2.3 Script languages for web applications
   - 2.4 Text formats

- 2.5 Raster, vector and meta graphic formats (PNG, TIFF, JPEG, SVG, WMF)

3. Conversion, compression and transformation of data
   - 3.1 Data conversion (XMI, Transcoding)
   - 3.2 Data compression
   - 3.3 Data transformation
   - 3.4 Application to audiovisual data

4. System software
   - 4.1 Firmware, BIOS, UEFI
   - 4.2 Operating systems for end users
   - 4.3 Server-based operating systems
   - 4.4 Mobile operating systems

5. Desktop applications
   - 5.1 Office software
   - 5.2 Graphics and image processing programs
   - 5.3 Software for mathematics and statistics
   - 5.4 Desktop publishing and visualization
   - 5.5 Audio and video systems

6. Database systems
   - 6.1 Relational databases and SQL
   - 6.2 NoSQL and non-relational databases
   - 6.3 In-memory databases
   - 6.4 Data warehouses

7. Business information systems
   - 7.1 Web-based systems and cloud solutions
   - 7.2 Document and content management
   - 7.3 Resource-based information management
   - 7.4 Knowledge management, dashboards and expert systems

8. Ergonomics at the computer workplace
   - 8.1 Anthropometry and system ergonomics
   - 8.2 Product and production ergonomics
   - 8.3 Computer workstation ergonomics
   - 8.4 Software ergonomics
   - 8.5 Design aspects of the graphical user interface

Literature
Compulsory Reading
Further Reading ▪ Bourke, P./Fairley, R.E. (Hrsg.) (2014): SWEBOK V3.0 – Guide to the Software Engineering Body of Knowledge. IEEE Computer Society. ▪ Brookshear, G., & Brylow, D. (2019). Computer science: An overview (13th ed.). Pearson.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Practice Exam
- ☑ Online Tests

IT Systems: Hardware

Module Code: CSEMIMITSH_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Markus Hemmer (IT Systems: Hardware)

Contributing Courses to Module

- IT Systems: Hardware (CSEMIMITSH01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Computer Arithmetics
- Integrated Circuits
- Storage systems
- Input/output systems
- Fundamentals of data transmission
- Computer networks
- Server and data centers

Learning Outcomes

IT Systems: Hardware

On successful completion, students will be able to

- understand computer arithmetic and to apply it to logical problems.
- know the components of computer systems and explain their functional principles.
- differentiate methods of data transmission and evaluate their conceptual differences in application.
- evaluate computer network technologies and their fields of application.
- know and assess requirements for the construction and operation of data centers.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

IT Systems: Hardware

Course Code: CSEMIMITSH01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

This course provides an understanding of how computer-based systems work and serves as a basis for communication and leadership for appropriate information technology professionals. It describes the logic with which digital computers work and the technique of creating digital circuits. It also explains the structure of typical computer systems and the functioning of processors, memory devices and peripheral input and output devices. The course clarifies the basics of communications engineering and compares the application criteria of wired and wireless data transmission technologies. On this basis, small server infrastructures, mainframes and supercomputers are introduced and knowledge about the construction and operation of data centers is taught.

Course Outcomes

On successful completion, students will be able to

- understand computer arithmetic and to apply it to logical problems.
- know the components of computer systems and explain their functional principles.
- differentiate methods of data transmission and evaluate their conceptual differences in application.
- evaluate computer network technologies and their fields of application.
- know and assess requirements for the construction and operation of data centers.

Contents

1. Basics of computer arithmetics
   - 1.1 value arithmetic, numeral systems
   - 1.2 propositional logic and boolean operators
   - 1.3 Computer Arithmetics
2. Integrated Circuits
   - 2.1 Integrated circuits and semiconductor production
   - 2.2 Parallel and serial interfaces
   - 2.3 Mainboard components
   - 2.4 Processors and memory
3. Storage systems

- 3.1 Hard disk space
- 3.2 Optical storage media
- 3.3 Magnetic storage media
- 3.4 Solid State Drive

4. Input/output systems
   - 4.1 Input Devices
   - 4.2 Touch Screen Systems
   - 4.3 Graphical output devices
   - 4.4 Printer Systems

5. Fundamentals of data transmission
   - 5.1 Wired data transmission and modulation
   - 5.2 Transmission via light
   - 5.3 Antennas and satellite technology
   - 5.4 Mobile networks
   - 5.5 RFID and Near-Field Communication

6. Computer networks
   - 6.1 Network Topology
   - 6.2 Ethernet frame and network protocols
   - 6.3 Switching, routing and data flow control
   - 6.4 Network diagnostics

7. Server and data centers
   - 7.1 Data center Tier Classification Standard
   - 7.2 Server systems, mainframes and supercomputers
   - 7.3 Building data centers
   - 7.4 Data center security and operations aspects
   - 7.5 Principles of virtualization

Literature
Compulsory Reading
Further Reading ▪ Gómez, J. M., Mora, M., Raisinghani, M. S., Nebel, W., & O'Connor, R. V. (2017). Engineering andmanagement of data centers: An IT service management approach. Springer. ▪ Hwaiyu Geng, P. E. (2014). Data center handbook. John Wiley & Sons. ▪ Tanenbaum, A. S., & Wetherall, D. (2014). Computer networks (5th ed.). Pearson Education. ▪ Van Steen, M., & Tanenbaum, A. S. (2017). Distributed systems. Maarten van Steen.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Instructional Methods

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Practice Exam
- ☑ Online Tests

Cyber Systems and Network Forensics

Module Code: CSEMCSECSNF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ahmed Taha (Cyber Systems and Network Forensics)

Contributing Courses to Module

- Cyber Systems and Network Forensics (CSEMCSECSNF01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Operating systems
- Networking
- Forensics
- Cryptography
- Cyber attacks

Learning Outcomes

Cyber Systems and Network Forensics

On successful completion, students will be able to

- understand basic internals of operating systems.
- understand the most important network protocols.
- diagnose attacks against computers and networks.
- understand the importance of evidence collection and preservation of evidence.
- understand basic attack patterns.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Cyber Systems and Network Forensics

Course Code: CSEMCSECSNF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The computer security practitioner has the difficult task of needing to know the fundamentals of both operating systems and networks. In this course we review operating systems and networks from a forensics perspective. The end result is the understanding of attacks against an organization.

Course Outcomes

On successful completion, students will be able to

- understand basic internals of operating systems.
- understand the most important network protocols.
- diagnose attacks against computers and networks.
- understand the importance of evidence collection and preservation of evidence.
- understand basic attack patterns.

Contents

1. Operating Systems
   - 1.1 Concepts
   - 1.2 Memory management
   - 1.3 Process management
   - 1.4 Device management
   - 1.5 Input/Output
2. Operating Systems internals
   - 2.1 Syscalls
   - 2.2 Process table analysis
   - 2.3 Windows Registry
   - 2.4 Filesystem forensics
   - 2.5 Common attacks
3. The Network Stack
   - 3.1 TCP/IP and OSI network stack
   - 3.2 Core Internet services

3.3 The World Wide Web
3.4 Transport layer encryption
3.5 Common attacks

4. Computer Forensics
   4.1 Evidence
   4.2 Malware
   4.3 Data exfiltration
   4.4 Attacks against computer forensics

5. Network Forensics
   5.1 Indicators of Compromise
   5.2 Data enrichment and pivot points
   5.3 Attacks against network forensics

6. Attacks as viewed from the Host and Network
   6.1 Techniques, Tactics and Procedures
   6.2 Intrusion Detection and Prevention
   6.3 Correlation of events

Literature

Compulsory Reading

Further Reading

- Kävrestad, J. (2020). Fundamentals of digital forensics: Theory, methods, and real-life applications (2nd ed.). Springer.
- Najarian, J. P. (2020). Computer operating systems. Salem Press Encyclopedia of Science.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	Mandatory attendance of at least 60% of the lectures
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Secure Networking

Module Code: CSEMCSEESN1_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	CSEMCSECSNF01_E, CSEMIMITSH01_E	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ahmed Taha (Secure Networking)

Contributing Courses to Module

- Secure Networking (CSEMCSEESN01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Cryptographic protocols
- Network security controls
- Application layer security issues
- Wireless security
- Intrusion detection and prevention

Learning Outcomes

Secure Networking

On successful completion, students will be able to

- understand the cryptography used in networks.
- understand how identity and authentication work.
- work with various network security protocols.
- deploy network access controls.
- understand the concepts of Cloud security.
- deploy intrusion detection.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Secure Networking

Course Code: CSEMCSEESN01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	CSEMCSECSNF01_E, CSEMIMITSH01_E

Course Description

Systems are internally interconnected between each other and are communicating over the Internet as well. The general mission of network security is about providing confidentiality, integrity, nonrepudiation and availability of data that is transmitted in networks or stored in networked systems.

Course Outcomes

On successful completion, students will be able to

- understand the cryptography used in networks.
- understand how identity and authentication work.
- work with various network security protocols.
- deploy network access controls.
- understand the concepts of Cloud security.
- deploy intrusion detection.

Contents

1. Overview of Network Security
   - 1.1 ISO/OSI and TCP/IP Model
   - 1.2 Attacks and Countermeasures
   - 1.3 Network Topologies
   - 1.4 Basic Security Models
2. Infrastructural Components
   - 2.1 Firewalls
   - 2.2 Routing ACLs
   - 2.3 Switches
   - 2.4 Attacks in Conjunction with Routers, Switches and Firewalls
3. Cryptography

- 3.1 Symmetric Cryptography
- 3.2 Asymmetric Cryptography and Key Management
- 3.3 Cryptographic Hash Function
- 3.4 Quantum Resistant Encryption and Quantum Key Exchange

4. Authentication
   - 4.1 Identity
   - 4.2 System and User Authentication
   - 4.3 Data Authentication
   - 4.4 Multi-Factor Authentication

5. Security Protocols
   - 5.1 Public-Key Infrastructure
   - 5.2 IPsec – Network Layer Security Protocol
   - 5.3 TLS – Transport Layer Security Protocol
   - 5.4 Kerberos – Authentication Protocol
   - 5.5 SSH – Remote Login Security Protocol
   - 5.6 PGP and S/MIME – E-Mail Security Protocol

6. Wireless Network Security
   - 6.1 Wi-Fi Protected Access
   - 6.2 WPA2/IEEE 802.11i
   - 6.3 Bluetooth Security
   - 6.4 ZigBee Security

7. Cloud Security
   - 7.1 Cloud Service Models
   - 7.2 Cloud Security Models
   - 7.3 Multiple Tenants
   - 7.4 Searching in Encrypted Data

8. Intrusion Detection and Prevention
   - 8.1 Basic Concepts
   - 8.2 Network-based and Host-based Detections
   - 8.3 Signature-based Approach
   - 8.4 Behavioral-based Approach

Literature
Compulsory Reading
Further Reading ▪ Bullock, J., & Parker, J. (2017). Wireshark for security professionals: Using wireshark and themetasploit framework. John Wiley & Sons. ▪ Monte, M. (2015). Network attacks and exploitation: A framework. John Wiley & Sons. ▪ Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners.Springer. ▪ Schneier, B. (2015). Applied cryptography: Protocols, algorithms and source code in C. (20thanniversary ed.). John Wiley & Sons. ▪ Wack, J. P. (2002). Guidelines on firewalls and firewall policy. National Institute of Standards andTechnology.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	Mandatory attendance of at least 60% of the lectures
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Theoretical Computer Science for IT Security

Module Code: CSEMCSETCSITS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Theoretical Computer Science for IT Security)

Contributing Courses to Module

- Theoretical Computer Science for IT Security (CSEMCSETCSITS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Algorithms and Data Structures
- Formal Languages and Automata Theory
- Computability, Decidability and Complexity
- Logic
- Algorithm and Program Verification
- Artificial Intelligence and Machine Learning

Learning Outcomes

Theoretical Computer Science for IT Security

On successful completion, students will be able to

- understand limitations of data structures, algorithms and computation in general.
- use formal languages and automata to solve security problems.
- use machine learning techniques in data analysis.
- use logic and knowledge representation.
- understand the principles of program analysis and verification.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Theoretical Computer Science for IT Security

Course Code: CSEMCSETCSITS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

In the practice of computer security, we often bump up on the limitations of IT and computing. What sometimes seems like it should be solvable, turns out to be hard or impossible for current computers. Computer science theory provides the framework for understanding difficult problems and often offers a path to other solutions. Here, machine learning often can provide a stochastic solution where there is no precise one. We also cover the program analysis and verification topic in this course.

Course Outcomes

On successful completion, students will be able to

- understand limitations of data structures, algorithms and computation in general.
- use formal languages and automata to solve security problems.
- use machine learning techniques in data analysis.
- use logic and knowledge representation.
- understand the principles of program analysis and verification.

