DEGGENDORF INSTITUTE OF TECHNOLOGY

Module Handbook
B.Sc. Cyber Security

Faculty of Computer Science
Examination regulations 01 October 2022
as of: 30 Nov 2022 13:27:00

Table of Contents

CY-B-01 Mathematics 1
CY-B-02 Programming 1
CY-B-03 Basics of Computer Science
CY-B-04 Operating Systems and Networks
CY-B-05 Basics of Information Security
CY-B-06 Key Qualification 1
CY-B-07 Mathematics 2
CY-B-08 Programming 2
CY-B-09 Algorithms and Data Structures
CY-B-10 Internet Technologies
CY-B-11 Cryptology 1
CY-B-12 Key Qualification 2
CY-B-13 Databases
CY-B-14 Stochastics
CY-B-15 Project Management
CY-B-16 Secure Programming
CY-B-17 Network Security
CY-B-18 Key Qualification 3
CY-B-19 Software Engineering
CY-B-20 Compulsory Elective Module: Project
CY-B-21 Cryptology 2
CY-B-22 Management of IT Security
CY-B-23 Distributed Ledger Technologies
CY-B-24 Key Qualification 4
CY-B-25 Practical Module
CY-B-26 Penetration Testing
CY-B-27 Digital Forensics
CY-B-28 Security of Interactive Systems
CY-B-29 Security Engineering
CY-B-30 Compulsory Elective Module 1
CY-B-31 Key Qualification 5

CY-B-32 Auditing of IT Systems

CY-B-33 Compulsory Elective Module 2

CY-B-34 Compulsory Elective Module 3

CY-B-35 Bachelor’s module

CY-B-01 Mathematics 1

Module no.	CY-B-01
Module coordinator	Prof. Dr. Thorsten Matje
Course number and name	Mathematics 1
Lecturers	Prof. Dr. Thorsten Matje
Semester	1
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students will acquire the basic mathematical knowledge of analysis, linear algebra, fuzzy mathematics and number theory that is required for bachelor's degree programme in Cyber Security. Students will acquire formal and mathematical skills so that they will be able to formally describe problems. They will be able to successfully apply their mathematical knowledge to solve formal tasks. Students will also be in a position to use the appropriate mathematical tools, such as a computer algebra system or a spreadsheet programme, to solve the tasks. They will learn cooperation skills through group work.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students will have a basic knowledge of mathematical modelling in the field of cyber security.

Methods expertise

- Students will have an in-depth knowledge of mathematical methods for working on practical tasks (dealing with complex relationships using matrices, linear systems of equations, functions of (several) variables as a basis for understanding models).

Personal skills

- Students will be capable of in-depth independent time management and self-study since they will have worked on approx. 50% of the material through virtual teaching.

Social skills

- Students will have an insight into solving problems through group work and team work.

Applicability in this and other degree programmes

This module is the foundation for the module CY-B-07 Mathematics 2. The module contents are dealt with in other modules of the programme.

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Mathematical and abstract faculty of thought

Content

1 Basic knowledge of mathematics
  - Logic and Boolean algebra, as well as inductive proof
  - Set theory and relations
  - Number ranges and arithmetic
  - Sequences and series
  - Mapping/function

2 Linear and non-linear functions and their properties
3 Differentiation (differentiation rules, higher order derivatives, curve sketching)
4 Basics of integral calculus
   - The Riemann integral
   - Integration rules (partial integration, substitution rules, partial fraction expansion)
5 Differential calculus for functions with several independent variables
   - Linear and non-linear functions with several independent variables
   - Partial derivatives
   - Hessian matrix and determination of extrema
   - Determination of extrema under constraints (Lagrange)
6 Linear algebra and matrix calculus
   - Vector spaces, basis and linear systems of equations
   - Linear mapping and invertible matrices
   - Gaussian algorithm for solving linear systems of equations
   - Determinants
7 Fuzzy mathematics
   - Fuzzy sets and their operations
   - Fuzzy numbers and fuzzy relations
   - Linguistic variables and fuzzy rules
   - Fuzzy multi-criteria analysis
8 Introduction to graph theory

Teaching and learning methods

- Lecture and exercises
- Tutorials along with lecture
- Collaborative learning with e-learning
- Students receive a list of which sub-chapters they have to prepare virtually by which classroom session date.

Remarks

By the end of the second semester, students must have taken the examination for this module for the first time.

Recommended reading

- Auer, Benjamin, Seitz, Franz, Grundkurs Wirtschaftsmathematik. 2nd edition Gabler, Wiesbaden, 2009

- Bauer, Ch., Clausen, M., Kerber, A., Meier-Reinhold, H., Mathematik für Wirtschaftswissenschaftler, Schäffer-Poeschel, 5th revised edition, 2008
- Bradley, Teresa, Patton, Paul, Essential Mathematics for Economics and Business, John Wiley & Sons, 1998
- Holland, Heinrich, Holland, Doris, Mathematik im Betrieb, 7th Ed., Gabler Verlag, Wiesbaden, 2004
- Jenks, R. D., Sutor, R. S., AXIOM -- The Scientific Computation System, Springer Verlag, Heidelberg, 1992
- Ohse, Dietrich, Mathematik für Wirtschaftswissenschaftler II, Lineare Wirtschaftsalgebra, 4th Ed. Verlag Vahlen, 2000
- Pfuff, Franz, Mathematik für Wirtschaftswissenschaftler kompakt, 3rd Ed., Vieweg+Teubner Verlag, Braunschweig, 2009
- Popp, Heribert: Anwendungen der Fuzzy-set-Theorie in Industrie- und Handelsbetrieben, Wirtschaftsinformatik, 1994
- Tilli, T. A: Fuzzy-Logik, 2nd edition, Francis 1992

CY-B-02 Programming 1

Module no.	CY-B-02
Module coordinator	Prof. Dr. Marcus Barkowsky
Course number and name	Programming 1
Lecturers	Prof. Dr. Marcus Barkowsky
Semester	1
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Assignment, written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students have a basic general and technical knowledge of programming. The focus is still on imperative programming, but initial object-oriented concepts are also taught. Students can apply their knowledge in practice and solve simple to moderately difficult problems.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students will understand the concepts of modular software design.
- Students will be able to implement their own simple software-technical ideas.
-

Methods expertise

- Students will have the ability to create programmes using a modern object-oriented programming platform.

Personal skills

- Students will be able to implement their own simple software-technical ideas and defend them against competing approaches.

Social skills

- Programming exercises are given during the course. Students can thus understand and criticise the content of the programmes of fellow students, and complement them with their own programmes. They can create programmes in a form that allows cooperation in a team.

Applicability in this and other degree programmes

Basic introduction to programming

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Abstract faculty of thought

Content

Outline:
Part 1: C++ for beginners (static)

1 Introduction to object-oriented programming: C++

2 Basic syntax in C++

3 Control structures

4 Fields and strings

5 Paradigms of object orientation (OO)

6 The class concept in C++

7 Sample application: ACCOUNT MANAGEMENT

8 Special class properties and methods

9 Inheritance

Part 2: C++ for advanced learners (dynamic)

1 File processing & error handling

2 References and pointers

3 Using objects

4 Memory reservation at runtime

5 Linked lists

6 Classes

Possible additional performance:

7 Operator overloading

8 Templates

Teaching and learning methods

- Flipped classroom with corresponding VHB course

Remarks

By the end of the second semester, students must have taken the examination for this module for the first time.

Recommended reading

- Notes
- Kernighan, Richie: The C programming language, Prentice Hall, 2000
- Stroustrup: The C++ programming language, Addison-Wesley Professional, 2013

CY-B-03 Basics of Computer Science

Module no.	CY-B-03
Module coordinator	Prof. Dr. Thomas Störtkuhl
Course number and name	Basics of Computer Science
Lecturers	Prof. Dr. Thomas Störtkuhl
Semester	1
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Assignment, written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students have a basic general and technical knowledge in the field of computer science.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Knowledge and understanding of the essential basics of computer science, its concepts and methods

- Professional competence to understand these basics independently and to apply them to examples

Methods expertise

- Students can carry out formal proofs in writing using suitable software
- They can formally describe the syntax of symbolic expressions
- They can implement regular expressions with finite automata
- They can develop digital circuits

Personal skills

- Students can formulate logically sound arguments independently
- Students can find gaps in incorrect arguments
- They can recognise the advantages and disadvantages of digitisation

Applicability in this and other degree programmes

This module is the basis for other subjects in the field of computer science. It can be used in other computer science programmes.

Admission requirements and/or recommended prerequisites

No prerequisites.

Content

- Basics of theoretical computer science
  - Logic
  - Computability
  - Finite automata
  - Formal languages
  - Complexity theory
- Basics of technical computer science:
  - Combinational circuits and control mechanisms
  - Computer architecture
  - Memory organisation
  - Internet technology

Teaching and learning methods

- Seminar-based lesson

- For every topic, corresponding software tools are introduced and used for exercises.
- Proof of performance using software tools

Recommended reading

- Jon Barwise and John Etchemendy: Sprache, Beweis und Logik, Volume I, Mentis 2005
- Susan H. Rodger and Thomas W. Finley: JFLAP: An Interactive Formal Languages and Automata Package, online at http://jflap.org/
- Erich Hehner: Digital Circuit Design, lecture notes online at http://www.cs.toronto.edu/~hehner/DCD/DCD.pdf
- J. Glenn Brookshear and Dennis Brylow: Computer Science--An Overview, 12th edition, Pearson, 2015

CY-B-04 Operating Systems and Networks

Module no.	CY-B-04
Module coordinator	Prof. Dr. Andreas Wölfl
Course number and name	Operating Systems and Networks
Lecturers	Prof. Dr. Peter Faber Prof. Dr. Andreas Wölfl
Semester	1
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Operating systems

Students will gain insight into the importance of operating systems as the central basis for information processing in companies. They will develop an understanding of the current manifestations of operating systems. After completing the Operating Systems sub-module, students will have achieved the following learning objectives:

- They will learn the concepts and technologies necessary for developing operating systems, and gain knowledge about the modular structure and functioning of operating systems.
- Students will acquire knowledge and skills required for the configuration, administration and secure application of operating systems on the basis of commercial operating systems.
- They will be able to organise and evaluate the modern operating forms of data centres, such as virtualisation or cloud computing, in the context of operating systems.
- They will get an insight into the theoretical basics of a Linux system and an overview of the most important shell commands.
- Students will be able to install and administer a Linux server.

Networks

- Students will understand the meaning of multi-layer models and the tasks and functions of the layers of the ISO/OSI model and will be able to explain the most important service representatives of each layer.
- Students will be able to reproduce the concepts of application protocols such as HTTP and SMTP and understand how they work, for example, using sequence diagrams.
- Students will be able to program simple Internet applications using sockets.
- They will be able to analyse and diagnose network problems using suitable tools.

Applicability in this and other degree programmes

This module is the basis for other subjects in the field of computer science.

Admission requirements and/or recommended prerequisites

No prerequisites.

Content

- Rights management (authentication, authorisation)
- Processes & threads, inter-process communication
- Deadlocks, Mutex process
- Peripherals/input/output
- Operating system API, user space/kernel space
- Use of Linux/Unix/POSIX

- Use of shells – graphical and text-based (particularly practical use of the command line)
- Use of system virtualisation (e.g.: Hypervisors, VirtualBox, XEN, Docker, ...)
- Use of system calls
- Multi-layer model: OSI
- Network topologies (bus, tree, star, partially/fully meshed)
- Application layer: HTTP, SMTP & IMAP, DNS
- Transport layer: sockets, UDP, TCP
- View of the network layer: IPv4/v6
- Use of tools and techniques for network analysis and configuration (e.g., Ping, Traceroute, PuTTY/telnet, nslookup, ...)
- Use of browser debugging tools (network consoles, ...)
- Understanding and implementing text-based application protocols (e.g., HTTP interactions)

Teaching and learning methods

Seminar-based lesson along with practical exercises

Recommended reading

- Andrew S. Tanenbaum, Herbert Bos; Modern Operating Systems; Prentice Hall, 4th ed., 2014
- Evi Nemeth, Garth Snyder, Trent R. Hein et al.; Unix and Linux System Administration Handbook, Addison-Wesley, 5th ed., 2018
- Micha Gorelick & Ian Ozsvald; High Performance Python; O'Reilly, 2014
- James F. Kurose, Keith F. Ross; Computer Networking: A Top-Down Approach; Pearson, 7th ed., 2017
- Andrew S. Tanenbaum, David J. Wetherall; Computer Networks; Pearson, 5th ed., 2014

CY-B-05 Basics of Information Security

Module no.	CY-B-05
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Fundamentals of Information Security
Lecturers	Amar Almaini
Semester	1
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students have a basic general and technical knowledge in the field of information security.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students can define and explain the common concepts of information security.

- They can describe the basic protection goals of information security.
- Students can differentiate between the different risks, classify them into damage classes, and suggest suitable approaches.
- They can compare different classic encryption and decryption methods and apply them.
- They know how asymmetric cryptography works and can compare common asymmetric cryptographic methods.
- They can summarise the basic principles of cryptographic protocols (key agreement; entity authentication; symmetric encryption; message authentication).
- They can explain the concept of programme security, and, for example, identify a buffer overflow attack in the code.
- They can discuss the basic principles of a secure operating system and explain how memory management works.
- They can define the various firewall types and implement a packet filter as an example.

Methods expertise

- Students can describe the methods of cryptanalysis and apply them to ciphertexts in order to draw conclusions about the original text.

Personal skills

- By participating in group discussions, listening respectfully, and demonstrating interest in the subject, students develop awareness and an increased receptiveness.

Social skills

- Through group work, students develop the ability to work in a team and increase their goal and result orientation.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor’s programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

No specific requirements

Content

1 Introduction, motivation and concepts
2 Protection goals of information security
3 Risks
  - Risk analysis
  - Damage classes
  - Risk matrix
  - Risk treatment
4 Introduction to cryptology
  - Basic classic methods
  - Main features of cryptanalysis
  - Introduction to modern cryptography
5 Introduction to cryptographic communication relationships
6 Basic concepts of programme security
7 Basics of operating system security
8 Basics of network security
9 Vulnerabilities, vulnerability analysis and vulnerability databases
10 Types of hackers and crackers
11 Information security management systems

Teaching and learning methods

- Seminar-based lesson along with practical exercises

Remarks

By the end of the second semester, students must have taken the examination for this module for the first time.

Recommended reading

- Secorvo: Informationssicherheit und Datenschutz, Handbuch für Praktiker und Begleitbuch zum T.I.S.P., dpunkt Verlag, 3rd updated and expanded edition, September 2019, 824 pages, ISBN-13: 978-3864905964

- Hanschke, I.: Informationssicherheit & Datenschutz - einfach & effektiv: Integriertes Managementinstrumentarium systematisch aufbauen und verankern, Carl Hanser Verlag GmbH & Co. KG, ISBN-13: 978-3446458185
- BSI – Federal Office for Information Security: Information Security and IT Baseline Protection, BSI Standards 200-1, 200-2, 200-3 (German) paperback, 9 October 2017, ISBN-13: 978-3846208151
- Sowa, A.: Management der Informationssicherheit: Kontrolle und Optimierung, Springer Vieweg; 1st edition 2017 (16 January 2017), ISBN-13: 978-3658156268
- Weber, K.: Grundlagen und Anwendung von Information Security Awareness: Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren, Springer Vieweg; 1st edition 2019 (10 May 2019), ISBN-13: 978-3658262570
- Eckert, C.: IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Oldenbourg; 10th expanded and updated edition (21st August 2018), ISBN-13: 978-3110551587

CY-B-06 Key Qualification 1

Module no.	CY-B-06
Module coordinator	Prof. Dr. Roland Zink
Course number and name	Business Administration Media Competence and Self-Organisation
Lecturers	Dr. Melanie Hazod Prof. Dr. Thomas Meier Prof. Dr. Roland Zink
Semester	1
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Transitioning from school to university presents many students with challenges right from the start of their studies. It requires them to move away from fixed timetables and curricula and move towards self-reliance and independence. The module Key Qualification 1 is intended to prepare students for these challenges, especially with regard to digitisation and the economic aspect (industrial placementin the 5th semester). The learning outcomes of the module therefore consist of the two subjects

"Business Administration" (Subject A) and "Media Skills and Self Organisation" (Subject B).

Subject A

In Business Administration, students deal Remarks with general business administration, cost and activity accounting, and human resource management. Although students take a technical or IT-oriented course, the business management knowledge they acquire should facilitate their career start. Broadening of the knowledge base of students is intended to prevent them from taking suboptimal decisions in companies.

Professional skills

- Students will obtain an overview of the functional areas of a company and learn selected concepts of corporate governance/strategy development.
- They will know and understand the principles and methods of systematic decision-making.
- Students will understand the purposes of cost and activity accounting and the building of a cost and activity accounting system.
- They will be familiar with the important instruments of cost and activity accounting, cost centre and cost unit accounting, as well as short-term profit and loss statement.
- They will be able to carry out and evaluate cost centre and order related target/actual comparisons.
- They will learn to apply marginal costing in the form of a break-even analysis.
- They will be able to carry out decision accounting on the basis of cost and activity accounting.

Subject B

The digital transformation of society continues to increasingly penetrate our professional and everyday life and is characterised by a rapidly increasing wealth of information.
Students need high media competence to be able to handle and communicate with this wealth of information. The content is based on the media competence grid of the conference of ministers of education of the German states (2016) with its six pillars:

1 Searching, processing and preservation
2 Communication and cooperation
3 Production and presentation

4 Protection and safe operation
5 Problem solving and taking action
6 Analysis and reflection

The skills acquired in school are to be expanded in a targeted manner to meet the challenges of the course. The focus is no longer on searching for and presenting information, but rather on selecting, evaluating and interpreting it, i.e., on its analysis and synthesis. The subject introduces students to the use of digital media in the context of studies, data protection and copyrights, as well as to the independent organisation of studies.

