MODULE HANDBOOK

Master of Science

Master Cyber Security (FS-MACSE-60)

60 ECTS

Distance Learning

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

Contents

2021-11-01

1. Semester

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	

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. Jesus Luna Garcia (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

Programming with Python

Module Code: DLMDSPWP

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.-Ing. Reza Shahbazfar (Programming with Python)

Contributing Courses to Module

- Programming with Python (DLMDSPWP01)

Module Exam Type

Module Exam	Split Exam
Study Format: Fernstudium Written Assessment: Written Assignment	

Weight of Module

see curriculum

Module Contents

- Introduction to the Python programming language
- Object-oriented concepts in Python
- Handling of exceptions and errors
- The Python library ecosystem
- Environments and package management
- Documentation and testing
- Version control

Learning Outcomes

Programming with Python

On successful completion, students will be able to

- remember basic Python syntax and programming concepts.
- understand object-oriented concepts in Python.
- analyze and apply different methods for error handling in Python.
- know common and important Python libraries and how to apply them to given programming tasks.
- understand concepts like environments and version control.

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.

Programming with Python

Course Code: DLMDSPWP01

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

Course Description

Python is one of the most versatile and widely used scripting languages. Its clean and uncluttered syntax as well as its straightforward design greatly contribute to this success and make it an ideal language for programming education. Its application ranges from web development to scientific computing. Especially in the fields of data science and artificial intelligence, it is the most common programming language supported by all major data-handling and analytical frameworks. This course provides a thorough introduction to the language and its main features, as well as insights into the rationale and application of important adjacent concepts such as environments, testing, and version control.

Course Outcomes

On successful completion, students will be able to

- remember basic Python syntax and programming concepts.
- understand object-oriented concepts in Python.
- analyze and apply different methods for error handling in Python.
- know common and important Python libraries and how to apply them to given programming tasks.
- understand concepts like environments and version control.

Contents

1. Introduction to Python
   - 1.1 Data structures
   - 1.2 Functions
   - 1.3 Flow control
   - 1.4 Input / Output
   - 1.5 Modules & packages
2. Classes and inheritance
   - 2.1 Scopes and namespaces
   - 2.2 Classes and inheritance
   - 2.3 Iterators and generators

3. Errors and exceptions
   - 3.1 Syntax errors
   - 3.2 Handling and raising exceptions
   - 3.3 User-defined exceptions

4. Important libraries
   - 4.1 Standard Python library
   - 4.2 Scientific calculations
   - 4.3 Speeding up Python
   - 4.4 Visualization
   - 4.5 Accessing databases

5. Working with Python
   - 5.1 Virtual environments
   - 5.2 Managing packages
   - 5.3 Unit and integration testing
   - 5.4 Documenting code

6. Version control
   - 6.1 Introduction to version control
   - 6.2 Version control with GIT

Literature

Compulsory Reading

Further Reading

- Beazley, D., & Jones, B. K. (2013). Python cookbook (3rd ed.). Sebastopol, CA: O'Reilly Publishing.
- Barry, P. (2016). Head first Python: A brain-friendly guide (2nd ed.). Sebastopol, CA: O'Reilly Publishing.
- Lutz, M. (2013). Learning Python. Sebastopol, CA: O'Reilly Publishing.
- Ramalho, L. (2015). Fluent Python: Clear, concise, and effective programming. Sebastopol, CA: O'Reilly Publishing.
- McKinney, W. (2017). Python for data analysis (2nd ed.). Sebastopol, CA: O'Reilly Publishing.

Study Format Fernstudium

Study Format	Course Type
Fernstudium	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** no **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	

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

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. (2016): The practice of social research. 14th ed., Cengage Learning, Boston, MA.
- Camargo, F. R./Henson, B. (2015): Beyond usability: Designing for consumers' product experience using the Rasch model. In: Journal of Engineering Design, 26(4–6), p. 121–139.
- Olson, L. E. (2014): Articulating a role for program evaluation in responsible conduct of research programs. In: Accountability in Research, 21(1), p. 26–33.
- Tumele, S. (2015): Case study research. In: International Journal of Sales, Retailing and Marketing, 4(9), p. 68–78.
- Tursch, P./Steinberg, F./Woll, R. (2014): A first step towards engineer-oriented adaptation of the Repetory Grid Technique. In: Total Quality Management & Business Excellence, 25(7-8), p. 734–749.
- Zickar, M. J. (2012): A review of recent advances in item response theory. In: Research in Personnel and Human Resources Management, 31, p. 145–176.

