HOCHSCHULE
MAINZ

Modulhandbuch

Bachelorstudiengänge

Cyber Security Management B.Sc.
Cyber Security Management dual B.Sc.

HOCHSCHULE
MAINZ

Inhalt

Einordnung und Gesamtdarstellung des Studiengangs . . . 3
Übergreifende Ziele des Studiengangs . . . 3
Qualifikationsziele des Studiengangs . . . 4
Thematische Fokussierungen von Modulen . . . 4
Studienstruktur . . . 6

Semester 1
Grundlagen der Programmierung . . . 8
Grundlagen der Informatik . . . 10
Grundlagen der Resilienz . . . 13
Mathematik . . . 15
Methodik, Systematik & Präsentation . . . 17
Grundlagen der BWL . . . 19

Semester 2
Webanwendungen . . . 22
Sichere Netzwerke & Infrastrukturen . . . 24
Data Management . . . 26
Kryptographische Methoden . . . 29
English . . . 32
IT-Projektmanagement . . . 34

Semester 3
Sichere Softwareentwicklung . . . 38
Pentesting I . . . 41
Härtung von Betriebsumgebungen . . . 43
Identity and Access Management . . . 46
Führung & Interaktion . . . 49
Geschäftsprozesse & Organisation . . . 51

Semester 4
IT-Forensik . . . 54
Pentesting II . . . 56
New Work und Change Management . . . 58
Message-Level Security . . . 61
Datenschutz . . . 64
SIEM/SOC und Vorfallsmanagement . . . 67

Semester 5
Interdisziplinäres Projekt Resilienz . . . 70
Informationssicherheitsmanagementsysteme (ISMS (BSI & ISO)) . . . 72
Innovation & Technologie . . . 76
IT-Sicherheitsrecht . . . 79

Semester 6
Aktuelle Themen der IT-Sicherheit . . . 83
Praxismodul . . . 85
Bachelorarbeit . . . 87

Einordnung und Gesamtdarstellung des Studiengangs

Die Hochschule Mainz verfolgt in ihren Studiengängen fachliche, fachübergreifende und berufsfeldbezogene Ziele in der umfassenden akademischen Bildung und für eine spätere berufliche Tätigkeit Ihrer Studierenden. Das daraus folgende Kompetenzprofil wird in den spezifischen Qualifikationszielen sowie dem Curriculum und Modulen des Bachelor-Studiengangs Cyber Security Management / Cyber Security Management dual umgesetzt:

- Entwicklung von fachlichen Kompetenzen mit ausgeprägter Forschungsorientierung;
- Entwicklung transdisziplinärer Dialogkompetenz;
- Aufbau von praxisorientierter Problemlösungskompetenz;
- Entwicklung von personalen und Sozialkompetenzen;
- Förderung der Bereitschaft zur Wahrnehmung gesellschaftlicher Verantwortung auf der Grundlage der erworbenen Kompetenzen.

Der Bachelor-Studiengang Cyber Security Management / Cyber Security Management dual wird vom Fachbereich Wirtschaft durchgeführt. In der notwendigen fachlichen Breite vermittelt der Bachelorstudiengang wissenschaftliche Grundlagen und methodische Fertigkeiten, die zum Berufsbeginn auf dem Gebiet der Cyber Security benötigt werden und zudem für ein konsekutives Master-Studium der Informatik, Wirtschaftsinformatik und verwandter Gebiete befähigen.

Übergreifende Ziele des Studiengangs

Der Bachelor-Studiengang Cyber Security Management / Cyber Security Management dual mit dem Abschluss Bachelor of Science wird als ein grundlagen- und anwendungsorientierter Studiengang des Fachbereichs Wirtschaft der Hochschule Mainz angeboten. Ziel der Ausbildung ist, die Studierenden mit den wichtigsten Teilgebieten der Cyber Security auf technischer sowie organisatorischer Ebene vertraut zu machen, die Methoden analytischen Denkens und Arbeitens zu erlernen, sowie Abstraktionsvermögen und die Fähigkeit, komplexe Zusammenhänge zu strukturieren, zu schulen.

Durch die Ausbildung dieser Fähigkeiten sollen die Studierenden in die Lage versetzt werden, die für einen Bachelor-Studiengang erforderlichen Grundkenntnisse zu erwerben, sowie sich später flexibel in die vielfältigen Aufgabengebiete unserer Gesellschaft einzuarbeiten, in denen informatische Methoden zum Einsatz kommen oder kommen können. Im Bachelor-Studium in Cyber Security Management / Cyber Security Management dual wird das Hauptaugenmerk auf fundierte Grundkenntnisse, Methodenkenntnisse und die Entwicklung der für die Cyber Security typischen Denkstrukturen gelegt. Darüber hinaus werden aktuelle Methodenkenntnisse in wichtigen Anwendungen vermittelt.

Durch die Abschlussarbeit sollen die Studierenden zeigen, dass sie in einem thematisch und zeitlich eng begrenzten Rahmen in der Lage sind, eine thematisch relevante Aufgabe nach den erlernten Methoden und wissenschaftlichen Gesichtspunkten unter Anleitung weitgehend selbstständig zu bearbeiten.

Der Studiengang ermöglicht den Erwerb eines international vergleichbaren Grades auf dem Gebiet der Cyber Security und stellt im Rahmen eines Bachelor-Studienganges einen ersten berufsqualifizierenden Abschluss dar, welcher u.a. Voraussetzung für das sich anschließende Master-Studium ist. Durch die Bachelorarbeit soll festgestellt werden, ob der Kandidat bzw. die Kandidatin die Zusammenhänge der grundlegenden Ausbildung in der Cyber Security überblickt und die Fähigkeit besitzt, die verwendeten wissenschaftlichen Methoden unter anderem in Hinblick auf das gewählte integrierte Anwendungsfach anzuwenden.

Qualifikationsziele des Studiengangs

Die Absolventinnen und Absolventen des Studiengangs Cyber Security Management / Cyber Security Managemt dual sollen nach Abschluss des Studiums folgende grundlegende Kompetenzen überfachlicher Art im Kontext der Informatik besitzen:

- Sie besitzen Problemlösungskompetenz und können ihr Wissen im Rahmen einer beruflichen Tätigkeit anwenden.
- Sie sind befähigt, die Verantwortung in einem Team zu übernehmen als auch effektiv in Teams zu arbeiten (Teamfähigkeit).
- Sie besitzen die Kompetenz zur Darstellung fachbezogener Sachverhalte (u.a. Fachproblemen, Lösungsansätzen und Ergebnissen), sowie zur fachbezogenen Argumentation und Austausch im Kontext ihrer Berufstätigkeit.
- Sie sind befähigt zu selbständiger Informationssammlung und Urteilsfähigkeit sowie zu eigenständigem Weiterlernen im Bereich der Informatik. Insbesondere sind sie befähigt zur Rezeption und Interpretation von Forschungsliteratur und zur Bewertung alternativer Lösungsansätze in fachlicher Hinsicht.
- Sie können eine informatische Aufgabe in Teams und eigenverantwortlich planen, durchführen, dokumentieren und präsentieren.
- Sie können innerhalb einer vorgegebenen Frist ein Problem aus dem Bereich der Cyber Security mit wissenschaftlichen Methoden bearbeiten und Lösungsvorschläge entwickeln und präsentieren.
- Sie beherrschen wissenschaftlich fundierte Methoden der Programmierung und können diese in Projekten mit unterschiedlichen Themenstellungen praktisch anwenden. Dazu gehören die wissenschaftlichen Methoden des Entwurfs, der Implementierung und des Debuggens von Software. Des Weiteren sind ihnen die Konzepte zum operativen Betrieb von Software vertraut.
- Sie kennen die Konzepte für die Analyse von Angriffen auf Systeme und können Gegenmaßnahmen bestimmen.
- Sie kennen die Grundlagen der Verwendung von Betriebssystemen, Infrastrukturen und Verwaltung von Ressourcen und sind in der Lage, diese Kenntnisse bei dem Entwurf, der Umsetzung und der Optimierung von informatischen Systemen einzusetzen.
- Sie kennen die organisatorischen Möglichkeiten und Maßnahmen, um ein Informationssicherheitsmanagementsystem aufzubauen und zu betreiben.
- Sie besitzen notwendige Grundlagen der BWL sind sicher verstanden, so dass Entscheidungen die wirtschaftlichen Bedürfnisse der jeweiligen Organisation berücksichtigen.

Besonderheit für den dualen Studiengang:

Im Studiengang Cyber Security Management dual werden die genannten Kompetenzen durch die enge Verzahnung von Hochschule und betrieblicher Praxis unterstützt. Die Studierenden übertragen ihr Wissen unmittelbar auf praxisrelevante Fragestellungen in den Partnerunternehmen. Prüfungsleistungen können ausdrücklich unternehmensbezogene Themen aufgreifen, was in den Modulbeschreibungen gesondert hervorgehoben wird.

Thematische Fokussierungen von Modulen

Die Themen Nachhaltigkeit, Interdisziplinarität und Internationalisierung werden in einer Vielzahl der Module aufgegriffen. Themen der Nachhaltigkeit werden dabei sowohl im Grundlagenbereich betrachtet (z.B. In den Grundlagen der Resilienz) aber auch später im Studium durch Module wie New Work and Change Management und können auch vertieft werden durch Optionen aus dem Katalog des gesamten Fachbereichs.

Interdisziplinarität und Internationalisierung sind im Studiengang Cyber Security Management generell immer betrachtet, da das Thema der Cyber Security kein auf Deutschland oder der EU abgeschlossenes Gebilde ist und stark durch die internationale Vorgänge beeinflusst wird. Dies reflektiert sich insbesondere in Modulen wie dem Interdisziplinären Projekt Resilienz, den Aktuellen Themen der IT-Sicherheit aber vor allem in der Kombination der Inhalte der Module.

Der Themenkomplex der künstlichen Intelligenz wird ebenfalls vertreten und insbesondere in den Modulen Data Management und IT-Forensik betrachtet.

Bei der Auflistung der einzelnen Module sind mit ¹ gekennzeichnete Angaben für den Vollzeit-Studiengang, die mit ² gekennzeichneten Angaben für den dualen Studiengang zu berücksichtigen. Die Gruppengrößen beziehen sich stets auf die gesamte Gruppe, welche aus dem Studiengang Cyber Security Management sowie dem Studiengang Cyber Security Management dual gebildet wird und dabei 40 Studierende nicht überschreiten soll.

Die Module Option 1 und Option 2 speisen sich aus den Modulen, die durch den Optionskatalog des Fachbereichs zur Verfügung gestellt werden. Hier besteht jeweils die Möglichkeit, aus diesem sich ändernden Katalog zu wählen und damit das Studium zu bereichern. Der Optionskatalog wird durch den Fachbereich entsprechend veröffentlicht.

Studienstruktur | Cyber Security Management B.Sc.
Cyber Security Management dual B.Sc.