Professional skills

- Students know the various digital media that can be used to organise learning and can use them.
- They will be able to select both analogue and digital teaching and learning content specifically for their studies.
- They can deal with digital media competently and purposefully.
- Students can organise their studies in terms of time and content, and can process the wealth of information in a targeted manner.

Subjects A and B

Methods expertise

- Students are enabled to work transparently and in a structure-oriented and decision-oriented manner with regards to cost and activity accounting.
- They become aware that cost and activity accounting must be designed in a purpose-oriented manner.
- Students are enabled to work independently.
- They acquire skills in dealing with digital media.
- They learn strategies for acquiring knowledge using blended learning methods.

Personal skills

- Through exercises, students learn to work independently and in a manner oriented on problems, solutions and action.

Social skills

- The exercises provide students with practice in partner work and teamwork.

- They learn to work independently.

Applicability in this and other degree programmes

The module lays the foundations for the course in general, and is particularly linked to the following advanced module:

KI-B and CY-B: Key qualification 3

KI-B and CY-B: Key qualification 4

KI-B and CY-B: Practical module

KI-B and CY-B: Bachelor's module

Degree programme: B.A. Cyber Security and B.A. Artificial Intelligence

Admission requirements and/or recommended prerequisites

No prerequisites.

Content

Subject A

- Overview of a company
    - Corporate governance and corporate policy
    - Vision, goals, strategies
    - Constitutive corporate decisions
    - Production factors
    - Operational functions
- Overview of the approaches of the decision theory
- Purposes of cost and activity accounting and cost allocation principles
- Cost and activity accounting systems
- Specific cost accounting content in the areas of AI and CS
- Cost and activity accounting based on full costing
    - Cost-type accounting
    - Cost centre accounting
    - Cost unit accounting
- Cost and activity accounting based on direct costing (break-even analysis)
- Short-term profit and loss statement
- Decision-oriented cost and activity accounting including the principle of relevant costs

Subject B

- Information, data and knowledge
- Self-organisation and organisation of studies
- Digital media in the context of student learning
- Digital media in science and communication
- Data protection and netiquette
- Copyrights and rights of use
- Media use and pillars of media competence

Teaching and learning methods

- Seminar-based lesson with group work and partner work
- Project work
- Blended learning

Recommended reading

Subject A

- Däumler K., Grabe J. (2013): Kostenrechnung 1 - Grundlagen, 11th edition, NWB-Verlag, Herne.
- Dörsam, P. (2013): Grundlagen der Entscheidungstheorie anschaulich dargestellt, 6th edition, PD-Verlag, Heidenau.
- Friedl G., Hofmann Ch., Pedell B. (2017): Kostenrechnung: Eine entscheidungsorientierte Einführung, 3rd edition, Vahlen Verlag, Munich.
- Jorasz W., Baltzer B. (2019): Grundlagen der Kosten- und Leistungsrechnung: Lehrbuch mit Aufgaben und Lösungen, Schäffer-Poeschel Verlag, Stuttgart.
- Wöhe, G. (2016), Einführung in die allgemeine Betriebswirtschaftslehre, 26th edition, Vahlen, Munich.

Subject B

- Bänisch, A. & Alewell, D. (2013): Wissenschaftliches Arbeiten. De Gruyter Oldenbourg.
- Gapski, H., Oberle, M. & Staufer, W. (2017): Medienkompetenz. Herausforderung für Politik, politische Bildung und Medienbildung. Bonn.

- Bühler, P. & Schlaich, P. (2016): Medienkompetenz. Digitale Medien verstehen - erstellen - einsetzen.
- (Internet documents and guides are also used.)

CY-B-07 Mathematics 2

Module no.	CY-B-07
Module coordinator	Prof. Dr. Thorsten Matje
Course number and name	Mathematics 2
Lecturers	Prof. Dr. Thorsten Matje Prof. Dr. Simon Zabler
Semester	2
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students will acquire an in-depth knowledge of mathematical topics that are important for application in computer science and in mathematical fields or for artificial intelligence or cyber security applications or that are necessary for perfecting the basic concepts of mathematics. The focus will also be on mathematical thinking, working and modelling methods.

Students will be able to recognise, model and solve mathematical problems from the fields of computer science, Remarks, artificial intelligence or cyber security.

For this, they will be in a position to use a computer algebra system for mathematical modelling and calculations. The associated algorithmic methods of mathematics will be developed using examples. Students will be able to successfully complete advanced courses associated with mathematical modelling.

The main focus is on professional skills and methods expertise in the subject areas handled.

Naturally, the acquisition of social skills is not the main focus of this module but is fostered through the cooperation of students and by developing solutions together.

Personal skills are fostered by in-depth, independent elaboration and solving of complex problems. By applying mathematical solution techniques and their critical penetration, students will develop the ability of abstract and analytical thinking.

Applicability in this and other degree programmes

Students will be able to successfully complete advanced courses associated with mathematical modelling.

The module can also be used for master's programmes that offer additional training, that are consecutive, and that are supportive.

Admission requirements and/or recommended prerequisites

Recommended:

- Content of the module Mathematics 1

Content

1 Analytical geometry and eigenvalues
   - Scalar products, angles, distance, norm (if not already covered in Mathematics 1)
   - Affine vector spaces (if not already covered in Mathematics 1)
   - Eigenvalues and eigenvectors
2 Quadrics and Bézier curves
   - Quadrics as solution sets of quadratic equations
   - Bézier curves
3 Selected chapters of discrete mathematics
   - Combinatorics
   - Introduction to the graph theory
   - Construction and ranking of discrete objects with trees

4 Mathematical principles of cryptography
   - Number-theoretical basics
   - Applications in the RSA method
   - Finite fields
5 Complex numbers and trigonometric functions
   - Complex numbers
   - Trigonometric functions
   - Circle graduation and fundamental theorem of algebra
6 Linear differential equations (might be omitted)
   - Solution methods for linear differential equations
   - The Bernoulli differential equation
   - Separable differential equations
7 Selected chapters of numerical mathematics
   - Floating-point arithmetic and rounding errors
   - Horner scheme
   - Iteration method for determining zeroes
   - Newton's method in a complex.

Teaching and learning methods

Theory and applications are taught and presented using traditional presentation techniques combined with the direct use of a computer algebra system. Many concepts are developed with the help of specific tasks and solved using a computer algebra system. Exercises are given to students to complete on their own. Solutions to some of these are presented by students at the beginning of the next lecture. Alternatively, solution proposals by students are discussed in the iLearn system.

Collaborative learning with e-learning.

Remarks

One of the four semester hours is offered by the lecturer as an exercise in the computer room in two groups.

Recommended reading

- Bauer, Ch., Clausen, M., Kerber, A., Meier-Reinhold, H., Mathematik für Wirtschaftswissenschaftler, Schäffer-Poeschel, 5th revised edition, 2008
- Buchmann, J., Einführung in die Kryptographie, 4th expanded edition, Springer- Verlag, Heidelberg, 2008
- Fischer, G., Analytische Geometrie, Vieweg+Teubner, 7th, revised Ed., 2001

- Gathen von zur, J., Gerhard, J., Modern Computer Algebra, Cambridge-University Press, 1999
- Hämmerlin, G., Hoffmann, K.-H., Numerische Mathematik, 4th edition, Springer-Verlag, Berlin, 1994
- Jenks, R. D., Sutor, R. S., AXIOM -- The Scientific Computation System, Springer Verlag, Heidelberg, 1992
- Walter, W., Gewöhnliche Differentialgleichungen, 7th revised and extended Ed., Springer-Verlag, Berlin, 2000

CY-B-08 Programming 2

Module no.	CY-B-08
Module coordinator	Prof. Dr. Andreas Wölfl
Course number and name	Programming 2
Lecturers	Prof. Dr. Andreas Wölfl
Semester	2
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Assignment, written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

This module aims to teach students advanced programming concepts, modelling methods, various programming paradigms, and different tools. Students gain a more solid foundation for designing and implementing software. They also learn how to use professional software tools. This will enable them to write high-quality software in teams.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students will understand the concepts of professional software development.
- Students will be able to implement their own software-technical ideas.

Methods expertise

- Students will have the ability to create high-quality programmes using modern tools.

Personal skills

- Students will be able to implement their own software-technical ideas and defend them against competing approaches.

Social skills

- Programming exercises are given during the course. Students can thus also understand, criticise and complement the programmes of other students.

Applicability in this and other degree programmes

Among others:

- Software Engineering
- Secure Programming
- Penetration Testing

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Content of the first semester, particularly Programming 1
- Basics of Mathematics

Content

- Introduction: repetition of basic programming concepts, introduction to Python
- Tools: IDEs, interactive environments, Jupyter notebooks, revision control, debugger, timing of code, profiler, Cython, logger, work packet tracker, bug tracker, build chains

- Code conventions: Style guides, clean code
- Modelling: use case diagrams, activity diagrams, class diagrams, object diagrams
- OOP: decorators, refactoring, design patterns
- Tests: unit tests, test-driven development, test coverage
- Memory management: stack and heap, manual release of memory, garbage collection, interning
- Exception handling: raising and catching, asserts
- Files: reading and writing, deleting, serialisation, JSON, pickle, tabular data
- Multithreading: parallelism and concurrency, creation of threads, Global Interpreter Lock (GIL)
- Logic programming: logic, declarative programming, Prolog

Teaching and learning methods

- Lectures
- Discussion of academic articles and current news
- Exercises, including computer exercises

Recommended reading

- S. Chacon and B. Straub, "Pro Git", Apress, 2nd edition, 2014.
- M. Goodrich et al., "Data Structures and Algorithms in Python", John Wiley & Sons, 2013.
- C. Larman, "Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development", 3rd edition, Prentice Hall, 2004.
- E. Matthes, "Python Crash Course: A Hands-On, Project-Based Introduction to Programming", 2nd edition, 2019.

CY-B-09 Algorithms and Data Structures

Module no.	CY-B-09
Module coordinator	Prof. Dr. Patrick Glauner
Course number and name	Algorithms and data structures
Lecturers	Prof. Dr. Patrick Glauner
Semester	2
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Assignment, written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

The aim of this module is to introduce students to two of the most important fundamentals of a computer science course: algorithms and data structures. A data structure enables a programmer to structure data in conceptually manageable relationships. An algorithm is a finite sequence of well-defined, computer-implementable instructions to solve a class of problems or to perform a calculation. Algorithms often work with data structures. This course takes students on a journey through computer science. Students will acquire a solid foundation in how the main algorithms and data structures work. They will also learn how to design efficient algorithms and data structures.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students will understand the concepts of the most common algorithms and data structures.
- They will be able to implement their own algorithms and data structures.

Methods expertise

- Students will have the ability to create high-quality programmes using algorithms and data structures.

Personal skills

- Students will be able to defend their own algorithms and data structures against competing approaches.

Social skills

- Programming exercises are given during the course.
  Students can thus also understand, criticise and complement the algorithms and data structures of other students.

Applicability in this and other degree programmes

Among others:

- Software Engineering
- Secure Programming

Admission requirements and/or recommended prerequisites

- Content of the first semester, particularly Programming 1
- Basics of Mathematics

Content

- Introduction: definition and classification of algorithms
- Graphs: graph definitions, applications in computer science, shortest path, lowest cost, A*
- Complexity analysis: time complexity, O, Omega, Theta, o and O tilde calculus, storage complexity

- Lists: arrays, dynamic arrays/lists, basic operations, stacks, queues, linked lists
- Recursion: search, divide and conquer, recurrence equations, master theorem, backtracking, dynamic programming
- Sorting: bubble sort, selection sort, insertion sort, merge sort, quicksort, lower bounds
- Trees: binary trees, traversal, advanced types of trees, decision trees
- Maps and hash tables: key-value memory, hashing, collision handling
- Selected algorithms: quick matrix multiplication, string matching, prime numbers
- Quantum computing: qubits, quantum gates, quantum computer, quantum algorithms

Teaching and learning methods

- Lectures
- Discussion of academic articles and current news
- Exercises, including computer exercises

Recommended reading

- M. Goodrich et al., "Data Structures and Algorithms in Python", John Wiley & Sons, 2013.
- R. Sedgewick, "Algorithms", Addison Wesley, 4th edition, 2011.
- M. Sipser, "Introduction to the Theory of Computation", Cengage Learning, 3rd edition, 2012.

CY-B-10 Internet Technologies

Module no.	CY-B-10
Module coordinator	Prof. Dr. Goetz Winterfeldt
Course number and name	Internet Technologies
Lecturers	Prof. Dr. Goetz Winterfeldt
Semester	2
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Portfolio
Weight of the grade	5/210
Language of instruction	German

Module objectives

Professional skills

Students will learn about technologies that they can use for designing interactive Internet applications. They will be able to use them efficiently in the implementation of projects.

Students will be able to design websites. They will know how to structure pages and they will know basic languages for designing websites (CSS, HTML, Java Script). They will write small Java Script programmes. In the project, they will set up a node.js infrastructure, integrate a socket server and implement web components to deliver content to the browser.

Methods expertise

Students will use command line tools to connect to servers and exchange data. They use server and client technologies to establish simple communication between systems. They will be able to use integrated development environments.

Social skills

Based on this knowledge, students can execute their own project. They apply their knowledge of web technologies in the process. They evaluate the results of other groups and also have their projects evaluated. In the process, students use standard web programming tools (GIT, Visual Code, Command Line).

Personal skills

After completing the course, students can carry out their own projects and develop Internet (web) applications. The course does not deal with databases and network technologies, as these topics are dealt with in other lectures.

Applicability in this and other degree programmes

This module is suitable for the programmes “Applied Computer Science", "Interactive Systems" and related programmes.

Admission requirements and/or recommended prerequisites

Basics of programming with Java or another object-oriented language. Knowledge from the field of network technologies and databases facilitates project implementation.

Content

The module is made up of two parts:

Part I Internet technologies - basics and Part II Project work - Internet technologies

Content of part 1

(1) Tools and installation

(2) Client-server basics, protocols

(3) Client web technologies

- Html

-CSS

- Java Script
(4) Server technologies
(5) Proprietary applications
- Sockets
- Data formats
- Session management

Content of part 2
Workshop: setup infrastructure - cloud-based services
Project: realisation of a web application

Teaching and learning methods

Lectures, tutorials and small internships, and a final project.

Remarks

The module takes place in two parts. It is necessary that the first part has been completed before starting the second part. Otherwise, important prerequisites would be missing (project work part 2).

Recommended reading

(1) Tutorials and basics of Internet technologies,
https://www.w3schools.com/
(2) Node.js das umfassende Handbuch, Sebastian Springer, 2021, Rheinwerk Computing, ISBN 978-3-8362-8765-4
(3) HTML5 und CCS3 für Einsteiger: Der leichte Weg zur eigenen Webseite, Paul Fuchs, 2019
(4) JQuery 3, Frank Bongers, Rheinwerk Computing, ISBN 978-3-8362-5664-3
(5) Responsive Web Design with HTML5 and CSS: Develop future-proof responsive websites using the latest HTML5 and CSS techniques, 3rd edition, 2020, 978-1839211560

CY-B-11 Cryptology 1

Module no.	CY-B-11
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Cryptology 1
Lecturers	Prof. Dr. Martin Schramm
Semester	2
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Practical task, written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students have a basic general and technical knowledge in the areas of cryptography, cryptanalysis and steganography.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students will be able to present and explain the basic existing protection goals and assets worth protecting.

- They will be able to apply different classic encryption and decryption methods and study them cryptanalytically.
- They will be able to explain existing prime number tests (both deterministic and probabilistic) and implement them to test/generate prime numbers of any length.
- They can explain the common symmetric cryptographic algorithms and can compare the advantages and disadvantages of the operating modes of block ciphers.
- They can describe the basic principles of asymmetric cryptography (encryption, decryption/generation and verification of digital signatures) and common asymmetric cryptographic methods and integrity algorithms.
- They will be able to carry out different attacks on mathematical problem classes in modern cryptography and justify why certain parameters of cryptographic methods were chosen correctly/incorrectly.

Methods expertise

- For a given scenario, students will be able to assess which assets are important and which protection goals must be fulfilled in this context, and select suitable cryptographic mechanisms for this.
- They can compare, differentiate between and contrast advanced cryptographic methods (that have not been dealt with).

Personal skills

- By participating in group discussions, listening respectfully and demonstrating interest in the subject, students develop awareness and an increased receptiveness, and feel satisfaction from actively participating in their own learning.

Social skills

- Through group work in practical experiments, students develop the ability to work in a team and increase their goal and result orientation.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor’s programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Mathematical and abstract faculty of thought
- Knowledge of the basics of elementary number theory

Content

1 Introduction
   - Thematic classification
   - Protection goals and assets
   - Threats, risks and countermeasures
   - Elements of cryptology

2 Classic methods
   - Design principles
   - Transposition methods
   - Substitution methods
   - Analysis of monoalphabetic ciphers
   - Homophonic, polygraphic and polyalphabetic methods
   - Combination of substitution and transposition
   - Transition to modern cryptography

3 Modern methods
   - Mathematical Principles of Modern Cryptography
   - Prime numbers and prime number tests
   - Prime fields and binary extension fields
   - Symmetric ciphers
   - Block ciphers and operating modes
   - Stream ciphers
   - Asymmetric cryptography
   - Hash functions and message authentication codes
   - Digital signatures
   - Digital certificates and public key infrastructures

4 Security of cryptographic methods
   - Perfect and pragmatic security
   - Selected attacks on the DLP
   - Selected attacks on the factoring problem

5 Basics of system and transaction security
   - Measures for data integrity and liability

- Authentication measures I: access control
- Authentication measures II: identification of partners
- Authentication measures III: document authenticity

Teaching and learning methods

- Seminar-based lesson along with practical exercises
- Internships

Remarks

Practical task (PrL) as eligibility criterion for the examination.

