Kernmodul-Katalog

Fakultät Informatik

gültig für die Bachelorstudiengänge
Technische Informatik B.Eng. einschließlich Technische Informatik B.Eng. berufsbegleitend, Wirtschaftsinformatik B.Sc. und IT Security B.Sc.

ab Sommersemester 2023
Bitte beachten Sie immer vorrangig die für Sie gültige StuPO!
Ersteller: Prof. Dr. Christian Henrich, Studiendekan
Verantwortlich: Prof. Dr. Christian Henrich, Studiendekan

Inhalt

⇨ ***Bitte beachten: Dieser Kernmodul-Katalog enthält vollständig alle Module, welche angeboten werden können. Nicht alle Module in diesem Katalog werden jedes Semester angeboten. Außerdem ist es möglich, dass ein Modul aufgrund geringer Anmeldezahlen nicht stattfindet. Bitte informieren Sie sich rechtzeitig darüber, ob ein bestimmtes Modul in Ihrem Semester stattfindet (Semesteraushang auf ILIAS).***

1 Qualifikationsziel-Modul-Matrix

Cyber-Physical-Systems and Security	**IT-Management**	**Application Development**	**Applied IT-Security**	**Cyber-Psychologie**
CPS-1 Entwicklung von Hardware/Software-Systemen *..sind in der Lage, die Planung, den Entwurf, die Implementierung und den Betrieb von Hardware/Software-Systemen wirkungsvoll zu unterstützen.*	ITM-1 Strategische Ausrichtung von IT-Organisationen und IT-Unternehmen *..können Ausrichtung von IT-Abteilungen / IT-Bereichen in Unternehmen analysieren und beschreiben sowie Methoden zur Entwicklung und Umsetzung von IT-Strategien anwenden und beurteilen.*	AD-1 Prozessmodelle *..kennen gängige Prozessmodelle in der Softwareentwicklung und können formale Vorgehensmodelle und andere Regelwerke (z.B. Style-Guides) im Softwareentwicklungs-prozess adäquat an die gegebene Situation anpassen und anwenden.*	AITS-1 Sicherung digitaler Spuren *..sind in der Lage, digitale Spuren mithilfe forensischer Methoden und Techniken zu sichern und zu analysieren.*	CYP-1 Social Engineering *..sind in der Lage, auf menschliches Verhalten zielende Angriffsvektoren in Cyber-Berohungslagen zu erkennen, deren Wirkungsweise nachzuvollziehen und Gegen-maßnahmen einzusetzen.*
CPS-2 Informationstechnologie in technischen Anwendungsgebieten *.. sind in der Lage, den in den technischen Anwendungsbereichen der Informatik stattfindenden und sich kontinuierlich verstärkenden Einzug von Informationstechnologie wirkungsvoll zu unterstützen und aktuelle Trendthemen der IT (z.B. „Internet der Dinge", „Industrie 4.0", „Elektromobilität", „Energiewende") in die praktische Anwendung zu überführen.*	ITM-2 Methoden der IT-Organisation *..wenden unterschiedliche Methoden des IT-Prozessmanagements an.* *..verfügen über Kenntnisse zu komplexen IT-Projekten und können geeignete Methoden (PRINCE2 u.a.) anwenden.* *..können die strategischen und rechtlichen Herausforderungen von IT-Führungskräften (IT-Governance, Risk and Compliance Management aus Sicht des CIO und des untergeordneten IT-Managem.) erklären.*	AD-2 Software Design Patterns *..können geeignete Patterns in den verschiedenen Phasen der Softwareentwicklung erkennen und umsetzen.*	AITS-2 Schwachstellenprüfung *.. sind in der Lage, offensive Sicherheitsmethoden im rechtlichen und moralischen Rahmen einzusetzen, um Sicherheitslücken in der Unternehmensinfrastruktur und -organisation zu identifizieren.*	CYP-2 Cyber Security Cultures / Awareness *..sind in der Lage, die Vulnerabilität gegenüber Bedrohungen der IT-Sicherheit auf Organisationsniveau zu verstehen, das Bewusstsein für IT-Sicherheitsrisiken auf User-Ebene einer Organisation systematisch zu erfassen und Maßnahmen zur Förderung zu konzipieren.*
CPS-3 Hardware-nahe Security *..sind in der Lage, Problemstellungen der hardware-nahen IT-Security bei der Hardware- und Softwareentwicklung zu berücksichtigen und dabei sowohl Sicherheitsprobleme zu erkennen, als auch geeignete Gegenmaßnahmen umzusetzen.*	ITM-3 Management von Anwendungssystemen *..können Motivation, Methodiken und Tools für das IT-Architekturmanagement analysieren und anwenden sowie Vorgehensweisen im Hard-Softwaremanagement (ITIL, Netzwerkmanagement, Client Management u.a.) beschreiben und planen.*	AD-3 Human Computer Interaction *...können User-Experience und Usability von Anwendungen nach ergonomischen Regelwerken wie z.B. ISO 9241 beurteilen. Sie können Anwendungen mit angemessener Usability und aktuellen Interaktions- und Navigationsformen unter Verwendung aktueller Design-Style-Guides und Frameworks entwickeln.*	AITS-3 Erstellung von Sicherheitskonzepten *..sind in der Lage, die Sicherheitsrisiken in Unternehmen zu analysieren und darauf aufbauend Sicherheitskonzepte herzuleiten und umzusetzen.*	CYP-3 Ethik *..verstehen die Relevanz ethischer Abwägungen und sind in der Lage, in diesem Anwendungsbereich typische ethische Herausforderungen zu erkennen und mit ihrem Wissen zur (Weiter-)Entwicklung berufsethischer Standards beizutragen.*