Semester 6 30 ECTS/8 SWS	Praxismodul 5 ECTS/2 SWS			Aktuelle Themen der IT-Sicherheit 3 ECTS/3 SWS	Bachelorarbeit 12 ECTS/3 SWS	
Semester 5 30 ECTS/24 SWS	Option 5 ECTS/4 SWS	Interdisziplinäres Projekt Resilienz 5 ECTS/4 SWS	Option 5 ECTS/4 SWS	ISMS (BSI und ISO) 5 ECTS/4 SWS	Innovation & Technologie 5 ECTS/4 SWS	IT-Sicherheitsrecht 5 ECTS/4 SWS
Semester 4 30 ECTS/24 SWS	IT Forensik 5 ECTS/4 SWS	Pentesting II 5 ECTS/4 SWS	Message-Level Security 5 ECTS/4 SWS	New Work & Change Management 5 ECTS/4 SWS	SIEM/SOC und Vorfallsmanagement 5 ECTS/4 SWS	Datenschutz 5 ECTS/4 SWS
Semester 3 30 ECTS/24 SWS	Sichere Softwareentwicklung 5 ECTS/4 SWS	Pentesting I 5 ECTS/4 SWS	Härtung von Betriebsumgebungen 5 ECTS/4 SWS	Geschäftsprozesse und Organisation 5 ECTS/4 SWS	Identity and Access Management 5 ECTS/4 SWS	Führung und Interaktion 5 ECTS/4 SWS
Semester 2 30 ECTS/24 SWS	Webanwendungen 5 ECTS/4 SWS	Sichere Netzwerke & Infrastrukturen 5 ECTS/4 SWS	Kryptographische Methoden 5 ECTS/4 SWS	Englisch 5 ECTS/4 SWS	Data Management 5 ECTS/4 SWS	Projektmanagement 5 ECTS/4 SWS
Semester 1 30 ECTS/24 SWS	Grundlagen der Programmierung 5 ECTS/4 SWS	Grundlagen der Informatik 5 ECTS/4 SWS	Grundlagen der Resilienz 5 ECTS/4 SWS	Mathematik 5 ECTS/4 SWS	Methodik, Systematik & Präsentation 5 ECTS/4 SWS	Grundlagen der BWL 5 ECTS/4 SWS

Total
180 ECTS/128 SWS

Semester 1

Grundlagen der Programmierung

Kennnnummer	ECTS-Leistungspunkte	Dauer des Moduls	Vorgesehenes Studiensemester	Häufigkeit des Angebots
	5	1 Semester	Semester 1	jährlich

Arbeitsaufwand (gesamt) (h)	Kontaktzeit (h)	Selbststudium (h)
150[1] / 125[2]	60	90[1] / 65[2]

Sprache	Geplante Gruppengröße	Verbindlichkeit
Deutsch	40 Studierende	Pflichtmodul

Modulverantwortliche/r	Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)
Prof. Dr. Markus Nauroth	Grundlagen der Programmierung

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • die grundlegenden Elemente ausgewählter aktueller Programmiersprachen (beispielsweise C++, Java, Go, Python) anzuwenden. • grundlegende Programmierparadigmen (Objektorientierung, funktionale Programmierung, prozedurale und logische Programmierung) anzuwenden sowie Einsatzszenarien zu erkennen. • einfach strukturierte, objektorientierte sowie funktionale Programme unter Verwendung grundlegender programmatischer Konstrukte zu erstellen. • grundlegende Algorithmen und Datenstrukturen differenzieren und anwenden. • wesentliche Schritte zur Programmerstellung mit einer objektorientierten Hochsprache mit einer integrierten Entwicklungsumgebung einzeln und in Teams auszuführen.
2	**Inhalte** Grundlagen zur Programmierung (Variablen, Zuweisungen, Datentypen, Operatoren) Grundbausteine: Anweisungen, Verzweigungen, Schleifen Mathematische Funktionen und Strings Modulare Programmierung (Methoden, Funktionen) Einfache und Referenz-Datentypen / -strukturen Objektorientiertes Denken und Programmieren (Polymorphismus, Hierarchien, Abstrakte Klassen, Interfaces)
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 30–40 %.
4	**Teilnahmevoraussetzungen** /

5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Liang, Y. Daniel: Introduction to Java Programming and Data Structures (Comprehensive Version) Stroustrup, B.: A Tour of C++ (C++ In Depth SERIES) Donovan, A., Kernighan, B.: The Go Programming Language (Addison-Wesley Professional Computing Series) Jeweils aktuelle Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Grundlagen der Informatik				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 1	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Nicolai Kuntze		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Grundlagen der Informatik		

1	**Qualifikationsziele/ Kompetenzen/ Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Strukturen, Formalismen sowie Beschreibungs- und Beweisprinzipien in der Informatik zu benennen und zu beschreiben • Wechselwirkungen zwischen Informatik und Gesellschaft zu benennen • Grundlegende Elemente formaler Sprachen der Informatik zu benennen und Fragestellungen in diesen Sprachen zu formulieren • unterschiedliche Hardware-Konzepte zu beschreiben • elementare Konzepte und Strukturen der Informatik losgelöst von einer aktuellen Programmier-sprache zu erkennen, einzuschätzen und geeignet anzuwenden • Bausteine von Rechnersystemen ihren Funktionen zuzuordnen und alternative Konzepte von HW-Strukturen zu identifizieren • diverse Ansätze zur Umsetzung elementarer Konzepte der Informatik zu diskutieren

2	**Inhalte** Zahlensysteme und Boolsche-/Aussagenlogik Elementare Datentypen Grundstrukturen der Hardware (z.B. Prozessoren/Speichertypen/Speicherverwaltung/BIOS/interne Bussysteme) Grundprinzipien der Programmierung und des Softwareentwurfs Rekursion und Induktion als zugehörige Beweisform Elementare Algorithmen, elementare Konzepte und formale Syntax und Semantik von Programmiersprachen Compiler/ Interpreter/Compreter Komplexität von Algorithmen Bedeutung der IT im Kontext von Unternehmen und der Wissenschaft
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165

10	**Literaturhinweise** Broy,M: Informatik – eine grundlegende Einführung (Teil 1+2), Springer Verlag Sommer, M; Gumm, H.-P.: Einführung in die Informatik, Oldenbourg Herold, H.; Lurz, B.; Wohlrab, J.: Grundlagen der Informatik (Gebundene Ausgabe), Pearson Cormen, T; Leiserson, C.: Algorithmen – Eine Einführung, De Gruyter Hoffmann, D.: Theoretische Informatik, Carl-Hanser-Verlag Witt, K.-U.; Mathematische Grundlagen für die Informatik, Springer Vieweg Biere, A.; Kroening, D.: Digitaltechnik – Eine praxisnahe Einführung, Springer Verlag Jeweils aktuelle Auflage
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Grundlagen der Resilienz				
Kennnnummer	**ECTS-Leistungs-punkte**	**Dauer des Moduls**	**Vorgesehenes Studiensemester**	**Häufigkeit des Angebots**
	5	1 Semester	Semester 1	jährlich
Arbeitsaufwand (gesamt) (h)		**Kontaktzeit (h)**		**Selbststudium (h)**
150[1] / 125[2]		60		90[1] / 65[2]
Sprache		**Geplante Gruppengröße**		**Verbindlichkeit**
Deutsch		40 Studierende		Pflichtmodul
Modulverantwortliche/r		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)**		
Prof. Dr. Dirk Loomans		Grundlagen der Resilienz		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • den Begriff der Resilienz im geschäftlichen Umfeld einzuordnen und zu erläutern • die Aufgaben IT-Sicherheit (Security) von der Betriebssicherheit (Safety) zu unterscheiden • in Szenarien die Konzepte der Security und Safety anzuwenden • typische Muster der Security und Safety zu erläutern • Ursachen für IT-Vorfälle zu erläutern
2	**Inhalte** Widerstandsfähigkeit ist auch bei der IT ein wichtiges Kriterium. Die Resilienz im IT-Umfeld bezieht sich auf die Fähigkeit eines Systems, einer Organisation oder einer Technologie, sich nach unvorhersehbaren Ereignissen, Störungen oder Angriffen zu erholen und ihre Funktionalität so schnell wie möglich wiederherzustellen. Um die Funktionalität eines Systems zu erhalten, sind geeignete Konzepte aus dem Bereich der Sicherheit (Security) und Betriebssicherheit (Safety) anzuwenden. Im Rahmen der Vorlesung werden die Ursachen und geeignete Methoden betrachtet, die in Fällen von Hardwareausfällen, Systemabstürzen, Cyberangriffen oder Hardwareschäden/Datenverlusten angewendet werden können. Konzepte wie Business Continuity, Risk Appetite und Risk Tolerance werden dabei eingeführt und mit Beispielen greifbar gemacht. Die Schutzziele der IT-Sicherheit sowie die Ziele der Betriebssicherheit sind in dem Modul von zentraler Bedeutung und werden entsprechend eingeführt.
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.

4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90min) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** BSI-Standard 200-4: Business Continuity Management Jeweils aktuelle Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Mathematik				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 1	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Sebastian Schlütter		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Mathematik		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • die grundlegenden Techniken und Methoden der linearen Algebra und Analysis anzuwenden • wirtschaftswissenschaftliche Problemstellungen mit mathematischen Methoden zu formulieren und zu lösen • analytisch fundierte Entscheidungen zu treffen und zu begründen • grundlegende Verfahren der Wahrscheinlichkeitsrechnung anzuwenden
2	**Inhalte** Mathematische Grundlagen (elementares Rechnen in ganzen Zahlen, Logarithmen und Potenzen, Gleichungen und Ungleichungen, Folgen und Reihen, Zahlensysteme, Boolesche Algebra) Grundlagen der Linearen Algebra, einschließlich Matrixoperationen und linearer Gleichungssysteme sowie wirtschaftswissenschaftlicher Anwendungen Methoden der Analysis (Differentialrechnung für Funktionen in einer und mehreren Variablen, einschließlich wirtschaftswissenschaftlicher Anwendungen) Optimierungsprobleme; Lagrange-Verfahren; wirtschaftswissenschaftliche Anwendungen Kombinatorik und Wahrscheinlichkeitsrechnung
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /

6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90min) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Iwanowski, S.: Diskrete Mathematik mit Grundlagen, Springer Verlag Königsberger, K.; Analysis 1, Springer Verlag Mehler-Bicher, A.; Mathematik für Wirtschaftswissenschaftler; Oldenbourg Merz, M., Wüthrich, M. V.: Mathematik für Wirtschaftswissenschaftler, Vahlen Schwarze, J.: Mathematik für Wirtschaftswissenschaftler. nwb Sydsaeter, K., Hammond, P., Strom, A., Carvajal, A.: Mathematik für Wirtschaftswissenschaftler. Pearson Teschl, G.; Teschl, S.: Mathematik für Informatiker (Band 1) – Diskrete Mathematik und Lineare Algebra, eXamen.press/Springer Verlag Teschl, G.; Teschl, S.: Mathematik für Informatiker (Band 2) – Analysis und Statistik, eXa-men. press/Springer Verlag Jeweils aktuelle Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Methodik, Systematik & Präsentation				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 1	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Anett Mehler-Bicher		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Methodik, Systematik & Präsentation		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Ziele, Merkmale und den Prozess wissenschaftlichen Arbeitens sowie den Nutzen von Wissenschaft für die Praxis zu erklären • Kreativitätstechniken zur Ideenentwicklung anzuwenden • relevante (insbesondere wissenschaftliche) Literatur zu recherchieren und zu beschaffen, dabei verschiedene Arten wissenschaftlicher und nicht-wissenschaftlicher Literatur zu unterscheiden und hinsichtlich ihrer Qualität einzuschätzen • einen Beitrag zu einem aktuellen Fachthema nach wissenschaftlichen Kriterien in Teamarbeit zu konzipieren, zu schreiben und zu redigieren • eine überzeugende Präsentation als Team zu entwickeln und vorzutragen • effektiv im Team vor Ort und virtuell zusammenzuarbeiten und mit Diversität sowie Konflikten konstruktiv umzugehen • Arbeits- und Lernprozesse zu organisieren und zu reflektieren, gezielt Feedback einzuholen und umzusetzen
2	**Inhalte** Einführung in das wissenschaftliche Arbeiten in der Wirtschaftsinformatik Grundlagen zu Teamarbeit, Zeit- und Selbstmanagement Literaturrecherche und Informationskompetenz Themenstrukturierung und Forschungsfragen Schreiben und Argumentation Kreativitätstechniken Gestaltung und Halten von Präsentationen Nutzung geeigneter Tools (Word, LaTex, Powerpoint, ..)