Recommended reading

Literature:

- Eckert, C.: IT-Sicherheit, Konzepte - Verfahren - Protokolle, De Gruyter Oldenbourg; 10th expanded and updated edition (21st August 2018), ISBN-13: 978-3110551587
- Schäfer, G.: Netzsicherheit, Algorithmische Grundlagen und Protokolle, dpunkt; 1st edition (1st February 2003), ISBN-13: 978-3898642125
- Buchmann, J.: Einführung in die Kryptologie, Springer Spektrum; 6th revised edition 2016 (26th April 2016), ISBN-13 978-3-642-39775-2
- Schneier, B.: Angewandte Kryptographie, Pearson Studium; 1st edition (3 December 2005), ISBN-13: 978-3827372284
- Schneier, B.: Secrets and Lies, Wiley; 1st edition (24th April 2015), ISBN-13: 978-1119092438
- Wätjen, D.: Kryptographie, Grundlagen, Algorithmen, Protokolle, Springer Vieweg; 3rd edition (14th June 2018), ISBN-13 978-3-658-22474-5
- Ertel, W.: Angewandte Kryptographie, Carl Hanser Verlag GmbH & Co. KG; 6th updated edition (11th November 2019), ISBN-13: 978-3446463134

Websites:

- Federal Office for Information Security
- www.CrypTool.de (cryptographic software)

CY-B-12 Key Qualification 2

Module no.	CY-B-12
Module coordinator	Tanja Mertadana
Course number and name	Professional English
Lecturers	Elective subject (AWP) and language lecturers Tanja Mertadana
Semester	2
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	English

Module objectives

The Professional English module aims to provide students with specialised language skills that are necessary for working independently in the globalised field of cyber security. German or international students with German language skills of level C1 as per the Common European Reference Framework for Languages attend the English course included in the timetable and international students (who have not completed the B2 level and do not have a certificate for it) attend the German language courses offered by the Language Centre.

Professional English

The module trains students in the four basic skills of listening, reading, speaking and writing. Students expand their subject-specific vocabulary and deepen their knowledge of linguistic structures. Students design their own knowledge acquisition by means of targeted needs analyses and self-directed projects.

The main focus of the module is to optimise language fluency and improve the ability to communicate in English in order to better understand texts and conversations. Through task-related speaking, listening, reading and writing activities, students improve their communication skills and expand their faculty of expression. This enables them to take part in discussions and independently write business correspondence, as well as to create effective software documentation and to make successful presentations in English.

After completing the module, students will have acquired the following competencies:

Professional skills

- Students will have a secure command of the English language (B2, CEFR) and can also understand technical discussions in the field of cyber security.
- They will have B2 level skills to understand specialist literature and to create texts independently.
- Students will have a B2 level knowledge of linguistic means of expression in a formal and professional context.
- They will understand discussions and more complex content in their area of specialisation.
- They will acquire the ability to functionally apply grammatical structures in their future professional fields.
- They will be able to give understandable and detailed presentations on relevant topics related to cyber security. They can present their own opinions, as well as different points of view in an understandable manner.
- Students have an inter-cultural approach.

Methods expertise

- Students expand their language acquisition skills by reflecting on their individual learning styles.
- They can filter information from various English sources and process it for presentations.

Social skills

- Students are trained in the social skills of teamwork, reliability and integrity.
- They acquire communication skills by working with other people to find solutions.
- They reflect on their learning experiences from independent projects and teamwork.

Professional German

The Module objectives can be found in the corresponding course description on the homepage of the Language Centre.

Applicability in this and other degree programmes

Applicable as a key qualification module for other bachelor's degree programmes at Deggendorf Institute of Technology

Admission requirements and/or recommended prerequisites

Professional English:
The prerequisite for successfully participating in the module is a command of the English language at the B2 level, based on the Common European Framework of Reference for Languages (CEFR).

Professional German:
At the start of their studies, the students' knowledge of German is determined by means of a placement test. Depending on the result, the students are assigned to a course that corresponds to their language level. After successfully completing a course, students can attend an advanced German course in the next semester.

Content

Professional English

1 Computers in context
2 Computers and numbers 2.1 The language of mathematics 2.2 Binary representation of information

3 Basics of Computer Science 3.1 Computer Architecture 3.2 Operating Systems 3.3 Networks 3.4 Data structures
4 Software engineering
5 Case studies (e.g.: Alan Turing, cyber security, AI)
6 Communication skills (e.g.: presentations, discussions)
7 Writing skills (e.g.: business correspondence, software documentation)
8 Grammar (e.g.: tenses, passive structures)

Professional German

The content can be found in the corresponding course description on the homepage of the Language Centre.

Teaching and learning methods

The teaching methods focus on improving the four main language skills (listening, speaking, reading and writing), and optimising professional and social skills. Examples of the teaching methods used include various forms of group and individual work, mini-presentations, intensive reading and listening exercises, role play and grammar games, running dictations, translations, peer feedback, working with learning stations and various writing activities to consolidate what has been learnt.

There are weekly assignments for self-study.

Remarks

Compulsory attendance 75%

Recommended reading

Professional English

- Bonamy, David. Technical English 4. Harlow, England: Pearson Education, 2011. Print.
- Brieger, Nick & Alison Pohl. Technical English: Vocabulary and Grammar. Oxford: Summertown, 2002. Print.
- Büchel, Wolfram, et al. Technical Milestones: Englisch für technische Berufe. Stuttgart: Ernst Klett, 2013. Print.
- Butterfield, Andrew & Gerard Ekembe Ngondi, editors. Oxford Dictionary of Computer Science. Oxford: OUP, 2016. Print.

- Dasgupta, Subrata. Computer Science: A Very Short Introduction. Oxford: OUP, 2016. Print.
- DK. The Science Book: Big Ideas Simply Explained. London: DK, 2014. Print.
- Emmerson, Paul. Business Vocabulary Builder. London: Macmillan, 2009. Print.
- Emmerson, Paul. Business English Handbook. London: Macmillan, 2007. Print.
- engine: Englisch für Ingenieure. <www.engine-magazin.de> (Darmstadt). Various issues. Print.
- Glendinning, Eric H. & John McEwan. Oxford English for Information Technology. 2nd edition Oxford: OUP, 2006. Print.
- Ibbotson, Mark. Cambridge English for Engineering. Cambridge: Cambridge UP, 2008. Print.
- Ince, David. The Computer: A Very Short Introduction. Oxford: OUP, 2011. Print.
- Inch: Technical English. (Karlsruhe). Various Issues. Print.
- Munroe, Randall. What If? London: John Murray, 2015. Print.
- Schäfer, Wolfgang, et al. IT Milestones: Englisch für IT-Berufe. Stuttgart: Ernst Klett, 2013. Print.
- Schulze, Hans Herbert. Computer-Englisch: Ein englisch-deutsches und deutsch-englisches Fachwörterbuch. Hamburg: Rowohlt Taschenbuch Verlag, 2015. Print.
- Vince, Michael. Advanced Language Practice. London: Macmillan, 2009. Print.
- Wagner, Georg & Maureen Lloyd Zo?rner. Technical Grammar and Vocabulary: A Practice Book for Foreign Students. Berlin: Cornelsen, 1998. Print.

Professional German

Recommended reading can be found in the corresponding course description on the homepage of the Language Centre.

CY-B-13 Databases

Module no.	CY-B-13
Module coordinator	Prof. Dr. Udo Garmann
Course number and name	Databases
Lecturers	Prof. Dr. Wolfgang Dorner Prof. Dr. Udo Garmann
Semester	3
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

After completing the module, students will understand the importance of databases and will be able to take a differentiated approach to their use. They will know the procedure for creating a data model and can implement this in a concrete database. During this course, they will learn how to access relational databases with SQL and develop applications based on a database. The participants will acquire knowledge of performance optimisation when storing and accessing data, and will understand the interaction between application, presentation and database servers during programming, especially in a web environment.

Specifically, students will have achieved the following learning objectives after completing this module:

Professional skills

- Students will understand the concepts of databases and their use.

Methods expertise

- Students will have the ability to create software using a database.

Social skills

- Exercises are given during lectures. Students can thus understand and criticise the database designs of their fellow students and complement them with their own contributions.

Personal skills

- Students will be able to implement their own software-technical ideas with the help of databases and defend them against competing approaches.

Applicability in this and other degree programmes

The modules Programming II, Programming Project, Data Visualisation and Data Management as well as Software Engineering are thematically based on this module. The module can be used in other programmes of the faculty.

Admission requirements and/or recommended prerequisites

Recommended:

Computer Science module

Knowledge of a programming language is desirable.

Knowledge of Office applications is required.

Content

1 Introduction
  1.1 Introduction
  1.2 Why databases?
  1.3 Examples

2 Data modelling
  2.1 Redundancy
  2.2 Data modelling
  2.3 Object-oriented
  2.4 Relational data model
  2.5 Normalisation
3 SQL
  3.1 SQLite, a database for the trouser packet
  3.2 SQL Data Definition Language
  3.3 SQL Data Manipulation Language
  3.4 Tables and relations
  3.5 Data models
  3.6 View
4 Advanced concepts
  4.1 Targets for data storage/access
  4.2 ACID
  4.3 Sequential data organisation
  4.4 Index sequential data organisation
  4.5 Relative set organisation
  4.6 Optimisation
  4.7 Trees
  4.8 Implementations
  4.9 Object relational mapping
5 Outlook on NoSQL
  5.1 Basics of distributed systems
  5.2 Key/value stores
  5.3 Document databases
  5.4 Graph databases

Teaching and learning methods

- Lectures with exercises
- The accompanying exercise makes up for approx. 25% of the face-to-face classes. In a similar scope to the teaching material, accompanying exercises are provided for consolidation and exam preparation for the lecture follow-up.
- The proof of performance consists of exercises.

Recommended reading

Thomas M. Conolly, Carolyn E. Begg: Database systems, A practical approach to design, implementation, and management. Addison-Wesley, an imprint of Pearson Education, 4th edition 2005.

Kemper A., Eickler A.: Datenbanksysteme: Eine Einführung, Oldenbourg Wissenschaftsverlag

Preiß, N. (2007), Entwurf und Verarbeitung relationaler Datenbanken, Oldenbourg, Munich among others

CY-B-14 Stochastics

Module no.	CY-B-14
Module coordinator	Prof. Dr. Stefan Hagl
Course number and name	Stochastics
Lecturers	Prof. Dr. Stefan Hagl
Semester	3
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

After completing this module, students will have achieved the following learning objectives: The main focus is on professional skills and methods expertise in stochastics. Students will have knowledge of the concepts of descriptive and inductive statistics. Naturally, the acquisition of social skills is not the main focus of this module, but is fostered through the cooperation of students and by developing solutions together. Personal skills are sharpened by in-depth, independent elaboration and solving of complex problems.
Descriptive statistics:

Students will become familiar with the concepts of descriptive statistics, especially for univariate and bivariate descriptions. They will be able to recognise, model and solve statistical problems from this field that arise during their industrial placement.
For this, they will make use of software tools such as the statistics functions in spreadsheet programmes (MS Excel, OpenOffice Calc or LibreOffice).

Inductive statistics:

Students will know the concepts of inductive statistics based on probability theory. The practical statistical problem of drawing an inference from the sampling of total populations can be solved by a statistical technique of estimating parameters, performing parametric hypothesis tests, and goodness of fit tests depending on the topic. They will be able to create the necessary model design with random variables, test functions and their probability distributions. For this, they will make use of software tools such as the statistics functions in spreadsheet programmes (MS Excel, OpenOffice Calc or LibreOffice).

Applicability in this and other degree programmes

Applicability for the module for B.Sc. Artificial Intelligence:

- KI-21 Machine Learning
- KI-28 AI Project
- KI-29 Deep Learning/Big Data
- KI-36 Bachelor’s Thesis

Applicability for the module for B.Sc. Cyber Security:

- CY-B-20: Compulsory Elective Module Project
- CY-B-21: Cryptology 2
- CY-B-22: Management of IT Security Incidents
- CY-B-27: Digital Forensics
- CY-B-29: Security Engineering
- CY-B-32: Auditing of IT Systems

Admission requirements and/or recommended prerequisites

Recommended:

- Mathematics 1

Content

Descriptive statistics:

1 Basics and basic terminology

- Attributes, statistical units
- Values, scale of measure
- Statistical population, complete/partial survey
- Primary and secondary statistical survey
- Survey techniques

2 Frequency distributions
- Master list
- Frequency distribution
- Grouping and classification
- Graphical presentations

3 Location parameters
- Arithmetic mean
- Weighted arithmetic mean
- Median or central value
- Mode or modal value
- Geometric mean
- Harmonic mean and trimmed mean

4 Statistical dispersion
- Range
- Mean absolute deviation
- Mean quadratic deviation (variance)
- Standard deviation
- Quantile, quartile and semi-interquartile range
- Quartile coefficient

5 Coefficients of concentration
- Absolute and relative concentration
- Herfindahl index
- Concentration ratios and concentration curves
- Lorenz/Münzner coefficient
- Lorenz coefficient
- Lorenz curve

6 Index numbers
- Time series
- Proportions, index numbers, growth rates
- Rebasing and chaining
- Price index
- Quantitative index
- Value index

7 Regression
- Regression analysis
- Simple linear regression
- Method of least squares

- Determination coefficient
- Forecast
- Non-linear regression and multiple regression

8 Correlation
- Bravais-Pearson correlation coefficient
- Properties of variance and covariance
- Spearman-Pearson's rank correlation
- Correlation measured values for nominal variables

Inductive statistics:

1 Elementary probability theory
- Probability concept
- Random experiments and occurrences
- Kolmogorov axioms
- Two-stage experiments and conditional probability
- Bayes' theorem

2 Random variables
- Random variables
- Discrete probability distributions and distribution functions
- Continuous probability distributions and density function
- Expected value and variance of random variables

3 Distributions I
- Binomial distribution
- Normal distribution
- Multinomial distribution
- Hypergeometric distribution
- Poisson distribution

4 Sampling distributions
- Samplings
- Selection process
- Sampling distribution

5 Central limit theorem and applications
- Central limit theorem
- Sampling distribution of the mean
- Sampling distribution of the proportion
- Sampling distribution of standard deviations
- Sampling distribution of differences

6 Parametric hypothesis tests
- Null hypotheses and test theory
- Decision errors
- Tests for mean, proportion, standard deviation and differences

- Quality of a test

7 Estimation statistics
- Point estimation method: method of moments
- Point estimation method: maximum likelihood
- Quality criteria
- Interval estimation and confidence interval

8 Distributions II
- Student's t-distribution
- Chi squared distribution
- F-distribution

9 Parametric hypothesis tests with small samplings
- Proportion test – binomial test
- Proportion difference test – Fisher’s test
- Mean and mean difference test
- Variance quotient test

10 Goodness of fit tests
- Distribution hypotheses
- Chi squared goodness of fit test
- Independence tests

Teaching and learning methods

Theory and applications are taught and presented using classical presentation techniques. Many concepts are developed with the help of specific tasks and solved using a software tool. Exercises are given to students to complete on their own. Solutions to some of these are presented by students at the beginning of the next lecture. Alternatively, solution proposals by students are discussed in the iLearn system.

Recommended reading

Literature:

- Bourier G. (2022), Beschreibende Statistik, Praxisorientierte Einführung. Mit Aufgaben und Lösungen, 14th edition Gabler-Verlag, ISBN 3658370203
- Bourier G. (2018), Wahrscheinlichkeitsrechnung und schließende Statistik, Praxisorientierte Einführung. Mit Aufgaben und Lösungen, 9th updated edition
Gabler-Verlag, ISBN 3658074809
- Falk, Becker, Marohn (2004), Angewandte Statistik mit SAS, Springer Verlag, Berlin
- Georgii, H.O. (2015), Stochastik, Einführung in die Wahrscheinlichkeitstheorie und Statistik, Walter de Gruyter, Berlin

- Grabmeier J., Hagl S. (2020), Statistik - Grundwissen und Formeln, 4th edition, Haufe Taschen Guide 215, ISBN: 978-3-648-13965-3
- Hagl, S. (2017), Crashkurs Statistik - inkl. Arbeitshilfen online. Daten erheben, analysieren und präsentieren. Haufe Verlag, ISBN: 978-3-648-09673-4
- Monka, Michael, Voss, Werner, Schöneck, Nadine (2008), Statistik am PC, Lösungen mit Excel, 5th updated and expanded edition, Hanser-Verlag, Munich
- Pflaumer, Heine, Hartung (2001), Statistik für Wirtschafts- und Sozialwissenschaftler, Deskriptive Statistik, Oldenbourg, Munich
- Puhani (2005), Statistik, Einführung mit praktischen Beispielen, Lexika-Verlag, Würzburg
- Schwarze, J. (2014), Grundlagen der Statistik: Vol. 1, 12th edition, nwb Studium.
- Schwarze, J. (2013), Grundlagen der Statistik: Vol. 2, 10th edition, nwb Studium
- Zwerenz, Karlheinz (2008), Statistik verstehen mit Excel, R. Oldenbourg Verlag, Munich Vienna

Internet sources:

- Hagl, S., VHB basic Statistics I and II, https://kurse.vhb.org/

CY-B-15 Project Management

Module no.	CY-B-15
Module coordinator	Prof. Dr. Michael Ponader
Course number and name	Project Management
Lecturers	Prof. Dr. Michael Ponader
Semester	3
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Assignment, written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students acquire a basic general and basic technical and methodological knowledge in the field of project management.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students will acquire knowledge about the planning, monitoring and controlling of projects and about designing the necessary structure and process organisation.