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	

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

2. 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	

IT Service and Architecture Management

Module Code: DLMCSEEITSAM

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. Inga Schlömer (IT Architecture Management) / Prof. Dr. André Köhler (IT Service Management)

Contributing Courses to Module

- IT Architecture Management (DLMBITPAM02)
- IT Service Management (DLMBITGSM01)

Module Exam Type

Module Exam	Split Exam
	IT Architecture Management • Study Format "Distance Learning": Written Assessment: Case Study IT Service Management • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

IT Architecture Management

- Architecture documentation
- Architecture governance
- Enterprise architecture management (EAM)
- IT application portfolio management
- Enterprise architecture patterns
- Architecture framework: TOGAF

IT Service Management

- IT infrastructure library (ITIL)
- ITIL service strategy
- ITIL service design
- ITIL service transition
- ITIL service operation

Learning Outcomes

IT Architecture Management

On successful completion, students will be able to

- understand that having a well-defined IT architecture blueprint in place is key to success for IT organizations.
- analyze the constraints of existing application, infrastructure and information/ data architectures.
- know different types of IT application portfolio management.
- manage enterprise architecture patterns proactively.
- understand how to initiate change requests in order to modify or extend the IT architecture if the introduction or modification of a service is not possible within a given framework.

IT Service Management

On successful completion, students will be able to

- understand IT service management as the enabler of information technology strategies and operations objectives.
- define the touchpoints between IT service management and management information systems.
- differentiate between lightweight and heavyweight approaches to IT service management.
- understand benchmarks and assessments to measure the capability of a service provider and its IT service management competences.
- apply IT services management tools and platforms proactively based on current information technology research and advisory.

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 Computer Science & Software Development	All Master Programmes in the IT & Technology field(s)

IT Architecture Management

Course Code: DLMBITPAM02

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

Course Description

The course IT Architecture Management aims to enable students to define a blueprint for the future development of a particular IT landscape, taking into account service strategies and available technologies given to an IT service provider.

Course Outcomes

On successful completion, students will be able to

- understand that having a well-defined IT architecture blueprint in place is key to success for IT organizations.
- analyze the constraints of existing application, infrastructure and information/ data architectures.
- know different types of IT application portfolio management.
- manage enterprise architecture patterns proactively.
- understand how to initiate change requests in order to modify or extend the IT architecture if the introduction or modification of a service is not possible within a given framework.

Contents

1. Introduction to IT Architectures
   - 1.1 The Term “Architecture” in the Context of IT
   - 1.2 Use Cases and Levels of IT Architectures
   - 1.3 Overview on IT Architecture Management
2. Enterprise Architecture Management (EAM)
   - 2.1 IT-Strategy
   - 2.2 Enterprise Architecture
   - 2.3 Roles and Activities in EAM
3. IT Application Portfolio Management
   - 3.1 Application Handbook
   - 3.2 Portfolio Analyses
   - 3.3 Planning the Application Landscape

4. Architecture Framework: TOGAF
   - 4.1 Purpose and Overview on TOGAF
   - 4.2 Architecture Development Method (ADM)
   - 4.3 Guidelines & Techniques
   - 4.4 Architecture Content Framework
   - 4.5 Architecture Capability Framework

5. Architecture Documentation
   - 5.1 Structures, Components, and Interfaces
   - 5.2 Processes and Applications
   - 5.3 Domain Architecture

6. Architecture Governance
   - 6.1 Roles and Committees
   - 6.2 Processes and Decisions
   - 6.3 Management of Architectural Policies

7. Enterprise Architecture Patterns
   - 7.1 Structures, Components, and Interfaces
   - 7.2 Processes and Applications
   - 7.3 Domain Architecture

Literature

Compulsory Reading

Further Reading

- Hanschke, I. (2009): Strategic IT management: A toolkit for enterprise architecture management. Springer, Berlin, Heidelberg.
- Ross, J. W. / Weill, P. / Robertson, D. C. (2006): Enterprise architecture as strategy: Creating a foundation for business execution. Harvard Business School Publishing, Boston, MA.
- Thabit, I. (2011): Architecture management body of knowledge: AMBOK guide for information technology. IT Architecture Management Institute.
- The Open Group Architecture Framework. (2018): TOGAF 9.2. Retrieved from www.theopengroup.org.

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	

IT Service Management

Course Code: DLMBITGSM01

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

Course Description

This course focuses on the nature and practice of IT services that keep IT systems running. It introduces students to the knowledge and experience needed to provide IT as a service to organizations, mainly based on the IT Infrastructure Library (ITIL) which is the industry standard for this purpose.