3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Balzert, Helmut; Schröder, Marion; Schäfer, Christian; Wissenschaftliches Arbeiten; Dortmund; W3L GmbH Herrmann, M. et al.; Schlüsselkompetenz Argumentation; Paderborn; UTB Hug, T., Poscheschnik, G.; Empirisch forschen; Wien; UTB Kornmeier, M.; Wissenschaftlich schreiben leicht gemacht; Bern; UTB Jeweils neueste Auflage. Weitere Literatur wird in der Veranstaltung bekannt gegeben.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Grundlagen der BWL

Kennnnummer	ECTS-Leistungs-punkte	Dauer des Moduls	Vorgesehenes Studiensemester	Häufigkeit des Angebots
	5	1 Semester	Semester 1	jährlich

Arbeitsaufwand (gesamt) (h)	Kontaktzeit (h)	Selbststudium (h)
150[1] / 125[2]	60	90[1] / 65[2]

Sprache	Geplante Gruppengröße	Verbindlichkeit
Deutsch	40 Studierende	Pflichtmodul

Modulverantwortliche/r	Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)
Prof. Dr. Anna Rosinus	Grundlagen der BWL

1 **Qualifikationsziele/Kompetenzen/Lernergebnisse**

Nach erfolgreichem Abschluss des Moduls Grundlagen der BWL sind die Studierenden in der Lage:

- zentrale betriebswirtschaftliche Grundbegri□e wie Umsatz, Gewinn, Produktivität oder Wirtschaftlichkeit sowie zentrale Begri□e der verschiedenen Funktionsbereiche zu erklären.
- betriebswirtschaftliche Ziele, Zusammenhänge und Zielkonflikte, wie z.B. das Spannungsfeld zwischen Gewinnmaximierung und nachhaltigem Wirtschaften im Sinne der „Tripple Bottom Line“, zu erklären und kritisch zu analysieren.
- Abhängigkeiten und Schnittstellen zwischen den Funktionsbereichen zu erläutern.
- die konstitutiven Entscheidungen, insbesondere die Wahl von Unternehmensgegenstand, Rechtsform und Standort, zu erläutern sowie für exemplarische Fälle zu lösen.
- betriebswirtschaftliche Fragestellungen nicht nur systematisch zu lösen, sondern die Ergebnisse auch zu visualisieren und zu präsentieren.
- in Teams zusammenzuarbeiten und dabei kritische Aspekte zu diskutieren, um gemeinsam Entscheidungen zu treffen.

2 **Inhalte**

- Die BWL im System der Wissenschaften: Grundbegriffe, Einordnung und Geschichte des Fachs
- Konstitutive Unternehmensentscheidungen: Wahl von Unternehmensgegenstand, Rechtsform und Standort
- Kompaktdarstellung der Funktionsbereiche: Forschung und Entwicklung, Einkauf/Materialwirtschaft, Produktion, Logistik, Marketing/Vertrieb/Kundenservice, Personalmanagement, Finanzen, IT und Management/Führung
- Planspiel

3 **Lehrformen**

Vorlesung im seminaristischen Stil mit integrierten Übungen sowie einem Unternehmensplanspiel.

4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90 Minuten) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Thommen, J.P., Achleitner, A.-K., Gilbert, D.U., Hachmeister, D., Jarchow, S., Kaiser, G.: Allgemeine Betriebswirtschaftslehre: Umfassende Einführung aus managementorientierter Sicht. Springer Gabler Wöhe, G., Döring, U.: Einführung in die Allgemeine Betriebswirtschaftslehre. Vahlen Jeweils in der neuesten Auflage. Weitere Literatur wird ggf. in der Veranstaltung bekannt gegeben.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Semester 2

Webanwendungen

Kennnnummer	ECTS-Leistungs-punkte	Dauer des Moduls	Vorgesehenes Studiensemester	Häufigkeit des Angebots
	5	1 Semester	Semester 2	jährlich

Arbeitsaufwand (gesamt) (h)	Kontaktzeit (h)	Selbststudium (h)
150[1] / 125[2]	60	90[1] / 65[2]

Sprache	Geplante Gruppengröße	Verbindlichkeit
Deutsch	40 Studierende	Pflichtmodul

Modulverantwortliche/r	Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)
Dr. Simon Rohlmann	Webanwendungen

1 **Qualifikationsziele/Kompetenzen/Lernergebnisse**

Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage:

- Grundprinzipien der Web-Programmierung für Client- und Serverseite Programme sowie dem Web-Mapping zu benennen und zu erläutern
- wichtige Internet-Dienste zu verwenden und typische Internet- und Web-Technologien praktisch einzusetzen
- wichtige Internet- und Web-Technologien sowie Internet-Protokolle aus einer Anwendungsperspektive zu erläutern und in Projekten mit begrenzter Komplexität einzusetzen
- zwischen wesentlichen technischen Ansätzen zu differenzieren und diese im Hinblick auf die Anforderungen einfacher Projekte zu bewerten
- grundlegende Methoden und Techniken zum Entwurf und zur Realisierung interaktiver, datenbankgestützter Webseiten einzusetzen
- typische Schwachstellen in den jeweiligen Technologien benennen und Gegenmaßnahmen zu benennen

2 **Inhalte**

Einführung Internet und Internettechnologien.

Client/Server, Mehrschichtige Architekturen.

Web-Applikationen in Unternehmensanwendungen.

Kopplung bzw. Integration von Web-Anwendungen.

Grundlagen der Web-gestützten Anwendungsentwicklung.

Ausgewählte Entwicklungstechniken und Sprachen für die Implementierung von Internet-Anwendungen (z.B. HTML, CCS, JavaScript, PHP, Angular).

Aktuelle Trends der Webentwicklung

3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 20–40%.
4	**Teilnahmevoraussetzungen** Empfohlen: Modul „Grundlagen der Programmierung“ bestanden
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer praktischen Prüfung oder Klausur (90min)[1] Bei einer praktischen Prüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Wolf, J.: HTML und CSS: Das umfassende Handbuch zum Lernen und Nachschlagen. Inkl. JavaScript, Re-sponsive Webdesign, React und Angular u. v. m, Rheinwerk Computing Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Sichere Netzwerke & Infrastrukturen				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 2	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Nicolai Kuntze		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Sichere Netzwerke & Infrastrukturen		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Grundlagen der digitalen, computergestützten Kommunikation zu beschreiben, zu erläutern und die Schwachstellen zu benennen • digitale Kommunikation beginnend bei den grundlegenden physikalischen Aspekten der Datenübertragung über die hardware- und betriebssystemnahe Realisierung bis zur Nutzung von etablierten Verfahren in Anwendungen zu beschreiben • Herausforderungen von großen und komplexen Netzstrukturen zu benennen • wesentliche Funktionsweisen von aktuellen Komponenten wie Switches und Routern oder Verfahren wie Routing zu beschreiben sowie deren Sicherheitseigenschaften zu benennen. • technische Grundlagen aktueller und kommunikationsorientierter Dienste wie E-Mail, WebRTC oder VoIP zu erläutern • rechnernetzrelevante Herausforderungen des Datenschutzes zu benennen • technische Grundlagen von aktuellen Verfahren wie Verschlüsselungen oder DPI zu erläutern.

2	**Inhalte** Etablierte und grundsätzliche Ansätze zur Strukturierung der Kommunikation. Darunter auch Topologien und verbreitete Referenzmodelle wie das OSI-Schichtenmodell etc. Physikalische und technische Grundlagen der Übertragung wie z.B. Kabeltypen, Aspekte der drahtlosen Übertragung unter Berücksichtigung von Netzen für den mobilen Einsatz, NFC. Technologien und Verfahren der unterschiedlichen Ebenen der Abstraktion, darunter beispielsweise: CSMA, IEEE-802.11 für die Schicht der Media Access Control. Protokolle wie IPv6, Routingverfahren, MPLS für die Schicht der Vermittlung. Protokolle wie TCP, UDP und deren Bedeutung in Betriebssystemen für die Schicht des Transports. Protokolle, Verfahren und Systeme rund um die Ebene der Anwendungen wie beispielsweise DNS oder http. Aktive und passive Komponenten auf allen Ebenen der Kommunikationsabstraktion, wie beispielsweise Bridges, Switches, Router, Firewalls (DPI etc.). Aspekte von Datenschutz und Datensicherheit mit Relevanz für Netzwerke, darunter Verschlüsselungsverfahren und die Abwehr netzbasierter Angriffe etc.
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 20–40%.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90min) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Kurose/Ross; Computernetzwerke: Der Top-Down-Ansatz; Pearson Schreiner; Computernetzwerke: Von den Grundlagen zur Funktion und Anwendung; Hanser Tanenbaum; Computernetzwerke; Pearson. Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Data Management				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 2	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150¹ / 125²		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90¹ / 65²
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Martin Huschens		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Data Management		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • aktuelle unternehmensrelevante Technologien und Methoden aus dem Fachgebiet Data Science einzuschätzen und anzuwenden • grundlegende Methoden des maschinellen Lernens sowie deren Anwendungsgebiete in der unternehmerischen Praxis sind von den Studierenden einzuordnen und zu beurteilen • Anforderungen an den Einsatz von Data Science im Unternehmensumfeld zu definieren • Anwendungsfälle von Data Science zu identifizieren und zu bewerten • Herausforderungen und Risiken bei der Implementierung und beim Betrieb von Data Science-Technologien in der Praxis zu erkennen und zu analysieren • eine eigene Datenanalyse basierend auf Python zu implementieren und Machine Learning Modelle miteinander zu vergleichen • praxisorientierte Fragestellungen in kleinen Teams zu analysieren und Lösungsalternativen zu beurteilen und Lösungsansätze zu entwickeln • ihre Ergebnisse innerhalb und außerhalb des Teams zu diskutieren und zu präsentieren • die Ergebnisse der Teamarbeit gegenüber Fachleuten und Vorgesetzten adäquat zu vertreten

2	**Inhalte** Methoden und Techniken (Data Analytics, Künstliche Intelligenz, Data Mining, Maschinelles Lernen, Algorithmen wie z.B. Neuronale Netze) Technologien (Soft- und Hardwareprodukte für KI in Unternehmen, Python und KI-Libraries, wie Pandas, Scikit-learn, Keras, TensorFlow) Architekturen (Integration von KI-Technologien in IT-Landschaften von Unternehmen) Konzeption und Management (Prozesse zur Identifikation und Implementierung von Anwendungsfällen und mögliche Organisationsformen) Datenmanagement (Datenqualität, Datenschutz), Rollen im Unternehmen (Data Owner, Data Steward usw.)
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil mit Coaching-Elementen statt. Der Übungsanteil beträgt ca. 30–40 %.
4	**Teilnahmevoraussetzungen** Empfohlen: Modul „Grundlagen der Programmierung“ bestanden
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Grus, J. Einführung in Data Science: Grundprinzipien der Datenanalyse mit Python, O‘Reilly. Provost, F., & Fawcett, T. (2013): Data Science for Business: What you need to know about data min-ing and data-analytic thinking, O‘Reilly Media, Inc. Russell, S. J.; Norvig, P. (2019): Artificial intelligence a modern approach. Pearson Education Geron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems, 2019, O‘Reilly Media Jeweils neueste Auflage Weitere Literatur wird in der Veranstaltung bekannt gegeben.

11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Kryptographische Methoden				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 2	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Susanne Griebsch; Prof. Dr. Sebastian Schlütter		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Kryptographische Methoden		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • den Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren zu erläutern • die Notwendigkeit von hybriden Verschlüsselungsverfahren zu erläutern • verschiedene Kryptosysteme (bspw. DES, AES, RSA, (Elliptic Curve-) Diffie-Hellman) zu be-schreiben und deren Anwendungsbereiche zu benennen • typische Angriffe auf kryptographische Systeme zu erkennen und zu erläutern • kryptographische Protokolle zu analysieren und auf mögliche Angriffe zu prüfen.