Methods expertise

- Students will apply selected techniques of project management.

Personal skills

- Students will gain knowledge about self-organisation.

Social skills

- Students will apply this knowledge in different teams on the basis of a practice-oriented software or organisational project. This will foster their ability to cooperate and communicate, as well as their ability to deal with conflict.

Applicability in this and other degree programmes

All modules with more extensive group/project work

Admission requirements and/or recommended prerequisites

No prerequisites.

Content

1 Classic project management
- Recognition of the characteristics of projects in comparison with line tasks in a company, requirements for a project manager and his/her tasks
- Project organisation - presentation and discussion of different forms of organisation of a project team, possible distribution of tasks and competencies between project manager and line managers, composition, tasks and competencies of other committees in project organisation
- Project planning and controlling – presentation of different types of project plans and their dependencies, procedure for project planning, presentation of risk management in projects, dimensions of project management and control with the associated tools, methods and procedures
- Project phases – presentation of selected project phases, learning of the tasks in these phases

- Techniques – presentation of soft skills of a project manager (creativity techniques, moderation, presentation)
- Acquisition of knowledge in dealing with SW for project planning and controlling with the help of practical exercises

2 Agile project management
- Agile values/principles
- Scrum – roles, events, artefacts
- Kanban – practices, process, rules, best practices

3 Fields of application and combination of classic and agile approaches
4 Project management with MS Project
5 Partial execution of a practice-oriented software or organisation project in a team

Teaching and learning methods

- Lectures
- Exercises/case studies in individual and group work
- Presentations

Remarks

The proof of performance consists of two group projects, each of which is completed with a joint presentation of 15 minutes.

Recommended reading

- Chatfield, C. and others, (2011), Microsoft Project 2010 - Das offizielle Trainingsbuch, O`Reilly, Cologne
- GPM Deutsche Gesellschaft für Projektmanagement, Gessler, M. (publisher) (2019), Kompetenzbasiertes Projektmanagement (PM4)-Handbuch für die Projektarbeit, Qualifizierung und Zertifizierung auf Basis der IPMA Competence Baseline Version 4, 1st edition, GPM Deutsche Gesellschaft für Projektmanagement, Nuremberg
- Kerzner, H. (2003), Projektmanagement Fallstudien, mitp-Verlag, Bonn
- Kuster, J. et al. (2019), Handbuch Projektmanagement, 4th edition, Springer Verlag, Berlin
- Martinelli, R.J., Milosevic, D.Z. (2016), Project Management ToolBox - Tools and Techniques for the Practicing Project Manager, 2nd edition, Wiley, Hoboken, NJ
- Project Management Institute (publisher) (2017), A guide to the project management body of knowledge. PMBOK(R) Guide, 6th edition, Project Management Institute, Newtown Square, Pa

- Schwaber, K., Sutherland, J. (2016), Der Scrum Guide, Scrum.Org and ScrumInc, no information on the place of publication
- Timinger, H. (2017), Modernes Projektmanagement: Mit traditionellem, agilem und hybridem Vorgehen zum Erfolg, Wiley, Hoboken, NJ
- Verzuh, E. (2016), The Fast Forward MBA in Project Management, 5th edition, Wiley, Hoboken, NJ
- Wies, P. (2014), Project 2013 Grundlagen, Herdt-Verlag, Bodenheim

CY-B-16 Secure Programming

Module no.	CY-B-16
Module coordinator	Prof. Dr. Michael Heigl
Course number and name	Secure Programming
Lecturers	Prof. Dr. Michael Heigl
Semester	3
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	PrA
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students will have an in-depth knowledge and specialised technical knowledge in the areas of secure programming, secure coding guidelines and the development of secure software.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students will be able to present and explain the fundamental criteria to be observed for secure software development.

- They can implement their own software-technical ideas securely and evaluate software with regard to compliance with the principles of secure programming.
- They will be able to explain the meaning of measures for the validation of input values and take them into account in their own software developments.
- Students can demonstrate the difference between security measures for input validation and the integration of external components (library functions, etc.) and differentiate between necessary and unnecessary measures.
- They will know the top vulnerability lists and coding guidelines and can use them for secure software development.

Methods expertise

- They will know the current tools for static and dynamic code analysis and can use these.
- For a given list of requirements for a programme, students will be able to assess which attack vectors exist, which protection goals must be met in this context, and create this programme securely.

Personal skills

- By discussing current vulnerabilities and software, students develop awareness and an increased receptiveness and feel satisfaction from actively participating in their own learning.

Social skills

- Through group work in practical programming exercises, students develop the ability to work in a team and increase their goal and result orientation.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor’s programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- In-depth knowledge of the content of Programming 1 and Programming 2
- Knowledge of the content of Algorithms and Data Structures

Content

1 Introduction
   - Thematic classification
   - Reasons for non-secure software
   - Current examples of non-secure software
   - Abstract overview of a software programme

2 Validation of input values
   - Attack vectors input sources
   - Whitelisting vs. blacklisting
   - Use of regular expressions

3 System attacks
   - Buffer/stack overflow and countermeasures
   - Format string attack
   - Multiple deallocation

4 Software design
   - Design principles of secure software
   - Coding guidelines

5 Calling up/integration of further components
   - Calling up of library functions
   - Injection attacks
   - Protection of event logs

6 Output behaviour
   - Secure, controlled output
   - Web applications
   - Cross-site scripting attack
   - Cross-site request forgery
   - Cross-origin resource sharing

7 Top vulnerability lists, taxonomies and style guides
   - Vulnerability lists
   - Common Vulnerabilities and Exposures (CVE)
   - Common Weakness Enumeration (CWE)
   - CWE/SANS Top 25 most dangerous software errors
   - NIST National Vulnerability Database (NVD)

- OWASP Top 10
- Coding standards
- Top 10 secure coding practices (CERT/SEI)
- CERT C coding standard
- SANS Securing Web Application Technologies (SWAT) checklist

8 Correct use of cryptographic primitives
9 Error, exception and debug handling
10 Code analysis
- Static analysis
- Dynamic analysis
- Fuzzing

11 Formal methods

Teaching and learning methods

- Seminar-based lesson along with many practical exercises
- Project work that is carried out across semesters

Recommended reading

- Seacord, R.: Secure Coding in C and C++, Addison-Wesley Professional; edition: 2nd edition (2nd April 2013), ISBN-13: 978-0321822130
- Seacord, R.: CERT® C Coding Standard, Second Edition, The: 98 Rules for Developing Safe, Reliable, and Secure Systems, Addison-Wesley Professional, edition: 2 (14th April 2014), ISBN-13: 978-0321984043
- Gebeshuber, K.: Exploit!: Code härten, Bugs analysieren, Hacking verstehen. Das Handbuch für sichere Softwareentwicklung, Rheinwerk Computing, edition: 1 (26th July 2019), ISBN-13: 978-3836265980
- Basu, T.: Secure Programming with Python, Packt Publishing Limited (31 January 2017), ISBN-13: 978-1786466464

CY-B-17 Network Security

Module no.	CY-B-17
Module coordinator	Prof. Dr. Thomas Störtkuhl
Course number and name	Network Security
Lecturers	Prof. Dr. Thomas Störtkuhl
Semester	3
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Practical task, written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students have a basic general and technical knowledge in the field of network security. After completing the module, students will have acquired the following competencies:

Professional skills

- Students will be in a position to compare the security protocols of individual network layers and explain the differences.

- They will be able to illustrate how different configurations (e.g., cipher suits) affect the security of the communication relationship.
- They will know techniques for the logical separation of networks and can implement them in a network.
- They can discuss general methods for authentication and authorisation in networks.
- They can formulate the security measures for connections in wireless networks.

Methods expertise

- For a given scenario, students can decide the network layer on which security measures have to be taken.
- For a given network and communication relationships, they can decide which protection structures and filters must be used and configured in which way.

Personal skills

- The internships that take place address the students, which increases active participation in their own learning.

Social skills

- By participating in group discussions about securing communication infrastructures, students learn to stand up for the ideas of others.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of module CY-B-04 Operating Systems and Networks

Content

1 Network security
- Motivation and introduction: integration of security services
- Protocols of individual layers
- Physical layer security
- Data link layer security
- IEEE 802.1Q VLAN
- IEEE 802.1X – Extensible Authentication Protocol (EAP)
- IEEE 802.1AE MACsec
- PPP and PPTP
- Network layer security – IPSec
- Authentication header
- Encapsulating security payload
- Security association – ISAKMP
- Transport layer security
- SSL
- (D)TLS
- SSH
- Virtual private networks

2 Secure wireless and mobile communication
- IEEE 802.11 (WLAN)
- Security in GSM, UMTS, LTE, 4G
- Security in 5G

3 Protection of communication infrastructures
- Routing security
- Securing of DNS
- Protection structures and filters
- Firewall
- Deep packet inspection
- Intrusion detection/prevention/reaction systems
- Security in software defined networking

Teaching and learning methods

- Seminar-based lesson along with practical exercises
- Internships

Remarks

Practical task (PrL) as eligibility criterion for the examination.

Completion of internships and exercises in the module Network Security requires basic prior knowledge. Therefore, only those students who obtain a minimum of 40 ECTS credit points, and have passed at least two Foundational Level and Orientation Exams, will be eligible to take these modules.

Recommended reading

- Schäfer, G.: Netzsicherheit, Algorithmische Grundlagen und Protokolle, dpunkt-Verlag;
- Wendzel, S.: IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung, Springer Vieweg
- Alexander, M.: Netzwerke und Netzwerksicherheit - Das Lehrbuch, mitp/ bhv;

CY-B-18 Key Qualification 3

Module no.	CY-B-18
Module coordinator	Prof. Dr. Roland Zink
Course number and name	Technology Ethics and Sustainability Academic work
Lecturers	Prof. Dr. Roland Zink
Semester	3
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	PrA
Weight of the grade	5/210
Language of instruction	German

Module objectives

The content of the module consist of two subjects "Technology Ethics and Sustainability" (Subject A) and "Academic Work" (Subject B). *(Corporate Strategy CS/From CS to IT Strategy/Computer Centre Management)*

Subject A

With the formulation of Sustainable Development Goals (SDGs) by the United Nations in 2015, there is a comprehensive orientation framework on how humanity should develop in the future, and how the actions and behaviour of people are to be assessed with regard to this development goal.

This also applies Remarks to technical developments, whereby it must be constantly checked whether the new technologies meet both ethical and sustainable requirements. During the course, the need for sustainable development is linked to the digital transformation of our society and economy, and the aspects of technology ethics are also addressed. In addition to an introduction to the ethical principles, the ACM Code of Ethics and Professional Conduct (The Code) is also discussed Remarks.

Professional skills

- Students will understand the basic idea of sustainable development and its necessity for the future.
- Students will know the global development goals (SDGs) and can evaluate their own behaviour and existing technologies, as well as potential inventions in this context.
- Students will especially also know the "Life Cycle Assessment" method and the idea of "Cradle to Cradle"
- Students know the ethical principles and requirements in the context of technical innovations and development, and can apply them in their studies or in subsequent professional activities.

Subject B

"Being able to write academic or technical texts is a key skill that is crucial for achieving progress in studies and profession. Students usually do not bring this academic writing skill with them from school, but acquire it parallel to acculturation in the subject." This quote from the brochure of the Centre for University Didactics (DIZ, 2016) indicates the orientation of the content of the module. This content should prepare the students for their studies and academic work at an early stage. The course covers the requirements of academic work, the process flow, research methods and the quality criteria for academic work.
In a practice-oriented way, students learn to find suitable academic literature, to manage it and also to use it for academic work (e.g., reading, understanding, citing). Through exercises, students learn academic writing, research data management and academic data visualisation.

Professional skills

- Students will know the requirements and quality criteria for academic work.
- They will work out the process flow and the structuring of academic work.
- They will be enabled to carry out academic work independently, particularly research, library, literature and writing work.
- Students will know the rules for writing student papers and quality criteria for academic work in the context of their studies and will be able to apply them.

Subjects A and B

Methods expertise

- Students are enabled to work independently.

Social skills

- The exercises provide students with practice in partner work and teamwork.
- Students can explain and present the solutions they have independently developed during the exercises in front of a group.
- They learn to work independently.

Personal skills

- Through exercises, students learn to work independently and in a manner oriented to problems and action.

Applicability in this and other degree programmes

The module lays the foundations for the course in general, and is particularly linked to the following advanced module:

CY-B and KI-B: Key qualification 5

CY-B and KI-B: Bachelor’s module

Degree programme: B.A. Artificial Intelligence and B.A. Cyber

Security

Admission requirements and/or recommended

prerequisites

No prerequisites.

Content

Subject A

- Concepts and definitions of sustainability and/or sustainable development
- Sustainability models
- Optimisation and innovation as operationalisation strategies
- Digital transformation and ethical and sustainable aspects
- Life cycle assessment, cradle to cradle and circular economy
- Ethical principles
- Ethical aspects for computer scientists and programmers
- The ACM Code of Ethics and Professional Conduct (The Code)

Subject B

- Academic work: requirements, process and quality criteria
- Science and research
- Literature search, assessment and analysis
- Research status and theory
- Academic methods
- Basics of research data management
- Basics of academic data visualisation
- Creation of academic work

Teaching and learning methods

- Seminar-based lesson with group work and partner work
- Project work
- Blended learning

Recommended reading

Subject A

- Braungart, M. & McDonough, W. (2014): Cradle to Cradle: Remaking the Way We Make Things. Piper Verlag.
- Pufe, I. (2018): Nachhaltigkeit. Bundeszentrale für politische Bildung. Bonn.
- Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen (WBGU) (2019): Unsere gemeinsame digitale Zukunft. Berlin.

Subject B

- Karmasin, M. & Ribing, R. (2017): Die Gestaltung wissenschaftlicher Arbeiten. Utb.
- Metschl, Ulrich (2016): Vom Wert der Wissenschaft und vom Nutzen der Forschung. Zur gesellschaftlichen Rolle akademischer Wissenschaft. Wiesbaden.
- Sandberg, Berit (2017): Wissenschaftliches Arbeiten von Abbildung bis Zitat. Lehr- und Übungsbuch für Bachelor, Master und Promotion. De Gruyter Oldenbourg.
- Voss, R. (2014): Wissenschaftliches Arbeiten. 3rd edition. Vienna.

(Internet documents and guides are also used.)

CY-B-19 Software Engineering

Module no.	CY-B-19
Module coordinator	Prof. Dr. Andreas Wölfl
Course number and name	Software Engineering
Lecturers	Prof. Dr. Andreas Wölfl
Semester	4
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	PrA
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students will have detailed technical and methodological knowledge of software development.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students will be able to apply the basics of project management.
- They will be able to formulate and evaluate requirements.
- They will know coding rules and will be able to apply them.
- They will be in a position to review work results.

Methods expertise

- Students will be able to systematically implement an object-oriented design (analysis and design) on the basis of requirements using UML.
- On the basis of requirements and the code, they will be able to define test cases according to black box and white box test strategies, define test end criteria, and carry out tests.

Personal skills

- Through goal-oriented work, students will develop a high degree of strength of purpose.
- The agile methods promote self-motivation in students.
- The problem-solving thought process in students is sharpened by the task-oriented manner of working.

Social skills

- Students will be able to organise themselves independently in working groups for a project and execute the project together.
- The ability to work in a team is strengthened through active participation in team meetings.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of the modules
  - Basics of Computer Science
  - Programming 1
  - Programming 2
  - Secure Programming (B.Sc. Cyber Security)

Content

1 Motivation and definition
2 Elements of software engineering
3 Methods
  - Requirements engineering
  - Software design (general)
  - Software design
  - Architecture and detailed design (general)
  - Object-Oriented Analysis and Design (OOA, OOD)
  - UML introduction
  - UML workshop (diagrams and their application)
  - Application example
  - Transition from analysis to design
4 Implementation
  - Coding rules (e.g., MISRA)
  - Static code analysis
  - Code metrics
5 Software test
  - Static test
  - Dynamic test
  - Test process
  - Test methods and test strategies
6 Software quality assurance
  - Definition
  - Reviews

Teaching and learning methods

- Seminar-based lesson with practical exercises, some group work
- Semester-accompanying project work in groups

Recommended reading

- H. Balzer, Lehrbuch der Software-Technik, Spektrum Akademischer Verlag
- I. Sommerville, Software Engineering, Addison Wesley Verlag
- B. Kahlbrandt, Software-Engineering mit der UML, Springer Verlag
- C Rupp et. al., UML 2 - Glasklar, Hanser Verlag
- A. Spillner, T. Linz, Basiswissen Softwaretest, dpunkt Verlag
- B. Beizer, Black - Box Testing: Techniques for Functional Testing of Software and Systems, Wiley Verlag

- P. Liggesmeyer, Software - Qualität: Testen, Analysieren und Verifizieren von Software, Spektrum Verlag
- H. Sneed, M. Winter, Testen objektorientierter Software, Hanser Verlag

CY-B-20 Compulsory Elective Module Project

Module no.	CY-B-20
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Compulsory Elective Module Project
Lecturers	Prof. Dr. Michael Heigl Prof. Dr. Martin Schramm Prof. Dr. Thomas Störtkuhl
Semester	4
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 0 hours Self-study: 90 hours Virtual learning: 60 hours Total: 150 hours
Type of Examination	PrA
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students will obtain practical knowledge and practical technical knowledge in the field of computer science, especially information security and IT security.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students independently develop solutions for technical tasks.
- They evaluate and assess the results of their work.

Methods expertise

- Students have the ability to obtain detailed information on a specific task.
- They can create concepts for coping with a task in a limited time frame.

Personal skills

- Students develop a high degree of personal responsibility through the practical tasks that they are given.
- They will strengthen their independence by working independently and using suitable work techniques.
- They will become aware of their own capacity and develop resilience.

