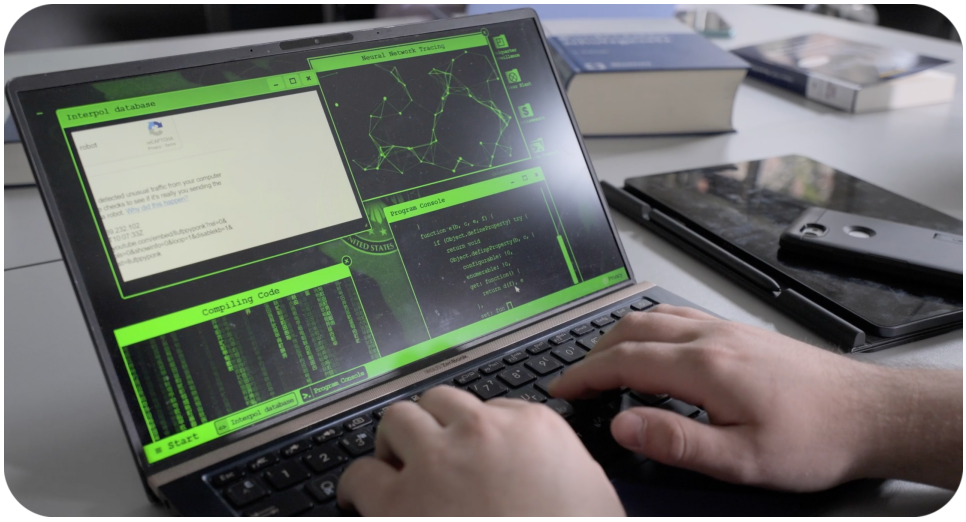
HOCHSCHULE ANSBACH

Bachelorstudiengang

Datenschutz und IT-Sicherheit (DIS)



Modulhandbuch

Version 1.2

(SPO DIS/HSAN 20192-6)

Inhaltsverzeichnis

Pflichtmodule

Einführung in die IT-Sicherheit

Modulkürzel:	Einführung in die IT-Sicherheit	**Modul-Nr.:**	01
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	1	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Spilker	
Sprache:	Deutsch	
Leistungspunkte / SWS:	8 ECTS / 6 SWS	
Arbeitsaufwand:	Kontaktstunden:	68 h
	Selbststudium:	172 h
	Gesamtaufwand:	240 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Einführung in die IT-Sicherheit	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden verfügen über ein breites Grundlagenwissen im Bereich IT-Sicherheit, welches sie u.a. zur Teilnahme an weiterführenden Lehrveranstaltungen befähigt. Die Studierenden besitzen ein grundlegendes Verständnis wichtiger Einsatzgebiete der IT-Sicherheit in einer Organisation und kennen die typischen Problemstellungen und Lösungsansätze der Informatik dafür. Darauf aufbauend verfügen die Studierenden über die Fähigkeit Entwicklungen und Tendenzen im Bereich der IT-Sicherheit kritisch zu hinterfragen und Querbeziehungen zu erkennen.

Handlungskompetenz
Die Studierenden können grundlegende fachliche Entscheidungen in den behandelten Bereichen selbständig treffen. Sie besitzen zudem die Fähigkeit sich eigenständig in Fachgebiete zielgerichtet einzuarbeiten und die dazu notwendigen Informationen zu beschaffen. Die Studierenden können bei der Auswahl von IT-Sicherheitswerkzeugen bzw. -Appliances, Methoden oder Konzepten aktiv mitwirken, um den operativen Betrieb einer Organisation möglichst sicher zu gestalten. Basierend auf der erworbenen Fachkompetenz können die Studierenden im 4. Fachsemester eine fundierte Wahl der Studienschwerpunkte treffen.

Sozialkompetenz
aufbauend auf ihren Erfahrungen in der Lehrveranstaltung besitzen die Studierenden die Fähigkeit Fachprobleme in Kleingruppen zu diskutieren und eigene Lösungsvorschläge im Kollegenkreis zielgerichtet zu vermitteln.

Inhalt:

- Motivation IT-Sicherheit: Aktuelle Fälle der IT-Sicherheit – Vorstellung, Recherche
- Grundbegriffe der IT-Sicherheit: Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit, Zurechenbarkeit/Accountability
- Bedrohungsszenarien, grundlegende Angriffsvektoren, z.B.o Social Engineeringo Vireno (Distributed) Denial of Service (DDOS)
- Hacking & Ransomeware

- Erster Einstieg in die Kryptographie (symmetrische und asymmetrische Verschlüsselung, Signaturen)
- Standards in der IT-Sicherheit: IT-Sicherheitsmanagement, Grundschutzkatalog BSI, ISO 27001
- Biometrie, Authentifizierung, Zugriffs-/Zugangangskontrolle
- Der Faktor Mensch in der IT-Sicherheit, Awareness IT-Sicherheit, Benutzbare Sicherheit
- Methoden der sicheren Softwareentwicklung
- Notfallplanung, Response, Veröffentlichung
- Ausblick / Motivation Datenschutz

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:

- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle, 10th expanded and updated edition (21. August 2018), De Gruyter Verlag, ISBN: 978-3110551587
- Secorvo: Informationssicherheit und Datenschutz, 4. Auflage (7. März 2ß24), Verlag dpunkt.Verlag, ISBN: 978-3-86490-978-8
- Michael Kofler et al.: Hacking & Security: Das umfassende Handbuch, 1. Auflage (27. April 2018), Verlag Rheinwerk Computing, ISBN: 978-3836245487
- Tom DeMarco, Timothy R. Lister: „Wien wartet auf Dich! -Der Faktor Mensch im DV-Management“ (engl.„Peopleware“), 2. Auflage, Hanser Verlag, ISBN: 3-446-21277-9

Grundlagen der Informatik

Modulkürzel:	Grundlagen der Informatik	**Modul-Nr.:**	02
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	1	

Modulverantwortliche(r):	Prof. Dr. Jens - Henrik Söldner
Dozierende:	Prof. Dr. Jens – Henrik Söldner
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Wintersemester
Lehrveranstaltungen des Moduls:	Grundlagen der Informatik
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan
Empfohlene Voraussetzungen:	keine
Verwendbarkeit:	DIS + WIF

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden haben einen umfassenden Überblick über die wichtigsten Aspekte moderner Betriebs- und Kommunikationssysteme. Sie kennen die Anforderungen an moderne Betriebssysteme und die Grundkonzepte für deren Lösung in verschiedenen Betriebssystemen. Sie haben das Prinzip der Abstraktion durch Definition von Netzwerkschichten verinnerlicht und können aktuelle Kommunikationstechnologien vor dem Hintergrund ihrer historischen Entwicklung einordnen und verstehen.

Handlungskompetenz
Die Studierenden können im Rahmen des Aufbaus von IT-Lösungen in einfachen Kommunikationsszenarien Empfehlungen für die Auswahl geeigneter Betriebssysteme und Kommunikationsmittel aussprechen. Auf-grund des erworbenen Grundwissens sind sie in der Lage, auch zukünftige Entwicklungen in diesen Bereichen einzuordnen und zu bewerten.

Inhalt:

Das Modul ist in zwei Teile gegliedert. Unter anderem werden folgende Themen behandelt:

Teil I: Betriebssysteme: Einführung in die Architektur moderner Betriebssysteme, Methoden der Prozess- und Betriebsmittelsteuerung, Methoden zur Hauptspeicherverwaltung, Aufbau moderner Dateiverwaltungssysteme und Methoden der Dateiverwaltung.

Teil II: Kommunikationssysteme:

Darstellung wesentlicher Entwicklungen im Bereich der Kommunikationstechnik, Funktionen von Kommunikationssystemen, Netzwerktopologien und – technologien, Netzwerk-Protokolle, Netzwerk-Referenzmodellen (ISO/OSI, TCP/IP), Algorithmen und Strategien für das Routing, Netzlaststeuerung, Fehlerbehandlung, Zugriffssteuerung, Anwendungsprotokolle (HTTP, IMAP, POP3, FTP, etc.), Netzwerkgeräte (Hub, Bridge, Switch, Router, Gateway, etc.).

Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten
Literatur:
Übergreifende Literatur: • Hansen, R., Neumann G.: Wirtschaftsinformatik 2; Informationstechnik. 9. Auflage,.Lucius & Lucius, Stutt- gart 2005. Zu Teil I: • Brause, R.: Betriebssysteme - Grundlagen und Konzepte. Springer-Verlag, Berlin-Heidelberg, 2. Auflage, 2013. ISBN 3540009000 • Stallings, W.: Betriebssysteme – Prinzipien und Umsetzung. Prentice Hall. 4. Auflage, 2003.ISBN 3-8273-7030-2 • A.-S. Tanenbaum: Moderne Betriebssysteme. Addison-Wesley Longman, 4. Auflage, 2016.ISBN 3-8273-70719-1 Zu Teil II: • Andrew, S. Tanenbaum, David J. Wetherall: Computernetzwerke. Pearson • James, F. Kurose, Keith W. Ross: Computernetzwerke: Der Top-Down-Ansatz. Pearson • Schreiner, R.: Computernetzwerke, Von den Grundlagen zur Funktion und Anwendung. Hanser • Schreiner, R.: Computernetzwerke, Von den Grundlagen zur Funktion und Anwendung. Hanser

Wirtschaftsenglisch			
Modulkürzel:	Wirtschaftsenglisch	**Modul-Nr.:**	03
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	1	

Modulverantwortliche(r):	Fr. McIntosch	
Dozierende:	Fr. Gabbey	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Wirtschaftsenglisch	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz:

Erwerb der Fähigkeit zur flüssigen sozialen Interaktion

Handlungskompetenz:

Fähigkeit die englische Sprache fach- und berufsbezogen im internationalen Kontext mündlich anzuwenden

Sozialkompetenz:

Verständnis von interkulturellen Faktoren

Inhalt:

- Ausbau von Grundfertigkeiten
- Einführung in landeskundliche Aspekte des englischen Sprachraumes unter besonderer Berücksichtigunginterkultureller Faktoren und Verhaltenskodizes
- Fähigkeit flüssig und angemessen in Bezug auf geschäftliche Situationen zu kommunizieren (Face to Face)
- Erwerb einer Sprechfertigkeit, die es erlaubt ohne Mühe die eigene Meinung klar und angemessendarzulegen (Meeting)
- Fähigkeit schwierige und komplexere Themenstellungen nicht nur zu erfassen, sondern auchzusammenfassend wiederzugeben (Telephoning)
- Übungen zu Textaufbau und Erstellen einer Präsentation
- Graphs und Charts.

Studien- / Prüfungsleistungen:

Mündliche Prüfung (15-20 min)

Literatur:
Wird zu Beginn bekannt gegeben Ergänzende Materialien werden über den Overhead-Projektor projiziert bzw. als Handouts verteilt. Im Sprachlabor werden Videos und Hörmaterialien eingesetzt.

Datenschutzrecht I			
Modulkürzel:	Datenschutzrecht I	**Modul-Nr.:**	04
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	1	

Modulverantwortliche(r):	Prof. Dr. Wolf Knüpffer	
Dozierende:	Hr. Kramer	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Datenschutzrecht 1	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden verfügen über Grundlagenwissen im Bereich des Datenschutzrechts, welches sie u.a. zur Teilnahme an weiterführenden Lehrveranstaltungen befähigt. Die Studierenden besitzen ein grundlegendes Verständnis wichtiger Prinzipien und Konstituenten des Datenschutz- und IT-Rechts, kennen die typischen Fragestellungen im Kontext der DS-GVO und nachfolgender Rechtsvorschriften. Darauf aufbauend verfügen die Studierenden über die Fähigkeit, Entwicklungen und Tendenzen im Bereich des Datenschutzrechts kritisch hinterfragen und Querbeziehungen erkennen zu können.

Handlungskompetenz
Die Studierenden können weitgehend eigenständig einfache Fragestellungen im Bereich des Datenschutz-rechts beantworten, bzw. Antworten begründet herleiten. Sie sind weiterhin in der Lage typische Fragestel-lungen in Organisationen als relevant für eine datenschutzrechtliche Betrachtung zu erkennen.

Sozialkompetenz
Die Studierenden können die Prinzipien des modernen Datenschutzes allgemeinverständlich erklären und plausibel herleiten. Aufbauend darauf können sie in einer Organisation für grundlegendes Verständnis und Awareness bzgl. der täglichen Umsetzung des Datenschutzes sorgen.

Inhalt:

- Rechtliche Grundlagen
- Grundsätze des Datenschutzrechts
- Rechte der Betroffenen
- Verantwortliche und Auftragsverarbeiter
- Erwägungsgründe & BDSG
- Typische/Beispielhafte Fragestellungen in der Praxis

Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten
Literatur:
• Beck / dtv: Datenschutzrecht und Datenwirtschaftsrecht: DatSchR; Verlag C.H.Beck ISBN 978-3-406-83138-6; 16. Auflage 2025 • Bayerisches Landesamt für Datenschutzaufsicht (Herausgeber), Thomas Kranig, Eugen Ehmann: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket, 1. Auflage (17. November 2017), Verlag C.H.Beck, ISBN: 978-3406716621 • DSK-Kurzpapiere (https://www.datenschutzkonferenz-online.de/kurzpapiere.html) • GDD-Praxishilfe DS-GVO :Verzeichnis von Verarbeitungstätigkeiten – Verantwortlicher https://www.gdd.de/wp-content/uploads/2023/06/GDD-Praxishilfe-DS-GVO-Verzeichnis-von-Verarbeitungstaetigkeiten-2.2.pdf • GDD-Praxishilfe DS-GVO: Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO https://www.gdd.de/wp-content/uploads/2023/06/GDD-Praxishilfe-DS-GVO-Praxishinweise-fuer-Auftragsverarbeiter-nach-Art.-28-DS-GVO.pdf • GDD-Praxishilfe DS-GVO: „Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung“ https://www.gdd.de/wp-content/uploads/2023/06/GDD-Praxishilfe-DS-GVO-DSB-nach-DS-GVO.pdf • GDD-Praxishilfe Checkliste: „Meldung von Datenschutzverletzungen nach Art. 33, 34 DS-GVO“ https://www.gdd.de/wp-content/uploads/2025/01/GDD-Praxishilfe-Checkliste-%E2%80%9EMeldung-von-Datenschutzverletzungen-nach-Art.-33-34-DS-GVO-1.pdf • BfDI: Datenschutz-Grundverordnung - Bundesdatenschutzgesetz - Texte und Erläuterungen; aktualisierte Auflage 2025; https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.html?nn=251928

Programmierung I

Modulkürzel:	Programmierung I	**Modul-Nr.:**	05
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	1	

Modulverantwortliche(r):	Prof. Dr. Michael Netter
Dozierende:	Prof. Dr. Michael Netter
Sprache:	Deutsch
Leistungspunkte / SWS:	7 ECTS / 6 SWS
Arbeitsaufwand:	Kontaktstunden: 68 h Selbststudium: 142 h Gesamtaufwand: 210 h
Moduldauer:	1 Semester
Häufigkeit:	nur Wintersemester
Lehrveranstaltungen des Moduls:	Programmierung I
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	DIS + WIF

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden können einfache Programme in einer höheren Programmiersprache entwickeln und wen-den dabei die Prinzipien der strukturierten Programmierung an. Sie verstehen es, geeignete Sprachelemente bei der Umsetzung von Programmierproblemen in lauffähige Programme zu verwenden.