2	**Inhalte** Die Vorlesung behandelt die Grundlagen der Kryptographie und gliedert sich in die folgenden Schwerpunkte: 1. Hashfunktionen: Einführung in Hashfunktionen, ihre Eigenschaften und Einsatzgebiete. Untersuchung der Sicherheit von Hashfunktionen und der Angriffsmöglichkeiten wie Kollisionen. 2. Symmetrische Kryptographie: • Stromchiffren: Grundlagen und Beispiele, wie das One-Time-Pad. • Blockchiffren: Vorstellung gängiger Blockchiffren wie DES, 3DES und AES. • Betriebsmodi: Erläuterung verschiedener Betriebsmodi wie ECB (Electronic Codebook), CBC (Cipher Block Chaining) und CTR (Counter Mode) sowie deren Schwächen. • Message Authentication Codes (MAC): Bedeutung von MACs in der Nachrichtenauthentifizierung, inklusive HMAC. 3. Asymmetrische Kryptographie: • Schlüsselverteilungsproblem und Schlüsselaushandlung: Vermittlung des Diffie-Hellman-Protokolls und seiner Rolle in der asymmetrischen Kryptographie. • Einführung in elliptische Kurven und deren Verwendung in modernen Kryptosystemen. • Verschlüsselung und Signieren: Einsatz von RSA für Verschlüsselung und digitale Signaturen. 4. Hybride Verschlüsselung: Kombination aus symmetrischen und asymmetrischen Verfahren zur effizienten und sicheren Kommunikation. 5. Angriffe auf Verschlüsselungsverfahren: Einführung in gängige Angriffsvektoren auf Kryptosysteme, wie bspw. Padding Oracle Attacken und Person-in-the-Middle-Angriffe. Diskussion von Abwehrmechanismen. 6. Quantencomputing und Post-Quanten-Kryptographie: Shor’s Algorithmus und die Gefährdung klassischer asymmetrischer Verfahren; Grover’s Algorithmus und seine Auswirkungen auf die Sicherheit symmetrischer Verfahren; aktuelle Entwicklungen zu quantensicheren Kryptosystemen.
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /

6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90min) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/147
10	**Literaturhinweise** • Beutelspacher, A., Schwenk, J., Wolfenstetter, K.-D.: Moderne Verfahren der Kryptographie. Springer Spektrum. • Buchmann, J.: Einführung in die Kryptographie; Springer Spektrum. • Menezes, A. J., van Oorschot, P. C., Vanstone, S. A.: Handbook of Applied Cryptography; CRC Press. • Paar, C., Pelzl, J.: Kryptografie verständlich; Springer Vieweg • Schneier, B.: Angewandte Kryptographie; Pearson Studium • Stallings, W.: Cryptography and Network Security; Pearson Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 22.04.2025

English				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 2	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache English		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Biljana Blank		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** English		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • anspruchsvollere, studienbezogene Literatur sowie Vorträge (audio-visuelle Materialien) in englischer Sprache zu verstehen und Fähigkeiten hinsichtlich Texterstellung und Präsentation zu trainieren. • ihre fachsprachliche Sprachfähigkeit zu entwickeln. • Fallstudien in kleinen Gruppen zu analysieren, zu diskutieren und zu bewerten. • digitale Medien (OpenOLAT Foren, Wiki) zur Ergebnispräsentation einzubinden. • Ergebnisse und Lösungen zu formulieren und diese zu präsentieren.
2	**Inhalte** • Überblick über wichtige grammatikalische Strukturen • Ausbau des Textverständnisses (lesend, schreibend) • Schreibstil
3	**Lehrformen** Lehrveranstaltung aus kombinierter Vorlesung/Übung. Die Lehrveranstaltung findet im seminaristischen Stil mit hohem Übungsanteil statt.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90min) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /

7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Aktuelle Texte von Oxford/Cambridge Verlagen sowie dem Internet zu Information Technology, Information Management, E-Business, Marketing, Investment u. a. Wirtschaftsthemen
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

IT-Projektmanagement				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 2	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Sven Pagel; Prof. Dr. Martin Huschens		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** IT-Projektmanagement		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • den Aufbau verschiedener Formen von IT-Projektorganisationen zu erläutern. • die Umsetzung einer vorgegebenen IT-Projektplanung unter Berücksichtigung von Nachhaltig-keitsprinzipien selbstständig durchzuführen. • Projekte mit den Steuerungsmöglichkeiten des IT-Projektcontrollings zu planen. • Design Thinking und Prototypen als Methoden zu beschreiben und anzuwenden • die in der Praxis eingesetzte Projektmanagement-Software anzuwenden. • in Gruppen ein vorgegebenes IT-Projekt durchzuführen (z.B. Softwareentwicklungsprojekt, Softwareeinführungsprojekt) und die Ergebnisse zu präsentieren sowie im Plenum zu diskutieren. • die wichtigsten Merkmale und Unterschiede gängiger Projektmanagement-Standards zu identifizieren. • klassische und agile Methoden gegeneinander abzugrenzen und die jeweils passenden auszuwählen.

2	**Inhalte** • Grundlagen des IT-Projektmanagements • Aufbau verschiedener Formen von IT-Projektorganisationen sowie die Umsetzung der Projektplanung • Klassische Methoden des IT-Projektmanagements • Agile Methoden des IT-Projektmanagements • Steuerungsmöglichkeiten im IT-Projektcontrolling • Anwendung von in der Praxis üblicher Projektmanagement-Software • Menschen im Projektmanagement (Kreativität, Kompetenzen, Stress, Flow, Selbstmanagement) • Teams im Projektmanagement (Phasen der Teambildung, Rollen, Konfliktbewältigung u.a.) • Requirements Engineering mit agilen Backlogs und User Stories. • Design Thinking mit (Software-)Prototypen
3	**Lehrformen** Seminar / Übung / Gruppenarbeit
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung (bspw. Projektbericht einschließlich Präsentation und ggf. IT-Artefakt/Prototyp)[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165

10	**Literaturhinweise** Kuster, J., Bachmann, C., Hubmann, M., Lippmann, R., & Schneider, P. (2022). Handbuch Projekt-ma-nagement: Agil – Klassisch – Hybrid (5th ed.). Berlin, Heidelberg: Springer. Meyer, H., & Reher, H.-J. (2020). Projektmanagement: Von der Definition über die Projektplanung zum erfolgreichen Abschluss (2nd ed.). Wiesbaden: Springer Fachmedien. Project Management Institute; A Guide to the Project Management Body of Knowledge; German edi-tion; Newton Square, PMI Vigenschow, U.: APM - Agiles Projektmanagement, dpunkt Verlag Wolf, H.: Agile Projekte mit Scrum, XP und Kanban, dpunkt Verlag Röpstorff, S./Wiechmann, R.; Scrum in der Praxis: Erfahrungen, Problemfelder und Erfolgsfakto-ren; dpunkt Verlag Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Semester 3

Sichere Softwareentwicklung				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 3	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Nicolai Kuntze		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Sichere Softwareentwicklung		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Grundmethoden der Softwarentwicklung zu benennen. • Patterns der Softwareentwicklung zu erläutern und anzuwenden • Klassische Schwachstellen wie Buffer Overflows, SQL-Injection, Cross-Side-Scripting zu diskutieren • Formale Ansätze zur Softwaresicherheit wie in MISRA-C, FRAMA-C oder RUST zu diskutieren • Sicherheitsherausforderungen in der Softwareentwicklung zu erläutern • Ziele einer Einbettung von Sicherheit in den Entwicklungsprozess zu benennen und anzuwenden

2	**Inhalte** In der Vorlesung werden die Grundlagen der Softwareentwicklung betrachtet und Design-Patterns sicherer Softwareentwicklung vermittelt. • Dabei wird auf die Schutzziele der IT-Sicherheit im Kontext der Implementierung sowie der Entwicklungsprozesse eingegangen. Anhand von Beispielen werden konkrete Schwachstellen, die sich aus der Softwareentwicklung ergeben betrachtet und erprobt, wie diese durch geeignete Gegenmaßnahmen behoben werden können. • Klassische Schwachstellen wie Buffer Overflows, SQL-Injection, Cross-Side-Scripting und weitere typische Beispiele werden bezüglich ihrer Ursachen in der Softwareentwicklung betrachtet. • Die Eigenschaften sicherer Software werden anhand von Beispielen betrachtet und formale Ansätze zur Softwaresicherheit wie in MISRA-C, FRAMA-C oder RUST diskutiert. • Ansätze der Sicherheitsmodellierung werden ab Beispiel von Microsoft Secure Development Library und STRIDE vermittelt mit dem Ziel einer Einbettung von Sicherheit in den Entwicklungsprozess. • Best-Pratice Ansätze in der Softwareentwicklung
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165

10	**Literaturhinweise** IBM Redbooks Michael Howard, Steve Lipner: The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software, Microsoft Rahul Sharma, Vesa Kaihlavirta: Mastering Rust: Learn about memory safety, type system, concurrency, and the new features of Rust Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski,Ana Oprea & Adam Stubblefield: Building Secure & Reliable Systems Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Pentesting I				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 3	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Dr. Simon Rohlmann		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Pentesting I		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Die Sicherheitslage von IT-Systemen und Anwendungen systematisch zu analysieren, um Schwachstellen zu identifizieren und deren Kritikalität zu bewerten. • Sicherheitslücken und deren Auswirkungen zu benennen und zu erläutern. • Gängige Techniken und Tools zur technischen Sicherheitsanalyse anzuwenden. • Methoden des Penetration Testing anzuwenden, um Sicherheitsprüfungen durchzuführen. • Die Ergebnisse technischer Analysen verantwortungsbewusst zu kommunizieren und Handlungsempfehlungen abzuleiten. • Effektiv in Teams zusammenzuarbeiten, um Aufgaben im Bereich IT-Sicherheit zu analysieren und zu bearbeiten.
2	**Inhalte** Die Lernveranstaltung ermöglicht es Studierenden, IT-Sicherheit in einer praxisnahen Umgebung zu erleben. In einem gesicherten Umfeld können die Studierenden Angriffsstrategien und Schutzmaßnahmen für Netzwerke und Systeme ausprobieren. Zusätzlich werden Themen der IT-Forensik behandelt. Der Schwerpunkt der Veranstaltung liegt auf der Analyse unbekannter IT-Systeme und Anwendungen zur gezielten Erkennung und Ausnutzung von Schwachstellen. Analyse- und Exploit-Tools können im kontrollierten Rahmen eines Pentest-Labs erprobt werden. Zusätzlich präsentieren die Studierenden in Teams pro Termin verschiedene IT-Sicherheitsthemen. Dabei wird sowohl theoretisches Hintergrundwissen vermittelt als auch ein praxisnaher Umgang mit Methoden und Tools zur Schwachstellenanalyse und -behebung. Am Ende des Semesters haben die Teilnehmenden die Möglichkeit, ihr Wissen praktisch anzuwenden, indem sie bisher unbekannte Schwachstellen in Open-Source-Software identifizieren, Lösungsvorschläge erarbeiten und diese den Entwicklern entsprechend den Best Practices des „Responsible Disclosure“-Prozesses melden.

