Hochschule Aalen
UNIVERSITY OF APPLIED SCIENCES

Modulhandbuch
Master Cyber Security
(berufsbegleitend)

Stand: 07.10.2026

Pflichtmodule

25807	Cyber Security
25808	Anwendungssicherheit
25809	Penetration Testing und Computerforensik
25610	IT-Sicherheitsmanagement

	Studienschwerpunkt IT Security Management
25605	Cloud Computing
25601	IT-Outsourcing und IT-Governance
25607	Business Analytics: Anwendungsentwicklung
25608	Business Analytics: Big Data

	Studienschwerpunkt Cybercrime
25605	Cloud Computing
25810	Incident Response / Recovery Management
25812	Cybercrime und Incident Detection
	Wahlpflichtfach (wähle 1 von 2)
25811	Digitale Polizeiliche Forensik
25611	Corporate Cyber Defense

	Studienschwerpunkt Cyber Security Technology
25810	Incident Response / Recovery Management
25812	Cybercrime und Incident Detection
25813	KI-gestützte IT-Sicherheit
	Wahlpflichtfach (wähle 1 von 2)
25612	Industrial Security / OT Security
25613	IT-Sicherheit in Dienstleistungsunternehmen

Hochschule Aalen
UNIVERSITY OF APPLIED SCIENCES

Wahlpflichtbereich Betriebswirtschaftslehre

25701	ABWL für Informatiker
25703	General Management
25704	Organisationslehre
25705	Accounting und Controlling
25706	Corporate Finance
25707	Projektmanagement
25708	Marketing Management
25709	Dienstleistungsmanagement
25710	IoT-Geschäftsmodelle

Wahlpflichtbereich Informatik

25801	Allgemeine Informatik für BWLer
25802	Datenbanken
25803	Programmieren für Data Science
25804	Text Mining und Web Analytics
25805	Machine Learning und Deep Learning
25806	Data Mining und Visual Analytics
25810	Incident Response / Recovery Management
25811	Digitale Polizeiliche Forensik
25812	Cybercrime und Incident Detection
25813	KI-gestützte IT-Sicherheit
25814	Modellgetriebene Analytics

Wahlpflichtbereich Wirtschaftsinformatik

25601	IT-Outsourcing und IT-Governance
25602	Enterprise Resource Planning
25603	Business Process Management
25604	Business Intelligence
25605	Cloud Computing
25606	In-Memory Data Management
25607	Business Analytics: Anwendungsentwicklung
25608	Business Analytics: Big Data
25609	Informationsmanagement
25611	Corporate Cyber Defense
25612	Industrial Security / OT Security
25613	IT-Sicherheit in Dienstleistungsunternehmen
25614	Industrial Analytics

Hochschule Aalen
UNIVERSITY OF APPLIED SCIENCES

Pflichtbereich

25901	Überfachliche Kompetenzen
91031	Projektarbeit
9999	Masterarbeit
91999	Studium Generale

Legende Abkürzungen Prüfungsarten

PLK	Klausurarbeiten
PLM	Mündliche Prüfung
PLS	Schriftliche Arbeiten
PLR	Referat
PLL	Laborarbeiten
PLA	Praktische Arbeiten
PLP	Projektarbeiten

Modul-Nr: 25807 Cyber Security SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Cyber Security
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	2x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines

Die Studierenden weisen breites Wissen im Zusammenhang mit Risiken bei Informationssystemen, sowie Spezialwissen zu Maßnahmen und Methoden zu deren sicherer Gestaltung auf.

Fachliche Kompetenzen

Die Studierenden können Angriffsmöglichkeiten und deren Abwehr beschreiben und real existierende Gefahren einschätzen sowie geeignete Maßnahmen auswählen. Sie verstehen grundlegende Verfahren der Kryptografie und können passende Verschlüsselungstools anwenden. Ferner können sie Internet-Technologien bzgl. Schwachstellen beschreiben, analysieren, beurteilen und erklären.

Überfachliche Kompetenzen

Die Übungen werden in Teams von Studierenden bearbeitet. Durch den Charakter als berufsbegleitendem Studiengang, weisen die Studierenden hinsichtlich Vorqualifikation und Berufserfahrung unterschiedliche Hintergründe auf, was dem fachlichen und überfachlichen Austausch der Studierenden zugute kommt.

Ggf. besondere Methodenkompetenz

In Übungen und im Abschlussprojekt lernen Studierende, selbständig die notwendigen analytischen Methoden einzusetzen, mit denen sie Gefährdungen für Informationssysteme erkennen und Schutzmaßnahmen auswählen und implementieren können. Hierzu erlernen sie auch, passende Sicherheitsprodukte auszuwählen und zum Einsatz zu bringen und ihre Entscheidungsfindung sowie die Ergebnisse geeignet zu dokumentieren.

Lerninhalte

- Rechtliche Grundlagen
- Angriffsklassifizierung
- Überblick über Kryptologie: Substitutions-Chiffren, One-Time-Pads, synchrone und sel Stromchiffren, Blockchiffren, Public-Key-Kryptosysteme, kryptographische Einweg-Has Signaturen, Verschlüsselungsprodukte, Steganographie
- Internet-Sicherheit: E-Mail, Browser, Web-Services, Malware, Firewalls, VPN
- Netzwerksicherheit: Netzwerkmethoden, Schichtenmodelle, SSL, TLS
- Benutzbare Sicherheit
- Bewertungskriterien: CC
-

Literatur

- Hellmann: IT-Sicherheit - Eine Einführung, DeGruyter (erscheint demnächst)
- Eckert, IT-Sicherheit, Oldenbourg
- Poguntke: Basiswissen IT-Sicherheit
- Ertel, Angewandte Kryptographie, Fachbuchverlag Leipzig

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25307	Cyber Security	Prof. Dr. Marta Gomez-Barrero	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25307	PLK 90“	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 15.10.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25808 Anwendungssicherheit SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Anwendungssicherheit
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden sind in der Lage, selbständig Fragestellungen für wissenschaftliche Probleme im Zusammenhang mit Sicherheitsaspekten von Anwendungssoftware zu entwickeln. Die Studierenden weisen breite Kompetenzen zu typischen Schwachstellen von Anwendungssoftware auf und können deren Funktionsweise beschreiben, analysieren, erklären und beurteilen. Die Studierenden weisen darüber hinaus Spezialwissen zu Sicherheitsgrundfunktionen und den Prozessen des Security Engineering auf.

Überfachliche Kompetenzen

Durch Teamarbeit innerhalb der Übungen sind die Studierenden in der Lage gemeinsam zu agieren. Durch den Charakter als berufsbegleitenden Studiengang, weisen die Studierenden hinsichtlich Vorqualifikation und Berufserfahrung unterschiedliche Hintergründe auf, was dem fachlichen und überfachlichen Austausch der Studierenden zugute kommt.

Ggf. besondere Methodenkompetenz

Die Studierenden sind in der Lage, die Auswirkungen einer Schwachstelle zu beschreiben, analysieren, erklären und beurteilen. Die Studierenden können selbständig Sicherheitsbewertungen von Software durchführen, hieraus weiterführende Schlussfolgerungen ziehen und gegenüber Laien und Fachleuten argumentativ verteidigen. Die Studierenden können Sicherheitsmechanismen, Sicherheitsbewertungen und die Prozesse des Security Engineering eigenständig und gestalterisch bearbeiten.

Modul-Nr: 25808 Anwendungssicherheit SPO 511

Lerninhalte

- Grundlagen der Anwendungssicherheit
- Verfahren zur Authentisierung
- Buffer Overflows
- Sicherheit von Webanwendungen
- Bewertung von Schwachstellen

Literatur

Dieter Gollmann: Computer Security, 2011.
Adam Shostack: Threat Modeling: Designing for Security, 2014.
John R. Vacca: Computer and Information Security Handbook, 2013.
Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle, 2014.
Alfred Basta, Wolf Halton: Computer Security and Penetration Testing, 2008.
Jon Erickson: Hacking The Art of Exploitation, 2008.
Ross Anderson: Security Engineering, 2008.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25308	Anwendungssicherheit	Prof. Dr. Christoph Karg	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25308	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 07.05.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*
2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25809 Penetration Testing und Computerforensik SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Penetration Testing und Computerforensik
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Benötigte Vorkenntnisse in den Bereichen: - HTTP/HTTPS - HTML/PHP/Javascript/SQL - Umgang mit der Linux- und Windows- Shell
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Veranstaltung vermittelt breites Wissen und Fertigkeiten auf den Gebieten des Penetration Testing und der Computerforensik. Die Studierenden können die Vorgehensweise bei der Planung und Durchführung eines Penetration Tests beschreiben, analysieren, erklären und beurteilen. Die Studierenden verfügen über forschungspraktische Fähigkeiten und Kenntnisse zu den verschiedenen Arten der forensischen Analyse. Die Studierenden können beschreiben, analysieren, erklären und beurteilen worauf bei der gerichtsverwertbaren Beweissicherung zu achten ist. Die Studierenden sind in der Lage, die Phasen der forensischen Ermittlung zu beschreiben, analysieren, erklären und beurteilen.

Überfachliche Kompetenzen

Die Übungen werden in Teams von Studierenden bearbeitet. Durch den Charakter als berufsbegleitendem Studiengang, weisen die Studierenden hinsichtlich Vorqualifikation und Berufserfahrung unterschiedliche Hintergründe auf, was dem fachlichen und überfachlichen Austausch der Studierenden zugute kommt.

Ggf. besondere Methodenkompetenz

Die Studierenden können Penetration Tests planen, durchführen und auswerten. Sie können gängige Werkzeuge für Penetration Testing auswählen und anwenden. Die Studierenden können eine Post-Mortem-Analyse durchführen und auswerten.

Modul-Nr: 25809 Penetration Testing und Computerforensik SPO 511

Lerninhalte

- Planung von Penetration Tests
- Netzwerkanalyse mit NMap
- Privilegieneskalation in Windows-Netzen
- Dokumentation der Ergebnisse eines Penetration Tests
- Incident Response
- Rechtliche Aspekte der Computer-Forensik
- Gerichtsverwertbare Beweissicherung
- Phasen der forensischen Ermittlung
- Post-Mortemanalyse
- Incident Readiness
- Sicherheitsanalysen von Webapplikationen
-

Literatur

Michael Messner: Hacking mit Metasploit: Das umfassende Handbuch zu Penetration Testing und Metasploit, 2015.
Alfred Basta und Wolf Halton: Computer Security and Penetration Testing,

Alexander Geschonnek: Computer-Forensik (iX Edition): Computerstraftaten kennen, ermitteln, aufklären, 2014.

Dafydd Stuttard, Marcus Pinto: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2011

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25309	Pen. Testing und Computerforensik	Dipl.-Inf. Sebastian Auwärter	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25309	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.03.2026

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25610 IT-Sicherheitsmanagement SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	IT-Sicherheitsmanagement
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden weisen breites Wissen über die Management-Aspekte der IT-Sicherheit, sowie Spezialwissen zu technischen, organisatorischen, betriebswirtschaftlichen und rechtlichen Aspekte auf. Die Studierenden können eine IT-Sicherheitsorganisation eigenständig und gestalterisch bearbeiten und können die analytischen Methoden eines IT- Sicherheitsbeauftragten anwenden, mit denen sie Zusammenhänge beschreiben, analysieren, erklären und beurteilen können. Ferner können sie die fachspezifischen Methoden der IT-Sicherheit bzw. Cyber Security mit denen der Managementlehre und BWL zusammenführen, um neue Problemlösungen in komplexen Zusammenhängen zu erarbeiten.

Überfachliche Kompetenzen

Die Übungen werden in Teams von Studierenden bearbeitet. Durch den Charakter als berufsbegleitendem Studiengang, weisen die Studierenden hinsichtlich Vorqualifikation und Berufserfahrung unterschiedliche Hintergründe auf, was dem fachlichen und überfachlichen Austausch der Studierenden zugute kommt.

Ggf. besondere Methodenkompetenz

Die Studierenden sind in der Lage, in Gruppen anhand von IT-Sicherheitskonzepten und Fallbeispielen selbständig Fragestellungen für wissenschaftliche Probleme zu entwickeln und weiterführende Schlussfolgerungen zu ziehen sowie diese gegenüber Laien (bspw. Geschäftsführung, Anwender und Betroffene) und Fachleuten (bspw. IT-Abteilung) argumentativ zu verteidigen.

Modul-Nr: 25610 IT-Sicherheitsmanagement SPO 511

Lerninhalte

- Überblick über rechtliche Grundlagen (u.a. Datenschutzrecht, Strafrecht)
- Aufbau einer IT-Sicherheitsorganisation
- IT-Sicherheits-Policy und Regeln
- Audits, Vorabkontrolle, Reporting, Haftung
- Mitarbeiter-Sensibilisierung
  Erstellung von IT-Sicherheitskonzepten
- BSI Grundschutzkataloge und Tools

Literatur

Harich: IT Sicherheitsmanagement Kersten,
Klett: Der IT Security Manager
Münch: Technisch-organisatorischer Datenschutz
Däubler, Klebe, Wedde, Weichert: Bundesdatenschutzgesetz, Bund-Verlag, SBN 978-3-7663-3917-1
Datenschutz – Eine Vorschriftensammlung D e.V., ISBN 978-3-8249-1103-5

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25110	IT-Sicherheitsmanagement	Dr. Andreas Höpken	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25110	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 22.01.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25605 Cloud Computing SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Cloud Computing
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse in BWL und Informatik (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen
Die Studierenden können fundiert zu technischen, wirtschaftlichen und organisatorischen Aspekten des Themenkomplexes Cloud Computing argumentieren. Auch können sie rechtliche Aspekte erörtern und Fragen der Informationssicherheit diskutieren. Die Studierenden können anhand der praktischen Beispiele den Aufwand zur Nutzung von gängigen Cloud-Technologien abschätzen. Die Studierenden sind in der Lage, Chancen und Risiken des Einsatzes von Cloud Computing in Unternehmen zu bewerten und abzuwägen. Die Studierenden können anhand der vermittelten Kriterien den Auswahlprozess einer geeigneten Cloud-Lösung für ein Unternehmen gestalten, andere von dieser überzeugen und die Lösung umsetzen.

Überfachliche Kompetenzen
Die Studierenden beschäftigen sich mit Problemstellungen, lösen diese mit wissenschaftlichen Methoden auf eigenständige Art.

Ggf. besondere Methodenkompetenz
Die Studierenden sind zur systematischen und strukturierten Anwendung verschiedener Cloud-Lösungsmöglichkeiten in der Lage, indem sie grundsätzliche Entscheidungshilfen und Checklisten an die Hand geliefert bekommen.

Lerninhalte

Einleitung
- Entstehungsgeschichte des Cloud Computing
- Charakteristika des Cloud Computing
- Klassifkation von Cloud Diensten
- Arten von Clouds
- Geschäftsmodelle für Cloud Dienste
- Entwicklung und Umsetzung einer Cloud Strategie

Docker
- Einführung in Container-Technologien
- Funktionsweise von Docker
- Beispiele
- Sicherheitsaspekte

Kubernetes
- Einführung
- Aufbau eines Kubernetes Clusters
- Arten von Kubernetes Deployments
- Beispiele
- Sicherheitsaspekte
- Kubernetes As A Service

Cybersicherheit in der Cloud
- Risiken beim Einsatz von Cloud Diensten
- Technische Maßnahmen
- Organisatorische Maßnahmen

Wirtschaftliche und organisatorische Aspekte
- Kostenabschätzung
- Anforderungen
- Auswahl des Cloud Anbieters
- Wirtschaftlichkeitsbetrachtungen
- Chancen und Risiken bei der Nutzung von Cloud Computing

Aktuelle Themen des Cloud Computing

Literatur

Lisdorf: Grundlagen des Cloud Computing: Eine nichttechnische Einführung, Springer, 2024

Erl, Monroy: Cloud Computing: Concepts, Technology, Security, and Architecture, Pearson, 2023

Vossen, Haselmann, Hoeren: Cloud Computing für Unternehmen, dpunkt Verlag, 2012

Mather, Kumaraswamy, Latif: Cloud Security and Privacy, O'Reilly, 2009

Hennrich: Cloud Computing nach der Datenschutz-Grundverordnung: Amazon Web Services, Google, Microsoft & Clouds anderer Anbieter in der Praxis, O'Reilly, 2022

Metzger, Reitz, Villar: Cloud Computing - Chancen und Risiken aus technischer und unternehmerischer Sicht, Hanser, 2011.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25105	Cloud Computing	Prof. Dr. Christoph Karg	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25105	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 09.10.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25601 IT-Outsourcing und IT-Governance SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	IT-Outsourcing und IT-Governance
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Vorkenntnisse: grundlegende BWL-Kenntnisse (Investitionsrechnung), Organisation, Prozess- und Informationsmanagement, Betriebliche Standardsoftware
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen
Die Studierenden sind in der Lage, die wichtigsten Bereiche der IT Governance und des IT Outsourcings zu beurteilen. Die Studierenden können Aufgabenstellungen und Handlungsfelder bewerten, um möglichst effiziente IT Governance Strukturen im Unternehmen aufbauen zu können. Dabei erlernen die Studierenden monetäre und nicht-monetäre Methoden, um die Positionierung und Steuerung der IT Funktion in einem Unternehmen einschätzen und optimieren zu können. Die Studierenden kennen die wichtigsten Erfolgsfaktoren für das IT-Outsourcing und sind in der Lage, ein fachliches Konzept inklusive einer zeitlichen Planung für ein IT-Outsourcingprojekt zu erstellen.

Überfachliche Kompetenzen
Die Studierenden bearbeiten mehrere Fallstudien in Teams. Dadurch werden Organisation, Planung, Aufgabenverteilung, Entscheidungsfindung im Team und Präsentationsfähigkeiten eingeübt und gefestigt.

Ggf. besondere Methodenkompetenz
Die Studierenden sind in der Lage, Problemstellung im Bereich der IT Governance und des IT Outsourcings im Unternehmenskontext zu analysieren und dafür eine unter betriebswirtschaftlichen, organisatorischen und IT Aspekten sinnvolle und nutzenstiftende Lösung zu entwickeln.