Handlungskompetenz
Die Studierenden können einfache Programme (Konsolprogramme) für betriebliche Aufgabenstellungen entwerfen und implementieren.

Inhalt:

- Programmiersprachen allgemein (Arten, Konzepte)
- Grundlegende Einführung in die Syntax und Semantik einer höheren Programmiersprache (elementare und komplexe Datentypen, Anweisungen, Kontrollstrukturen), Einsatz von Programmbibliotheken
- Einführung in die Grundlagen der objektorientierten Programmierung (Klassen, Objekte, Attribute, Methoden)
- Entwicklungsmethodik für das Programmieren im Kleinen, schrittweise Verfeinerung, Prinzipien der strukturierten Programmierung
- Einführung in eine moderne Entwicklungsumgebung für das Erstellen, Verwalten und Testen von Programmen

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:

- H. Mössenböck: Sprechen Sie Java? dpunkt.verlag, jeweils neuste Auflage

- Ratz, Scheffler, Seese, Wiesenberger: Grundkurs Programmieren in Java, Hanser, jeweils neuste Auflage
- Fritz Jobst: Programmieren in Java, Hanser, jeweils neuste Auflage
- Guido Krüger: Java-Programmierung – das Handbuch, O'Reilly, jeweils neuste Auflage
- Christian Ullenboom: Java ist auch eine Insel, Galileo Computing, jeweils neuste Auflage

Programmierung II

Modulkürzel:	Programmierung II	**Modul-Nr.:**	06
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	2	

Modulverantwortliche(r):	Prof. Dr. Michael Netter	
Dozierende:	Prof. Dr. Michael Netter	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Programmierung II	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Programmierung I	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Vertiefung der Fähigkeiten, die in Programmieren I erworben wurden. Die Studierenden beherrschen die Grundlagen und Konzepte der objektorientierten Programmierung und können diese in mindestens einer objektorientierten Programmiersprache anwenden.

Handlungskompetenz
Die Studierenden können Programme (Konsolprogramme, grafisch-interaktive) für anspruchsvolle betriebliche Aufgabenstellungen entwerfen und implementieren.

Inhalt:

Einführung in die „Paradigmen“ der objektorientierten Programmierung (assoziative Beziehungen, Vererbung, Aggregation, Schnittstellen)

Vertiefung in objektorientierte Programmiertechniken (Polymorphismus, Kommunikation zwischen den Objekten, einfache Design-Pattern, typische Datenstrukturen, Benutzung von Klassenbibliotheken)

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:

- H. Mössenböck: Sprechen Sie Java? dpunkt.verlag, jeweils neuste Auflage
- Ratz, Scheffler, Seese, Wiesenberger: Grundkurs Programmieren in Java, Hanser, jeweils neuste Auflage
- Fritz Jobst: Programmieren in Java, Hanser, jeweils neuste Auflage
- Guido Krüger: Java-Programmierung – das Handbuch, O’Reilly, jeweils neuste Auflage
- Christian Ullenboom: Java ist auch eine Insel, Galileo Computing, jeweils neuste Auflage

Algorithmen und Datenstrukturen

Modulkürzel:	Algorithmen und Datenstrukturen	**Modul-Nr.:**	07
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	2	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Ewald	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Algorithmen und Datenstrukturen	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz

Grundlegende Datenstrukturen und die dazugehörigen Algorithmen kennen und verstehen. Einfache Algorithmen analysieren, beschreiben und auf Korrektheit prüfen können. Algorithmen hinsichtlich ihres Laufzeit-verhaltens und sonstigen Ressourcenverbrauchs bewerten können. Die algorithmische Komplexität von Programmieraufgaben einschätzen können.

Handlungskompetenz

Die Studierenden sollen die wichtigsten, im wirtschaftlichen Umfeld verwendeten Datenstrukturen und Algorithmen kennen, um für vorgegebene Anwendungsfälle geeignete Datenstrukturen und Algorithmen fin-den, analysieren und bewerten zu können. Überführung von realen Problemstellungen in geeignete, algorithmische Lösungen.

Sozialkompetenz

Die Studierenden sollen sich in einfachen fachlichen Diskussionen über Algorithmen und Datenstrukturen aktiv beteiligen können und z.B. bei der Auswahl einer geeigneten Datenstruktur eine fundierte fachliche Meinung vertreten können. Zudem sollen die Studierenden in der Lage sein, grundlegende Funktionsweisen von einfachen Algorithmen allgemeinverständlich zu erklären.

Inhalt:

- Was sind Algorithmen und Eigenschaften von Algorithmen
- Elementare/grundlegende Datenstrukturen
- Abstrakte Datenstrukturen (Stack, Queue, Bäume, Heap, Hash, …)
- Algorithmische Verfahren (Suche, Sortierung, Rekursion, dynamische Programmierung, …)
- Bewertung von Algorithmen und Datenstrukturen bzgl. Korrektheit, Komplexität, Effizienz und Aufwand

Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten
Literatur:
• T.H.Cormen, C.E.Leiserson, R.L.Rivest, C.Stein: Algorithmen – Eine Einführung, 4. Aufl., 2013, De Gruyter Oldenbourg • R. Sedgewick, K. Wayne: Algorithmen: Algorithmen und Datenstrukturen, 2014, Pearson Studium – IT, neueste Auflage • G. Saake, K.-W. Sattler: Algorithmen und Datenstrukturen: Eine Einführung mit Java, 5. Aufl., 2013, dpunkt Verlag

Kryptographie

Modulkürzel:	Kryptographie	**Modul-Nr.:**	08
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	2	

Modulverantwortliche(r):	Prof. Dr. Michael Netter
Dozierende:	Hr. Hartmann
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Sommersemester
Lehrveranstaltungen des Moduls:	Kryptographie
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	DIS

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden verfügen über ein breites Grundlagenwissen im Bereich der Kryptographie. Sie besitzen ein vertieftes Verständnis für die zeitlich Entwicklung früherer und aktuellen kryptografische Verfahren und sind in der Lage, die entsprechenden Verfahren zu bewerten. Die Studierenden haben ein Grundverständnis für die Kryptoanalyse zum Bewerten und Brechen von Verschlüsselungsverfahren.

Handlungskompetenz
Die Studierenden können für typischen Problemstellungen passende aktuelle Verfahren auswählend und sind in der Lage die Auswahl mit Referenzen zu entsprechenden Standards zu begründen.

Inhalt:

- Klassische Verschlüsselungsverfahren
- Kriterien für sichere Verschlüsselung
- symmetrische Verschlüsselungsverfahren
- asymmetrische Verschlüsselungsverfahren
- Methoden des sicheren Schlüsselaustausch
- Hashverfahren
- Erzeugung von Zufall
- Quantencomputing und Postquantenkryptografie

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:
Wird zu Beginn bekannt gegeben

Technische und organisatorische Datenschutz-Maßnahmen			
Modulkürzel:	DIS-Techn. und organ. Datenschutz-Maßnahmen	**Modul-Nr.:**	09
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	2	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Spilker	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Technische und organisatorische Datenschutz-Maßnahmen	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Module Datenschutzrecht I und Einführung in die IT-Sicherheit	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden haben einen umfassenden Überblick über die wichtigsten technische und organisatorische Datenschutzmaßnahmen. Sie kennen die gesetzliche Datenschutz-Anforderungen an die Verarbeitung per-sonenbezogener Daten und die Grundkonzepte, um die entsprechende Sicherheitsziele zu gewährleisten.

Handlungskompetenz
Die Studierenden können im Rahmen des Aufbaus von einem Datenschutzmaßnahmenkonzept in einer Or-ganisation Empfehlungen für die Auswahl geeigneter Maßnahmenpaketen aussprechen. Aufgrund des er-worbenen Grundwissens sind sie in der Lage, auch zukünftige Entwicklungen in diesen Bereichen einzuord-nen und zu bewerten.

Sozialkompetenz
Die Studierenden sollen sich in einfachen fachlichen Diskussionen über technische und organisatorische Da-tenschutzmaßnahmen aktiv beteiligen können. Zudem sollen die Studierenden bei der Auswahl einer geeig-neten Maßnahmenpaket eine fundierte fachliche Meinung vertreten können.

Inhalt:

- Abgrenzung technische vs. organisatorische Datenschutzmaßnahmen
- Gesetzlicher Rahmen: Art. 32 DSGVO, Art. 64 BDSG• Datenschutz und Sicherheitsziele: Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit
- Überprüfung, Bewertung, und Evaluierung der Wirksamkeit der Maßnahmen
- Management:
    - Behandlung von Sicherheitsvorfällen
    - Hardware und Software-Management: Patch-Management, …

- Personal Management: MA-Schulungen, …
- Datensicherung, Archivierung, Datenlöschung
- Verschlüsselung und Pseudonymisierung
- Infrastrukturelle Sicherheitsmaßnahmen:
  - Zutrittskontrolle
  - Klimakontrolle
  - Maßnahmen gegen Feuer, Wasser, Uber- und Unterspannung
- IT-Systeme und Netze:
  - Berechtigungsmanagement / Need-to-know-Prinzip
  - Mobile Device Management / VPN
  - Firewall/Antivirus/Back-up
  - Webserver / Mail-Server

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:

- U. Schläger, J. C. Thode: Handbuch Datenschutz und IT-Sicherheit, 1. Auflage (2018), Erich Schmidt Verlag GmbH & Company, ISBN: ISBN 978-3503177271
- Peter Münch: Technisch-organisatorischer Datenschutz: - Leitfaden für Praktiker, 4. Auflage (27. April 2010), DATAKONTEXT Verlag, ISBN: 978-3895775864

Bayerisches Landesamt für Datenschutzaufsicht (Herausgeber), Thomas Kranig, Eugen Ehmann: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket, 1. Auflage (17. November 2017), Verlag C.H.Beck, ISBN: 978-3406716621

Mathematik

Modulkürzel:	Mathematik	**Modul-Nr.:**	10
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	2	

Modulverantwortliche(r):	Prof. Dr. Christine Dauth
Dozierende:	Hr. Westrich
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Sommersemester
Lehrveranstaltungen des Moduls:	Mathematik
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	DIS/WIF

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden beherrschen die mathematischen Grundlagen, die als Instrumentarium in den verschiedenen fachspezifischen Modulen benötigt werden.

Handlungskompetenz
Die Studierenden sind in der Lage, das Instrumentarium der Mathematik anzuwenden, um Problemstellungen im Umfeld der Ökonomie zu analysieren und zu lösen.

Inhalt:

Lineare Algebra
Lineare Gleichungssysteme; Matrizen und Vektoren; Grundlagen der Linearen Optimierung.

Analysis
Differentialrechnung mit einer und mit mehreren unabhängigen Veränderlichen, d.h.: Diskussion der bei ökonomischen Anwendungen wichtigsten Funktionen, Extremwertbestimmung ohne und mit Nebenbedingungen; Integralrechnung samt deren ökonomischen Anwendungen.

Finanzmathematik
Zins-, Renten- und Tilgungsrechnung.

Studien- / Prüfungsleistungen:

Schriftliche Prüfung, 90 Minuten

Literatur:
• Schwarze, Jochen: Mathematik für Wirtschaftswissenschaftler, 5 Bände, Verlag Neue Wirtschaftsbriefe (NWB) • Holland, Heinrich und Doris Holland: Mathematik im Betrieb, Gabler-Verlag3. Tietze, Jürgen: Einführung in die angewandte Wirtschaftsmathematik, Vieweg-Verlag4. Ohse, Dieter: Mathematik für Wirtschafts-wissenschaftler, 2 Bände, Verlag Franz Vahlen5. Rommelfanger, Heinrich: Mathematik für Wirtschafts-wissenschaftler, 2 Bände, Spektrum Akademischer Verlag

Datenschutzrecht II

Modulkürzel:	Datenschutzrecht II	**Modul-Nr.:**	11
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	2	

Modulverantwortliche(r):	Prof. Dr. Wolf Knüpffer
Dozierende:	Hr. Kramer
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Sommersemester
Lehrveranstaltungen des Moduls:	Datenschutzrecht II
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Datenschutzrecht I
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	DIS

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden verfügen über vertieftes Wissen im Bereich des Datenschutzrechts und angrenzender Rechtsfelder. Die Studierenden besitzen ein umfassendes Verständnis der wichtigsten Rechtsvorschriften und können Rechtsfragen den einzelnen Rechtsgebieten zuordnen. Die Studierenden sind selbstständig in der Lage weitergehende Recherchen im Kontext des Datenschutzrechts durchzuführen und können klar

Gültigkeiten und Zuständigkeiten abgrenzen.

Handlungskompetenz
Die Studierenden können weitgehend eigenständig fortgeschrittene Fragestellungen im Bereich des Daten-schutzrechts und angrenzender Rechtsgebiete beantworten, bzw. Antworten begründet herleiten. Sie sind weiterhin in der Lage für typische Fragestellungen in Organisationen zu erkennen, wann weitergehendes ju-ristisches Fachwissen notwendig ist, bzw. wann ggf. Aufsichtsbehörden einzuschalten sind.

Sozialkompetenz
Die Studierenden können auch im vertieften Fachgespräch unter KollegInnen folgen und aktiv daran teilneh-men. Aufbauend darauf können Sie in einer Organisation an rechtskonformen Regelungen für den Daten-schutz mitarbeiten.