Contents

1. Algorithms and Data Structures
   - 1.1 Algorithms, Programming Languages and Data Structures
   - 1.2 Graphs and Trees
   - 1.3 Sorting and Searching
   - 1.4 Algorithm Analysis
2. Formal Languages and Automata Theory
   - 2.1 Languages and Grammars
   - 2.2 Regular Languages and Finite State Machines
   - 2.3 Context-free Languages and Pushdown Automata
   - 2.4 Context-sensitive Languages and Turing Machines
3. Computability, Decidability and Complexity
   - 3.1 Computability
   - 3.2 Decidability and Decision Problems

3.3 Complexity Theory
3.4 Quantum Computing

4. Logic
   4.1 Propositional Logic
   4.2 Predicate Logic
   4.3 Resolution Calculus
   4.4 Tableau Calculus

5. Algorithm and Program Verification
   5.1 Program Analysis
   5.2 Algebraic, Operational and Denotational Semantics
   5.3 Abstract Interpretation

6. Artificial Intelligence and Machine Learning
   6.1 Supervised vs. Unsupervised Learning
   6.2 Linear and non-linear Regression
   6.3 Logistic Regression
   6.4 Artificial Neural Networks

Literature

Compulsory Reading

Further Reading

- Goodfellow, I. / Bengio, Y. / Courville, A. (2016): Deep Learning. MIT Press, Cambridge, MA.
- Graham, R. L. / Knuth, D. E. / Patashnik, O. (1994): Concrete Mathematics. A Foundation for Computer Science. 2nd Edition, Addison-Wesley, Upper Saddle River, NJ.
- Hopcroft, J. E. / Ullman J. D. (2006): Introduction to Automata Theory, Languages, and Computation. 3rd Edition, Pearson Education, London.
- Nielson, F. / Nielson, H. R. / Hankin, C. (1999): Principles of Program Analysis. Springer-Verlag, Berlin.
- Nipkow T. / Klein, G. (2016): Concrete Semantics. With Isabelle/HOL. Springer, Berlin.
- Russell, S. / Norvig, P. (2016): Artificial Intelligence: A Modern Approach, Pearson Education, London.
- Shaffer, C. A. (2011): Data Structures and Algorithm Analysis in C++. 3rd Edition, Dover Books on Computer Science, Mineola, NY.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	Mandatory attendance of at least 60% of the lectures
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
84 h	36 h	0 h	30 h	0 h	150 h

Seminar: Standards and Frameworks

Module Code: CSEMIMSSF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Andrew Adjah Sai (Seminar: Standards and Frameworks)

Contributing Courses to Module

- Seminar: Standards and Frameworks (CSEMIMSSF01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Research Essay	

Weight of Module

see curriculum

Module Contents

The seminar presents a methodology to question principles of standards and frameworks, to identify and validate explicit and implicit assumptions and to evaluate recommended categorizations and workflows with respect to their feasibility.

Learning Outcomes

Seminar: Standards and Frameworks

On successful completion, students will be able to

- name IT-relevant standards and frameworks and to define their areas of application.
- question principles of standards and frameworks with regard to their feasibility and logical argumentation.
- identify and validate assumptions made in standards.
- check recommended categorizations and workflows for plausibility
- identify administrative and technical requirements for implementation
- identify and prioritize stakeholder expectations.
- make recommendations for the implementation and maintenance of the standards.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Seminar: Standards and Frameworks

Course Code: CSEMIMSSF01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The seminar familiarizes students with a procedure for the critical evaluation of international standards and frameworks of IT. It brings students into the position to evaluate the value and the constraints of a standard for a given industry scenario and to give advice to the executive management in this regard. The seminar focuses on the critical evaluation of the principles and assumptions of standards, the consistency and coherence of recommended categories and work instructions and the assessment of the feasibility, implementation and maintenance of the standard. On this basis, the students prepare a report for a given standard in a given industry scenario, which evaluates the standard according to these criteria and concludes with a recommendation for endorsement or rejection of the standard.

Course Outcomes

On successful completion, students will be able to

- name IT-relevant standards and frameworks and to define their areas of application.
- question principles of standards and frameworks with regard to their feasibility and logical argumentation.
- identify and validate assumptions made in standards.
- check recommended categorizations and workflows for plausibility
- identify administrative and technical requirements for implementation
- identify and prioritize stakeholder expectations.
- make recommendations for the implementation and maintenance of the standards.

Contents

- In this seminar, international standards for the IT sector are examined for their usability and preconditions. The selected standards include de facto and de jure standards, good practices (GxPs), frameworks (such as ARIS, TOGAF, COBIT, ITIL, CMMI), project management frameworks and various IT-relevant ISO standards.The analysis starts with an evaluation of the similarities and differences with regard to the application areas of the standards. This is followed by an assessment of the intention of the editors, the popularity of the standard and the reasons for its introduction in selected industry sectors. On this basis, the students write a seminar paper in which they make a critical assessment of the feasibility for a given standard in a given industry scenario. The seminar paper covers the following criteria:
  - Principles: A critical evaluation of the principles of the standard for the given industry scenario.

- Assumptions: Identification of the explicit and implicit assumptions made in the standard and their plausibility check in the given industrial scenario.
- Categories: Evaluation of the conformity of the given categorizations with the industry scenario.
- Processes: Determination of the necessary workflows and assessment of feasibility.
- Expectations: Identification of stakeholder requirements and expectations.
- Consistency check: Identification of contradictions in one of the above categories.
- Coherence check: assessment of completeness and, if necessary, recommendations for further standardization.
- Requirements: Determination of the preconditions for implementing the standard.
- Maintenance: An estimate of the effort required to maintain and update the standard. The seminar paper concludes with either an endorsement or a rejection of the standard for the given industry scenario, rationally justified with the results of the analysis.

Literature

Compulsory Reading

Further Reading

- Limited, A. (2020). ITIL 4 [electronic resource] : Digital and IT Strategy. London The Stationery Office Ltd, 2020.
- TOGAF Version 9.1. (2014). Zaltbommel Van Haren Publishing 2014.
- Project Management Institute H. (2017): A Guide to the Project Management Body of Knowledge (PMBOK® Guide)–Sixth Edition. Newtown Square, Pennsylvania: Project Management Institute.
- van Wessel, R. (Hrsg.) (2010): Toward Corporate IT Standardization Management. Frameworks and Solutions. IGI Global, Hershey, PA.

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	Mandatory attendance of at least 60% of the lectures
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
114 h	36 h	0 h	0 h	0 h	150 h

Project: Current Challenges of Cyber Security

Module Code: CSEMCSEPCCCS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	CSEMCSITSDP01-01	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ahmed Taha (Project: Current Challenges of Cyber Security)

Contributing Courses to Module

- Project: Current Challenges of Cyber Security (CSEMCSEPCCCS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Campus Studies Written Assessment: Project Report	

Weight of Module

see curriculum

Module Contents

Computer Security is constantly evolving. This course brings the student in touch with the state-of-the art security research and practice by applying his/her knowledge to a current problem in this field.

Learning Outcomes

Project: Current Challenges of Cyber Security

On successful completion, students will be able to

- complete a project in the field of computer security that includes a research angle.
- explore computer security beyond the established state of the art.
- write a report highlighting the student's contribution to the interdisciplinary science of computer security.
- contribute to the state-of-the-art in computer security.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Project: Current Challenges of Cyber Security

Course Code: CSEMCSEPCCCS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	CSEMCSITSDP01-01

Course Description

Computer Security is constantly evolving. In this project, students will have the opportunity to contribute to the interdisciplinary science of computer security by applying their knowledge to a current topic in computer science that requires a comprehensive novel computer security approach. Topics may be the analysis of a particular threat, a report and analysis of a new security technology, the implementation of a security solution or a project specifically using security best practices, etc. In this way, students can demonstrate proficiency of computer security and prepare for the Master's thesis.

Course Outcomes

On successful completion, students will be able to

- complete a project in the field of computer security that includes a research angle.
- explore computer security beyond the established state of the art.
- write a report highlighting the student's contribution to the interdisciplinary science of computer security.
- contribute to the state-of-the-art in computer security.

Contents

- To a given problem and/or a given context, the student will research the subject, develop an appropriate solution and then submit the report and if appropriate any code and specific data. Specific problems and contexts will be provided by the tutor but proposals by the students can be considered.

Literature
Compulsory Reading
Further Reading ▪ Case Studies (Cyber): https://www.securitymagazine.com/topics/2664-case-studies-cyber ▪ Falliere, N. / O Murchu, L. / Chien, E. (2010): W32.Stuxnet Dossier. Symantec, Tempe, AZ. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf ▪ Hacquebord, F. (2020): Pawn Storm in 2019 A Year of Scanning and Credential Phishing on High-Profile Targets. Trend Micro Research, Irving, TX. https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf ▪ Vulnerability Notes Database: https://www.kb.cert.org/vuls/

Study Format Campus Studies

Study Format	Course Type
Campus Studies	Campus Lecture

Information about the examination	
Examination Admission Requirements	
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
114 h	36 h	0 h	0 h	0 h	150 h

Instructional Methods	
Learning Material	**Exam Preparation**
☑ Slides	☑ Guideline

Cyber Criminality

Module Code: DLMIMWCK_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Jetzabel Maritza Serna- Olvera (Attack Scenarios and Incident Response) / Dr. Jetzabel Maritza Serna- Olvera (Project: Cyber Forensics)

Contributing Courses to Module

- Attack Scenarios and Incident Response (DLMIMWCK01_E)
- Project: Cyber Forensics (DLMIMWCK02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Scenarios and Incident Response • Study Format "Distance Learning": Exam, 90 Minutes Project: Cyber Forensics • Study Format "Distance Learning": Portfolio

Weight of Module

see curriculum

Module Contents

Attack Scenarios and Incident Response

- Threat scenarios
- attack vectors
- Preventive measures
- Reactive measures
- Current situation of IT security

Project: Cyber Forensics

The project is concerned with the question of which procedure is suitable to react to computer-criminal incidents in a company. It deals with forensic procedures for the collection of evidence that can be used in court as well as recommendations for risk minimization, communication and prevention of such incidents. A current list of topics can be found in the Learning Management System.

Learning Outcomes

Attack Scenarios and Incident Response

On successful completion, students will be able to

- assess threat scenarios and their effects.
- name attack vectors and select adequate countermeasures.
- apply electronic evidence procedures to selected attack scenarios.
- develop preventive measures.
- identify reactive measures and assess their effectiveness.
- collect and evaluate information on the current threat situation.

Project: Cyber Forensics

On successful completion, students will be able to

- name basic methods and techniques of computer forensics and their limitations.
- identify the systems and business processes affected by a computer crime and carry out a risk assessment.
- recommend measures to secure electronic evidence and evaluate its usability in court.
- develop recommendations for incident communication, response and prevention.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Attack Scenarios and Incident Response

Course Code: DLMIMWCK01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

This course provides students with knowledge for identification and action planning in dealing with criminal offences in the digital environment. It describes how weaknesses in hardware and software and their application can be exploited for criminal activities. In addition, the course introduces typical threat scenarios and the ways in which attacking systems can penetrate a computer system. The course also introduces methods of electronic evidence and shows how legally usable information can be obtained in case of an attack. This is followed by a discussion of the development of preventive measures and the possibilities for reacting in the event of a concrete threat. The course concludes with a discussion of how information on the current security situation can be obtained from reports by security authorities (such as BSI, Europol, NCA, FBI).

Course Outcomes

On successful completion, students will be able to

- assess threat scenarios and their effects.
- name attack vectors and select adequate countermeasures.
- apply electronic evidence procedures to selected attack scenarios.
- develop preventive measures.
- identify reactive measures and assess their effectiveness.
- collect and evaluate information on the current threat situation.

Contents

1. Introduction
   - 1.1 Computer crime as distinct from other offences
   - 1.2 Vulnerabilities in computers and mobile devices
   - 1.3 An overview of malware
   - 1.4 Social engineering and the human factor

2. Criminal basis
   - 2.1 Identity abuse
   - 2.2 Theft of intellectual property
   - 2.3 Falsification of evidentiary data
   - 2.4 Computer fraud

3. Specific offences
   - 3.1 Data Theft
   - 3.2 Digital blackmailing
   - 3.3 Computer sabotage
   - 3.4 Industrial espionage

4. Attack vectors
   - 4.1 Attacks on Chip and Firmware Level
   - 4.2 Attacks at operating system level
   - 4.3 Attacks at network and server level
   - 4.4 Attacks at application level
   - 4.5 Attacks at the organizational level

5. IT forensics and electronic evidence
   - 5.1 Identification, localization and handling of polymorphisms
   - 5.2 Detection mechanisms
   - 5.3 Finding electronic evidence
   - 5.4 Data recovery and evidence recovery
   - 5.5 Legal limits and predictive policing

6. Preventive measures
   - 6.1 Measures on hardware level
   - 6.2 Access permission, authorization and authentication
   - 6.3 Awareness & Training
   - 6.4 Incident Response Planning

7. Reactive measures
   - 7.1 Initial assessment and extent of damage
   - 7.2 Prevention of persistent damage
   - 7.3 Collection, exchange and distribution of information
   - 7.4 Cooperation with security authorities and cooperation partners
   - 7.5 Recommended actions for companies

8. The current security situation
   - 8.1 Current reports of the safety authorities
   - 8.2 Evaluation of the recommendations of the safety authorities
   - 8.3 Current topics of the Europol Awareness Campaign

Literature
Compulsory Reading
Further Reading ▪ Sherman, A. T., DeLatte, D., Neary, M., Oliva, L., Phatak, D., Scheponik, T., Herman, G. L., & Thompson, J. (2018). Cybersecurity: Exploring core concepts through six scenarios. Cryptologia, 42(4), 337—377. ▪ Breitinger, F., & Baggili, I. (2019). Digital Forensics and Cyber Crime: 10th International EAI Conference, ICDF2C 2018, New Orleans, LA, USA, September 10—12, 2018, Proceedings (1st ed.). ▪ Lewis, J., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage. McAfee. ▪ Forshaw, J. (2018). Attacking network protocols: A hacker's guide to capturing, analysis, and exploitation. No Starch Press.Chapter 2.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Slides	

Project: Cyber Forensics

Course Code: DLMIMWCK02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	DLMIMWCK01_E

Course Description

This project aims to create an action plan for digital investigation and incident handling for a given threat scenario. Starting with a concrete suspicion of a computer-criminal act (e.g. a suspected server attack, loss of customer data or manipulation of business data) the students plan to conduct a digital investigation for electronic evidence and to secure evidence that can be used in court. The data obtained will be used to evaluate risks for affected business processes and to make recommendations for incident treatment and prevention.