3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung oder Schriftliche Prüfung in Form einer Klausur (90 min)[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Wird je nach Bedarf in der Veranstaltung bekanntgegeben.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Härtung von Betriebsumgebungen				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 3	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Dr. Simon Rohlmann		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Härtung von Betriebsumgebungen		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • die Bedeutung der Härtung von ITK-Systemen zu erläutern und diese als Teil einer umfassenden Sicherheitsstrategie zu implementieren • ungenutzte und potenziell unsichere ITK-Systemkomponenten zu identifizieren und zu deaktivieren • Sicherheitsfunktionen auf Hardware-/Betriebssystemebene zu aktivieren und korrekt zu konfigurieren • eine sichere Sicherheitskonfiguration für Betriebssysteme festzulegen und umzusetzen • das Prinzip der minimalen Rechtevergabe (Least-Privilege-Prinzip) in Betriebssystemen anzuwenden • sichere Konten- und Passwortpraktiken zu etablieren • erweiterte Protokollierungsmaßnahmen der Systeme zu konfigurieren.

2	**Inhalte** Die Vorlesung umfasst folgende Themenbereiche: 1. Einführung in die Systemhärtung • Bedeutung der Härtung von Betriebssystemen für die IT-Sicherheit. • Bedrohungen, denen ungepatchte und schlecht konfigurierte Betriebssysteme ausgesetzt sind, z. B. Datenmanipulation, Datenabfluss, Malware-Einbringung oder Missbrauch von Ressourcen für illegale Aktivitäten (z. B. Crypto-Mining, DDoS-Angriffe, usw.). 2. Deaktivierung ungenutzter Komponenten • Identifizierung von nicht benötigten Diensten und Komponenten. • Deaktivierung oder Deinstallation von nicht benötigten Systemkomponenten und Schnittstellen (z. B. veraltete Protokolle, Autostart-Prozesse, ungenutzte Dateifreigaben). • Vermeidung von Telemetriedatenübertragung, sofern diese nicht für Monitoring notwendig ist. 3. Aktivierung hardwarenaher Schutzfunktionen • Einsatz von CPU-Sicherheitsfunktionen wie Address Space Layout Randomization (ASLR) und Data Execution Prevention (DEP). • Absicherung BIOS und Boot-Verfahren durch z. B. BIOS-Passwörter, sichere Bootmechanismen. • Schutzmaßnahmen gegen Seitenkanalangriffe. 4. Sicherheitskonfiguration • Aktivierung von Verschlüsselungsmethoden zur Übertragung von Daten und Authentifizierungsinformationen. • Verwendung von Zertifikaten für den sicheren Schlüsselaustausch. • Deaktivierung von unsicheren Mechanismen wie Autostart-Funktionen und USB-Medien. • Starke Benutzerkontensteuerung und Protokollierung sicherheitsrelevanter Ereignisse. 5. Berechtigungsmanagement (Least-Privilege-Prinzip) • Überprüfung der vergebenen Rechte und Minimierung von Berechtigungen. • Verwaltung von Benutzerkonten mit minimalen Zugriffsrechten auf Dateien und Systemkomponenten. • Beschränkung des Zugriffs auf Konfigurationsdateien und physische Serverressourcen.

	6. Konten und Kennwörter • Etablierung starker Kennwortrichtlinien, z. B. Kennwortlänge, Komplexität, Änderungsintervall. • Einsatz von Zwei-Faktor-Authentifizierung und Passkeys. • Deaktivierung von Standard- und Gastkonten sowie Änderung von Standardpasswörtern. 7. Technische und organisatorische Maßnahmen zur Härtung • Automatisierung der Härtung mittels Skripten und Härtungspaketen, um Konsistenz über mehrere Systeme hinweg zu gewährleisten. • Sicherstellung, dass neue Systeme unmittelbar nach der Installation gehärtet werden, um Schwachstellen von Anfang an zu minimieren. • Aktivierung erweiterter Protokollierungsfunktionen für IT-forensische Analysen.
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90 min) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** CIS Benchmarks; Center for Internet Security Security Technical Implementation Guides (STIGs); Defense Information Systems Agency (DISA) IT-Grundschutz-Kompendium, Bundesamt für Sicherheit in der Informationstechnik (BSI) Handreichung zum „Stand der Technik“; Bundesverband IT-Sicherheit e.V. (TeleTrusT) Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Identity and Access Management				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 3	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Nicolai Kuntze		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Identity and Access Management		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Die grundlegenden Konzepte des Identity & Access Managements (IAM) zu erläutern und deren Bedeutung für die Sicherheit in IT-Systemen und Anwendungen zu bewerten. • Verschiedene Authentifizierungs- und Autorisierungsmechanismen zu analysieren, einschließlich Multi-Faktor-Authentifizierung (MFA), Kerberos und rollenbasierter Zugriffskontrolle (RBAC). • Die wichtigsten Herausforderungen bei der Verwaltung digitaler Identitäten zu identifizieren, insbesondere in Bezug auf Skalierbarkeit, Sicherheit und Integration von Systemen. • Die Prozesse der Identity Governance & Administration (IGA) zu beschreiben und die Rolle der Automatisierung in der Verwaltung von Identitäten und Berechtigungen zu erläutern. • Die Anwendung zentraler Verzeichnisdienste (bspw. Microsoft Active Directory) zu erklären und deren Nutzung in der Identitäts- und Zugriffsverwaltung zu bewerten. • Sicherheitsrisiken im Zusammenhang mit digitalen Identitäten zu analysieren und geeignete Schutzmaßnahmen zur Risikominderung zu entwickeln.

2	**Inhalte** 1. Grundlagen des Identity & Access Managements (IAM) • Einführung in IAM und seine Bedeutung für die Sicherheit von IT-Systemen • Die fünf A im IAM: Authentifizierung, Autorisierung, Auditierung, Administration und Analytics • Zielsetzung und Anwendungsgebiete von IAM-Systemen 2. Authentifizierungs- und Autorisierungsmechanismen • Authentifizierungstechnologien: Benutzername/Passwort, Multi-Faktor-Authentifizierung (MFA), biometrische Verfahren • Autorisierungsmodelle: Rollenbasierte Zugriffskontrolle (RBAC), regelbasierte und attributbasierte Zugriffskontrolle (ABAC) • Single-Sign-On (SSO) und Zertifikatsbasierte Authentifizierung • Kerberos-Protokoll: Funktionsweise, Schlüsselverteilung und Authentifizierungsprozess • Schutzmaßnahmen zur Verbesserung der Authentifizierungssicherheit 3. Verwaltung digitaler Identitäten • Aufbau und Struktur digitaler Identitäten • Herausforderungen der Identitätsverwaltung: Skalierbarkeit, Sicherheit und Integration • Risiken im Zusammenhang mit digitalen Identitäten und Schutzmaßnahmen (z.B. Phishing, Social Engineering, Brute-Force) 4. Identity Governance & Administration (IGA) • Prozesse der IGA: Benutzerverwaltung, Rechtezuweisung, Rezertifizierung und Berechtigungs-Workflows • Automatisierung von IGA-Prozessen zur Effizienzsteigerung und Minimierung von Fehlerquellen • Berechtigungs-Management im Unternehmen: Onboarding, Abteilungswechsel und Austritte 5. Zentrale Verzeichnisdienste und deren Nutzung • Lightweight Directory Access Protocol: Aufbau und Funktionalitäten • Verwaltung von Benutzerkonten, Gruppen und Multi-Faktor-Authentifizierung 6. Risiken und Schutzmaßnahmen für digitale Identitäten • Analyse der häufigsten Bedrohungen für digitale Identitäten • Sicherheitsstrategien und Schutzmaßnahmen: Multi-Faktor-Authentifizierung (MFA), Verschlüsselung • Best Practices zur Prävention und Reaktion auf Identitätsdiebstahl und -missbrauch
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /

5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung oder schriftliche Prüfung in Form einer Klausur (90 min)[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Osmanoglu; Identity and Access Management; Syngress Tsolkas/Schmidt; Rollen und Berechtigungskonzepte; Springer Rawal/Manogaran/Peter; Cybersecurity and Identity Access Management; Springer Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Führung & Interaktion				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 3	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Michael Christ, Prof. Dr. Markus Nauroth		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Führung & Interaktion		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • die grundlegenden Theorien und Konzepte der Führung zu erläutern und deren Anwendung in verschiedenen Kontexten zu analysieren. • verschiedene Führungsstile zu identifizieren und deren Vor- und Nachteile in Bezug auf unter-schiedliche Situationen und Mitarbeiterbedürfnisse zu diskutieren. • Emotionen in Führungs- und Interaktionsprozessen zu analysieren und deren Einfluss auf Entscheidungsfindung und Teamleistung zu erläutern. • die Bedeutung von sozialen Interaktionen in Führungsprozessen zu erkennen und deren Einfluss auf Teamdynamik sowie Mitarbeitermotivation zu bewerten. • Kommunikations- und Interaktionsstrategien zu entwickeln, die effektiv zur Förderung von Zu-sammenarbeit und Teamarbeit in Gruppen beitragen. • Konfliktmanagement-Techniken anzuwenden, um ein positives Arbeitsumfeld zu fördern.
2	**Inhalte** • Überblick über verschiedene Führungstheorien und deren Anwendungsgebiete • Team- und Mitarbeitendenentwicklung • Analyse von autoritären, demokratischen und laissez-faire Führungsstilen und deren Auswirkungen. • Rollenmodelle und deren Einfluss auf die Arbeitsatmosphäre und Produktivität in Teams • Kommunikationsmodelle von Schulz von Thun, Thomas Gordon & Transaktionsanalyse • Aspekte der Kommunikation (Fragetechniken, Feedback, Feedback, Einwandbegegnung) • Konfliktmanagementstrategien in Teams

3	**Lehrformen** Seminaristische Lehrveranstaltung mit Übungen (Gruppenarbeit und Coaching durch die Lehrenden)
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** Eine Anwesenheit der Teilnehmer/innen wird wg. der kontinuierlichen Teamarbeiten erwartet. Ab-meldungen bedürfen der schriftlichen Form. Bei einem mehr als zweimaligen, unentschuldigten Fernbleiben erfolgt einer Überprüfung des Ausschlusses von der Veranstaltung durch den Veranstaltungsleiter.
6	**Prüfungsart und -umfang** Hausarbeit und Präsentation[1] Bei einer Hausarbeit und Präsentation sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Bastian, Johannes; Combe, Arno; Langer, Roman: Feedback-Methoden. Erprobte Konzepte, evaluierte Erfahrungen. Bruno, Tiziana; Adamczyk, Gregor; Bilinski, Wolfgang: Körpersprache und Rhetorik. Ihr souveräner Auftritt. Fengler, Jörg: Feedback geben. Strategien und Übungen. Lubienetzki, U., & Schüler-Lubienetzki, H.: Was wir uns wie sagen und zeigen. Nerdinger, F.W.: Arbeits- und Organisationspsychologie. Innerhofer, C., & Innerhofer, P.: Handlungsorientierte Führung: Motive und Ziele erfolgreich mana-gen. Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Geschäftsprozesse & Organisation				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 3	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Tobias Walter		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Geschäftsprozesse & Organisation		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Grundlegende Begriffe des Geschäftsprozessmanagements zu benennen. • Ablauforganisationen und Aufbaubauorganisationen zu erläutern und zu gestalten. • den Ablauf der kontinuierlichen Prozessverbesserung darzustellen. • Methoden aus dem Geschäftsprozessmanagements anzuwenden. • Geschäftsprozesse zu analysieren und zu untersuchen. • die Leistungsfähigkeit von Prozessen zu bewerten und kritisch zu hinterfragen. • Verbesserte Prozesse zu planen und zu konzipieren.
2	**Inhalte** • Einführung in das Geschäftsprozessmanagement und das Organisationsmanagement • Strategische und Operative Planung von Geschäftsprozessen • Erkennen, Entwurf und Dokumentation von Geschäftsprozessen • Modellierung von Geschäftsprozessen mit BPMN • Überwachen und Kontrollieren von Geschäftsprozessen • Analyse und Simulation von Geschäftsprozessen • Kontinuierliche Prozessverbesserung, Redesign und Reengineering • Anwendung in der Praxis
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 20–30%.
4	**Teilnahmevoraussetzungen** /

