Module handbook Master's degree program (M.Sc.) **Cyber Security** Full-time / part-time

Status: March 2019

This translation serves to inform our international students. The valid legal reference can be found in the original „Studien- und Prüfungsordnung für den Masterstudiengang Digital Business Modelling and Entrepreneurship (Vollzeit / Teilzeit) an der Hochschule der Bayerischen Wirtschaft für angewandte Wissenschaften“

Contents

Glossary

BP	Work placement
BS	Block seminar
ECTS	European Credit Transfer System
BL	Blended learning
GA	Group work
GBWL	Fundamentals of business administration
HA	Term paper
KO	Colloquium
KR	Short presentation
LN	Proof of performance
LP	Credit point
LVA	Course
LVF	Type of course
MoP	Module examination
mP	Oral examinations
PA	Project work
PL	Practice-oriented courses
PR	Presentation
PZ	Attendance time
R	Unit
S	Seminar
SK	Language courses
SoSe	Summer semester
SP	Study Plus
sP	Written examinations
SPJ	Study project
SSt	Self-study
SWS	Semester hours per week
UE	Exercise
VL	Lecture
ECONOMICS	Economics
winter semester	Winter semester
WL	Workload

Introductory information about studying at the HDBW

Objective	Students are able to deal with a topic conceptually comprehensively and in depth and to apply the theoretical knowledge gained to a practical problem
Information options	Prospective students can find basic information about the course content, course structure and procedure, application and examination matters at www.hdbw-hochschule.de. Subject-specific study advice, in particular with regard to the content of the course and options, is provided by the subject advisors of the respective departments.
Study and examination regulations	Knowledge of and compliance with the examination regulations is essential for a successful course of study. Examination regulations are available for download at www.hdbw-hochschule.de.
Lecture language	Lectures can be offered in German or English. A language level B2 or adequate proof must be provided by the student.
Course structure Modules Course content Courses	The full-time degree program is designed for a standard period of study of of 3 semesters, in part-time mode 5 semesters. Each module consists of one or more courses (lecture, seminar, exercise, etc.). These include compulsory and compulsory elective courses. Detailed descriptions of the module and course content can be found in the module handbook of the respective degree program.
Credit points / Workload	The Master's degree program comprises 90 ECTS points. Credit points (CP) are awarded for the workload associated with each module in accordance with the European Credit Transfer System (ECTS). In general, 30 hours of work = 1 CP. Each module is completed by a module examination (MoP), which consists of course-related assessments (LN). LN are usually graded. A performance is deemed to have been passed if it has been assessed with a grade of at least 4.0. 20 CP are awarded for the final module (18 for the Master's thesis and 2 for the defense). Detailed descriptions of the LN required per module can be found in the module handbook of the respective degree program. Regulations on the forms of examination can be found in the study and examination regulations of the respective degree program. The workload in full-time study is approx. 900 hours (30 ECTS per semester), in part-time mode approx. 600 hours (20 ECTS per semester).
Lecture and examination period	The lecture period lasts 16 weeks. The winter semester (WiSe) usually begins at the beginning of October. The summer semester (SoSe) usually begins in mid-March. The examination period takes place from the 16th to 18th week of lectures (1st examination date). The make-up date usually takes place in the last two weeks of the semester break or after announcement (2nd examination date).
Recognition periods of study and practical activities	The examination board is responsible for the recognition of periods of study and practical activities.
Examinations and Repetition of examinations	Students are automatically registered for the examinations of the respective semester. Cancellations must be sent to the degree program administration.

Content of the degree program

The Master's degree program is assigned to the "application-oriented" profile type. The program therefore includes the following qualification objectives:

1. Students are familiar with the various system and network architectures and can assess them in terms of their security and potential threats.

2. Students master the essential theoretical principles of encryption and their practical application.

3. Students know methods and tools that can be used to attack the various systems.

4. Students use methods and tools to detect, protect and defend against attacks at various levels and in various ways and are familiar with disaster recovery procedures.

5. Students know the importance of security throughout the entire life cycle of applications and are able to implement cyber security requirements from design to end-of-life.

6. Students know the essential organizational and legal aspects in a national and international context as well as the requirements for governance and compliance that are relevant in the field of cyber security and are familiar with the latest approaches, e.g. from artificial intelligence, and their possible applications in cyber security.

7. Students have an application-oriented understanding of the aspects listed and are able to implement them independently as employees in a responsible position in the field of cyber security, both technically and organizationally.

Structure of the degree program

The Master's degree program in Cyber Security comprises 90 ECTS credits with a total workload (WL) of 2700 hours.

The course consists of a core area for all students with 55 ECTS and two elective focus areas "Technology" and "Organization and Management" with 15 ECTS each. The courses are very application-oriented. All courses follow a clear pattern in their didactic concept:

1. In each course, the relevant theoretical and conceptual foundations of the respective subject are taught on the basis of the current state of science and practice.

2. Practical course components (e.g. speakers from the field, case study discussions) are used to create an application-oriented basic understanding.

3. All courses are interactive and include assessed or unassessed project work components of varying degrees. As this is the philosophy of the entire, application-oriented Master's program and each course, an explicit separation between lectures and exercises was deliberately avoided.

4. The involvement of international lecturers ensures that the global nature of digital technologies and business models is also reflected in the teaching content.