Kernmodule können einen unwesentlichen (0), wesentlichen (1) oder besonderen Beitrag (2) zur Vermittlung der Qualifikationsziele beitragen.
Ein Kernmodul ist einem Schwerpunkt zuzuordnen, wenn über alle Qualifikationsziele des Studiengangs hinweg ein Mindestscore von 3 erreicht wird.

		CPS			ITM			AD			AITS			CYP			
	Qualifikationsziel (QuZ)	Entwicklung v. Hard-/Softwaresystemen	Informationstechnologie in techn. Anwendungsgebieten	Hardwarenahe Security	Strategische Ausrichtung von IT-Organisationen und IT-Unternehmen	Methoden der IT-Organisation	Management v. Anwendungssystemen	Prozessmodelle	Software Design Patterns	Human Computer Interaction	Sicherung digitaler Spuren	Schwachstellenprüfung	Erstellung von Sicherheitskonzepten	Social Engineering	Cyber Security Cultures / Awareness	Ethik	Zuordnung zum Schwerpunkt
22500	Reverse Engineering	2	1	2	0	0	0	1	1	1	2	2	1	1	1	1	CPS/ AD/ AITS/ CYP
23100	Unternehmenskonzepte / Digitale Fabrik	1	2	0	0	0	0	1	0	2	0	0	0	0	0	0	CPS/ AD
23200	Verteilte Systeme (Technik)	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	CPS
23600	Advanced Database Technology	1	0	0	0	0	2	1	2	0	0	0	1	0	0	0	AD
23700	GUI Development	2	0	0	0	0	2	1	2	2	0	0	0	0	1	1	AD
23800	Softwarearchitektur	2	0	0	0	1	1	1	2	0	0	1	0	0	0	0	AD
24000	IT-Management	0	0	0	2	1	2	0	0	0	0	0	0	0	0	0	ITM
24100	IT Consulting	0	0	0	2	2	1	1	0	0	0	0	0	0	0	0	ITM
24400	Offensive Sicherheitsmethoden	0	0	1	0	1	0	0	0	0	1	2	1	1	1	1	AITS/ CYP
30200	Simulationstechnik	1	2	0	0	0	2	0	0	0	0	0	0	0	0	0	CPS
32100	Mobile Systeme und Cloud	2	1	0	0	0	0	1	1	1	0	0	0	0	0	0	CPS/ AD
32300	IT-GRC	0	0	0	2	1	1	0	0	0	0	0	0	0	0	0	ITM
32400	IT-Sicherheits-management	0	0	0	1	1	1	0	1	2	0	0	0	0	0	0	ITM/ AD
32500	Mobile und Cloud Forensik	0	0	0	0	0	0	0	0	0	2	2	0	2	1	2	AITS/ CYP
xxxxx	Cybersecurity Awareness and Behavior	0	0	0	1	1	0	0	1	2	1	1	2	2	2	2	AD/ AITS/ CYP