Modul-Nr: 25601 IT-Outsourcing und IT-Governance SPO 511

Lerninhalte

- IT-Business-Alignment,
- Wertbeitrag der IT,
- Organisationsstrukturen für die IT Funktion im Unternehmen,
- CobiT,
- strategische Planung, IT Strategie und Balanced Scorcard,
- Varianten des IT Outsourcings,
- Erfolgsfaktoren für das IT Outsourcing,
- Next Generation Outsourcing und
- IT Governance für IT Outsourcing
- Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Hofmann, J., Schmidt, W. (2010): Masterkurs IT-Management. 2. Auflage. Wiesbaden: Friedrich Vieweg & Sohn Verlag.

Rüter, A., Schröder, J., Göldner, A., Niebuhr Jens (2010): IT-Governance in der Praxis. 2. Auflage. Berlin, Heidelberg, New York: Springer Verlag.

Keller, W. (2012): IT Unternehmensarchitektur. 2. Auflage Heidelberg: dpunkt.verlag.

Leimeister, S. (2010): IT Outsourcing Governance. Wiesbaden: Gabler Verlag.

Pfaller, R. (2013): IT-Outsourcing-Entscheidungen. Wiesbaden: Gabler Verlag.

Schwertsik, A.R. (2013): IT-Governance als Teil der organisationalen Governance. Wiesbaden: Springer Gabler Verlag.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25101	IT-Outsourcing und IT-Governance	Prof. Dr. Heiko Gewald	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25101	PLP	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 22.01.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25607 BA: Anwendungsentwicklung SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Business Analytics: Anwendungsentwicklung
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse quantitativer Methoden und imperativer Programmiersprachen (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden lernen die Umsetzung von BA Fragestellungen mittels der statistischen Software R. Dazu gehört die Beschaffung und Aufarbeitung (Datenqualität) von Daten. Die Verbindung aus Theorie (Statistik) und der praktischen Umsetzung mittels R (Programmiersprache) wird den Studierenden helfen, sich schnell auf Fragestellungen zu konzentrieren und zu diese fachgemäß zu beantworten.

Überfachliche Kompetenzen

Die Übungen können als Gruppenarbeit abgegeben werden, dies fördert die Teamarbeit in IT-nahen Umfeld.

Ggf. besondere Methodenkompetenz

e Kombination aus Vorlesung (Theorie - Statistik), Labor (Umsetzung der Theorie mittels R) und Übungsaufgaben (eigenständiges bearbeiten von Fragestellungen) vermitteln eine Reihe an Kompetenzen: in einem abstrakten Kontext zu arbeiten und zu entwickeln, abstrakte Konzepte zu entwickeln und umzusetzen, Statistik mittels R umzusetzen, Datenhandling und -beschaffung, analytisches Denken, selbständiges Einarbeiten in Theorie um neue Fragestellungen zu bearbeiten, wissenschaftliches Arbeiten mittels BA Fragestellungen.

Lerninhalte

- Uni-/ Multivariate deskriptive Statistik
- Explorative Statistik
- Induktive Statistik
- Einführung in R / RStudio
- Algorithmen

Erstellung von Grafiken

- Datendesign
- Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Ohri, A: R for Business Analytics, Springer Verlag, 2012
Robert I. Kabacoff: R in Action, Manning, 2011 Fahrmeier:
Statistik, Springer, 2007
Thomas Rahlf: Datendesign mit R, Open Source Press, 2014

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25107	Business Analytics: Anwendungsentw.	Prof. Dr. Christian Koot	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25107	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 19.09.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25608 Business Analytics: Big Data SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Business Analytics: Big Data
Modulverantwortliche/r	Prof. Dr. Gregor Grambow
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Relationale Datenbanken, SQL, Kenntnis imperativer Programmiersprachen, Umgang mit Virtualisierungstechnologien
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen
Die Teilnehmenden können die Problematik und die Spezifika der verteilten Datenverarbeitung beurteilen. Sie können verschiedene moderne Datenbankparadigmen und -technologien einordnen und bewerten. Sie sind in der Lage, für eine bestimmte Problemstellung die korrekten Datenbankparadigmen und -technologien zu kombinieren. Die Teilnehmenden können Konzepte für verteilte Datenverarbeitung und -analyse ausarbeiten. Sie können die Spezifika von Datenstromverarbeitung beurteilen und gegen Batchverarbeitung abgrenzen. Die Studierenden haben bereits erste Erfahrungen im praktischen Umgang mit Big-Data-Technologien erlangt.

Überfachliche Kompetenzen
Die Studierenden sind in der Lage, Big Data Projekte im Team zu analysieren und zu kommunizieren.

Ggf. besondere Methodenkompetenz
Die Fähigkeit zur systematischen und strukturierten Anwendung von Lösungsmöglichkeiten aus dem Bereich Big Data wird eingeübt.

Lerninhalte

- Definition und Eigenschaften von Big Data
- Datenverteilung
- Key-Value Stores
- Wide Column Stores
- Dokumentdatenbanken
- Graphdatenbanken
- Massivparallele Datenverarbeitung
- Stream Processing
- Data Lakes

Literatur

- Perrin: Spark in Action, Second Edition, Manning Publications
- Wiese: Advanced Data Management: For SQL, NoSQL, Cloud and Distributed.

aktuelle wiss. Fachartikel

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25108	Business Analytics: Big Data	Prof. Dr. Gregor Grambow	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25108	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 07.05.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25810 Incident Response / Recovery Management SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Incident Response / Recovery Management
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen
Die Studierenden analysieren den Incident Response Prozess und diskutieren die zentralen Problemstellungen mit denen Wirtschaftsunternehmen, Behörden und andere Institutionen bei der Bewältigung kritischer Cyberangriffe konfrontiert werden. Darüber hinaus können sie die verschiedenen Rollenbilder, Aufgabenbereiche und Zuständigkeiten der beteiligten Akteure beschreiben sowie die Rolle der involvierten Sicherheitsbehörden reflektieren. Auf Basis des erworbenen Wissens und der erlangten Fähigkeiten sind die Studierenden eigenständig in der Lage Verantwortung im Incident Response und Recovery Management zu übernehmen sowie im eigenen Zuständigkeitsbereich eine effektive und effiziente Vorfallskoordination sicherzustellen.

Überfachliche Kompetenzen
Durch den hohen Anteil an selbstständigem Lernen im Team entwickeln die Studierenden ihre personalen Schlüsselqualifikationen weiter. Zur erfolgreichen Erreichung der Lernziele sind außerdem Kreativität, Verbindlichkeit, Selbstmanagement sowie die Etablierung effektiver Arbeitsstrukturen notwendig. Diese Fähigkeiten und Kompetenzen werden durch geeignete Prüfungsformen gefördert und unterstützt.

Besondere Methodenkompetenz
Die Studierenden entwickeln neben den fachlichen und überfachlichen Aspekten zudem methodische Kompetenz im Bereich des operativen Krisenmanagements. Darüber hinaus generieren die Studierenden auf Basis verschiedener Übungsfälle ein individuelles Methoden- und Instrumentenportfolio, das sie im Rahmen der beruflichen Praxis unterstützt.

Modul-Nr: 25810 Incident Response / Recovery Management SPO 511

Lerninhalte

- Herausforderungen beim Umgang mit kritischen Cyberangriffen
- Rechtliche Grundlagen
- Aufbau und Inhalte verschiedener Incident Response Modelle
- Grundlagen des Incident Response und Recovery Managements
- Rollen und Zuständigkeiten verschiedener Akteure
- Umgang mit Konflikten und krisenartigen Situationen
- Interdisziplinäre und organisationsübergreifende Zusammenarbeit
- Remote und physische Kooperationsmodi
- Ganzheitliche Vorbereitungsmaßnahmen auf kritischer Cyberangriffe
- Ganzheitliche Interventionsmaßnahmen bei kritischen Cyberangriffen
- Incident Evaluation und Nachbereitung

Literatur

Da das Modul einen sehr dynamischen, sich ständig wandelnden Wissensbereich beschreibt, wird aktuelle Literatur jeweils in der Veranstaltung benannt.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25310	Incident Response / Recovery Management	Dr. Moritz Huber	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25310	PLM	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 22.01.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25812 Cybercrime und Incident Detection SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Cybercrime und Incident Detection
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines
Die Studierenden weisen bereits Wissen im Kontext von Cybercrime auf, welches sie vertiefen und ausbauen möchten. Zusätzlich kennen sie bereits erste Risiken, die durch das Kriminalitätsphänomen entstehen können oder sind in der Lage diese einzuordnen.

Fachliche Kompetenzen
Die Studierenden verstehen den Begriff Cybercrime im engeren und weiteren Sinne und die dazugehörigen Straftaten. Sie werden mit Statistiken konfrontiert, lernen diese zu lesen und zu interpretieren. Es gibt eine Einführung in die wichtigsten Gesetze und rechtliche Grundlagen. Die Studierenden kennen die zentralen Problemstellungen, mit denen sich verschiedenste Unternehmen, der Staat oder andere Institutionen beschäftigen und lernen diese kritisch zu bewerten. Darüber hinaus werden sie in die Arbeit der Strafverfolgungsbehörden eingeführt und bekommen einen Einblick, wie die Bewältigung von Cyberangriffen dort stattfindet. Gleichzeitig wird so Wissen für die Zusammenarbeit aufgebaut. Auf Basis dieses Wissens sind die Studierenden am Ende dieses Modules in der Lage, Cybercrime Angriffe nach Möglichkeit zu erkennen und Verantwortung – auch für Dritte – in diesem Bereich zu übernehmen.

Überfachliche Kompetenzen
Die Übungen werden in Teams bearbeitet, um verschiedene Schlüsselqualifikationen weiterzuentwickeln und gemeinsam geeignete Lösungen auszuarbeiten. Durch den Charakter des berufsbegleitenden Studienganges, weisen die Studierenden hinsichtlich Vorqualifikation und Berufserfahrung unterschiedliche Hintergründe auf, was dem fachlichen und überfachlichen Austausch der Studierenden zugutekommt. Durch Selbstmanagement und geeignete Arbeitsstrukturen können Skills ausgebaut werden.

Ggf. besondere Methodenkompetenz
Um im Bedarfsfall korrekte Handlungen durchzuführen, erlernen die Studierenden das Handwerkzeug, um Cyberangriffe zu erkennen, einzudämmen und mit diversen Skills, sowie emotionaler Intelligenz entgegenwirken zu können. Hiermit werden sie in die Lage versetzt im operativen Krisenmanagement zielgerichtete Entscheidungen zu treffen und diese auch logisch begründen zu können. Mit dem Erlernten wird das individuelle Portfolio der Studenten erweitert und ergänzt. Dabei sollen sie ebenfalls in der Lage sein, ihre Entscheidungsfindung sowie die Ergebnisse geeignet zu dokumentieren und gegenüber Laien oder Fachleuten argumentativ zu verteidigen.

Lerninhalte

- Einführung Cybercrime (Entstehung, Arten, Auswirkungen, Rechtliche Grundlagen, Akteure)
- Cybercrime Arten im Detail / Angriffsmöglichkeiten
- Einführung in das Internet in Bezug auf Cybercrime
- Einführung Incident Detection
- Tools für Incident Detection
- Fallstudien aktuelle Trends u.a. Künstliche Intelligenz
- Polizeiliche Aufgaben

Literatur

- Global Hack: Hacker, die Banken ausspähen. Cyber-Terroristen, die Atomkraftwerke kapern. Geheimdienste, die unsere Handys knacken - Marc Goodman
- Cyberkriminologie: Kriminologie für das digitale Zeitalter - Thomas-Gabriel Rüdiger, Petra Saskia Bayerl
- Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen – Manfred Wernert
- Internetkriminalität: Phänomene Ermittlungshilfen Prävention (Grundlagen der Kriminalistik) - Michael Büchel und Peter Hirsch
- Cybercrime: Eine Einführung – Edith Huber

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25312	Cybercrime und Incident Detection	Eileen Köhler, M.Sc.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25312	PLS/ PLA	70% / 30%	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -**Bemerkungen**:

-

Letzte Aktualisierung: 22.01.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25811 Digitale Polizeiliche Forensik SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Digitale Polizeiliche Forensik
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden generalisieren die theoretischen Grundlagen der digitalen Forensik aus polizeilicher Perspektive und sind in der Lage, eigenständig IT-forensische Maßnahmen zu planen, in der Praxis umzusetzen und die Ergebnisse gerichtsverwertbar in Ermittlungsverfahren zu dokumentieren und argumentativ zu verteidigen.
Darüber hinaus unterscheiden sie etablierte Methoden und Instrumente der digitalen Forensik im polizeilichen Umfeld.

Überfachliche Kompetenzen

Durch den hohen Anteil an selbstständigem Lernen im Team entwickeln die Studierenden ihre personalen Schlüsselqualifikationen weiter. Zur erfolgreichen Erreichung der Lernziele sind außerdem Kreativität, Verbindlichkeit, Selbstmanagement sowie die Etablierung effektiver Arbeitsstrukturen notwendig. Diese Fähigkeiten und Kompetenzen werden durch geeignete Prüfungsformen gefördert und unterstützt.

Besondere Methodenkompetenz

Die Studierenden entwickeln neben den fachlichen Aspekten auch die Kompetenz, forensische Methoden und Tools verstehen und im Hinblick auf deren Einsatz im Sicherheitsbehördlichen Kontext hinterfragen zu können. Auch werden experimentelle Verfahrensweisen thematisiert und umgesetzt.

Lerninhalte

- Grundlagen der Digitalen Forensik aus polizeilicher Perspektive
- Vergleich der klassischen Kriminaltechnik und der digitalen Kriminaltechnik
- Vorgehensmodelle beim Umgang mit digitalen Spuren im Ermittlungsverfahren
- Untersuchung von Dateisystemen (FAT, NTFS, ExFAT, Ext)
- Digitale Spuren auf Betriebssystemen (Windows 11 und Linux)
- Smartphone-Forensik im Ermittlungsverfahren
- Maßnahmenvorbereitung und Tools im Ermittlungsverfahren
- Forensische Datensicherung im Ermittlungsverfahren
- Live-Forensik und –Analyse im Ermittlungsverfahren
- Post-Mortem Forensik und –Analyse im Ermittlungsverfahren
- Dokumentation und Berichterstellung im Ermittlungsverfahren
- Grenzen der digitalen Forensik aus polizeilicher Perspektive

Literatur

Da das Modul einen sehr dynamischen, sich ständig wandelnden Wissensbereich beschreibt, wird aktuelle Literatur jeweils in der Veranstaltung benannt.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25311	Digitale Polizeiliche Forensik	Alexander Gehrig, M.Eng., Kriminaloberrat	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25311	PLS	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 02.03.2026

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*

2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25611 Corporate Cyber Defense SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Corporate Cyber Defense
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können die Bedeutsamkeit von Corporate Cyber Defense erklären. Sie erkennen den Zusammenhang präventiver und reaktiver betrieblicher Aufgaben einer betrieblichen Sicherheitsorganisation im Zusammenwirken mit anderen staatlichen und nicht-staatlichen Organen. Die Studierenden können darüber hinaus Steuerungsmöglichkeiten und Checklisten für die Corporate Cyber Defense entwickeln und gezielt einsetzen.

Überfachliche Kompetenzen

Durch den hohen Anteil an selbstständigem Lernen im Team entwickeln die Studierenden ihre persönlichen Schlüsselqualifikationen weiter. Zur erfolgreichen Erreichung der Lernziele sind außerdem Kreativität, Verbindlichkeit, Selbstmanagement sowie die Etablierung effektiver Arbeitsstrukturen notwendig. Diese Fähigkeiten und Kompetenzen werden durch geeignete Prüfungsformen gefördert und unterstützt.

Besondere Methodenkompetenz

Die Studierenden erwerben neben den fachlichen und überfachlichen Aspekten zudem methodische Kompetenz im Bereich der Kommunikation und des Sicherheitsmanagements. Darüber hinaus entwickeln die Studierenden auf Basis verschiedener Übungsfälle ein individuelles Methoden- und Instrumentenportfolio, das sie im Rahmen der beruflichen Praxis unterstützt.

Lerninhalte

- Angriffsvektoren und -szenarien im betrieblichen Kontext
- Security Modelle: Security as a Service und unternehmensinterne Sicherheit
- Reduktion der Angriffsfläche auf eigene Infrastruktur: Asset Register, IT-Service & Asset Lifecycle Management und Risk Assurance
- Organisationsaufbau und Management der Corporate Security und dessen risikobasierte Entscheidungsprozesse
- Corporate Information Security Governance: Einhaltung des gültigen Security Framework anhand regulatorischer und rechtlicher Anforderungen, die Überführung in Security Policy und die Ableitung von Standards & Guidelines
- Corporate Cyber Defence: Überwachung, Response und die Wiederherstellung der eigenen Systeme im Falle eines Angriffs
- Vernetzung und Rückkopplung von Erkenntnissen: in verschiedenen Phasen der Informationssicherheit und in den unterschiedlichen Bereichen (z. B. regulatorische Lebenszyklen, Netzwerke und Arbeitskreise)

Literatur

Da das Modul einen sehr dynamischen, sich ständig wandelnden Wissensbereich beschreibt, wird aktuelle Literatur jeweils in der Veranstaltung benannt.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25111	Corporate Cyber Defense	Philipp Schlinsog Dipl.-Oec., M.Sc.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25111	PLS	70 %	--
25111	PLR	30 %	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 22.01.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25813 KI-gestützte IT-Sicherheit

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	KI-gestützte IT-Sicherheit
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden diskutieren die Anwendung von KI zur Verbesserung der Cybersicherheit im Kontext der Produkt- und Lösungssicherheit und des Risikomanagements. Sie entwickeln Phishing-Anwendungen und Abwehrmaßnahmen gegen indirekte Prompt Injection, Data Loss Prevention und Model Extraction.
Sie reflektieren ethische und datenschutzrechtliche Anforderungen und führen projektbasierte Experimente mit Prototypen und Evaluationen durch.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, den Einsatz bestimmter Methoden in der Gruppe zu diskutieren. Durch kleine Gruppenarbeiten sowie durch Diskussionen im Plenum wird die Sozialkompetenz gestärkt und die Studierenden befähigt, eigenverantwortlich sowohl im Team als auch selbstständig Ergebnisse zu diskutieren und zu interpretieren.