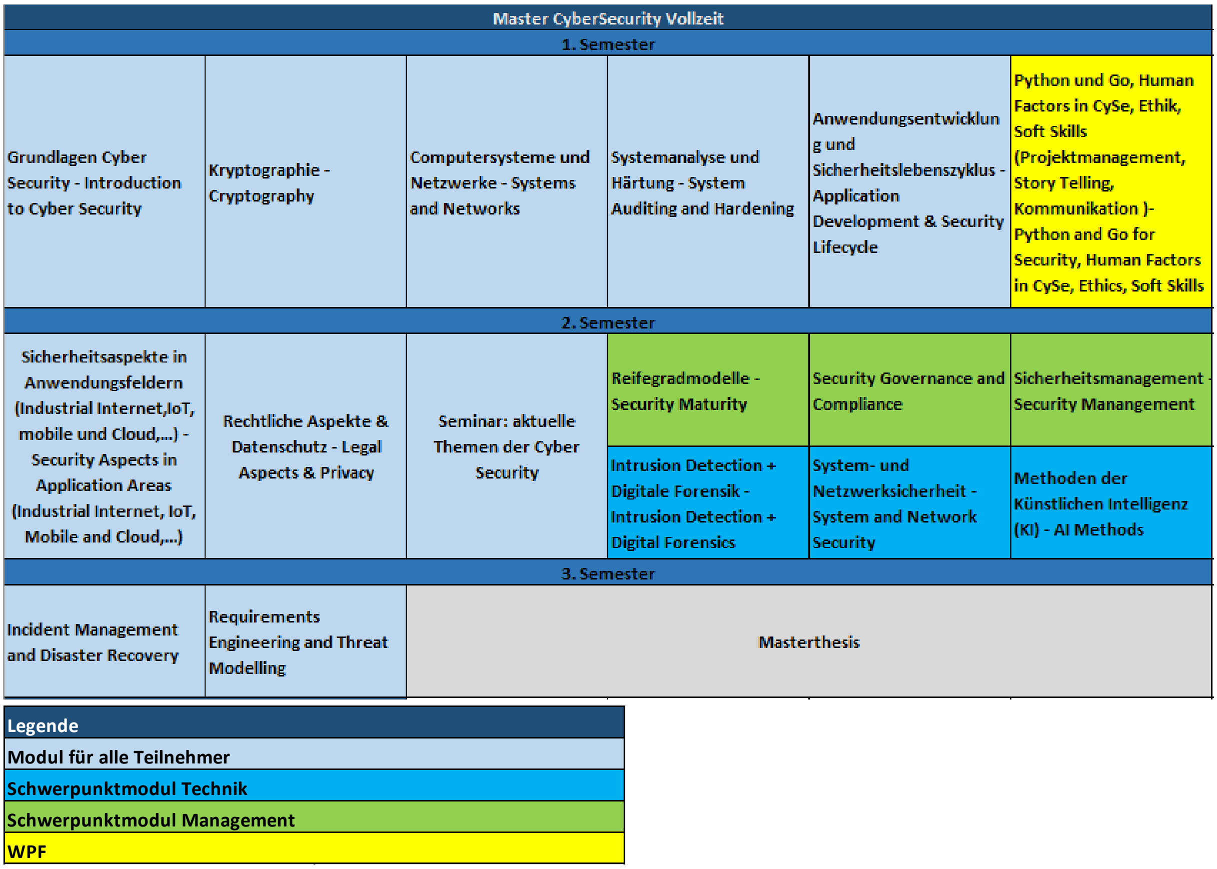
Master's thesis

The program concludes with a Master's thesis, in the course of which students should demonstrate that they are able to deal with a topic in a conceptually comprehensive and in-depth manner and apply the theoretical knowledge gained to a practical business issue. The Master's thesis therefore consists of the following three components:

1. The independent preparation of a Master's thesis of up to 80 pages.

2. The defense and presentation of the results of the Master's thesis with an examination discussion in which the content of the Master's thesis is also linked to other content of the degree program. The duration should not exceed 10 minutes. The total duration of the defense may not exceed 30 minutes.

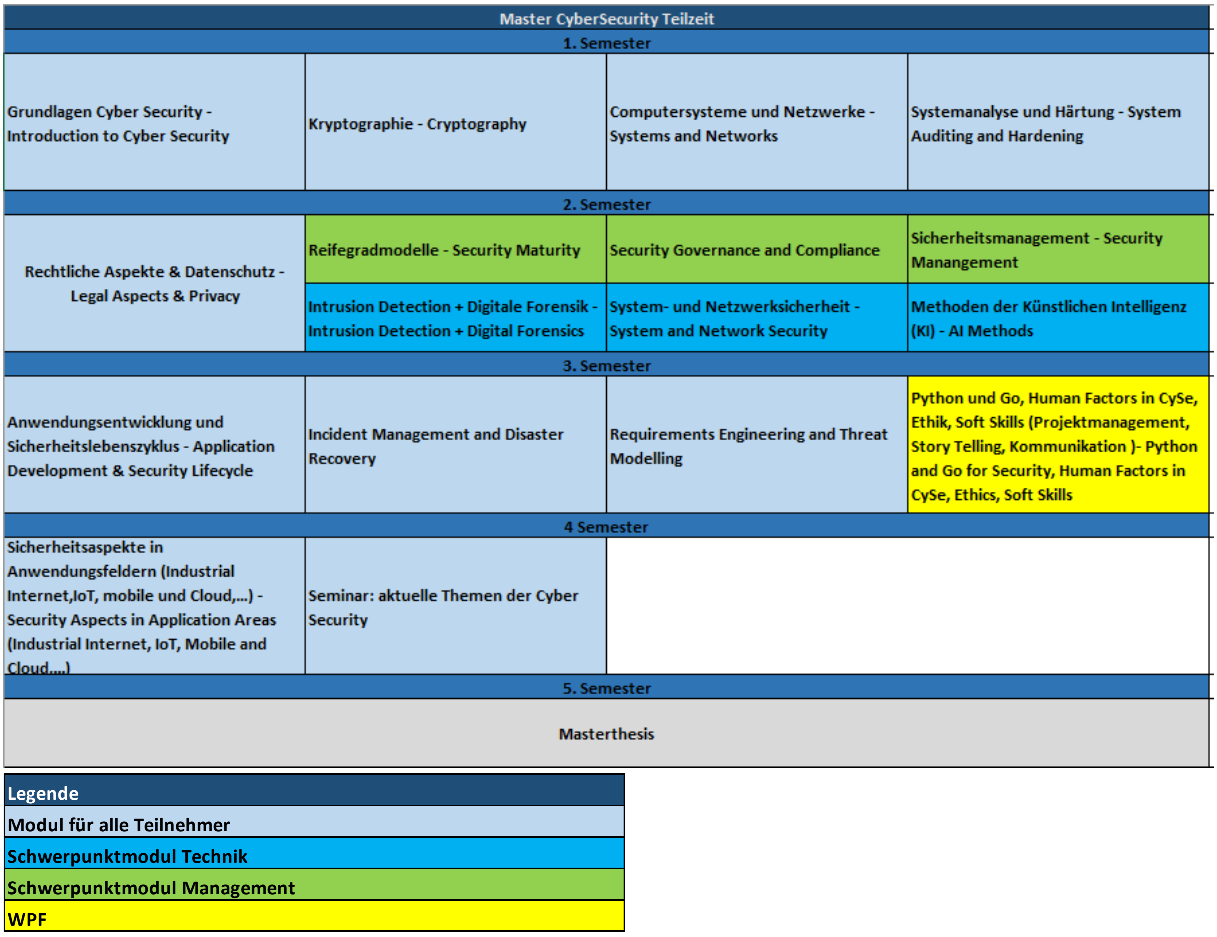
The following diagrams provide an overview of the full-time and part-time structure of the degree program:



Master CyberSecurity Vollzeit					
1. Semester					
Grundlagen Cyber Security - Introduction to Cyber Security	Kryptographie - Cryptography	Computersysteme und Netzwerke - Systems and Networks	Systemanalyse und Härtung - System Auditing and Hardening	Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	Python und Go, Human Factors in CySe, Ethik, Soft Skills (Projektmanagement, Story Telling, Kommunikation)- Python and Go for Security, Human Factors in CySe, Ethics, Soft Skills
2. Semester					
Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	Seminar: aktuelle Themen der Cyber Security	Reifegradmodelle - Security Maturity	Security Governance and Compliance	Sicherheitsmanagement - Security Manangement
			Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics	System- und Netzwerksicherheit - System and Network Security	Methoden der Künstlichen Intelligenz (KI) - AI Methods
3. Semester					
Incident Management and Disaster Recovery	Requirements Engineering and Threat Modelling	Masterthesis			

Legende
Modul für alle Teilnehmer
Schwerpunktmodul Technik
Schwerpunktmodul Management
WPF