Inhalt:

- Verhaltensregeln und Zertifizierung
- Vertiefung Datenschutzrecht und angrenzende Rechtsgebiete wie z.B. TDDDG und UWG
- Drittstaatentransfer
- Grundfragen zu Big-Data / Künstliche Intelligenz
- Aufgaben der Aufsichtsbehörden
- Sanktionen

Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten
Literatur:
Beck / dtv: Datenschutzrecht und Datenwirtschaftsrecht: DatSchR; Verlag C.H.Beck ISBN 978-3-406-83138-6; 16. Auflage 2025 Bayerisches Landesamt für Datenschutzaufsicht (Herausgeber), Thomas Kranig, Eugen Ehmann: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket, 1. Auflage (17. November 2017), Verlag C.H.Beck, ISBN: 978-3406716621 DSK-Kurzpapiere (https://www.datenschutzkonferenz-online.de/kurzpapiere.html) BfDI: Datenschutz-Grundverordnung - Bundesdatenschutzgesetz - Texte und Erläuterungen; aktualisierte Auflage 2025; https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.html?nn=251928 GDD-Praxishilfe DS-GVO: Datenschutzrechtliche Anforderungen an internationale Datentransfers https://www.gdd.de/wp-content/uploads/2023/08/GDD-Praxishilfe-DS-GVO-Internationale-Datentransfers-2.0.pdf GDD-Praxishilfe DS-GVO: „ePrivacy und Datenschutz beim Onlineauftritt“ https://www.gdd.de/wp-content/uploads/2024/05/GDD-Praxishilfe-DS-GVO-ePrivacy-und-Datenschutz-beim-Onlineauftritt.pdf GDD-Musterrichtlinie: Betriebliche Richtlinie zum Einsatz „Künstlicher Intelligenz“ https://www.gdd.de/publikationen/gdd-musterrichtlinie-einsatz-von-kuenstliche-intelligenz/

Fachspezifische Pflichtmodule

Webentwicklung

Modulkürzel:	Webentwicklung	**Modul-Nr.:**	12
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	3	

Modulverantwortliche(r):	Prof. Dr. Jonas Härtfelder
Dozierende:	Hr. Betzel
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Wintersemester
Lehrveranstaltungen des Moduls:	Webentwicklung
Lehrformen des Moduls:	DIS/WIF
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	DIS + WIF

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden erhalten die Kompetenz einfache Webanwendungen eigenständig zu entwerfen undumzusetzen. Sie sind in der Lage unterschiedlicher Web-Technologien zu verstehen, einzusetzen und inKombination zu nutzen. Sie erhalten die Kompetenz Inhalte zu strukturieren und plausibel zu verlinken.Weiterhin sind die Studierenden befähigt Inhalte technisch aufzubereiten und in geeigneten Formatenabzuspeichern. Die Studierenden verfügen über die Fähigkeit einfache 2D-Animationen zu gestalten. Sieverfügen über die Kompetenz komplexere Anwendungssysteme, die auf Content Managementsystemenbasieren, individuell hinsichtlich Layouts und Funktionalitäten auszurichten und zu gestalten.

Handlungskompetenz
Die Studierenden erhalten die Kompetenz zielgerichtet Entwicklungswerkzeuge auszuwählen und dieseprofessionell zu nutzen. Sie sind in der Lage statische Web-Anwendungen komplett umzusetzen. DieStudierenden erwerben die Kompetenz komplexe Web-Anwendungen technisch einzuordnen und hinsichtlich einer technischen und gestalterischen Modifikation zu beurteilen.

Inhalt:

- Begriffsdefinition und generelle Einsatzmöglichkeiten von Multimedia- und Internetanwendungen.
- Beschreibungssprachen zur Darstellung von Inhalten im Internet (HTML) und Arbeiten mit einschlägigen Entwicklungstools. Darstellung einer Sprache zur Text-, Webseiten- und Bildformatierung, hier CascadingStylesheets (CSS).
- Bildbearbeitungssoftware zur Aufbereitung von Bildern für das Web.
- Grundlegende Techniken zur Bildbearbeitung. Programmiersprachen zur Umsetzung von Funktionalitäten und interaktiven Abfragen auf dem Client, hier JavaScript.
- Einsatz von Programmierframeworks. Grundlegende Programmierkonzepte dieser Sprache sowie spezifische Eigenschaften und Methoden innerhalb des zugrunde gelegten Objektmodells.

- Anlegen von bewegten interaktiven Web-Elementen unter Verwendung von einschlägigen Werkzeugen.
- Aufbau einer, auf einem Content Management System basierenden, Web-Anwendung.
- Modifikation der bereitgestellten Basisfunktionen durch Programmierung.

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:

- Münz, Gull: HTML Handbuch Franzis Verlag, jeweils neueste Auflage
- Ackermann: JavaScript, Rheinwerk Computing
- Wenz: JavaScript, Galileo Computing, jeweils neueste Auflage
- Laborenz: CSS-Praxis, Galileo Verlag, jeweils neueste Auflage
- Videotutorials laut aktueller Empfehlung
- Webseiten laut aktueller Empfehlung, z.B.: www.selfhtml.org

Cyber Security

Modulkürzel:	Cyber Security	**Modul-Nr.:**	13
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	3	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Voitel	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Cyber Security	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz:
Die Studierenden vertiefen und verbreitern ihr Grundlagenwissen im Bereich der IT-Sicherheit und erhalten einen umfassenden Überblick über die wichtigsten Aspekte der IT-Sicherheit, was sie zur Teilnahme anweiterführenden, vertiefenden und praktischen Lehrveranstaltungen befähigt.

Handlungskompetenz:
Die Studierenden können fachliche Entscheidungen in den behandelten Bereichen selbständig treffen. Siebesitzen zudem die Fähigkeit, sich eigenständig in Fachgebiete zielgerichtet einzuarbeiten und die dazunotwendigen Informationen zu beschaffen. Die Studierenden können bei der Auswahl von IT-Sicherheitswerkzeugen bzw. -Appliances, Methoden oder Konzepten aktiv mitwirken, um den operativen Betriebeiner Organisation möglichst sicher zu gestalten. Basierend auf der erworbenen Fachkompetenz können dieStudierenden im 4. Fachsemester eine fundierte Wahl der Studienschwerpunkte treffen.

Sozialkompetenz:
aufbauend auf Ihren Erfahrungen in der Lehrveranstaltung besitzen die Studierenden die Fähigkeit,Fachprobleme in Kleingruppen zu diskutieren und eigene Lösungsvorschläge im Kollegenkreis zielgerichtet zu vermitteln.

Inhalt:

- Sicherheit und Risikomanagement
- Asset Security
- Security Architecture and Engineering
- Physische Sicherheit
- Netzwerksicherheit
- Firewalls und Intrusion Detection / Prevention
- Authentifizierung und Berechtigungsmanagement

- Betriebssystemsicherheit: Windows, Unix, Linux
- Sicherheit von mobilen Endgeräten
- Web Security und Anwendungssicherheit
- Datensicherung
- Incident Management
- Standards der Informationssicherheit

Studien- / Prüfungsleistungen:

Studienarbeit (außerhalb Prüfungszeitraum)

Literatur:

- Secorvo (Herausgeber): Informationssicherheit und Datenschutz: Handbuch für Praktiker und Begleitbuch-zum T.I.S.P., 3. Auflage 2019 (2. Oktober 2019), dpunkt Verlag, ISBN: 978-3864905964
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle, 10th expanded and updated edition (21.August 2018), De Gruyter Verlag, ISBN: 978-3110551587
- Michael Bartsch et al.: Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz fürUnternehmen und Behörden, 1. Auflage 2018 (8. August 2018), Springer Vieweg Verlag, ISBN: 978-3658216542
- Michael Kofler et al.: Hacking & Security: Das umfassende Handbuch, 1. Auflage (27. April 2018), Verlag-Rheinwerk Computing, ISBN: 978-3836245487

Privacy Engineering

Modulkürzel:	Privacy Engineering	**Modul-Nr.:**	14
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	3	

Modulverantwortliche(r):	Prof. Dr. Michael Netter	
Dozierende:	Prof. Dr. Michael Netter	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Privacy Engineering	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden kennen die wichtigsten Auffassungen von Privatsphäre sowie grundlegende Begriffe wie Anonymität und Pseudonymität. Sie haben einen umfassenden Überblick über die wichtigsten technischen Werkzeuge zum Schutz der Privatsphäre. Die Studierenden können danach eine Lösung entwickeln, die die Privatsphäre des Nutzers während des gesamten Lebenszyklus schützt.

Handlungskompetenz
Die Studierenden können im Rahmen der Entwicklung von Systemen in einer Organisation Empfehlungen zum Schutz der Daten und der Privatsphäre der Nutzer aussprechen. Aufgrund des erworbenen Grundwissens sind sie in der Lage, auch zukünftige technische Entwicklungen in diesen Bereichen einzuordnen und zu bewerten.

Sozialkompetenz
Die Studierenden vertiefen die Kompetenz sich in Projektteams zu integrieren. Die Studierenden können mit Rechtsexperten in einem Team zusammenarbeiten und in einer einfachen Sprache kommunizieren, um eine effiziente Lösung zur Wahrung der Privatsphäre zu entwickeln.

Inhalt:

- Grundlagen der Privatsphäre
- Privacy Frameworks
- Kryptographische Grundlagen zum Schutz der Privatsphäre
- Anonymisierung, Pseudonymisierung
- Anonyme und sichere Kommunikation (Mix-Netzwerke, TOR, Signal-Protokoll)
- Browser Tracking & Fingerprinting
- Privatsphäre in Sozialen Netzwerken
- Usable Privacy

Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten
Literatur:
• Michelle Dennedy, et al.: The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value, Apress Verlag, 1. Auflage (27. Januar 2014), ISBN: 978-1430263555

Compliance-Management

Modulkürzel:	Compliance-Management	**Modul-Nr.:**	15
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	3	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner
Dozierende:	Hr. Rühl
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Wintersemester
Lehrveranstaltungen des Moduls:	Compliance-Management
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	DIS

Angestrebte Lernergebnisse:

Compliance-Managements. Dies enthält

- Die Ermittlung relevanter rechtlicher Anforderungen für einen bestimmten Anwendungsbereich
- Zusammenarbeit mit anderen Stellen in einem Unternehmen (Datenschutz, Rechtsabteilung, Personalabteilung) zur Beurteilung der Relevanz
- Führen eines Rechtsanforderungsregisters
- Ableiten von Maßnahmen, Schulungen und anderen Maßnahmen für das Compliance Management

Fach- und Methodenkompetenz:

- Navigation durch wichtige Rechtsquellen (Deutsches Recht, EU Recht)
- Verstehen der Prinzipien eines Compliance-Management-Systems
- Ermitteln der Relevanz einer rechtlichen Anforderung für ein bestimmtes Anwendungsgebiet
- Übersetzen rechtlicher Anforderungen in Maßnahmen in einem Unternehmen

Handlungskompetenz:

- Recherche in Rechtsdatenbanken
- Anwenden einfacher rechtlicher Fragestellungen
- Bewerten der Relevanz ggf. zusammen mit anderen Fachabteilungen eines Unternehmens

Inhalt:

- Compliance Management Systeme – Aufbau und Funktion
- Rechtsdatenbanken Deutschland und Europa
- Anwenden von Prüffragen zur Bewertung der Relevanz von rechtlichen Anforderungen
- Verstehen des Zusammenwirkens von EU-Recht und nationalem Recht

Studien- / Prüfungsleistungen:
Studienarbeit (außerhalb Prüfungszeitraum)
Literatur:
• Brauweiler, J., Will, M. (2015): Auditierung und Zertifizierung von Managementsystemen. • Pachinger, M., Beham, G. (2020): Datenschutz-Audit: Recht - Organisation - Prozess - IT. • Roßnagel (1999): Datenschutzaudit: Konzeption, Durchführung, gesetzl. Grundlage. • Sowa, A., Duscha, P. et al. (2005): IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die ITPrüfung. Graham, L. (2015): Internal Control Audit and Compliance: Documentation and Testing under the new COSO Framework.

Big Data Analytics und Statistik

Modulkürzel:	Big Data Analytics und Statistik	**Modul-Nr.:**	16
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	1	

Modulverantwortliche(r):	Prof. Dr. Wolf Knüpffer
Dozierende:	Hr. Enders
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Wintersemester
Lehrveranstaltungen des Moduls:	Big Data Analytics und Statistik
Lehrformen des Moduls:	2 SWS seminaristischer Unterricht Big Data Analytics, 2 SWS seminaristischer Unterricht Statistik
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	DIS

Angestrebte Lernergebnisse:

Big Data Analytics:

Die Studierenden beherrschen Methoden, um mit großen Datenbeständen in der statistischen Programmiersprache R umzugehen. Dies deckt den kompletten Data Analysis Lifecycle ab: Daten laden, bereinigen und transformieren sowie modellieren. Ergänzt wird dies durch Vermittlung von Methoden zur Visualisierung und Kommunikation von Analyseergebnissen. Die Übungseinheiten thematisieren die einzelnen Themenbereiche und trainieren die praktische Umsetzung aller Schritte in der Programmiersprache R. Statistik.

Die Studierenden sollen die wichtigsten Grundkonzepte aus den Bereichen der deskriptiven und induktiven Statistik verstehen. Ergänzend werden Inhalte der Elementaren Wahrscheinlichkeitsrechnung als Basis vermittelt. Abschließend befasst sich der Kurs mit Indexrechnung. Neben der Vermittlung von theoretischem Verständnis zielt die Veranstaltung auf die konkrete Anwendung der kennengelernten Techniken im Zuge der Übungseinheiten ab.

Fach- und Methodenkompetenz:

Studierenden werden befähigt

- die Anwendung statistischer Methoden zur Analyse und zur Interpretation von Daten zu verstehen,
- Daten aufzubereiten und so darzustellen, dass diese zu bestimmte Inhalte objektiv vermitteln,
- selbständig statistische Tests und Analysen durchzuführen sowie
- die Sprache R für Datenimport, -aufbereitung sowie -auswertung und Präsentation zu verwenden.