Course Outcomes

On successful completion, students will be able to

- name basic methods and techniques of computer forensics and their limitations.
- identify the systems and business processes affected by a computer crime and carry out a risk assessment.
- recommend measures to secure electronic evidence and evaluate its usability in court.
- develop recommendations for incident communication, response and prevention.

Contents

- The project aims to develop an action plan for conducting a digital investigation and incident management for a given threat scenario. Beginning with the concrete suspicion of a computer crime*, the students develop a plan of action that covers the following measures:
  - Localization of the affected systems (hardware and software)
  - Identification of the affected business processes
  - Risk assessment for the impact on affected business processes
  - Communication with internal departments, cooperation partners, customers and the public
  - Identification and preservation of relevant data
  - Examination of the data
  - Securing electronic evidence and its usability in court
  - Recommendations for prevention
  - The action plan should be written in such a way that it serves as a process template for continuous incident handling.

- Examples of suspicious cases are a suspected server attack, loss of customer data, manipulation of business data, publication of internal company data, suspicion of product piracy, inconsistency of electronic signatures in company documents, digital blackmailing of a decision maker or suspicion of industrial espionage.

Literature

Compulsory Reading

Further Reading

- ISO/IEC 27001 (2022): Information Security Management. Tech. rep.
- ISO/IEC 27001:2022.ISO/IEC 27002 (2022): Information Technology - Security Techniques - Code of Practice for Information Security Management. Tech. rep. ISO/IEC 27002:2022.
- NIST (2020): Security Controls for Federal Information Systems. Tech. rep. NIST SP-800-53 Rev. 5.
- CSA (Cloud Security Alliance) (2021): “Cloud Controls Matrix v4.”
- CSA (Cloud Security Alliance): “The Consensus Assessments Initiative Questionnaire v4.”
- Luna, J., Langenberg, R., Suri, N. (2012): “Benchmarking cloud security level agreements using quantitative policy trees.”, Proc. of ACM Workshop on Cloud computing security workshop, pp. 103–112.
- NIST Cloud Computing Reference Architecture and Taxonomy Working Group (2008): “Performance and Measurements Guide for Information Technology.” In: NIST 800-55 Revision 1.
- NIST Cloud Computing Reference Architecture and Taxonomy Working Group (2020): “Performance and Measurements Guide for Information Technology.” In: NIST 800-55 Revision 2.
- NIST (2013): “Security Controls for Federal Information Systems.” Tech. rep. NIST SP-800-53. 2013.
- CIS (2014): “Cloud Service Level Agreement Standardisation Guidelines.” Tech. rep. C-SIG SLA 2014. European Commission, C-SIG SLA.
- Pannetrat, A. et al (2013): “D2.1 Security-Aware SLA Specification Language and Cloud Security Dependency model.”

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Portfolio

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Slides	☑ Guideline

Blockchain and Quantum Computing

Module Code: DLMCSEBCQC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	None	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. David Florysiak (Blockchain) / Prof. Dr. Simon Martin (Quantum Computing)

Contributing Courses to Module

- Blockchain (DLMCSEBCQC01)
- Quantum Computing (DLMCSEBCQC02)

Module Exam Type

Module Exam	Split Exam
	Blockchain • Study Format "Distance Learning": Written Assessment: Written Assignment Quantum Computing • Study Format "Distance Learning": Oral Assignment

Weight of Module

see curriculum

Module Contents

Blockchain

- Basic concepts of blockchain and related technologies
- Applications of blockchain and DLT
- Security
- Development of blockchain and DLT applications
- Social and legal aspects

Quantum Computing

- Physics of quantum computing
- Quantum computing models
- Quantum algorithms
- Quantum computing with the IBM framework Qiskit
- Applications, potential for and challenges of quantum computing

Learning Outcomes

Blockchain

On successful completion, students will be able to

- outline the functions provided by and the technology used in blockchains.
- explain important applications of block chains, in particular BitCoin.
- demonstrate the technical architecture of blockchain applications.
- appraise the benefits and challenges of suggested blockchain applications.
- discuss the social and legal aspects of blockchain technology.

Quantum Computing

On successful completion, students will be able to

- outline the basic concepts of quantum mechanics as they relate to quantum computing.
- describe the computation models used in quantum computing.
- demonstrate the role of quantum computing for cryptography and other application areas.
- compare the theoretical and practical potential of quantum computing to classical computing.
- apply the concepts of quantum computing to develop simple programs within the Qiskit framework.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Computer Science & Software Development.	All Bachelor Programmes in the IT & Technology field.

Blockchain

Course Code: DLMCSEBCQC01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	None

Course Description

Started by the cryptocurrency BitCoin, blockchain and related topics such as distributed ledger technologies and smart contracts have become increasingly important over the last few years and are claimed to be a major disruptive technologies. As BitCoin shows, systems that today need a trustworthy central coordinating body may become genuinely distributed systems without the need for such a body in the future. While blockchain has the potential for completely new types of applications, these suggested applications do not always make use of the strengths of the technology; rather, they simply provide a different approach to solving problems that could be solved more easily and efficiently using standard technologies such as database systems. Furthermore, blockchain applications have led to new social challenges and legal questions, such as the legal status of "smart contracts". Different infrastructures such as Ethereum and Hyperledger have been developed to form the basis for blockchain applications. The goal of this course is to provide an understanding of the technical, as well as social and legal, aspects of blockchain and related technologies.

Course Outcomes

On successful completion, students will be able to

- outline the functions provided by and the technology used in blockchains.
- explain important applications of block chains, in particular BitCoin.
- demonstrate the technical architecture of blockchain applications.
- appraise the benefits and challenges of suggested blockchain applications.
- discuss the social and legal aspects of blockchain technology.

Contents

1. Basic Concepts
   - 1.1 The Functional View: Distributed Ledger Technologies
   - 1.2 The Technical View: Blockchain
   - 1.3 History of Blockchain and DLT
   - 1.4 Consense Mechanisms
2. BitCoin
   - 2.1 The BitCoin Payment System
   - 2.2 The Technology Behind BitCoin

- 2.3 Security of BitCoin
- 2.4 Scalability and Other Limitations of BitCoin
- 2.5 BitCoin Derivatives and Alternatives

3. Smart Contracts and Decentralized Apps
   - 3.1 Smart Contracts
   - 3.2 Decentralized Apps (DApps)
   - 3.3 Ethereum
   - 3.4 Hyperledger
   - 3.5 Alternative Platforms for Smart Contracts and DApps

4. Security of Block Chain and DLT
   - 4.1 Cryptology Used
   - 4.2 Attacks on Blockchain and DLT
   - 4.3 Resolving Bugs and Security Holes
   - 4.4 Long-Term Security

5. Block Chain and DLT Application Scenarios
   - 5.1 Benefits and Limits of Applying Blockchain and DLT
   - 5.2 Registers for Land and Other Property
   - 5.3 Applications in the Supply Chain
   - 5.4 Applications in Insurance
   - 5.5 Initial Coin Offerings for Sourcing Capital
   - 5.6 Examples of Further Applications

6. Development of Blockchain and DLT Applications
   - 6.1 Architecture of Blockchain and DLT Applications
   - 6.2 Platform Selection
   - 6.3 Design of Blockchain and DLT Applications

7. Blockchain and Society
   - 7.1 (Mis-)Trust in Institutions
   - 7.2 Blockchain and the Environment
   - 7.3 Cyber-Currencies in the Darknet
   - 7.4 ICO Fraud

8. Legal Aspects
   - 8.1 DLT and Smart Contracts as Legal Contracts
   - 8.2 Cryptocurrencies as Legal Currencies

8.3 Regulation of ICOs
8.4 Data Protection / Privacy in Blockchains

Literature

Compulsory Reading

Further Reading

- De Filippi, P., & Wright, A. (2018). Blockchain and the law. The rule of code. Cambridge, MA: Harvard University Press.
- Meinel, C., Gayvoronskaya, T. & Schnjakin, M. (2018). Blockchain. Hype or innovation. Potsdam: Universitätsverlag Potsdam.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system [white paper]. Retrieved from https://bitcoin.org/bitcoin.pdf
- Tapscott, D., & Tapscott, N. (2018). Blockchain revolution. How the technology behind bitcoin is changing money, business, and the world. New York, NY: Portfolio/Penguin.
- Xu, W., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Cham: Springer.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Written Assignment

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Quantum Computing

Course Code: DLMCSEBCQC02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Quantum computing is a completely new paradigm for the architecture of computers. It currently is in the early stage of development but has the potential to speed up certain kinds of computations, not just by orders of magnitude but by moving them from exponential to linear growth. One of the issues that will be affected is the prime factorization of large numbers which currently forms the basis for important cryptographic algorithms, in particular the RSA algorithm which would in that case would no longer be secure. This course gives an introduction to the physics behind quantum computing and the computation models used. Students are familiarized with the most important algorithms for quantum computing and write a few programs for quantum computers. The application potential and challenges of quantum computing are also discussed.

Course Outcomes

On successful completion, students will be able to

- outline the basic concepts of quantum mechanics as they relate to quantum computing.
- describe the computation models used in quantum computing.
- demonstrate the role of quantum computing for cryptography and other application areas.
- compare the theoretical and practical potential of quantum computing to classical computing.
- apply the concepts of quantum computing to develop simple programs within the Qiskit framework.

Contents

1. Basic concepts
    - 1.1 Quantum physics as a basis for computing
    - 1.2 Types of quantum computers
    - 1.3 Qbits
    - 1.4 Linear algebra

2. The physics of quantum computers
    - 2.1 Basic concepts of quantum mechanics
    - 2.2 Spin and entanglement
    - 2.3 Architecture of quantum computers

2.4 Noise and error correction
2.5 Current state and outlook

3. Quantum computing models
   3.1 Quantum gates and circuits
   3.2 Single qubit quantum systems
   3.3 Multiple qubit quantum systems

4. Quantum algorithms
   4.1 Computability and complexity in quantum computing
   4.2 Quantum Fourier transform
   4.3 The Shor algorithm
   4.4 The Grover algorithm

5. Quantum computing with the IBM framework Qiskit
   5.1 Overview of Qiskit and the IBM Q Provider
   5.2 Quantum circuits in Qiskit
   5.3 First steps in programming with Qiskit

6. Applications, potential and challenges of quantum computing
   6.1 Applications of quantum computing
   6.2 Quantum cryptography and post-quantum cryptography
   6.3 Quantum supremacy

Literature

Compulsory Reading

Further Reading

- Mermin, N. D. (2007). Quantum computer science: An introduction. Cambridge University Press.
- Nielsen, M. A., & Chuang, I. L. (2000). Quantum computation and quantum information. Cambridge University Press.
- Rieffel, E. G., & Polak, W. H. (2011). Quantum computing: A gentle introduction. MIT Press.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
	☑ Audio	
	☑ Slides	

Secure Software Development

Module Code: DLMCSEEDSO_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Petra Beenken (Secure Software Development) / Prof. Dr. Jesus Luna Garcia (Project: Secure Software Implementation)

Contributing Courses to Module

- Secure Software Development (DLMCSEEDSO01_E)
- Project: Secure Software Implementation (DLMCSEEDSO02_E)

Module Exam Type

Module Exam	Split Exam
	Secure Software Development • Study Format "Distance Learning": Exam, 90 Minutes Project: Secure Software Implementation • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Secure Software Development

- Security by design
- Privacy by Design
- Testing and Auditing
- Software Supply Chain Security
- Common Coding Anti-Practices
- Project Management
- DevSecOps

Project: Secure Software Implementation

- Secure software design and implementation
- Testing and auditing for security
- Patch and vulnerability management
- Software lifecycle

Learning Outcomes

Secure Software Development

On successful completion, students will be able to

- design secure applications.
- understand what leads to software compromise.
- avoid common coding errors.
- manage the secure software lifecycle.
- employ a rigorous security testing regime.
- manage vulnerability disclosures.

Project: Secure Software Implementation

On successful completion, students will be able to

- design the security for a simple software project.
- avoid common coding and design mistakes.
- define what steps are needed to implement secure code.
- create a process to maintain the continuous security of the application over its lifetime.
- effectively use vulnerability disclosures.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Secure Software Development

Course Code: DLMCSEEDSO01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Attacking vulnerabilities in insecure software is a leading attack vector for criminals and malicious state actors. Finding unknown, so-called zero-day vulnerabilities is a key weapon for professional criminals. So, it is of utmost importance to design and implement secure software. First we must understand common software weaknesses and then avoid these as early in the software development and lifecycle as possible through a security-by-design philosophy. We also must run and manage a security testing and vulnerability disclosure process. Providing and implementing timely patches is essential.