Figure 1 - Studying full-time



Master CyberSecurity Teilzeit			
1. Semester			
Grundlagen Cyber Security - Introduction to Cyber Security	Kryptographie - Cryptography	Computersysteme und Netzwerke - Systems and Networks	Systemanalyse und Härtung - System Auditing and Hardening
2. Semester			
Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	Reifegradmodelle - Security Maturity	Security Governance and Compliance	Sicherheitsmanagement - Security Manangement
	Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics	System- und Netzwerksicherheit - System and Network Security	Methoden der Künstlichen Intelligenz (KI) - AI Methods
3. Semester			
Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	Incident Management and Disaster Recovery	Requirements Engineering and Threat Modelling	Python und Go, Human Factors in CySe, Ethik, Soft Skills (Projektmanagement, Story Telling, Kommunikation)- Python and Go for Security, Human Factors in CySe, Ethics, Soft Skills
4 Semester			
Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	Seminar: aktuelle Themen der Cyber Security		
5. Semester			
Masterthesis			

Legende
Modul für alle Teilnehmer
Schwerpunktmodul Technik
Schwerpunktmodul Management
WPF

Figure 2 - Part-time study model

Types of courses

Lectures* (VL)
Lectures serve to impart theoretical knowledge, which is usually supplemented by exercises or laboratory lessons. As a rule, they are 2 hours per week per semester. Lecture notes and slides can be made available to students online on the corresponding platform. Lectures usually end with an examination. The type of examination is determined by the respective lecturer

Seminars* (S) and block seminars* (BS)
Seminars are interactive courses in which small groups work together on various topics and teaching content. Components of the collaboration are, for example, exercises, discussions and presentations. Seminars conclude either with the writing of a presentation, the completion of a term paper or a written examination. Active participation is a prerequisite for successful completion of the course. Block seminars use the same teaching methods as seminars. In contrast to normal seminars, however, block seminars generally comprise a workload of 8 hours and take place on fixed days.

Exercises* (UE)
Exercises mainly serve to support lectures. Depending on the module, they can also be offered without an associated lecture. Theoretical knowledge is repeated and consolidated through exercises. As a rule, they take place in the form of face-to-face lectures and take up to 2 hours per week per semester, but can also be offered in the form of blended learning. Active participation is a prerequisite for successful completion of the course.

Language courses* (SK)
As the name suggests, language courses are exclusively geared towards the acquisition of a foreign language. The teaching format is similar to that of seminars and is characterized in particular by interactive teaching methods. Performance assessments often take the form of papers or presentations, for example. Language courses can also take place as block courses. The following also applies here: active participation is advisable in order to pass the module.

Practice-oriented courses* (PL)
Practice-oriented courses serve to acquire subject-specific application knowledge and key qualifications. As a rule, they include the same teaching methods as seminars and tutorials. They can also take the form of excursions, workshops and training sessions.

All course types marked with * are offered in the didactic concept of blended learning (BL). Blended learning events serve to present and process larger areas of material, which is why they also take place as part of lectures and often as a supplement to exercises. However, they also serve to deepen theoretical content with case studies and exercises. Blended learning events include all teaching methods in the form of both face-to-face and virtual events. The learning management system (LMS) can be used to provide participants with various learning materials such as scripts and tutorials as well as audios and videos. The detailed description of the course and the dates for the face-to-face events are made available at the beginning of each semester in the LMS and from the relevant student advisor. Tutors are available throughout the semester to answer questions about content and organization.

Study project (SPJ)

Study projects are courses with an increased workload. They are carried out, for example, as part of a research project or group work and particularly promote the independent application of typical research working methods, which is why they are often used to find topics for final theses. Study projects are implemented in the sense of independent study and therefore generally do not require fixed attendance times.

Self-study (SSt)

Self-study is used for the independent preparation and follow-up of lectures and is a prerequisite for all modules.

Colloquium (KO)

Colloquia generally comprise interactive discussion rounds during which topics are presented and discussed. They always take place as face-to-face events. They often serve to support students in writing their Bachelor's thesis.

Learning Management System (LMS)

The learning management system (LMS) is an electronic, web-based system that presents course content in a structured form on a platform and provides teachers and participants with interactive functions for collaborative work. It includes participant administration, document management, performance measurement functions, calendar functions and the option of integrating interactive learning units. Further information on the LMS can be obtained from the student advisory service of the respective department.

Proof of performance

Module examination (MoP)

Each module can consist of one or more courses (LVA). There is one module examination (MoP) per module, which may comprise the components of one or more courses. The MoP can consist of different assessments (LN). These can be of a course-related nature or be completed during the examination period at the end of the semester. The module grade is calculated from the performance achieved in the MoP according to the scheme announced at the beginning of the module. The following forms of examination can be used as LNs as part of the MoP (the prescribed form of examination can be found in the handbook for each module):

Written examinations (sP)

Written examinations usually last 60 minutes and take place at the end of the semester. They are usually set and assessed by the lecturers of the relevant courses. For written examinations, students must generally carry their student ID with them, including an official photo ID.

Oral examinations (mP)

Oral examinations take place either individually or in groups. Depending on the importance of the examination, they last a minimum of 15 and a maximum of 60 minutes. They usually take place towards the end of the semester.

Term paper (HA)

Term papers are written assignments on a topic agreed with the responsible professor. They can be between 5 and 25 DIN A4 pages in length. The maximum processing time for term papers is four weeks. They can usually be completed during the lecture-free period, although it is advisable to complete them during the semester in order to reduce the examination stress at the end of the semester.

Unit (R)

Presentations are an oral examination in which a topic previously agreed with the responsible lecturer is presented to fellow students in the course. The content should be scientifically researched. All theses of the presentation should be summarized on a thesis ball for the fellow students. The duration of a presentation is between 20 and 45 minutes, depending on the agreement with the responsible lecturer. Presentations can also be prepared and given in groups. It is usually supplemented by a written elaboration in the form of a term paper.

Short presentation (KR)

Short papers differ from presentations only in terms of their length: they last a maximum of 10 minutes. All other aspects are the same.

presentation (PR)

Presentations can be carried out either as individual work or in the form of group work. The results of the work are presented to fellow students and the head of the relevant course. In contrast to the presentation, the presentation is more extensive in terms of content, methodology and presentation.

Project work (PA)
Project work can be completed as a term paper or as a presentation. The topic of the project work is determined in advance with the responsible lecturer. Project work can be carried out either as individual work or in the form of group work.

The form of the examination is determined at the beginning of the semester by the lecturer responsible for the module and communicated on an HDBW information system accessible to students.

Further details on examination types, duration and conditions can be found in the current Study Examination Regulations (SPO) of the degree program or the General Examination Regulations (APO) of the university.

Literature

The lecturer of the respective course determines which accompanying literature is required before the start of the semester. This information will be announced at the beginning of the course or via the LMS. Further supporting materials (e.g. scripts, exercises, lecture slides , etc.) will be made available in good time via the LMS and this handbook.