5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung oder schriftliche Prüfung in Form einer Klausur (90 min)[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Dumas, M., Rosa, L. M., Mendling, J., & Reijers, A. H. (2018). Fundamentals of Business Process Man-agement. Springer. Weske, M. (2007). Business Process Management: Concepts, Languages, Architectures. Springer. Weitere Literatur wird in der Veranstaltung bekannt gegeben. Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Semester 4

IT-Forensik				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 4	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Dirk Loomans		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** IT-Forensik		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • IT-forensische Untersuchungen systematisch zu erläutern und dabei Maßnahmen der Beweissicherung darzustellen. • IT-forensische Werkzeuge zu benennen. • Ausgewählte IT-forensische Werkzeuge einzusetzen um Vorfälle zu analysieren und aufzuklären. • aus technische technischer Sicht den Beweiswert der Daten zu diskutiert und zu betrachten.
2	**Inhalte** Maßnahmen und Vorgehensmodelle der Beweissicherung Secure-Analyse-Present (S-A-P) Modell Verschiedene Bereiche der IT-Forensik wie Netzwerkforensik, Speicherforensik, Mobile Device Fo-rensik, Life Forensik, Dokumentenforensik Ansätze der forensischen Datenanalyse auf der Basis gesammelter Log-Informationen Anwendung von Tools wie Write Blocker, Microsoft COFEE, WinDD, R oder WindowsSCOPE
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** **/**
5	**Regelungen zur Präsenz** /

6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Portfolioprüfung[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Schmid, Viola: XXXV: Zur „Beweiskraft informationstechnologischer Expertise“ BSI: Leitfaden „IT-Forensik“ Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Pentesting II				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 4	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Markus Nauroth		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Pentesting II		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • die rechtlichen und ethischen Aspekte zum Thema Hacken zu erläutern • die wichtigsten Werkzeuge für Sicherheitsanalysen anzuwenden • die verschiedenen Standards und Anwendungsgebiet für Penetrationstest darzustellen • Pentests anzuwenden. • technische Sicherheitsanalysen von IT-Infrastrukturen zu planen und durchzuführen • die Risiken von Schwachstellen zu bewerten und auf aktuelle Angriffe zu reagieren • effektiv zu kommunizieren und in Form von Berichten/Präsentationen ihre Ergebnisse vorzustellen.
2	**Inhalte** Kali Linux Grundlagen, Werkzeuge Gesetze, Ethik Pentest Standards Phasen eines Pentests Phasen eines Angriffs Verschiedene Arten von Angriffen und Schwachstellen Grundlagen der Exploit Entwicklung Risikobewertung
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.

4	**Teilnahmevoraussetzungen** **/**
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung oder Schriftliche Prüfung in Form einer Klausur (90 min)[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** • Hacking: The Art of Exploitation, 2nd Edition 2nd Edition, Jon Erickson • Ethical Hacking: A Hands-on Introduction to Breaking In, Daniel G. Graham Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

New Work und Change Management				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 2	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 30 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Susanne Rank		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** New Work & Change Management		

1 **Qualifikationsziele/Kompetenzen/Lernergebnisse**

Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage:

- Klassische vs. moderne Organisationsmodelle und -Formen zu unterscheiden und zu bewerten
- Externe vs. interne Einflussfaktoren auf organisationale Veränderungen zu bewerten und in Beziehung zum erfolgreichen Change Management zu setzen
- Neue Arbeitsformen und -Gestaltung (New Work) zu erkennen und deren Einfluss auf Organisationsformen zu schildern.
- Change Management Konzepte für Veränderungsprogramme zu definieren sowie deren Umsetzung auf Maßnahmenebene zu planen
- die zentralen Dimensionen der Change Management-Konzepte in Bezug auf spezifische Transformation-Fragestellungen der Unternehmen zu erkennen.
- wissenschaftliche Studien und Trends zu unterschiedlichen Transformationen und Change Management-Konzepten aufzuzählen und zu vergleichen.
- ausgewählten und erprobten Change Management-Tools zu differenzieren.
- themenspezifischen Fragestellungen zum Change Management zu entwickeln
- selbstständig im Team Lösungen zu erarbeiten, anschließend diese als Team zu präsentieren sowie ein Lösungskonzept zu einer Fallstudie zu erarbeiten und zu dokumentieren
- den Transfer der wirtschaftlichen, gesellschaftlichen, ökologischen und kulturellen Implikationen der Unternehmenstransformationen zu reflektieren sowie mit anderen zu diskutieren.

2	**Inhalte** Grundlagen der Organisationstheorie und Change Managements (CM), insbesondere: • Externe vs. interne Einflussfaktoren auf Organisationsformen • Klassische vs. moderne Organisationsmodelle • New Work mit strukturellem vs. psychologischen Empowerment, Arbeitsortformen • Erfolgsfaktoren und Phasenmodell des CM sowie die Psychologie der Veränderung (z. B. Change-Kurve) • Arbeitspakete des Change Managements (Analysen, Beteiligung und Change Agent Netzwerke, Sponsor- und Leadership, Kommunikation und Mobilisierung, Organisation Alignement, Trainingsstrategie und Change Monitoring Modelle) • Messbarkeit der Effektivität und der Effizienz des Change Management-Konzepts, insbesondere für Reorganisationen
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 30–40 %.
4	**Teilnahmevoraussetzungen** **/**
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Hausarbeit einschließlich Präsentation (60:40)[1] Bei einer Hausarbeit und Präsentation sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung**
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165

10	**Literaturhinweise** Hiatt, J.; Creasey, T. J.: Change Management AKDAR Model, Proci Research. Kraus, G.; Becker-Kolle, C.; Fischer, T.: Handbuch Change Management, Cornelsen. Krüger, W.: Excellence in Change – Wege zur strategischen Erneuerung, Gabler. Kotter, J.: Leading change, McGraw-Hill. Kotter, J.; Rathgeber, H.: Our Iseberg is melting, Saint Martin's Press. Rank, S.; Scheinpflug, R.: Change Management in der Praxis, ESV Verlag. Vahs, D.: Organisation, Schäffer-Poeschel. Rank, S, Neumann, J.: Change Monitoring in Veränderungsprozessen. Springer Gabler Verlag. Jeweils neueste Auflage Weitere Literatur wird in der Veranstaltung bekannt gegeben.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Message-Level Security				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 4	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Dr. Simon Rohlmann		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Message-Level Security		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • die Unterschiede zwischen Transportkanal-Sicherheit und Message-Level Security zu erläutern • Verfahren wie JSON Web Signature und JSON Web Encryption anzuwenden und deren Sicherheitsaspekte zu bewerten • Technologien wie OAuth, OpenID Connect, SAML detailliert zu beschreiben und typische Schwachstellen zu identifizieren • Angriffe auf Authentifizierungs- und Autorisierungstechnologien wie OAuth, OpenID Connect, SAML zu erkennen und in praktischen Szenarien zu demonstrieren • die Sicherheitsmechanismen moderner Dokumentenformate (z. B. PDF, ODF, OOXML) zu erläutern und auf Schwachstellen zu überprüfen

2	**Inhalt** 1. Einführung in Message-Level Security: Erläuterung des Konzepts der Nachrichtensicherheit im Vergleich zur Transportsicherheit (z. B. SSL/TLS). Erklärung der Notwendigkeit von Message-Level Security in modernen verteilten Systemen, wie z. B. bei der Absicherung von HTTP-Requests. 2. JSON Web Encryption (JWT/JWE): • Einführung in die Datenbeschreibungssprache JSON und ihre Rolle im Web. • Schutz von JSON-Nachrichten bzw. JSON-Tokens durch Signaturen und Verschlüsselung. • Analyse von Sicherheitslücken und Angriffsmöglichkeiten auf JSON-Sicherheitsmechanismen 3. OAuth: • Erläuterung des OAuth-Protokolls als Technologie zum Delegieren von Berechtigungen. • Detaillierte Betrachtung der Authentifizierung und Autorisierung über OAuth. • Analyse von typischen Schwachstellen und Angriffen, wie z. B. Phishing, Token-Hijacking und Token-Manipulation. 4. OpenID Connect: • Einführung in OpenID Connect als Erweiterung von OAuth für die Authentifizierung über Drittanbieter. • Unterschiede zwischen OAuth und OpenID Connect. • Analyse und praktische Demonstration von Angriffen auf OpenID Connect (z. B. Cross-Site Scripting, Token-Substitution, Replay-Angriffe). 5. SAML: • Einführung in SAML als ein Standard für Single Sign-On in Unternehmensumgebungen. • Beschreibung der Funktionsweise von SAML und der Authentifizierungs-Workflows. • Angriffsvektoren auf SAML: Identitätsdiebstahl, XML Signature Wrapping und Remote Code Execution. • Analyse der Angriffe und mögliche Sicherheitsmaßnahmen zum Schutz von SAML-gestützten Systemen. 6. Sicherheit moderner Dokumentenformate (PDF, ODF, OOXML): • Einführung in die Funktionsweise von modernen Dokumentenformaten. • Anwendung von kryptographischen Verfahren zur Sicherstellung von Vertraulichkeit, Integrität und Authentizität in Dokumenten. • Untersuchung der Sicherheitsfeatures von PDF, ODF und OOXML, wie z. B. digitale Signaturen und Verschlüsselung. • Praktische Analyse von Sicherheitslücken und Schwachstellen, z. B. Manipulation signierter Dokumente.

3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90 Min) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Jones/Bradley/Sakimura; RFC 7515 (JSON Web Signature (JWS)); IETF Jones/Hildebrand; RFC 7516 (JSON Web Encryption (JWE)); IETF Jones; RFC 7517 (JSON Web Key (JWK)); IETF Jones; RFC 7518 (JSON Web Algorithms (JWA)); IETF Jones/Bradley/Sakimura; RFC 7519 (JSON Web Token (JWT)); IETF OAuth Working Group Specifications OpenID Connect Specifications SAML Specifications PDF Specification OpenDocument OASIS Standard Office Open XML file formats ECMA Standard Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Datenschutz				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 4	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Bianca Baldus		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Datenschutz		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • die Grundlagen des Datenschutzrechts zu erläutern. • einschlägige Fragestellungen zum nationalen und internationalen Datenschutz zu beantworten und datenschutzrechtliche Problemstellungen in einen praxisbezogenen Kontext zu setzen und zu bearbeiten. • rechtliche Risikofelder zu erkennen und daraus resultierende Rechtsfragen mit Hilfe des Gesetzestextes zu beantworten. • praxisorientierte rechtliche Lösungen für den Datenschutz in Unternehmen oder Behörde – einschl. zu Fragen des Beschäftigtendatenschutzes – zu erarbeiten. • datenschutzrechtliche Probleme und deren praktisch relevante Lösungswege zu skizzieren und vor einer Managementebene zu präsentieren.