Course Outcomes

On successful completion, students will be able to

- design secure applications.
- understand what leads to software compromise.
- avoid common coding errors.
- manage the secure software lifecycle.
- employ a rigorous security testing regime.
- manage vulnerability disclosures.

Contents

1. Security by design
   - 1.1 IT-Support and testing by “Shifting Left” Methodology
   - 1.2 Infrastructure as Code
   - 1.3 Advantages of Considering Security Early
2. Privacy by Design
   - 2.1 Encryption
   - 2.2 Differential Privacy
   - 2.3 Zero-Knowledge Proofs/Protocols
3. Testing and Auditing
   - 3.1 Unit Testing
   - 3.2 Security Testing

3.3 Security Code Auditing

4. Software Supply Chain Security
   - 4.1 Package Security
   - 4.2 Container Security
   - 4.3 Programming Language Considerations

5. Common Coding Anti-Practices
   - 5.1 Classes of Bugs
   - 5.2 Sources Of Bugs
   - 5.3 Severity Of Bugs

6. Project Management
   - 6.1 The Software Lifecycle
   - 6.2 Managing Vulnerability Disclosures
   - 6.3 Managing Patches/Updating
   - 6.4 Managing Pentesting and Bug Bounty Programs

7. DevSecOps
   - 7.1 DevOps
   - 7.2 Cloud Security
   - 7.3 Continuous Integration, Testing, and Deployment
   - 7.4 Ephemeral Processes
   - 7.5 Automation

Literature

Compulsory Reading

Further Reading

- Adkins, H. et al (2020): Building Secure and Reliable Systems. 1st edition, O'Reilly Media, Newton, MA.
- Common Weakness Enumeration, https://cwe.mitre.org/
- Dwork, C. / Roth, A. (2014): The Algorithmic Foundations of Differential Privacy. In Foundations and Trends in Theoretical Computer Science Vol. 9, Nos. 3–4 (2014) 211–407.
- The Open Web Application Security Project, https://owasp.org/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Secure Software Implementation

Course Code: DLMCSEEDSO02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSEEDSO01_E or DLMCSEEDSO01_D

Course Description

Software is eating the world, so no organization can afford to deploy insecure code without eventually suffering dire consequences. In this project the student will tackle a secure application implementation and write a report justifying decisions made to ensure the security of the running system.

Course Outcomes

On successful completion, students will be able to

- design the security for a simple software project.
- avoid common coding and design mistakes.
- define what steps are needed to implement secure code.
- create a process to maintain the continuous security of the application over its lifetime.
- effectively use vulnerability disclosures.

Contents

- To a given problem and/or a given context, the student will design and develop a simple software project and then submit a report, code and data describing the security design decisions as well as plans for the future software lifecycle. Specific projects will be provided by the tutor but proposals by the students can be considered.

Literature

Compulsory Reading

Further Reading

- Adkins, H. et al (2020): Building Secure and Reliable Systems. 1st edition, O'Reilly Media, Newton, MA.
- Common Weakness Enumeration, https://cwe.mitre.org/
- Dwork, C. / Roth, A. (2014): The Algorithmic Foundations of Differential Privacy. In Foundations and Trends in Theoretical Computer Science Vol. 9, Nos. 3–4 (2014) 211–407.
- The Open Web Application Security Project, https://owasp.org/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Slides	☑ Guideline

Organizational Transformation

Module Code: DLMCSDWTO-02_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Zeljko Sevic (Tools in Organizational Analysis) / Prof. Dr. Andrew Adjah Sai (Management of IT Services and Architecture)

Contributing Courses to Module

- Tools in Organizational Analysis (DLMWPWOAE01_E)
- Management of IT Services and Architecture (MWIT02-02_E)

Module Exam Type

Module Exam	Split Exam
	Tools in Organizational Analysis • Study Format "Distance Learning": Exam, 90 Minutes Management of IT Services and Architecture • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Tools in Organizational Analysis

- The Organization
- Organizational Research
- Organization Diagnostics
- Organization Analysis
- Practical application in specific areas

Management of IT Services and Architecture

- Basics of IT Service Management and Terminology
- IT Infrastructure Library (ITIL)
- IT Outsourcing
- IT Architecture Management
- IT Application Portfolio Management
- Structural Organization of IT and Architecture Governance

Learning Outcomes

Tools in Organizational Analysis

On successful completion, students will be able to

- deal with the concept of organization in a differentiated way.
- evaluate the possibilities of organizational diagnostics.
- use selected instruments of organizational and team diagnosis.
- carry out, evaluate and reflect on organizational diagnostic measures.
- work on specific organizational analyses.

Management of IT Services and Architecture

On successful completion, students will be able to

- name, explain and distinguish the basic principles of IT strategy, IT governance and IT architecture management.
- explain and apply concepts from main areas in IT service management on the basis of the IT Infrastructure Library (ITIL).
- explain and apply goals and typical activities of IT architecture management, their interrelationships and their dependencies.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Business Administration & Management and Computer Science & Software Development	All Master Programs in the Business and IT & Technology fields

Tools in Organizational Analysis

Course Code: DLMWPWOAE01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Organizations are more than ever like living organisms, which due to external changes must also change internally and adapt to new conditions. This course deals with a differentiated view of entrepreneurially oriented organizations, their goals, possible strategies, their function and performance. It sheds light on the possibilities of organizational research and its fields of research, in order to then address the goals, possibilities and fields of application of the diagnosis of organizations. Various methods and instruments of organizational diagnosis are presented with the aim of using them in the organizational analysis process. This enables students to initiate and implement change measures on the basis of diagnostic instruments and to evaluate such measures. The course also deals with the practical application of topics that arise in everyday business life, such as the analysis of change management processes, of careers and in connection with risk assessment in the acquisition of companies or company investments (due diligence). In this way, students are taught the spectrum and possible applications of the measures and methods of a targeted organizational analysis through diagnostic measures.

Course Outcomes

On successful completion, students will be able to

- deal with the concept of organization in a differentiated way.
- evaluate the possibilities of organizational diagnostics.
- use selected instruments of organizational and team diagnosis.
- carry out, evaluate and reflect on organizational diagnostic measures.
- work on specific organizational analyses.

Contents

1. The Organization
   - 1.1 The concept of organization
   - 1.2 Goals and strategies of an organization
   - 1.3 Function and performance of organizations
   - 1.4 Role of people in organizations
   - 1.5 Differences between organizations
2. Organizational Research
   - 2.1 Perspectives of organizational research

2.2 Fields of research
2.3 Empirical research on organizations

3. Organization Diagnostics
   3.1 Definition and goals of organizational diagnostics
   3.2 Fields of application of surgical diagnostics
   3.3 The Organizational Diagnosis as a Management Tool
   3.4 Target groups of organizational diagnostic findings
   3.5 Selected instruments of team and organization diagnosis

4. Organization Analysis
   4.1 The organizational analysis
   4.2 Preliminary considerations and analysis process
   4.3 Conception and operationalization
   4.4 Data collection methods
   4.5 Survey and evaluation
   4.6 Presentation of the analysis and reflection

5. Practical application in specific areas
   5.1 Analysis of change processes
   5.2 Network analysis
   5.3 Analysis of careers in organizations
   5.4 Organizational Analysis and Due Diligence

Literature

Compulsory Reading

Further Reading

- Harris, O. J., & Hartman, S. J. (2002). Organizational behavior. Taylor & Francis.
- Luthans, F. (2015). Organizational behavior: An evidence-based approach (13th ed.). InformationAge Publishing.
- Stroh, L. K., Northcraft, G. B., Neale, M. A., Kern, M., Langlands, C., & Greenberg, J. (2003).Organizational behavior: A management challenge (2nd ed.). Psychology Press.
- Tolbert, P. S. (2016). Organizations structures, processes, and outcomes (10th ed.). Routledge.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Slides	

Management of IT Services and Architecture

Course Code: MWIT02-02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

This course addresses two major areas in information technology (IT) management: service management as well as architecture management. IT service management is an approach to align and understand a company's IT department as a service provider and enabler of operational and business processes. Here, the focus is on planning and operating the organization-wide IT infrastructure. The area of architecture management focuses on the strategic alignment of the company's IT to the organization's business and IT strategy. This course provides concepts, methods, procedures and models for executing this management task.

Course Outcomes

On successful completion, students will be able to

- name, explain and distinguish the basic principles of IT strategy, IT governance and IT architecture management.
- explain and apply concepts from main areas in IT service management on the basis of the IT Infrastructure Library (ITIL).
- explain and apply goals and typical activities of IT architecture management, their interrelationships and their dependencies.

Contents

1. Introduction to IT Management
   - 1.1 IT Management and IT Governance
   - 1.2 IT Services
   - 1.3 IT Service Management (ITSM)
   - 1.4 IT Architecture Management (ITAM)
   - 1.5 Reference Models for IT Organizations
2. IT Service Management: Incident and Problem Management
   - 2.1 Overview
   - 2.2 Service Quality, Service Level Agreements and Customer Expectations
   - 2.3 Problem Management
   - 2.4 Software Tools for Supporting Incident and Problem Management

Literature
Compulsory Reading
Further Reading ▪ Ahlemann, F., Messerschmidt, M., Stettiner, E., & Legner, C. (2012). Strategic Enterprise Architecture Management. Challenges, Best Practices, and Future Developments (1. Aufl.). Springer-Verlag. ▪ Hanschke, I. (2010). Strategic IT Management: a Toolkit for Enterprise Architecture Management. Springer.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
	☑ Slides	

IT Law for IT Security

Module Code: DLMCSEEITLS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Mohammad Shackow (International IT Law) / Dr. Mohammad Shackow (Seminar: Legal Framework for IT-Security)

Contributing Courses to Module

- International IT Law (DLMIMWITR01_E)
- Seminar: Legal Framework for IT-Security (DLMCSEEITLS01_E)

Module Exam Type

Module Exam	Split Exam
	International IT Law • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Legal Framework for IT-Security • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

International IT Law

- Introduction
- E-Business and E-Commerce
- Intellectual Property
- Privacy and Data Protection
- Information Security and Computer Crime
- Online Media and Telecommunication

Seminar: Legal Framework for IT-Security

Compliance with the law is a major driver of security in organizations. The student must understand the various legal frameworks and jurisdictions that may apply to her/his work. Law also plays a role in pursuing criminals that attack an organization. Therefore, the support of preservation of evidence plays a key role. In this module, we explore these legal frameworks and apply them to realistic problems from the field of computer security.

Learning Outcomes

International IT Law

On successful completion, students will be able to

- identify and explain the differences between national, transnational and international legal systems.
- identify interfaces between general legal concepts and IT-relevant law.
- identify legal requirements for IT contracting and assess their impact on the (electronic) commercialization of IT products or services.
- assess the impact of the European Data Protection Regulation on business processes and make recommendations for implementation.
- identify the legal views of selected transnational institutions and to assess their impact on international IT law.

Seminar: Legal Framework for IT-Security

On successful completion, students will be able to

- understand how laws apply to cyberspace and IT-Security in organizations and enterprises.
- understand the legal limitations of pursuing criminals for law enforcement agencies and the importance of preservation of evidence.
- appreciate the differences in international law as applied to computer operations.
- understand how legal frameworks drive computer security compliance.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the field of Law	All Master Programs in the Business & Management fields

International IT Law

Course Code: DLMIMWITR01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

This course presents in depth national and international legal framework conditions of information processing for companies. After an examination of the differences between international legal systems, an introduction is given to those legal constructs which serve as a basis for the development of IT-relevant legislation. Subsequently, areas of law are discussed from the perspective of concrete application-oriented business scenarios, such as contract law, licensing and patenting.An introduction to the EU legal system is followed by a detailed discussion of the European General Data Protection Regulation (GDPR), which gains increasingly international interest. This leads into a consideration of transnational legal systems and concludes with recommendations from supranational organizations.

Course Outcomes

On successful completion, students will be able to

- identify and explain the differences between national, transnational and international legal systems.
- identify interfaces between general legal concepts and IT-relevant law.
- identify legal requirements for IT contracting and assess their impact on the (electronic) commercialization of IT products or services.
- assess the impact of the European Data Protection Regulation on business processes and make recommendations for implementation.
- identify the legal views of selected transnational institutions and to assess their impact on international IT law.