Module overview

MoNo.	*Modules with courses*	*LVF*	*V*	*SWS*	*MoP*	*LP**	*Sem VZ*	*Sem TZ*
CSM1	**Basics of Cyber Security - Introduction to Cyber Security**				**sP**	**5**	**1**	**1**
CSM1	Basics of Cyber Security - Introduction to Cyber Security	VL/UE	P	4				
CSM2	**Cryptography - Cryptography**				**sP**	**5**	**1**	**1**
CSM2	Cryptography - Cryptography	VL/UE	P	4				
CSM3	**Computer Systems and Networks - Systems and Networks**				**sP**	**5**	**1**	**1**
CSM3	Computer Systems and Networks - Systems and Networks	VL/UE	P	4				
CSM4	**System Analysis and Hardening - System Auditing and Hardening**				**PA**	**5**	**1**	**1**
CSM4	System Analysis and Hardening - System Auditing and Hardening	VL/UE	P	4				
CSM5	**Application Development and Security Lifecycle - Application Development & Security Lifecycle**				**sP**	**5**	**1**	**3**
CSM5	Application Development and Security Lifecycle - Application Development & Security Lifecycle	VL/UE	P	4				
CSM6	**Compulsory elective module**					**5**	**1**	**3**
CSM6-1	Python and Go - Python and Go	VL/UE	WP	2	**PA**	**2,5**	**1**	**3**
CSM6-2	Human Factors in Cyber Security	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**
CSM6-3	Ethics - Ethics	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**
CSM6-4	Softskills - Softskills	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**
CSM7	**Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)**				**PA**	**5**	**2**	**4**
CSM7	Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and	PA	P	4				

	Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)							
CSM8	**Legal aspects & data protection - Legal Aspects & Privacy**				**sP**	**5**	**2**	**2**
CSM8	Legal aspects & data protection - Legal Aspects & Privacy	VL/UE	P	4				
CSM9	**Seminar: current topics in cyber security**				**PA**	**5**	**2**	**4**
CSM9	Seminar: current topics in cyber security	VL/UE	P	4				
Technology elective area								
CSMT1	**Intrusion Detection + Digital Forensics - Intrusion Detection + Digital Forensics**				**PA**	**5**	**2**	**2**
CSMT1	Intrusion Detection + Digital Forensics - Intrusion Detection + Digital Forensics	VL/UE	P	2				
CSMT2	**System and Network Security - System and Network Security**				**PA**	**5**	**2**	**2**
CSMT2	System and Network Security - System and Network Security	VL/UE	P	4				
CSMT3	**Methods of artificial intelligence (AI)**				**sP**	**5**	**2**	**2**
CSMT3	Methods of artificial intelligence (AI)	VL/UE	P	4				
Compulsory elective area Organization and Management								
CSMO1	**Maturity models - Security Maturity**				**sP**	**5**	**2**	**2**
CSMO1	Maturity models - Security Maturity	VL/UE	P	2				
CSMO2	**Security Governance and Compliance**				**sP**	**5**	**2**	**2**
CSMO2	Security Governance and Compliance	VL/UE	P	4				

CSMO3	**Security Management - Security Manangement**				**sP**	**5**	**2**	**2**
CSMO3	Security Management - Security Manangement	VL/UE	WP	4				
CSM10	**Incident Management and Disaster Recovery**				**PA**	**5**	**3**	**3**
CSM10	Incident Management and Disaster Recovery	VL/UE	WP	4				
CSM11	**Requirements Engineering and Threat Modeling**				**sP**	**5**	**3**	**3**
CSM11	Requirements Engineering and Threat Modeling	VL/UE	WP	4				
CSMMT	**Master thesis**						**3**	**5**
CSMMT1	Master's thesis	SSt	P		**HA**	**18**		
CSMMT2	Verteidigung / defense	mP	P		**mP**	**2**		

Module descriptions

Basics of Cyber Security - Introduction to Cyber Security	
Module number	**CSM1**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Prof. Dr. Sabine Rathmayer, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	Students gain an insight into the various aspects of cyber security and are able to understand the significance and interrelationships of various technical and organizational factors influencing cyber security. With the knowledge they have acquired, students can carry out systematic assessments of protection requirements and security levels. - modern IT systems, - IT infrastructures and - OT (Operational Technology) which also includes non-technical factors that are often underestimated in practice. Here, a distinction is made between small, medium-sized and large companies. In addition, an understanding of the various stakeholder groups and their motivation also plays an important role.
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: Classic methods of technical and organizational information security, including - Threats and hazards, risk analyses - BSI IT baseline protection - Basics of applied cryptography - Security Engineering - Security models and mechanisms and their implementation in distributed systems and computer networks - Security of mobile devices - Practical aspects of information security - Security incident response with breach and malware analysis - Social engineering: the human factor in information security from an attacker's perspective - Identity & access management, data protection and privacy - Security of outsourced services (e.g. in cloud computing)
Literature	- Whitman, M.; Mattord, H.: Principles of Information Security, 5th Edition, Cengage Learning, Boston 2016 - Graham, J.; Howard, R.; Olson, R.: Cyber Security Essentials, CRC Press, Boca Raton 2011 - Voeller, J.: Cyber Security, Wiley 2014
Other information	Working in small groups can make up part of the contact time.

Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	Digital Technology (MA)
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Cryptography - Cryptography	
Module number	**CSM2**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Dr. Stephan Spitz , other lecturers as required
Frequency of the offer	Every academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	In this introduction, students learn the basics of encryption methods and modern cryptography. You will learn to understand industry standards and their implementation. The module covers modern cryptography via algorithms and cryptosystems, cryptanalysis and best practices for application and implementation in software systems. The basics of quantum cryptography are also taught.
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: - Classic cryptography: substitution, transposition, rotor machine - Modern cryptography: stream and block ciphers, DES, AES - Hash and data integrity: SHA - Asymmetric cryptography: Diffie-Hellman, RSA, elliptic curve - Public key infrastructure: X.509 certificates, key management, Kerberos, SSH, SSL/TLS
Literature	**A final selection of literature will be made by the respective lecturer.** - Spitz, S., Pramateftakis, M., Swoboda, J.: Cryptography and IT Security, Vieweg+Teubner Verlag 2011 - Schmeh, K.: Cryptography, 6th edition, Heidelberg 2016 - Stallings, W.: Cryptography and Network Security, 7th Edition, Pearson, Essex 2017 - Schneier, B.: Applied Cryptography, Wiley, Indianapolis 1996
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Computer Systems and Networks - Systems and Networks

Module number	**CSM3**
Duration	1 semester
Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Prof. Dr. Jianmin Chen, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	The module teaches the principles and techniques used in operating systems and communication networks, in particular the TCP/IP protocol suite. Topics also include wireless and cellular protocols as well as RFID and other WPAN (Wireless Personal Area Network). In addition, an overview of technologies and specifics in "Operational Technology" is given.
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: - Computer architecture and operating systems - Network architectures and communication protocols - Network layers and OSI reference model - Local Area Network - Internet and intranet - Virtual Private Network - Mobile networks and WLAN - WPAN and RFID - Operational Technology (OT) and Supervisory Control and Data Acquisition (SCADA)
Literature	**A final selection of literature will be made by the respective lecturer.** - Bryant, R.; O'Hallaron, D.R.: Computer systems, Boston, Pearson 2011 - Tanenbaum, A.: Computer Networks, International Edition 2011 - Tanenbaum, A.: Modern Operating Systems, 4th Edition, Boston, Pearson 2015
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