Handlungskompetenz:

Studierende können

- Daten für die Analyse aufbereiten (Import, Bereinigung und Transformation)

- Daten anhand von Modellen interpretieren
- Schlussfolgerungen auf Basis einfacher, statistischer Tests ableiten Sozialkompetenz: Studierende können
- Auf den jeweiligen Anwendungsfall basierend den richtigen statischen Test auswählen um ein bestimmtes Ziel zu validieren oder zu widerlegen
- Daten mit Hilfe von Modellen objektiv beschreiben und diese visuell aufbereitet kommunizieren

Inhalt:

Big Data Analytics

- Data Analysis Lifecycle
- Datenaufbereitung: ETL-Prozess (Extraktion, Transformation, Loading) für einfache und große Datenbestände
- Datenvisualisierung
- Modellierung: Daten mit mathematischen Modellen beschreiben5. Kommunikation von Modellen und Ergebnissen

Statistik

- Elementare Wahrscheinlichkeitsrechnung: Mengenoperationen und der Wahrscheinlichkeitsbegriff, Kombinatorik, Bedingte Wahrscheinlichkeit, Stochastische Unabhängigkeit, Bernoulli-Experiment
- Deskriptive Statistik: Empirische Verteilungen, Verteilungsparameter (Lagemaße, Streuungsmaße, Zusammenhangsmaße), Theoretische Verteilungen (Diskrete und stetige Verteilungen)
- Induktive Statistik: Punktschätzung, Intervallschätzung, Hypothesen-Tests, Regressionen,
- Indexrechnung

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:

Statistik:

- Sibbertsen P.; Lehne H.: Statistik – Einführung für Wirtschafts- und Sozialwissenschaftler, 2. Auflage, Springer Gabler
- Grabmeier J.; Hagl S.: Statistik – Grundwissen und Formeln, 2. Auflage, Haufe
- Grolemund, G.; Wickham, H.: R for Data Science, 1. Auflage, O'Reilly, 2016
- Sauer, S.: Moderne Datenanalyse mit R, Springer Gabler, 2019

Cloud-Computing			
Modulkürzel:	DIS-Cloud-Computing	**Modul-Nr.:**	17
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	5	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Dr. C. Söldner	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Cloud-Computing	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Die Studierenden kennen die Grundlagen zum Erstellen von IT-Infrastrukturen in Public Clouds (am Beispiel von Amazon AWS, Google GCP und Microsoft Azure). Sie sind in der Lage, Dienste von Public Clouds zu be-dienen und über programmatische Techniken zu kombinieren und zu automatisieren. Durch die praxisnahen Übungen und Fallstudien sind die Studierenden mit der Anwendung vertraut.

Fach- und Methodenkompetenz:
Die Studierenden werden befähigt …

- … die Anwendungsparadigmen und Dienste der Public Cloud zu benennen und diese im Kontext einzuordnen.
- … eigenständig geeignete Cloud-Dienste auszuwählen und diese zu konfigurieren und zu verwalten.
- … moderne Anwendungsarchitekturen auf Basis von Cloud Native Techniken zu beschreiben und einzusetzen.
- … Cloud-Dienste zu automatisieren und abzusichern.

Handlungskompetenz:
Die Studierenden können …

- ... Public und Private Cloud Dienste umfassend bedienen.
- … IT-Architekturen für die Bereitstellung von Anwendungen in der Public Cloud umsetzen.

Sozialkompetenz:
Die Studierenden können …

- … komplexe Problemstellungen aus dem Bereich der IT-Infrastruktur und des Applikationsdesigns im Team erörtern.
- … die Fähigkeit zum Zeitmanagement verbessern.

Inhalt:

Noch zu bestimmen
Studien- / Prüfungsleistungen:
Studienarbeit (außerhalb Prüfungszeitraum)
Literatur:
Wird zu Beginn bekannt gegeben

Projektmanagement			
Modulkürzel:	DIS-Projektmanagement	**Modul-Nr.:**	18
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	5	

Modulverantwortliche(r):	Prof. Dr. Dominik Kögel
Dozierende:	Prof. Dr. Dominik Kögel
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Wintersemester
Lehrveranstaltungen des Moduls:	Projektmanagement
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Keine
Empfohlene Voraussetzungen:	Das Modul kann als Fortgeschrittenenmodul studiert werden, wenn bereits Vorkenntnisse vorliegen – etwa aus einem bereits belegten Grundlagenmodul zu Projektmanagement. In diesem Fall bietet dieses Modul nützliche Verfeinerungen und Erweiterungen bisheriger Kenntnisse. **Das Modul ist jedoch auch ohne Vorkenntnisse studierbar.**
Verwendbarkeit:	DIS

Angestrebte Lernergebnisse:

Projektmanagement ist eine Schlüsselkompetenz für Unternehmen und Führungskräfte. Die Fähigkeit, komplexe Vorhaben – seien es neue Produktentwicklungen oder organisatorische Veränderungen – im Termin, im Budget und in der gefragten Qualität umsetzen zu können, bestimmt über Erfolg und Misserfolg.

In diesem Modul werden Ihnen die entsprechenden Kenntnisse in professionellen Projektmanagementmethoden – basierend auf international anerkannten Standards – vermittelt. Dabei liegt ein besonderer Fokus auf der Anwendung von Projektmanagement in der Praxis. Zudem in modernen Methoden des Projektmanagements (insbes. auch Agiles Projektmanagement, Scrum) sowie Project Leadership (also Soft Skills für Projektmanagement). **Das Modul kann auch studiert werden, wenn bereits Vorkenntnisse – etwa aus einem bereits belegten Grundlagenmodul zu Projektmanagement – vorliegen. In diesem Fall bietet dieses Modul nützliche Verfeinerungen und Erweiterungen bisheriger Kenntnisse. Das Modul ist jedoch auch ohne Vorkenntnisse studierbar.** Zudem recherchieren Sie eigenständig relevantes Detailwissen zu den wichtigen Aspekten des Projektmanagements.

Projektmanagement als überaus praktische Fachdisziplin ist praxisnah. Im Modul werden daher Fragestellungen aus der Praxis für die Praxis bearbeitet.

Fach- und Methodenkompetenz

- Kenntnis der wesentlichen Projektmanagementmethoden, basierend auf internationalen Standards, z.B. GPM/IPMA, PMI, PRINCE2, Scrum.

Handlungskompetenz:

- Fähigkeit zur Anwendung von modernen Projektmanagementmethoden in realen Projektsituationen.

- Fähigkeit zur Recherche relevanten Wissens aus Literatur und Projektmanagement-Standards.
- Eigenständiger Erwerb von relevantem Fach- und Kontextwissen.

Sozialkompetenz:

- Entwicklung von Sozialkompetenz im Projekt, insbesondere Führungskompetenzen, Teamfähigkeit und Kommunikationsfähigkeit.

Inhalt:

Die Inhalte der Veranstaltung umfassen den Aufbau technischer, Verhaltens- und Kontextkompetenzen rund um das Thema Projektmanagement sowie eigene Recherchetätigkeit.

Im Rahmen des Moduls werden in Teams Aufgaben aus realen Projekten simuliert. Auf fortgeschrittene und aktuelle Themen im Projektmanagement wird eingegangen.

Studien- / Prüfungsleistungen:

Schriftliche Ausarbeitung mit Präsentation. Präsentation mit starkem Fokus auf Rückfragen zu allgem. Projektmanagement-Theorie (analog mündlicher Prüfung). Teil der Prüfungsleistung ist zudem die aktive Teilnahme an der die Präsentationen ergänzenden mündlichen Diskussion.

Literatur:

- Timinger, H. (2017): Modernes Projektmanagement. Wiley, Hoboken
- Roock, S. und Wolf H. (2018): Scrum verstehen und erfolgreich einsetzen. dpunkt.verlag
- Weitere Literatur i.R. selbständiger Literaturrecherche. Empfohlen u.a.:
- Deutsche Gesellschaft für Projektmanagement e.V. GPM (Hrsg.) (2019): Kompetenzbasiertes Projektmanagement (PM4). Handbuch für Praxis und Weiterbildung im Projektmanagement. 1. Auflage, GPM, Nürnberg
- Kerzner, H. (2017) Project Management: a Systems Approach to Planning, Scheduling and Controlling. 12th Edition. Wiley, Hoboken.
- Axelos (2017) Managing Successful Projects with PRINCE2. 6th Edition. The Stationary Office.
- PMI (2017) A Guide to the Project Management Body of Knowledge (PMBOK). 6th Edition. Project Management Institute
- Empfohlene Literatur zur Zertifizierungsvorbereitung (oder zum Lernen):
- Dittmann, K. und Dirbanis, K. (2020) Projektmanagement (IPMA) Lehrbuch für Level D und Basiszertifikat (GPM). Haufe.
- Gubelmann, J., Sommer, C.-J., Sedlmayer, M. (2021) Projektmanagement - Zertifizierung nach IPMA (ICB4)-Ebenen D und C - Grundlagen und Kompetenzen, Methoden und Techniken mit zahlreichen Beispielen. compendio Bildungsmedien

IT-Sicherheitsmanagement

Modulkürzel:	DIS-IT-Sicherheitsmanagement	**Modul-Nr.:**	19
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	5	

Modulverantwortliche(r):	Prof. Dr. Michael Netter
Dozierende:	Prof. Dr. Michael Netter
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Wintersemester
Lehrveranstaltungen des Moduls:	IT-Sicherheitsmanagement
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Keine
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	DIS

Angestrebte Lernergebnisse:

Die Studierenden kennen die gängigen Standards im Bereich des IT-Sicherheitsmanagements. Sie könnenRisikoanalysen durchführen und ein Notfallmanagement konzipieren und etablieren.

Fach- und Methodenkompetenz:
Die Studierenden werden befähigt …

- ... die Aufgaben des IT Sicherheitsmanagements zu benennen.
- ... Risikoanalysen durchzuführen.
- ... ein ISMS gemäß ISO 27001 / IT-Grundschutz aufzubauen

Handlungskompetenz:
Die Studierenden können …

... die BSI Grundschutz-Methode anwenden.

… die Eigenschaften sicherer Netzwerkarchitekturen benennen.

... Audits planen.

Sozialkompetenz:
Die Studierenden können …

… komplexe Problemstellungen aus dem Bereich des IT-Sicherheitsmanagements im Team erörtern.

... ihre Präsentationsfähigkeiten verbessern.

… die Fähigkeit zum Zeitmanagement verbessern.

Inhalt:

- Grundlegende Begriffe des IT-Sicherheitsmanagements (Schwachstelle, Bedrohung, Schutzmaßnahmen)
- Risikomanagement

- Einführung in die ISO/IEC 27001-Familie
- Einführung in BSI IT-Grundschutz
- Der Faktor Mensch (Social Engineering und Awareness Kampagnen)

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 60 Minuten

Literatur:

- Michael Brenner, et al.: Praxisbuch ISO/IEC 27001 – Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 2. Auflage, neu bearbeitet und erweitert, Hanser Verlag, 2017,ISBN: 978-3446451391
- Thomas W. Harich: IT-Sicherheitsmanagement: Praxiswissen für IT Security Manager, mitp Verlag, 2.Auflage 2018 (30. Juni 2018), 978-3958452732
- Jaqueline Naumann; Ihr Kampf als Informationssicherheitsbeauftragter (ISB) (Die ganze Härte der ISO27001), Books on Demand Verlag; 2. Auflage (18. September 2018), ISBN: 978-3746091303

Datenschutzfolgenabschätzung mit Risikomanagement			
Modulkürzel:	DIS-Datenschutzfolgenabschätzung m.RM	**Modul-Nr.:**	20
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	5	

Modulverantwortliche(r):	Prof. Dr. Michael Netter	
Dozierende:	Hr. Rehfeld	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Datenschutzfolgenabschätzung mit Risikomanagement	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Die Studierenden haben ein Verständnis vom Risikomanagement und können dies im Kontext des Datenschutzes anwenden. Sie sind in der Lage, methodisch sicher eine Datenschutzfolgeabschätzung durchzuführen. Ferner sind sie mit den datenschutzrechtlichen Grundlagen und Standards im Kontext der Datenschutzfolgeabschätzung vertraut. Durch die praxisnahen Übungen in Form eines Planspiels sind die Studierenden mit der Anwendung auf konkrete Sachverhalte vertraut.

Fach- und Methodenkompetenz:
Die Studierenden werden befähigt …

- … eigenständig Risiken zu identifizieren.
- … eigenständig eine Risikoanalyse durchzuführen.
- … Schritte zur Vorbereitung auf die Datenschutzfolgeabschätzung zu benennen und diese im Kontext einzuordnen.
- … die Phasen der Datenschutzfolgeabschätzung zu durchlaufen und diese eigenständig durchzuführen.

Handlungskompetenz:
Die Studierenden können …

- ... im Anwendungsfall die Risiken erkennen und hieraus Folgemaßnahmen ableiten.
- … im Anwendungsfall die Notwendigkeit einer Datenschutzfolgeabschätzung benennen sowie die Folgeschritte einleiten.

Sozialkompetenz:
Die Studierenden können …

- … die Risiken definieren und hieraus Handlungsschritte ableiten.
- … eigenständig eine Datenschutzfolgeabschätzung durchführen.

Inhalt:
• Definition Strategisches Risikomanagement • Risiken im Sinne der DSGVO • Durchführung von Risikoidentifikation und – analysen • Begriffsbestimmung Datenschutzfolgeabschätzung • Verantwortlichkeit für die Datenschutzfolgeabschätzung • Notwendige Vorarbeiten (Tätigkeiten, Beteiligte, etc.) • Phasen einer Datenschutzfolgeabschätzung • Zusatz: Planspiel Datenschutzfolgeabschätzung
Studien- / Prüfungsleistungen:
Studienarbeit (außerhalb Prüfungszeitraum)
Literatur:
• Martin, N., Friedewald, M. et al. (2020): Die Datenschutz-Folgeabschätzung nach Art. 35 DSGVO • Romeike, F. (2018): Risikomanagement. • Vanini, U. (2021): Risikomanagement: Grundlagen Instrumente Unternehmenspraxis. • Kühling, J., Klar, M., Sachkmann, F. (2018): Datenschutzrecht. • Eßner, M., Franck, L. (2021): Datenschutzrecht: Fälle und Lösungen.

Gesetze, Institutionen und Aufgaben			
Modulkürzel:	DIS-Gesetze, Institutionen und Aufgaben	**Modul-Nr.:**	21
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	5	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Rothgang	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Gesetze, Institutionen und Aufgaben	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Die Studierenden verfügen über Kenntnisse des deutschen Verfassungsrechts und seinen Bezügen zum Europarecht. Sie kennen die verfassungsrechtlich geschützten wirtschaftsrelevanten Grundrechte und sind in der Lage, Eingriffe in diese Grundrechte methodisch korrekt zu beurteilen. Sie erkennen die stetig wach-sende Bedeutung des europäischen Primär- und Sekundärrechts im Datenschutz und sind in der Lage, Ver-stöße gegen europäisches Sekundärrecht zu erkennen methodisch korrekt zu prüfen. Die Übung unterstützt die methodische Anwendung der gelernten Inhalte auf konkrete Sachverhalte.

Fach- und Methodenkompetenz:
Die Studierenden werden befähigt ….

- … die Begriffe und Funktionen des Rechts zu definieren.
- ... die Grundrechte im Kontext des Datenschutzes zu erläutern und daraus Grundrechtseingriffe abzuleiten, z. B. informationelle Selbstbestimmung.
- … die Gesetzgebungsverfahren auf nationaler und europäischer Ebene zu benennen.
- … die Zuständigkeit von Institutionen in Bezug auf Datenschutz zu bestimmen.