Contents

1. Introduction
   - 1.1 General Concepts of Law
   - 1.2 Areas of Law
   - 1.3 International, Transnational and EU Law
   - 1.4 Definition and Scope of IT Law
   - 1.5 International, Transnational and European IT Law
   - 1.6 Law in Cross-Border Systems
2. E-Business and E-Commerce

- 2.1 General Terms and Conditions of Business
- 2.2 Electronic Commerce
- 2.3 IT Contracts
- 2.4 Intermediaries and Platforms
- 2.5 Antritrust Law and IT

3. Intellectual Property
   - 3.1 Basic Concepts of Intellectual Property
   - 3.2 Copyright
   - 3.3 Software Copyright and Software Licensing
   - 3.4 Free and Open Licensing
   - 3.5 Patenting of Software

4. Privacy and Data Protection
   - 4.1 Basic Concepts of Privacy and Data Protection
   - 4.2 European General Data Protection Regulation (GDPR)
   - 4.3 Implementation Approaches of the GDPR
   - 4.4 International Data Transfer

5. Information Security and Computer Crime
   - 5.1 Information Security Law
   - 5.2 Electronic Signatures and Digital Identities
   - 5.3 Cybercrime

6. Online Media and Telecommunication
   - 6.1 Basics of Online Media Law
   - 6.2 Social Media and Freedom of Expression
   - 6.3 Fundamentals of Telecommunications Law
   - 6.4 Internet and Domain Law

Literature
Compulsory Reading
Further Reading ▪ Lloyd, I. (2020): Information Technology Law. Oxford University Press. ▪ Lutzi, T. (2020): Private International Law Online: Internet Regulation and Civil Liability in the EU. Oxford University Press. ▪ Nirmal, B. C. & Singh, R. K. (ed.) (2018): Contemporary Issues in International Law. Environment, International Trade, Information Technology and Legal Education. Springer. ▪ Savin, A. (2017): EU Internet Law. Edward Elgar Publishing. ▪ Siems, M. (2018): Comparative law. Cambridge University Press. ▪ Thirlway, H. (2019): The sources of international law. Oxford University Press.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Seminar: Legal Framework for IT-Security

Course Code: DLMCSEEITLS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	(CSEMIGCR01-01_E or (DLMIMWITR01_E or DLMIMWITR01)

Course Description

Computer security does not operate in a legal vacuum. It is subject to legal frameworks in regard of the applicability of international law in cyberspace, National Cyber Security strategies and national policies and legislation. Due to the global nature of Cyberspace, not limited to national boundaries, Organizations often operate in a variety of jurisdictions with a variety of laws. Criminals are using this fact by putting their key operations outside the reach of their victim's jurisdiction. State actors and non-State actors operate in legal grey zones to pursue their targets. Therefore, international organizations, such as the EU, OSCE, ASEAN, are developing compliance frameworks and mechanisms. In this seminar we examine cases and legal frameworks that IT-Security personnel has to recognize.

Course Outcomes

On successful completion, students will be able to

- understand how laws apply to cyberspace and IT-Security in organizations and enterprises.
- understand the legal limitations of pursuing criminals for law enforcement agencies and the importance of preservation of evidence.
- appreciate the differences in international law as applied to computer operations.
- understand how legal frameworks drive computer security compliance.

Contents

- Students will be given an aspect of law or a legal case to study and report on. Of particular importance is to understand what potential consequences the case or law will have on an organization and enterprises. Specific legal text or cases will be provided by the tutor but proposals by the students can be considered.

Literature
Compulsory Reading
Further Reading ▪ Clarke, R. A., & Knake, R. K. (2010). Cyber war. (1st ed.). HarperCollins. ▪ Lusthaus, J. (2018). Industry of anonymity. Harvard University Press. ▪ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. ▪ Schneier, B. (2015). Data and Goliath. (1st ed.). W. W. Norton & Company.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Audit- and Security Testing

Module Code: DLMCSEEAST_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Christian Prause (Attack Models and Auditing) / Dr. Radiah Rivu (Seminar: IT Security Tests)

Contributing Courses to Module

- Attack Models and Auditing (DLMCSEEAST01_E)
- Seminar: IT Security Tests (DLMCSEEAST02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Models and Auditing • Study Format "Distance Learning": Exam, 90 Minutes Seminar: IT Security Tests • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Attack Models and Auditing

- Threat modelling
- Software testing and verification
- Pentesting tools
- Self-assessment and third-party audits
- Ethical hacking

Seminar: IT Security Tests

Software and system auditing; Pentesting; Red/Blue teams; Bug Bounty programs

Learning Outcomes

Attack Models and Auditing

On successful completion, students will be able to

- plan what to test and audit for.
- understand common pentesting tools.
- understand software testing and verification.
- organize self-assessments of the implemented ISMS.
- familiarize with widely used cybersecurity audit frameworks.
- run remote system audits.

Seminar: IT Security Tests

On successful completion, students will be able to

- understand how bug bounty programs work.
- understand how to run a red/blue team or pentesting exercise.
- write a report showing aptitude in the subject.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Attack Models and Auditing

Course Code: DLMCSEEAST01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The cybersecurity lifecycle comprehends a range of activities, where "checking" the implemented security concept provides a feedback loop to continuously improve the designed security levels. In practice, cybersecurity checks include an initial threat modeling step before the right tools and techniques can be used to test the security of the software or system. This can be a type of ethical hacking (e.g., pentesting, red/blue team exercise or bug bounty program), or a self-assessment or this-party audit of the deployed information security management system (ISMS).

Course Outcomes

On successful completion, students will be able to

- plan what to test and audit for.
- understand common pentesting tools.
- understand software testing and verification.
- organize self-assessments of the implemented ISMS.
- familiarize with widely used cybersecurity audit frameworks.
- run remote system audits.

Contents

1. Threat Modelling
   - 1.1 System Security Life Cycle
   - 1.2 Modelling applications and profiling threats
   - 1.3 Security testing based on a threat model
   - 1.4 OWASP Threat Dragon and Microsoft Threat Modelling Tool
2. Ethical Hacking
   - 2.1 Legal and compliance framework
   - 2.2 Pentesting process
   - 2.3 Red/Blue teams
   - 2.4 Bug bounty programs
3. Multi-layer system security testing
   - 3.1 Operating system exploits

3.2 Network penetration testing and tools
3.3 Web app penetration testing with OWASP and OSINT
3.4 Exploit development

4. Software testing
   4.1 Whitebox, blackbox and graybox testing
   4.2 Unit testing for security
   4.3 Fuzzing
   4.4 ISO/IEC 29119

5. Software verification
   5.1 Static code analysis
   5.2 Dynamic code analysis
   5.3 Peer review
   5.4 Formal verification

6. Cybersecurity Audits
   6.1 Self-assessments and third-party audits
   6.2 Risk-based approach to cybersecurity checks
   6.3 Auditing cybersecurity based on ISO/IEC 27001
   6.4 Toolset for automated audits

Literature

Compulsory Reading

Further Reading

- Graham, D. (2021). Ethical hacking: A hands-on introduction to breaking in. No Starch Press Incorporated.
- Keith Yorkston. (2021). Performance Testing: An ISTQB Certified Tester Foundation Level Specialist Certification Review: Vol. 1st ed . apress.
- Páez, F., & Kaschel, H. (2022). Design and Testing of a Computer Security Layer for the LIN Bus †. Sensors (14248220), 22(18), 6901–N.PAG.
- Li, H. (2022). Computer Security Issues and Legal System Based on Cloud Computing. Computational Intelligence & Neuroscience, 1–11.
- Shostack, A. (2014). Threat Modeling. Designing for Security. John Wiley & Sons, Hoboken, NJ. h
- Stallings, W., & Brown, L. (2018). Computer Security [electronic resource]: Principles and Practice (4th ed., global edition). Pearson Education, Limited.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Seminar: IT Security Tests

Course Code: DLMCSEEAST02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSEEAST01_E

Course Description

A good security architecture is a fine thing, but it is always better to test it than to find out too late that there was one more hole to patch. In this seminar, the student will complete a report on a security audit method. This can be a type of pentesting, red/blue team exercise or bug bounty program. Alternatively, the report can cover a vulnerability report created from a public bug bounty program. The intension is that the student has the opportunity to go in depth with an aspect of this subject.

Course Outcomes

On successful completion, students will be able to

- understand how bug bounty programs work.
- understand how to run a red/blue team or pentesting exercise.
- write a report showing aptitude in the subject.

Contents

- Testing security is just as important as implementing it. This seminar will address this topic with reports on a variety of subjects the student can choose from. The student will use current literature to research the topic and write a report on it. Possible topics can be based on tools in the areas of WWW pentesting, fuzzing, code security auditing. Or topics can be chosen from playbooks from red and blue teams. Or the student may choose to look into best practices for setting up and managing bug bounty programs.

Literature
Compulsory Reading
Further Reading ▪ Kim, P. (2014): The Hacker Playbook: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA. ▪ Kim, P. (2015): The Hacker Playbook 2: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA. ▪ Kim, P. (2018): The Hacker Playbook 3: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA. ▪ Klein, T. (2011): A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security. No Starch Press, San Francisco, CA. ▪ McClure, S. / Scambray, J. / Kurtz, G. (2012): Hacking Exposed 7, McGraw-Hill, New York City, NY. ▪ The Zero-day Initiative blog: https://www.zerodayinitiative.com/blog

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Slides	☑ Guideline

Business Analyst

Module Code: DLMDSEBA

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum		MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Silke Vaas (Business Intelligence I) / Prof. Dr. Silke Vaas (Project: Business Intelligence)

Contributing Courses to Module

- Business Intelligence I (DLMDSEBA01)
- Project: Business Intelligence (DLMDSEBA02)

Module Exam Type

Module Exam	Split Exam
	Business Intelligence I • Study Format "Distance Learning": Written Assessment: Case Study Project: Business Intelligence • Study Format "Distance Learning": Portfolio

Weight of Module

see curriculum

Module Contents

Business Intelligence I

- Data acquisition and dissemination
- Data warehouse and multidimensional modeling
- Analytical systems
- Future Business Intelligence Application Areas

Project: Business Intelligence

Implementation of a business intelligence use case.

Learning Outcomes

Business Intelligence I

On successful completion, students will be able to

- understand the motivations and use cases for, as well as fundamentals of, business intelligence.
- explain relevant types of data.
- know and disambiguate techniques and methods for modeling and dissemination of data.
- expound upon the techniques and methods for the generation and storage of information.
- select apposite business intelligence methods for given requirements.
- explain current and future business intelligence application areas.

Project: Business Intelligence

On successful completion, students will be able to

- transfer knowledge of business intelligence methodology to real-world use cases.
- analyze the suitability of different approaches with respect to the project task.
- critically reason about relevant design choices.
- make apposite architectural choices.
- formulate and implement a business intelligence use case.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Computer Science & Software Development and Data Science & Artificial Intelligence	All Master Programs in the IT & Technology field

Business Intelligence I

Course Code: DLMDSEBA01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Business Intelligence is about the generation of information based on operational data. It is used to enable goal-oriented management practices as well as the optimization of relevant business activities. This course introduces and discusses techniques, methods, and models for data provisioning and the generation, analysis, and dissemination of information.

Course Outcomes

On successful completion, students will be able to

- understand the motivations and use cases for, as well as fundamentals of, business intelligence.
- explain relevant types of data.
- know and disambiguate techniques and methods for modeling and dissemination of data.
- expound upon the techniques and methods for the generation and storage of information.
- select apposite business intelligence methods for given requirements.
- explain current and future business intelligence application areas.

Contents

1. Motivation and Introduction
   - 1.1 Motivation and Historical Development of the Field
   - 1.2 Business Intelligence as a Framework
2. Data Provisioning
   - 2.1 Operative and Dispositive Systems
   - 2.2 The Data Warehouse Concept
   - 2.3 Architecture Variants
3. Data Warehouse
   - 3.1 The ETL-Process
   - 3.2 DWH and Data-Mart Concepts
   - 3.3 ODS and Meta-Data
4. Modeling Multidimensional Dataspaces

- 4.1 Data Modeling
- 4.2 OLAP-Cubes
- 4.3 Physical Storage Concepts
- 4.4 Star-Schema and Snowflake-Schema
- 4.5 Historization

5. Analytical Systems
   - 5.1 Freeform Data Analysis and OLAP
   - 5.2 Reporting Systems
   - 5.3 Model-Based Analytical Systems
   - 5.4 Concept-Oriented Systems

6. Distribution and Access
   - 6.1 Information Distribution
   - 6.2 Information Access

7. Current and Future Business Intelligence Application Areas
   - 7.1 Mobile Business Intelligence
   - 7.2 Predictive and Prescriptive Analytics
   - 7.3 Artificial Intelligence
   - 7.4 Agile Business Intelligence

Literature

Compulsory Reading

Further Reading

- Grossmann, W., Rinderle-Ma, S. (2015). Fundamentals of Business Intelligence. Berlin/ Heidelberg: Springer.
- Kolb, J. (2013). Business intelligence in plain language: A practical guide to data mining and business analytics. Createspace.
- Sharda, R., Delen, D., & Turban, E. (2014). Business intelligence and analytics: Systems for decision support. Pearson.
- Sharda, R., Delen, D., & Turban, E. (2017). Business intelligence, analytics, and data science: A managerial perspective. Pearson.
- Sherman, R. (2014). Business intelligence guidebook: From data integration to analytics. Morgan Kaufmann.
- Turban, E., Sharda, R., Aronson, J., & King, D. (2010). Business intelligence. A managerial approach (2nd ed.). Prentice Hall.
- Vaisman, A., & Zimányi, E. (2016). Data warehouse systems: Design and implementation. Springer.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Online Tests
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Guideline
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Project: Business Intelligence

Course Code: DLMDSEBA02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	DLMDSEBA01

Course Description

In this course the students will transfer knowledge of business intelligence approaches and methods to the implementation of a real-world business analytical use case. To accomplish this goal, students must look closely at the given task and find an apposite approach by analyzing, evaluating, and comparing different solution strategies and their constituent parts. The found solution then has to be implemented in order to arrive at a running business analytical system.