		CPS			ITM			AD			AITS			CYP			
	Qualifikationsziel (QuZ)	Entwicklung v. Hard-/Softwaresystemen	Informationstechnologie in techn. Anwendungsgebieten	Hardwarenahe Security	Strategische Ausrichtung von IT-Organisationen und IT-Unternehmen	Methoden der IT-Organisation	Management v. Anwendungssystemen	Prozessmodelle	Software Design Patterns	Human Computer Interaction	Sicherung digitaler Spuren	Schwachstellenprüfung	Erstellung von Sicherheitskonzepten	Social Engineering	Cyber Security Cultures / Awareness	Ethik	Zuordnung zum Schwerpunkt
xxxxx	Digitaler Schaltungsentwurf	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	CPS
Xxxxx	Hardware-orientierte IT-Sicherheit	2	1	2	0	0	0	0	0	0	1	1	1	0	1	1	CPS/ AITS
Xxxxx	Hardware Sicherheitsmethoden	2	1	2	0	0	0	0	0	0	1	2	1	0	1	1	CPS/ AITS
Xxxxx	SAP Application Design	2	1	0	0	0	0	1	1	1	0	0	0	0	0	0	CPS/ AD
Xxxxx	Sichere Digitale Schaltkreise	2	0	2	0	0	0	0	0	0	0	0	2	0	1	0	CPS
Xxxxx	Social Engineering	1	1	0	0	1	0	0	1	2	1	1	2	2	2	2	AD/ AITS/ CYP

2 Studiengangs-Kompetenzmatrix

	Kompetenzen	Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozial-kompetenz			Selbständig-keit		
	Ausprägung	Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/ Führungs-fähigkeit	Mitge-staltung	Kommuni-kation	Eigenständigkeit / Verantwortung	Reflexivität	Lern-kompetenz
22500	Reverse Engineering	6		6					6	6		
23100	Unternehmenskonzepte / Digitale Fabrik	6	6	6			6	6	6	6		
23200	Verteilte Systeme (Technik)	6	6	6					6	6		
23600	Advanced Database Technology	6		6	6							
23700	GUI Development	6	6	6	6	6			6	6		6
23800	Softwarearchitektur	6		6						6		
24000	IT-Management	6	6	6	6		6		6	6		
24100	IT Consulting	6	6	6	6		6		6	6		
24400	Offensive Sicherheitsmethoden	6	6	6	6	6			6		6	
32000	Simulationstechnik	6			6					6		
32100	Mobile Systeme und Cloud	6	6	6	6	6			6	6		6
32300	IT-GRC	6	6	6			6			6	6	
32400	IT-Sicherheitsmanagement	6	6	6		6			6		6	
32500	Mobile und Cloud Forensik	6	6	6	6	6			6	6		6
xxxxx	Cybersecurity Awareness and Behavior	6	6			6			6	6		
xxxxx	Digitaler Schaltungsentwurf	6	6	6					6	6		
xxxxx	Hardware Sicherheitsmethoden	6	6	6	6			6		6		
xxxxx	Hardware-orientierte IT-Sicherheit	6	6			6			6	6		
xxxxx	SAP Application Design	6	6	6	6				6	6	6	
xxxxx	Sichere Digitale Schaltkreise	6	6		6				6			6
xxxxx	Social Engineering	6	6			6			6	6		