Besondere Methodenkompetenz

Die Studierenden sind in der Lage, angemessene KI-Modelle in geeigneten Funktionsbereichen der Cybersicherheit einzusetzen.

Modul-Nr: 25813 KI-gestützte IT-Sicherheit

Lerninhalte

- Grundlagen der Produktsicherheit und des Risikomanagements bei der Entwicklung von KI-Lösungen
- Social Engineering und psychologische Aspekte bei der Täuschung durch KI-Anwendungen
- Sicherheit in LLMs, Datenschutz, Data Loss Prevention, Prompt Injection in LLMs und Jailbreaking
- KI-Applikationen in der Cybersicherheit
- Ethische Aspekte, Auditierung von KI-Lösungen und zukünftige Entwicklungsfelder von KI und Cybersicherheit

Literatur

Carlini N. et al.: Extracting Training Data from Large Language Models, 2021

Greshake K. et al.: Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection, 2023
Andrew Ng: Machine Learning Yearning, 2024

ISO/IEC 62443-4-1: Cybersecurity für industrielle Automatisierungs- und Steuerungssysteme – Teil 4-1: Anforderungen an sichere Produktentwicklungs-Lebenszyklen

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25313	KI-gestützte IT-Sicherheit	Dr. Andreas Aschenbrenner.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25813	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 02.03.2026

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25612 Industrial Security / OT Security

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Industrial Security / OT Security
Modulverantwortliche/r	Prof. Dr. Sara Sommer
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können eine die Aspekte der Industrial Security eigenständig und gestalterisch bearbeiten und die zugehörigen analytischen Methoden anwenden, mit denen sie Zusammenhänge beschreiben, analysieren, erklären und beurteilen können. Ferner können sie die technischen Methoden der Industrial Security / OT Security mit den nicht-technischen Aspekten zusammenführen, um neue Problemlösungen in komplexen Zusammenhängen zu erarbeiten.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, den Einsatz bestimmter Methoden in der Gruppe zu diskutieren. Durch kleine Gruppenarbeiten sowie durch Diskussionen im Plenum wird die Sozialkompetenz gestärkt und die Studierenden befähigt, eigenverantwortlich sowohl im Team als auch selbstständig Ergebnisse zu diskutieren und zu interpretieren.

Besondere Methodenkompetenz

Die Studierenden sind in der Lage, angemessene, unternehmensspezifische Implementierungen der Industrial Security / OT Security zu entwickeln und deren Anwendung zu diskutieren.

Modul-Nr: 25612 Industrial Security / OT Security

Lerninhalte

- Grundlagen der Industrial Security / OT-Sicherheit (Definition und Bedeutung, Besonderheiten der OT-Security, Bedrohungslandschaft, Typische Angriffsvektoren, Sicherheitsanforderungen und -ziele)
- Normen und Standards (Spezifische Normen wie IEC 62443, NIST SP 800-82; Hineinwirken allgemeiner Normen wie ISO/IEC 27001 und 27019 sowie EU NIS-Richtlinie)
- Sicherheitsarchitekturen und -konzepte (Zonen- und Conduits-Modell, Defense-in-Depth, Segmentierung und Netzwerkarchitekturen)
- Risikomanagement und Bedrohungsanalyse (Risikoidentifikation und -bewertung, Bedrohungsmodelle und -analysen, Sicherheitsmaßnahmen und -kontrollen)
- Technische Maßnahmen zur OT-Sicherheit (Netzwerk-Sicherheitslösungen, Endpoint-Security, Patch-Management und Systemhärtung, Protokollsicherheit und Verschlüsselung)
- Physische Sicherheit (Zugangskontrollen, Überwachung und Schutz kritischer Infrastrukturen, Schutz vor physischen Angriffen)
- Sicherheitsbewusstsein und Schulung (Sensibilisierung der Mitarbeiter, Schulungsprogramme und Übungen, Sicherheitskultur im Unternehmen)
- Incident Response und Notfallmanagement (Erkennung und Reaktion auf Sicherheitsvorfälle, Incident Response Plans, Business Continuity und Disaster Recovery)

Literatur

Ackerman, P.: Industrial Cybersecurity, 2. Auflage, Packt 2021

Weitere Literaturhinweise werden in der Veranstaltung gegeben

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25112	Industrial Security / OT Security	Judith Herkommer, M.Eng.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25112	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 01.09.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25613 IT-Sicherheit in Dienstleistungsunternehm. SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	IT-Sicherheit in Dienstleistungsunternehmen
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden beherrschen die Werkzeuge der IT-Sicherheit in Dienstleistungsunternehmen (bspw. Risikoanalyse, Bedrohungsmodellierung und Sicherheitsarchitekturen, Incident Management) Sie können Sicherheitsmaßnahmen planen, umzusetzen und evaluieren. Sie können Aspekte wie Datenschutz und rechtliche Rahmenbedingungen kritisch diskutieren. Praktische Übungen und Fallstudien im institutionellen Kontext erklären die Anwendung der theoretischen Konzepte in realen Szenarien.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, den Einsatz bestimmter Methoden in der Gruppe zu diskutieren. Durch kleine Gruppenarbeiten sowie durch Diskussionen im Plenum wird die Sozialkompetenz gestärkt und die Studierenden befähigt, eigenverantwortlich sowohl im Team als auch selbstständig Ergebnisse zu diskutieren und zu interpretieren.

Besondere Methodenkompetenz

Die Studierenden sind in der Lage, angemessene, unternehmensspezifische Implementierungen der IT-Sicherheit in Dienstleistungsunternehmen zu entwickeln und deren Anwendung zu diskutieren.

Lerninhalte

- IT-Sicherheitsgrundlagen
- Risikoanalyse und Bedrohungsmodellierung
- Sicherheitsarchitekturen
- Datenschutz und rechtliche Aspekte
- Netzwerksicherheit und Firewalls
- Kryptografie und sichere Kommunikation
- Authentifizierung und Autorisierung
- Sicherheitsrichtlinien und Compliance
- Incident Management und Notfallpläne
- Fallstudien und Praxisübungen

Literatur Die Literatur wird in der Lehrveranstaltung bekannt gegeben.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25113	IT-Sicherheit in Dienstleistungsunt.	Philipp Schlinsog Dipl.-Oec., M.Sc.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25113	PLP	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 07.05.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25701 ABWL für Informatiker SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	ABWL für Informatiker
Modulverantwortliche/r	Prof. Dr. Anke Rahmel / Prof. Dr. Jana Wolf
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Keine spezifischen Zugangsvoraussetzungen (bewusst als Grundlagenmodul für Informatiker konzipiert).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können die wesentlichen Aspekte und Teilbereiche der Allgemeinen Betriebswirtschaftslehre bestimmen. Die Studierenden setzen sich aktiv mit wesentlichen Aspekten und Teilbereichen der Allgemeinen Betriebswirtschaftslehre auseinander, diskutieren Ansätze und Modelle und entwickeln im Dialog ein substantielles Verständnis der aktuellen Herausforderungen der ABWL. Sie sind in der Lage, verschiedene Kennzeichen, Gliederungsformen und Unternehmensbereiche von Betrieben voneinander abzugrenzen und deren Bedeutung und Zielsetzungen zu erkennen. Die Studierenden können Ziele ableiten und systematisieren sowie die Annahmen und Prinzipien von Entscheidungsmodellen diskutieren. Somit können die Studierenden erfolgreich in betriebswirtschaftlich gesteuerten Tätigkeitsfeldern für Wirtschaftsinformatiker agieren.

Überfachliche Kompetenzen

Durch Teamarbeit in den Präsenzeinheiten wird die Kommunikations- und Teamfähigkeit unter zeitlicher Restriktion und mit unterschiedlichen Persönlichkeitsstrukturen gefördert und ausgebildet. In den Online-Einheiten lernen die Studierenden, sich in neuer (virtueller) Umgebung zurechtzufinden und konstruktiv in den Unterrichtsverlauf als Teil der Gruppe durch eigenständige Beiträge einzubringen und zu behaupten.

Ggf. besondere Methodenkompetenz

Die in Gruppen- und Einzelarbeit zu erarbeitenden Themen und Fallstudien geben den Studierenden die Möglichkeit, ihr Fachwissen zu vertiefen und dabei Kompetenzen in der Selbstorganisation, der Gruppenarbeit, der Präsentationstechnik und des Zeit- und Projektmanagements auszubauen.

Lerninhalte

- Einführung in die Betriebswirtschaftslehre
- Kennzeichen und Gliederung von Betrieben
- Ableitung und Systematisierung von Zielen
- Prinzipien und Entscheidungsmodelle

Mitteleinsatz - Überblick und Rechenkategorien

Literatur

Bea, Franz Xaver, Erwin Dichtl und Marcell Schweitzer: Allgemeine Betriebswirtschaftslehre, Band 1-3

Wöhe, Günter: Einführung in die ABWL

Vahs, Dietmar und Jan Schäfer-Kunz: Einführung in die BWL

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25201	ABWL für Informatiker	Prof. Dr. Anke Rahmel / Prof. Dr. Jana Wolf	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25201	PLK 60	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.02.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*

2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25703 General Management SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	General Management
Modulverantwortliche/r	Prof. Dr. habil. Patrick Ulrich
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können die Kernelemente des strategischen Managements auf Geschäftsfeldebene sowie auf Corporate-Level bestimmen und einstufen. Die Studierenden sind in der Lage, die Notwendigkeit für strategische Entscheidungen zu erkennen. Sie können den Stellenwert und die Rolle des Top Managements bei der Ausrichtung von Unternehmen beurteilen. Die Studierenden können strategische Konzepte und Instrumente bewerten und sind in der Lage, diese auf Fallbeispiele in der Praxis anzuwenden. Die Studierenden können relevante Controlling-Instrumente klassifizieren, mit denen die Geschäftsbeziehungen, die ein Unternehmen zu wesentlichen Stakeholdergruppen (Mitarbeiter, Kunden, Kapitalgeber, Lieferanten) unterhält, nachhaltig erfolgreich gesteuert werden können. Die Studierenden können Aspekte der Unternehmenskultur und des Change Management diskutieren.

Überfachliche Kompetenzen

Die Studierenden können im Rahmen von Gruppenarbeiten Ergebnisse diskutieren und interpretieren sowie im Rahmen von Gruppenpräsentationen Ihre Präsentationstechnik verbessern.

Ggf. besondere Methodenkompetenz

Im Rahmen eines Projektes bzw. alternativ im Rahmen eines Unternehmensplanspiels können die Studierenden das Erlernte umsetzen und anwenden. Studierende sind in der Lage, Sachverhalte logisch aufzubereiten und auf Basis des Erlernten konkrete Schlussfolgerungen für praktische Anwendungsbeispiele zu ziehen.

Modul-Nr: 25703 General Management SPO 511

Lerninhalte

- Strategie und Strategiegestaltung auf Unternehmens- und Geschäftsfeldebene
- Unternehmenskultur / Change Management
- Grundlegende Herausforderungen bei der Unternehmensführung

Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Berens, W.; Brauner, H.; Strauch, J.: Due Diligence bei Unternehmens-akquisitionen, Verlag Schäffer Poeschel, 2005
Wöhe, Günter: Einführung in die Allgemeine Betriebswirtschaftslehre, Vahlen Verlag und Übungsbuch zur Allgemeinen Betriebswirtschaftslehre, Vahlen Verlag
Goold, M., Campbell, A., Alexander, M.: Corporate-Level-Strategy, 1994.
Hugenberg, H.: Strategisches Management in Unternehmen, 5. Aufl., 2008.
Johnson, G., Scholes, K.: Exploring Corporate Strategy, 6. Aufl., 2000. Dess, G., Lumpkin, G., Eisner, A.: Strategic Management, 4. Aufl., 2008.
Coenenberg, A.-G./Fischer, T. M./Günther, T.: Kostenrechnung und Kostenanalyse, 7. Aufl., 2009.
Coenenberg, A. G./Haller, A./Schultze, W.: Jahresabschluss und Jahres-abschlussanalyse, 21. Aufl., 2009
Schein, E.: Organizational culture and leadership. Jossey-Bass-Verlag, 1985.
Richter F./Timmreck C. (Hrsg.): Effiziente Unternehmenssanierung in der Praxis, Schäffer-Poeschel, 2013
Richter F. (Hrsg.): Wettbewerbsfaktor Unternehmenskultur, Schäffer-Poeschel erlag, 2015
Becker, W./Ulrich, P., Strategic Value Management, Stuttgart 2019

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25203	General Management	Prof. Dr. habil. Patrick Ulrich	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25203	PLS	Schriftliche Leistung 70%, Präsentation 30%	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.02.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25704 Organisationslehre SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Organisationslehre
Modulverantwortliche/r	Prof. Dr.-Ing. Karl-Christof Renz
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse der BWL (bspw. im grundständigen Studium, im Rahmen der qualifizierten Berufstätigkeit oder in 25701 ABWL für Informatiker erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können erklären, worin sich die Aufbau- und Ablauforganisation unterscheiden und können mit grundlegenden Konzepten aus der Organisationslehre argumentieren. Die Studierenden sind in der Lage, den grundsätzlichen Aufbau einer Organisation zu beurteilen, zu strukturieren und zu planen. Sie können im Sinne der Aufbauorganisation die grundlegenden Organisationsformen bewerten, um anhand von praktischen Fallbeispielen Verbesserungspotenziale zu ermitteln. Was die Ablauforganisation betrifft, so können die Studierenden organisatorische Abläufe analysieren und bewerten, um sie dann neu strukturieren und optimieren zu können.

Überfachliche Kompetenzen

Die Studierenden können verschiedene Problemstellungen im Plenum diskutieren und die anderen von bestimmten Lösungen überzeugen. Die Studierenden führen die Projekt- und Übungsaufgaben in Teamarbeit durch, so dass die Studierenden auch Erfahrungen mit Team- bzw. Kleingruppenarbeiten machen und den Umgang mit Problemen in Teams üben.

Ggf. besondere Methodenkompetenz

Die Studierenden führen einen Teil der Anwendungsaufgaben und Beispielfälle in Form von kleinen Projektarbeiten bzw. Übungsaufgaben durch. Die Studierenden können relevante Fragestellungen der Organisation selbständig auf Basis ihres Fachwissens reflektieren und praktische Lösungen für angewandte Fragestellungen entwickeln.

Modul-Nr: 25704 Organisationslehre SPO 511

Lerninhalte

Grundlagen der Organisation (z.B. formelle/informelle Organisation)
- Organisationstheorien (z.B. klassische, neo-klassische, moderne Organisationstheorien)
- Aufbau-Organisation (Spezialisierung/Arbeitsteilung, Koordination, Konfiguration /Leitungssysteme / Organisationsstrukturen, Delegation /Entscheidungsbefugnis, Formalisierung)
- Ablauf-Organisation (Abläufe und Prozesse, Geschäftsprozesse, Prozessgestaltung, Prozessoptimierung, Arbeitsorganisation im Verwaltungsbereich und in der Fertigung, Kapazitätsplanung, Arbeitsplatzplanung)

Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Kieser, Alfred; Walgenbach, Peter (2007): Organisation, 5., überarb. Aufl., Schäffer-Poeschel-Verlag, Stuttgart,

Vahs, Dietmar (2012): Organisation: Ein Lehr- und Managementbuch, 8., Aufl., Schäffer-Poeschel-Verlag, Stuttgart,

Schmelzer, Hermann Josef ; Sesselmann, Wolfgang (2013): Geschäftsprozessmanagement in der Praxis: Kunden zufrieden stellen - Produktivität steigern - Wert erhöhen, 8., Aufl., Hanser-Verlag

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25204	Organisationslehre	Prof. Dr.-Ing. Karl-Christof Renz	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25204	PLP	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.02.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25705 Accounting und Controlling SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Accounting und Controlling
Modulverantwortliche/r	Prof. Dr. Tobias Nemmer
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse der BWL (bspw. im grundständigen Studium, im Rahmen der qualifizierten Berufstätigkeit oder in 25701 ABWL für Informatiker erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können wesentliche Teilgebiete des Accounting und Controlling erklären und deren Schnittstellenfunktion mit Managementbezug bewerten. Die Studierenden sind in der Lage, Ziele und Instrumente der Bilanzpolitik zu diskutieren und den Einsatz verschiedener Methoden und Auswertungen der Bilanzanalyse zu bewerten. Die Studierenden analysieren verschiedene Bereiche des operativen und strategischen Controllings, um gewisse Planungs- und Kontrollinstrumente beurteilen zu können. Die Studierenden sind daher in der Lage, anspruchsvolle Tätigkeiten im betrieblichen Berichtswesen und der quantitativen Unternehmensführung und -kontrolle auszufüllen sowie Ergebnisse gegenüber Kapitalgebern zu präsentieren.

Überfachliche Kompetenzen

Die Studierenden vertiefen ihre Kenntnisse durch die Bearbeitung von Übungsaufgaben.

Ggf. besondere Methodenkompetenz

Die Studierenden können systematisch und strukturiert über die Anwendung geeigneter Methoden der Bilanzpolitik und Bilanzanalyse sowie der Ziele und Instrumente des Controllings reflektieren. Fallstudien und Beispielfälle ermöglichen die Anwendung wissenschaftlicher Methoden und einen hinreichend gehaltvollen Theorie-Praxis-Transfer.