Course Outcomes

On successful completion, students will be able to

- transfer knowledge of business intelligence methodology to real-world use cases.
- analyze the suitability of different approaches with respect to the project task.
- critically reason about relevant design choices.
- make apposite architectural choices.
- formulate and implement a business intelligence use case.

Contents

- This second course in the Business Analyst specialization aims at the practical implementation of a business intelligence project. Students can choose from a list of project topics or contribute their own ideas.

Literature

Compulsory Reading

Further Reading

- Kimball, R. (2013). The data warehouse toolkit: The definitive guide to dimensional modeling (3rd ed.). Indianapolis, IN: Wiley.
- Linstedt, D., & Olschimke, M. (2015). Building a scalable data warehouse with Data Vault 2.0. Waltham, MA: Morgan Kaufmann.
- Provost, F. (2013). Data science for business: What you need to know about data mining and data-analytic thinking. Sebastopol, CA: O'Reilly.
- Sherman, R. (2014). Business intelligence guidebook: From data integration to analytics. Waltham, MA: Morgan Kaufmann.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Portfolio

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Continuous and Lifecycle Security

Module Code: DLMCSEECLS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Nils Kannengießer (Cyber Resilience) / Prof. Dr. Stephan Spitz (Seminar: Applying Threat Intelligence)

Contributing Courses to Module

- Cyber Resilience (DLMCSEECLS01_E)
- Seminar: Applying Threat Intelligence (DLMCSEECLS02_E)

Module Exam Type

Module Exam	Split Exam
	Cyber Resilience • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Applying Threat Intelligence • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Cyber Resilience

- Cyber resilience
- DevSecOps
- Threat Intelligence
- Crisis Management
- Security Culture

Seminar: Applying Threat Intelligence

- Cyber resilience
- DevSecOps
- Threat Intelligence
- Crisis Management
- Security Culture

Learning Outcomes

Cyber Resilience

On successful completion, students will be able to

- implement defense in depth and fault tolerance.
- work with resilience frameworks.
- use threat intelligence to design better resilience.
- use DevSecOps practices to improve resilience.
- manage crises that arise from attacks and corporate culture.

Seminar: Applying Threat Intelligence

On successful completion, students will be able to

- understand weaknesses in an organization's defenses.
- make recommendations on how to make the organization more resilient.
- utilize threat intelligence for secure application and systems design.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Cyber Resilience

Course Code: DLMCSEECLS01_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Even with state-of-the-art security controls in place, attacks will still be successful with enough persistence, and state actors and some criminals have shown a willingness to go that extra mile to penetrate their target. A resilient organization will have the monitoring and procedures in place and rapidly detect, triage and react to any attack. Furthermore, this organization will have enough fault tolerance so that an attack cannot affect the entire organization at the same time.

Course Outcomes

On successful completion, students will be able to

- implement defense in depth and fault tolerance.
- work with resilience frameworks.
- use threat intelligence to design better resilience.
- use DevSecOps practices to improve resilience.
- manage crises that arise from attacks and corporate culture.

Contents

1. Defense in depth
   - 1.1 The fallacy of complete security
   - 1.2 Byzantine fault tolerance
   - 1.3 Intrusion and fault detection
   - 1.4 Layers of protection
2. Design Principles
   - 2.1 Least Privilege
   - 2.2 Role and domain separation
   - 2.3 Revocation and Rollback
   - 2.4 Towards an anti-fragile organization
3. Fault tolerance
   - 3.1 Data protection and lifecycle
   - 3.2 Distributed and redundant data processing
   - 3.3 Applications of Blockchain technology

4. Frameworks
   - 4.1 NIST Cyber resilience engineering framework
   - 4.2 OODA-loop: Observe. Orient. Decide. Act.

5. Threat Intelligence
   - 5.1 Techniques, Tactics and Procedures
   - 5.2 Common weaknesses
   - 5.3 Threat Intelligence data

6. DevSecOps best practices
   - 6.1 Ephemeral processes
   - 6.2 Tiered data storage
   - 6.3 Continuous integration, testing and deployment with Caneries
   - 6.4 Availability zones for data and processes
   - 6.5 Avoiding complexity

7. Crisis management
   - 7.1 The Incident Response team
   - 7.2 Incident triage
   - 7.3 Communication
   - 7.4 Recovery planning and execution
   - 7.5 Postmortem

8. Organization and Culture
   - 8.1 Roles and responsibilities
   - 8.2 Security as a first-class citizen in an organization
   - 8.3 Influencing corporate culture
   - 8.4 Leadership buy-in

Literature
Compulsory Reading
Further Reading ▪ Adkins, H. et al (2020): Building Secure and Reliable Systems. First Edition, O'Reilly Media, Newton, MA. ▪ Ross, R. et al (2019): Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-160 Volume 2. https://doi.org/10.6028/NIST.SP.800-160v2 ▪ Ross, R. / McEvilley, M. / Oren, J. C. (2016): Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
	☑ Audio	
☑ Recorded Live Sessions	☑ Slides	

Seminar: Applying Threat Intelligence

Course Code: DLMCSEECLS02_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Cyber resilience is the practice of accepting that security will never be 100% watertight but the ability to limit damage and quickly detect and respond to incidents is of utmost importance. In this seminar, we examine reports from past incidents and identify threat intelligence, in particular the Techniques, Tactics and Procedures of criminals, that help in identifying effective defenses.

Course Outcomes

On successful completion, students will be able to

- understand weaknesses in an organization's defenses.
- make recommendations on how to make the organization more resilient.
- utilize threat intelligence for secure application and systems design.

Contents

- With a given report, the student will research the incident and independently find threat intelligence reports and data relevant to the given incident. A report will then summarize the security issues responsible for the incident and make recommendations as to how the victim could become more resilient to such attacks. Specific incident reports will be provided by the tutor but proposals by the students can be considered.

Literature

Compulsory Reading

Further Reading

- Adkins, H. et al (2020): Building Secure and Reliable Systems. First Edition, O'Reilly Media, Inc.
- Mitre ATT&CK®: https://attack.mitre.org/
- OASIS Cyber Threat Intelligence: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
- Ross, R. et al (2019): Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-160 Volume 2. https://doi.org/10.6028/NIST.SP.800-160v2

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint	☑ Slides	☑ Guideline

Data Science and Big Data Technologies

Module Code: DLMCSEEDSBDT-01_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Gissel Velarde (Data Science) / Prof. Dr. Christian Müller-Kett (Big Data Technologies)

Contributing Courses to Module

- Data Science (DLMBDSA01-01)
- Big Data Technologies (DLMDSBDT01)

Module Exam Type

Module Exam	Split Exam
	Data Science • Study Format "Distance Learning": Exam, 90 Minutes Big Data Technologies • Study Format "Distance Learning": Oral Assignment

Weight of Module

see curriculum

Module Contents

Data Science

- Introduction to Data Science
- Use Cases and Performance Evaluation
- Pre-processing of Data
- Processing of Data
- Selected Mathematical Techniques
- Selected Artificial Intelligence Techniques

Big Data Technologies

- Data Types and Data Sources
- Databases
- Modern data storage frameworks
- Data formats
- Distributed Computing

Learning Outcomes

Data Science

On successful completion, students will be able to

- identify use cases and evaluate the performance of data-driven approaches.
- understand how domain specific knowledge for a particular application context is required to identify objectives and value propositions for data science use cases.
- appreciate the role and necessity for business-centric model evaluation apposite to the respective area of application.
- comprehend how data are pre-processed in preparation for analysis.
- develop typologies for data and ontologies for knowledge representation.
- decide for appropriate mathematical algorithms to utilize data analysis for a given task.
- understand the value, applicability, and limitations of artificial intelligence for data analysis.

Big Data Technologies

On successful completion, students will be able to

- identify different types and sources of data.
- understand different database concepts.
- learn to build new database structures.
- evaluate various data storage frameworks w.r.t. project requirements.
- analyze which data format to use for a given project.
- understand what roles you could take in such projects.
- create a distributed computing environment for a given project.
- understand the ethical impact of big data technology choices.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the fields of Data Science & Artificial Intelligence	All Master Programs in the IT & Technology fields

Data Science

Course Code: DLMBDSA01-01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The course provides the framework to create value from data. After an introduction the course covers how to identify suitable use cases and evaluate the performance of data-driven methods. In an interdisciplinary approach, the requirements from a specific application domain need to be understood and transferred to the technological understanding to identify the objectives and value proposition of a Data Science project. The course covers techniques for the technical processing of data and then introduces advanced mathematical techniques and selected methods from artificial intelligence that are used to analyze data and make predictions.

Course Outcomes

On successful completion, students will be able to

- identify use cases and evaluate the performance of data-driven approaches.
- understand how domain specific knowledge for a particular application context is required to identify objectives and value propositions for data science use cases.
- appreciate the role and necessity for business-centric model evaluation apposite to the respective area of application.
- comprehend how data are pre-processed in preparation for analysis.
- develop typologies for data and ontologies for knowledge representation.
- decide for appropriate mathematical algorithms to utilize data analysis for a given task.
- understand the value, applicability, and limitations of artificial intelligence for data analysis.

Contents

1. Introduction to Data Science
    - 1.1 Overview of Data Science
    - 1.2 Data Science Activities
    - 1.3 Sources and Types of Data
    - 1.4 Stages of Data Processing
    - 1.5 Mathematical Basics for Data Scientists
2. Use Cases and Performance Evaluation
    - 2.1 Data Science Use Cases (DSUCs)
    - 2.2 Model-Centric Evaluation: Performance Metrics
    - 2.3 Business-Centric Evaluation: the Role of KPIs

Literature
Compulsory Reading
Further Reading

- Akerar, R., & Sajja, P.S. (2016). Intelligent techniques for data science. Cham: Springer.
- Bruce, A., & Bruce, P. (2017). Practical statistics for data scientists: 50 essential concepts. Newton, MA: O'Reilly Publishers.
- Fawcett, T. & Provost, F. (2013). Data science for business: What you need to know about data mining and data-analytic thinking. Newton, MA: O'Reilly Media.
- Hodeghatta, U. R., & Nayak, U. (2017). Business analytics using R – A practical approach. Berkeley, CA: Apress Publishing. (Database: ProQuest).
- Liebowitz, J. (2014). Business analytics: An introduction. Boca Raton, FL: Auerbach Publications. (Available online).
- Runkler, T. A. (2012). Data analytics: Models and algorithms for intelligent data analysis. Wiesbaden: Springer Vieweg.
- Skiena, S. S. (2017). The data science design manual. Cham: Springer.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Slides	

Big Data Technologies

Course Code: DLMDSBDT01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Data are often considered the “new oil”, the raw material from which value is created. To harness the power of data, the data need to be stored and processed on a technical level. This course introduces the four “Vs” of data, as well as typical data sources and types. This course then discusses how data are stored in databases. Particular focus is given to database structures and different types of databases, e.g., relational, noSQL, NewSQL, and time-series.Beyond classical and modern databases, this course covers a wide range of storage frameworks such as distributed filesystems, streaming, and query frameworks. This is complemented by a detailed discussion of data storage formats ranging from classical approaches such as CSV and HDF5 to more modern approaches like Apache Arrow and Parquet.Finally, this course gives an overview of distributed computing environments based on local clusters, cloud computing facilities, and container-based approaches.

Course Outcomes

On successful completion, students will be able to

- identify different types and sources of data.
- understand different database concepts.
- learn to build new database structures.
- evaluate various data storage frameworks w.r.t. project requirements.
- analyze which data format to use for a given project.
- understand what roles you could take in such projects.
- create a distributed computing environment for a given project.
- understand the ethical impact of big data technology choices.

Contents

1. Data Types and Data Sources
    - 1.1 The 4Vs of data: volume, velocity, variety, veracity
    - 1.2 Data sources
    - 1.3 Data types
2. Databases
    - 2.1 Database structures
    - 2.2 Introduction to SQL

2.3 Relational databases
2.4 nonSQL, NewSQL databases
2.5 Timeseries DB

3. Modern data storage frameworks
   3.1 Distributed Filesystems
   3.2 Streaming frameworks
   3.3 Query frameworks

4. Data formats
   4.1 Traditional data exchange formats
   4.2 Apache Arrow
   4.3 Apache Parquet

5. Distributed Computing
   5.1 Cluster-based approaches
   5.2 Containers
   5.3 Cloud-based approaches

Literature
Compulsory Reading
Further Reading ▪ Date, C. J. (2003). An introduction to database systems. Pearson. ▪ Kleppmann, M. (2017). Designing data-intensive applications. O'Reilly. ▪ Wiese, L. (2015). Advanced data management. De Gruyter.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods

Tutorial Support
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Online Tests
- ☑ Guideline

Modeling in Automation Engineering and Internet of Things

Module Code: DLMDSEIAAIT

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	10	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Dr. Sahar Qaadan (Modeling in Automation Engineering) / Rachel John Robinson (Internet of Things)

Contributing Courses to Module

- Modeling in Automation Engineering (DLMDSINDA01)
- Internet of Things (DLMBMMIIT01)

Module Exam Type

Module Exam	Split Exam
	Modeling in Automation Engineering • Study Format "Distance Learning": Exam, 90 Minutes Internet of Things • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Modeling in Automation Engineering

- Mathematical frameworks for the formal description of discrete event systems
- Analysis and evaluation methods
- Simulation of discrete event systems
- Supervisory control
- Advanced issues (fault diagnosis, adaptive supervision, optimization)

Internet of Things

- Consumer use cases and risks
- Business use cases and risks
- Social-economic issues
- Enabling technologies and networking fundamentals

Learning Outcomes

Modeling in Automation Engineering

On successful completion, students will be able to

- identify the main issues related to industrial automation and Industry 4.0 automation in particular.
- describe a discrete event system in a formal way by means of different mathematical models.
- analyze the performance of a system using formalisms and numerical simulation approaches.
- choose the best formalism for a given design scenario and formulate requirements.
- design and implement a supervisory controller to fulfill requirements.
- understand advanced topics related to Industry 4.0 industrial automation.