Social skills

- Self-organised work in small teams promotes respect and tolerance, as well as helpfulness among students.
- Students will acquire the ability to deal with conflict and a willingness to cooperate.

Applicability in this and other degree programmes

It is a special module for consolidating and acquiring practical skills in the field of data centre management.

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Content of the modules of the 1st - 3rd semesters

Content

Individual, depending on the specific topic

Teaching and learning methods

- Practical work
- Technical support provided by the professor who sets the topic

Remarks

- Students learn to work on a project independently or in a small team
- The topic is given by a professor from the DIT – if necessary, in cooperation with a regional company
- The professor who sets the topic evaluates the work

Recommended reading

Individual, depending on the specific topic

CY-B-21 Cryptology 2

Module no.	CY-B-21
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Cryptology 2
Lecturers	Prof. Dr. Martin Schramm
Semester	4
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Project work, practical task
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students have in-depth general and technical knowledge in the field of cryptology.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students are able to present the facets of elliptic curve cryptography.
- They can carry out cryptographic calculations and factorisation using elliptical curves.

- They know the types of random number generators and can compare them critically.
- They can explain the basic principles of pairing-based cryptography.
- They can demonstrate and discuss the current endeavours of post-quantum technology.
- They can describe measures of lightweight cryptography and measures of conventional cryptography.

Methods expertise

- For a given scenario, the students can decide whether conventional or lightweight cryptographic measures are more suitable.
- They can evaluate for how long current (non-PQC) methods will still be valid and decide which PCQ methods are best suited for a particular use case.

Personal skills

- Motivation, curiosity and capacity of students are developed by working on individual projects, as well as through internships.

Social skills

- The implementation of project work and the joint discussion of project groups sharpen empathy, the ability to work in a team, and the critical faculties of students.

Applicability in this and other degree programmes

Advanced compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Mathematical and abstract faculty of thought
- Knowledge of the content of module CY-B-11 Cryptology 1

Content

1 Elliptic curve cryptography
- Elliptic Curves and their Groups
- Elliptic curves over prime fields
- about the security of elliptic curves
- Elliptic curves over binary extension fields
- Efficiency of Calculations on Elliptic Curves
- Elliptic Curve Domain Parameter
- Elliptic Curve Cryptography (ECC) – algorithms
- Montgomery and (Twisted)-Edwards curves
- ECC – current recommendations and key lengths
- Factorisation using elliptic curves

2 Entropy and true random numbers
- PRNG
- TRNG
- Online test, tot test, and start-up test

3 Current topics of modern cryptography
- Pairing-based cryptography – using the example of elliptic curves
- Algebraic isolation
- Frobenius trace
- Frobenius endomorphism
- Divisors
- Evaluation of functions for divisors
- André Weil's reciprocity law
- Pairings (Weil pairing, Tate pairing, Ate pairing)
- Miller's algorithm
- Selected topics of post-quantum cryptography
- Hash-based cryptography
- Lattice-based cryptography
- Code-based cryptography
- Multivariant cryptography
- Supersingular isogeny-based cryptography
- Standardisation
- Selected topics of lightweight cryptography
- Lightweight stream and block ciphers
- Lightweight asym. techniques
- Lightweight hash functions and MACs
- Standardisation

Teaching and learning methods

- Seminar-based lesson along with practical exercises
- Internships

Remarks

Practical task (PrL) as eligibility criterion for the examination.

Completion of internships and exercises in the module Network Security requires basic prior knowledge. Therefore, only those students who obtain a minimum of 40 ECTS credit points, and have passed at least two Foundational Level and Orientation Exams, will be eligible to take these modules.

Recommended reading

Literature:

- Werner, A.: Elliptische Kurven in der Kryptographie, Springer; 2002 edition (4th October 2013), ISBN-13: 978-3540425182
- Jonas, T.: Elliptische-Kurven-Kryptographie, GRIN Publishing; 1st edition (24th August 2016), ISBN-13: 978-3668270381
- Mirbach, A.: Elliptische Kurven: Die Bestimmung ihrer Punktezahl und Anwendung in der Kryptographie, Verlagshaus Monsenstein und Vannerdat; 1st edition (1st November 2003), ISBN-13: 978-3937312224
- Johnston, D.: Random Number Generators-Principles and Practice: A Guide for Engineers and Programmers, Walter de Gruyter (7th May 2018), ISBN-13: 978-1501506079

Websites:

- BSI – instructions for use and interpretations (AIS) – AIS 20/31
- https://csrc.nist.gov/projects/post-quantum-cryptography
- https://csrc.nist.gov/projects/lightweight-cryptography
- www.CrypTool.de (cryptographic software)

CY-B-22 Management of IT Security

Module no.	CY-B-22
Module coordinator	Prof. Dr. Thomas Störtkuhl
Course number and name	Management of IT Security
Lecturers	Prof. Dr. Thomas Störtkuhl
Semester	4
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	PrA
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students have in-depth general and technical knowledge in the field of management of information security.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students are able to describe all elements of information security management in their function for information security.

- They can relate all elements of information security management to the continuous improvement process.
- They know essential methods of information security such as analysis methods, and can apply analyses to IT systems and IACS.
- Students know the essential content of relevant standards.
- They can apply the essential content of relevant standards to IT systems and IACS.

Methods expertise

- For a given IT system and IACS, students can derive useful IT security measures on the basis of an analysis.
- Students can assess whether certain IT security measures are suitable to avert or reduce certain threats and risks.

Personal skills

- Through the exercises that take place, students are encouraged to work through facts independently and to present them in an understandable manner.

Social skills

- Through the preparation of analyses in a team based on real examples from practice, students learn to work together constructively, during which the knowledge and ideas of other students are seen as helpful and beneficial.

Applicability in this and other degree programmes

Advanced compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of module CY-B-04 Operating Systems and Networks

- Knowledge of the content of module CY-B-17 Network Security

Content

- Motivation for the management of information security: current situation of information security; regulatory requirements at a national and European level; protection of critical infrastructures
- Information security layers with a holistic approach: ISO/IEC 27001, Defence-in-Depth, continuous improvement process, lifecycle of an IT system or an IACS (Industrial Automation and Control System), prevention, detection, reaction cycle.
- Elements of information security management: all elements along the continuous improvement process are addressed: definition of scope, stakeholder analysis, description of the context, document control, analysis of protection needs, threats and risks, definition of an IT security architecture, processes: user & rights management, change management, backup & recovery, security incident management, vulnerability management,
  auditing and management review, business continuity, process for the development of products with IT security, quality, management of suppliers and service providers
- The elements of information security management focus on risk analysis and business continuity: methods, process, documentation
- Essential content of standards such as ISO/IEC 27001, IEC 62443, BSI Grundschutzkompendium (Basic Protection Compendium) or ICS Security Compendium or National Institute of Standards and Technology (NIST) are presented.

Teaching and learning methods

- Seminar-based lesson along with practical exercises

Recommended reading

- ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary, third edition, 2014-01-15
- ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 + Cor. 1:2014), English translation of DIN ISO/IEC 27001:2015-03
- ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls, second edition, 2013-10-01

- ISO/IEC 27005:2018-07 Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement, English title: Information technology – Security techniques – Information security risk management
- IT Basic Protection Compendium, Federal Office for Information Security, Bonn 2020; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html (last accessed on 3.10.2020)
– 65/756/CDV:2019-08 – IEC 62443-2-1 Ed.2.0 – Security for industrial automation and control systems – Part 2-1: Security programme requirements for IACS asset owners
- IEC 62443-2-3, Edition 1, 2015-06, Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment
- DIN EN 62443-3-2:2018-10; VDE 0802-3-2 – Draft Sicherheit für industrielle Automatisierungssysteme – Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 65/690/CDV:2018); German and English version prEN 62443-3-2:2018; English title: Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design (IEC 65/690/CDV:2018)
- IEC 62443-3-3, Edition 1, 2013-08, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014
- DIN ISO 31000:2018-10: Risikomanagement – Leitlinien (ISO 31000:2018), English title: Risk management – Guidelines (ISO 31000:2018), 2018-10
- Zusammenhang von Security und Funktionaler Sicherheit (Connection between Security and Functional Security), Felix Wieczorek, Frank Schiller, Roland Fiat, Thomas Störtkuhl, atp edition, 6/2013
- Ganzheitliches Management der Informationssicherheit (Holistic Management of Information Security), Thomas Störtkuhl, et al., SecuMedia, 19th September 2008
- Alles im Blick, Ganzheitliches Sicherheitsmanagement mit Kennzahlen für IT-Betrieb und -Sicherheit (Everything in Sight, Holistic Security Management with Key Figures for IT Operations and IT Security), Udo Adlmanninger, Thomas Störtkuhl

CY-B-23 Distributed Ledger Technologies

Module no.	CY-B-23
Module coordinator	Prof. Dr. Thomas Störtkuhl
Course number and name	Distributed Ledger Technologies (DLT)
Lecturers	Prof. Dr. Thomas Störtkuhl
Semester	4
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students have basic general and technical knowledge, as well as procedural knowledge, in the field of distributed ledger technologies.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students can classify and explain the different proposed solutions for distributed ledgers.

- They can summarise and explain the different consensus-building methods.
- They can specify the possible uses of various distributed ledger technologies and derive other possible uses.
- They can implement selected examples of distributed ledgers and consensus protocols.

Methods expertise

- Students are able to differentiate between existing and future proposals for distributed ledgers and compare their respective advantages and disadvantages.
- They can check for a given use case whether the use of a DLT technology makes sense or whether conventional database solutions are sufficient.

Personal skills

- Students develop diligence and conscientiousness by preparing and processing a current topic in the area of DLT.

Social skills

- Group discussions and the interlinking of the practical projects promote networking skills, ability to deal with conflict and critical skills.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of modules CY-B-11 Cryptology 1, CY-B-13 Databases and CY-B-17 Network Security

Content

1 Introduction
- Motivation
- Overview
- Distributed ledger taxonomy

2 Consensus building
- Proof-based/computational-based consensus protocols
- Proof of Work (PoW)
- Proof of Stake (PoS)
- Other concepts
- Voting-based/computational-based consensus protocols
- (Byzantine) Fault Tolerance
- Practical-Byzantine-Fault-Tolerance (PBFT)
- Other concepts

3 Applications
- Cryptocurrency – e.g.: Bitcoin – BTC (Blockchain)
- Smart Contracts and DApps – e.g.: Ethereum
- Mobility concepts – e.g.: IOTA (Tangle – Transaction Directed Acyclic Graph (TDAG))
- Platform for open-source blockchain applications

4 Potentials
- Five theses for the potential of DLT
- How to evaluate a use case for the suitability of DLT use
- Assistance in the decision-making process

5 Practical project

Teaching and learning methods

Seminar-based lesson along with practical exercises

Recommended reading

Literature:

- Schütz, A., Fertig, T.: Blockchain für Entwickler: Das Handbuch für Software Engineers. Grundlagen, Programmierung, Anwendung. Mit vielen Praxisbeispielen, Rheinwerk Computing; 1st edition (22 February 2019), ISBN-13: 978-3836263900

- Hellwig, D., Karlic, G.: Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology, Springer; 1st ed. 2020 edition (30th June 2020), ISBN-13: 978-3030401412
- Treiblmaier, H., Clohessy, T.: Blockchain and Distributed Ledger Technology Use Cases: Applications and Lessons Learned, Springer; 1st ed. 2020 edition (13th July 2020), ISBN-13: 978-3030443368
- Lemieux, V., Feng, C.: Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers, Springer; 1st edition 2021 edition (13th December 2020), ISBN-13: 978-3030544133
- Köhler-Schute, C.: Blockchains und Distributed-Ledger-Technologien in Unternehmen: Grundlagen, Konzepte und Praxisbeispiele, juristische Aspekte, KS-Energy-Verlag (26th September 2019), ISBN-13: 978-3945622094

Websites:

- Blockchain – https://www.blockchain.com/de/
- Ethereum – https://ethereum.org/
- IOTA Tangle – https://www.iota.org/
- HaderaHashgraph – https://www.hedera.com
- Hyperledger – https://www.hyperledger.org

CY-B-24 Key Qualification 4

Module no.	CY-B-24
Module coordinator	Prof. Dr. Josef Scherer
Course number and name	Compliance, Data Protection and IT Law
Lecturers	Michael Donnert Anke Hofmeyer Prof. Dr. Josef Scherer
Semester	4
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Written examination, 90 min.
Duration of Examination	90 min.
Weight of the grade	5/210
Language of instruction	German

Module objectives

1 The course should generate transparency and understanding for the often "nebulous" topic and show clear structures and practical work aids.
2 After the course, participants should know, understand and be able to explain in simple terms
- what the relevant components of the presented processes/systems/organisation are,

    - to what extent it affects them (role, tasks, responsibility, benefit) and
    - how the process flows that are relevant to them can be enriched in this regard.
- In addition, participants should be enabled to make the relevant requirements for their own work area transparent as goals and to meet them.
- Presentation of the value contributions of the system/processes for the company/organisation and employees should generate awareness, interest and motivation for the "proactive life" of the system.

Participants should acquire basic knowledge in the areas of
Compliance, Data Protection and IT Law
and should be able to find an operational organisational solution to practical problems from these areas, in the case of standard problems perhaps even in the form of procedural instructions and process descriptions.

In addition, it is expected that after completing this module, participants will be able to clearly explain the relevant content in their own words.

Software and Licence Management

After completing the module, participants should have achieved the following learning objectives:

- Participants can conceptualise and implement a digitalised integrated management system in the areas of compliance, data protection and IT law or relevant process flows, and enrich the structure and process organisation with corresponding compliance, risk and ICS components.
- Participants can solve problem cases using the judicial case-solution method.
- They can implement the knowledge they have acquired about target-actual comparisons and recommendations for action in companies/organisations.
- Participants have the ability to assign facts and tasks to the appropriate area in a company or environment and recognise interfaces to other functions.
- Using SWOT analyses, target-actual comparisons, etc., participants will be able to submit recommendations for action to manage governance (corporate governance and corporate monitoring) risks.
- Participants will become familiar with auditing methods and will be oriented firstly towards the “current state of legislation and jurisdiction (compliance)” and secondly towards the “recognised state of science and practice” with regard to the relevant topics.

In the process, they will make use of the standards, of which they have basic knowledge (sets of rules of (international) institutionalised expert committees) (e.g., DIN/ISO/COSO/IDW/DIIR etc.).

- Participants can understand networking within the various corporate functions (leadership, core and support process topics), taking into account the legal framework conditions, and can conceptualise and improve a corresponding architecture.
- SWOT analyses and target-actual comparisons in the context of practical work in companies (or on the basis of case studies) help participants improve the organisation of companies or sub-sectors in their professional life.
- Participants reflect on a topic in an international context (e.g., international law, international standards). They reflect on all content under the aspect of digital transformation and modelling as process flows.

Value contribution of the module/course

After spending a little time,

- the lecturers/coaches with highly relevant personal, professional and pedagogical competence
- give the participants transparency in an easily memorable form about the requirements for them and the organisation, as well as
- pragmatic and structured implementation recommendations
- based on checklists, models, process flow descriptions

and

- virtual courses with many short sequences.

Applicability in this and other degree programmes

Applicability of the module for this programme

The Compliance, Data Protection and IT Law module is one of the key qualifications.

Applicability of the module for other programmes

The module Compliance, Data Protection and IT Law can be used in all other technical, legal, business psychological and business programmes,

since the knowledge of governance, compliance and corporate social responsibility/sustainability, as well as the rights and duties of managers, other executives and employees, are almost indispensable for “proper and conscientious” management.

Admission requirements and/or recommended prerequisites

This module builds on the content of the relevant essays of *Scherer/Fruth/N.N.*:

Compare scherer-grc.net/publikationen and books by *Scherer/Fruth* (publisher):

- Scherer/Fruth/Grötsch (publishers), "Digitalisierung, Nachhaltigkeit und Unternehmensführung 4.0" (GRC) (analogue), 2021, ISBN-No. 978-3-947301-27-0, available at a price of 15?
- Scherer/Fruth (publishers), "Digitalisiertes Integriertes Risiko-Managementsystem mit Governance, Risk und Compliance (GRC)", (analogue), 2019, ISBN-No. 978-3-947301-21-8, available at a price of 15?
- Scherer, "Management reloaded" - "GRC & ESG in Strategy & Performance" (GRC & ESG in S & P), RiskNet, 2021 (available for free download at scherer-grc.net).
- Scherer/Romeike/Grötsch, Unternehmensfürhung 4.0: CSR / ESG, GRC & Digitalisierung integrieren, RiskNet, 2021 (available for free download at scherer-grc.net).