Handlungskompetenz:
Die Studierenden können …

- … im Anwendungsfall Grundrechtseingriffe definieren und die Folgen ableiten.
- ... im Anwendungsfall die Zuständigkeit der jeweiligen Institution benennen und ihre Eingriffsbefugnis definieren.
- … aktuelle Gesetzgebungsverfahren den jeweiligen Ebenen zu ordnen (National oder Europa).

Sozialkompetenz:

Die Studierenden können …

- … methodisch Sachverhalte im Kontext des Moduls prüfen und anwenden.
- … den aktuellen Diskussionen um Gesetzgebungsverfahren folgen.

Inhalt:

- Grundzüge des Staatsorganisationsrechts (z.B. Gesetzgebungs- und Verwaltungskompetenzen)
- Wirtschaftsordnung und Grundgesetz (allgemein)
- Wirtschaftsrelevante Grundrechte (Eigentumsschutz, Berufsfreiheit, Koalitionsfreiheit, Gleichheitssatz) und sonstige wirtschaftlich relevante Grundrechte und Verfassungsprinzipien
- Grundzüge des Europarechts; europäische Grundfreiheiten und europäisches Sekundärrecht am Beispiel der DSGVO
- Mit dem Datenschutz & IT-Sicherheit befassten Institutionen und ihrer Aufgaben sowie Zuständigkeiten
- Zusammenwirken der Institutionen, insb. auch bei grenzübergreifenden Organisationen

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 60 Minuten

Literatur:

- Schliesky, U. (2014): Öffentliches Wirtschaftsrecht.
- Pieroth, B., Schlink, B. (2005): Staatsrecht II – Grundrechte.
- Gleixner, A. (2018): Staatliche Durchsetzung von Datenschutz: Die Institution des Landes- (und Bundes-) Datenschutz.
- Hauser, W., Unger, K. (2015): Grundzüge des Datenschutzrechts.
- Rosenmayr-Klemenz, C., Bogendorfer, R. (2018): EU-Datenschutzgrundverordnung und Datenschutz-Anpassungsgesetz

Unternehmensauditing

Modulkürzel:	DIS-Unternehmensauditing	**Modul-Nr.:**	22
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	7	

Modulverantwortliche(r):	Prof. Dr. Michael Netter	
Dozierende:	Hr. Rühl	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Unternehmensauditierung	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	Keine	

Angestrebte Lernergebnisse:

Die Studierenden kennen die Auditprinzipien und sind in der Lage ein Audit mit den Schwerpunkten Informationssicherheit, Datenschutz sowie Compliance zu konzipieren und zu managen. Ferner können sie zwischen internen, externen Audit sowie Zertifizierungen differenzieren. Außerdem erhalten sie einen Überblick über die EU-Zertifizierungsverfahren für Produkte (Cyber Resilience Act) und für Prozesse/Produkte/Services (NIS2, EU AI Act) und akkreditierten/notifizierten Zertifizierungsverfahren.

Den Studierenden sind die gängigen Formen eines Audits bekannt und sie können die üblichen Zertifizierungsverfahren benennen. Durch die praxisnahen Übungen festigen sich die konkreten Anwendungsfälle, indem die Studierenden ein Audit vorbereiten und in der Rolle als Auditteam durchführen.

Fach- und Methodenkompetenz:
Die Studierenden werden befähigt …

- … den Begriffe Audit, Zertifizierung, Notifzierung zu definieren.
- … die Rolle des Auditors zu kennen.
- … zwischen (internen/externen) Audits und Zertifizierungen zu unterscheiden.
- … den Ablauf eines Audits zu konzipieren.
- … einen Fragenkatalog für ein Compliance-, Informationssicherheits- und Datenschutz-Audit zu entwickeln.

Handlungskompetenz:
Die Studierenden…

- … können zwischen internen und externen Audits differenzieren.
- … können die Schwierigkeiten bei der Durchführung von Audits erkennen und Handlungsoptionen ableiten.
- …üben erste Schritte ein, ein Audit vorzubereiten, durchzuführen und darüber zu berichten.

Sozialkompetenz:
Die Studierenden können …

- … einen Fragenkatalog für ein (Teil-) Audit entwickeln.
- … eigenständig ein (Teil-) Audit durchführen.

Inhalt:

- Wesen, Arten und Planung von Audits
- Vorbereitung, Durchführung und Nachbereitung eines Audits
- Zertifizierungsverfahren
- Qualifikationsanforderungen an Auditoren
- Methodische Aspekte der Auditierung
- Aktuelle Prüfungsstandards

Studien- / Prüfungsleistungen:

mündliche Prüfung, 10-20 Minuten

Literatur:

- Brauweiler, J., Will, M. (2015): Auditierung und Zertifizierung von Managementsystemen.
- Pachinger, M., Beham, G. (2020): Datenschutz-Audit: Recht - Organisation - Prozess - IT.
- Roßnagel (1999): Datenschutzaudit: Konzeption, Durchführung, gesetzl. Grundlage.
- Sowa, A., Duscha, P. et al. (2005): IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die ITPrüfung. Graham, L. (2015): Internal Control Audit and Compliance: Documentation and Testing under the new COSO Framework.

Professionelle Kommunikation

Modulkürzel:	DIS-Professionelle Kommunikation	**Modul-Nr.:**	23
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	7	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner
Dozierende:	Hr. Mielentz
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	nur Wintersemester
Lehrveranstaltungen des Moduls:	Professionelle Kommunikation
Lehrformen des Moduls:	T - Tutorium
Teilnahmevoraussetzung:	Keine
Empfohlene Voraussetzungen:	Keine
Verwendbarkeit:	Keine

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden beherrschen Kenntnisse in der Problemanalyse und Entwicklung von Vorgehensweisen im kommunikativen Umgang mit Projektpartnern und Teilöffentlichkeiten.

Handlungskompetenz

- Konzeptentwicklung allgemein Kampagnen einordnen und entwickeln
- Modelle zur Einordnung von Konfliktsituationen
- Interventions- und Konfliktmanagementmethoden
- Konfliktverhalten
- Mitarbeiter-, Führungskräfte- und Change-Kommunikation

Sozialkompeten

- Medienkompetenz
- Kommunikationsfähigkeit Empathie
- Emotionale Kompetenz
- Konfliktfähigkeit
- Problemlösungskompetenz

Inhalt:

- Was bedeutet professionelle Kommunikation?
- Vorbereitung auf den Krisenfall
- Grundzüge der medialen Logik bei Risiken und Krisen, erwartete und unerwartete Auswirkungen

• Wie verhalte ich mich richtig vor der Kamera? • Souveräne Reaktion auf journalistische Fragestellungen. • Praktische Übungen vor der Kamera mit Aufnahme und Analyse
Studien- / Prüfungsleistungen:
Studienarbeit mit Präsentation
Literatur:
Wird zu Beginn bekannt gegeben

Allgemeine Wahlpflichtmodule

Marketing

Modulkürzel:	Marketing	**Modul-Nr.:**	24
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	3/7	

Modulverantwortliche(r):	Prof. Dr. Michael Schugk
Dozierende:	Prof. Dr. Michael Schugk
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 48 h Selbststudium: 102 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	Wintersemester
Lehrveranstaltungen des Moduls:	Marketing
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung
Teilnahmevoraussetzung:	Keine
Empfohlene Voraussetzungen:	Schulwissen
Verwendbarkeit:	DIS + WIF

Angestrebte Lernergebnisse:

Fachkompetenz:

- Überblick und Detailkenntnisse bezüglich eines ganzheitlichen Ansatzes zu den Grundlagen des Marketings
- Kenntnis der Bedeutung DV-technischer Applikationen für das Marketing

Methodenkompetenz

- Befähigung zur problemlösungsorientierten Umsetzung der erlernten Inhalte in allen Teilgebieten der Marketinggrundlagen
- Verständnis und Anwendbarkeit der erlernten Theorie auf Basis des entscheidungsorientierten Ansatzes
- Marketingorientierte Kompetenz / Verständnis

Persönlichkeitskompetenz:

- Teamfähigkeit / Verhandlungsfähigkeit
- Zielorientierte, gruppenbezogene Erarbeitung von
- Problemlösungen (Fallstudien, TOPSIM Marketing-
- Simulation, CRM-Schulung am System) unter Zeitdruck

Inhalt:

Strategisches Marketing:

- Analyse und Prognose
- Planung
- Implementierung/Durchführung

• Kontrolle **Operatives Marketing:** • Produktpolitik • Kontrahierungspolitik • Kommunikationspolitik • Vertriebspolitik • Marktforschung
Studien- / Prüfungsleistungen:
Schriftliche Prüfung, 90 Minuten
Literatur:
Wird zu Beginn bekannt gegeben

Hackathon			
Modulkürzel:	Hackathon	**Modul-Nr.:**	25
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	3/7	

Modulverantwortliche(r):	Prof. Dr. Michael Walter	
Dozierende:	Prof. Dr. Michael Walter	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	23 h
	Selbststudium:	53 h
	Gesamtaufwand:	76 h
Moduldauer:	1 Semester	
Häufigkeit:	Wintersemester	
Lehrveranstaltungen des Moduls:	Hackathon	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Schulwissen	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Fachkompetenz:

Die Studierenden durchlaufen in der Veranstaltung einen realitäts-nahen Innovations- und Produktentwicklungsprozess

Dies beinhaltet zunächst die grundsätzliche Zusammenstellung eines interdisziplinären Teams

Im weiteren Verlauf erfolgt die Entwicklung und Anwendung von Problemlösungsstrategien nach der Design Thinking Methode

Die Studierenden erlernen des weiteren Methoden zur Generierung von Produkt- oder Serviceideen.

Des Weiteren erhalten die Studierenden ein gezieltes Pitch-Training und verbessern ihre Präsentationsskills.

Persönlichkeitskompetenz:

Aufbau, Strukturierung und Arbeitskoordination von interdisziplinären Teams

Die Studierenden wenden teamorientiertes Arbeiten und inhalts-bezogene Arbeitsteilung an

Fokussiertes und zielorientiertes Arbeiten unter Zeitdruck und da-bei Fokussierung auf die wesentlichen Elemente der Produktentwicklung

Die Studierenden müssen Präsentationsfähigkeiten durch Zwischenpräsentationen und Live-Pitches beweisen und anwenden.

Handlungskompetenz:

Die Studierenden erlernen und vertiefen Schlüsselkompetenzen in den Bereich Projektmanagement, Problemlösungsmethoden, betriebswirtschaftliche Teildisziplinen, Team- und Kommunikationsfähigkeit sowie Präsentationstechniken.

Durch den Besuch der Veranstaltung können die Studierenden zu-dem einen Innovationsprozess einschätzen und selbst in entsprechenden Projektteams durchlaufen.

Inhalt:

- Teambuilding
- Problemlösungstrategien
- Ideation
- Design Thinking
- Business Design
- Research & Development
- Validation
- Prototyping
- Pitching

Studien- / Prüfungsleistungen:

Für Bachelor-Studierende: Abschlusspräsentation + Schriftliche Beschreibung Geschäftskonzept (Umfang ca. 5 Seiten)

Literatur:

Wird zu Beginn bekannt gegeben

Datenbanken			
Modulkürzel:	DIS-Datenbanken	**Modul-Nr.:**	26
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Decker	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	0 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Datenbanken	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	Keine	

Angestrebte Lernergebnisse:

Qualifikationsziele:

Fach- und Methodenkompetenz:

Die Studierenden

- kennen Sinn und Gründe für den Datenbanksystem(DBS)-Einsatz
- können konzeptuelle Datenmodelle erstellen (semantische Modellierung) – insbesondere Entity-Relationship-Modelle (ERM) - und diese in logische Datenmodelle transformieren – insbesondere in das relationale,
- kennen die Normalformentheorie und ihre Anwendung,
- können Standard SQL und Datendefinitions- bzw. Datenmanipulationssprachen ausgewählter Datenbanksysteme anwenden, kennen die Konzepte und Mittel der Datenbankanwendungsprogrammierung,
- kennen die Anwendungsbereiche und Architektur objektorientierter und objektrelationaler Datenbanken,
- kennen wichtige Administrationsmethoden von Datenbanksystemen.

Handlungskompetenz:

Die Studierenden können für typische betriebliche Aufgabenstellungen ein Datenbanksystem entwerfen, einrichten und die für den Endbenutzer notwendigen Funktionen bereitstellen/implementieren – auch unter dem Aspekt der Mehrbenutzersynchronisation.

Inhalt:

- Einführung in relationale Datenbanken: Architektur, Drei-Ebenen- Konzept nach ANSI/SPARC, Gegenüberstellung traditioneller und moderner, semantischer und logischer Datenbankmodelle
- Modellierung, Design und Implementierung: ERM, Normalformen und Designfragen relationaler Datenbanken, Sprachklassen, Structured Query Language (SQL)
- Datenbankprogrammierung: Embedded SQL mit Java und c#, Java Database Connectivity (JDBC), Datenbankprozeduren, O/R-Mapping: Abbildung von Klassen auf Datenbanktabellen und umgekehrt; Trigger und Transaktionen
- Einführung in die Datenbankadministration: Datenbank-, Nutzer-, und Rechteverwaltung, Backup und Recovery, Sicherheitskonzepte

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:

- Heuer, G. Saake, K--U. Sattler: Datenbanken kompakt, mitp
- Heuer, G. Saake, K--U. Sattler: Datenbanken Konzepte und Sprachen, mitp
- Kemper, A. Eickler: Datenbanksysteme – Eine Einführung, Oldenbourg Verlag
- G. Vossen: Datenmodelle, Datenbanksprachen und Datenbankmanagementsysteme, Oldenbourg Verlag Webcast und Online-/Video-Tutorials laut aktueller Empfehlung
- R. A. Elmasri, S.B. Navathe: Grundlagen von Datenbanksystemen – Bachelorausgabe, Pearson Studium

Unternehmensführung

Modulkürzel:	Unternehmensführung	**Modul-Nr.:**	27
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
		3/7	
Modulverantwortliche(r):	Prof. Dr. Dominik Kögel		
Dozierende:	Prof. Dr. Dominik Kögel		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:		45 h
	Selbststudium:		105 h
	Gesamtaufwand:		150 h
Moduldauer:	1 Semester		
Häufigkeit:	Wintersemester		
Lehrveranstaltungen des Moduls:	AWPM: Unternehmensführung		
Lehrformen des Moduls:	AWPM: SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan		
Empfohlene Voraussetzungen:	keine		
Verwendbarkeit:	Datenschutz und IT-Sicherheit		

Angestrebte Lernergebnisse:

Dieses Modul vermittelt grundlegende Kenntnisse in Unternehmensführung bzw. Management.