System Analysis and Hardening - System Auditing and Hardening

Module number	**CSM4**
Duration	1 semester

Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Dr. Max Moser, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	Students will learn examples of cyber attacks that can be used to find vulnerabilities in networks, operating systems and applications. Practice is carried out using various techniques and currently available tools. Passwords and wireless networks are hacked and web applications are examined for vulnerabilities. Exploits are tested using frameworks (Metasploit, w3af, ...) and own modules are written. Further learning objectives are the automation of social media attacks, the circumvention of antivirus software and the capture of complete computers. The students know approaches and methods for defense and hardening of the examined attack scenarios.
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: - IT security and security measures - Motivation and weak points of networked computer systems - Procedures, mechanisms and tools for system analysis - Procedures, mechanisms and tools for system hardening - Intrusion detection and prevention systems for attack detection and defense - Log file analysis and analysis of web activities - Kali LInux, Wireshark, Nmap and Burp Suite
Literature	**A final selection of literature will be made by the respective lecturer.** - Donald A. Tevault: Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats, Packt Publishing - Eric D. Knapp, Joell T. Langill: Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Syngress Press
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Application Development and Security Lifecycle - Application Development & Security Lifecycle	
Module number	**CSM5**
Duration	1 semester
Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Dagmar Moser, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	Students are familiar with the importance of security in application development. While for a long time the focus of security was on securing systems and networks, in recent years the focus has increasingly shifted to the applications themselves. By taking security into account at an early stage of application development, not only can the level of security be significantly improved, but effort and complexity in other areas can also be reduced. The entire life cycle of the applications - from requirements analysis to deployment and reaction to security-relevant events - is considered over and above pure "coding". Regardless of the chosen software development process (V-model, RUP, SCRUM, etc.), security aspects are consciously planned and implemented in every development phase, in every iteration and in every sprint. Students know how to collect security requirements, identify and evaluate security risks and plan specific measures. In the design and implementation phase, familiar architecture principles and design patterns as well as basic rules for secure coding are used. Tests accompany the entire development process, particularly in the case of an iterative or agile approach. Security tests are also systematically integrated here. Established methods from practice are presented here as examples.
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: - Safety requirements - Secure software design, including Secure Design Principles and Secure Design Patterns - Secure coding - Security tests, including penetration testing, grey box - Build and deployment - Examples of established models
Literature	**A final selection of literature will be made by the respective lecturer.** - Basic knowledge of secure software, Sachar Paulus, dpunkt-Verlag - Microsoft Security Development Lifecycle https://www.microsoft.com/en-us/sdl - Security Engineering, Ross Anderson, Wiley Verlag - Secure by Design, Dan Bergh Johnsson, Daniel Deogun, Daniel Sawano, Manning-Verlag - Securing DevOps - Security in the Cloud, Julien Vehent, Manning-Verlag

Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Python and Go - Python and Go	
Module number	**CSM6-1**
Duration	1 semester
Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Dr. Max Moser, other lecturers as required
Frequency of the offer	Every academic year
LVF / SWS	2 SWS: PL
Workload (WL)	75h: 30h BL / 45h SSt
LP (ECTS)	2,5
MoP / LN	PA
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	In this module, students learn about two of the most common programming languages in the context of security-relevant developments: Python and Go. Both enable the rapid development of both simple tools and complex applications. In addition, Go enables the creation of independent programs without dependencies and thus simplifies installation and use. Even though various tools are already available for offensive and defensive use in cyber security, usually offering graphical user interfaces or operable via the command line, e.g. Metasploit, there are many situations where more customized actions are required or where existing tools need to be combined or integrated. The ability to quickly implement logic for customized purposes can prove to be a crucial skill.
Liability	Compulsory elective, two of the modules offered
Module content	The following knowledge and skills are taught as part of the course: - History and essential paradigms of Python and Go - Setting up the development environment for implementing "Hello World". - Introduction to the most important language constructs and functions - Use of the existing standard libraries - Use of specialized libraries - Applications of Python and Go in "Red Team" and "Blue Team" situations - e.g. reverse tunneling - e.g. network analysis
Literature	**A final selection of literature will be made by the respective lecturer.** - "Python Crash Course - A Hands-On, Project-Based Introduction to Programming" by Eric Matthes, NoStarch Press - "Black Hat Python - Python Programming for Hackers and Pentesters" by Justin Seitz, NoStarch Press - "Gray Hat Python - Python Programming for Hackers and Reverse Engineers" by Justin Seitz, NoStarch Press - Introducing Go" by Caleb Doxsey, O-Reilly - "A Tour to Go", https://tour.golang.org - "Go by Example", https://gobyexample.com/ - "Black Hat Go - Go Programming for Hackers and Pentesters" by Tom Steele, Chris Patten, and Dan Kottmann, NoStarch Press

Other information	Group work
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Human Factors in Cyber Security	
Module number	**CSM6-2**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Prof. Dr. Sabine Rathmayer, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	2 SWS: PL
Workload (WL)	75h: 30h BL / 45h SSt
LP (ECTS)	2,5
MoP / LN	PR
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	Students know the importance of the human factor in the field of cyber security. They develop an understanding of the relationships between information security, privacy and the usability of information systems. Students know which risks arise from people as weak points and as affected parties and which solutions are possible.
Liability	Compulsory elective, two of the modules offered
Module content	The following knowledge and skills are taught as part of the course: - Overview of different aspects of the human factor in cyber security - Research, presentation and discussion of different aspects and challenges
Literature	**A final selection of literature will be made by the respective lecturer.** - Usable Security: History, Themes, and Challenges (Synthesis Lectures on Information Security, Privacy, and Trust): Simson Garfinkel and Heather Richter Lipford. 2014 - Melanie Volkamer, Karen Renaud: Mental Models - General Introduction and Review of Their Application to Human-Centred Security. In Number Theory and Cryptography (2013): 255-280: https://link.springer.com/chapter/10.1007/978-3-642-42001-6_18 - Melanie Volkamer, Karen Renaud: Mental Models - General Introduction and Review of Their Application to Human-Centred Security. In Number Theory and Cryptography (2013): 255-280: https://link.springer.com/chapter/10.1007/978-3-642-42001-6_18 - Melanie Volkamer, Karen Renaud: Mental Models - General Introduction and Review of Their Application to Human-Centred Security. In Number Theory and Cryptography (2013): 255-280: https://link.springer.com/chapter/10.1007/978-3-642-42001-6_18 -
Other information	Group work after introductory presentation
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Ethics - Ethics	
Module number	**CSM6-3**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Dr. Josephine Müller, other lecturers as required
Frequency of the offer	Every academic year
LVF / SWS	2 SWS: PL
Workload (WL)	75h: 30h BL / 45h SSt
LP (ECTS)	2,5
MoP / LN	PR
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	Students know the importance of the discussion about ethics in the context of cyber security. The enforcement of cyber security harbors the risk that other fundamental values such as equality, fairness or privacy are ignored. At the same time, downplaying cyber security can have a massive impact on citizens' trust in the digital infrastructure.
Liability	Compulsory elective, two of the modules offered
Module content	The following knowledge and skills are taught as part of the course: - Definition of ethics, especially in the context of cyber security - Research, presentation and discussion of different aspects and challenges
Literature	**A final selection of literature will be made by the respective lecturer.** Yaghmaei, Emad and van de Poel, Ibo and Christen, Markus and Gordijn, Bert and Kleine, Nadine and Loi, Michele and Morgan, Gwenyth and Weber, Karsten, Canvas White Paper 1 - Cybersecurity and Ethics (October 4, 2017). Available at SSRN: https://ssrn.com/abstract=3091909 or http://dx.doi.org/10.2139/ssrn.3091909
Other information	Group work after introductory presentation
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Soft skills	
Module number	**CSM6-4**
Duration	1 semester
Person responsible for the module	Silke Biermann
Lecturer/s	Silke Biermann, other lecturers as required
Frequency of the offer	Every academic year
LVF / SWS	2 SWS: PL
Workload (WL)	75h: 30h BL / 45h SSt
LP (ECTS)	2,5
MoP / LN	PR
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	Students have comprehensive knowledge in the areas of communication, presentation and moderation and develop deeper social skills. Students are able to apply various moderation and presentation techniques in lectures, interviews and trend forums.
Liability	Compulsory elective, two of the modules offered
Module content	The following knowledge and skills are taught as part of the course: - Introduction to the basic issues of communication, presentation and moderation - Fundamentals of communication processes, corporate communication, presentation and moderation methods
Literature	**A final selection of literature will be made by the respective lecturer.** - Watzlawick, P./Beavin J. H./ Jackson D. D. (2003): Human communication; forms, disturbances, paradoxes. Bern. - Will, H. (2000): Mini handbook; lecture and presentation. Weinheim; Basel.
Other information	Group work
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	
Module number	**CSM7**
Duration	1 semester

Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Dr. Stephan Spitz, , other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Recommendation for participation	**Formal:** none; **Content:** CSM1, CSM2, CSM3
Learning outcomes of the module	Students are familiar with specific aspects of cyber security from various application areas. IoT based on embedded systems under cost pressure, open-access environments and limited resources pose particular security challenges. Industrial internet and operations technology with a large installed base of SCADA (Supervisory Control and Data Acquisition) is becoming a valuable target for cyber attacks. The emergence of mobile and cloud computing, with its broad market acceptance, brings new challenges for cyber security.
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: IoT systems and networks - Security and privacy principles of complex interconnected IoT - Types of threads, attacks and countermeasures - Confidentiality, authentication, integrity and availability OT (Operation Technology) / SCADA: - Threats and Vulnerabilities - Resilient Systems and Defense in Depth Cloud computing: - Service models, key concepts and enabling technologies of cloud computing - Confidentiality, availability and integrity - Risk management and division of responsibility - Trusted cloud security Mobile Computing: - Threads and vulnerability of mobile smart devices - Security aspects of mobile network
Literature	**A final selection of literature will be made by the respective lecturer.** - Colbert, E. (ed.): Cyber-security of SCADA and Other Industrial Control Systems, Springer 2016 - Loukas, G.: Cyber-Physical Attacks, Elsevier 2015 - Winkler, V.: Securing the Cloud, Elsevier 2011 - Industrial Internet Consortium: Industrial Internet of Things, Volume G4: Security Framework, 2016 - Vacca, J.: Cloud Computing Security, Taylor & Francis 2017
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.

Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Legal aspects & data protection - Legal Aspects & Privacy	
Module number	**CSM8**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Michaela Braun, other lecturers as required
Frequency of the offer	Every academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** CSM1, CSM2
Learning outcomes of the module	Students are familiar with the legal aspects of cyber security, in particular the regulatory requirements of IT security and data protection. With global networking in a flat world, the legal and regulatory frameworks in Germany, the EU, the USA and other important regions with their specific characteristics and significance with regard to cyber security are dealt with. Numerous other areas of law that are affected, such as corporate law (best practices of corporate organization and due diligence obligations of management), insurance law, employment law, but also transaction and supervisory practice, are also addressed. The requirements of these legal and regulatory frameworks for compliance and governance are presented. In addition, the dynamic development of political and sociological aspects with regard to cyber security, which may become normative as future requirements in legal, regulatory and interest group terms, will be addressed. In order to increase the practical benefit, a distinction is generally made between the legal requirements for prevention ("preparedness") and the legal guard rails in an emergency ("response").
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: - Consideration of various areas of law such as corporate law, insurance law, labor law, criminal law in connection with cyber security - Regulatory requirements - Regional, national and international aspects - Measures for prevention and in an emergency
Literature	**A final selection of literature will be made by the respective lecturer.** - Gabel / Heinrich / Kiefner Legal Handbook Cyber-Security - Stallings, W. et al: Foundations of Modern Networking, Pearson 2016 - Kizza, J.: Computer Network Security and Cyber Ethics, 4th Edition. McFarland, Jefferson 2014
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	

Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Seminar: current topics in cyber security	
Module number	**CSM9**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Prof. Dr. Sabine Rathmayer, other lecturers as required
Frequency of the offer	Every academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Recommendation for participation	**Formal:** none; **Content:** CSM1
Learning outcomes of the module	Selected topics are dealt with on the basis of current publications. The topics are determined at the beginning of each semester. The forms of submission are a paper and a presentation. Students are introduced to academic work in terms of content, concept, implementation and formal requirements.
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: - Research on current topics and developments in the field of cyber security - Preparation and presentation of the research results
Literature	**A final selection of literature will be made by the respective lecturer.** - Current literature according to the respective topics
Other information	Working in small groups can make up part of the contact time. The project work includes a presentation.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Intrusion Detection + Digital Forensics - Intrusion Detection +Digital Forensics	
Module number	**CSMT1**
Duration	1 semester
Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Dr. Max Moser,, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Recommendation for participation	**Formal:** none; **Content:** CSM1, CSM4
Learning outcomes of the module	This module examines the building blocks and requirements for intrusion detection systems, examines and evaluates the various approaches and looks at practical applications of an IDS and selected IDS products. Intrusion detection systems, or IDS for short, aim to detect and report attacks directed at computers or networks. In this way, they supplement the functions usually provided by firewalls by also looking at the processes behind the firewall and investigating them over a longer period of time. For this purpose, IDSs usually use more or less extensive data obtained from the various monitored computer systems and from the network. In this data, an IDS looks for patterns of an attack or conspicuous anomalies - and can thus provide important information to either ward off a current attack or analyze an attack that has already taken place. IDS developments have recently received a major boost from new artificial intelligence methods. In addition to the use of IDS systems, the extensive and ongoing collection of data from systems and networks also allows forensic procedures to be used in order to gain in-depth knowledge about an intrusion that has taken place. On the one hand, this allows measures to be derived for future defense and, on the other, the basis for criminal prosecution. This module therefore also looks at important forensic concepts and tools relating to storage technologies and forensic data analysis and recovery. Practical aspects in the areas of mobile, smart devices, network and cloud forensics are covered.
Liability	Compulsory within the selected focus on technology
Module content	The following knowledge and skills are taught as part of the course: - Assets and their risk potential - Intrusion Detection Systems (IDS) - Evaluation of relevant data and its collection - Filtering, transforming and enriching data - Use cases of the analysis and examples - Data mining on collected data - Applications of AI - Cyber attacks and criminality - Computer forensics: data analysis and reconstruction - Network forensics: attack tracing and **attribution**
Literature	**A final selection of literature will be made by the respective lecturer.** - Casey, E. (ed.): Handbook of Digital Forensics and Investigation, Elsevier 2010