Further introductory/accompanying literature:

Scherer/Fruth (publishers):

- Integriertes Managementsystem "on demand", 2018
- Integriertes Compliance-Managementsystem, 2018
- Integriertes Qualitäts-Managementsystem, 2018
- Handbuch Integriertes Personal-Managementsystem, 2018

Content

Scherer (blended learning/virtual): 2 SWS

Classic vhb: Governance, risk and compliance in the area of personnel/HR

- Sequence 30-45: legally compliant, process-oriented corporate organisation
  - Component K11 – Organisational framework (company-wide) – legally compliant, process-oriented corporate organisation

  - Component K11 – Company-wide organisational framework - Introduction part I: Definitions, tools & methods, components, conception
  - Component K11 – Company-wide organisational framework – Introduction part II: Legal framework conditions and standards
  - Component K11 – Company-wide organisational framework – Introduction part III: "Process-oriented organisation"
  - Component K11/1 – Company-wide organisational framework/corporate (group) structure that is appropriate under company law
  - Component K11/2 – Company-wide organisational framework/legally compliant organisational charts
  - Component K11/3 – Company-wide organisational framework/interface management
  - Component K11/4 – Company-wide organisational framework/legally compliant job descriptions
  - Component K11/5 – Company-wide organisational framework/legally compliant interaction management
  - Component K11/6 – Company-wide organisational framework/legally compliant delegation
  - Component K11/7 – Company-wide organisational framework/legally compliant process descriptions
  - Component K11/8 – Company-wide organisational framework/effective supervisory or control mechanisms
  - Component K11/9 – Company-wide organisational framework/implemented and effective information and communication management
  - Component K11/10 – Company-wide organisational framework/implemented and effective documentation management
  - Component K11/11 – Company-wide organisational framework/supported (integrated) management system
  - Component K11/12 – Company-wide organisational framework/appropriate (personnel) resources
- Sequence 63-75: risk management in the area of human resources

    - Component K29 - Implementation of a risk management process with a “lines of defence” model
    - K29/1: Top risk: high fluctuation
    - K29/2: Top risk: extremely high personnel costs
    - K29/3: Top risk: criminal behaviour of employees
    - K29/4: Top risk: lack of motivation in employees
    - K29/5: Top risk: liability and litigation risks due to complex and constantly changing labour laws
    - K29/6: Top risk: discontinuation of service providers
    - K29/7: Top risk: very few qualified employees
    - K29/8: Top risk: incorrect prognosis of personnel requirement
    - K29/9: Top risk: incorrect estimation of technological changes and trends
    - K29/10: Top risk: management-related risk
    - K29/11: Top risk: use of external resources
    - Component K30 - Implementation of a goal deviation, (violation), detection and response process
- Sequence 76-83: personnel processes
    - K31/8 Personnel processes: Introduction
    - K31/8-1 Personnel processes: 1. Personnel planning
    - K31/8-2 Personnel processes: 2. Personnel acquisition
    - K31/8-3 Personnel processes: 3. Personnel administration
    - K31/8-4 Personnel processes: 4. Personnel leadership
    - K31/8-5 Personnel processes: 5. Personnel development
    - K31/8-6 Personnel processes: 6. Personnel layoff
    - K31/8-7 Personnel processes: 7. Personnel controlling
- Sequence 84-95: labour law
- K31/10-5.A.3 - Labour law and compliance management in the area of personnel/1. Introduction
- K31/10-5.A.3 - Labour law/2. Legal basics of labour law
- K31/10-5.A.3 - Labour law/3. Basic concepts
- K31/10-5.A.3 - Labour law/4. Establishment of the employment relationship
- K31/10-5.A.3 - Labour law/5. Remuneration without work
- K31/10-5.A.3 - Labour law/6. Termination of the employment relationship by expiry of a fixed-term contract
- K31/10-5.A.3 - Labour law/7. Termination of the employment relationship by dismissal
- K31/10-5.A.3 - Labour law/8. General protection against dismissal
- K31/10-5.A.3 - Labour law/9. Collective labour law: Definitions
- K31/10-5.A.3 - Labour law/10. Collective labour law: Law on collective agreement

- K31/10-5.A.3 - Labour law/11. Collective labour law: Right to take industrial action
- K31/10-5.A.3 - Labour law/12. Collective labour law: Industrial constitution law

OPEN vhb: Corporate governance 4.0: The prudent businessman and his digitalised, integrated management system with GRC

Chapter 1: "Digital, fit, proper, sustainable, successful & safe: The prudent businessman 4.0!"

1. Introduction: "At a glance and overview": Facts and the story
2. “Doing the right thing the right way”: The “prudent businessman 4.0”: OK!
3. Releasing effect and other value contributions of a digitalised integrated management system 4.0
4. Which management system(s) and how many standard(s) for digitalisation and GRC does the manager need?
5. Terms that the prudent businessman and his employees need to know
6. What does the digitalisation of business processes and enrichment with GRC methods and tools mean?
7. Corporate, environment, interested parties, risk and SWOT analysis: Everyone wants the same thing: No deficiencies in digitalisation and GRC
8. "Ready for take off: The new tone from the top in a corporate flying ship"
9. Governance: Interaction between bodies, conscientious corporate governance and corporate monitoring
10. "Hard Facts": What does the prudent businessman have to take care of and what expertise is required?
11. How should top managers allocate their most important resource, i.e., time, to their most important tasks
12. "We cannot improve so easily!" The "habitus" of the "prudent businessman 4.0": Knowledge, social, cultural, linguistic, physical, psychological, digital capital and soft skills
13. Manager liability: Civil and criminal liability of bodies and (special) agents
14. Manager risk case and liability firewall
15. New goals in a new world
16. (Digitalisation) vision/objectives/strategy/planning
17. "Why does it often not work?": Homo irrationalis versus fit & proper: Behavioural economics and economic psychology

18. Implementation of (digitalisation) measures with accompanying control and monitoring

Chapter 2: "One fits all": The digitised integrated management system (IMS) with GRC

1. "Step by step" – The first steps for introducing an integrated GRC management system
2. "The backbone of organisation" – Process modelling
3. Scope of standards for a digitised "integrated management system with GRC" (IMS) – which management system(s) and standards does a manager need?
4. Relevant standards, tools and methods
5. Explanation of relevant terms
6. Context of organisation, goals, value contribution, scope, structure and components of the digitalised integrated GRC management system
7. Integrated financial management system
8. Integrated quality management system, product compliance and contract management with GRC
9. Integrated compliance management system
10. Integrated risk management system with GRC
11. Integrated personnel management system with GRC
12. Integrated sustainability management system
13. Integrated digitalisation, IT, information security, data protection management system
14. The "tone from the top" is what counts
15. Planning of an appropriate digitised GRC management system
16. Support: Implementation of the digitalised integrated GRC management system and appropriate framework conditions
17. Operation: Implementation and effectiveness (operation) of the digitalised integrated GRC management system and the process
18. Accompanying control, monitoring and evaluation of the digitised integrated GRC management system (through the "lines of defence")
19. Adjustments in the event of deficiencies and changes in the organisation and environment

Hofmeyer (1 SWS):

New data protection rules have been applicable in all member states of the European Union since 25 May 2018. This reform aims to ensure the same standard of data protection in all member states.

As Germany already had high data protection requirements, the new regulations resulted in numerous formal changes, but the reform was not accompanied by the imposition of more stringent requirements in terms of content.

A data protection concept or data protection management system established within an organisation can prove and verify compliance with legal requirements. The practical establishment requires detailed information from the departments and organisational units of the organisation and, if used successfully, offers added value with regard to possible audits by the data protection or supervisory authority.

Regardless of the chosen form of operation, most of the risks in IT operations have - their origin in inadequacies, different types of errors and failures. These may originate from:

- employees, customers and other partners
- incorrect, incomplete or outdated data (e.g., parameters, configurations, versions)
- applications and the IT infrastructure
- IT processes and the entire IT organisation
- IT environment (building, location, other general conditions)

There can be no complete protection against IT risks, because the risk factors are too diverse and the human factor plays a large role that cannot be clearly predicted. However, effective risk and compliance management in a company's data processing can prevent a total failure or loss of data that threatens the company's existence, thus reducing costs by avoiding damage and liability.

Learning objectives:

1 Introduction to the EU-GDPR + BDSG-new (Federal Data Protection Act)
2 Consequences of the EU-GDPR
3 Structure and responsibility
4 Record of processing activities
5 Involvement of external service providers
6 Information obligations and data subject rights
7 TOMs
8 Dealing with data protection breaches
9 Data protection in everyday business

Donnert (1 SWS):

Participants

- can explain the basic definition of IT security,
- can describe the differences between data protection, IT security and information security (IS),
- can explain why IS is necessary,

- can name the protection goals of IS,
- can explain the basic differences between the various management systems,
- can describe the different IS threats,
- know about awareness-raising activities to improve IS.
- They are in a position to manage IS risks.

Teaching and learning methods

Seminar-based lesson, exercises, case solutions based on examples from the (highest) judicial jurisdiction, self-study, student presentations and research papers.

Through a multifunctional, interdisciplinary approach (law, business administration, technology,
economic psychology, behavioural economics) imparted in the course and understood by participants, the participants gain different perspectives and insights into the subjects and objects of (economic) life, as well as their own selves.

Remarks

The module contains virtual components:

2 SWS:

Prof. Dr. Josef Scherer:

vhb course:

“Integrated management system in the area of personnel/HR with governance, risk and compliance", sequences 30-45 (legally compliant, process-oriented corporate organisation) and sequences 63-95 (risk management in the area of human resources, personnel processes, labour law)

OPEN vhb course:

"Corporate governance 4.0 with governance, risk and compliance" – The prudent businessman and his digitalised, integrated management system with GRC.

Complete course!

Recommended reading

Introductory literature

Scherer,
Good Governance und ganzheitliches, strategisches und operatives Management: Die Anreicherung des "unternehmerischen Bauchgefühls" mit Risiko-, Chancen- und Compliancemanagement, in: Corporate Compliance Zeitschrift (CCZ), 6/2012, p. 201-211 (available for free download at www.scherer-grc.net/publikationen).

Scherer,
"Management reloaded" - "GRC in Strategy & Performance" (GRC in S & P), 2021 (available for free download at www.scherer-grc.net/publikationen)

Course-accompanying

literature

Books:

Scherer/Fruth
(publishers), Digitalisierung, Nachhaltigkeit und "Unternehmensführung 4.0", 2021

Scherer/Fruth
(publishers),

Handbuch: Integriertes Personal-Managementsystem, 2018

Scherer/Fruth
(publishers),

Handbuch: Integriertes Compliance-Managementsystem, 2018

Essays (available for free download at: Scherer-grc.net/Publikationen):

Scherer, "Management reloaded" - "GRC & ESG in Strategy & Performance" (GRC & ESG in S & P), RiskNet, 2021.

Scherer/Romeike/Grötsch, Unternehmensfürhung 4.0: CSR / ESG, GRC & Digitalisierung integrieren, RiskNet, 2021.

Scherer,

"Healthcare und Pflege 4.0" - Die digitale Transformation von Compliance, Risikomanagement und Standards im Gesundheitswesen, Journal für Medizin- und Gesundheitsrecht, 1/2019, p. 33 ff.

Scherer,
"Healthcare und Pflege 4.0" - Die digitale Transformation von Compliance, Risikomanagement und Standards im Gesundheitswesen, Teil 2: Organhaftung und Beweislast bei Verstoß gegen Regeln der Technik, Journal für Medizin- und Gesundheitsrecht, 2/2019, p. 109 ff.

Scherer,
"Healthcare und Pflege 4.0" - Die digitale Transformation von Compliance, Risikomanagement und Standards im Gesundheitswesen, Teil 3: Integration von Standards in digitalisierte, vernetzte Managementsysteme, Journal für Medizin- und Gesundheitsrecht, 3/2019, p. 171 ff.

Scherer,
"Healthcare und Pflege 4.0" - Die digitale Transformation von Compliance, Risikomanagement und Standards im Gesundheitswesen, Teil 4: "Digital Governance": "Wirksamkeit" eines Integrierten GRC-Managementsystems durch Digitalisierung und "nudges", 4/2019, p. 171 ff.

Scherer,
"Unternehmensführung 4.0" in der Health-Care- und Pflege-Branche: Der "Ordentliche Kaufmann 4.0" und sein digitalisiertes Integriertes GRC-Managementsystem: "Das Richtige richtig tun in unsicheren Zeiten", Journal für Medizin- und Gesundheitsrecht, 1/2020, p. 34 ff.

Scherer,
"Digital, fit & proper": Neue Anforderungen an Management und Mitarbeiter durch digitale Transformation und Corona-Krise, Journal für Medizin- und Gesundheitsrecht, 2/2020, p. 102 ff.

Scherer,
Resilienz & Zukunftsfähigkeit: Aktuelle Anforderungen an Unternehmensführung (GRC), Digitalisierung und Nachhaltigkeit, Journal für Medizin- und Gesundheitsrecht, 03/2020, p. 165 ff.

Scherer / Grötsch,
Gemeinsamkeiten von Nachhaltigkeit (ESG/CSR) und Governance (GRC) im Healthcare- und Pflegebereich, Journal für Medizin- und Gesundheitsrecht, 1/2021.

Further literature:

Scherer/Fruth
(publishers), Digitalisiertes Integriertes Risiko-Managementsystem, 2019

Scherer/Fruth
(publishers),

Handbuch: Integriertes Managementsystem (IMS), 2018

Scherer/Fruth
(publishers),

Handbuch: Integriertes Qualitäts-Managementsystem, 2018

Scherer/Fruth
(publishers),

Handbuch: Integriertes Product-Compliance-, Vertragsmanagement und Qualitätsmanagement, 2018

Scherer/Fruth
(publishers),

Geschäftsführer-Compliance, Praxiswissen zu Pflichten, Haftungsrisiken und Vermeidungsstrategien, 2009

Scherer/Fruth
(publishers),

Gesellschafter-Compliance, Praxiswissen zu Pflichten, Haftungsrisiken und Vermeidungsstrategien, 2011

Plus numerous relevant essays for free full-text download at:
www.govsol.de/Publikationen

CY-B-25 Practical Module

Module no.	CY-B-25
Module coordinator	Prof. Dr. Udo Garmann
Course number and name	Industrial placement Practice accompanying course Practical seminar
Semester	5
Duration of the module	1 semester
Module frequency	Annual
Course type	PLV, Compulsory course
Level	Undergraduate
SWS	4
ECTS	30
Workload	Contact hours: 60 hours Self-study: 840 hours Total: 900 hours
Type of Examination	Assignment, internship report
Weight of the grade	30/210
Language of instruction	German

Module objectives

The knowledge, abilities and skills acquired so far during the course are to be used methodically and in context in a project in the field of cyber security with the aim of providing practical experience to anchor and expand what has already been learned. In addition, students will get to know the importance of teamwork in industrial practice.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- By working on a topic in the area of industrial placements, students will gain practical experience in the respective topic of focus.
- Students will gain the competence to independently apply the knowledge and skills acquired so far during their studies to partially complex tasks and present them in an appropriate oral and written form.

Methods expertise

- By planning and executing work steps and completing them in the form of an internship report, students will gain the ability to complete a practical project independently and successfully.

Personal skills

- By completing the practical module, students will develop personal responsibility, self-discipline, self-reflection and self-confidence.

Social skills

- Students will acquire the ability to present the components of a task in a target group-oriented manner during the industrial placement and the results achieved in the placement.

Applicability in this and other degree programmes

It is a special module for this course **Admission requirements**

and/or recommended prerequisites

Formal:

- According to § 6 of the study and examination regulations, admission to the practical study semester requires a minimum of 70 ECTS credits.

Content-related:

- Knowledge and applicability of the content of previous semesters

Content

The practical module of the practical study semester is made up of the parts In-company Internship, Practical Seminar and Internship-Supplementary Specialisation.

The duration of the module is at least 20 weeks and includes an internship in a company (industrial placement), seminars offered by Career Service (Advanced courses to complement the practice), as well as internship accompanying courses according to the curriculum (Practical Seminar), which take place as block courses at the beginning and/or end of the semester.

More information on the advanced courses to complement the practice:

This will be replaced by seven seminars offered by Career Service. By the end of the 7th semester, every student of the Cyber Security programme is required to attend five seminars from the “Study and Personality Competence” category and two seminars from the “Professional Competence” category.

At least five seminars from both categories must be attended by the start of the internship in the 5th semester.

Compulsory seminars:

- Presentation techniques
- LaTex
- Library seminar "Databases/Literature Research"

Optional seminars:

- A seminar topic from the area of Study and Personal Skills can be freely selected
- A seminar topic from the area of Study and Personal Skills can be freely selected
- A seminar topic from the area of Professional Skills can be freely selected
- A seminar topic from the area of Professional Skills can be freely selected

Students can obtain more detailed information on the respective seminars offered from Career Service.

Teaching and learning methods

- Industrial Placement: internship
- Practical seminar: seminar-based lesson
- Advanced courses to complement the practice: seminar

Remarks

- In duly justified exceptional cases, proof of practical activity (In-company Internship) can be substituted by relevant subject-related practical training.
- The practical study semester (In-company Internship) can also be completed abroad.

Recommended reading

None

CY-B-26 Penetration Testing

Module no.	CY-B-26
Module coordinator	Prof. Dr. Michael Heigl
Course number and name	Penetration Testing
Lecturers	Prof. Dr. Michael Heigl
Semester	6
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Project work, practical task
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students should have fundamental, in-depth technical knowledge and methodological knowledge in the areas of penetration testing and vulnerability analysis.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students can explain the individual phases of a penetration test.
- They know the existing exploiting frameworks and can use them.

- They can determine auxiliary modules for the individual phases of a penetration test and implement them.
- They can analyse the suitability of existing automation mechanisms for a given use case and apply them.
- They can independently carry out a vulnerability analysis and evaluate the results.

Methods expertise

- For a sample penetration test, students can assess which type of documentation is most suitable during the test.
- Students are able to develop their own tools for penetration testing.

Personal skills

- The independent implementation of a penetration test with all its phases promotes personal responsibility and self-discipline, which in turn promote the self-efficacy of students.