Fach- und Methodenkompetenz:

Kenntnis der Managementtheorie, wesentlicher Konzepte des strategischen Managements sowie Entscheidungstheorie, Leadership, operative Unternehmensplanung und -steuerung.

Handlungskompetenz:

Fähigkeit zur Anwendung von theoretischem Wissen zur Unternehmensführung in einer Managementtätigkeit. Analyse der strategischen Positionierung eines Unternehmens und Entwicklung strategischer Optionen. Schlagen der Brücke zur Umsetzung in Form von Zielsystemen.

Sozialkompetenz:

Leadership.

Inhalt:

Unternehmensführung, konkret: wesentliche Aspekte der Managementtheorie, Strategie, Entscheidungsfindung, Führung / Leadership, integrierte Unternehmensplanung.

Sie beschäftigen sich in diesem Modul intensiv mit der Theorie zu Management bzw. Unternehmensführung sowie Strategie und Leadership ebenso wie zum Treffen von Managemententscheidungen. Das Modul vermittelt Ihnen die Kenntnisse und Fähigkeiten, die Sie zum Führen eines Unternehmens brauchen.

Sie führen eine Strategische Analyse für ein ausgewähltes Unternehmen durch und entwickeln strategische Optionen für die Erreichung einer nachhaltigen Steigerung im Unternehmenswert. Im Rahmen von behandelter Theorie ebenso wie in Form von Ihnen durchgeführten Referaten, beschäftigen Sie sich mit wichtigen Konzepten aus der strategischen Managementliteratur. Sie lernen zentrale Aspekte der Organisation als Brückenfunktion zwischen strategischen Zielen und der Umsetzung kennen, die Bedeutung von Kultur, und Sie beschäftigen sich mit Leadership sowie Konzepten aus der strategischen und operativen Unternehmensplanung.
Studien- / Prüfungsleistungen:
Schriftliche Prüfung, 90 Minuten. Durchführung Referat für Prüfung dringend zu empfehlen. Voraussetzung für die Vergabe von Leistungspunkten ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.
Literatur:
• Rumelt, R. (2011) Good strategy – bad strategy. Crown Business • Bob de Wit & Ron Meyer (2014) Strategy – An International Perspective. Cengage • Schreyögg, G. & Koch, J. (2020) Management – Grundlagen der Unternehmensführung. Konzepte – Funktionen - Fallstudien . Springer Weitere Literatur wird im Modul bekanntgegeben.

Fachspezifische Wahlpflichtmodule

Virtualisierungs- und Containertechniken

Modulkürzel:	DIS-Virtualisierungs- und Container-techniken	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Landau	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Virtualisierungs- und Containertechniken	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Fachkompetenz:

- Die Studierenden erhalten einen umfassenden Überblick über moderne Arten der Bereitstellung von Compute-Workloads, virtuelle Maschinen und Container. Sie erlernen, wie komplexe Infrastrukturen zur Bereitstellung von virtuellen Maschinen und Containern aufgesetzt, administriert, gewartet und genutzt werden können.

Handlungskompetenz:

- Die Studierenden können fachliche Entscheidungen in den behandelten Bereichen selbständig treffen. Sie besitzen zudem die Fähigkeit, sich eigenständig in Fachgebiete zielgerichtet einzuarbeiten und die dazu notwendigen Informationen zu beschaffen. Die Studierenden können bei der Auswahl von Virtualisierungs- und Containerinfrastrukturen aktiv mitwirken, um den operativen Betrieb dieser Techniken in Organisationen möglichst effizient zu gestalten.

Persönlichkeitskompetenz:

- Aufbauend auf Ihren Erfahrungen in der Lehrveranstaltung besitzen die Studierenden die Fähigkeit, Fachprobleme in Kleingruppen zu diskutieren und eigene Lösungsvorschläge im Kollegenkreis zielgerichtet zu vermitteln.

Inhalt:

- Geschichte der Virtualisierung und Containerisierung
- Typen von Hypervisoren

- Arten der Virtualisierung: Servervirtualisierung,
- Geschichte der Virtualisierung und Containerisierung
- Typen von Hypervisoren
- Arten der Virtualisierung: Servervirtualisierung, Speichervirtualisierung, Netzwerkvirtualisierung, Desktopvirtualisierung
- Erstellen von virtuellen Maschinen und Containern
- Grundlagen von Firmennetzen für die Architektur von Virtualisierungs- und Containersysteme: VLAN-Segmentierung, Routing, Layer 2 und Layer 3 Switches, Overlay-Protokolle
- Einbindung von virtuellen Maschinen und Containern in Netzwerkinfrastrukturen
- Exkurs Speichersysteme: Fibre Channel, iSCSI, NFS, Block vs File, Hyperconverged Storage
- Cluster- und Hochverfügbarkeitstechniken
- Sicherheit von Virtualisierungsinfrastrukturen
- Container: Ausblick auf Kubernetes, Automatisierung (Ansible und Terraform) und CI/CD

Studien- / Prüfungsleistungen:

Mündliche Prüfung, 15-20 Minuten mit LAS

Literatur:

- Bertram Wöhrmann et al.: VMware vSphere 7 - Das umfassende Handbuch, 6. aktualisierte und erwei-terte Auflage (2020), Verlag Rheinwerk Computing, ISBN: 978-3-8362-7578-1
- Michael Kofler et al.: Hacking & Security: Das umfassende Handbuch, 1. Auflage (27. April 2018), Verlag Rheinwerk Computing, ISBN: 978-3836245487
- Nigel Poulton: Docker Deep Dive: Zero to Docker in a single book, 1. Auflage (18. November 2020), Selbstverlag, ISBN: 978-1916585010
- Online-Materialien der VMware IT Academy
- Online-Materialien der Red Hat IT Academy
- aktuelle Artikel aus Fachzeitschriften (iX, IT Administrator)

Software Craftmanship und Clean Code

Modulkürzel:	DIS-Software Craftmanship und Clean Code	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Hock	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Software Craftmanship und Clean Code	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Vertiefung der Kenntnisse und praktischen Fähigkeiten im Bereich der Softwarequalität. Erwerb von Kenntnissen über Werkzeuge und Verfahren aus der Praxis.

Die Studierenden erwerben vertiefte Kenntnisse und Fähigkeiten zur Analyse, Bewertung und Verbesserung der Softwarequalität. Sie sind in der Lage, Prinzipien, Muster, Techniken und Werkzeuge anzuwenden, die zum Schreiben von sauberem Code benötigt werden.

Inhalt:

- Übersicht über die Grundlagen der Software-Qualität
- Softwaremetriken, Metrikanwendung in der Praxis
- Strukturierter Entwurf, Kohäsion und Kopplung
- Überblick über Prinzipien, Best Practices und Code Smells
- Einhaltung und Überprüfung Java Code Conventions
- Statische Softwareprüfung, insbesondere Review-Techniken und statische Programmanalyse
- Sicherung der Softwarequalität mit Werkzeugen wie SonarQube, PMD, SpotBugs, Checkstyle, Spotless, EqualsVerifier, ArchUnit, jQAssistant, Renovate und Dependency-Track
- Softwaretests mit JUnit
- Überprüfen der Testabdeckung (Code Coverage)

- Atlassian Compass, Backstage, Naikan
- CI/CD
- Design Prinzipien
- Design Patterns (GoF)

Studien- / Prüfungsleistungen:

Schriftliche Prüfung, 90 Minuten

Literatur:

- Schneider, Kurt: Abenteuer Software Qualität – Grundlagen und Verfahren für Qualitätssicherung und Qualitätsmanagement, dpunkt.verlag, 2007
- Robert, Martin: Clean Code – Refactoring, Patterns, Testen und Techniken für sauberen Code, mitp-Verlag, 2009
- Lilienthal, Carola: Langlebige Software-Architekturen, Dpunkt Verlag, 2015
- Bloch, Joshua: Effective Java – Second Edition, Addison Wesley, 2008
- Roock, Stefan: Refactorings in großen Softwareprojekten, Dpunkt Verlag, 2004
- Gamma, Erich: Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley Professional, 1994
- Robert C. Martin: Agile Software Development: Principles, Patterns and Practices, Prentice Hall, 2003
- Bugayenko, Yegor: Elegant Objects Volume 1, CreateSpace Independent Publishing Platform, 2016
- Bugayenko, Yegor: Elegant Objects Volume 2, CreateSpace Independent Publishing Platform, 2017
- Harrer, Simon: Java by Comparison: Become a Java Craftsman in 70 Examples, O'Reilly UK Ltd., 2018
- Robert, Martin: Clean Architecture: A Craftman's Guide to Software Structure and Design, Prentice Hall, 2017
- Robert, Martin: The Clean Coder: A Code of Conduct for Professional Programmers, Prentice Hall, 2011
- David, Thomas: Pragmatic Programmer special 2nd, Addison-Wesley Professional, 2019
- Kaczanowski, Tomek: Practical Unit Testing with TestNg, 2012
- Meszaros, Gerard: xUnit Test Patterns, Addison-Wesley, 2007

Anwendungsentwicklung für iOS und VisionOS			
Modulkürzel:	DIS-Anwendungsentwicklung für iOS und VisionOS	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	

Modulverantwortliche(r):	Prof. Dr. Wolf Knüpffer	
Dozierende:	Prof. Dr. Wolf Knüpffer	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Anwendungsentwicklung für iOS und VisionOS	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	Keine	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz

Die Studierenden werden in die Grundlagen der Entwicklung nativer Apps für iOS eingeführt. Dabei erwerben Sie Kenntnisse der Programmiersprache SWIFT sowie wesentlicher Frameworks zum Aufbau KI-basierter Apps (z. B. CoreML und Vision). Die erworbenen Kenntnisse werden im Rahmen der Konzeption und Erstellung einer eigenständigen App als Studienarbeit im Team vertieft

Handlungskompetenz

Die Studierenden vertiefen die Kompetenz im Umgang mit komplexen Programmierwerkzeugen sowie der Erstellung und Integration von Ki-Modellen in mobile Anwendungen und lernen diese in Projekten einzusetzen.

Inhalt:

Phase I: Einführung in die Grundlagen (Teaching)

1.1 Einführung in die Programmiersprache SWIFT und die Entwicklungsumgebung xCode

1.2 Wichtige Frameworks für künstliche Intelligenz, Virtual Reality und Augmented Reality

Phase 2: Projektarbeit (Coaching)

2.1 Projektabstimmung

2.2 Projektdurchführung
Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten
Literatur:
• Nhan Jayve: Mastering ARKit: Apple's Augmented Reality App Development Platform (English Edition). Apress 2022. • Misrah, A.: Machine Learning for iOS Developers. Willey 2020. • Knüpffer, W.: Integration mobiler IT-Systeme; Einsatzfelder – Management – Strategie. Erich Schmidt Verlag 2017 • Knüpffer, W.(Hrsg.): Von der Idee zur eigenen App. 3. Auflage. Ansbach 2015

Unternehmensberatung			
Modulkürzel:	DIS-Unternehmensberatung	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	

Modulverantwortliche(r):	Prof. Dr. Jonas Härtfelder	
Dozierende:	Hr. Künne	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Unternehmensberatung	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz:

Studierende können nach der Teilnahme an dem Modul in IT-Beratungsprojekte inhaltlich und in ihren Wechselbeziehungen analysieren. Darüber hinaus sind Sie in der Lage, typische Probleme der Praxis mit adäquaten Lösungsansätzen zu bewältigen.

Inhalt:

- Überblick über die Strukturen und relevanten Problemstellungen der Unternehmensberatung im IT-Kontext.
- Grundlagen zur IT-Strategie, IT-Organisation und Prozesse, IT-Governance.
- Anschauliche und praxisnahe Beispiele aus der Unternehmensberatung.

Studien- / Prüfungsleistungen:

Schriftliche Prüfung, 60 Minuten und StAmPR

Literatur:

Aktuelle Fallstudien und Folien aus der Praxis der Beratung.

87 **Spezialisierungen**

Netzwerksicherheit: Analyse

Modulkürzel:	SPM-Netzwerksicherheit: Analyse	**Modul-Nr.:**	27
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	4	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Voitel	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Netzwerksicherheit: Analyse	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Modul "Grundlagen der Informatik"	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Die Studierenden kennen die Protokolle des TCP/IP Netzwerkstacks im Detail. Sie sind in der Lage, die Me-chanismen von TCP/IP und Ethernet zu beschreiben und Werkzeuge zur Netzwerkanalyse anzuwenden.

Fach- und Methodenkompetenz:
Die Studierenden werden befähigt …

- ... die Protokolle des TCP/IP Stacks in ihrem Zusammenspiel zu verstehen.
- ... Netzwerktopologien zu verstehen und Protokolle zu analysieren.
- ... Schwachstellen in Netzwerken zu identifizieren.
- … Netzwerke abzusichern.

Handlungskompetenz:
Die Studierende können …

- ... Netzwerkprobleme und Applikationsprobleme unterscheiden.
- … Netzwerkanalysewerkzeuge einsetzen.
- ... Fehler in TCP/IP Applikationen suchen.

Sozialkompetenz:
Die Studierenden können …

- … komplexe technische Problemstellungen aus dem Bereich Netzwerksicherheit im Team erörtern.
- ... ihre Präsentationsfähigkeiten ausbauen.
- … die Fähigkeit zum Zeitmanagement verbessern.

Inhalt:
• Vertiefte Grundlagen von Netzwerkprotokollen, insb. TCP/IP • Analyse von Netzwerktopologien, Auffinden von Schwachstellen • Analyse von Netzwerkprotokollen, Identifikation von Schwachstellen • Absicherung von Netzwerken / Netzwerkprotokollen • Vertiefung und Veranschaulichung der behandelten Themen in der Übung
Studien- / Prüfungsleistungen:
Studienarbeit (außerhalb Prüfungszeitraum)
Literatur:
• James Forshaw: Netzwerkprotokolle hacken: Sicherheitslücken verstehen, analysieren und schützen, dpunkt.verlag GmbH, 1. Auflage (25. Juni 2018), ISBN: 978-3864905698 • Laura Chappel: Wireshark® 101: Einführung in die Protokollanalyse, mitp Verlag, 2. Auflage 2018 (31. Januar 2018), ISBN: 978-3958456839 • Tim Philipp Schäfers: WLAN Hacking: Schwachstellen aufspüren, Angriffsmethoden kennen und das eigene Funknetz vor Hackern schützen. WLAN-Grundlagen und Verschlüsselungsmethoden erklärt, FRANZIS Verlag GmbH, 1. Auflage (15. Januar 2018), ISBN: 978-3645605236 • Steffen Wendzel: IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung, Springer Vieweg Verlag,1. Auflage 2018 (5. September 2018), ISBN: 978-3658226022 Eric D. Knapp et al.: Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Syngress Verlag, 2. Auflage (15. Dezember 2014), ISBN: 978-0124201149

Netzwerksicherheit: Client & Server			
Modulkürzel:	SPM-Netzwerksicherheit Client & Server	**Modul-Nr.:**	28
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	4	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende:	Hr. Gerd Pflüger	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Netzwerksicherheit: Client & Server	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Grundlagen der Informatik, Einführung in die IT-Sicherheit	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Angestrebte Lernergebnisse

Nach Abschluss des Moduls können die Studierenden End-to-End-Netzwerkarchitekturen im Campus- und Datacenter-Kontext (physisch und virtuell) planen, konfigurieren, absichern und im Betrieb bewerten. Sie verstehen die IP/TCP-IP-Mechanismen für Konfiguration, Kommunikation und Sicherheit von Clients und Servern und wenden diese in typischen Praxis-Szenarien an.

