MODULE HANDBOOK

Master of Science

Master Cyber Security (FS-MACSE-120)

120 ECTS

Distance Learning

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

Contents

---

3. Semester

2021-05-01

1. Semester

Corporate Governance of IT, Compliance, and Law

Module Code: DLMIGCR-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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. André Köhler (Corporate Governance of IT, Compliance, and Law)

Contributing Courses to Module

- Corporate Governance of IT, Compliance, and Law (DLMIGCR01-01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Corporate Governance of IT, Compliance, and Law

Course Code: DLMIGCR01-01_E

Study Level	Language of Instruction	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 Term: Governance and IT Governance
   - 1.2 Parameters for IT Governance
   - 1.3 Typical IT Governance Frameworks
2. COBIT framework
   - 2.1 Overview of the elements of COBIT
   - 2.2 The goals cascade of COBIT
   - 2.3 Governance and Management Objectives
   - 2.4 Use of COBIT
3. IT Compliance
   - 3.1 IT Compliance and IT Governance
   - 3.2 Examples of national and international guidelines
   - 3.3 Typical measures

4. Basic IT protection according to BSI
   - 4.1 Overview and structure
   - 4.2 The approach to IT protection
   - 4.3 Usage example of IT protection

5. IT Law
   - 5.1 Overview of relevant laws
   - 5.2 Protection of intellectual property
   - 5.3 IT Contracts
   - 5.4 Privacy

Literature

Compulsory Reading

Further Reading

- Harmer, G. (2014): Governance of Enterprise IT based on COBIT 5. A Management Guide. itgp,Ely (UK).
- ISACA (Hrsg.) (2012): COBIT 5. A Business Framework for the Governance and Management of Enterprise IT. Isaca, Berlin.
- ISACA (2018): COBIT® 2019 Framework: Introduction & Methodology. Isaca, Schaumburg, IL.
- Weill, P./Ross, J. W. (2004): IT Governance. How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business Review Press, Watertown, MA.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLMIGCR01-01_E

Advanced Mathematics

Module Code: DLMDSAM

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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Eric Guiffo Kaigom (Advanced Mathematics)

Contributing Courses to Module

- Advanced Mathematics (DLMDSAM01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
This module is similar to other modules in the field of Methods.	All Master Programmes in the Business & Management field.

Advanced Mathematics

Course Code: DLMDSAM01

Study Level	Language of Instruction	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 & Integration
   - 1.2 Partial Differentiation & Integration
   - 1.3 Vector Analysis
   - 1.4 Calculus of Variations
2. Integral Transformations
   - 2.1 Convolution
   - 2.2 Fourier Transformation
3. Vector Algebra
   - 3.1 Scalars and Vectors
   - 3.2 Addition, Subtraction of Vectors
   - 3.3 Multiplication of Vectors, Vector Product, Scalar Product

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

5. Matrices and Vector Spaces
   - 5.1 Basic Matrix Algebra
   - 5.2 Determinant, Trace, Transpose, Complex, and Hermitian Conjugates
   - 5.3 Eigenvectors and Eigenvalues
   - 5.4 Diagonalization
   - 5.5 Tensors

6. Information Theory
   - 6.1 MSE
   - 6.2 Gini Index
   - 6.3 Entropy, Shannon Entropy, Kulback Leibler Distance
   - 6.4 Cross Entropy

Literature

Compulsory Reading

Further Reading

- Cover, T., & Joy, A. (2006). Elements of information theory (2nd ed.). Hoboken, NJ: John Wiley & Sons, Inc.
- McKay, D. (2003). Information theory, inference and learning algorithms. Cambridge: Cambridge University Press.
- Riley, K. F., Hobson, M. P., & Bence, S. J. (2006). Mathematical methods for physics and engineering (3rd ed.). Cambridge: Cambridge University Press.
- Strang, G. (2016). Introduction to linear algebra. Wellesley, MA: Wellesley-Cambridge Press.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☑ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLMDSAM01

Cyber Security and Data Protection

Module Code: DLMCSITSDP

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
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 (DLMCSITSDP01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Oral Assignment	

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.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
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: DLMCSITSDP01

Study Level	Language of Instruction	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.

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 ▪ Bowman, C., Gesher, A., Grant, J., & Slate, D. (2015). The architecture of privacy: On engineering technologies that can deliver trustworthy safeguards. Sebastopol, CA: O'Reilly. ▪ Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2015). Foundations of information security (3rd ed.). Zaltbommel: Van Haren Publishing. ▪ ISO/IEC 29100. (2011). Information technology — Security techniques — Privacy framework. ISO. Retrieved from https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip ▪ Paar, C., & Pelzl, J. (2011). Understanding cryptography: A textbook for students and practitioners. Heidelberg: Springer. ▪ The Open Web Application Security Project (OWASP). (2005). A guide to building secure web applications and web services. OWASP. Retrieved from https://www.um.es/atica/documentos/OWASPGuide2.0.1.pdf

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Advanced Research Methods

Module Code: DLMARM

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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Josephine Zhou-Brock (Advanced Research Methods)

Contributing Courses to Module

- Advanced Research Methods (DLMARM01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Written Assessment: Written Assignment	

Weight of Module

see curriculum

Module Contents

- Social science and research paradigms
- Case study research
- Specific topics of qualitative research
- Advanced issues of qualitative research conceptualization and data analysis
- Underlying assumptions of quantitative research: concepts and consequences
- Evaluation research

Learning Outcomes

Advanced Research Methods

On successful completion, students will be able to

- understand and apply scientific methodologies in conducting empirical research.
- plan, design, and prepare research proposals.
- differentiate between different types of case studies, select and apply different data collection strategies.
- plan, conduct, and analyze case studies and surveys.
- scientifically analyze quantitative and qualitative data.
- conduct evaluation research to determine quality of research.