Social skills

- Project work in a team and working together on a task strengthens communication skills, the willingness to compromise, as well as critical faculties.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of the basic modules
- Knowledge of the content of module Network Security
- Knowledge of the content of modules Cryptology 1 Cryptology 2

Content

1 Introduction
- Motivation
- Thematic classification
- What is pen-testing?

2 Methodology – phases of a penetration test
- Preparation
- Information gathering and evaluation
- Evaluation of information/risk analysis
- Active penetration tests
- Final analysis

3 Exploiting frameworks
- Scope of exploiting frameworks
- Existing frameworks

4 Documentation during a penetration test

5 Introduction to the Metasploit framework
- History and architecture
- Installation and updates
- User interfaces
- Data stores and databases
- Workspaces
- Logging and debugging

6 The pre-exploitation phase
- Auxiliary modules and their application
- Shodan search engine
- Internet archive
- Analysis of the DNS environment
- Discovery scanner
- Port scanner
- SNMP community scanner
- VNC attacks
- Other selected auxiliary modules
- Netcat

7 The exploiting phase
- Introduction to exploiting theme
- Metasploit console

8 The post-exploitation phase
- Basics of Meterpreter
- Properties and basic functions
- Post-exploitation modules
- Post-information gathering

- VNC connection
- Network enumeration
- Other selected modules
- Timestomp
- Expansion of privileges
- Running programmes from the memory
- Pivoting

9 Automation mechanisms
10 Special fields of application
11 Vulnerability scanner

Teaching and learning methods

- Seminar-based lesson along with practical exercises
- Internships

Remarks

Practical task (PrL) as eligibility criterion for the examination.

Recommended reading

- Messner, M.: Hacking mit Metasploit: Das umfassende Handbuch zu Penetration Testing und Metasploit, dpunkt.verlag GmbH; 3rd updated and expanded edition (30th October 2017), ISBN-13: 978-3864905230
- Brabetz, S.: Penetration Testing mit Metasploit: Praxiswissen für mehr IT-Sicherheit, mitp; 2018 edition (31st March 2018), ISBN-13: 978-3958455955
- Kofler, M., Zingsheim, A., et al.: Hacking & Security: Das umfassende Handbuch, Rheinwerk Computing; 1st edition (27th April 2018), ISBN-13: 978-3836245487
- Seitz, J.: Mehr Hacking mit Python: Eigene Tools entwickeln für Hacker und Pentester, dpunkt.verlag GmbH; 1st edition (1st September 2015), ISBN-13: 978-3864902864
- Noors, A.: Hacken mit Python und Kali-Linux: Entwicklung eigener Hackingtools mit Python unter Kali-Linux, Books on Demand; 1st edition (6th November 2018), ISBN-13: 978-3748165811

CY-B-27 Digital Forensics

Module no.	CY-B-27
Module coordinator	Prof. Dr. Michael Heigl
Course number and name	Digital Forensics
Lecturers	Prof. Dr. Michael Heigl
Semester	6
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Project work, practical task
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students should have fundamental, in-depth technical knowledge and methodological knowledge in the area digital forensics.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students know the terminology of digital forensics and can describe types of digital traces.
- They can explain the methodology and procedure of digital forensics.

- They can present the current legal status, as well as current standards and norms in the field of digital forensics.
- They understand the components of computer forensics, mobile and embedded forensics, as well as Internet forensics, and can conduct forensic investigations in these areas.

Methods expertise

- Students can distinguish between relevant and irrelevant information in a forensic investigation.
- For a given scenario, they can assess which steps of the digital forensics phases have to be carried out in which order.
- Students are able to independently plan and carry out digital forensics.

Personal skills

- The independent implementation of forensic investigations arouses the curiosity of students in the subject and promotes their willingness to deepen self-study.

Social skills

- By applying forensic methods in the context of group-based project work, students practise their willingness to cooperate and their motivational capability.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of the basic modules
- Knowledge of the content of module Network Security
- Knowledge of the content of module Management of IT Security Incidents

Content

1 Introduction
   - History of forensics
   - Terms
   - Approach
   - Documentation
   - Digital traces
   - Anti-forensics
2 The process of digital forensics
   - Identification phase
   - Recording phase
   - Investigation phase
   - Analysis phase
   - Presentation phase
3 Legal status, standards and norms
4 Digital forensics – use cases in detail
   - Data carrier forensics
   - Operating systems forensics
   - RAM forensics
   - (File)/Application forensics
   - Malware analysis & reverse engineering
   - Network forensics
   - Mobile device forensics
   - Cloud forensics
   - VM forensics
5 Challenges of digital forensics

Teaching and learning methods

- Seminar-based lesson along with practical exercises
- Internships

Remarks

Practical task (PrL) as eligibility criterion for the examination.

Recommended reading

- Geschonneck, A.: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag GmbH; 6th updated and expanded edition (1st March 2014), ISBN-13: 978-3864901331

- Meseke, B.: Digitale Forensik: Praxiswissen Cybercrime für Manager, Erich Schmidt Verlag GmbH & Co; 1st edition (27th June 2019), ISBN-13: 978-3503182671
- Kuhlee, L.: Computer-Forensik Hacks, O'Reilly Verlag GmbH & Co. KG; 1st edition (1 April 2012), ISBN-13: 978-3868991215
- Siegert, M.: Forensisches Reverse Engineering: Entwurf eines Teilgebietes der digitalen Forensik unter besonderer Berücksichtigung der Systemmodellierung, Books on Demand; 2nd edition (10th November 2017), ISBN-13: 978-3744815727
- Årnes, A.: Digital Forensics, Wiley; 1st edition (21st July 2017), ISBN-13: 978-1119262381

CY-B-28 Security of Interactive Systems

Module no.	CY-B-28
Module coordinator	Prof. Dr. Thomas Störtkuhl
Course number and name	Security of Interactive Systems
Lecturers	Prof. Dr. Thomas Störtkuhl
Semester	6
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	PrA
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students will obtain in-depth general and technical knowledge in the field of security of interactive systems.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students can describe various IoT or IIoT infrastructures and their components.
- They know the essential (security) elements of an IT security architecture for the various infrastructures discussed.

- Students know essential protocols and their security properties that are implemented in these environments.
- They are able to carry out security analyses for the IoT and IIoT infrastructures introduced.
- Students know the essential security requirements stipulated by the relevant standards that should apply to the IoT and IIoT infrastructures introduced.
- They can carry out audits for an object of investigation (IT system, part of an IT system, process).

Methods expertise

- Students can assess whether an IT security architecture provides sufficient protection for the infrastructures discussed or whether it has deficiencies.

Personal skills

- Through the exercises that take place, which involve the processing/presentation of specific topics, students are encouraged to work through facts independently and to present them in an understandable manner.

Social skills

- In a team, students carry out security analyses on case studies or design an IT security architecture. Through this collaboration, they see that the knowledge and skills of other students can be helpful and beneficial.

Applicability in this and other degree programmes

Advanced compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of module CY-B-04 Operating Systems and Networks
- Knowledge of the content of module CY-B-17 Network Security
- Knowledge of the content of module CY-B-11 Cryptology 1

- Knowledge of the content of module CY-B-21 Cryptology 2
- Knowledge of the content of module CY-B-22 Management of IT Security Incidents

Content

- Motivation for the security of interactive systems: the ever-increasing depth of system networking, for example, in the field of Industry 4.0; progressing integration of devices in networks and via communication platforms for new business models
- IT security in the IoT environment:
  - Typical infrastructures for IoT environments, for example in the field of MQTT or LoRaWan protocols; application of analyses to derive suitable IT security measures such as implementation of secured communication tunnels via TLS or IPsec. Representation of IT security architectures of communication platforms in the IoT environment.
- IT security in an industrial environment (IIoT, Industrial IoT):
  - Solutions for predictive maintenance and data analytics are shown. Cloud technologies are included here. Remarks, secure Machine2Machine communications and connections via platforms are explained.
    Various infrastructures from the areas of production (e.g., the use of OPC UA, defence-in-depth approaches such as those offered by manufacturers/system integrators), railways (train routing, train control, ERTMS (European Rail Traffic Management System)), chemistry (here, specifically, the wirelessHART protocol) and energy (e.g., MMS, standard IEC 62351) are presented along with their special features.
- Connection to a public key infrastructure:
  - Since many security protocols are based on certificates, the management of identities, certificates and rights in distributed infrastructures also poses a particular challenge. For example, an automatic roll-out of certificates via protocols such as Simple Certificate Enrolment Protocol (SCEP)/Network Device Enrollment Service (NDES) is explained.
- Network structuring:
  - For the integration of communication platforms and cloud services, suitable network structuring with network segments (zones) and communication channels (conduits) for securing communications is explained.
- Security Incident and Event Monitoring:

- Possibilities of technical Security Incident and Event Monitoring (SIEM) are presented, for example, using honeypot solutions or new approaches to monitoring using edge computing.

Teaching and learning methods

- Seminar-based lesson along with practical exercises

Recommended reading

- ZVEI – German Electrical and Electronic Manufacturers – Association, Industry 4.0: The Reference Architectural Model Industry 4.0 (RAMI 4.0), Frankfurt am Main, 2015
- Industrial Internet Consortium, Industrial Internet Reference Architecture. Link: http://www.iiconsortium.org/IIRA.htm (last accessed on 4.12.2020).
- ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, NOVEMBER 2017
- ENISA, Towards secure convergence of Cloud and IoT, TLP GREEN | SEPTEMBER 2018
- Fraunhofer AISEC: White Paper, IoT 2020: Smart and secure IoT platform, October 2003, link: r10secu.lo (cmu.edu) (last accessed on 4.12.2020).
- SANS Institute Information Security Reading Room, Tools and Standards for Cyber Threat Intelligence Projects, 2020, link: Tools and Standards for Cyber Threat Intelligence Projects (sans.org) (last accessed on 4.12.2020).
- Jin-Yong Yu, Young-Gab Kim: Analysis of IoT Platform Security: A Survey; 2019 International Conference on Platform Technology and Service (PlatCon)
- Security and Privacy in Sensor Networks, Haowen Chan and Adrian Perrig, Carnegie Mellon University,
- Klasen Frithjof, Oestreich Volker, Volz Michael (publisher): Industrielle Kommunikation mit Feldbus und Ethernet, VDE Verlag, Berlin, Offenbach, 2010
- BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. & Oesterreichs E-Wirtschaft, whitepaper Anforderungen an Österreich sichere Steuerungs- und Telekommunikationssysteme (Requirements for Secure Control and Telecommunications Systems in Austria), fully revised version 2.0 05/2018: Vienna/Berlin, 8th May 2018

- Security Analysis of Open Platform Communications Unified Architecture (OPC UA), on behalf of BSI published on: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/OPCUA/OPCUA.pdf
- Risikoanalyse industrieller Steuerungsumgebungen, itsecurity, (Risk Analysis of Industrial Control Environments, IT Security) July-August, 2014

CY-B-29 Security Engineering

Module no.	CY-B-29
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Security Engineering
Lecturers	Prof. Dr. Martin Schramm
Semester	6
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	PrA
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students will obtain a basic general and technical knowledge in the field of interdisciplinary security engineering.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students understand the principles of interdisciplinary security engineering and can also explain them.
- They can apply the security/privacy by design approach when implementing their own solutions.

- Students can carry out maturity assessments regarding the quality of processes when developing secure IT systems.

Methods expertise

- Students can analyse existing products and solutions for compliance with the principles of security engineering.
- Furthermore, they can evaluate these for security and decide which additional steps have to be taken for increased security.
- Students can assess which interdisciplinary team of specialists is necessary to cope with a specific challenge in cryptographic engineering or security engineering.

Personal skills

- Through exercises, students learn to work independently and in a manner oriented to problems and action.

Social skills

- Through group work on practical case studies, students develop the ability to work in a team and increase their goal and result orientation.

Applicability in this and other degree programmes

Compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of basic modules (CY-B-01 to CY-B-05, CY- B-08 to CY-B-11, CY-B-13 and CY-B-14)
- Knowledge of the content of module CY-B-16 Secure Programming
- Knowledge of the content of module CY-B-17 Network Security
- Knowledge of the content of module CY-B-21 Cryptology 2

- Knowledge of the content of module CY-B-22 Management of IT Security Incidents
- Knowledge of the content of module CY-B-23 Distributed Ledger Technologies

Content

1 Introduction
   - Thematic classification and definition of terms
   - Security engineering as a holistic approach
   - Comparison between software engineering – security engineering
2 Overview of the components of security engineering (excerpt)
   - Protocols
   - Access protection
   - Cryptography
   - Multi-level security
   - Multilateral security
   - Monitoring
   - Biometrics
   - Physical falsification protection
   - Copy protection and data protection
   - Processes, management and evaluation
3 Security engineering
   - Principles
   - Security in the development process
   - Maturity level model for quality assessment
   - Mechanisms, measures, tools
   - Evaluation and certification
4 Cryptographic engineering
   - Messaging security
   - Key agreement
   - Key management
   - Quality of random number generators
   - Side-channel attacks – basics
   - Side-channel attacks – advanced techniques
5 Current topics and (research) activities

Teaching and learning methods

- Seminar-based lesson along with practical exercises

Recommended reading

Literature:

- Anderson, S.: Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley; 3rd edition (22nd December 2020), ISBN-13: 978-1119642787
- Koc, C. K.: Cryptographic Engineering, Springer; softcover reprint of hardcover 1st ed. 2009 edition (4th November 2010), ISBN-13: 978-1441944177
- Ferguson, N., Schneier, B., Kohno, T., Cryptography Engineering: Design Principles and Practical Applications, Wiley; 1st edition (15th March 2010), ISBN-13: 978-0470474242

CY-B-30 Compulsory Elective Module 1

Module no.	CY-B-30
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Compulsory Elective Module 1
Semester	6
Duration of the module	1 semester
Module frequency	Annual
Course type	FWP (subject oriented elective)
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Type of examination of the selected module
Weight of the grade	5/210
Language of instruction	German

Module objectives

In compulsory elective modules, students can freely choose a module from a given module catalogue. Content is related to the study subject, e.g., from the subject areas of computer science, cyber security, artificial intelligence or other relevant modules. The module catalogue is always announced along with the curriculum.

This allows students to select the subjects that they want to focus on and learn in greater depth and/or that help expand their competencies.

The importance placed on professional skills and methods expertise, as well as on personal and social skills, differs according to the module selected.

Applicability in this and other degree programmes

In accordance with the module description of the selected compulsory module

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of the basic modules

Content

Content depends on the module selected.

Teaching and learning methods

In accordance with the module description of the selected compulsory module

Remarks

There is no claim that all available compulsory elective and optional modules will actually be offered. Likewise, there is no claim that the accompanying courses will be held when the number of participants is insufficient.

Recommended reading

In accordance with the module description of the selected compulsory module

CY-B-31 Key Qualification 5

Module no.	CY-B-31
Module coordinator	Prof. Dr. Thomas Geiß
Course number and name	Team Building and Intercultural Communication Starting a business
Lecturers	Eva Baumgartner Prof. Dr. Thomas Geiß Prof. Dr. Johann Nagengast
Semester	6
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Portfolio
Weight of the grade	5/210
Language of instruction	German

Module objectives

The learning outcomes of the module therefore consist of the two subjects "Team Building and Inter-cultural Communication" (Subject A) and "Starting a business" (Subject B).

Subject A

Learning outcomes of the module:

Cultural and interdisciplinary differences among international business partners, customers and suppliers often result in tension and misunderstandings in the IT world, specifically for individuals working in modern fields like Artificial Intelligence. Managers and team members who competently navigate in different cultural and disciplinary environments and teams can contribute substantially to the success of globally active enterprises.

A condition for the acquisition of "intercultural and interdisciplinary competence" is the recognition that one's own actions are influenced by one's own values and norms. Reflecting on one's own cultural and disciplinary background forms the basis for the understanding of other cultures and functions.

In the first part of the course, the participants acquire the knowledge they need to explain and understand various cultures and disciplines. Through the study of comparative cultures, they discover the relevance of the cultural framework to management theory and for explaining management and team behaviour.

Participants learn how to independently apply the "culture assimilator" technique to broaden their knowledge through a qualitative research project. This involves soliciting international and functional managers and employees and collecting "critical incidents" of cross-cultural and cross-functional business and team interactions, which are then analysed with the help of theory. Carrying out qualitative interviews with members of foreign cultures and functions further develops the participants' social, cross-functional and intercultural skills.

The second part of the course is conducted as an off-campus intensive "teambuilding and social, interdisciplinary and intercultural competence" training workshop. Here, the results of the culture-assimilator research projects are presented through role-playing in situational re-enactments. The implications are further clarified through a variety of interaction exercises. For example, simulation of expatriate and cross-functional team situations is used to transfer concrete practical knowledge.

The social, interdisciplinary, and intercultural competence training assists the participants in their ability to reflect on cultural and disciplinary identities, to avoid value judgements in their perception of foreign and functional cultures, to empathize and accept differences, as well as to develop additional options for the actions which international and cross-functional managers and employees can take.

In the context of the learning environment, the students enjoy the opportunity to increase their observation, communication, co-operation, self-reflection, teamwork, and management skills as well as their self-confidence. By working together to solve complex problems and through structured feedback sessions, the participants become sensitised to the roles they assume in group interactions, to the limitations imposed by the German and their own cultures, and to the conditions required for effective team work. The participants learn to influence the co-operation in team positively and learn how to avoid negative team atmospheres.

Subject B

Qualification goals

The importance of detailed corporate planning is illustrated using examples. In the process, students are given knowledge on the topic of business start-ups and motivated for it. Students are also given the opportunity to apply and practise the imparted knowledge by creating an individual business plan as part of a group project and thus to understand the process, possible problems, and limits of corporate planning based on a practical example. This course equips students with the 'starting block' with the help of entrepreneurial fundamentals, management knowledge and personal key qualifications to prepare them for the entrepreneurial race, and gives them knowledge on the topics of self-employment and business start-ups. Knowledge of identifying market opportunities and business models is also imparted, in addition to the theoretical knowledge of entrepreneurship. Expansion of practical knowledge gained from the start-up process > from the idea stage to the product/service stage and then to the business model stage. The group project encompasses the overall planning of a business idea from idea generation, information gathering to the creation of a detailed business plan. The commitment of participants and group dynamics during a project make a decisive contribution to the learning success.