Lerninhalte

- Grundlagen der Bilanzierung
- Ziele und Instrumente der Bilanzpolitik
- Methoden und Auswertungen der Bilanzanalyse
- Controlling als Schnittstellenfunktion des Managements
- Operatives und strategisches Controlling
- Planungs- und Kontrollinstrumente

Betriebliches Berichtswesen

Lerninhalte zum wissenschaftlichen Arbeiten:

- Analytische und empirische Untersuchung jahresabschluss-relevanter Phänomene und Zusammenhänge sowie Erarbeitung steuerungs- und kontrollrelevanter Themenfelder aus der betrieblichen Praxis mit Hilfe wissenschaftlicher Analyse- und Auswertungsmethoden.

Literatur

Coenenberg, A. G., Haller, A. & Schultze, W. (2024). Jahresabschluss und Jahresabschlussanalyse (27. Auflage). Stuttgart: Schäffer-Poeschel.

Döring, U. & Buchholz, R. (2025). Buchhaltung und Jahresabschluss: Mit Aufgaben und Lösungen (17. Auflage). Berlin: Erich Schmidt Verlag.

Schmolke, S. & Deitermann M. (2025): Industrielles Rechnungswesen – IKR (54. Auflage). Darmstadt: Winklers.

Wöhe, G. & Kußmaul H. (2022). Grundzüge der Buchführung und Bilanztechnik (11. Auflage). München: Vahlen.

Graumann, M. (2021). Kostenrechnung und Kostenmanagement mit Kontrollfragen, Übungsaufgaben und Fallstudien (7. Auflage). Herne: nwb.

Haberstock, L. (2022). Kostenrechnung I – Einführung (15. Auflage). Berlin: Erich Schmidt Verlag.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25205	Accounting und Controlling	Prof. Dr. Tobias Nemmer	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25205	PLK 60	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 02.03.2026

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25706 Corporate Finance SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Corporate Finance
Modulverantwortliche/r	Prof. Dr. Ingo Scheuermann
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse der BWL sowie ihrer quantitiven Methoden (bspw. im grundständigen Studium, im Rahmen der qualifizierten Berufstätigkeit oder in 25701 ABWL für Informatiker erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Studierende erkennen die Wichtigkeit der finanziellen Unternehmensführung. Sie erwerben u.a. die Fähigkeit, unterschiedliche Ansätze der finanziellen Unternehmensführung zu beurteilen und können somit eine Unternehmung kompetent und angemessen leiten. Studierende kennen das Zielsystem mit den quantitativen und qualitativen Elementen und können daraus typische Führungssituationen reflektieren, analysieren und entsprechende Verhaltensweisen ableiten.

Überfachliche Kompetenzen

Die Studierenden vertiefen ihre Kenntnisse durch die Bearbeitung von Übungsaufgaben.

Ggf. besondere Methodenkompetenz

Neben der Fachkompetenz wird im Rahmen des Corporate Finance besonderer Wert auf die Methodenkompetenz gelegt. Die Teilnehmer zeigen anhand von Übungsaufgaben Spezialthemen auf, die sie die Inhalte besser verstehen lassen.

Lerninhalte

- Finanzwirtschaftliche Grundlagen
- Beteiligungsfinanzierung
- Kreditfinanzierung
- Innenfinanzierung
- Finanzwirtschaftliche Unternehmensanalyse
- Grundlagen von Investitionsentscheidungen
- Statische Investitionsrechenverfahren
- Dynamische Investitionsrechenverfahren

Literatur

Pape, U., Grundlagen der Finanzierung und Investition, 4. Auflage, München, 2018

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25206	Corporate Finance	Prof. Dr. Ingo Scheuermann	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25206	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.02.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25707 Projektmanagement SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Projektmanagement
Modulverantwortliche/r	Prof. Dr. Manfred Rössle
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse der BWL sowie ihrer quantitiven Methoden (bspw. im grundständigen Studium, im Rahmen der qualifizierten Berufstätigkeit oder in 25701 ABWL für Informatiker erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden sind in der Lage, aus der Perspektive eines Projektleiters betriebliche Abläufe und Organisationsformen zu analysieren sowie Steuerungsmechanismen und entsprechendes Berichtswesen zu entwickeln. Die Studierenden können ein Projekt im Sinne der jeweils passenden Struktur und Methodik planen, in seinen jeweiligen Projektphasen konzipieren und ausarbeiten, im weiteren Verlauf steuern und kontrollieren sowie zuletzt Ergebnisse präsentieren bzw. Berichte verfassen. Die Studierenden können die Risiken eines Projektes abschätzen, unerwarteten Problemen strukturiert begegnen und Lösungen entwickeln. Die Studierenden sind in der Lage, als ausgebildete Projektleiter anspruchsvolle Aufgaben in Profit- und auch Non- Profit-Organisationen zu übernehmen.

Überfachliche Kompetenzen

Es werden Übungsprojekte in Teams bearbeitet. Dabei erleben die Studierenden Teamarbeit, Umgang mit Problemen und das Arbeiten unter Zeitdruck in der Realität. Die Studierenden sind auch in der Lage, als Teamleiter oder -mitglied kompetent und angemessen auf Probleme zu reagieren.

Ggf. besondere Methodenkompetenz

Die Studierenden können mit verschiedenen Projektmanagementmethoden umgehen und geeignete Methoden für ein konkretes Projekt abwägen. Die Studierenden wenden diese Kompetenzen an einem eigenen auszuarbeitenden Projekt an, indem sie dieses planen, durchführen, Projekt-Controlling betreiben und die Projektergebnisse präsentieren.

Lerninhalte

- Grundlagen des Projektmanagements
- Projektdefinition, Zielbildung und Projektstrukturierung
- Konzept der Projektphasen
- Planungsmethoden

Projektcontrolling und Projektsteuerung

- Präsentation und Projektberichte
- Projektaufgabe: Die Studierenden müssen in kleinen Teams selbstständig ein Projekt planen, dokumentieren und präsentieren.

Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Vorlesungsskript auf der Lernplattform Moodle
Kuster, J., et al. Handbuch Projektmanagement, 3. Auflage, Springer Verlag, 2011
Litke, H.-D., Projektmanagement, Taschenguide, 5. Auflage, Haufe Verlag, 2007
Litke, H.-D., Projektmanagement, 5. Auflage, Hanser Verlag, 2007
Gehr S. et al: Systemische Werkzeuge für erfolgreiches Projektmanagement, 1. Auflage Springer Verlag 2018
Sutherland, J.: Scrum: The Art of Doing Twice the Work in Half the Time, Random House, 1. Auflage Random House Business, 2015

Weitere Literaturangaben in der Vorlesung

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25207	Projektmanagement	Rainer Krull, M.Sc.	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25207	PLP	Note der Präsentation und Hausarbeit zum Projekt (je 50 %)	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 22.02.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25708 Marketing Management SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Marketing Management
Modulverantwortliche/r	Prof. Dr. Christina Ravens
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse der BWL (bspw. im grundständigen Studium, im Rahmen der qualifizierten Berufstätigkeit oder in 25701 ABWL für Informatiker erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden sind in der Lage, die Grundlagen des Marketings und die wichtigsten Methoden zu erklären. Die Studierenden können auf Basis der zur Verfügung stehenden Informationen und unter Berücksichtigung aller Marketing-Mix-Instrumente Marketingentscheidungen treffen. Die Studierenden können wesentliche Analysemethoden bewerten, um zu einer strategischen und operativen Planung auf Unternehmens-, Geschäftsfeld-, Marken- und Produktebene zu gelangen. Auch sind die Studierenden in der Lage, die Spezifika von verschiedenen Anwendungskontexten (z.B. Investitionsgüter vs. Dienstleistungen) zu entschlüsseln.

Überfachliche Kompetenzen

Die Studierenden bearbeiten die Fallstudien in Teams und können hierbei Strategien in Teamarbeit entwickelt und diese überzeugend kommunizieren. Auch können Sie von dem Ideenreichtum im Team profitieren, aber auch den Umgang mit Problemen in heterogenen Teams einüben.

Ggf. besondere Methodenkompetenz

Indem sie kleine Fallstudien bearbeiten, können die Studierenden die notwendige Methodenkompetenz im Bereich Marktforschung trainieren, die Fähigkeit, strategische Marketingziele zu setzen und diese auf operative Ebene herunter zu brechen sowie ihre allgemeine Analyse- und Entscheidungsfähigkeit ausbauen.

Modul-Nr: 25708 Marketing Management SPO 511

Lerninhalte

- Grundlagen des Marketings
- Informationsmanagement im Marketing
- Strategische Marketingplanung
- Operative Marketingplanung
- Marketing in speziellen Anwendungskontexten (Investitionsgüter-Marketing, Dienstleistungs-Marketing, Online- Marketing)

Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Meffert et al (2024) - Marketing: Grundlagen marktorientierter Unternehmensführung Konzepte-Instrumente-Praxisbeispiele, Springer Gabler Verlag.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25208	Marketing Management	Prof. Dr. Christina Ravens	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25208	PLP	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.02.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*

2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25709 Dienstleistungsmanagement SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Dienstleistungsmanagement
Modulverantwortliche/r	Prof. Dr. Christina Ravens
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse der BWL (bspw. im grundständigen Studium, im Rahmen der qualifizierten Berufstätigkeit oder in 25701 ABWL für Informatiker erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden sind in der Lage, wesentliche Aspekte des Dienstleistungsmanagements zu beurteilen sowie deren Anwendung in der unternehmerischen Praxis zu organisieren. Darüber hinaus können die Studierenden Handlungsalternativen kritisch bewerten und die geeignetste Alternative auswählen. Dies befähigt die Masterabsolventen dazu, in anspruchsvollen Tätigkeitsfeldern innerhalb von Dienstleistungsunternehmen zu agieren.

Überfachliche Kompetenzen

Das Semesterprojekt wird in Teams bearbeitet. Hierdurch können die Studierenden vielfältige Erfahrungen in Teamarbeit sammeln und den Umgang mit Problemen in heterogenen Teams einüben.

Ggf. besondere Methodenkompetenz

Das verbindlich zu belegende Semesterprojekt zu ausgewählten Themen des Dienstleistungsmanagements bietet den Studierenden praktische Möglichkeiten zum Erwerb von Kompetenzen in den Bereichen Projektmanagement und Präsentationstechnik. Das verbindlich zu belegende Semesterprojekt stellt hinsichtlich der wissenschaftlichen Methodik einen Vorbereitungsbaustein für die Masterarbeit

Modul-Nr: 25709 Dienstleistungsmanagement SPO 511

Lerninhalte

Charakteristika von Dienstleistungen.
- Volkswirtschaftliche Bedeutung von Dienstleistungen.
- Strategisches Dienstleistungsmarketing.
- Instrumentelles Dienstleistungsmarketing.
- Management von Dienstleistungsprozessen.
- Dienstleistungsindustrialisierung.
- Spezielle Wirtschaftsinformatik für Dienstleistungen.

Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Fließ, Sabine: Dienstleistungsmanagement - Kundenintegration gestalten und steuern; Wiesbaden; Wiesbaden; Gabler 2009

Haller, Sabine: Dienstleistungsmanagement, Grundlagen - Konzepte - Instrumente; 6. Auflage; Wiesbaden; Gabler 2015

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25209	Dienstleistungsmanagement	Prof. Dr. Christina Ravens	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25209	PLA	Semesterarbeit 50% und Take-Home Exam 50%	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 19.09.2024

[1] ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*

[2] ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25710 IoT-Geschäftsmodelle SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	IoT-Geschäftsmodelle
Modulverantwortliche/r	Prof. Dr. Markus Weinberger
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines

Die Studierenden können das Konzept des Internets der Dinge in den größeren Kontext von Digitalisierung und Internet-Technologie einordnen. Sie sind in der Lage, Auswirkungen des IoT auf verschiedene Branchen und Domänen zu bewerten. Grundlegende Wirkmechanismen des Internet der Dinge auf Geschäftsmodelle können auf eigene Ideen angewendet werden.

Fachliche Kompetenzen

Die Studierenden können IoT-Technologien im Sinne grober Architekturentwürfe anwenden und bewerten. Vor- und Nachteile von unterschiedlichen Wertversprechen und IoT-Architekturen in Bezug auf mögliche Ertragsmechaniken können diskutiert und evaluiert werden. Durch das IoT induzierte organisatorische Veränderungen in Unternehmen können in den Kontext durch neue Technologien oder Geschäftsmodelle eingeordnet werden.

Überfachliche Kompetenzen

Studierende sind in der Lage Privacy- und Security-Aspekte von IoT-Anwendungen abzuwägen und zu diskutieren.

Ggf. besondere Methodenkompetenz

Erlernte Schemata wie die Asset Integration Architecture können zur Analyse von Fallstudien eingesetzt werden. Fallstudien können mit Hilfe von Konzepten zur Darstellung und Analyse von IoT-Geschäftsmodellen ausgewertet werden.

Modul-Nr: 25710 IoT-Geschäftsmodelle SPO 511

Lerninhalte

Einführung Internet der Dinge: Zahlen und Schätzungen, IoT-Lösungen, IoT-Wertschöpfungsebenen und Technology Stack. Die Produktlogik smarter Produkte. Das Konzept des ”High Resolution Management”, was kann eine neue Qualität von Daten bewirken? Die Rolle der Corporate IT, Zusammenarbeit innerhalb der Firmen - Clash of Cultures. Beispiele aus: Smart Home, Connected Car, Industrie 4.0, Health, Agriculture. Aspekte von Security und Privacy: Risiken-Nutzen-Abwägung, Privacy-Paradox.

Einführung Geschäftsmodelle: Osterwalder-Definition und Canvas, St. Galler Magic Triangle, IoT-Einfluss auf Geschäftsmodelle und Geschäftsmodellmuster, IoT-Ertragsmechaniken im B2C- und B2B-Bereich; Komponentengeschäft für Technologieanbieter, IoT Business Model Development, Kreativitätstechniken für Use Case Development, Value Proposition Canvas, Network Diagramme, 20 Linsen für Digital Business nach Prof. Fleisch, z. B. Netzwerkeffekte Grenzkosten

Literatur

- Fleisch, E., Weinberger, M., Wortmann, F., Business Models and the Internet of Things, Bosch IoT Lab Whitepaper.

- Weinberger, M., Bilgeri, D., Fleisch, E., Bosch Flottenmanagement: Das IoT fordert die Organisation, In O. Gassmann & P. Sutter (Eds.). Führen der Digitalen Transformation. Hanser Verlag.

- Weinberger, M., Bilgeri, D., Fleisch, E., Digitale Geschäftsmodelle – 20 Linsen, In O. Gassmann & P. Sutter (Eds.). Führen der Digitalen Transformation. Hanser Verlag.

- Fleisch, E., Wortmann, F., Bilgeri, D., Weinberger, M., Revenue models and the Internet of Things? A Consumer IoT-based Investigation, Bosch IoT Lab Whitepaper

- Wortmann, F., Bilgeri, D., Weinberger, M., Fleisch, E., Ertragsmodelle im Internet der Dinge, Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung, Sonderheft 71(17), 1-28

- O. Gassmann, K. Frankenberger, M. Czik; Geschäftsmodelle entwickeln: 55 innovative Konzepte mit dem St. Galler Business Model Navigator - 2016 - Carl Hanser Verlag GmbH Co KG

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25210	IoT-Geschäftsmodelle	Prof. Dr. Markus Weinberger	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25210	PLS	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.02.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*

2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25801 Allgemeine Informatik für BWLer SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Allgemeine Informatik für BWLer
Modulverantwortliche/r	Prof. Dr. Carsten Lecon
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines
In diesem Modul erwerben die Studierenden die Fähigkeit, Grundprinzipien der Informatik, die für die Wirtschaftsinformatik relevant sind, zu analysieren.

Fachliche Kompetenzen

Auf Basis dieses Moduls können Studierende die Begriffe der Informatik, den Aufbau und die Funktionsweise von Computern erklären. Darüber hinaus können sie unterschiedliche Programmier-Paradigmen, Grundlagen der Algorithmen und Datenstrukturen und die Methoden des Software Engineerings unterschieden und hinsichtlich des jeweiligen Einsatzbereiches bewerten.

Überfachliche Kompetenzen

Die Studierenden können im Team (kleinere) Projekte bearbeiten und die Ergebnisse präsentieren sowie argumentativ verteidigen.

Ggf. besondere Methodenkompetenz

Sie verstehen, welche Methoden der Informatik für ein beliebiges Anwenderprojekt geeignet sind und können die verschiedenen Verfahren beurteilen. Zudem können sie unterschiedliche Medien zur Rezeption des Lernstoffs einschätzen und hinterfragen.

Modul-Nr: 25801 Allgemeine Informatik für BWLer SPO 511

Lerninhalte

1. Informatik/ Teilgebiete/ Anwendungen (MI, SE, WI, Medizin,…)/ Begriffe
   a. Historie
   b. Anwendungen
2. Zahlensysteme/ -Darstellung
   a. Binär, Oktal, Hexadezimal
   b. Gleitkomma-Zahlen
3. Rechnerarchitektur
4. Systemsoftware
   a. Prozessverwaltung
   b. Speicherverwaltung
5. Rechnernetze I
   a. Digitale Datenübertragung
   b. Netzwerk-Topologien
6. Rechnernetze II
   a. ISO/ OSI-Schichtenmodell
   b. Netzwerkprotokolle im Internet
   c. Verteile Verarbeitung
7. Programmierung I
   a. Programmierparadigmen
   b. Interpreter/ Compiler
8. Programmierung II
   a. Vergleich von Programmiersprachen
9. Datenstrukturen I
   a. Felder
   b. Listen
10. Datenstrukturen II
    a. Graphen
11. Datenstrukturen III
    a. Bäume
12. Algorithmen: Grundlagen
    a. Notation von Algorithmen
    b. Komplexität von Algorithmen
13. Ausgewählte Algorithmen-Paradigmen
    a. Greedy
    b. Backtracking
14. Software Engineering
    a. Auswahl von SE-Methoden
15. Theoretische Informatik
    a. Automaten
    b. Grammatiken
    c. Komplexitätsklassen

Literatur

Helmut Herold: „Grundlagen der Informatik“, Pearson Studium IT, 1. September 2017
ISBN-10: 3868943161
ISBN-13: 978-3868943160

Arne Boockmeyer: „Fit fürs Studium – Informatik: Gut vorbereitet an die Hochschule“, Rheinwerk Computing, 29. Mai 2017
ISBN-10: 3836244063
ISBN-13: 978-3836244060

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25301	Allgemeine Informatik für BWLer	Prof. Dr. Carsten Lecon	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25301	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.02.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25802 Datenbanken SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Datenbanken
Modulverantwortliche/r	Prof. Dr. Marc Fernandes
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines

Die Studierenden können den Einsatz von RDBMS planen, hierzu die Anforderungen des jeweiligen Anwendungsszenarios einschätzen und geeignete Lösungsalternativen auswählen.