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

Advanced Research Methods

Course Code: DLMARM01

Study Level	Language of Instruction	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

- understand and apply scientific methodologies in conducting empirical research.
- plan, design, and prepare research proposals.
- differentiate between different types of case studies, select and apply different data collection strategies.
- plan, conduct, and analyze case studies and surveys.
- scientifically analyze quantitative and qualitative data.
- conduct evaluation research to determine quality of research.

Contents

1. Theoretical Background: Social Science and Research Paradigms
   - 1.1 What is a Paradigm?
   - 1.2 Empiricism
   - 1.3 Critical Rationalism
   - 1.4 Epistemological Anarchism
   - 1.5 Structural Functionalism
   - 1.6 Symbolic Interactionism
   - 1.7 Ethnomethodology

2. Case Study Research
   - 2.1 Types of Case Study Research
   - 2.2 Maintaining Quality in Case Study Research
   - 2.3 Case Study Design
   - 2.4 Implementing Case Studies
   - 2.5 Analyzing Case Studies

3. Specific Topics of Qualitative Research
   - 3.1 Idea Generation
   - 3.2 Critical Incident Technique
   - 3.3 Understanding Communication: Discourse Analysis
   - 3.4 Perceiving Perception: Interpretive Phenomenological Analysis

4. Advanced Issues of Qualitative Research Conceptualizing and Data Analysis
   - 4.1 Measurement Theory
   - 4.2 Index and Scale Construction
   - 4.3 Types of Scale Construction
   - 4.4 The Problem of Nonresponse and Missing Data
   - 4.5 Implications of IT for Research Strategies

5. Underlying Assumptions of Quantitative Research: Concepts and Consequences
   - 5.1 Classical Test Theory
   - 5.2 Probabilistic Test Theory
   - 5.3 Advanced Topics of Test Theory

6. Evaluation Research
   - 6.1 What is Evaluation Research?
   - 6.2 Types of Evaluation Research
   - 6.3 Meta-Analysis
   - 6.4 Meta-Evaluation

Literature
Compulsory Reading
Further Reading ▪ Babbie, E. R. (2021). The practice of social research (15th ed.). Cengage Learning. ▪ Giles, D. C. (2002). Advanced research methods in psychology. Routledge. ▪ Saunders, M., Thornhill, A., & Lewis, P. (2009). Research methods for business students (5th ed.). Pearson.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Written Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Seminar: Advanced Cyber Security

Module Code: DLMCSSAITS

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLMCSITSDP01, DLMDSAM01	MA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
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 (DLMCSEAITSC01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
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: DLMCSEAITSC01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSITSDP01 or DLMCSITSDS01

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 ▪ Bowman, C. et al. (2015). The architecture of privacy. On engineering technologies that can deliver trustworthy safeguards. O'Reilly, Sebastopol, CA:. ▪ Hintzbergen, J. et al. (2015): Foundations of information security. 3rd ed., Van Haren Publishing, Zaltbommel. ▪ ISO/IEC 29100 (2011): Information technology — Security techniques — Privacy framework. ISO. (URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip [Retrieved: 22.3.2020]). ▪ Paar, C./Pelzl, J. (2011). Understanding cryptography: A textbook for students and practitioners. Springer, Heidelberg. ▪ The Open Web Application Security Project (OWASP) (2005): A guide to building secure web applications and web services. OWASP. (URL: https://www.um.es/atica/documentos/OWASPGuide2.0.1.pdf [Retrieved: 22.3.2020]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☑ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Cryptology

Module Code: DLMCSC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLMCSEAITSC01; DLMCSITSDP01 or DLMCSITSDS01	MA	5	150 h

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

Module Coordinator

Prof. Dr. Ralf Kneuper (Cryptology)

Contributing Courses to Module

- Cryptology (DLMCSEAITSC02)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Oral Assignment	

Weight of Module

see curriculum

Module Contents

- Symmetric and asymmetric cryptosystems
- Authentication
- Cryptanalysis
- Cryptology in the internet
- 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 IUBH**
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: DLMCSEAITSC02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSEAITSC01; DLMCSITSDP01 or DLMCSITSDS01

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 Kerckhoffs's principle

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)

3. Asymmetric cryptosystems
   - 3.1 The RSA algorithm
   - 3.2 Elliptic curves
   - 3.3 Cryptographic hash functions
   - 3.4 Signatures and MACs
   - 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 – how to break encryption
   - 5.1 Frequency analysis
   - 5.2 Brute-force attacks
   - 5.3 Rainbow tables
   - 5.4 Known/chosen plaintext
   - 5.5 Side-channel attacks