Course Outcomes

On successful completion, students will be able to

- understand IT service management as the enabler of information technology strategies and operations objectives.
- define the touchpoints between IT service management and management information systems.
- differentiate between lightweight and heavyweight approaches to IT service management.
- understand benchmarks and assessments to measure the capability of a service provider and its IT service management competences.
- apply IT services management tools and platforms proactively based on current information technology research and advisory.

Contents

1. Introduction to IT Service Management
   - 1.1 IT Services, Business IT Services
   - 1.2 Service Level Agreement (SLA)
   - 1.3 IT Service Management
   - 1.4 Reference Models for IT Service Management
2. IT Infrastructure Library (ITIL)
   - 2.1 Purpose and content of the IT Infrastructure Library
   - 2.2 Service Live Cycle in ITIL
   - 2.3 Overview on Service Strategy and Operational Processes
   - 2.4 Continual Service Improvement

3. ITIL – Service Strategy
   - 3.1 Business Relationship Management
   - 3.2 Service Portfolio Management
   - 3.3 Financial Management for Services
   - 3.4 Demand Management

4. ITIL – Operational Processes: Service Design
   - 4.1 Service Level Management
   - 4.2 Service Catalogue Management
   - 4.3 Availability Management
   - 4.4 Service Continuity Management

5. ITIL – Operational Processes: Service Transition
   - 5.1 Transition Planning and Support
   - 5.2 Change Management
   - 5.3 Service Asset and Configuration Management
   - 5.4 Release and Deployment Management

6. ITIL – Operational Processes: Service Operation
   - 6.1 Incident Management
   - 6.2 Problem Management
   - 6.3 Request Fulfilment
   - 6.4 Event Management

Literature

Compulsory Reading

Further Reading

- Orand, B. (2011). Foundations of IT service management with ITIL 2011: ITIL foundations course in a book. Create Space Independent Publishing Platform.
- Sturm, R. (2000). Foundations of service level management (1st ed.). Hoboken, NJ: Sams Publishing.
- van Bon, J. (2007). Foundations of ITIL V3. Reading: Van Haren Publishing.

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. Ulrich Kerzel (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	

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	

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) / Prof. Dr. Ralf Kneuper (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®
- ☑ Course Book
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☐ Exam Template
- ☐ Review Book
- ☐ Creative Lab
- ☑ Guideline
- ☐ Live Tutorium/Course Feed

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	

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

Advanced Cyber Security and Cryptology

Module Code: DLMCSEAITSC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLMCSITSDP01 or DLMCSITSDS01 ▪ DLMCSEAITSC01; DLMCSITSDP01 or DLMCSITSDS01	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. Ralf Kneuper (Seminar: Advanced Cyber Security) / Prof. Dr. Ralf Kneuper (Cryptology)

Contributing Courses to Module

- Seminar: Advanced Cyber Security (DLMCSEAITSC01)
- Cryptology (DLMCSEAITSC02)

Module Exam Type

Module Exam	Split Exam
	Seminar: Advanced Cyber Security • Study Format "Distance Learning": Written Assessment: Research Essay Cryptology • Study Format "Distance Learning": Oral Assignment

Weight of Module

see curriculum

Module Contents

Seminar: Advanced Cyber Security

- 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.

Cryptology

- Symmetric and asymmetric cryptosystems
- Authentication
- Cryptanalysis
- Cryptology in the internet
- Applications

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.

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

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

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	

Master Thesis

Module Code: DLMMTHES

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	See current study and exam regulations (SPO)	MA	15	450 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 (DLMMTHES01)
- Colloquium (DLMMTHES02)

Module Exam Type

Module Exam	Split Exam
	Master Thesis • Study Format "Fernstudium": Written Assessment: Master Thesis (90) Colloquium • Study Format "Fernstudium": Presentation: Colloquium (10)

Weight of Module

see curriculum

Module Contents

Master Thesis

- Written Master Thesis

Colloquium

- Thesis Defense

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**
All modules in the master program	All Master Programmes

Master Thesis

Course Code: DLMMTHES01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		13.5	See current study and exam regulations (SPO)

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

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

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
405 h	0 h	0 h	0 h	0 h	405 h

Instructional Methods

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

Colloquium

Course Code: DLMMTHES02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		1.5	See current study and exam regulations (SPO)

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:** no
Type of Exam	Presentation: Colloquium

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
45 h	0 h	0 h	0 h	0 h	45 h

Instructional Methods

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