Fachliche Kompetenzen

Die Studierenden können Anwendungsdaten in einem geeigneten Datenmodell repräsentieren. Sie können die Auswirkungen der Normalisierung von Datenbeständen einschätzen und finden einen geeigneten Kompromiss zwischen Konsistenz und Performance.

Überfachliche Kompetenzen

Die Studierenden können in Teams unterschiedliche Sichtweisen bei der Modellierung von Daten diskutieren und konstruktiv integrieren.

Ggf. besondere Methodenkompetenz

Die Studierenden ziehen zur Lösung von Projektaufgaben im Zusammenhang mit Datenbanken geeignete Methoden heran (bspw. ER-Modellierung, SQL).

Lerninhalte

Datenbankmodelle (bspw. Hierarchisch, Netzwerk, Relational, Objektorientiert)
- Datenmodellierung im ER-Diagramm
- Normalisierung und ihre Auswirkungen (Redundanz, Performance)
- Speicherstrukturen und Indexierung
- SQL
- Transaktionen und Mehrbenutzerbetrieb
- Sicherheitsaspekte

Literatur

Wird in der Veranstaltung bekanntgegeben.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25302	Datenbanken	Prof. Dr. Marc Fernandes	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25302	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.02.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*
2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25803 Programmieren für Data Science SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Programmieren für Data Science
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	2x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines

Die Studierenden lernen die Elemente und Funktionalitäten der Sprachen von R und Python an praktischen Programmierbeispielen anwendungszweckbezogen zu beurteilen. Auf die Nutzung der umfangreichen Methodenbibliotheken von R und Python wird dabei bewusst verzichtet. Die Studierenden entwickeln eigene Programme in diesen beiden für das Data-Science-Umfeld sehr bedeutenden Programmiersprachen.

Fachliche Kompetenzen

Die Studierenden lernen spezifizierte Funktionalitäten in den Sprachen von R und Python umzusetzen. Dabei können sie die Performanceauswirkungen unterschiedlicher Implementierungsansätze beurteilen und eigenständig Optimierungen vornehmen. Sie werden befähigt eigenständig Programme und Algorithmen zur abstrakten Problemlösung zu entwickeln.

Überfachliche Kompetenzen

Peer Instruction wird in den Rechnerübungen aktiv gefördert.

Ggf. besondere Methodenkompetenz

Die Studierenden werden in die Lage versetzt, sich eigenständig fortgeschrittene Programmiertechniken anzueignen, die über die in der Veranstaltung behandelten Techniken hinausgehen. Sie werden ferner in die Lage versetzt, den Aufbau von Computerprogrammen zu verstehen und auch auf andere Programmiersprachen zu übertragen und anzuwenden.

Lerninhalte

- Funktionale Programmierung in Python
- Daten, Datenmanipulation und Datenimport
- Datenvisualisierung durch Diagramme
- Aufbau und Entwicklung von Funktionen
- Programmierung in R
- Daten und Datenimport
- Wichtige Funktionen zur Datenmanipulation
- Besonderheiten von R

Literatur

Padmanabhan, T.R.: Programming with Python, aktuelle Auflage, Singapore: Springer.

Igual, L.; Seguí, S.: Introduction to Data Science: A Python Approach to Concepts, Techniques and Applications, aktuelle Auflage, Cham: Springer.

Weitere Literatur wird in der Vorlesung bekannt gegeben.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25303	Programmieren für Data Science	Prof. Dr. Christian Koot	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25303	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 25.03.2026

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*

2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25804 Text Mining und Web Analytics SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Text Mining und Web Analytics
Modulverantwortliche/r	Prof. Dr. Marc Fernandes
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines

Die Studierenden sind in der Lage, internet-basierte Daten wie beispielsweise Textdaten hinsichtlich potentiell enthaltener Informationen zu analysieren, auf Basis der Analyseergebnisse neue Prognosemodelle zu entwerfen und zu evaluieren sowie Analyse- und Prognosemodelle im betriebswirtschaftlichen Kontexten praktisch anzuwenden.

Fachliche Kompetenzen

Die Studierenden können grundlegende und erweiterte Verfahren des Text Mining beschreiben und deren Einsatz in unterschiedlichen Anwendungsgebieten beurteilen. Darauf aufbauend sind die Studierenden in der Lage diese Analyse- und Prognoseverfahren in unterschiedlichen betriebswirtschaftlichen Kontexten anzuwenden. Weiterhin können die Studierenden die Prognoseverfahren mittels der verfahrensspezifischen Parameter hinsichtlich der Prognosegüte optimieren. Im wissenschaftlichen Kontext können die Studierenden aus der Anwendung der Analyseverfahren neue empirische Hypothesen bilden und gegebene Hypothesen testen

Überfachliche Kompetenzen

Die Studierenden können in Zusammenarbeit untereinander reale Problemstellungen in der Gruppe analysieren, gemeinschaftliche Lösungen erarbeiten, vorstellen und die Lösungen anderer konstruktiv kritisieren.

Ggf. besondere Methodenkompetenz

Die Studierenden sind in der Lage, die Entwicklung und Evaluation von Prognosemodellen methodisch anhand des Design-Science Ansatzes der gestaltungsorientierten Wirtschaftsinformatik in der Programmiersprache Prolog durchzuführen.

Lerninhalte

- Grundlagen der Linguistik und Computerlinguistik
- Einführung in Text Mining
- Grundlagen der künstlichen Intelligenz und Pythonprogrammierung
- Einführung in Web Analytics

Literatur

- H. Angermann, N. Ramzan, Taxonomy Matching Using Background Knowledge – Linked Data, Semantic Web and Heterogeneous Repositories, Springer (2017).
- W. Ertel, Grundkurs Künstliche Intelligenz – Eine praxisorientierte Einführung, ISBN: 978-3-658-13548-5, Springer (2016).
- V. Wittpahl, Künstliche Intelligenz: Technologie, Anwendung, Gesellschaft, ISBN: 978-3-662-58041-7, Springer (2019).
- C. Zong, R. Xia and J. Zhang, Text Data Mining, ISBN: 978-981-16-0099-9, Springer (2021).
- M. Swamynathan, Mastering Machine Learning with Python in Six Steps, ISBN: 978-1-4842-4946-8, Springer (2019).
- G. Hajba, Website Scraping with Python, ISBN: 978-1-4842-3924-7, Springer (2018).
- S. Dipper, R. Klabunde und W. Mihatsch, Linguistik, ISBN: 978-3-662-55588-0, Springer (2018).
- R. Schäfer, Einführung in die grammatische Beschreibung des Deutschen, ISBN: 978-3-96110-117-7, Language Science Press (2018).
- S. Dipper, R. Klabunde, und W. Mihatsch, Linguistik, ISBN: 978-3-662-55588-0, Springer (2018).

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25304	Text Mining und Web Analytics	Christian Wilhelm, M.Sc.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25304	PLS	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 01.09.2025

[1] ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*

[2] ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25805 Machine Learning und Deep Learning SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Machine Learning und Deep Learning
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines

Die Studierenden sollen nach Absolvierung des Moduls in der Lage sein, eigenständig eine Datenanalyse mit Machine Learning-Verfahren durchzuführen. Die theoretischen Grundlagen und die praktische Anwendung der notwendigen Schritte sind bekannt, passende Algorithmen können ausgewählt und angewendet werden.

Fachliche Kompetenzen

Die Studierenden werden in die Lage versetzt, passende Verfahren für gegebene Problemstellungen auszuwählen, anzuwenden und ggf. anzupassen. Die wesentlichen Vor- und Nachteile der Verfahren und Vorgehensweisen werden anwendungsspezifisch bewertet.

Überfachliche Kompetenzen

Durch Projektarbeit wird die Zusammenarbeit in einem Team aus Data Scientists erlernt. Die argumentative Verteidigung der gefundenen Lösungen stellt hierbei einen Schwerpunkt dar.

Ggf. besondere Methodenkompetenz

Die Studierenden können mögliche Probleme bei der Datenanalyse beurteilen und können geeignete Lösungen auswählen.

Modul-Nr: 25805 Machine Learning und Deep Learning SPO 511

Lerninhalte Folgende Vorlesungsinhalte sind enthalten: Prozessschritte, Datenvorverarbeitung, Datentransformation, Distanzmaße, Merkmalsextraktion, Dimensionsreduktion, grundlegendes Machine Learning-Vorgehen, Machine Learning-Verfahren (Clustering, Klassifikation), Deep Learning. Der Fokus liegt auf der Vermittlung der Verfahren, wie beispielsweise k-nearest neighbours, decision trees, support vector machines, artificial neural networks.

Literatur wird in der Vorlesung bekanntgegeben

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25305	Machine Learning und Deep Learning	Prof. Dr. Andreas Theissler	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25305	PLP	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 01.09.2025

[1] *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
[2] *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25806 Data Mining und Visual Analytics SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Data Mining und Visual Analytics
Modulverantwortliche/r	Prof. Dr. Manfred Rössle
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines

Die Studierenden können die Ansätze aus Data Mining und Visual Analytics zur Analyse, Exploration und Entdeckung neuer Erkenntnisse beurteilen und bewerten.

Fachliche Kompetenzen

Die Studierenden können die Ansätze aus Data Mining und Visual Analytics anhand des vorliegenden Datenmaterials und verfolgten Analysezwecks kompetent auswählen, anwenden und interpretieren.

Überfachliche Kompetenzen

Peer Instruction wird aktiv gefördert. Die Studierenden können in Projektteams Probleme aus Data Mining und Visual Analytics bearbeiten und gefundene Ergebnisse argumentativ verteidigen.

Ggf. besondere Methodenkompetenz

Die Studierenden sind in der Lage, existierterende Methodenbanken aus Programmiersprachen und Standardsoftwarelösungen (bspw. Python, R, SPSS) zur Implementierung von Data-Mining- und Visual-Analytics-Anwendungen heranzuziehen.

Lerninhalte

- Definitionen und Anwendungsbereiche von Data Mining und Visual Analytics
- Einordnung und Abgrenzung zu verwandten Disziplinen mit Fokus Datenanalyse und Einschätzung der Rolle des Menschen bei der Datenanalyse (Interaktivität)
- Grundlagen der Datenanalyse: Analytische Fragestellungen und Analyseaufgaben
- CRISP-DM als generisches Vorgehensmodell für Datenanalysen
- Visual-Analytics-Prozess: Zusammenspiel von Data Mining und Visualisierung
- Best Practices: Analytische Entwurfsmuster (Preprocessing, Validation, etc.)
- Einführung und Anwendung von Methoden der Merkmalsauswahl und Dimensionsreduktion als Vorbereitung (Feature Selection, PCA, MDS, Embeddings)
- Einführung und Anwendung ausgewählter Analyse- und Visualisierungsmethoden für die explorative Datenanalyse
- Einführung und Anwendung ausgewählter Analysemethoden für die vorhersagende Datenanalyse, insbesondere Entscheidungs- und Regressionsbäume wegen der sehr guten Kombinierbarkeit mit visuellen Methoden bei der interaktiven Datenanalyse
- Methoden der Visualisierung von Lernprozessen und Analyseergebnissen (Modellen)
- Ensemble-Methoden für die Kombination von Modellen (Random Forests etc.)

- Anwendung und Nutzung von Analyseergebnissen im Unternehmen (Deployment)

Literatur

- Aggarwal, C.C. (2015): Data Mining: The Textbook. Springer.
- Azzalini, A. und Scarpa, B. (2012): Data Analysis and Data Mining: An Introduction. Oxford University Press.
- Huang, M.L. und Huang, W. (2014): Innovative Approaches of Data Visualization and Visual Analytics. IGI Global.
- Kerren, A. et al. (2008): Information Visualization: Human-Centered Issues and Perspectives. Springer.
- Kovalerchuk, B. (2018): Visual Knowledge Discovery and Machine Learning. Springer.
- Myatt, J. (2014): Making Sense of Data I: A Practical Guide to Exploratory Data Analysis and Data Mining. Wiley.
- Provost, F. und Fawcett, T. (2013): Data Science for Business. O'Reilly.
- Simoff J. et al. (2008): Visual Data Mining: Theory, Techniques and Tools for Visual Analytics. Springer.
- Wu, X. und Kumar, V. (2009): The Top Ten Algorithms in Data Mining. Chapman&Hall.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25306	Data Mining und Visual Analytics	Prof. Dr. Carsten Lanquillon	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25306	PLS	20% Referat und 80% Projektarbeit mit Abschlussbericht und Abschlusspräsentation	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 01.09.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25810 Incident Response / Recovery Management SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Incident Response / Recovery Management
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden analysieren den Incident Response Prozess und diskutieren die zentralen Problemstellungen mit denen Wirtschaftsunternehmen, Behörden und andere Institutionen bei der Bewältigung kritischer Cyberangriffe konfrontiert werden. Darüber hinaus können sie die verschiedenen Rollenbilder, Aufgabenbereiche und Zuständigkeiten der beteiligten Akteure beschreiben sowie die Rolle der involvierten Sicherheitsbehörden reflektieren. Auf Basis des erworbenen Wissens und der erlangten Fähigkeiten sind die Studierenden eigenständig in der Lage Verantwortung im Incident Response und Recovery Management zu übernehmen sowie im eigenen Zuständigkeitsbereich eine effektive und effiziente Vorfallskoordination sicherzustellen.

Überfachliche Kompetenzen

Durch den hohen Anteil an selbstständigem Lernen im Team entwickeln die Studierenden ihre personalen Schlüsselqualifikationen weiter. Zur erfolgreichen Erreichung der Lernziele sind außerdem Kreativität, Verbindlichkeit, Selbstmanagement sowie die Etablierung effektiver Arbeitsstrukturen notwendig. Diese Fähigkeiten und Kompetenzen werden durch geeignete Prüfungsformen gefördert und unterstützt.

Besondere Methodenkompetenz

Die Studierenden entwickeln neben den fachlichen und überfachlichen Aspekten zudem methodische Kompetenz im Bereich des operativen Krisenmanagements. Darüber hinaus generieren die Studierenden auf Basis verschiedener Übungsfälle ein individuelles Methoden- und Instrumentenportfolio, das sie im Rahmen der beruflichen Praxis unterstützt.

Modul-Nr: 25810 Incident Response / Recovery Management SPO 511

Lerninhalte

- Herausforderungen beim Umgang mit kritischen Cyberangriffen
- Rechtliche Grundlagen
- Aufbau und Inhalte verschiedener Incident Response Modelle
- Grundlagen des Incident Response und Recovery Managements
- Rollen und Zuständigkeiten verschiedener Akteure
- Umgang mit Konflikten und krisenartigen Situationen
- Interdisziplinäre und organisationsübergreifende Zusammenarbeit
- Remote und physische Kooperationsmodi
- Ganzheitliche Vorbereitungsmaßnahmen auf kritischer Cyberangriffe
- Ganzheitliche Interventionsmaßnahmen bei kritischen Cyberangriffen
- Incident Evaluation und Nachbereitung

Literatur

Da das Modul einen sehr dynamischen, sich ständig wandelnden Wissensbereich beschreibt, wird aktuelle Literatur jeweils in der Veranstaltung benannt.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25310	Incident Response / Recovery Management	Dr. Moritz Huber	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25310	PLM	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 22.01.2025

[1] *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*

[2] *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25811 Digitale Polizeiliche Forensik SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Digitale Polizeiliche Forensik
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden generalisieren die theoretischen Grundlagen der digitalen Forensik aus polizeilicher Perspektive und sind in der Lage, eigenständig IT-forensische Maßnahmen zu planen, in der Praxis umzusetzen und die Ergebnisse gerichtsverwertbar in Ermittlungsverfahren zu dokumentieren und argumentativ zu verteidigen.
Darüber hinaus unterscheiden sie etablierte Methoden und Instrumente der digitalen Forensik im polizeilichen Umfeld.

Überfachliche Kompetenzen

Durch den hohen Anteil an selbstständigem Lernen im Team entwickeln die Studierenden ihre personalen Schlüsselqualifikationen weiter. Zur erfolgreichen Erreichung der Lernziele sind außerdem Kreativität, Verbindlichkeit, Selbstmanagement sowie die Etablierung effektiver Arbeitsstrukturen notwendig. Diese Fähigkeiten und Kompetenzen werden durch geeignete Prüfungsformen gefördert und unterstützt.

Besondere Methodenkompetenz

Die Studierenden entwickeln neben den fachlichen Aspekten auch die Kompetenz, forensische Methoden und Tools verstehen und im Hinblick auf deren Einsatz im Sicherheitsbehördlichen Kontext hinterfragen zu können. Auch werden experimentelle Verfahrensweisen thematisiert und umgesetzt.