6. Cryptology and the internet
   - 6.1 Basic setup of the Internet and its protocols
   - 6.2 IPSec
   - 6.3 Transport Layer Security
   - 6.4 Secure E-Mail (TLS, S/MIME and PGP)
   - 6.5 Secure DNS

7. Practical aspects of cryptology
   - 7.1 Random number generation
   - 7.2 Long-term security (key lengths, perfect forward security, quantum computing)
   - 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

- Beutelspacher, A. (1994). Cryptology. Washington, DC: Mathematical Association of America.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography engineering. Design principles and practical applications. Indianapolis, IN: Wiley.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. Boca Raton, FL: CRC Press.
- Paar, C., & Pelzl, J. (2011). Understanding cryptography: A textbook for students and practitioners. Berlin, Heidelberg: Springer.
- Singh, S. (2002). The code book: The secret history of codes and code-breaking. New York, NY: Harper Collins.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** yes
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

2. Semester

Cyber Risk Assessment and Management

Module Code: DLMCSECRAM_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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Cyber Risk Assessment and Management)

Contributing Courses to Module

- Cyber Risk Assessment and Management (DLMCSECRAM01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
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: DLMCSECRAM01_E

Study Level	Language of Instruction	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 Incident Response Planning
   - 6.5 Cyber Insurance

Literature

Compulsory Reading

Further Reading

- Coburn, A./Leverett, E./Woo, G. (2018): Solving Cyber Risk: Protecting Your Company and Society. John Wiley & Sons, Hoboken, NJ.
- Joint Task Force Transformation Initiative. (2012): Guide for Conducting Risk Assessments. Revision 1, NIST Computer Security Division. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- Pfleeger, C. P. (1996): Security in Computing. Prentice-Hall, Upper Saddle River, NJ.
- Schneier, B. (1999): Attack Trees. In Doctor Dobb's Journal December 1999. https://www.schneier.com/academic/archives/1999/12/attack_trees.html
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLMCSECRAM01_E

IT Systems: Software

Module Code: DLMIMITSS_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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Christian Prause (IT Systems: Software)

Contributing Courses to Module

- IT Systems: Software (DLMIMITSS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH
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: DLMIMITSS01_E

Study Level	Language of Instruction	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 workstation
   - 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.
- Chambers, J.M. (2014): Object-Oriented Programming, Functional Programming and R. Statistical Science. 29. Jg., Heft 2, S.167–180.
- Tanenbaum, A.S. (2016): Modern Operating Systems. 4th edition, Pearson India, Delhi/Chennai.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

IT Systems: Hardware

Module Code: DLMIMITSH_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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Damir Ismailovic (IT Systems: Hardware)

Contributing Courses to Module

- IT Systems: Hardware (DLMIMITSH01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
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: DLMIMITSH01_E

Study Level	Language of Instruction	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 Disk

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 ▪ Gomez, M. et al (eds.) (2017) : Engineering and Management of Data Centers: An IT Service Management Approach. Springer International Publishing, Cham. ▪ Hwaiyu Geng, P.E. (2014): Data Center Handbook. John Wiley & Sons, New York City, NY. ▪ Tanenbaum, A. / Austin, T. (2012): Structured Computer Organization. 6th edition, Pearson, London. ▪ Tanenbaum, A. / van Stehen, M. (2016): Distributed Systems: Principles and Paradigms. 2nd edition, CreateSpace Independent Publishing Platform. ▪ Tanenbaum, A. / Wetherall, D. (2010): Computer Networks. 5th edition, Pearson, London.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Cyber Systems and Network Forensics

Module Code: DLMCSECSNF_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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Cyber Systems and Network Forensics)

Contributing Courses to Module

- Cyber Systems and Network Forensics (DLMCSECSNF01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
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: DLMCSECSNF01_E

Study Level	Language of Instruction	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

- Kaufman C. / Perlman, R. / Speciner, M. (2002): Network Security: Private Communication in a Public World, Second Edition, Pearson Education, London.
- Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.
- Pfleeger C. P. / Pfleeger S. L. / Marguilies, J. (2015): Security in Computing. 5th Edition, Pearson Education, London.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLMCSECSNF01_E

Secure Networking

Module Code: DLMCSEESN1_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLMIMITSS01_E or DLMIMITSS01; DLMIMITSH01_E or DLMIMITSH01	MA	5	150 h

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

Module Coordinator

Prof. Dr. Tobias Brückmann (Secure Networking)

Contributing Courses to Module

- Secure Networking (DLMCSEESN01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
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: DLMCSEESN01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	DLMIMITSS01_E or DLMIMITSS01; DLMIMITSH01_E or DLMIMITSH01

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 ▪ Kaufman, C./Perlman, R./Speciner, M. (2002): Network Security. Private Communication in a Public World, Second Edition, Pearson Education, London. ▪ Pfleeger, C. P./Pfleeger, S.L./ Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London. ▪ van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature AG, Berlin/ Heidelberg.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Theoretical Computer Science for IT Security