Fach- und Methodenkompetenz:

- Netzwerkkomponenten (Switching, Routing, Firewall, Remote Access) sicher konfigurieren und betreiben (Hardening, Segmentierung, Zugriffskontrollen, Logging/Monitoring).
- Kommunikationsprotokolle und Services für Client-Server-Betrieb zielgerichtet konfigurieren und optimieren.
- Campus- und Datacenter-Designs begründen und umsetzen, inkl. Underlay/Overlay-Prinzipien und Netzwerkvirtualisierung (z. B. ACI/NSX auf konzeptioneller Ebene).
- Moderne Sicherheitskonzepte (Zero Trust, SASE) in ein konsistentes Zielbild überführen und geeignete Kontrollpunkte ableiten.
- Sicherheitswerkzeuge und -prozesse (z. B. IDS/IPS, NDR, SIEM/SOAR – je nach Schwerpunkt) einordnen und in grundlegenden Use Cases anwenden.

Handlungskompetenz:

- Standardaufgaben der Netzwerkadministration strukturiert durchführen (Change, Troubleshooting, Dokumentation) und geeignete Tools einsetzen.
- Konfigurationen und Architekturentscheidungen anhand von Best Practices, Risikoabwägungen und Betriebsanforderungen prüfen und verbessern.

Sozialkompetenz:

- Komplexe technische Problemstellungen im Team analysieren, Lösungen erarbeiten und Ergebnisse verständlich präsentieren.
- Arbeitsaufgaben in Übungen/Labs eigenständig planen und fristgerecht umsetzen (Zeitmanagement).

Inhalt:

- Konfiguration von Switchen, Routern und Wireless Access Points
- Absicherung von Client- & Serversystemen (insb. Windows & Linux)
- Grundlagen Public Key Infrastruktur (PKI) & Zertifikate
- Richtige Konfiguration von Firewalls, Einrichtung von VPNs
- Verschlüsselung der Dateiablage, z:B. Bitlocker, True-/VeraCrypt, etc.
- Intrusion Detection & Prevention Systeme, z.B. Snort, OSSEC, Security Onion, etc.
  Honey Pots & Co.

Studien- / Prüfungsleistungen:

mündliche Prüfung, 20 Minuten

Literatur:

- Peter Kloep: PKI und CA in Windows-Netzwerken: Das Handbuch für Administratoren. Zertifikat-Management und Sicherheit für Ihre Windows-Systeme, Rheinwerk Computing, 1. Auflage (27. Dezember 2017), ISBN: 978-3836255905
- Donald A. Tevault: Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats, Packt Publishing - ebooks Account (January 11, 2018), %0AISBN: 978-1788620307
- Kyle Rankin: Linux Hardening in Hostile Networks: Server Security from TLS to Tor, Addison-Wesley Professional, 1 edition (August 5, 2017), ISBN: 978-0134173269

IT-Infrastruktur: IT – Planung und Administration			
Modulkürzel:	IT – Planung und Administration	**Modul-Nr.:**	29
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	4	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner
Dozierende:	Prof. Dr. Jens-Henrik Söldner
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	Sommersemester
Lehrveranstaltungen des Moduls:	IT – Planung und Administration
Lehrformen des Moduls:	Seminaristischer Unterricht (SU) und Übung (Ü)
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan
Empfohlene Voraussetzungen:	
Verwendbarkeit:	DIS + WIF

Angestrebte Lernergebnisse:

Fachkompetenz und Methodenkompetenz

- Die Studierenden verfügen über detaillierte Kenntnisse der typischen administrativen Aufgaben und Abläufe, die im Kontext des Betriebs eines modernen Betriebssystems anfallen.
- Die Studierenden können grundlegende Zusammenhänge zwi-schen administrativen Tätigkeiten und dem Management des IT-Betriebs erkennen.

Handlungskompetenz

- Die Studierenden können die administrativen Kernaufgaben der Einrichtung und Administration eines modernen Betriebssystems in typischen Einsatzszenarien selbstständig durchführen. Weiter-hin können die Studierenden aktiv an der Planung, Realisierung und Leitung eines IT-Betriebs teilnehmen.

Sozialkompetenz

- Die Studierenden können sowohl mit IT-Fachleuten als auch mit Fachanwendern effektiv und situationsgerecht kommunizieren. Sie sind geübt in der Zusammenarbeit in kleinen bis mittleren Teams und kennen grundlegende Strategien der Arbeitsteilung.

Inhalt:

- Administration und Verwaltung von Linux und Windows Systemen
- Automatisierung von grundlegenden administrativen Tätigkeiten
- Grundlagen in der IT-Sicherheit, um die Systeme vor Bedrohungen zu schützen

Studien- / Prüfungsleistungen:

Schriftliche Prüfung, 90 Minuten
Literatur:
• Michael Kofler et al.: Hacking & Security: Das umfassende Handbuch, 3. Auflage und erweiterte Auflage (2023), Verlag Rheinwerk Computing, ISBN: 978-3836245487 • Online-Materialien der Red Hat IT Academy • Karsten Bratvogel, Thomas Joos et al.: Windows Server 2022 Netzwerkadministration, 1. Ausgabe (März 2022), HERDT-Verlag, ISBN: 978-3-98569-054-1

IT-Infrastruktur: IT - Servicemanagement

Modulkürzel:	IT - Servicemanagement	**Modul-Nr.:**	30
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	4	

Modulverantwortliche(r):	Prof. Dr. Claudia Santa
Dozierende:	Prof. Dr. Claudia Santa
Sprache:	Deutsch
Leistungspunkte / SWS:	5 ECTS / 4 SWS
Arbeitsaufwand:	Kontaktstunden: 45 h Selbststudium: 105 h Gesamtaufwand: 150 h
Moduldauer:	1 Semester
Häufigkeit:	Sommersemester
Lehrveranstaltungen des Moduls:	IT - Servicemanagement
Lehrformen des Moduls:	Seminaristischer Unterricht (SU) und Übung (Ü)
Teilnahmevoraussetzung:	Laus SPO bzw. Studienplan
Empfohlene Voraussetzungen:	
Verwendbarkeit:	DIS + WIF

Angestrebte Lernergebnisse:

Fachkompetenz:

- Die Studierenden verfügen über ein umfassendes Basiswissen im Bereich IT-Servicemanagement (ITSM). Neben den Grundkonzepten des Servicewertesystems nach ITIL4(R), kennen Sie die wichtigsten Herausforderungen und Abläufe in IT-Betrieben.

Handlungskompetenz:

- Die Studierenden verfügen über die Fähigkeit, das Servicewertesystem so zu verstehen, dass sie die Komponenten und Aktivitäten einer Organisation planen und optimieren können, um Wertschöpfung zu erzielen.

Sozialkompetenz:

- Aufbauend auf Ihren Erfahrungen in der Lehrveranstaltung besitzen die Studierenden die Fähigkeit, Fachprobleme in Kleingruppen zu diskutieren und eigene Lösungsvorschläge im Kollegenkreis zielgerichtet zu vermitteln.

Inhalt:

Umfassender Einblick in die wichtigsten IT-Servicemanagementprozesse eines IT-Betriebs, basierend auf dem IT Best-Practice-Rahmenwerk IT Infrastructure Library (ITIL).

Am Rande werden zudem ISO 20k, CoBIT und ISO 27001 behandelt. Neben den Prozessdefinitionen werden u.a. die kritischen Erfolgsfaktoren, Rollen, Kennzahlen und Schnittstellen der ITIL-Kernprozesse im Detail behandelt und durch Fallstudien weiter vertieft.

Optional ist die Teilnahme an einer zusätzlichen und kostenpflichtigen ITIL-Foundation-Zertifizierungsprüfung möglich.

Studien- / Prüfungsleistungen:
Studienarbeit (außerhalb Prüfungszeitraum)
Literatur:
• Nadin Ebel: Basiswissen ITIL 4: Grundlagen und Know-how für das IT Service Management und die ITIL-4-Foundation-Prüfung. dpunkt.verlag GmbH; 1. Auflage, 2021. ISBN: 978-3-86490-710-4. • Reiss, Manuela, Reiss, Georg: IT-Dokumentation im Wandel: Konzepte für Compliance, Agilität und Digitalisierung. Carl Hanser Verlag; 1. Auflage, 2023. ISBN 978-446-47757-5 • Tiemeyer, Ernst (Herausgeber: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. Carl Hanser Verlag; 8.Auflage, 2023. ISBN 978-3-446-47372-0.verlag GmbH; • 1. Auflage, 2014. ISBN: 978-3864901478

Potenziale des E – Business und Mobile Business			
Modulkürzel:	Potenziale des E – Business und Mobile Business	**Modul-Nr.:**	31
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	4	

Modulverantwortliche(r):	Prof. Dr. Wolf Knüpffer	
Dozierende:	Prof. Dr. Wolf Knüpffer	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Potenziale des E – Business und Mobile Business	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Fachkompetenz und Methodenkompetenz

- Die Studierenden kennen wichtige Technologien und Patterns zur Implementierung von Web- und mobilen Anwendungen (HTML, CSS, Java-/Typescript, REST Webservices, Local Storage, Session Management) und wissen, wie Apps basierend auf einer gemeinsamen Codebasis für mehrere Plattformen erstellt werden (Cross-Plattform Entwicklung)
- Die Studierenden vertiefen Charakteristika der Modellierung von Anwendungen und Daten sowie deren Abstimmung im Rahmen eines größeren, komplexen Anwendungsszenarios
- Die Studierenden kennen wichtige Werkzeuge des Softwareentwicklungsprozesses (Projektmanagement, Bug-Tracking, Quellcodeverwaltung, Enterprise Wiki zur Dokumentation) und können diese in der Entwicklung anwenden
- Die Studierenden erarbeiten eine Lösung für eine aktuelle, aus der Forschung / dem Transfer stammenden Fragestellung

Persönlichkeitskompetenz und Sozialkompetenz

- Die Studierenden erarbeiten eine Lösung für eine aktuelle, aus der Forschung oder dem Transfer stammenden Fragestellung. Sie organisieren sich selbst in kleinen Gruppen (max. 5 Personen) und stimmen ihre Entwicklungsschritte innerhalb ihrer Gruppe ab. Sie reviewen ihren Code untereinander und sind in der Lage, positive Kritik zu üben.

Handlungskompetenz

- Die Studierenden können mehrbenutzerfähige Webanwendungen und Apps systematisch entwerfen und implementieren. Dies umfasst Entwurf und Implementierung von Backend-Services, Web-Services und

Frontends. Sie setzen hierzu Frameworks wie z.B. Ionic für die Cross-Plattform-Entwicklung sowie Werkzeuge für die Unterstützung des Softwareentwicklungsprozesses ein.
Inhalt:
• Modellierung, Architektur und Deployment von Webanwendungen und Apps • Erstellung von Webanwendungen und Apps: Ionic, Angular, JavaScript, Typescript, NodeJS • Frameworks zur Implementierung von REST Webservices und Persistenztechnologien: Directus, Strapi • Einführung und Aufbau einer umfassenden Entwicklungsumgebung für Cross-Plattform Apps sowie Backend: Docker, JetBrains WebStorm, Bitbucket, JIRA, Confluence, Bamboo • Muster zur Implementierung asynchroner Methoden in Apps: Promises, async/await, Verbindung zum Observer Pattern • Administration des Backends: Updates von Datenschemata, Versionsmanagement, Versionierung von Datenschemata und REST Webservices
Studien- / Prüfungsleistungen:
Schriftliche Prüfung, 90 Minuten
Literatur:
• Ackermann, P. – Fullstack-Entwicklung: Das Handbuch für Webentwickler, Rheinwerk Computing, neueste Auflage • Ackermann, P. – JavaScript: Das umfassende Handbuch, Rheinwerk Computing, neueste Auflage • Goldberg, J.; Koch, J.O. – TypeScript – ein praktischer Einstieg, O'Reilly, neueste Auflage • Gupta, K. – Mastering Angular-15 and Ionic-7: A Comprehensive Guide to Building Your First Powerful Mobile App, independently published, 2023

88

Werkzeuge für E-Business und Mobile Business			
Modulkürzel:	Werkzeuge für E-Business und Mobile Business	**Modul-Nr.:**	32
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	4	

Modulverantwortliche(r):	Prof. Dr. Wolf Knüpffer	
Dozierende:	Prof. Dr. Wolf Knüpffer	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	48 h
	Selbststudium:	102 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Werkzeuge für E-Business und Mobile Business	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Laut SPO bzw. Studienplan	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS + WIF	

Angestrebte Lernergebnisse:

Handlungskompetenz

- Die Studierenden sind mit grundlegenden Architekturen von E-Business-Anwendungen vertraut und kennen die Werkzeuge zum Aufbau und der Administration solcher Anwendungen.
- Sie sind in der Lage, die verschiedenen Typen umfassender Entwicklungswerkzeuge und marktgängige Standatdsoftwarelösungen für E-Business einzuordnen und in Projekten einzusetzen und kennen die verschiedenen Ansätze der App-Entwicklung und sind mit wichtigen Werkzeugen für die App-Entwicklung vertraut.

Fach- und Methodenkompetenz

- Die Studierenden kennen die wesentlichen Eigenschaften der Grundtypen von E-Business Standardsoftware und die Grundtypen mobiler Anwendungen und
- besitzen grundlegende Fähigkeiten, um je nach Bedarf geeignete Systeme für ein Projekt auszuwählen.
- Sie kennen die verschiedenen Entwicklungsansätze und Werkzeige zur mobilen App-Entwicklung.
- Sie beherrschen wichtige Methoden, um diese Werkzeuge zielgerecht im Projekt einzusetzen.