2	**Inhalt** 1. Grundlagen • Entwicklung und Zwecke des Datenschutzrecht • Rechtlicher Rahmen: Aufbau und Anwendungsbereich von DSGVO und BDSG 2. Rechtmäßigkeit der Datenverarbeitung und Rechte des Betroffenen • Begriff der personenbezogenen Daten und Zulässigkeitstatbestände • Verarbeitung besonderer Kategorien personenbezogener Daten • Einwilligung der betroffenen Person • Verantwortlichkeit und Datenverarbeitung im Auftrag • Rechte der betroffenen Person 3. Datenschutzkontrolle und Datenschutzaufsicht • Der/die Datenschutzbeauftragte • Organisation der Datenschutzaufsicht • Rechtsfolgen bei Verstößen 4. Dokumentations-, Melde- und Kontrollpflichten des Verantwortlichen • Verzeichnis von Verarbeitungstätigkeiten • Meldepflichten • Datenschutz-Folgenabschätzung 5. Besondere Verarbeitungssituationen • Datenschutz im Beschäftigtenkontext • Videoüberwachung • Datenschutz im Marketing und datenschutzkonforme Webseite • Verbraucherkredite, Scoring- und Bonitätsauskünfte 6. Grenzüberschreitender Datenverkehr 7. Aktuelle Fragestellungen zum Datenschutz
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 20–30 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90 Min.) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /

7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** **Lehrbücher (jeweils aktuelle Auflage)** Kühling/Klar/Sackmann: Datenschutzrecht, C.F. Müller Spieker gen. Döhmann, Datenschutzrecht, Nomos (erscheint 2025) **Kommentare (zur Vertiefung) (jeweils aktuelle Auflage)** Ehmann/Selmayr: Datenschutz-Grundverordnung: DS-GVO, C.H. Beck Gola: Datenschutz-Grundverordnung, C.H. Beck Kühling/Buchner: DS-GVO / BDSG, C.H. Beck Taeger/Gabel: DSGVO - BDSG, Fachm. Recht u.Wirtschaft **Datenbanken/Gesetzestext** Beck-Online, beck-eBibliothek, Juris, Datenschutzrecht: DatSchR, C.H. Beck
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

SIEM/SOC und Vorfallsmanagement				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 4	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Dirk Loomans		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** SIEM/SOC und Vorfallsmanagement		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Strukturen eines Security Incident and Event Management (SIEM) aufzubauen • einen Notfallmanagementplan zu erläutern und durch praktische Übungen umzusetzen • Methoden zur Informationsgewinnung und -bewertung zu nutzen • Werkzeuge zur Analyse sicherheitsrelevanter Informationen anzuwenden • Protokolle zur Automatisierung von Aktivitäten in einem Security Operations Center zu erläutern.
2	**Inhalte** Es werden die wichtigen Aspekte eines SOC bzw. Notfallreaktionsmechanismus betrachtet. Dazu gehört der Aufbau von Security Incident and Event Management Strukturen bis hin zur Notfallplanung als Aufgabe eines Security Operations Centers. Das Modul verbindet dabei organisatorische und technische Betrachtungen. Es werden dabei der Aufbau eines Notfallmanagements erläutert und mit praktischen Übungen umgesetzt, um die Vorbereitung auf einen Angriff zu implementieren. Aber auch die verschiedenen Quellen für Informationen werden erkundet und Methoden zur Informationserlangung und Beurteilung vermittelt. Aus technischer Sicht werden Werkzeuge zur Analyse relevanter Informationen angewendet und Protokolle zur Automatisierung von SOC-Aktivitäten vorgestellt.
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 20–30 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /

6	**Prüfungsart und -umfang** Portfolioprüfung oder Schriftliche Prüfung in Form einer Klausur (90 min)[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** BSI-Standard 200-4 (Business Continuity Management), Bundesamt für Sicherheit in der Informations-technik (BSI) IT-Grundschutz-Kompendium, Bundesamt für Sicherheit in der Informationstechnik (BSI) Jeweils neueste Auflage. Weitere Literatur wird in der Veranstaltung bekannt gegeben.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Semester 5

Interdisziplinäres Projekt Resilienz				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 5	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Dr. Simon Rohlmann		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Interdisziplinäres Projekt Resilienz		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • Sicherheitsrisiken von Webanwendungen zu identifizieren und mit Methoden wie STRIDE zu analysieren. • Sicherheitsmaßnahmen zur Absicherung von Anwendungen gegen gängige Bedrohungen (z.B. SQL Injection, XSS, CSRF, usw.) zu implementieren. • Sicherheitskonzepte zu entwickeln und die Wirksamkeit durch Tests und Audits zu überprüfen. • Projekte mithilfe agiler Managementtechniken zu planen, zu überwachen und erfolgreich umzusetzen. • Effektiv in interdisziplinären Teams zu arbeiten und kommunikative sowie organisatorische Herausfor-derungen zu meistern. • Fortschritte, Risiken und Ergebnisse des Projekts zu dokumentieren und zu präsentieren. • Anforderungen der DSGVO und anderer relevanter Datenschutzrichtlinien zu identifizieren und in Softwareprojekten umzusetzen. • Datenschutzkonzepte zu erstellen, die den rechtlichen Vorgaben gerecht werden. • Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten in Webanwendungen zu implementieren und zu überprüfen.

2	**Inhalte** Das Modul vermittelt praxisorientierte Kompetenzen zur Entwicklung sicherer Webanwendungen im interdisziplinären Kontext von Informatik/IT-Sicherheit, Projektmanagement und Datenschutzrecht. Die Studierenden arbeiten in Teams an einem Softwareprojekt, in dem eine Webanwendung geplant, entwickelt und auf Sicherheitsrisiken analysiert wird. Schwerpunkte des Moduls: • IT-Sicherheit: Identifikation und Analyse gängiger Sicherheitsrisiken (z.B. mit STRIDE), Anwendung von Sicherheitsmaßnahmen zur Härtung der Anwendung, Behandlung von Schwachstellen wie bspw. SQL Injection, XSS, CSRF, usw. • Projektmanagement: Planung, Umsetzung und Überwachung des Projekts mithilfe gängiger Managementtechniken. • Datenschutz: Analyse der Datenschutzanforderungen gemäß DSGVO, Berücksichtigung datenschutzrechtlicher Vorgaben bei der Verarbeitung personenbezogener Daten und Erstellung eines Datenschutzkonzepts.
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Projektdokumentation und Präsentation der Projektergebnisse[1] Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung sollten ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Wird zum Kursbeginn bekannt gegeben.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Informationssicherheitsmanagementsysteme (ISMS (BSI & ISO))				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 5	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Dirk Loomans		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Informationssicherheitsmanagementsysteme (ISMS (BSI & ISO))		

1 **Qualifikationsziele/Kompetenzen/Lernergebnisse**

Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage:

- die Anforderungen und Prozesse eines ISMS gemäß ISO 27001 und BSI IT-Grundschutz zu beschreiben und anzuwenden
- Informationssicherheitsrisiken zu identifizieren, zu bewerten und geeignete Maßnahmen zur Risikobehandlung zu planen
- Sicherheitsrichtlinien und -verfahren zu entwickeln und diese auf die spezifischen Bedürfnisse eines Unternehmens zuzuschneiden
- Prozesse zur Erkennung, Reaktion und Behebung von Sicherheitsvorfällen zu etablieren und Incident-Response-Strategien zu implementieren
- Die Fortführung kritischer Prozesse einer Organisation bei anhaltenden IT-Ausfällen zu gewährleisten
- das ISMS kontinuierlich zu überwachen und anzupassen, um auf sich ändernde Bedrohungen und Anforderungen zu reagieren

2	**Inhalte** 1. Risikomanagement • Identifizierung, Bewertung und Behandlung von Informationssicherheitsrisiken im Unternehmenskontext. • Anwendung von Risikomanagementmethoden zur Analyse und Priorisierung von Sicherheitsmaßnahmen. • Durchführung von Risikobewertungen nach BSI-Standard 200-3. 2. Policies und Richtlinien • Entwicklung von Sicherheitsrichtlinien, die den Unternehmenszielen und -strategien entsprechen. • Beispielhafte Sicherheitsrichtlinien für verschiedene Unternehmensbereiche, wie Zugriffskontrolle, Kryptographie und Notfallmanagement. 3. Compliance • Anwendung von ISO 27001, BSI IT-Grundschutz zur Erfüllung von Compliance-Anforderungen. 4. Incident Response • Aufbau eines Meldesystems und Implementierung von Prozessen zur Erkennung und Bewältigung von Sicherheitsvorfällen. 5. Schulung und Sensibilisierung: • Sensibilisierungsprogramme zur Vermittlung der Bedeutung von Informationssicherheit und des korrekten Umgangs mit Sicherheitsrichtlinien. 6. Kontinuierliche Verbesserung • Anwendung des PDCA-Zyklus (Plan-Do-Check-Act) bei Sicherheitsprozessen. 7. Asset Management: • Identifikation und Kategorisierung von unternehmenskritischen Ressourcen, wie Hardware, Software, Daten und Infrastruktur. 8. Zugriffskontrolle: • Definition von Zugriffsrechten und Implementierung von technischen und organisatorischen Maßnahmen zur Verhinderung unbefugter Zugriffe. • Verwaltung/Überprüfung der Zugriffskontrollen basierend auf Prinzip geringster Berechtigung. • Entwicklung von Notfall- und Geschäftskontinuitätsplänen, um die Aufrechterhaltung der Geschäftsprozesse im Falle eines Sicherheitsvorfalls zu gewährleisten. 9. Kontinuitätsplanung (BCM): • Entwicklung von Notfall- und Geschäftskontinuitätsplänen, um die Aufrechterhaltung der Geschäftsprozesse im Falle eines Sicherheitsvorfalls zu gewährleisten. 10. Auditierung und Überwachung: • Durchführung von internen Audits zur Überprüfung der Einhaltung von Sicherheitsrichtlinien und -standards.

3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 50 %.
4	**Teilnahmevoraussetzungen** **/**
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Portfolioprüfung oder schriftliche Prüfung in Form einer Klausur (90 min)[1] Bei einer Portfolioprüfung sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165

10	**Literaturhinweise** BSI-Standard 200-1, BSI-Standard 200-2, BSI-Standard 200-3, BSI-Standard 200-4 BSI IT-Grundschutz-Kompendium Kersten/Klett; Der IT Security Manager; Vieweg+Teubner Verlag Sowa; Management der Informationssicherheit; Springer Fachmedien Wiesbaden ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 Jeweils neueste Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Innovation & Technologie

Kennnnummer	ECTS-Leistungs-punkte	Dauer des Moduls	Vorgesehenes Studiensemester	Häufigkeit des Angebots
	5	1 Semester	Semester 5	jährlich

Arbeitsaufwand (gesamt) (h)	Kontaktzeit (h)	Selbststudium (h)
150[1] / 125[2]	60	90

Sprache	Geplante Gruppengröße	Verbindlichkeit
Deutsch	40 Studierende	Pflichtmodul

Modulverantwortliche/r	Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)
Prof. Dr. Anna Rosinus, Prof. Dr. Anett Mehler-Bicher	Innovation & Technologie

1 **Qualifikationsziele/Kompetenzen/Lernergebnisse**

Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage:

- grundlegende Begriffe und Prinzipien des Innovations- und Technologiemanagements zu erklären, z. B. Innovationsprozesse, Technologielebenszyklen und disruptive Innovationen.
- verschiedene Innovationsarten (z. B. Produkt-, Prozess-, Geschäftsmodell- und soziale Innovationen) zu unterscheiden und deren Relevanz für Organisationen zu bewerten.
- Technologietrends zu identifizieren, zu analysieren und deren potenzielle Auswirkungen auf Unternehmen kritisch zu beurteilen.
- Methoden und Werkzeuge des Innovationsmanagements wie Design Thinking, Open Innovation oder Stage-Gate-Modelle anzuwenden.
- den Wert von Innovationen durch IT auf wirtschaftliche Aspekte für Unternehmen und entsprechende Auswirkungen auf Geschäftsstrategien zu beschreiben.
- in Teams kreative Lösungsansätze für praxisnahe Innovations- und Technologieprobleme zu erarbeiten.
- Projektergebnisse und Innovationsempfehlungen professionell zu präsentieren und zu verteidigen.