Modul-Nr: 25811 Digitale Polizeiliche Forensik SPO 511

Lerninhalte

- Grundlagen der Digitalen Forensik aus polizeilicher Perspektive
- Vergleich der klassischen Kriminaltechnik und der digitalen Kriminaltechnik
- Vorgehensmodelle beim Umgang mit digitalen Spuren im Ermittlungsverfahren
- Untersuchung von Dateisystemen (FAT, NTFS, ExFAT, Ext)
- Digitale Spuren auf Betriebssystemen (Windows 11 und Linux)
- Smartphone-Forensik im Ermittlungsverfahren
- Maßnahmenvorbereitung und Tools im Ermittlungsverfahren
- Forensische Datensicherung im Ermittlungsverfahren
- Live-Forensik und –Analyse im Ermittlungsverfahren
- Post-Mortem Forensik und –Analyse im Ermittlungsverfahren
- Dokumentation und Berichterstellung im Ermittlungsverfahren
- Grenzen der digitalen Forensik aus polizeilicher Perspektive

Literatur

Da das Modul einen sehr dynamischen, sich ständig wandelnden Wissensbereich beschreibt, wird aktuelle Literatur jeweils in der Veranstaltung benannt.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25311	Digitale Polizeiliche Forensik	Alexander Gehrig, M.Eng., Kriminaloberrat	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25311	PLS	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 02.03.2026

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*

2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25812 Cybercrime und Incident Detection SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Cybercrime und Incident Detection
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines
Die Studierenden weisen bereits Wissen im Kontext von Cybercrime auf, welches sie vertiefen und ausbauen möchten. Zusätzlich kennen sie bereits erste Risiken, die durch das Kriminalitätsphänomen entstehen können oder sind in der Lage diese einzuordnen.

Fachliche Kompetenzen
Die Studierenden verstehen den Begriff Cybercrime im engeren und weiteren Sinne und die dazugehörigen Straftaten. Sie werden mit Statistiken konfrontiert, lernen diese zu lesen und zu interpretieren. Es gibt eine Einführung in die wichtigsten Gesetze und rechtliche Grundlagen. Die Studierenden kennen die zentralen Problemstellungen, mit denen sich verschiedenste Unternehmen, der Staat oder andere Institutionen beschäftigen und lernen diese kritisch zu bewerten. Darüber hinaus werden sie in die Arbeit der Strafverfolgungsbehörden eingeführt und bekommen einen Einblick, wie die Bewältigung von Cyberangriffen dort stattfindet. Gleichzeitig wird so Wissen für die Zusammenarbeit aufgebaut. Auf Basis dieses Wissens sind die Studierenden am Ende dieses Modules in der Lage, Cybercrime Angriffe nach Möglichkeit zu erkennen und Verantwortung – auch für Dritte – in diesem Bereich zu übernehmen.

Überfachliche Kompetenzen
Die Übungen werden in Teams bearbeitet, um verschiedene Schlüsselqualifikationen weiterzuentwickeln und gemeinsam geeignete Lösungen auszuarbeiten. Durch den Charakter des berufsbegleitenden Studienganges, weisen die Studierenden hinsichtlich Vorqualifikation und Berufserfahrung unterschiedliche Hintergründe auf, was dem fachlichen und überfachlichen Austausch der Studierenden zugutekommt. Durch Selbstmanagement und geeignete Arbeitsstrukturen können Skills ausgebaut werden.

Ggf. besondere Methodenkompetenz
Um im Bedarfsfall korrekte Handlungen durchzuführen, erlernen die Studierenden das Handwerkzeug, um Cyberangriffe zu erkennen, einzudämmen und mit diversen Skills, sowie emotionaler Intelligenz entgegenwirken zu können. Hiermit werden sie in die Lage versetzt im operativen Krisenmanagement zielgerichtete Entscheidungen zu treffen und diese auch logisch begründen zu können. Mit dem Erlernten wird das individuelle Portfolio der Studenten erweitert und ergänzt. Dabei sollen sie ebenfalls in der Lage sein, ihre Entscheidungsfindung sowie die Ergebnisse geeignet zu dokumentieren und gegenüber Laien oder Fachleuten argumentativ zu verteidigen.

Modul-Nr: 25812 Cybercrime und Incident Detection SPO 511

Lerninhalte

- Einführung Cybercrime (Entstehung, Arten, Auswirkungen, Rechtliche Grundlagen, Akteure)
- Cybercrime Arten im Detail / Angriffsmöglichkeiten
- Einführung in das Internet in Bezug auf Cybercrime
- Einführung Incident Detection
- Tools für Incident Detection
- Fallstudien aktuelle Trends u.a. Künstliche Intelligenz
- Polizeiliche Aufgaben

Literatur

- Global Hack: Hacker, die Banken ausspähen. Cyber-Terroristen, die Atomkraftwerke kapern. Geheimdienste, die unsere Handys knacken - Marc Goodman
- Cyberkriminologie: Kriminologie für das digitale Zeitalter - Thomas-Gabriel Rüdiger, Petra Saskia Bayerl
- Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen – Manfred Wernert
- Internetkriminalität: Phänomene Ermittlungshilfen Prävention (Grundlagen der Kriminalistik) - Michael Büchel und Peter Hirsch
- Cybercrime: Eine Einführung – Edith Huber

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25312	Cybercrime und Incident Detection	Eileen Köhler, M.Sc.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25312	PLS/ PLA	70% / 30%	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -**Bemerkungen**: -

Letzte Aktualisierung: 22.01.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25813 KI-gestützte IT-Sicherheit

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	KI-gestützte IT-Sicherheit
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden diskutieren die Anwendung von KI zur Verbesserung der Cybersicherheit im Kontext der Produkt- und Lösungssicherheit und Risikomanagement. Sie entwickeln Phishing-Anwendung und Abwehrmassnahmen gegen indirekte Prompt Injection, Data Loss Prevention und Model Extraction.
Sie reflektieren ethische und datenschutzrechtliche Anforderungen und führen projektbasierte Experimente mit Prototypen und Evaluationen durch.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, den Einsatz bestimmter Methoden in der Gruppe zu diskutieren. Durch kleine Gruppenarbeiten sowie durch Diskussionen im Plenum wird die Sozialkompetenz gestärkt und die Studierenden befähigt, eigenverantwortlich sowohl im Team als auch selbstständig Ergebnisse zu diskutieren und zu interpretieren.

Besondere Methodenkompetenz

Die Studierenden sind in der Lage, angemessene KI-Modelle in geeigneten Funktionsbereichen der Cybersicherheit einzusetzen.

Modul-Nr: 25813 KI-gestützte IT-Sicherheit

Lerninhalte

- Grundlagen der Produktsicherheit und des Risikomanagement bei der Entwicklung von KI Lösungen
- Social Engineering und Psychologische Aspekte bei der Täuschung durch KI Anwendungen
- Sicherheit in LLMs, Datenschutz, Data Loss Prevention, Prompt Injection in LLMs und Jailbraking
- KI Applikationen im der Cybersicherheit
- Ethische Aspekte, Auditierung von KI Lösungen und zukünftige Entwicklungsfelder von KI und Cybersicherheit

Literatur

Carlini N. et al.: Extracting Training Data from Large Language Models, 2021

Greshake K. et al.: Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection, 2023
Andrew Ng: Machine Learning Yearning, 2024

ISO/IEC 62443-4-1: Cybersecurity für industrielle Automatisierungs- und Steuerungssysteme – Teil 4-1: Anforderungen an sichere Produktentwicklungs-Lebenszyklen

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25313	KI-gestützte IT-Sicherheit	Dr. Andreas Aschenbrenner	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25813	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

letzte Aktualisierung: 15.10.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*

2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25814 Modellgetriebene Analytics SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Modellgetriebene Analytics
Modulverantwortliche/r	Prof. Dr. Daniel Gartner
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Keine spezifischen Zugangsvoraussetzungen (bewusst als Grundlagenmodul für Informatiker konzipiert).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können wesentliche Aspekte und Teilbereiche der Modellgetriebenen Analytics erklären und anwenden. Hierzu zählen Methoden des Operations Research und der Statistik. Die Studierenden können diese Methoden bewerten und mittels des auif NumPy basierenden Data Analytics Stack anwenden sowie können deren Einsatz in verschiedenen Kontexten abschätzen.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, den Einsatz bestimmter Methoden in der Gruppe zu diskutieren. Durch kleine Gruppenarbeiten sowie durch Diskussionen im Plenum wird die Sozialkompetenz gestärkt und die Studierenden befähigt, eigenverantwortlich sowohl im Team als auch selbstständig Ergebnisse zu diskutieren und zu interpretieren.

Ggf. besondere Methodenkompetenz

Die Studierenden sind in der Lage, auf Basis der gezeigten mathematischen Methoden eigenständig angemessene mathematische Modelle zu entwickeln und deren Anwendung zu diskutieren.

Modul-Nr: 25814 Modellgetriebene Analytics SPO 511

Lerninhalte

- Operations Research
- Statistik
- Implementierungsgrundlagen (Jupyter Notebook, Python, NumPy, SciPy, pandas, statsmodels)

Literatur Wird in der Veranstaltung bekannt gegeben.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25314	Modellgetriebene Analytics	Prof. Dr. Daniel Gartner	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25314	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 05.09.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25601 IT-Outsourcing und IT-Governance SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	IT-Outsourcing und IT-Governance
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Vorkenntnisse: grundlegende BWL-Kenntnisse (Investitionsrechnung), Organisation, Prozess- und Informationsmanagement, Betriebliche Standardsoftware
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen
Die Studierenden sind in der Lage, die wichtigsten Bereiche der IT Governance und des IT Outsourcings zu beurteilen. Die Studierenden können Aufgabenstellungen und Handlungsfelder bewerten, um möglichst effiziente IT Governance Strukturen im Unternehmen aufbauen zu können. Dabei erlernen die Studierenden monetäre und nicht-monetäre Methoden, um die Positionierung und Steuerung der IT Funktion in einem Unternehmen einschätzen und optimieren zu können. Die Studierenden kennen die wichtigsten Erfolgsfaktoren für das IT-Outsourcing und sind in der Lage, ein fachliches Konzept inklusive einer zeitlichen Planung für ein IT-Outsourcingprojekt zu erstellen.

Überfachliche Kompetenzen
Die Studierenden bearbeiten mehrere Fallstudien in Teams. Dadurch werden Organisation, Planung, Aufgabenverteilung, Entscheidungsfindung im Team und Präsentationsfähigkeiten eingeübt und gefestigt.

Ggf. besondere Methodenkompetenz
Die Studierenden sind in der Lage, Problemstellung im Bereich der IT Governance und des IT Outsourcings im Unternehmenskontext zu analysieren und dafür eine unter betriebswirtschaftlichen, organisatorischen und IT Aspekten sinnvolle und nutzenstiftende Lösung zu entwickeln.

Modul-Nr: 25601 IT-Outsourcing und IT-Governance SPO 511

Lerninhalte

- IT-Business-Alignment,
- Wertbeitrag der IT,
- Organisationsstrukturen für die IT Funktion im Unternehmen,
- CobiT,
- strategische Planung, IT Strategie und Balanced Scorcard,
- Varianten des IT Outsourcings,
- Erfolgsfaktoren für das IT Outsourcing,
- Next Generation Outsourcing und
- IT Governance für IT Outsourcing
- Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Hofmann, J., Schmidt, W. (2010): Masterkurs IT-Management. 2. Auflage. Wiesbaden: Friedrich Vieweg & Sohn Verlag.

Rüter, A., Schröder, J., Göldner, A., Niebuhr Jens (2010): IT-Governance in der Praxis. 2. Auflage. Berlin, Heidelberg, New York: Springer Verlag.

Keller, W. (2012): IT Unternehmensarchitektur. 2. Auflage Heidelberg: dpunkt.verlag.

Leimeister, S. (2010): IT Outsourcing Governance. Wiesbaden: Gabler Verlag.

Pfaller, R. (2013): IT-Outsourcing-Entscheidungen. Wiesbaden: Gabler Verlag.

Schwertsik, A.R. (2013): IT-Governance als Teil der organisationalen Governance. Wiesbaden: Springer Gabler Verlag.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25101	IT-Outsourcing und IT-Governance	Prof. Dr. Heiko Gewald	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25101	PLP	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 22.01.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr.: 25602 Enterprise Resource Planning SPO 511

Studiengang	M. Sc. Cyber Security (berufsbegleitend)
Modulname	Enterprise Resource Planning
Modulverantwortliche/r	Prof. Dr. Manfred Rössle
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse in integrierten Anwendungssystemen und den Grundlagen der BWL (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen
Die Studierenden können die Bedeutung, die Bestandteile und die Funktionsweise von betriebswirtschaftlichen Anwendungssystemen (ERP) bewerten. Die Studierenden können die Tätigkeiten und das Zusammenspiel verschiedener Funktionsbereiche (Vertrieb, Beschaffung, Disposition, Rechnungswesen…) in einem Unternehmen einschätzen. Aufbauend auf diesen Kompetenzen können die Studierenden z.B. Integrations- und Optimierungsprojekte im Umfeld betriebswirtschaftlicher Anwendungssysteme und der damit verbundenen Geschäftsprozesse durchführen. Die Studierenden sind aufgrund der vielen praktischen Übungen mit mySAP ERP 6.0 in der Lage, die theoretischen Betrachtungen anzuwenden und praktisch zu überprüfen.

Überfachliche Kompetenzen
Die Studierenden sind in der Lage, Rücksicht zu nehmen auf andere und deren Daten und übernehmen Verantwortung für ihre eigenen Arbeitsergebnisse.

Ggf. besondere Methodenkompetenz
Durch das Durchspielen mehrerer Geschäftsprozesse sind die Studierenden in der Lage, die theoretischen Kenntnisse im Rahmen von mySAP ERP 6.0 in die Praxis umzusetzen und allgemeine Zusammenhänge von Theorie und Praxis zu reflektieren.

Lerninhalte

- -Bestandteile und Funktionsweise betriebswirtschaftlicher Anwendungssystem (ERP)
- -Integration (u.a. Kosten-/Nutzenbetrachtung)
- -Grundlegende Bedienung von SAP S/4HANA (für diejenigen ohne Vorkenntnisse)
- -Suchen und Finden von Daten und Informationen im System
- -Theoretische Betrachtung eines grundlegenden Vertriebsprozesses, grundlegenden Bescha eines umfassenden Auftragsabwicklungsprozesses inkl. Disposition / Verfügbarkeitsprüfung Transportterminierung / Umlagerung / Fakturierung mit allen relevanten Stamm- und Beweg Durchspielen am System.
- -Organisationseinheiten in einem Unternehmen und deren Abbildung im System
- -Bedeutung und Einblicke ins Customizing.

Literatur

Gronau, Norbert: ERP-Systeme: Architektur, Management und Funktionen des Enterprise Resource Planning; De Gruyter Studium 2021

Fitzner, Wolfgang: SAP S/4HANA: Der Grundkurs für Einsteiger und Anwender – Für SAP Fiori und SAP GUI geeignet; SAP PRESS 2021

Bohren, Martin: Vertrieb mit SAP S/4HANA: Ihr praktischer Ratgeber zu SAP S/4HANA Sales; SAP PRESS 2022

Baltes, Oliver: Materialwirtschaft mit SAP S/4HANA: Einkauf, Rechnungsprüfung, Bestandsführung und Disposition: Ihr Ratgeber zu allen wichtigen MM-Funktionen; SAP PRESS 2022

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25102	Enterprise Resource Planning	Prof. Dr.-Ing. Alexander Kolb	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25102	PLK 60	Note der theoretischen und praktischen Prüfung (je 50%)	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 07.05.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25603 Business Process Management SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Business Process Management
Modulverantwortliche/r	Prof. Dr. Marc Fernandes
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse in integrierten Anwendungssystemen und den Grundlagen der BWL (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden sind in der Lage, das breite Spektrum des Geschäftsprozessmanagements kritisch zu bewerten. Die Studierenden können ihr erworbenes theoretisches Wissen praktisch anwenden und bei der Geschäftsprozessanalyse, -modellierung und -optimierung umsetzen. Die Studierenden entwickeln Frage- und Problemstellungen aus dem Bereich des Geschäftsprozessmanagements und entwerfen geeignete Vorgehensweisen, Methoden und Techniken, um die Prozesse zu beschreiben und Probleme zu lösen. Die Studierenden sind in der Lage, geeignete Werkzeuge auszuwählen und einzusetzen, um organisatorische und technische Konzeptionen für das Geschäftsprozessmanagement anzufertigen.

Überfachliche Kompetenzen

Die Studierenden können die Anforderungen an die Gestaltung von Geschäftsprozessen einschätzen. Die Studierenden üben im Rahmen der Bearbeitung von Fallstudien, zielführend zu kommunizieren, Lösungsansätze zu moderieren und die unterschiedlichen Zielsetzungen und Anforderungen der Prozessbeteiligten zu berücksichtigen.

Ggf. besondere Methodenkompetenz

Die Studierenden können ein bestimmtes Repertoire an geeigneten methodischen Werkzeugen des Geschäftsprozessmanagements einsetzen, um Geschäftsprozesse zu analysieren, zu modellieren und zu optimieren.

Modul-Nr: 25603 Business Process Management SPO 511

Lerninhalte

1. Geschäftsprozessmanagement
2. Architektur von Geschäftsprozessen
   - Paradigmen der Geschäftsprozessmodellierung
   - Geschäftsprozesse übersichtlich strukturieren
   - Geschäftsprozessanalyse
3. Analyse von textuellen Geschäftsprozessbeschreibungen
   - Prozesslandschaft
   - Organigramm
   - Datenmodell
4. Modellierung von Geschäftsprozessen mit der BPMN

Literatur

Herbert Fischer, Albert Fleischmann, Stefan Obermeier
Geschäftsprozesse realisieren
vieweg, 2.Auflage, 2014, ISBN: 978-3-8348-1900-0

Thomas Barton, et.al.
Geschäftsprozesse – Von der Modellierung zur Implementierung
Springer Vieweg, 1. Auflage, 2017, ISBN: 978-3658172961

Thomas Allweyer
BPMN 2.0 Business Process Model and Notation
Books on Demand, 1. Auflage, 2015, ISBN: 978-3738626711

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25103	Business Process Management	Prof. Dr. Herbert Fischer	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25103	PLS	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 22.01.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25604 Business Intelligence SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Business Intelligence
Modulverantwortliche/r	Prof. Dr. Manfred Rössle
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse in integrierten Anwendungssystemen sowie den Grundlagen der BWL und Informatik (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können den ETL-Prozess bewerten und umsetzen. Sie sind in der Lage, die Herausforderungen bei der Integration operativer (Datenbank-) Systeme in ein Data Warehouse zu erkennen und hierfür passende Lösungen zu entwickeln. Die Studierenden können den Nutzen von SQL-OLAP beurteilen. Darüber hinaus erlernen die Studierenden bestimmte Analyseverfahren (Reporting, OLAP, Data Mining) und können diese werkzeugbasiert anwenden.