Professional skills

Students are able to iteratively generate and evaluate solutions to a problem during the process of idea generation (design thinking process, Where2Play method). They can choose from a set of methods and question and analyse problems at a suitable point. They can implement their ideas in prototypes and test and evaluate them with their users.

Methods expertise

Students are able to assign methods to appropriate phases and apply them. The learning methods for this are: interactive seminar, problem-based learning, lectures/presentations on special aspects, self-organisation, coaching sessions with the lecturer. The aim is to integrate already existing knowledge and to find solutions with a high willingness to communicate.

Personal skills

The presented concepts and corporate examples allow a large scope for interpretation for possible solution alternatives. Each student has to independently develop strategy options for corporate governance and reflect on their effects.

Selected management tools are prepared as part of the group work, and presented during the course. Students also have a start-up mindset that enables them to understand disruptive problems and develop user-centred solutions.

Social skills

Students develop the ability to discuss and work in a team and their critical faculties. They are able to bring their strengths into the development process and business model designing and develop a creative self-confidence. The analysis of current company situations in teams leads to an in-depth exchange about different strategic concepts for corporate governance in the conflicting areas of financial value orientation and value-oriented corporate governance. Due to the heterogeneity of group opinions and standpoints in these discussions, students develop critical faculties and the ability to deal with conflict.

Applicability in this and other degree programmes

Applicability of the module for this programme

- This module is one of the interdisciplinary key qualifications.

Applicability of the module for other programmes

- This module can be used in all other technical, legal, business-psychology and business programmes.

Admission requirements and/or recommended prerequisites

No prerequisites.

Content

Subject A

- The following concepts are emphasised in theoretical discussions, research projects and in the practical training workshop:
  - Defining culture
  - The characteristics of culture
  - The functions of culture

- Organisational culture
- The layers and elements of culture
- Comparing cultures
- The impact on the individual: the "culture shock"
- Cultural contexts: Hall
- Culture and the workplace: Hofstede practical aspects of intercultural behaviour
- International human resource development
- Expatriate management
- Language and social reality
- Reasons for cross-cultural misunderstandings
- Improving cross-cultural cooperation
- Group dynamics, processes, and structures in groups
- Roles in groups (roles in tasks and supporting roles)
- Group leadership
- Effect of one's actions in groups
- The "give and take" of feedback
- Self-image and how others see you
- Communication levels (content versus relationship)
- Conditions for successful cooperation
- Cultural influences on teamwork.
- Team building

More topics are to be added based on the actual demand for graduates in this programme, evaluated constantly by qualitative and quantitative research of future employers

Subject B

The course builds on the fundamentals of corporate governance and motivates students to transfer their knowledge to specific case studies of business start-ups. Analytical instruments and solutions from the field of entrepreneurship research and various entrepreneurial functions are used in the process. Furthermore, the entrepreneurial decision-making paths and the consequences of entrepreneurial action are presented with a focus on companies from various industries.

- Competences relevant to start-ups
- Idea generation and evaluation of business ideas
- Structure and content of business plans
- Business models
- Venture capital and corporate financing
- Financial planning, scenario building and sensitivity analysis

- Investment planning and fixed-asset movement schedule
- Personnel planning
- Public subsidies
- Possibilities of limiting liability
- Liability for founders
- Practical application of theoretical knowledge when creating a business plan as part of a group project

Teaching and learning methods

Subject A:

The course begins by conveying the fundamentals of cross-cultural and interdisciplinary management, as well as team building via theoretical lectures and moderated discussions. Since most of the participants have teamwork, intercultural and interdisciplinary experience assembled from a wide variety of cultures and functions, the theory can be directly tied to many of the individual experiences.

The theoretical fundamentals are then extended through the development, application and presentation of the culture and functional assimilators. The qualitative research projects are performed in groups organised along the principles of self-organised learning. The projects help develop individual competence in applying the scientific method, and further the development of presentation, social and intercultural skills.

Short case studies, "critical incidents", are selected from the international and interdisciplinary business world. Explanations and analysis of these cases support the integration of the participants' existing management knowledge with intercultural and interdisciplinary perspectives.

Social, interdisciplinary and intercultural skills, as well as team building capabilities, are further developed in the training workshop through roll playing, interaction exercises, problem solving tasks, simulations and feedback rounds.

Subject B:

Lecture with exercises, seminar, writing workshop, presentations, discussions, teaching of the basics through case-related presentation. Systematic presentation of theory with method transfer, diagrams and case studies.

Remarks

Subject A:

Led by Prof. Dr. Johann Nagengast, the course implements a multi-cultural and multi-functional team teaching approach.

Mr. Florian Oberhofer offers expertise in expatriate management, global entrepreneurship and international human resources, and adds a foreign cultural and management perspective.

Various external tutors (carefully selected and already experienced in the content of this module) assure that the participants receive small group, qualified feedback.

The course is always conducted by two lecturers in order to ensure individual supervision for participants. If the number of participants is higher, a third lecturer may be called in, in coordination with the respective programme director.

Recommended reading

Subject A

- Hall, E. T., Hall, M. R.: Understanding Cultural Differences, reprint, Yarmouth, Intercultural Press (2015)
- Hofstede, G.: Cultures and Organizations, 2nd ed., New York et al., Mc Graw-Hill (2015)
- Hofstede, G.: Culture's Consequences, 2nd edition, Thousand Oaks, Sage, (2014)
- Trompenaars, F., Hampden-Turner, C.: Riding the Waves of Culture, London, Brealey Publishing, (1997)
- Trompenaars, F., Hampden-Turner, C.: Managing People across Cultures, Chichester, Capstone Publishing (2004)
- Lewis, R. D.: When Cultures Collide, 3rd ed. (or more current), London, Brealey Publishing (2006)
- Baron, R. S.: Group Process, Group Decision, Group Action, 2nd. Ed., Buckingham, 2003
- Buchanan, D., Huczynski, A.: Organizational Behavior, 5th Ed., Harlow, 2004

Subject B

- Koch, Wolfgang/Wegmann, Jürgen (2002): Praktiker-Handbuch Due Diligence, Analyse mittelständischer Unternehmen, 2nd revised and updated edition, Schäffer-Poeschel Verlag, Stuttgart 2002.

- Kreditanstalt für Wiederaufbau (KfW)-Akademie, (2004): Finanzierungsmöglichkeiten der KfW bei Unternehmensübernahmen und Beteiligungen, Frankfurt a. M. 2004, p. 32-34.
- Timmons, Jeffrey A.: New venture creation, McGraw-Hill Verlag, Boston, 2004
- Sahlman, William A.: The entrepreneurial venture, Havard Business School Press, Boston, 1999
- Dowling, Michael J.: Gründungsmanagement, Springer Verlag, Berlin, 2003
- Bernd Fischl/Stefan Wagner: Der perfekte Businessplan, 2010 – Verlag Franz Vahlen GmbH
- C. Bayerl; 30 Minuten für Kreativitätstechniken; GABAL Verlag GmbH; 3rd edition 2007; Offenbach
- G. Bayer; G.R. Berrit; Diagnose der Innovationbedingungen im Unternehmen; Digitale Fachbibliothek Innovationsmanagement; Symposium Publishing GmbH; 2007
- A. Blumenschein; I.U. Ehlers; "Ideen managen"; Rosenberger Fachverlag; Leonberg; 2007
- BPW Nordbayern GmbH Schritt für Schritt wachsen - finanzieren - gründen - planen; participant handbook 2020; 4th revised edition;
- Pott, Oliver, Pott, André: Entrepreneurship, Unternehmensgründung, Businessplan und Finanzierung, Rechtsformen und gewerblicher Rechtsschutz, Poeschl-Verlag, 2017
- A. Förster; P. Kreuz; Different Thinking; Redline Wirtschaft; Frankfurt 2005
- Engelen Andreas: Corporate Entrepreneurship, paperback, 2014, Gabler.
- Fritsch Michael: Entrepreneurship, Theorie, Empirie, Politik, Engelen, Bachmann, Springer, 2017

CY-B-32 Auditing of IT Systems

Module no.	CY-B-32
Module coordinator	Prof. Dr. Thomas Störtkuhl
Course number and name	Auditing of IT Systems
Lecturers	Prof. Dr. Thomas Störtkuhl
Semester	7
Duration of the module	1 semester
Module frequency	Annual
Course type	Compulsory course
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	PrA
Weight of the grade	5/210
Language of instruction	German

Module objectives

Students will obtain in-depth general and technical knowledge in the field of auditing of IT systems.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- Students can describe all steps of an auditing process for the information security of IT systems/IACS/processes.
- They know all the essential steps/phases of the auditing process, and can apply auditing processes to IT systems, IACS and processes.

- Students know the essential requirements for an auditing process that are stipulated by relevant standards.
- They can carry out audits for an object of investigation (IT system, part of an IT system, process).

Methods expertise

- Students can select the correct type and appropriate procedure of an audit for an object of investigation (IT system, part of an IT system, process) and evaluate the criticality of identified deficiencies.
- Students can assess whether certain measures are suitable for eliminating or mitigating identified deficiencies/vulnerabilities/findings.

Personal skills

- Through the exercises that take place, students are encouraged to work through facts independently and to present them in an understandable manner.

Social skills

- Students conduct audits in a team in changing roles using case studies. Through this collaboration, they see that the knowledge and skills of other students can be helpful and beneficial.

Applicability in this and other degree programmes

Advanced compulsory elective module of other bachelor's programmes (for example: Applied Computer Science/Infotronics, Interactive Systems/Internet of Things, Artificial Intelligence, Business Informatics, Electrical Engineering and Information Technology)

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of module CY-B-04 Operating Systems and Networks
- Knowledge of the content of module CY-B-17 Network Security

Content

- Motivation for auditing IT systems: management of information security; current situation of information security; regulatory requirements at a national and European level; protection of critical infrastructures
- Types of audits: technical audits, management audits, audits of processes, penetration tests, audit of documents, management review, certification audits.
- Methods: round table simulation, interview, workshop, technical vulnerability audit
- Elements of the audit processes of various types of audits such as preparation, implementation, logging and reporting, involvement of various roles/stakeholders. Remarks, it is seen how an audit can be used as a control instrument in the event of outsourcing.
- Definition and evaluation of the maturity level of processes: an auditing process not only identifies vulnerabilities, but also assesses the maturity level of audited processes using clearly defined criteria. For this purpose, the requirements for processes as stipulated by relevant standards (see below) are used.
- Embedding of audits in the continuous improvement process for information security and in the reporting system according to the IT Security Act. The focus here is on:
  - the audit process for the management of information security; ISO 19011, for example, is introduced as the basis
  - the development of products with the quality IT security; the standard IEC 62443-4-1, for example, is used here as the basis
  - certification audits (ISO/IEC 27001 and IEC 62443) for operators, system integrators and manufacturers

Teaching and learning methods

- Seminar-based lesson along with practical exercises

Recommended reading

- DIN EN ISO 19011, Guidelines for Auditing Management Systems (ISO 19011:2011); German and English version EN ISO 19011:2011, December 2011

- ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary, third edition, 2014-01-15
- ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 + Cor. 1:2014), English translation of DIN ISO/IEC 27001:2015-03
- ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls, second edition, 2013-10-01
- ISO/IEC 27005:2018-07 Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement, English title: Information technology – Security techniques – Information security risk management
- IT Basic Protection Compendium, Federal Office for Information Security, Bonn 2020; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html (last accessed on 3.10.2020)
- ISO/IEC 21827: Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®), 2008
- DIN ISO 31000:2018-10: Risikomanagement – Leitlinien (ISO 31000:2018), English title: Risk management – Guidelines (ISO 31000:2018), 2018-10
- ENISA, GOOD PRACTICES FOR SECURITY OF IOT, Secure Software Development Lifecycle, November 2019
- ENISA, IoT Security Standards Gap Analysis, Mapping of existing standards against requirements on security and privacy in the area of IoT, V1.0, December 2018
- IEC 62443 certification for manufacturers and system integrators, Kai Wollenweber, Thomas Störtkuhl, Special it-sa, October 2015

CY-B-33 Compulsory Elective Module 2

Module no.	CY-B-33
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Compulsory Elective Module 2
Semester	7
Duration of the module	1 semester
Module frequency	Annual
Course type	FWP (subject oriented elective)
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Type of examination of the selected module
Weight of the grade	5/210
Language of instruction	German

Module objectives

In compulsory elective modules, students can freely choose a module from a given module catalogue. Content is related to the study subject, e.g., from the subject areas of computer science, cyber security, artificial intelligence or other relevant modules. The module catalogue is always announced along with the curriculum.

This allows students to select the subjects that they want to focus on and learn in greater depth and/or that help expand their competencies.

The importance placed on professional skills and methods expertise, as well as on personal and social skills, differs according to the module selected.

Applicability in this and other degree programmes

In accordance with the module description of the selected compulsory module

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of the basic modules

Content

Content depends on the module selected.

Teaching and learning methods

In accordance with the module description of the selected compulsory module

Remarks

There is no claim that all available compulsory elective and optional modules will actually be offered. Likewise, there is no claim that the accompanying courses will be held when the number of participants is insufficient.

Recommended reading

In accordance with the module description of the selected compulsory module

CY-B-34 Compulsory Elective Module 3

Module no.	CY-B-34
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Compulsory Elective Module 3
Semester	7
Duration of the module	1 semester
Module frequency	Annual
Course type	FWP (subject oriented elective)
Level	Undergraduate
SWS	4
ECTS	5
Workload	Contact hours: 60 hours Self-study: 90 hours Total: 150 hours
Type of Examination	Type of examination of the selected module
Weight of the grade	5/210
Language of instruction	German

Module objectives

In compulsory elective modules, students can freely choose a module from a given module catalogue. Content is related to the study subject, e.g., from the subject areas of computer science, cyber security, artificial intelligence or other relevant modules. The module catalogue is always announced along with the curriculum.

This allows students to select the subjects that they want to focus on and learn in greater depth and/or that help expand their competencies.

The importance placed on professional skills and methods expertise, as well as on personal and social skills, differs according to the module selected.

Applicability in this and other degree programmes

In accordance with the module description of the selected compulsory module

Admission requirements and/or recommended prerequisites

Admission requirements:

- No specific requirements

Recommended prerequisites:

- Knowledge of the content of the basic modules

Content

Content depends on the module selected.

Teaching and learning methods

In accordance with the module description of the selected compulsory module

Remarks

There is no claim that all available compulsory elective and optional modules will actually be offered. Likewise, there is no claim that the accompanying courses will be held when the number of participants is insufficient.

Recommended reading

In accordance with the module description of the selected compulsory module

CY-B-35 Bachelor’s module

Module no.	CY-B-35
Module coordinator	Prof. Dr. Martin Schramm
Course number and name	Bachelor’s Thesis, Bachelor’s Seminar
Semester	7
Duration of the module	1 semester
Module frequency	As required
Course type	Compulsory course
Level	Undergraduate
SWS	2
ECTS	15
Workload	Contact hours: 30 hours Self-study: 420 hours Total: 450 hours
Type of Examination	Colloquium, Bachelor’s thesis
Weight of the grade	30/210
Language of instruction	German

Module objectives

Students should be able to apply the knowledge, abilities and skills acquired during studies methodically and in context in an extensive project from the field of cyber security. Students should be able to independently structure a problem, systematically process it using scientific methods and, finally, document it transparently within a given period of time. In the concluding presentation, the project and work results must be presented in a way that is appropriate for the target group. In the bachelor’s thesis, students prove that they have completed their bachelor’s studies successfully and acquired the ability for independent academic work.

Specifically, students will have achieved the following learning outcomes after completing this module:

Professional skills

- By working on the bachelor's thesis topic, students gain in-depth specialist knowledge of the respective topic of focus.
- They gain the competence to independently apply the knowledge and skills acquired during their studies to complex tasks and to present them in an appropriate written form.

Methods expertise

- Through the planning of work steps, as well as their execution and conclusion in the form of a document, students gain the ability to complete an extensive project independently and successfully.

Personal skills

- By completing the bachelor's module, students develop a high degree of personal responsibility, self-discipline, self-reflection and self-confidence.

Social skills

- Bachelor's theses are often written in cooperation with companies in the region. By working as part of a project team from a company, students develop the ability to master a personal challenge in a social context.
- Students can solve an extensive task and develop an argumentation/strategy to represent and defend their thesis.

Applicability in this and other degree programmes

It is a special module for this course

Admission requirements and/or recommended prerequisites

Formal:

- Pursuant to § 11 of the study and examination regulations, anyone who has successfully completed the modules in the Foundational and Orientation Examinations and has acquired a minimum of 120 ECTS credits can apply for the bachelor's thesis.

Content-related:

- Knowledge of course content

Content

A bachelor's thesis is a written composition on an individual topic. It is issued, supervised and evaluated by an authorised examiner in the programme (professor, lecturer). The student can make suggestions for the topic. The bachelor's thesis must be prepared within 6 months. During the final thesis, a colloquium is organised in the form of a seminar (oral presentation). Students have to defend their thesis during the colloquium.

Teaching and learning methods

Guidance on independent work using scientific methods

Remarks

- The bachelor's thesis can be written in German or English in coordination with the examiner.
- The bachelor's thesis must be prepared within 6 months.
- The bachelor's thesis must be written in accordance with the guidelines of the Framework Examination Regulations (RaPO) and General Examination Regulations (APO) of Deggendorf Institute of Technology.

Recommended reading

- Individual, depending on the specific topic.

The thesis must contain a complete list of the literature used, as well as gathered information and other sources. The following literature should be referred to for formal requirements:

- Lück, W. (1990), Technik des wissenschaftlichen Arbeitens, 4th edition, Oldenbourg, Munich, p. 10ff.
- Lück, W., Henke, M. (2009), Technik des wissenschaftlichen Arbeitens, Seminararbeit, Diplomarbeit, Dissertation, 10th revised and extended edition, Oldenbourg, Munich