2	**Inhalte** 1. Einführung in das Innovations- und Technologiemanagement • Bedeutung von Innovationen und Technologien für Unternehmen • Grundlagen und Begriffe: Innovationstypen, Technologiemanagement und deren Schnittstellen 2. Innovationsprozesse und -methoden • Design Thinking, Lean Startup, Stage-Gate-Modelle • Open Innovation und Co-Creation-Ansätze 3. Technologiemanagement (Fokus IT) • Technologielebenszyklen und Technologieportfolio-Management • Bewertung und Priorisierung von Technologien 4. Aktuelle Trends und Herausforderungen • Digitalisierung, Künstliche Intelligenz und Nachhaltigkeit • Umgang mit disruptiven Innovationen und technologischem Wandel 5. Praxisprojekte und Fallstudien • Entwicklung und Präsentation von Innovationslösungen • Analyse realer Technologien und Innovationsstrategien in Teams
3	**Lehrformen** Lehrveranstaltung im seminaristischen Stil mit Gruppenarbeiten, Fallstudien und Präsentationen.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Präsentation und Projektbericht oder Portfolioprüfung als Teamleistung[1] Es sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165

10	**Literaturhinweise** Bea, F.X., Haas, J.: Strategisches Management, Stuttgart, Konstanz, UVK Bleicher, K., Abegglen, C.: Das Konzept Integriertes Management, Frankfurt, New York, Campus Hungenberg, H,: Strategisches Management im Unternehmen, Berlin, Heidelberg, Springer Gabler. Kühn, R.; Grünig, R: Methodik der strategischen Planung, Bern et al., Haupt Lombriser, R., Aplanalp, P. A.: Strategisches Management, Zürich, Versus Müller-Stewens, G., Lechner, C.: Strategisches Management, Stuttgart, Schäffer-Poeschel Paul, H.; Wollny, V. Instrumente des strategischen Managements, München, Oldenbourg Lynch, R.: Strategic Management, Harlow, UK et al., Pearson Johnson, G., Scholes, K., Whittington, R.: Exploring Corporate Strategy, Harlow, UK et al., Pearson Wheelen, T., Hunger, J., Hoffmann, A.N., Bamford, C.E.: Strategic Management and Business Policy, Up-per Saddle River, NJ et al., Pearson Jeweils in der neusten Auflage.
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

IT-Sicherheitsrecht				
Kennnnummer	**ECTS-Leistungs-punkte** 5	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 5	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 150[1] / 125[2]		**Kontaktzeit (h)** 60		**Selbststudium (h)** 90[1] / 65[2]
Sprache Deutsch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Bianca Baldus		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** IT-Sicherheitsrecht		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • den grundlegenden rechtlichen Rahmen zu IT-Sicherheitspflichten zu erläutern (IT-Compliance) und sich daraus ergebende Verpflichtungen für Unternehmen zu identifizieren • entsprechende Umsetzungsvorschläge zu entwickeln und daraus resultierende Umsetzungsmaßnahmen auch aus rechtlicher Sicht im Unternehmen zu bewerten und zu begleiten • Haftungsrisiken im Zusammenhang mit IT-Sicherheitsdefiziten zu erkennen und zu bewerten • branchenspezifische Rechtspflichten zur Erreichung der IT-Compliance zu berücksichtigen • unter Berücksichtigung rechtlicher und ggf. branchenspezifischer Vorgaben ein IT-Sicherheitskonzept zu entwickeln

2	**Inhalte** 1. IT-Sicherheit in der Unternehmensorganisation • Bedeutung für Unternehmen • IT-Sicherheitspflichten der Geschäftsleitung • Pflichten bei der elektronischen Buchführung • Schutz von Geschäftsgeheimnissen (GeschGehG) • Rechtslage im Konzern und Einbeziehung des Betriebsrats 2. IT-Sicherheit als vertragliche Pflicht • IT-Sicherheit als Haupt- und Nebenpflicht • Sichere „IT-Produkte“ 3. Datenschutz und IT-Sicherheit • Datenschutzrechtliche IT-Sicherheitsvorgaben • Folgen der Verletzung von Datenschutzverstößen 4. Branchenspezifische Regelungen • IT-Sicherheitspflichten nach dem BSI-Gesetz • IT-Sicherheitspflichten in ausgewählten Branchen (z.B. Telemedien, Telekommunikation, Gesundheitswesen, Energieversorgung, Versicherungs-, Finanz- und Bankwesen) 5. Haftung für IT-Sicherheit • Haftung der Geschäftsleitung • Haftung des Unternehmens gegenüber Dritten (Vertragliche Haftung, Deliktische Haftung, Ordnungswidrigkeiten und Strafrecht) 6. Aufbau eines IT-Sicherheitskonzepts • Der/Die IT-Sicherheitsbeauftragte(r) • Entwicklung eines IT-Sicherheitsmanagemensystems • IT-Betriebsrichtlinien • Notfallkonzepte
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 20–30 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Klausur (90 Min.) **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /

7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 5/165
10	**Literaturhinweise** Voigt, IT-Sicherheitsrecht, Verlag Otto Schmidt KG Hornung/Schallbruch, IT-Sicherheitsrecht, Nomos Kipker, Cybersecurity, C.H. Beck (zur Vertiefung) jeweils aktuelle Auflage Datenbanken/Gesetzestexte Beck-Online, beck-eBibliothek, Juris, IT- und Computerrecht: CompR, C.H. Beck Datenschutzrecht: DatSchR, C.H. Beck jeweils neueste Auflage
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Semester 6

Aktuelle Themen der IT-Sicherheit				
Kennnnummer	**ECTS-Leistungs-punkte** 3	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 6	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 90¹ / 65²		**Kontaktzeit (h)** 45		**Selbststudium (h)** 45¹ / 20²
Sprache Deutsch/Englisch		**Geplante Gruppengröße** 40 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Dirk Loomans		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Aktuelle Themen der IT-Sicherheit		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • sich selbständig mit einer komplexen Problemstellung, der dazugehörigen Forschungsmethodik und Literatur auseinanderzusetzen, d.h. ein Problem im Rahmen ihrer Bachelorarbeit zu identifizieren, zu entwickeln und zu beschreiben. • eine Forschungsmethodik zur Bearbeitung der Problemstellung festzulegen und zu beschreiben • die geplante Bachelorarbeit zeitlich und inhaltlich zu strukturieren und den Status quo der Forschung abzuleiten • ihr geplantes Vorhaben zu strukturieren, zu präsentieren und damit in Verbindung stehende Fragen adäquat zu beantworten
2	**Inhalte** Ein Problem und eine Forschungsfrage zu identifizieren, die es wert sind, in der Bachelorarbeit analysiert und diskutiert zu werden. Die Fragestellungen beziehen sich in der Regel auf reale Probleme eines Unternehmens im Bereich der Cyber Resilienz (Capstone Projekt). Strukturierung, Darstellung und Kommunikation der Problemstellung und der entsprechenden Ergebnisse
3	**Lehrformen** Die Lehrveranstaltung findet im seminaristischen Stil statt. Der Übungsanteil beträgt ca. 20–30 %.
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /

6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form von Assignments (60%) und Präsentation (40%)[1] Bei Assignments und Präsentation sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 3/165
10	**Literaturhinweise** Theisen; Wissenschaftliches Arbeiten; Vahlen Jeweils aktuelle Auflage. Leitfaden zur Anfertigung von Hausarbeiten, Praxisberichten und Bachelor-Arbeit
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Praxismodul				
Kennnnummer	**ECTS-Leistungs-punkte** 15	**Dauer des Moduls** 1 Semester	**Vorgesehenes Studiensemester** Semester 6	**Häufigkeit des Angebots** jährlich
Arbeitsaufwand (gesamt) (h) 450[1] / 375[2]		**Kontaktzeit (h)** 10		**Selbststudium (h)** 440[1] / 365[2]
Sprache Deutsch		**Geplante Gruppengröße** 10 Studierende		**Verbindlichkeit** Pflichtmodul
Modulverantwortliche/r Prof. Dr. Anett Mehler-Bicher		**Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)** Praxismodul		

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • ein Praxisprojekt aus dem Bereich Cyber Security eigenständig zu planen, durchzuführen und abzuschließen • die in den Lehrveranstaltungen gelernten Inhalte in der Praxis bzw. in Form von Projekten an der Hochschule anzuwenden • ihre Kenntnisse aus dem Projektmanagement einzusetzen. • Fragestellungen aus einem Unternehmensumfeld oder hochschulinternen Themen zu analysieren und zu bearbeiten • Interdisziplinäres Wissen aus verschiedenen Bereichen der Cyber Security in die Praxis bzw. in Form des Projekts an der Hochschule zu integrieren
2	**Inhalte** Projekte zu Fragestellungen aus dem Themenspektrum der Cyber Security
3	**Lehrformen** Coaching/Individuelle Betreuung der Studierenden in Kleingruppen
4	**Teilnahmevoraussetzungen** /
5	**Regelungen zur Präsenz** /

6	**Prüfungsart und -umfang** Projektbericht (einschließlich Präsentation)1 Beim Projektbericht sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /
7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 0/165
10	**Literaturhinweise** Leitfaden zur Anfertigung von Hausarbeiten, Praxisberichten und Bachelor-Arbeit
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025

Bachelorarbeit

Kennnnummer	ECTS-Leistungs-punkte	Dauer des Moduls	Vorgesehenes Studiensemester	Häufigkeit des Angebots
	12	1 Semester	Semester 6	jährlich

Arbeitsaufwand (gesamt) (h)	Kontaktzeit (h)	Selbststudium (h)
360[1] / 300[2]	30	330[1] / 270[2]

Sprache	Geplante Gruppengröße	Verbindlichkeit
Deutsch	10 Studierende	Pflichtmodul

Modulverantwortliche/r	Lehrveranstaltung(en) (ggf. mit Schwerpunkt/Modulgruppe)
Prof. Dr. Nicolai Kuntze	Bachelorarbeit

1	**Qualifikationsziele/Kompetenzen/Lernergebnisse** Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage: • ein studienspezifisches Problem aus dem Themenfeld Cyber Security Management (in der Regel Capstone-Projekt) eigenständig zu planen, durchzuführen und zu lösen • bisher gewonnene Erfahrungen und Kompetenzen anzuwenden, um eigenständig eine erste wissenschaftlichen Arbeit anzufertigen • sowohl reale Probleme eines Unternehmens Themenfeld Cyber Security Management als auch theoretische Fragestellungen zu entwickeln und zu bearbeiten • ihre Forschungsfrage und -ergebnisse adäquat zu strukturieren, zu präsentieren und zu verteidigen
2	**Inhalte** Projekte zu Fragestellungen aus dem Themenspektrum der Cyber Security
3	**Lehrformen** Coaching/Individuelle Betreuung der Studierenden
4	**Teilnahmevoraussetzungen** **/**
5	**Regelungen zur Präsenz** /
6	**Prüfungsart und -umfang** Schriftliche Prüfung in Form einer Bachelorarbeit mit Präsentation/Kolloquium[1] Es sollten Themen aus dem unternehmerischen Umfeld mit einer für das Unternehmen relevanten Themenstellung ermöglicht werden.[2] **Studienleistungen als Voraussetzung für Teilnahme an der Prüfung** /

7	**Voraussetzungen für die Vergabe von Leistungspunkten (ECTS)** Bestandene Modulprüfung
8	**Verwendbarkeit des Moduls (in anderen Studiengängen)** /
9	**Stellenwert der Note für die Endnote** 12/165
10	**Literaturhinweise** Theisen; Wissenschaftliches Arbeiten; Vahlen Jeweils aktuelle Auflage. Leitfaden zur Anfertigung von Hausarbeiten, Praxisberichten und Bachelor-Arbeit
11	**Sonstige Informationen** /
12	**Zuletzt bearbeitet** 11.09.2025