Module Code: DLMCSETCSITS_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
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 (DLMCSETCSITS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
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: DLMCSETCSITS01_E

Study Level	Language of Instruction	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 Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLMCSETCSITS01_E

3. Semester

Seminar: Standards and Frameworks

Module Code: DLMIMSSF_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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. André Köhler (Seminar: Standards and Frameworks)

Contributing Courses to Module

- Seminar: Standards and Frameworks (DLMIMSSF01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 IUBH**
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: DLMIMSSF01_E

Study Level	Language of Instruction	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

- Johannsen, W./Goeken, M. (2011): Referenzmodelle für IT-Governance. Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co. dpunkt.verlag, Heidelberg.
- Krallmann, H./Bobrik, A./Levina, O. (Hrsg.) (2013): Systemanalyse im Unternehmen. Prozessorientierte Methoden der Wirtschaftsinformatik. Walter de Gruyter, Berlin.
- Müller, K. R. (2018): IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts-und Risikomanagement–Sichere Anwendungen–Standards und Practices. Springer, Berlin.
- Rüter, A. et al. (Hrsg.) (2010): IT-Governance in der Praxis. Erfolgreiche Positionierung der IT im Unternehmen. Anleitung zur erfolgreichen Umsetzung regulatorischer und wettbewerbsbedingter Anforderungen. Springer, Berlin.
- Tiemeyer, E. (Hrsg.) (2016): Handbuch IT-Systemmanagement. Handlungsfelder, Prozesse, Managementinstrumente, Good-Practices. Carl Hanser Verlag, München.
- van Wessel, R. (Hrsg.) (2010): Toward Corporate IT Standardization Management. Frameworks and Solutions. IGI Global, Hershey, PA.
- Wagner, K. P. (2015): Ermittlung des Reifegrads von Informationstechnologie in kleinen und mittleren Unternehmen. Berliner Wissenschaftsverlag, Berlin.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Project: Current Challenges of Cyber Security

Module Code: DLMCSEPCCCS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLMCSITSDP01 or DLMCSITSDS01	MA	5	150 h

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

Module Coordinator

Prof. Dr. Ralf Kneuper (Project: Current Challenges of Cyber Security)

Contributing Courses to Module

- Project: Current Challenges of Cyber Security (DLMCSEPCCCS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning 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 This module is similar to other modules in the fields of Computer Science & Software Development	**Links to other Study Programs of IUBH** All Master Programs in the IT & Technology fields

Project: Current Challenges of Cyber Security

Course Code: DLMCSEPCCCS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSITSDP01 or DLMCSITSDS01

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 Distance Learning

Study Format	**Course Type**
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLMCSEPCCCS01_E

Cyber Criminality

Module Code: DLMIMWCK_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLMIMWCK01_E	MA	10	300 h

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

Module Coordinator

Prof. Dr. Alexander Lawall (Attack Scenarios and Incident Response) / Prof. Dr. Alexander Lawall (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 IUBH
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	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

- Fleischer, D. (2016): Wirtschaftsspionage. Springer Fachmedien, Wiesbaden.
- Klipper, S. (2015): Cyber Security. Ein Einblick für Wirtschaftswissenschaftler. Springer, Berlin.
- Kraft, P./Weyert, A. (2017): Network Hacking. Professionelle Angriffs-und Verteidigungstechniken gegen Hacker und Datendiebe. Franzis Verlag, München.
- Labudde, D./Spranger, M. (Hrsg.) (2017): Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. Springer, Berlin.
- Lenhard, T. H. (2017): Datensicherheit. Technische und organisatorische Schutzmassnahmen gegen Datenverlust und Computerkriminalität. Springer, Berlin.
- Lewis, J./Baker, S. (2013): The economic impact of cybercrime and cyber espionage. McAfee, Santa Clara, CA.
- Müller, K. R. (2018): IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts-und Risikomanagement–Sichere Anwendungen–Standards und Practices. Springer, München.
- Yar, M./Steinmetz, K. F. (2019): Cybercrime and society. SAGE Publications, Thousand Oaks, CA.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Cyber Forensics

Course Code: DLMIMWCK02_E

Study Level	Language of Instruction	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 ▪ Aebi, D. (2013): Praxishandbuch Sicherer IT-Betrieb. Risiken erkennen, Schwachstellen beseitigen, IT-Infrastrukturen schützen. Springer, Berlin. ▪ Banaschik, M. (2011): Internationale E-Discovery und Information Governance. Praxislösungen für Juristen, Unternehmer und IT-Manager. Erich Schmidt Verlag, Berlin. ▪ Geschonneck, A. (2014): Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. dpunkt.verlag, Heidelberg. ▪ Hamid, J./Gianluigi, M./Lilburn, W. D. (2010): Handbook of electronic security and digital forensics. World Scientific Publishing, Singapur. ▪ Labudde, D./Spranger, M. (Hrsg.) (2017): Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. Springer, Berlin. ▪ Meier, S. (2017): Digitale Forensik in Unternehmen (Doktorarbeit). Universität Regensburg, Regensburg.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Portfolio