Überfachliche Kompetenzen

Die Studierenden können (Teil-) Verantwortung für ein Arbeitsergebnis einer Kleingruppe übernehmen und die eigenen Fähigkeiten zielgerichtet in ein Team einbringen.

Ggf. besondere Methodenkompetenz

Die Studierenden sind in der Lage das erworbene Fachwissen anhand praktischer Aufgabenstellungen anzuwenden, zu diskutieren und eigene Lösungsansätze zu entwickeln. Darüber hinaus präsentieren die Studierenden ihre Arbeitsergebnisse nach wissenschaftlichen Maßstäben.

Lerninhalte

- DataWarehousing
- Schemaintegration und multidimensionale Datenmodelle (Stern- und Schneeflocken-Schema)
- ETL-Prozess und ETL-Tools
- Reporting
- SQL-OLAP
- Data Mining
- Historisierung zur Behandlung von Slowly Changing Dimensions
- Data Mining
- Vermittlung geschieht mittels Fallstudien

Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

-Gabriel/Gluchowski/Pastwa: Data Warehouse und DataMining, w3l Verlag, 1. Auflage, 2010
- Bauer/Günzel: Data-Warehouse-Systeme, 3. Auflage 2009, dpunkt

Weitere Literaturangaben in der jeweils aktuellen Veranstaltung.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25104	Business Intelligence	Prof. Dr. Manfred Rössle	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25104	PLP	Projektarbeit 80%, Online-Präsentation 20%	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 19.09.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25605 Cloud Computing SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Cloud Computing
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse in BWL und Informatik (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen
Die Studierenden können fundiert zu technischen, wirtschaftlichen und organisatorischen Aspekten des Themenkomplexes Cloud Computing argumentieren. Auch können sie rechtliche Aspekte erörtern und Fragen der Informationssicherheit diskutieren. Die Studierenden können anhand der praktischen Beispiele den Aufwand zur Nutzung von gängigen Cloud-Technologien abschätzen. Die Studierenden sind in der Lage, Chancen und Risiken des Einsatzes von Cloud Computing in Unternehmen zu bewerten und abzuwägen. Die Studierenden können anhand der vermittelten Kriterien den Auswahlprozess einer geeigneten Cloud-Lösung für ein Unternehmen gestalten, andere von dieser überzeugen und die Lösung umsetzen.

Überfachliche Kompetenzen
Die Studierenden beschäftigen sich mit Problemstellungen, lösen diese mit wissenschaftlichen Methoden auf eigenständige Art.

Ggf. besondere Methodenkompetenz
Die Studierenden sind zur systematischen und strukturierten Anwendung verschiedener Cloud-Lösungsmöglichkeiten in der Lage, indem sie grundsätzliche Entscheidungshilfen und Checklisten an die Hand geliefert bekommen.

Lerninhalte

Einleitung
- Entstehungsgeschichte des Cloud Computing
- Charakteristika des Cloud Computing
- Klassifkation von Cloud Diensten
- Arten von Clouds
- Geschäftsmodelle für Cloud Dienste
- Entwicklung und Umsetzung einer Cloud Strategie

Docker
- Einführung in Container-Technologien
- Funktionsweise von Docker
- Beispiele
- Sicherheitsaspekte

Kubernetes
- Einführung
- Aufbau eines Kubernetes Clusters
- Arten von Kubernetes Deployments
- Beispiele
- Sicherheitsaspekte
- Kubernetes As A Service

Cybersicherheit in der Cloud
- Risiken beim Einsatz von Cloud Diensten
- Technische Maßnahmen
- Organisatorische Maßnahmen

Wirtschaftliche und organisatorische Aspekte
- Kostenabschätzung
- Anforderungen
- Auswahl des Cloud Anbieters
- Wirtschaftlichkeitsbetrachtungen
- Chancen und Risiken bei der Nutzung von Cloud Computing

Aktuelle Themen des Cloud Computing

Literatur

Lisdorf: Grundlagen des Cloud Computing: Eine nichttechnische Einführung, Springer, 2024

Erl, Monroy: Cloud Computing: Concepts, Technology, Security, and Architecture, Pearson, 2023

Vossen, Haselmann, Hoeren: Cloud Computing für Unternehmen, dpunkt Verlag, 2012

Mather, Kumaraswamy, Latif: Cloud Security and Privacy, O'Reilly, 2009

Hennrich: Cloud Computing nach der Datenschutz-Grundverordnung: Amazon Web Services, Google, Microsoft & Clouds anderer Anbieter in der Praxis, O'Reilly, 2022

Metzger, Reitz, Villar: Cloud Computing - Chancen und Risiken aus technischer und unternehmerischer Sicht, Hanser, 2011.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25105	Cloud Computing	Prof. Dr. Christoph Karg	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25105	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 09.10.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25606 In-Memory Data Management SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	In-Memory Data Management
Modulverantwortliche/r	Prof. Dr. Manfred Rössle
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse relationaler Datenbanken und ihrer Abfragesprache SQL (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden erlernen und verstehen die grundlegenden technischen Konzepte von In-Memory Datenbanken. Sie können argumentieren, welche Methoden zu welchem Performancegewinn führen. Sie können abschätzen in welchen Fällen der Einsatz einer IN-Memory Datenbank sinnvoll ist und können entsprechende Lösungen entwerfen und beurteilen.

Überfachliche Kompetenzen

Anwendungsgebiete für In-Memory Datenbanken erkennen und beurteilen. Sie können in interdisziplinären Teams Anwendungen planen, entwickeln und evaluieren.

Ggf. besondere Methodenkompetenz

Studierende können die Prinzipien der Datenorganisation anwenden und performanceorientiere Abfragen erstellen und deren Wirkung beurteilen und analysieren.

Modul-Nr: 25606 In-Memory Data Management SPO 511

Lerninhalte

Ausgangslage: SQL-Datenbanken und ihre Konsequenzen in der Unternehmensdatenverarbeitung Konzept und technische Hintergründe von In-Memory Datenbanken
Grundlegende Datenbankspeichertechniken
- Datenlayout im Hauptspeicher
- Dictionary Encoding und Compression
- Partitionierung

Im-Memory Datenbank Operatoren
- Delete, Insert, Update, Select
- Tupel Rekonstruktion
- Join

Parallelisierung

Fortgeschritten Speichertechniken
- Differentioal Buffer und Merge
- Insert Only
- Logging und Recovery

Auswirkung auf die Anwendungsentwicklung und Einsatzszenarien Praktische Anwendungsbeispiele
Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Plattner, Hasso: Lehrbuch In-Memory Data Management, Wiesbaden 2013

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25106	In-Memory Data Management	Prof. Dr. Manfred Rössle	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25106	PLS	Ausarbeitung und Präsentation in Gruppenarbeit.	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen: Die Studierenden entwickeln in Teamarbeit eine Analyseanwendung auf Basis einer In-Memorydatenbank

Letzte Aktualisierung: 19.09.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25607 BA: Anwendungsentwicklung SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Business Analytics: Anwendungsentwicklung
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse quantitativer Methoden und imperativer Programmiersprachen (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden lernen die Umsetzung von BA Fragestellungen mittels der statistischen Software R. Dazu gehört die Beschaffung und Aufarbeitung (Datenqualität) von Daten. Die Verbindung aus Theorie (Statistik) und der praktischen Umsetzung mittels R (Programmiersprache) wird den Studierenden helfen, sich schnell auf Fragestellungen zu konzentrieren und zu diese fachgemäß zu beantworten.

Überfachliche Kompetenzen

Die Übungen können als Gruppenarbeit abgegeben werden, dies fördert die Teamarbeit in IT-nahen Umfeld.

Ggf. besondere Methodenkompetenz

e Kombination aus Vorlesung (Theorie - Statistik), Labor (Umsetzung der Theorie mittels R) und Übungsaufgaben (eigenständiges bearbeiten von Fragestellungen) vermitteln eine Reihe an Kompetenzen: in einem abstrakten Kontext zu arbeiten und zu entwickeln, abstrakte Konzepte zu entwickeln und umzusetzen, Statistik mittels R umzusetzen, Datenhandling und -beschaffung, analytisches Denken, selbständiges Einarbeiten in Theorie um neue Fragestellungen zu bearbeiten, wissenschaftliches Arbeiten mittels BA Fragestellungen.

Lerninhalte

- Uni-/ Multivariate deskriptive Statistik
- Explorative Statistik
- Induktive Statistik
- Einführung in R / RStudio
- Algorithmen

Erstellung von Grafiken

- Datendesign
- Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Ohri, A: R for Business Analytics, Springer Verlag, 2012
Robert I. Kabacoff: R in Action, Manning, 2011 Fahrmeier:
Statistik, Springer, 2007
Thomas Rahlf: Datendesign mit R, Open Source Press, 2014

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25107	Business Analytics: Anwendungsentw.	Prof. Dr. Christian Koot	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25107	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 19.09.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25608 Business Analytics: Big Data SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Business Analytics: Big Data
Modulverantwortliche/r	Prof. Dr. Gregor Grambow
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Relationale Datenbanken, SQL, Kenntnis imperativer Programmiersprachen, Umgang mit Virtualisierungstechnologien
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen
Die Teilnehmenden können die Problematik und die Spezifika der verteilten Datenverarbeitung beurteilen. Sie können verschiedene moderne Datenbankparadigmen und -technologien einordnen und bewerten. Sie sind in der Lage, für eine bestimmte Problemstellung die korrekten Datenbankparadigmen und -technologien zu kombinieren. Die Teilnehmenden können Konzepte für verteilte Datenverarbeitung und -analyse ausarbeiten. Sie können die Spezifika von Datenstromverarbeitung beurteilen und gegen Batchverarbeitung abgrenzen. Die Studierenden haben bereits erste Erfahrungen im praktischen Umgang mit Big-Data-Technologien erlangt.

Überfachliche Kompetenzen
Die Studierenden sind in der Lage, Big Data Projekte im Team zu analysieren und zu kommunizieren.

Ggf. besondere Methodenkompetenz
Die Fähigkeit zur systematischen und strukturierten Anwendung von Lösungsmöglichkeiten aus dem Bereich Big Data wird eingeübt.

Lerninhalte

- Definition und Eigenschaften von Big Data
- Datenverteilung
- Key-Value Stores
- Wide Column Stores
- Dokumentdatenbanken
- Graphdatenbanken
- Massivparallele Datenverarbeitung
- Stream Processing
- Data Lakes

Literatur

- Perrin: Spark in Action, Second Edition, Manning Publications
- Wiese: Advanced Data Management: For SQL, NoSQL, Cloud and Distributed.

aktuelle wiss. Fachartikel

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25108	Business Analytics: Big Data	Prof. Dr. Gregor Grambow	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25108	PLK 90	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 07.05.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*

2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25609 Informationsmanagement SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Informationsmanagement
Modulverantwortliche/r	Prof. Dr. Marc Fernandes
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	Grundlegende Kenntnisse quantitativer Methoden und imperativer Programmiersprachen (bspw. im grundständigen Studium oder im Rahmen der qualifizierten Berufstätigkeit erworben).
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Nach der Veranstaltung verfügen die Teilnehmer über die Kompetenz, die Aufgaben und Prozesse im Zusammenhang mit dem Management der Ressource Information, die im Unternehmen meist im Einflussbereich eines Chief Information Officers angesiedelt sind, zu bewerten. Die Studierenden sind in der Lage, die Dienstleistungen, Aufgaben, Planungsobjekte und Organisation einer IT-Abteilung im Unternehmen zu analysieren. Der Besuch der Veranstaltung befähigt die Studierenden zu Folgendem:

- Die Rolle der Ressource Information und des Information Managements im Unternehmen verstehen und anhand ihrer Entwicklung beschreiben können.
- Die wesentlichen Prozesse des IT Managements verstehen und in Zusammenhang bringen können.
- Methoden zur Erfassung und Administration von Anforderungen kennen und einsetzen können.
- IT Strategien nachvollziehen und bezüglich der Angleichung (Alignment) zur Unternehmensstrategie bewerten können.
- IT Landschaften analysieren, bewerten und Vorschläge zu deren Verbesserung machen können
- IT Projektportfolios bewerten und priorisieren können.
- Die Prozesse und Aufgaben des IT Servicemanagements anhand der IT Infrastructure Library (ITIL) strukturieren können.

Die Aufgaben der IT Governance verstehen, strukturieren und analysieren können.

Überfachliche Kompetenzen

Die Fallstudien werden in der Regel in Teams bearbeitet. Hierdurch können die Studierenden vielfältige Erfahrungen in Teamarbeit sammeln und den Umgang mit Problemen in heterogenen Teams einüben.

Ggf. besondere Methodenkompetenz

Die Studierenden lernen Methoden, die das Planen, die Projektierung und den Betrieb von IT Systemen und IT System Landschaften ermöglichen. Insbesondere werden Methoden des Anforderungsmanagements, des Projekt-Portfoliomanagement und des Enterprise Architektur-Managements vermittelt. Dazu werden Fallstudien eingesetzt.

Modul-Nr: 25609 Informationsmanagement SPO 511

Lerninhalte

1. IT-Management und Wert der IT – Herausforderungen und Rollenverständnis
2. IT Strategie
3. Demand Management
4. Enterprise Architecture Management/ IT Architektur Management
5. Project Portfolio Management
6. Service Management
7. IT Governance

Wissenschaftliches Fallbeispiel (IMRAD) zum Inhalt des Moduls.

Literatur

Tielmeyer, Handbuch IT Management, Hanser 8. Auflage 2023
Hanschke, Strategische Planung in Business und IT – lean, agil & systematisch: Strategien, Roadmap und Leitplanken für den ständigen Wandel einfach & effektiv, Springer 2024

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25109	Informationsmanagement	Prof. Dr. Joerg-Oliver Vogt	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25109	PLA	Ausarbeitung und Präsentation in Gruppenarbeit	--

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 15.10.2025

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25611 Corporate Cyber Defense SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Corporate Cyber Defense
Modulverantwortliche/r	Prof. Dr. Christoph Karg
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können die Bedeutsamkeit von Corporate Cyber Defense erklären. Sie erkennen den Zusammenhang präventiver und reaktiver betrieblicher Aufgaben einer betrieblichen Sicherheitsorganisation im Zusammenwirken mit anderen staatlichen und nicht-staatlichen Organen. Die Studierenden können darüber hinaus Steuerungsmöglichkeiten und Checklisten für die Corporate Cyber Defense entwickeln und gezielt einsetzen.

Überfachliche Kompetenzen

Durch den hohen Anteil an selbstständigem Lernen im Team entwickeln die Studierenden ihre persönlichen Schlüsselqualifikationen weiter. Zur erfolgreichen Erreichung der Lernziele sind außerdem Kreativität, Verbindlichkeit, Selbstmanagement sowie die Etablierung effektiver Arbeitsstrukturen notwendig. Diese Fähigkeiten und Kompetenzen werden durch geeignete Prüfungsformen gefördert und unterstützt.

Besondere Methodenkompetenz

Die Studierenden erwerben neben den fachlichen und überfachlichen Aspekten zudem methodische Kompetenz im Bereich der Kommunikation und des Sicherheitsmanagements. Darüber hinaus entwickeln die Studierenden auf Basis verschiedener Übungsfälle ein individuelles Methoden- und Instrumentenportfolio, das sie im Rahmen der beruflichen Praxis unterstützt.

Modul-Nr: 25611 Corporate Cyber Defense SPO 511

Lerninhalte

- Angriffsvektoren und -szenarien im betrieblichen Kontext
- Security Modelle: Security as a Service und unternehmensinterne Sicherheit
- Reduktion der Angriffsfläche auf eigene Infrastruktur: Asset Register, IT-Service & Asset Lifecycle Management und Risk Assurance
- Organisationsaufbau und Management der Corporate Security und dessen risikobasierte Entscheidungsprozesse
- Corporate Information Security Governance: Einhaltung des gültigen Security Framework anhand regulatorischer und rechtlicher Anforderungen, die Überführung in Security Policy und die Ableitung von Standards & Guidelines
- Corporate Cyber Defence: Überwachung, Response und die Wiederherstellung der eigenen Systeme im Falle eines Angriffs
- Vernetzung und Rückkopplung von Erkenntnissen: in verschiedenen Phasen der Informationssicherheit und in den unterschiedlichen Bereichen (z. B. regulatorische Lebenszyklen, Netzwerke und Arbeitskreise)

Literatur

Da das Modul einen sehr dynamischen, sich ständig wandelnden Wissensbereich beschreibt, wird aktuelle Literatur jeweils in der Veranstaltung benannt.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25111	Corporate Cyber Defense	Philipp Schlinsog Dipl.-Oec., M.Sc.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25111	PLS	70 %	--
25111	PLR	30 %	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -**Bemerkungen**:

-

Letzte Aktualisierung: 22.01.2025

[1] *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*

[2] *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25612 Industrial Security / OT Security

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Industrial Security / OT Security
Modulverantwortliche/r	Prof. Dr. Sarah Sommer
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können eine die Aspekte der Industrial Security eigenständig und gestalterisch bearbeiten und die zugehörigen analytischen Methoden anwenden, mit denen sie Zusammenhänge beschreiben, analysieren, erklären und beurteilen können. Ferner können sie die technischen Methoden der Industrial Security / OT Security mit den nicht-technischen Aspekten zusammenführen, um neue Problemlösungen in komplexen Zusammenhängen zu erarbeiten.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, den Einsatz bestimmter Methoden in der Gruppe zu diskutieren. Durch kleine Gruppenarbeiten sowie durch Diskussionen im Plenum wird die Sozialkompetenz gestärkt und die Studierenden befähigt, eigenverantwortlich sowohl im Team als auch selbstständig Ergebnisse zu diskutieren und zu interpretieren.