3 Modulbeschreibungen

3.1 22500 – Reverse Engineering

Modul: Reverse Engineering						
Kennnummer 22500	**Workload** 75	**Modulart** P	**Studiensemester** 4. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Reverse Engineering	**Sprache** Deutsch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5	
2	**Lehrform(en) / SWS:** Vorlesung und Übungen: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die für das Reverse Engineering wichtigen Merkmale der prozessorarchitektur und der Assemblersprache. *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, ausführbare Programme mittels der Verhaltensanalyse, der statichscen und der dynamischen Codeanalyse zu analysieren. *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz* Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen *[Kommunikation, 6]* *Selbstständigkeit* Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen *[Eigenständigkeit/Verantwortung, 6]*					
4	**Inhalte***:* • Grundlagen der Analyse von Schadsoftware • Prozessorarchitekturen: x86, x64 • Assemblersprache • Compiler-Konstrukte auf Assembler-Ebene • Disassemblierung und Debugging von Code auf Assemblerebene • Analysemethoden und Werkzeuge • Windows Grundlagen: Speicherbild von Prozessen, Formate von ausführbaren Programmen. Laden und Ausführen von Programmen • Programmiertechniken von Malware: Code-Verschleierung, Emulation, Erkennung von Virtualisierung oder Debuggern • Statische und dynamische Analyse von Schadsoftware für die Windows-Plattform • Schutzmechanismen von audführbaren Programmen und deren Überwindung • Verhaltensanlyse von ausführbaren Programmen • Reverse Engineering von Python-basierter Malware					

	Empfohlene Literaturangaben: Eldad Eilam: Reversing: Secrets of Reverse Engineering, John Wiley & Sons, 2005 Michael Sikorski, Andrew Honig: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012 Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sebastien Josse: Practical Reverse Engineering, John Wiley & Sons, 2014
5	**Teilnahmevoraussetzungen:** Kenntnisse in einer Programmiersprache und in Rechnertechnik
6	**Prüfungsformen***:* Klausur 60 min, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Martin Rieger Dozent(in): Prof. Dr. Martin Rieger
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.2 23100 – Unternehmenskonzepte / Digitale Fabrik

<table>
<tr><td colspan="7">Modul: Unternehmenskonzepte / Digitale Fabrik</td></tr>
<tr><td colspan="2">Kennnummer
23100</td><td>Work-load
150</td><td>Modulart
P</td><td>Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Unternehmenskonzepte / Digitale Fabrik</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Unternehmenskonzepte / Digitale Fabrik:
Vorlesung, Umfang: 15x4 = 60 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Entwicklung eines Konzepts und Systems aus dem Bereich Industrie 4.0 über Fachbereichsgrenzen hinweg. [Wissen, 6]

Kompetenz Fertigkeiten
Der Studierende programmiert Schnittstellen für ein ERP, um Informationen daraus weiterzuverarbeiten. Es werden Protokolle angewendet (MQTT, OPCUA), um Informationen aus dem ERP weiter zu verteilen [Instrumentelle Fertigkeiten, 6]

Sozialkompetenz
Teams bekommen Aufgabenstellung, die während des Semesters bearbeitet werden. [Team-/Führungsfähigkeit, 6]

Jedes Teammitglied bekommt innerhalb des Teams eine Aufgabe gestellt, welcher im Laufe des Semesters in ein Produkt integriert wird. [Mitgestaltung, 6]

Jede Woche findet ein Meeting statt, bei dem der Status kommuniziert wird und die weiteren Schritte geplant werden. [Kommunikation, 6]

Selbstständigkeit
Teams organisieren sich selbst, und erstellen eigenständig Projektpläne. [Eigenständigkeit/Verantwortung, 6]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Steuerung der digitalen Fabrik
Komponenten der digitalen Fabrik, u.a. Steuerungen für Maschinen und Anlagen, Sensoren und Aktoren, Netzwerke und Busse, Informations- und Kommunikationssysteme, Mensch-Maschine Schnittstellen, Autoidentifikation.