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLMIMWCK02_E

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
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Rald Kneuper (Blockchain) / Dr. Carsten Blank (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 IUBH**
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	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	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Written Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Quantum Computing

Course Code: DLMCSEBCQC02

Study Level	Language of Instruction	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 ▪ Bernhardt, C. (2019): Quantum computing for everyone. MIT Press, Cambridge, MA. ▪ Faro, I. (2017): A developer's guide to using the Quantum QISKit SDK. Retrieved from https://developer.ibm.com/code/2017/05/17/developers-guide-to-quantum-qiskit-sdk/ ▪ Rieffel, E. G. (2014): Quantum computing. A gentle introduction. MIT Press, Cambridge, MA. ▪ Susskind, L. / Friedman, A. (2015): Quantum mechanics. The theoretical minimum. Penguin, London. ▪ Zygelman, B. (2018): A first introduction to quantum computing and information. Springer, Cham.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

DevSecOps

Module Code: DLMCSEEDSO_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLMCSEEDSO01_E or DLMCSEEDSO01_D	MA	10	300 h

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

Module Coordinator

Prof. Dr. Jesus Luna Garcia (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

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

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 IUBH
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	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	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Secure Software Implementation

Course Code: DLMCSEEDSO02_E

Study Level	Language of Instruction	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	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Organizational Transformation

Module Code: DLMCSDWTO_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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Eike Christiane Fismer (Tools in Organizational Analysis) / N.N. (Management of IT Services and Architecture)

Contributing Courses to Module

- Tools in Organizational Analysis (DLMWPWOAE01_E)
- Management of IT Services and Architecture (MWIT02_E)

Module Exam Type

Module Exam	Split Exam
	Tools in Organizational Analysis • Study Format "Fernstudium": 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 and terms of IT service management
- IT Infrastructure Library (ITIL)
- ITIL - Service Design
- ITIL - Service Transition
- ITIL - Service Operation
- Basics and terms of IT architecture management
- IT Application Portfolio Management
- 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

- identify, explain and differentiate the basic principles of IT strategy, IT governance and IT architecture management.
- explain and differentiate the typical activities of IT architecture management, their interrelationships and their dependencies.
- explain the basics and challenges of IT service management.
- describe the motivation and structure of the IT Infrastructure Library (ITIL), explain the main elements and locate concrete activities in the service lifecycle.
- describe and differentiate the activities of ITIL Governance and ITIL Operational Processes.

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

Tools in Organizational Analysis

Course Code: DLMWPWOAE01_E

Study Level	Language of Instruction	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

- Balzac, S. R. (2014): Organizational Psychology for Managers. Springer, New York, NY.
- Knights, D. / Willmott, H. (2010): Organizational Analysis: Essential Readings. South-Western Cengage Learning, San Francisco, CA.
- Lauer, T. (2021): Change Management. Fundamentals and Success Factors. Springer, Berlin.

Study Format Fernstudium

Study Format	Course Type
Fernstudium	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Management of IT Services and Architecture

Course Code: MWIT02_E

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

Course Description

IT service management is an approach to align and understand information technology of a company as a service provider and supporter of operational and business processes. Quality management and the handling of daily operations are central. In addition to concrete IT projects, e.g. the new development of an IT system or the introduction of a standard software, strategic management must be applied to the organization-wide IT infrastructure - i.e. the quantity of all IT hardware and software systems used. The task of IT architecture management is the strategic alignment of the IT infrastructure with the business and IT strategy of the organization. This course teaches typical concepts, methods, procedures and models for the tasks involved in IT architecture management.

Course Outcomes

On successful completion, students will be able to

- identify, explain and differentiate the basic principles of IT strategy, IT governance and IT architecture management.
- explain and differentiate the typical activities of IT architecture management, their interrelationships and their dependencies.
- explain the basics and challenges of IT service management.
- describe the motivation and structure of the IT Infrastructure Library (ITIL), explain the main elements and locate concrete activities in the service lifecycle.
- describe and differentiate the activities of ITIL Governance and ITIL Operational Processes.

Contents

1. Basics and terms of IT service management
   - 1.1 IT services (also: IT services)
   - 1.2 IT Service Management
2. IT Infrastructure Library (ITIL)
   - 2.1 Service Livecycle and Process Groups in ITIL
   - 2.2 Service Strategy
   - 2.3 Continual Service Improvement

3. ITIL - Service Design
   - 3.1 Service Level Management
   - 3.2 Service Catalog Management
   - 3.3 Availability Management
   - 3.4 Further processes in Service Design

4. ITIL - Service Transition
   - 4.1 Transition Planning and Support
   - 4.2 Change Management
   - 4.3 Service Asset and Configuration Management (SACM)
   - 4.4 Other Processes in the Service Transition

5. ITIL - Service Operation
   - 5.1 Event Management
   - 5.2 Incident Management
   - 5.3 Problem Management
   - 5.4 Further Processes in Service Operation

6. Basics and terms of IT architecture management
   - 6.1 IT enterprise architecture
   - 6.2 Goals of Enterprise Architecture Management
   - 6.3 Processes in the management of IT enterprise architectures