Internet of Things

On successful completion, students will be able to

- distinguish and discuss a broad range of use cases for the internet of things (IoT).
- understand and reflect upon the different perspectives on IoT.
- apply distinct techniques to engineer internet-of-things products.
- evaluate and identify appropriate IoT communication technology and standards according to given IoT product requirements.
- reflect on the respective theoretical foundation, evaluate different approaches, and apply appropriate approaches to practical questions and cases.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
This module is similar to other modules in the fields of Engineering and Computer Science & Artificial Intelligence	All Master Programmes in the IT & Technology fields

Modeling in Automation Engineering

Course Code: DLMDSINDA01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Production systems can be described as discrete event systems where the evolution is characterized by the occurrence of events. In the era of Industry 4.0 and highly-flexible manufacturing, there is the need to provide adequate means for the modeling, analysis, design, and control of flexible production environments.This course introduces several modeling approaches for the mathematical description of discrete event systems, such as Automata, Petri Nets, and Markov processes. Each approach is presented in both theory and practice with examples taken from the industry. The approaches are grouped into logic—where only the logic sequence of events determines the evolution—and timed, where the time schedule of the events also plays an important role. Although simple discrete event systems can be analyzed mathematically, complex systems need the support of computer simulation. The main issues concerning the simulation of discrete event systems are addressed.The final part of this course introduces the concept of supervisory control, which aims at changing the properties of a given system to improve specified behaviors and fulfill defined design specifications. Supervisory control is addressed both from the theoretical practical sides, describing how it can be implemented in a modern industrial environment.The course wraps up with discussion of interesting applications for modeling and design approaches, e.g., in the modeling and analysis of an industrial production unit. Additional conversation on topics like fault-diagnosis, decentralized and distributed supervision, optimization, and adaptive supervision provide a contingent connection between classical industrial automation and the recent, (big) data-driven, flexible, Industry 4.0 advanced industrial automation.

Course Outcomes

On successful completion, students will be able to

- identify the main issues related to industrial automation and Industry 4.0 automation in particular.
- describe a discrete event system in a formal way by means of different mathematical models.
- analyze the performance of a system using formalisms and numerical simulation approaches.
- choose the best formalism for a given design scenario and formulate requirements.
- design and implement a supervisory controller to fulfill requirements.
- understand advanced topics related to Industry 4.0 industrial automation.

Contents

7.1	Production system supervision
7.2	Monitoring and diagnosis of faults
7.3	Distributed and de-centralized supervision
7.4	Model-based optimization of production systems
7.5	Adaptive supervisory control

Literature

Compulsory Reading

Further Reading

- Cassandras, C. G., & Lafortune, S. (2021). Introduction to discrete event systems. Springer.
- Hooley, G., Nicoulaud, B., Rudd, J. M., & Piercy, N. (2020). Marketing strategy and competitive positioning. (7th ed.). Pearson.
- Kaplan, R. and McMillan, D. (2021), . Harvard Business Review Digital Articles.
- Linz, P. (2017). An introduction to formal languages and automata. (6th ed.). Jones & Bartlett Learning.
- Reisig, W. (2013). Understanding Petri nets: Modeling techniques, analysis methods, case studies. Springer.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Practice Exam
- ☑ Online Tests

Internet of Things

Course Code: DLMBMMIIT01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The Internet of Things (IoT), once a rough vision, has become reality today in a broad manner. There is a plethora of devices and services available to both consumers and businesses. From smart homes to smart cities, from smart devices to smart factories – internet-of-things technologies impact on our lives and environments. This course follows a top-down approach, discussing a broad set of aspects connected with the internet of things. It starts with use cases and risks from the perspectives of customers and businesses and winds up with a technical foundation of the internet of things. To address the engineering perspective, a set of techniques is proposed.

Course Outcomes

On successful completion, students will be able to

- distinguish and discuss a broad range of use cases for the internet of things (IoT).
- understand and reflect upon the different perspectives on IoT.
- apply distinct techniques to engineer internet-of-things products.
- evaluate and identify appropriate IoT communication technology and standards according to given IoT product requirements.
- reflect on the respective theoretical foundation, evaluate different approaches, and apply appropriate approaches to practical questions and cases.

Contents

1. Introduction into the Internet of Things
    - 1.1 Foundations and Motivations
    - 1.2 Potential and Challenges
2. Social and Business Relevance
    - 2.1 Innovations for Consumers and Industry
    - 2.2 Impact on Human and Work Environment
    - 2.3 Privacy and Security
3. Architectures of Internet of Things and Industrial Internet of Things
    - 3.1 Elements of IoTs and IIoTs
    - 3.2 Sensors and Nodes

3.3 Power Systems
3.4 Fog Processors
3.5 Platforms

4. Communication Standards and Technologies
   4.1 Network Topologies
   4.2 Network Protocols
   4.3 Communication Technologies

5. Data Storage and Processing
   5.1 NoSQL and MapReduce
   5.2 Linked Data and RDF(S)
   5.3 Semantic Reasoning
   5.4 Complex Event Processing
   5.5 Machine Learning
   5.6 Overview of Existing Data Storage and Processing Platforms

6. Fields of Application
   6.1 Smart Home/Living
   6.2 Smart Buildings
   6.3 Ambient Assisted Living
   6.4 Smart Energy/Grid
   6.5 Smart Factory
   6.6 Smart Logistics
   6.7 Smart Healthcare
   6.8 Smart Agriculture

Literature

Compulsory Reading

Further Reading

- Lea, P. (2018). Internet of things for architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security. Birmingham: Packt Publishing Ltd. (Database: Dawson).
- McEwen, A., & Cassimally, H. (2013). Designing the internet of things. Chichester: John Wiley & Sons. (Database: ProQuest).
- Raj, P., & Raman, A. C. (2017). The Internet of Things: Enabling technologies, platforms, and use cases. Boca Raton, FL: Auerbach Publications. (Database: ProQuest).
- Weber, R. H., & Weber, R. (2010). Internet of Things. Heidelberg: Springer. (Database: Dawson).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed	☑ Course Book	☑ Practice Exam
☑ Intensive Live Sessions/Learning Sprint	☑ Video	☑ Online Tests
☑ Recorded Live Sessions	☑ Audio	
	☑ Slides	

Artificial Intelligence

Module Code: DLMIMWKI

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Claudia Heß (Artificial Intelligence) / Prof. Dr. Tim Schlippe (Seminar: AI and Society)

Contributing Courses to Module

- Artificial Intelligence (DLMAIAI01)
- Seminar: AI and Society (DLMAISAIS01)

Module Exam Type

Module Exam	Split Exam
	Artificial Intelligence • Study Format "Distance Learning": Exam, 90 Minutes Seminar: AI and Society • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Artificial Intelligence

- History of AI
- AI application areas
- Expert systems
- Neuroscience
- Modern AI systems

Seminar: AI and Society

In this module, students will reflect on current societal and political implications of artificial intelligence. To this end, pertinent topics will be introduced via articles that are then critically evaluated by the students in the form of a written essay.

Learning Outcomes

Artificial Intelligence

On successful completion, students will be able to

- remember the historical developments in the field of artificial intelligence.
- analyze the different application areas of artificial intelligence.
- comprehend expert systems.
- apply Prolog to simple expert systems.
- comprehend the brain and cognitive processes from a neuro-scientific point of view.
- understand modern developments in artificial intelligence.

Seminar: AI and Society

On successful completion, students will be able to

- name selected current societal topics and issues in artificial intelligence.
- explain the influence and impact of artificial intelligence on societal, economic, and polital topics.
- transfer theoretically-acquired knowledge to real-world cases.
- treat in a scientific manner a select topic in the form of a written essay.
- critically question and discuss current societal and political issues arising from the recent advances in artificial intelligence methodology.
- develop own problem-solving skills and processes through reflection on the possible impact of their future occupation in the sector of artificial intelligence.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence.	All Master Programmes in the IT & Technology field.

Artificial Intelligence

Course Code: DLMAIAI01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The quest for artificial intelligence has captured humanity's interest for many decades and has been an active research area since the 1960s. This course will give a detailed overview of the historical developments, successes, and set-backs in AI, as well as the development and use of expert systems in early AI systems.In order to understand cognitive processes, the course will give a brief overview of the biological brain and (human) cognitive processes and then focus on the development of modern AI systems fueled by recent developments in hard- and software. Particular focus will be given to discussion of the development of "narrow AI" systems for specific use cases vs. the creation of general artificial intelligence.The course will give an overview of a wide range of potential application areas in artificial intelligence, including industry sectors such as autonomous driving and mobility, medicine, finance, retail, and manufacturing.

Course Outcomes

On successful completion, students will be able to

- remember the historical developments in the field of artificial intelligence.
- analyze the different application areas of artificial intelligence.
- comprehend expert systems.
- apply Prolog to simple expert systems.
- comprehend the brain and cognitive processes from a neuro-scientific point of view.
- understand modern developments in artificial intelligence.

Contents

1. History of AI
   - 1.1 Historical Developments
   - 1.2 AI Winters
   - 1.3 Notable Advances in Artificial Intelligence
2. Early Systems in Artificial Intelligence
   - 2.1 Overview of Expert Systems
   - 2.2 Introduction to Prolog
   - 2.3 Pattern Recognition and Machine Learning (ML)
   - 2.4 Use Cases

3. Neuroscience and Cognitive Science
   - 3.1 Neuroscience and the Human Brain
   - 3.2 Cognitive Science
   - 3.3 The Relationship Between Neuroscience, Cognitive Science, and Artificial Intelligence

4. Modern Artificial Intelligence Systems
   - 4.1 Recent Developments in Hardware and Software
   - 4.2 Narrow versus General Artificial Intelligence
   - 4.3 Natural Language Processing (NLP) and Computer Vision

5. Applications of Artificial Intelligence
   - 5.1 Mobility and Autonomous Vehicles
   - 5.2 Personalized Medicine
   - 5.3 FinTech
   - 5.4 Retail and Industry

Literature

Compulsory Reading

Further Reading

- Chowdhary, K. R. (2020). Fundamentals of Artificial Intelligence. Springer India.
- Russell, S. & Norvig, P. (2022). Artificial intelligence. A modern approach (4th ed.). Pearson Education.
- Ward, J. (2020). The student's guide to cognitive neuroscience. (4th ed.). Taylor & Francis Group.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Practice Exam
- ☑ Online Tests

Seminar: AI and Society

Course Code: DLMAISAIS01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

In the current decade, impressive advances have been achieved in the field of artificial intelligence. Several cognitive tasks like object recognition in images and video, natural language processing, game strategy, and autonomous driving and robotics are now being performed by machines at unprecedented levels of ability. This course will examine some of societal, economic, and political implications of these developments.

Course Outcomes

On successful completion, students will be able to

- name selected current societal topics and issues in artificial intelligence.
- explain the influence and impact of artificial intelligence on societal, economic, and polital topics.
- transfer theoretically-acquired knowledge to real-world cases.
- treat in a scientific manner a select topic in the form of a written essay.
- critically question and discuss current societal and political issues arising from the recent advances in artificial intelligence methodology.
- develop own problem-solving skills and processes through reflection on the possible impact of their future occupation in the sector of artificial intelligence.

Contents

- The seminar covers current topics concerning the societal impact of artificial intelligence. Each participant must create a seminar paper on a topic assigned to him/her. A current list of topics is given in the Learning Management System.

Literature
Compulsory Reading
Further Reading ▪ Bailey, S. J. (2020). Academic writing for international students of business and economics (Third edition). Routledge. ▪ Day, T. (2018). Success in academic writing. (2nd ed.). ▪ Fang, Z. (2021). Demystifying academic writing: genres, moves, skills, and strategies. Routledge, Taylor & Francis Group. ▪ Silvia, P. J. (2019). How to write a lot: a practical guide to productive academic writing (2nd ed.). American Psychological Association.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

AI and Mastering AI Prompting

Module Code: DLMEAIMAIP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Claudia Heß (Artificial Intelligence) / Prof. Dr. Gissel Velarde Perez (Project: AI Excellence with Creative Prompting Techniques)

Contributing Courses to Module

- Artificial Intelligence (DLMAIAI01)
- Project: AI Excellence with Creative Prompting Techniques (DLMPAIECPT01)

Module Exam Type

Module Exam	Split Exam
	Artificial Intelligence • Study Format "Distance Learning": Exam, 90 Minutes Project: AI Excellence with Creative Prompting Techniques • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Artificial Intelligence

- History of AI
- Expert Systems
- Neuroscience
- Modern AI Systems
- AI Application Areas

Project: AI Excellence with Creative Prompting Techniques

In this module, students delve into the world of generative AI applications, creating AI-generated content such as text, images, and videos. They learn to design, analyze, and evaluate different prompting techniques in these systems and apply them within their respective fields of study.