Inhalt:

Teil 1: Einführung

- Rahmenbedingungen der Systementwicklung im E- und M-Business
- Übersicht der Werkzeuge und deren Entwicklung

Teil 2: Werkzeuge zum effizienten Aufbau von Websites

- Einer Lösungen für Content Management (CMS) und Online Shopping
- Führende CMS im Vergleich

Teil 3: Werkzeuge für die Entwicklung (intelligenter) mobiler Apps

- Einführung in die native App-Entwicklung
- Entwicklung von AR-Apps
- Integration von KI in mobile Anwendungenzur Objekterkennung, Motion Detection, NLP, etc.
- Werkzeuge für die plattformübergreifende Systementwicklung

Teil 4: Deployment, Systemintegration und Anwendungsbetrieb

Studien- / Prüfungsleistungen:

Studienarbeit und schriftliche Prüfung, 60 Minuten

Literatur:

- Nhan Jayve: Mastering ARKit: Apple's Augmented Reality App Development Platform (English Edition).
- Apress 2022.
- Misrah, A.: Machine Learning for iOS Developers. Willey 2020.
- Knüpffer, W.: Integration mobiler IT-Systeme; Einsatzfelder – Management – Strategie. Erich Schmidt Verlag 2017
- Knüpffer, W.(Hrsg.): Von der Idee zur eigenen App. 3. Auflage. Ansbach 2015

89 # Vertiefung der Spezialisierung

90

Secure Software Engineering

Modulkürzel:	Secure Software Engineering	**Modul-Nr.:**	33
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	4	

Modulverantwortliche(r):	Prof. Dr. Michael Netter	
Dozierende:	Prof. Dr. Michael Netter	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Urheberrecht	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz:

- Die Studierenden verstehen den Secure Software Development Lifecycle (SSDL) und können dessen Prinzipien anwenden.
- Sie erkennen typische Schwachstellen und Sicherheitsrisiken in der Softwareentwicklung.

Handlungskompetenz:

- Die Studierenden sind in der Lage, konkrete Schwachstellen (z. B. SQL Injection, XSS, SSRF) zu analysieren und zielgerichtet zu beheben.
- Sie können anhand von Codebeispielen geeignete Schutzmaßnahmen entwickeln.

Sozialkompetenz:

Die Studierenden vertiefen Ihre Fähigkeiten zur Arbeit in Teams und in der Kommunikation.

Inhalt:

- Secure Software Development Lifecycle: Vermittlung des SSDL und dessen Anwendung
- Cryptographic Failures: Analyse und Bewertung kryptographischer Schwächen
- Broken Access Control: Identifikation und Behebung von Zugriffssteuerungsfehlern

• SQL Injection & Command Injection: Erkennen und Absichern gegen injektionsbasierte Angriffe • XSS (Cross-Site Scripting) & SSRF (Server-Side Request Forgery): Analyse typischer Web-Schwachstellen • Path Traversal: Sicherheitsrisiken und Gegenmaßnahmen • SCA (Software Composition Analysis): Einsatz von Dependency Checks zur Erkennung von Sicherheitslücken • Assignments: Bearbeitung themenspezifischer Aufgaben zur praktischen Vertiefung
Studien- / Prüfungsleistungen:
Studienarbeit (außerhalb Prüfungszeitraum)
Literatur:
• Gary McGraw: Software Security: Building Security In, Addison-Wesley, 2006:

IT-Infrastruktur: End-to-End Quality Engineering			
Modulkürzel:	VESPM-IT-Collaboration und Integration	**Modul-Nr.:**	34
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	4	

Modulverantwortliche(r):	Prof. Dr. Claudia Santa	
Dozierende:	Prof. Dr. Claudia Santa	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	End-to-End Quality Engineering	
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS/WIF	

Angestrebte Lernergebnisse:

Noch zu bestimmen

Inhalt:

Noch zu bestimmen

Studien- / Prüfungsleistungen:

Studienarbeit

Literatur:

Noch zu bestimmen

IT-Forensik / Ethical Hacking			
Modulkürzel:	DIS – IT - Forensik	**Modul-Nr.:**	35
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Dozierende	Hr. Wagner / Hr. Ortmann	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	IT - Forensik	
Lehrformen des Moduls:		
Teilnahmevoraussetzung:		
Empfohlene Voraussetzungen:		
Verwendbarkeit:		

Angestrebte Lernergebnisse:

Inhalt:

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Literatur:

91 Praktisches Studiensemester

Praxisseminar			
Modulkürzel:	Praxisseminar	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	6	

Modulverantwortliche(r):	Prof. Dr. Michael Netter	
Sprache:	Deutsch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	45 h
	Selbststudium:	105 h
	Gesamtaufwand:	150 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Wintersemester	
Lehrveranstaltungen des Moduls:	Praxisseminar	
Lehrformen des Moduls:	S - Seminar	
Teilnahmevoraussetzung:	Als Zulassungsvoraussetzung für Module aus der Modulgruppe „Praktisches Studiensemester“ müssen mindestens 120 ECTS-Punkte erzielt worden sein.	
Empfohlene Voraussetzungen:	Teil I und Teil II des Bachelorstudiums	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Fachkompetenz

- Kenntnis typischer Schwachstellenklassen und deren Ausnutzung in einer kontrollierten Umgebung
- Fähigkeit, einschlägige Sicherheitswerkzeuge (z. B. CyberChef, Debugger, Disassembler) gezielt einzusetzen
- Fähigkeit, Aufgabenstellungen systematisch zu analysieren, Lösungsansätze abzuleiten und iterativ weiterzuentwickeln

Methodenkompetenz

- Selbstständige Bearbeitung praxisnaher Sicherheitsherausforderungen auf Basis eigener Recherche und Analyse von Writeups
- Strukturiertes und zielorientiertes Vorgehen unter Zeitdruck in einem kompetitiven Umfeld

Sozialkompetenz

- Zusammenarbeit (Koordination und Kommunikation) im Team mit verteilten Aufgaben und unterschiedlichen Spezialisierungen

Inhalt:

- Einführung in Capture-the-Flag-Wettbewerbe: Konzept, Formate und Infrastruktur
- Überblick über CTF-Aufgabenkategorien und typische Schwachstellenklassen (Web Exploitation, Cryptography, Forensics, Reverse Engineering, Binary Exploitation)
- Aufbau der Kollaborations- und Tool-Infrastruktur
- Praktisches Training anhand vergangener CTF-Challenges mit steigendem Schwierigkeitsgrad

• Analyse von Writeups zur Ableitung von Lösungsstrategien und typischen Angriffsmustern • Teilnahme an einem internationalen CTF-Wettbewerb
Studien- / Prüfungsleistungen:
Teilnahme und Projektarbeit (außerhalb Prüfungszeitraum)
Literatur:
Wird bei Bedarf in der Veranstaltung bekanntgebeben

92

Praxisbegleitende Lehrveranstaltung (wissenschaftliches Arbeiten)			
Modulkürzel:	praxisbegl. Lehrveranstaltung	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	6	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Sprache:	Deutsch	
Leistungspunkte / SWS:	3 ECTS / 2 SWS	
Arbeitsaufwand:	Kontaktstunden:	23 h
	Selbststudium:	68 h
	Gesamtaufwand:	91 h
Moduldauer:	1 Semester	
Häufigkeit:	nur Sommersemester	
Lehrveranstaltungen des Moduls:	Praxisbegleitende Lehrveranstaltung (wissenschaftliches Arbeiten)	
Lehrformen des Moduls:	SU - seminaristischer Unterricht	
Teilnahmevoraussetzung:	Als Zulassungsvoraussetzung für Module aus der Modulgruppe „Praktisches Studiensemester“ müssen mindestens 120 ECTS-Punkte erzielt worden sein.	
Empfohlene Voraussetzungen:	Teil I und Teil II des Bachelorstudiums	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Fach- und Methodenkompetenz
Die Studierenden kennen die fachlichen Anforderungen an wissenschaftliche Abschlussarbeiten und mögliche Strategien, um diese zu erfüllen. Die Studierenden haben im Rahmen eines Arbeitsmusters bereits erste Erfahrungen mit wissenschaftlichem Arbeiten gemacht und kennen die typische Struktur einer wissenschaftlichen Abschlussarbeit.

Handlungskompetenz
Die Studierenden sind in der Lage eine erste wissenschaftliche Arbeit erfolgreich zu erstellen. Die Studierenden können selbständig korrekt zitieren und zielorientiert recherchieren.

Sozialkompetenz
Die Studierenden können ihren KommilitonInnen ihre wissenschaftliche Fragestellung schildern und im Team Lösungsstrategien entwickeln.

Inhalt:

Die Lehrveranstaltung dient zur Vorbereitung auf die Bearbeitung des Bachelor-Projekts und der Bachelorarbeit. Grundlegende Methoden und Verfahren des wissenschaftlichen Arbeitens werden erläutert und anhand eines Arbeitsmusters eingeübt.

Studien- / Prüfungsleistungen:

Teilnahme und Projektarbeit (außerhalb Prüfungszeitraum)

Literatur:

Heesen, Wissenschaftliche Arbeiten schreiben mit Word 2016, Prescient, 2016

Bachelor-Projekt			
Modulkürzel:	Bachelorpr Projekt	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	6	

Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner	
Sprache:	Deutsch	
Leistungspunkte / SWS:	4 ECTS / 2 SWS	
Arbeitsaufwand:	Kontaktstunden:	23 h
	Selbststudium:	98 h
	Gesamtaufwand:	121 h
Moduldauer:	1 Semester	
Häufigkeit:	Winter- und Sommersemester	
Lehrveranstaltungen des Moduls:	Bachelor-Projekt	
Lehrformen des Moduls:	PA - Projektarbeit	
Teilnahmevoraussetzung:	Als Zulassungsvoraussetzung für Module aus der Modulgruppe „Praktisches Studiensemester“ müssen mindestens 120 ECTS-Punkte erzielt worden sein.	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Handlungskompetenz
Die Studierenden erwerben die Kompetenz ein Projekt zur Vorbereitung ihrer Bachelorarbeit eigenständig und zielgerichtet zu definieren und ganz oder teilweise umzusetzen. Dabei erwerben sie die Fähigkeit Projekte zu dokumentieren und zu präsentieren.

Sozialkompetenz
Die Teilnehmer erwerben die Kompetenz vor einem kleineren Auditorium ein Projekt zu präsentieren und zu verteidigen. Dabei erlangen sie die Fähigkeit der Gruppe zu kommunizieren und zu diskutieren.

Inhalt:

- Planung und Umsetzung von individuellen Projekten aus dem Bereich des Datenschutzes und der IT-Sicherheit.
- Gestaltung von Präsentationen mit entsprechenden Visulisierungsprogrammen.
- Präsentationstechniken und Gestaltung von Vorträgen.
- Präsentation von Ergebnissen und oder Teilergebnissen auslaufenden Praxisprojekten.
- Darstellung aktueller Themen aus Projekten.

Studien- / Prüfungsleistungen:

Studienarbeit (außerhalb Prüfungszeitraum)

Literatur:

Wird zu Beginn bekannt gegeben

Bachelorarbeit			
Modulkürzel:	Bachelorarbeit	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit	7	

Modulverantwortliche(r):	Professoren DIS / WIF	
Sprache:	Deutsch/Englisch	
Leistungspunkte / SWS:	5 ECTS / 4 SWS	
Arbeitsaufwand:	Kontaktstunden:	0 h
	Selbststudium:	360 h
	Gesamtaufwand:	360 h
Moduldauer:	1 Semester	
Häufigkeit:	Winter- und Sommersemester	
Lehrveranstaltungen des Moduls:	Bachelorarbeit	
Lehrformen des Moduls:	BAr - Bachelorarbeit	
Teilnahmevoraussetzung:	Die Ausgabe des Themas der Bachelorarbeit setzt die erfolgreiche Ableistung von Modulen im Gesamtumfang von 160 ECTS-Punkten voraus.	
Empfohlene Voraussetzungen:	Keine	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Handlungskompetenz

Befähigung zur Anfertigung einer wissenschaftlichen Arbeit basierend auf einem praktischen Projekt. Hinführen zum selbstständigen wissenschaftlichen Arbeiten.

Inhalt:

Das Thema der Bachelorarbeit wird individuell aus dem Bereich des Themengebietes des Datenschutzes und der IT-Sicherheit gewählt. Die theoretische Arbeit wird auf der Grundlage eines praktischen Projektes formuliert und zeigt die aktuellen Fragestellungen des gewählten Themas sowie deren Lösungsansätze und -wege im Kontext des Projektes auf.

Studien- / Prüfungsleistungen:

Bachelorarbeit (außerhalb Prüfungszeitraum)

Literatur:

Heesen, Wissenschaftliche Arbeiten schreiben mit Word 2016, Prescient Verlag, 2016

93

Bachelorseminar			
Modulkürzel:	Bachelorseminar	**Modul-Nr.:**	
Zuordnung zum Curriculum:	**Studiengang u. -richtung**	**Studiensemester**	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	7	

Modulverantwortliche(r):	Professoren DIS / WIF	
Sprache:	Deutsch	
Leistungspunkte / SWS:	3 ECTS / 2 SWS	
Arbeitsaufwand:	Kontaktstunden:	23 h
	Selbststudium:	68 h
	Gesamtaufwand:	91 h
Moduldauer:	1 Semester	
Häufigkeit:	Winter- und Sommersemester	
Lehrveranstaltungen des Moduls:	Bachelorseminar	
Lehrformen des Moduls:	Teilnahme und Referat	
Teilnahmevoraussetzung:	Keine	
Empfohlene Voraussetzungen:	Grundkenntnisse des wissenschaftlichen Arbeitens	
Verwendbarkeit:	DIS	

Angestrebte Lernergebnisse:

Handlungskompetenz
Die Studierenden erhalten die Kompetenz den Hergang ihre Bachelorarbeit in unterschiedliche Entwicklungsstufen zu beleuchten und wissenschaftlich darzustellen.

Sozialkompetenz
Die Teilnehmer erlangen weiterhin die Kompetenz ihre Arbeit fachlich fundiert in einem studentischen Plenum zu präsentieren und zu verteidigen.

Inhalt:

- Präsentation von Zwischen- und Endergebnissen
- Diskussion von Thesen
- Diskussion von Ergebnissen
- Fortentwicklung von wissenschaftlichen Arbeiten
- Wissenschaftliches Arbeiten

Studien- / Prüfungsleistungen:

Teilnahme und Referat (außerhalb Prüfungszeitraum)

Literatur:

Wird zu Beginn bekannt gegeben

94