7. IT Application Portfolio Management
   - 7.1 Overview of IT Application Portfolio Management
   - 7.2 Application Manual
   - 7.3 Portfolio analysis
   - 7.4 Development planning

8. Architecture Governance
   - 8.1 Organizational structure
   - 8.2 Policy development and enforcement
   - 8.3 Project support

Literature
Compulsory Reading
Further Reading ▪ Ahlemann, F. et al (2012): Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments. Springer, Heidelberg. ▪ van Bon, H. (2016): ITIL 2011 Edition - A Pocket Guide. Van Haren Publishing, Zaltbommel. ▪ Kotusev, S. (2018): The Practice of Enterprise Architecture: A Modern Approach to Business and IT Alignment. ▪ Pilorget, L. / Schell, T. (2018): IT Management. The art of managing IT based on a solid framework leveraging the company´s political ecosystem. Springer Vieweg, Wiesbaden. ▪ Ross, J. W./Weill, P./Robertson, D. C. (2006): Enterprise Architecture as Strategy. Creating a Foundation for Business Execution. Harvard Business Review Press, Boston.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

IT Law for IT Security

Module Code: DLMCSEEITLS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLMIGCR01-01_E or DLMIGCR01-01; DLMIMWITR01_E or DLMIMWITR01 ▪ none	MA	10	300 h

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

Module Coordinator

Prof. Dr. Valentin Köppert (International IT Law) / N.N. (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
- Fundamental legal opinions
- Relevant areas of law
- European IT law
- Transnational IT law

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 IUBH**
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	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 Case-based (common law) vs. codified law (civil law)
   - 1.2 International, transnational and European law
   - 1.3 Differentiation of IT law from other areas of law

2. Fundamental legal opinions
   - 2.1 Intellectual property and copyright
   - 2.2 Information and verification obligations under civil law
   - 2.3 Basics of telemedia law
   - 2.4 Fundamentals of telecommunications law
   - 2.5 Legal views on data protection and information security

3. Relevant areas of law
   - 3.1 General terms and conditions of business
   - 3.2 IT contract law and contract drafting
   - 3.3 IT service contracts
   - 3.4 Software contracts, license models and general public license
   - 3.5 Electronic commerce (e-commerce)
   - 3.6 Signature law
   - 3.7 Patenting of software

4. European IT law
   - 4.1 EU regulations, directives, decisions and recommendations
   - 4.2 Relationship to the national legal system
   - 4.3 European General Data protection Regulation (GDPR)
   - 4.4 Implementation approaches of the GDPR
   - 4.5 The GDPR as the basis for international jurisdiction

5. Transnational IT law
   - 5.1 Internet law
   - 5.2 Domain law
   - 5.3 Legal consideration of social media
   - 5.4 WTO Information Technology Agreement
   - 5.5 OECD guidelines and recommendations
   - 5.6 Recommendations of the United Nations Information and Communication Technologies Task Force

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

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Legal Framework for IT-Security

Course Code: DLMCSEEITLS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	DLMIGCR01-01_E or DLMIGCR01-01; 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 edition, HarperCollins, New York City, NY. ▪ Lusthaus, J. (2018): Industry of Anonymity. Harvard University Press, Cambridge, MA. ▪ Schmitt, M. N. (ed.) (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge. ▪ Schneier, B. (2015): Data and Goliath. 1st edition, W. W. Norton & Company, New York City, NY.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLMCSEEITLS01_E

Audit- and Security Testing

Module Code: DLMCSEEAST_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLMCSEEAST01_E	MA	10	300 h

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

Module Coordinator

Prof. Dr. Alexander Lawall (Attack Models and Auditing) / Prof. Dr. Jesus Luna Garcia (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 IUBH
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	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

- Bellovin, S. M. (2016): Thinking Security. Stopping Next Year's Hackers. Addison-Wesley, Boston, MA.
- Joint Task Force Transformation Initiative (2012): Guide for Conducting Risk Assessments. Revision 1, NIST Computer Security Division. (URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final [Retrieved: 11.03.2021]).
- Kim, P. (2014): The Hacker Playbook. A Practical Guide to Penetration Testing. CreateSpace Independent Publishing Platform. 4th Edition. (URL: https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf4 [Retrieved: 11.03.2021]).
- Information Systems Audit and Control Association (2020): IT Audit Framework (ITAF). A Professional Practices Framework for IT Audit. Isaca, Rolling Meadows, IL.
- Schneier, B. (1999): Attack Trees. (URL: https://www.schneier.com/academic/archives/1999/12/attack_trees.html [Retrieved: 11.3.2021]).
- Shostack, A. (2014): Threat Modeling. Designing for Security. John Wiley & Sons, Hoboken, NJ.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: IT Security Tests

Course Code: DLMCSEEAST02_E

Study Level	Language of Instruction	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	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLMCSEEAST02_E

Business Analyst

Module Code: DLMDSEBA

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLMDSEBA01 ▪ none	MA	10	300 h

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

Module Coordinator

Prof. Dr. Peter Poensgen (Business Intelligence I) / Prof. Dr. Peter Poensgen (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

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.