Learning Outcomes

Artificial Intelligence

On successful completion, students will be able to

- remember the historical developments in the field of artificial intelligence.
- analyze the different application areas of artificial intelligence.
- comprehend expert systems.
- apply Prolog to simple expert systems.
- comprehend the brain and cognitive processes from a neuro-scientific point of view.
- understand modern developments in artificial intelligence.

Project: AI Excellence with Creative Prompting Techniques

On successful completion, students will be able to

- comprehend and implement various prompting techniques in generative AI applications.
- analyze, assess, and combine different prompt techniques for various expected AI outputs.
- implement ethical considerations into the design and execution of various generative AI applications.
- design, implement, and refine effective prompts and their combinations for real-world scenarios through various hands-on exercises.
- showcase creative and innovative thinking and reasoning in the application of advanced prompting techniques to solve multidimensional problems in their specialized area of study.

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Data Science & Artificial Intelligence	All Master Programs in the IT & Technology field

Artificial Intelligence

Course Code: DLMAIAI01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The quest for artificial intelligence has captured humanity's interest for many decades and has been an active research area since the 1960s. This course will give a detailed overview of the historical developments, successes, and set-backs in AI, as well as the development and use of expert systems in early AI systems.In order to understand cognitive processes, the course will give a brief overview of the biological brain and (human) cognitive processes and then focus on the development of modern AI systems fueled by recent developments in hard- and software. Particular focus will be given to discussion of the development of "narrow AI" systems for specific use cases vs. the creation of general artificial intelligence.The course will give an overview of a wide range of potential application areas in artificial intelligence, including industry sectors such as autonomous driving and mobility, medicine, finance, retail, and manufacturing.

Course Outcomes

On successful completion, students will be able to

- remember the historical developments in the field of artificial intelligence.
- analyze the different application areas of artificial intelligence.
- comprehend expert systems.
- apply Prolog to simple expert systems.
- comprehend the brain and cognitive processes from a neuro-scientific point of view.
- understand modern developments in artificial intelligence.

Contents

1. History of AI
   - 1.1 Historical Developments
   - 1.2 AI Winters
   - 1.3 Notable Advances in Artificial Intelligence
2. Early Systems in Artificial Intelligence
   - 2.1 Overview of Expert Systems
   - 2.2 Introduction to Prolog
   - 2.3 Pattern Recognition and Machine Learning (ML)
   - 2.4 Use Cases

3. Neuroscience and Cognitive Science
   - 3.1 Neuroscience and the Human Brain
   - 3.2 Cognitive Science
   - 3.3 The Relationship Between Neuroscience, Cognitive Science, and Artificial Intelligence

4. Modern Artificial Intelligence Systems
   - 4.1 Recent Developments in Hardware and Software
   - 4.2 Narrow versus General Artificial Intelligence
   - 4.3 Natural Language Processing (NLP) and Computer Vision

5. Applications of Artificial Intelligence
   - 5.1 Mobility and Autonomous Vehicles
   - 5.2 Personalized Medicine
   - 5.3 FinTech
   - 5.4 Retail and Industry

Literature

Compulsory Reading

Further Reading

- Chowdhary, K. R. (2020). Fundamentals of Artificial Intelligence. Springer India.
- Russell, S. & Norvig, P. (2022). Artificial intelligence. A modern approach (4th ed.). Pearson Education.
- Ward, J. (2020). The student's guide to cognitive neuroscience. (4th ed.). Taylor & Francis Group.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Theory Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods

Tutorial Support
- ☑ Course Feed
- ☑ Intensive Live Sessions/Learning Sprint
- ☑ Recorded Live Sessions

Learning Material
- ☑ Course Book
- ☑ Video
- ☑ Slides

Exam Preparation
- ☑ Practice Exam
- ☑ Online Tests

Project: AI Excellence with Creative Prompting Techniques

Course Code: DLMPAIECPT01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

In this course, students explore the exciting world of prompting in various generative AI applications. They involve themselves in hands-on exercises that combine various prompting techniques to create new AI-generated content, including text, images, and videos. Through these exercises, students learn how to effectively use, analyze, combine, and assess these systems within their specialized fields of study.

Course Outcomes

On successful completion, students will be able to

- comprehend and implement various prompting techniques in generative AI applications.
- analyze, assess, and combine different prompt techniques for various expected AI outputs.
- implement ethical considerations into the design and execution of various generative AI applications.
- design, implement, and refine effective prompts and their combinations for real-world scenarios through various hands-on exercises.
- showcase creative and innovative thinking and reasoning in the application of advanced prompting techniques to solve multidimensional problems in their specialized area of study.

Contents

- In this course, students engage in a practical application of a generative AI use case by choosing from the options provided in the extensive supplementary guide. The course presents practical examples as study materials and exercises with both individual and combined prompting techniques for open-source text, image, and video generation use cases. The exercises are crafted to inspire and lead students in executing their distinct generative AI use case work and provide guidance on describing the use case and selecting a mixture of prompting techniques. Additionally, students are led to critically evaluate the design, implementation, and the outcomes from both technical and ethical perspectives.

Literature
Compulsory Reading
Further Reading ▪ Dang, H., Mecke, L., Lehmann, F., Goller, S., & Buschek, D. (2022). How to prompt? Opportunities and challenges of zero- and few-shot learning for human-AI interaction in creative applications of generative models. arXiv. https://arxiv.org/pdf/2209.01390.pdf ▪ Epstein, Z., Hertzmann, A., Herman, L., Mahari, R., Frank, M. R., Groh, M., Schroeder, H., Smith, A., Akten, M., Fjeld, J., Farid, H., Leach, N., Pentland, A. S., & Russakovsky, O. (2023). Art and the science of generative AI: A deeper dive. arXiv. https://arxiv.org/pdf/2306.04141.pdf ▪ Gozalo-Brizuela, R., & Garrido-Merchán, E. C. (2023). A survey of generative AI applications. arXiv. https://arxiv.org/pdf/2306.02781.pdf ▪ Wei, J., Wang, X., Schuurmans, D., Bosma, M. Ichter, B., Xia, F., Chi, E. H., Le., Q. V., & Zhou, D. (2023). Chain-of-though prompting elicit reasoning in large language models. arXiv. https://arxiv.org/pdf/2201.11903.pdf

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods		
Tutorial Support	**Learning Material**	**Exam Preparation**
☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions	☑ Slides	☑ Guideline

Internship

Module Code: FSINTER

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	None		10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Andreas Simon (Internship)

Contributing Courses to Module

- Internship (FSINTER01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Internship Re lection Paper (passed / not passed)	

Weight of Module

see curriculum

Module Contents

Internship according to the Internship Regulations of the IU.

Learning Outcomes

Internship

On successful completion, students will be able to

- apply skills and knowledge they have obtained previously during their study program in an entrepreneurial environment.
- develop his / her practical and analytical skills in order to improve his / her employability.
- have practical knowledge and learn to work within an organization.
- acquire a first deep insight into organizational structures and communication procedures.
- apply comminication skills, socials skills, problem solving, time and project management which will shape their general management skills.
- shape their personality with the help of the interdisciplinary nature of the course especially in the area of the key qualifications like interpersonal skills or intercultural skills.

Links to other Modules within the Study Program	**Links to other Study Programs of the University**
Builds on modules of the chosen degree program	All myStudies programs

Internship

Course Code: FSINTER01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
	English		10	None

Course Description

This module consists of two parts: (1) preparation tutorials and (2) the internship itself. During the preparation tutorials, students will learn about the intention of the internship and about the intellectual as well as social requirements of the working environment.

Course Outcomes

On successful completion, students will be able to

- apply skills and knowledge they have obtained previously during their study program in an entrepreneurial environment.
- develop his / her practical and analytical skills in order to improve his / her employability.
- have practical knowledge and learn to work within an organization.
- acquire a first deep insight into organizational structures and communication procedures.
- apply comminication skills, socials skills, problem solving, time and project management which will shape their general management skills.
- shape their personality with the help of the interdisciplinary nature of the course especially in the area of the key qualifications like interpersonal skills or intercultural skills.

Contents

- Internship according to the Internship Regulations of the IU.

Literature

Compulsory Reading

Further Reading

- Sweitzer, F. H. & King, M. A. (2009). The Successful Internship: Personal, Professional, and Civic Development. 3rd ed.. Cengage. ISBN: 0-495-59642-6.
- Kaser, K., Brooks, J. R. & Brooks, K. (2007). Making the Most of your Internship. Thomson. ISBN: 0-538-44432-0.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Internship Reflection Paper (passed / not passed)

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
0 h	0 h	0 h	0 h	300 h	300 h

Instructional Methods
Tutorial Support ☑ Course Feed ☑ Intensive Live Sessions/Learning Sprint ☑ Recorded Live Sessions

Master Thesis

Module Code: MMTHE

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	30	900 h

Semester / Term	Duration	Regularly offered in	Language of Instruction and Examination
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Degree Program Advisor (SGL) (Master Thesis) / Degree Program Advisor (SGL) (Colloquium)

Contributing Courses to Module

- Master Thesis (MMTHE01)
- Colloquium (MMTHE02)

Module Exam Type

Module Exam	Split Exam
	Master Thesis • Study Format "Distance Learning": Master Thesis (90) Colloquium • Study Format "Distance Learning": Colloquium (10)

Weight of Module

see curriculum

Module Contents

Master Thesis

- Master's thesis

Colloquium

- Colloquium on the Master's thesis

Learning Outcomes

Master Thesis

On successful completion, students will be able to

- work on a problem from their major field of study by applying the specialist and methodological skills they have acquired during their studies.
- analyse selected tasks with scientific methods, critically evaluate them and develop appropriate solutions under the guidance of an academic supervisor.
- record and analyse existing (research) literature appropriate to the topic of the Master's thesis.
- prepare a detailed written elaboration in compliance with scientific methods.

Colloquium

On successful completion, students will be able to

- present a problem from their field of study under consideration of academic presentation and communication techniques.
- reflect on the scientific and methodological approach chosen in the Master's thesis.
- actively answer subject-related questions from subject experts (experts of the Master's thesis).

Links to other Modules within the Study Program	Links to other Study Programs of the University
This module is similar to other modules in the field of Methods	All Master Programmes in the Business field

Master Thesis

Course Code: MMTHE01

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		27	none

Course Description

The aim and purpose of the Master's thesis is to successfully apply the subject-specific and methodological competencies acquired during the course of study in the form of an academic dissertation with a thematic reference to the major field of study. The content of the Master's thesis can be a practical-empirical or theoretical-scientific problem. Students should prove that they can independently analyse a selected problem with scientific methods, critically evaluate it and work out proposed solutions under the subject-methodological guidance of an academic supervisor. The topic to be chosen by the student from the respective field of study should not only prove the acquired scientific competences, but should also deepen and round off the academic knowledge of the student in order to optimally align his professional abilities and skills with the needs of the future field of activity.

Course Outcomes

On successful completion, students will be able to

- work on a problem from their major field of study by applying the specialist and methodological skills they have acquired during their studies.
- analyse selected tasks with scientific methods, critically evaluate them and develop appropriate solutions under the guidance of an academic supervisor.
- record and analyse existing (research) literature appropriate to the topic of the Master's thesis.
- prepare a detailed written elaboration in compliance with scientific methods.

Contents

- Within the framework of the Master's thesis, the problem as well as the scientific research goal must be clearly emphasized. The work must reflect the current state of knowledge of the topic to be examined by means of an appropriate literature analysis. The student must prove his ability to use the acquired knowledge theoretically and/or empirically in the form of an independent and problem-solution-oriented application.

Literature
Compulsory Reading
Further Reading ▪ Bui, Y. N. (2013). How to Write a Master's Thesis (2nd ed.). SAGE Publications, Incorporated. ▪ Turabian, K. L. (2013). A Manual for Writers of Research Papers, theses, and dissertations (8th ed.). University of Chicago Press. ▪ Further subject specific literature

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Thesis Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Master Thesis

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
810 h	0 h	0 h	0 h	0 h	810 h

Instructional Methods

Colloquium

Course Code: MMTHE02

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
MA	English		3	none

Course Description

The colloquium will take place after submission of the Master's thesis. This is done at the invitation of the experts. During the colloquium, the students must prove that they have fully independently produced the content and results of the written work. The content of the colloquium is a presentation of the most important work contents and research results by the student, and the answering of questions by the experts.

Course Outcomes

On successful completion, students will be able to

- present a problem from their field of study under consideration of academic presentation and communication techniques.
- reflect on the scientific and methodological approach chosen in the Master's thesis.
- actively answer subject-related questions from subject experts (experts of the Master's thesis).

Contents

- The colloquium includes a presentation of the most important results of the Master's thesis, followed by the student answering the reviewers' technical questions.

Literature

Compulsory Reading

Further Reading

- Renz, K.-C. (2016): The 1 x 1 of the presentation. For school, study and work. (2nd ed.). Springer Gabler.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Thesis Course

Information about the examination	
Examination Admission Requirements	**Online Tests:** no
Type of Exam	Colloquium

Student Workload					
Self Study	**Contact Hours**	**Tutorial/Tutorial Support**	**Self Test**	**Independent Study**	**Hours Total**
90 h	0 h	0 h	0 h	0 h	90 h

Instructional Methods