	- Hu, F.: Security and Privacy in Internet of Things (IoTs), CRC Press 2016 - Northcutt S., Novak, J.: Network Intrusion Detection 3rd Edition, New Riders 2003 - Sammons, J.: The Basics of Digital Forensics, Elsevier 2012
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

System and Network Security - System and Network Security

Module number	CSMT2
Duration	1 semester
Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Prof. Dr. Jianmin Chen, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Recommendation for participation	**Formal:** none; **Content:** CSM2, CSM3, CSM4
Learning outcomes of the module	Building on the "System analysis and hardening" module, students are familiar with the risks and vulnerabilities of systems and networks. Networks include standard IT networks such as Local Area Network, Wireless Network, Cellular Network, Cellular Network, Internet, Intranet as well as more recent developments such as RFID, NFC, WPAN and ZigBee in the consumer and IoT area with their specific architectures and, above all, risk and security assessments. In addition, special aspects of operational technology and critical infrastructure are examined. Various intrusion tools and methods are presented and used for practical exercises. Measures for monitoring and preventing attacks are practiced in a simulated environment.
Liability	Compulsory within the selected focus on technology
Module content	The following knowledge and skills are taught as part of the course: - Operating system security - Security aspects of networks - Concepts and architectures of firewalls - Methodology of attack and countermeasures - Security of mobile and cloud computing - Intrusion detection and prevention systems - Honeypots and honeynets
Literature	**A final selection of literature will be made by the respective lecturer.** - Stallings, W.: Cryptography and Network Security, 7th Edition, Pearson 2017 - Kizza, J.: Computer Network Security, Springer 2005 - Knapp, E.: Industrial Network Security, 2nd Edition, Elsevier 2015 - Vacca, J.(ed.): Network and System Security, Elsevier 2010
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Methods of artificial intelligence (AI)

Module number	**CSMT3**

Duration	1 semester
Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Dr. Max Moser, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** none
Learning outcomes of the module	Students acquire a sound overview of selected areas of artificial intelligence as well as practical and methodological knowledge and skills in the application of AI methods and algorithms. This includes the ability to evaluate the performance and selection of suitable techniques for the respective problem domain. They can assess the quality of the results of such methods.
Liability	Compulsory within the selected focus on technology
Module content	The event covers the following topics, among others: - Overview and introduction - Intelligent agents - Representation of knowledge and problems - Problem solving by searching, adversarial search, heuristics - Knowing, closing, planning - Uncertain knowledge and closure - Machine learning and data mining - Neural networks - Learning through reinforcement - Communicating, perceiving and acting - Capture and visualize typical AI software architectures - Develop the ability to apply these methods in the context of simple problems. - Designing and implementing small agent programs. The methods presented in the lecture will be deepened during the exercise.
Literature	**A final selection of literature will be made by the respective lecturer.** - Stuart Russell, Peter Norvig: Artificial intelligence. A modern approach. Pearson Studium. 2012. - W. Ertel, Basic Course in Artificial Intelligence, Springer Vieweg, 2016 - George F. Luger: Artificial Intelligence. Structures and Strategies for Complex Problem Solving. Addison Wesley. 2004. - J. Kaplan, Artificial Intelligence: An Introduction, mitp Prefessional, 2017 - T. Rashid, F. Langenau, Programming neural networks yourself, O'Reilly, 2017 - C.N. Nguyen, O. Zeigermann, Machine Learning - short & sweet: An introduction with Python, Pandas and Scikit-Learn, O'Reilly, 2017 - G.D. Rey, K.F. Wender, Neural Networks: An Introduction to the Basics, Huber, 2010

	- I. Witten, E. Frank and M. Hall, Data Mining: Practical Machine Learning Tools and Techniques, 3rd edition, Morgan Kaufmann (2011)
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	Digital Technology (MA)
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Maturity models - Security Maturity	
Module number	**CSMO1**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Dagmar Moser, other lecturers as required
Frequency of the offer	Every academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** CSM1
Learning outcomes of the module	Students know how to use standardized procedures to evaluate and optimize the existing security level of a company. The aim of these standards is to provide companies and those responsible for security with current and internationally recognized best practices and benchmarks, thus improving the (further) development of a company's security. The standards mentioned are discussed in an overview and with selected focus areas using practical examples. The topics of legacy applications, OT and critical infrastructures pose a particular challenge. In addition to the established standards that can be used across the board, the aim is to provide an insight into the requirements that are relevant in specific sectors or countries, for example. Economic aspects and considerations (ROI, TCO,...) are also taken into account.
Liability	Compulsory within the selected specialization Organization and Management
Module content	The following knowledge and skills are taught as part of the course: - Security maturity models and standards - motivation and use - Overview and discussion of selected security maturity models, e.g. - Common criteria - BSIMM - OWASP SAMM - Overview and discussion of important security standards, e.g. - NIST Framework - ISO 2700x - Key performance indicators (KPIs) - Example applications and practical applications
Literature	**A final selection of literature will be made by the respective lecturer.** - Common Criteria, https://www.commoncriteriaportal.org/cc/ - BSIMM https://www.bsimm.com/ - OWASP SAMM https://www.owasp.org/index.php/OWASP_SAMM_Project - NIST Framework https://www.nist.gov/cyberframework - ISO 2700X http://www.iso27001security.com/
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.

Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Security Governance and Compliance	
Module number	**CSMO2**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Franz Obermayer, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** CSM1
Learning outcomes of the module	Students know the importance of security governance, which provides normative, strategic and organizational framework conditions for IT and especially its security aspects. It structures and specifies secure IT management and information management. In doing so, it is in the area of conflict between the best possible support of corporate goals and strategies through IT and the achievement of a high utility value with the necessary consideration of possible risk potentials through the use of IT (security, failure, violation of specifications). In this context, students are familiar with compliance with the primary aim of ensuring that the development and operation of IT complies with and observes specific laws, guidelines, norms, codes, standards and contracts. Compliance ensures demonstrable adherence to these requirements vis-à-vis internal (auditing) and external institutions (auditors, supervisory authorities).
Liability	Compulsory within the selected specialization Organization and Management
Module content	The following knowledge and skills are taught as part of the course: - Embedding information security governance in corporate governance - Organization and structure of information security guidelines - Task of compliance and control in the area of security governance - Risk management within security governance
Literature	**A final selection of literature will be made by the respective lecturer.** - von Solms, S.H.; von Solms, R.: Information Security Governance. Springer 2009 - ISO/IEC 27002 (2005). Information Technology - Security Techniques - Code of Practice for Information Security Management. ISO. www.iso.ch - COBIT (2005). Control Objectives for Information and Related Technology. ISACA. www.isaca.org
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	

Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Security Management - Security Manangement	
Module number	**CSMO3**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Franz Obermayer, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** CSM1
Learning outcomes of the module	Students are familiar with the structure and tasks of information security management and information security management systems. They are provided with organized processes for dealing with information security issues.
Liability	Compulsory within the selected specialization Organization and Management
Module content	The following knowledge and skills are taught as part of the course: - The information security organization, with roles and resources as well as regulations on responsibility, - Defined processes in which risks are recorded and evaluated (risk management with analysis of hazards and attacker models) and a security concept in which the measures to be taken to achieve a targeted security level are documented, - Measures to check compliance with the security requirements - Information security management using the ISO standards 27001 and 27002 as examples
Literature	**A final selection of literature will be made by the respective lecturer.** - Smith, C.; Brooks, D.: Security Science. Elsevier. Waltham 2013 - Schoenfield, B.: Securing Systems. CRC Press. Boca Raton 2015 - ISO/IEC 27002 (2005). Information Technology - Security Techniques - Code of Practice for Information Security Management. ISO. www.iso.ch
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Incident Management and Disaster Recovery	
Module number	**CSM10**
Duration	1 semester

Person responsible for the module	Prof. Dr. Jianmin Chen
Lecturer/s	Dr. Max Moser, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	PA
Recommendation for participation	**Formal:** none; **Content:** CSM1, CSM2, CSM3, CSM4
Learning outcomes of the module	The students know the organizational procedure for dealing with detected or suspected security incidents as well as preparatory and supplementary measures and the respective processes. These measures and processes are intended to enable a coordinated approach by all those involved in order to prevent damage to the company after a security incident occurs, restore the affected service to the defined quality and ensure the integrity of company data and services. Organizational, legal and technical aspects must be taken into account. Students know the rules, tools and processes that should enable the resumption or continuation of business-critical processes, applications and infrastructures after a security incident. The basis for such a disaster recovery is a systematic assessment of the relevant components and a business impact analysis that evaluates their business criticality.
Liability	Mandatory
Module content	The following knowledge and skills are determined as part of the course: - Overview and motivation - Computer Emergency Response Teams - CERT - Organization, equipment and communication of a CERT - Incident processes - Incident Management Systems (IMS) - Examples from practice and well-known CERT organizations - Disaster recovery vs. business continuity management - Business impact analysis - Incident classes and key figures for crisis management - Organizational preparations for disaster recovery and embedding in the company organization - Guidelines from ISO, BSI and other practical examples
Literature	**A final selection of literature will be made by the respective lecturer.** - Rob Schnepp, Ron Vidal, Chris Hawley: Incident Management for Operations, O'Reilly - Matthew William Arthur Pemble, Wendy Fiona Goucher: The CIO's Guide to Information Security Incident Management, Auerbach Publications - Jamie Watters, Janet Watters: Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference, Apress Publishers - Vacca, J.: Cyber Security and IT Infrastructure Protection. Syngress. Waltham 2014 - Griffor, E.: Handbook of Safety and Security, Syngress, Cambridge 2017 - Kostopoulos, G.: Cyberspace and Cybersecurity. CRC Press. Boca Raton 2013

	- Computer Security Incident Handling Guide - NIST Special Publication 800-61R2
Other information	Work in small groups can make up part of the contact time. The quality of the project work is ensured on the basis of given case studies.
Prerequisite Award of LP	Passed MoP
Use of the module (in other degree programs)	
Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Requirements Engineering and Threat Modeling	
Module number	**CSM11**
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	Dagmar Moser, other lecturers as required
Frequency of the offer	Each academic year
LVF / SWS	4 SWS: VL (2 SWS) & UE (2 SWS)
Workload (WL)	150h: 60h BL / 90h SSt
LP (ECTS)	5
MoP / LN	sP
Recommendation for participation	**Formal:** none; **Content:** CSM1
Learning outcomes of the module	Students are aware of the great importance of security requirements in requirements engineering, which are often still given too little attention. Security requirements that are overlooked at the beginning of a development project are usually not implemented at all or are implemented far too late. This leads to security gaps in applications, which can cause considerable costs later on. This module teaches the basics of requirements engineering, with a particular focus on the elicitation of security requirements. Functional as well as non-functional requirements or requirements for the architecture are considered. Security requirements can only be partially concretized with the help of common requirements engineering techniques (e.g. questioning techniques). For this reason, threat modeling is presented as a special technique for identifying threats and deriving corresponding security requirements from them.
Liability	Mandatory
Module content	The following knowledge and skills are taught as part of the course: - Fundamentals of requirements engineering, including functional and non-functional requirements - Techniques for collecting requirements - Threat modeling - Deriving security requirements from threats
Literature	**A final selection of literature will be made by the respective lecturer.** - Basic knowledge of secure software, Sachar Paulus, dpunkt-Verlag - Threat Modeling - Designing for Security, Adam Shostack, Wiley-Verlag - Basic knowledge of requirements engineering, Klaus Pohl, Chris Rupp, dpunkt-Verlag - Requirements Engineering and Management, Chris Rupp, Hanser Verlag
Other information	Working in small groups can make up part of the contact time.
Prerequisite Award of LP	Passed MoP.
Use of the module (in other degree programs)	

Importance of the grade for the final grade	The module grade is the weighted arithmetic mean of the module performance(s). The overall grade of the Master's examination is the weighted arithmetic mean of the module grades and the grade of the final examination. The weighting generally corresponds to the proportion of CP (ECTS) in the total number of 90.

Master's thesis	
Module number	CSMT
Subject area	Final module
Duration	1 semester
Person responsible for the module	Prof. Dr. Sabine Rathmayer
Lecturer/s	To be determined individually according to topic
Frequency of the offer	Every semester
LVF / SWS	SSt & KO
Workload (WL)	600 h
LP (ECTS)	20 (18 CP: Master's thesis; 2 CP: defense)
MoP	HA & mP
Recommendation for participation	
Learning outcomes of the module	As part of the Master's thesis, students should demonstrate that they are able to - treat a topic conceptually comprehensively and in depth - and apply the theoretical knowledge gained to a practical business problem.
International and practical connection to the dual partner company	In accordance with the learning objectives of the HDBW, the Master's thesis must deal with a subject-relevant topic in an international context. The thesis must also be written in cooperation with partner companies on a topic relevant to the company. The topic for the Master's thesis is agreed between the supervising professor, the student and, if applicable, a company representative.
Liability	Mandatory
Contents	The preparation of the Master's thesis consists of two components 1. The independent preparation of a master's thesis of up to 80 pages. 2. The defense and presentation of the results of the Master's thesis with an examination discussion in which the content of the Master's thesis is also linked to other content of the degree program. The duration should not exceed 10 minutes. The total duration of the defense may not exceed 30 minutes.
Other information	The Master's thesis can be written in German or English.
Prerequisite Award of credit points	Passed Master's thesis and passed defense.
Use of the module (in other degree programs)	
Importance of the grade for the final grade	In this case, the assessment of the Master's thesis is given a weighting of 9/10 and the assessment of the defense (KO) of the thesis is given a weighting of 1/10 in the grade of the final examination.

Index