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 IUBH
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 fields

Business Intelligence I

Course Code: DLMDSEBA01

Study Level	Language of Instruction	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.

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

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.
- Turban, E., Sharda, R., Delen, D., & King, D. (2010). Business intelligence. A managerial approach (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Case Study

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Project: Business Intelligence

Course Code: DLMDSEBA02

Study Level	Language of Instruction	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.
- Turban, E., Sharda, R., Delen, D., & King, D. (2010). Business intelligence. A managerial approach (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Portfolio

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☑ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Cyber Resilience) / Prof. Dr. Jesus Luna Garcia (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 IUBH
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	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	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Applying Threat Intelligence

Course Code: DLMCSEECLS02_E

Study Level	Language of Instruction	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	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Data Science and Big Data Technologies

Module Code: DLMCSEEDSBDT_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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ulrich Kerzel (Data Science) / Prof. Dr. Thomas Zöller (Big Data Technologies)

Contributing Courses to Module

- Data Science (DLMBDSA01)
- 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
- 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 the different types and sources of data.
- understand different database concepts.
- build new database structures.
- evaluate various data storage frameworks w.r.t. project requirements.
- analyze which data format to use for a given project.
- create a distributed computing environment for a given project.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
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

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

Course Description

The course Data Science 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. 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
- 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 Terms and Definitions
   - 1.3 Applications & Notable Examples
   - 1.4 Sources of Data
   - 1.5 Structured, Unstructured, Streaming
   - 1.6 Typical Data Sources and their Data Type
   - 1.7 The 4 V's of Data: Volume, Variety, Velocity, Veracity
   - 1.8 Introduction to Probability Theory
   - 1.9 What Are Probabilities and Probability Distributions
   - 1.10 Introduction to Bayesian Statistics
   - 1.11 Relation to Data Science: Prediction as a Probability

2. Use Cases and Performance Evaluation
   - 2.1 Identification of Use Cases for Data Science
   - 2.2 Identifying Data Science Use Cases
   - 2.3 From Prediction to Decision: Generating Value from Data Science
   - 2.4 Evaluation of Predictions
   - 2.5 Overview of Relevant Metrics
   - 2.6 Business-centric Evaluation: the Role of KPIs
   - 2.7 Cognitive Biases and Decision-making Fallacies

3. Pre-processing of Data
   - 3.1 Transmission of Data
   - 3.2 Data Quality and Cleansing of Data
   - 3.3 Transformation of Data (Normalization, Aggregation)
   - 3.4 Reduction of Data Dimensionality
   - 3.5 Data Visualisation

4. Processing of Data
   - 4.1 Stages of Data Processing
   - 4.2 Methods and Types of Data Processing
   - 4.3 Output Formats of Processed Data

5. Selected Mathematical Techniques
   - 5.1 Linear Regression
   - 5.2 Principal Component Analysis
   - 5.3 Clustering
   - 5.4 Time-series Forecasting
   - 5.5 Overview of Further Approaches

6. Selected Artificial Intelligence Techniques
   - 6.1 Support Vector Machines
   - 6.2 Neural Networks and Deep Learning
   - 6.3 Feed-forward Networks
   - 6.4 Recurrent Networks and Memory Cells
   - 6.5 Convolutional Networks
   - 6.6 Reinforcement Learning
   - 6.7 Overview of Further Approaches

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	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Big Data Technologies

Course Code: DLMDSBDT01

Study Level	Language of Instruction	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 the different types and sources of data.
- understand different database concepts.
- build new database structures.
- evaluate various data storage frameworks w.r.t. project requirements.
- analyze which data format to use for a given project.
- create a distributed computing environment for a given project.

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. (2012). Database design and relational theory: Normal forms and all that jazz. Sebastopol, CA: O'Reilly Publishing.
- Karau, H., Konwinski, A., Wendell, A., & Zaharia, M. (2015). Learning spark: Lightning-fast data analysis. Sebastopol, CA: O'Reilly Publishing.
- Narkhede, N., Shapira, G., & Palino, T. (2017). Kafka: The definitive guide: Real-time data and stream processing at scale. Sebastopo, CA: O'Reilly Publishing.
- Poulton, N. (2017). Docker deep dive. Nigel Poulton.
- Psaltis, A. (2017). Streaming data: Understanding the real-time pipeline. Shelter Island, NY: Manning Publications.
- Redmond, E., & Wilson, J. R. (2012). Seven databases in seven weeks: A guide to modern databases and the noSQL movement. Dallas, TX: Pragmatic Bookshelf.
- Sadalage, P., & Fowler, M. (2012). NoSQL distilled: A brief guide to the emerging world of polyglot persistence. Ann Arbor, MI: Addison-Wesley.
- Viescas, J., & Hernandez, M. (2014). SQL queries for mere mortals: A hands-on guide to data manipulation in SQL, (3rd ed.). Ann Arbor, MI: Addison-Wesley.
- White, T. (2015). Hadoop: The definitive guide: Storage and analysis at Internet scale. Sebastopol, CA: O'Reilly Publishing.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** yes
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