Besondere Methodenkompetenz

Die Studierenden sind in der Lage, angemessene, unternehmensspezifische Implementierungen der Industrial Security / OT Security zu entwickeln und deren Anwendung zu diskutieren.

Modul-Nr: 25612 Industrial Security / OT Security

Lerninhalte

- Grundlagen der Industrial Security / OT-Sicherheit (Definition und Bedeutung, Besonderheiten der OT-Security, Bedrohungslandschaft, Typische Angriffsvektoren, Sicherheitsanforderungen und -ziele)
- Normen und Standards (Spezifische Normen wie IEC 62443, NIST SP 800-82; Hineinwirken allgemeiner Normen wie ISO/IEC 27001 und 27019 sowie EU NIS-Richtlinie)
- Sicherheitsarchitekturen und -konzepte (Zonen- und Conduits-Modell, Defense-in-Depth, Segmentierung und Netzwerkarchitekturen)
- Risikomanagement und Bedrohungsanalyse (Risikoidentifikation und -bewertung, Bedrohungsmodelle und -analysen, Sicherheitsmaßnahmen und -kontrollen)
- Technische Maßnahmen zur OT-Sicherheit (Netzwerk-Sicherheitslösungen, Endpoint-Security, Patch-Management und Systemhärtung, Protokollsicherheit und Verschlüsselung)
- Physische Sicherheit (Zugangskontrollen, Überwachung und Schutz kritischer Infrastrukturen, Schutz vor physischen Angriffen)
- Sicherheitsbewusstsein und Schulung (Sensibilisierung der Mitarbeiter, Schulungsprogramme und Übungen, Sicherheitskultur im Unternehmen)
- Incident Response und Notfallmanagement (Erkennung und Reaktion auf Sicherheitsvorfälle, Incident Response Plans, Business Continuity und Disaster Recovery)

Literatur

Ackerman, P.: Industrial Cybersecurity, 2. Auflage, Packt 2021

Weitere Literaturhinweise werden in der Veranstaltung gegeben

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25112	Industrial Security / OT Security	Judith Herkommer, M.Eng.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25112	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 01.09.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*

2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25613 IT-Sicherheit in Dienstleistungsunternehm. SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	IT-Sicherheit in Dienstleistungsunternehmen
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden beherrschen die Werkzeuge der IT-Sicherheit in Dienstleistungsunternehmen (bspw. Risikoanalyse, Bedrohungsmodellierung und Sicherheitsarchitekturen, Incident Management) Sie können Sicherheitsmaßnahmen planen, umzusetzen und evaluieren. Sie können Aspekte wie Datenschutz und rechtliche Rahmenbedingungen kritisch diskutieren. Praktische Übungen und Fallstudien im institutionellen Kontext erklären die Anwendung der theoretischen Konzepte in realen Szenarien.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, den Einsatz bestimmter Methoden in der Gruppe zu diskutieren. Durch kleine Gruppenarbeiten sowie durch Diskussionen im Plenum wird die Sozialkompetenz gestärkt und die Studierenden befähigt, eigenverantwortlich sowohl im Team als auch selbstständig Ergebnisse zu diskutieren und zu interpretieren.

Besondere Methodenkompetenz

Die Studierenden sind in der Lage, angemessene, unternehmensspezifische Implementierungen der IT-Sicherheit in Dienstleistungsunternehmen zu entwickeln und deren Anwendung zu diskutieren.

Lerninhalte

- IT-Sicherheitsgrundlagen
- Risikoanalyse und Bedrohungsmodellierung
- Sicherheitsarchitekturen
- Datenschutz und rechtliche Aspekte
- Netzwerksicherheit und Firewalls
- Kryptografie und sichere Kommunikation
- Authentifizierung und Autorisierung
- Sicherheitsrichtlinien und Compliance
- Incident Management und Notfallpläne
- Fallstudien und Praxisübungen

Literatur Die Literatur wird in der Lehrveranstaltung bekannt gegeben.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25113	IT-Sicherheit in Dienstleistungsunt.	Philipp Schlinsog Dipl.-Oec., M.Sc.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25113	PLP	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 07.05.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*

2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25614 Industrial Analytics

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Industrial Analytics
Modulverantwortliche/r	Prof. Dr. Sara Sommer
Modulart	Wahlpflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	1x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	105 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden können die grundlegenden Konzepte und Methoden der Datenanalyse im industriellen Kontext (darunter auch fortgeschrittene Analysetechniken wie maschinelles Lernen sowie statistische Modelle und Optimierungsmodell) erklären. Sie können die Methoden zur Datenaufbereitung, -visualisierung und -interpretation gezielt einsetzen. Ferner können sie Industrial Analytics-Lösungen zur Entscheidungsunterstützung implementieren und bewerten.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, den Einsatz bestimmter Methoden in der Gruppe zu diskutieren. Durch kleine Gruppenarbeiten sowie durch Diskussionen im Plenum wird die Sozialkompetenz gestärkt und die Studierenden befähigt, eigenverantwortlich sowohl im Team als auch selbstständig Ergebnisse zu diskutieren und zu interpretieren.

Besondere Methodenkompetenz

Die Studierenden sind in der Lage, angemessene mathematische Modelle im industriellen Kontext zu entwickeln und deren Anwendung zu diskutieren.

Modul-Nr: 25614 Industrial Analytics

Lerninhalte

- Einführung in Industrial Analytics
- Datenmanagement (Datenerfassung, -aufbereitung, -integration)
- Statistische Methoden (Deskriptive Statistik, Datenanalyse, Hypothesentests)
- Maschinelles Lernen (Überwachtes/unüberwachtes Lernen, Modellbewertung
- Datenvisualisierung (Tools, Techniken, Dashboards)
- Praxisprojekte und Fallstudien
- Ethische und rechtliche Aspekte

Literatur

Hill, R.; Berry, S.: Guide to Industrial Analytics : Solving Data Science Problems for Manufacturing and the Internet of Things; Springer Intl. Publishing 2021

Weitere Literaturhinweise werden in der Veranstaltung gegeben

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art	SWS	CP
25114	Industrial Analytics	Sahil-Jai Arora, M.Sc.	V, Ü, L	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25114	PLA	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 08.09.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*

2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 25901 Überfachliche Kompetenzen SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Überfachliche Kompetenzen
Modulverantwortliche/r	Prof. Dr. Daniel Gartner
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	1 Term (3 Monate)
Zahl LV	Die Präsenz im Umfang von 3 SWS verteilt sich auf 1 SWS im Rahmen von eineinhalb Präsenztagen und 2 SWS Online-Präsenz (ca. 6-10 x Online-Präsenzen)
Angebotshäufigkeit	2x Jahr
Credits	5 CP
Workload Präsenz	45 Stunden
Workload Selbststudium	300 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Englisch

Modulziele

Allgemeines
Die Studierenden analysieren wissenschaftliche Methoden, um eine wissenschaftliche Ausarbeitung zu entwickeln. Ziel ist hierbei, die Studierenden auf ein Niveau zu heben, sodass eine wissenschaftliche Ausarbeitung in einem wissenschaftlichen Peer-Review-Prozess bestehen könnte. Die geschaffenen Kenntnisse dienen als Basis für die Master-Arbeit sowie ggf. wissenschaftlicher Publikationen.

Fachliche Kompetenzen
Die Studierenden werden in die Lage versetzt, sich eigenständig, analytisch und kritisch mit aktuellen Forschungsthemen zu beschäftigen und daraus Forschungslücken und Forschungsfragen abzuleiten. Dies dient als Grundlage, eine wissenschaftliche Arbeit zu verfassen, welche einen wissenschaftlichen Beitrag leistet („contribution to the body of knowledge“). Hierbei schlüsseln die Studierenden vertieftes Wissen zu Forschungsmethoden, zur Erarbeitung des Stands der Technik und zur Erarbeitung von Forschungslücken und Forschungsfragen als Voraussetzung für Neuheiten und wissenschaftliche Beiträge eigener Ausarbeitungen, auf. Durch das Entwickeln eines wissenschaftlichen Papers innerhalb des Moduls vertiefen die Studierenden ihre Fähigkeit eine Abhandlung auszuarbeiten, die gehobenen wissenschaftlichen Kriterien entspricht (Niveau: internationaler wissenschaftlicher Peer-Review-Prozess). Dies wird ergänzt um Diskussion von Vorgehensweisen zum Publizieren in der wissenschaftlichen Community.

Überfachliche Kompetenzen
Peer Instruction wird durch die Zusammenarbeit mit weiteren Studierenden aktiv gefördert. Die Studierenden können in Projektteams wissenschaftliche Standpunkte darstellen, gefundene Ergebnisse argumentativ verteidigen und reflektieren.

Besondere Methodenkompetenz
Die Studierenden erwerben und vertiefen Fähigkeiten zu analytischem, forschungsmethodischem Vorgehen. Durch das Verfassen einer wissenschaftlichen Abhandlung in Zusammenarbeit mit weiteren Studierenden wird darüber hinaus Problemlösungskompetenz und Sozialkompetenz gefördert.

Lerninhalte

- Vorstellung und Gegenüberstellung von Forschungsmethoden
- Typische Inhalte wissenschaftlicher Ausarbeitungen
- Literaturrecherche und analytisches Lesen wissenschaftlicher Arbeiten
- Erarbeiten von Forschungslücken und Forschungsfragen
- Finden von Neuheiten und wissenschaftlichen Beiträgen der wissenschaftlichen Ausarbeitung
- Schreibprozess
- Vorgehensweisen zum Publizieren in der wissenschaftlichen Community

Literatur

Wayne Booth et al. (2016), The Craft of Research. University of Chicago Press.
Michael Alley (2018), The Craft of Scientific Writing. Springer.
Hannah Snyder. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339.

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
25401	Scientific Writing	Felix Gerschner, M.Sc.	V, Ü	3	5

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
25401	PLS	Modulprüfung	--

Voraussetzungen für die Zulassung zur Modulprüfung: -

Weitere studienbegleitende Rückmeldungen: -

Bemerkungen: -

Letzte Aktualisierung: 08.09.2025

1 ***E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung*** *(SPO-Ba § 48; SPO-Ma § 38)*
2 ***PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit*** *(SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 91031 Projektarbeit SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Projektarbeit
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	3 Monate
Zahl LV	
Angebotshäufigkeit	
Credits	10 CP
Workload Präsenz	
Workload Selbststudium	300 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden sind in der Lage sich mit einer dem Fachgebiet entnommenen Problemstellung selbstständig kritisch auseinanderzusetzen und mit den erlernten, wissenschaftlichen Methoden ausführlich darzustellen. In der Masterarbeit ist der Studierende befähigt innerhalb einer vorgegebenen Frist, die Aufgabenstellung selbstständig, strukturiert und nach wissenschaftlichen Methoden, unter Nutzung des bis dahin im Studium Gelernten auszuarbeiten.
Zentraler Bestandteil ist die schriftliche, wissenschaftlich fundierte Ausarbeitung der Arbeitsergebnisse und Diskussion derselben unter Miteinbeziehung von Literatur und anderen Quellen.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, eigenverantwortlich und termingerecht ein Projekt zu bearbeiten, indem sie komplexe Probleme analysieren, strukturieren und lösen können, im Rahmen einer praxisrelevanten Fragestellung.

Ggf. besondere Methodenkompetenz

Die Studierenden können die Grundlagen der Forschungsmethodik anwenden, indem sie relevante Informationen sammeln, eigenständig Projekte bearbeiten, Daten interpretieren, bewerten und geeignete Methoden auswählen, um diese dann professionell einzusetzen.

Modul-Nr: 91031 Projektarbeit SPO 511

Lerninhalte Selbständige Bearbeitung eines Themas aus den Bereichen Wirtschaftsinformatik oder Betriebswirtschaftslehre

Literatur

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
91402	Projektarbeit	Professoren der Hochschule Aalen			

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
91402	PLS		

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 19.09.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*

2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 9999 Masterarbeit SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Masterarbeit
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	8 Monate
Zahl LV	
Angebotshäufigkeit	
Credits	24 CP
Workload Präsenz	
Workload Selbststudium	720 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in anderen Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Fachliche Kompetenzen

Die Studierenden sind in der Lage sich mit einer dem Fachgebiet entnommenen, komplexen Problemstellung selbstständig kritisch auseinanderzusetzen und mit den erlernten, wissenschaftlichen Methoden ausführlich darzustellen. In der Masterarbeit ist der Studierende befähigt innerhalb einer vorgegebenen Frist, die Aufgabenstellung selbstständig, strukturiert und nach wissenschaftlichen Methoden, unter Nutzung des bis dahin im Studium Gelernten auszuarbeiten. Zentraler Bestandteil ist die schriftliche, wissenschaftlich fundierte Ausarbeitung der Arbeitsergebnisse und Diskussion derselben unter Miteinbeziehung von Literatur und anderen Quellen.
Im Kolloquium ist der Studierende befähigt, seine Arbeit zusammenfassend, verständlich darzustellen und unter objektiven Gesichtspunkten mit dem Fachpublikum zu diskutieren.

Überfachliche Kompetenzen

Die Studierenden sind in der Lage, eigenverantwortlich und termingerecht ein Projekt zu bearbeiten, indem sie komplexe Probleme analysieren, strukturieren und lösen können, im Rahmen einer praxisrelevanten Fragestellung. Die Studierenden sind fähig, sich selbstständig zu organisieren, indem sie in angemessener Weise Prioritäten setzen und den Belastungen während des Moduls standhalten. Sie können Kritik annehmen und sich konstruktiv damit auseinandersetzen.

Ggf. besondere Methodenkompetenz

Die Studierenden können die Grundlagen der Forschungsmethodik anwenden, indem sie relevante Informationen sammeln, eigenständig Projekte bearbeiten, Daten interpretieren, bewerten und geeignete Methoden auswählen, um diese dann professionell einzusetzen. Sie können komplexe fachbezogene Inhalte klar und zielgruppengerecht präsentieren und verteidigen, sowohl mündlich als auch schriftlich. Sie sind in der Lage effiziente Arbeitstechniken zu entwickeln.

Modul-Nr: 9999 Masterarbeit SPO 511

Lerninhalte Selbständige Bearbeitung eines Forschungsthemas aus den Bereichen Wirtschaftsinformatik oder Betriebswirtschaftslehre. Die Masterarbeit muss für ein wissenschaftliches Publikum als mündliche Präsentation aufbereitet werden.

Literatur

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
9999	Masterarbeit	Professoren der Hochschule Aalen			

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
9999	PLS		

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 19.09.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*

Modul-Nr: 91999 Studium Generale SPO 511

Studiengang	M.Sc. Cyber Security (berufsbegleitend)
Modulname	Studium Generale
Modulverantwortliche/r	Prof. Dr. Christian Koot
Modulart	Pflichtmodul
Studiensemester	
Moduldauer	
Zahl LV	
Angebotshäufigkeit	
Credits	1 CP
Workload Präsenz	
Workload Selbststudium	30 Stunden
Teilnahmevoraus-setzung Modul	
Verwendung in ande-ren Studiengängen	Master WIB Master CSC Master DSB
Sprache	Deutsch

Modulziele

Allgemeines

In den Veranstaltungen im Rahmen des Studium Generale wird die ganzheitliche Bildung der Studierenden gefördert. Die Veranstaltungen ergänzen das jeweilige Fachstudium durch interdisziplinäre Themengebiete. Die Angebote ermöglichen den Studierenden die Auseinandersetzung mit grundlegenden wissenschaftlichen Themenfeldern sowie aktuellen Fragenstellungen.
Die Studierenden erwerben Schlüsselqualifikationen, die für ihr späteres Berufsleben von Bedeutung sind. Um die sozialen Kompetenzen der Studierenden zu stärken, wird das ehrenamtliche Engagement gefördert.

Fachliche Kompetenzen

Die Studierenden kennen überfachliche komplexe Themengebiete und können deren Zusammenhänge einordnen. Sie sind in der Lage, sich mit gesellschaftspolitischen Fragen selbstständig auseinanderzusetzen.

Überfachliche Kompetenzen

Je nach Wahl der Veranstaltungen stärken die Studierenden ihre Fähigkeit zur Teamarbeit, verbessern ihr Zeitmanagement und/oder Konfliktmanagement oder vertiefen ihre Präsentationskompetenz. Die Studierenden sind in der Lage, die erlangten Kompetenzen zielgerecht einzusetzen. Die Studierenden erkennen die Bedeutung des ehrenamtlichen Engagements für die persönliche Entwicklung und für die Gesellschaft.

Lerninhalte In jedem Semester wird ein thematischer Schwerpunkt angeboten. Die jeweiligen Lerninhalte sind flexibel und somit jedes Semester dem jeweils erstellten Programm zu entnehmen. Verschiedene Veranstaltungen aus dem Angebot des CareerCenters und der Studiengänge

Literatur

Enthaltene Lehrveranstaltungen (LV)

LV-Nr.	Name der Lehrveranstaltung	Lehrender	Art[1]	SWS	CP
91999	Studium Generale				

Modulprüfung (Voraussetzung für die Vergabe von Leistungspunkten)

LV-Nr.	Art und Dauer des Leist.nachweises[2]	Ermittlung der Modulnote	Bemerkung
91999	PLS	Die Studierenden erstellen einen Gesamtbericht über die besuchten Veranstaltungen oder Tätigkeiten.	

Voraussetzungen für die Zulassung zur Modulprüfung

Weitere studienbegleitende Rückmeldungen

Bemerkungen:

Letzte Aktualisierung: 19.09.2024

1 *E Exkursion, L Labor, P Projekt, S Seminar, Ü Übung, V Vorlesung (SPO-Ba § 48; SPO-Ma § 38)*
2 *PLK Klausur, PLS Sonstige schriftliche Arbeiten, PLM Mündliche Prüfung, PLR Referat, PLP Projektarbeit, PLL Laborarbeit, PLE Entwurf, PLA Praktische Arbeit (SPO-Ba § 15; SPO-Ma § 12)*