DLMDSBDT01

Industrial Automation and Internet of Things

Module Code: DLMDSEIAAIT

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
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Leonardo Riccardi (Industrial Automation) / Prof. Dr. Leonardo Riccardi (Internet of Things)

Contributing Courses to Module

- Industrial Automation (DLMDSINDA01)
- Internet of Things (DLMBMMIIT01)

Module Exam Type

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

Weight of Module

see curriculum

Module Contents

Industrial Automation

- 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

Industrial Automation

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 IUBH**
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

Industrial Automation

Course Code: DLMDSINDA01

Study Level	Language of Instruction	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. Applications
   - 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. (Eds.). (2008): Introduction to discrete event systems. Springer, Boston, MA.
- Choi, B. K./Kang, D. (2013): Modeling and simulation of discrete-event systems. Wiley, Hoboken, NJ.
- Ding, D./Wang, Z./Wei, G. (2018): Performance analysis and synthesis for discrete-time stochastic systems with network-enhanced complexities. CRC Press, Boca Raton, FL.
- Hrúz, B./MengChu, Z. (2007): Modeling and control of discrete-event dynamic systems. Springer, London.
- Seatzu, C./Silva, M./van Schuppen, J. H. (Eds.). (2013): Control of discrete-event systems. Springer, London.
- Wonham, W. M./Cai, K. (2019): Supervisory control of discrete-event systems. Springer, Cham.
- Zimmermann, A. (2008): Stochastic discrete event systems. Springer, Berlin/Heidelberg.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Module Exam

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Internet of Things

Course Code: DLMBMMIIT01

Study Level	Language of Instruction	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	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

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
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ulrich Kerzel (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 IUBH**
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	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 Winter
   - 1.3 Notable Advances in AI
2. Expert Systems
   - 2.1 Overview Over Expert Systems
   - 2.2 Introduction to Prolog
3. Neuroscience
   - 3.1 The (Human) Brain
   - 3.2 Cognitive Processes

4. Modern AI Systems
   - 4.1 Recent Developments in Hard- and Software
   - 4.2 Narrow vs General AI
   - 4.3 NLP and Computer Vision

5. AI Application Areas
   - 5.1 Autonomous Vehicles & Mobility
   - 5.2 Personalized Medicine
   - 5.3 FinTech
   - 5.4 Retail & Industry

Literature

Compulsory Reading

Further Reading

- Bear, F., Barry, W., & Paradiso, M. (2006). Neuroscience: Exploring the brain (3rd ed.). Baltimore, MD: Lippincott Williams and Wilkins.
- Bratko, I. (2011). Prolog programming for artificial intelligence (4th ed.). Hoboken, NJ: Pearson.
- Jackson, P. (1998). Introduction to expert systems (3rd ed.). Chicago, IL: Addison Wesley Longman.
- Nilsson, N. (2009). The quest for artificial intelligence. Cambridge: Cambridge University Press.
- Russel, S., & Norvig, P. (2009). Artificial intelligence: A modern approach (3rd ed.). Malaysia: Pearson.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: AI and Society

Course Code: DLMAISAIS01

Study Level	Language of Instruction	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 ▪ Boddington, P. (2017): Towards a code of ethics for artificial intelligence. Springer International Publishing, New York, NY. ▪ Bostrom, N. (2016): Superintelligence: Paths, dangers, strategies. Oxford University Press, Oxford. ▪ Tegmark, M. (2018): Life 3.0: Being human in the age of artificial intelligence. Penguin, New York, NY. ▪ Wachter-Boettcher, S. (2017): Technically wrong: Sexist apps, biased algorithms, and other threats of toxic tech. W. W. Norton & Company, New York, NY.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

4. Semester

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
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 "Fernstudium": Masterarbeit (90) Colloquium • Study Format "Fernstudium": Presentation: 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 IUBH
This module is similar to other modules in the field(s) of Methods.	All Master Programmes in the Business & Management field(s).

Master Thesis

Course Code: MMTHE01

Study Level	Language of Instruction	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 ▪ Hunziker, A. W. (2010): Fun at scientific work. This is how you write a good semester, bachelor or master thesis. 4th edition, SKV, Zurich. ▪ Wehrlin, U. (2010): Scientific work and writing. Guide to the preparation of Bachelor's theses, Master's theses and dissertations - from research to book publication. AVM, Munich. ▪ Selection of literature according to topic

Study Format Fernstudium

Study Format	Course Type
Fernstudium	Thesis-Kurs

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** yes
Type of Exam	Masterarbeit

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
810 h	0 h	0 h	0 h	0 h	810 h

Instructional Methods

- ☐ Learning Sprints®
- ☐ Course Book
- ☐ Vodcast
- ☐ Shortcast
- ☐ Audio
- ☐ Exam Template
- ☐ Review Book
- ☐ Creative Lab
- ☐ Guideline
- ☐ Live Tutorium/Course Feed

Colloquium

Course Code: MMTHE02

Study Level	Language of Instruction	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 edition, Springer Gabler, Wiesbaden.

Study Format Fernstudium

Study Format	Course Type
Fernstudium	Thesis Defense

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** yes
Type of Exam	Presentation: Colloquium

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	0 h	0 h	0 h	90 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	