Unternehmenskonzepte
Methoden um Planungsprozesse zu beschleunigen und Kosten zu senken,
Vermeidung von Planungsfehlern und Prozesssicherung durch geeignete Simulationsverfahren,
Beherrschung komplexer Produkt- und Prozessstrukturen,
Standardisierung von Methoden und Prozessen,
Schnittstellen zwischen virtuellen Modelle und realen Prozessen Interaktion,
Kommunikation und Datenaustausch zwischen den Produktionskomponenten und</td></tr>
</table>

	Produkten, Anpassung der Betriebsorganisation an die Erfordernisse der digitalen Fabrik, lernende und selbstoptimierende Organisation, *Empfohlene Literaturangaben:* VDI-Richtlinie 4499, Blatt 1: Digitale Fabrik – Grundlagen, VDI-Gesellschaft Fördertechnik Materialfluss Logistik, 2008, Schack, R.: Methodik zur bewertungsorientierten Skalierung der Digitalen Fabrik, Kühn, W.: Fabriksimulation für Produktionsplaner, Bullinger, H.-J.: Einführung in das Technologiemanagement, B.G. Teubner Verlag, Stuttgart. Kühn, W.: Fabriksimulation für Produktionsplaner, Bullinger, H.-J.: Einführung in das Technologiemanagement, B.G. Teubner Verlag, Stuttgart.
5	**Teilnahmevoraussetzungen:** Keine. Hilfreich sind jedoch Grundkenntnisse der Betriebsabläufe
6	**Prüfungsformen***:* Unternehmenskonzepte / Digitale Fabrik: Referat 15 min., Mündliche Prüfung 20 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Der Studierende soll in der Lage sein, ein technisches Projekt aus dem Bereich Industrie 4.0 zu planen und zu bearbeiten. Teil des Projekts soll der Zugriff von Informationen aus ERP enthalten. Ein weiterer Teil soll die Verarbeitung der Informationen und die Steuerung eines industriellen Prozesses enthalten.
8	***Verwendbarkeit des Moduls:*** PM in B.Eng. Technische Informatik (CPS) PM in B.Eng. IT-Security (CPS) PM in B.Eng. Wirtschaftsinformatik (CPS) Wahlrichtung: Cyber-Physical Systems
9	***Modulverantwortliche(r):*** Prof. Dr. Derk Rembold, Bernd Stauss Dozenten: Prof. Dr. Derk Rembold, Prof. Dr. Bernd Stauss
10	***Optionale Informationen:*** Dieses Fach ist insbesondere für Studierende der Wirtschaftsinformatik interessant, da es hier um den Einsatz von ERP geht und es viele Informationen aus ERP Systeme zu verarbeiten gilt.
11	***Bearbeitungsstand:*** 23.01.2023

3.3 23200 – Verteilte Systeme (Technik)

<table>
<tr><td colspan="7">Modul: Verteilte Systeme (Technik)</td></tr>
<tr><td colspan="2">Kennnummer
23200</td><td>Work-load
150 h</td><td>Modulart
P</td><td>Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Verteilte Systeme (Technik)
Praktikum Verteilte Systeme (Technik)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Unternehmenskonzepte / Digitale Fabrik:
Vorlesung, Umfang: 15x4 = 60 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Dem Studierenden sind Systeme und Methoden zur Verteilung von Informationen über Rechnergrenzen hinweg bekannt. [Wissen, 6]
Kompetenz Fertigkeiten
Der Studierende kann verschiedene Kommunikationssysteme anwenden und beispielhaft an verteilten Rechnersystemen austesten.
[Instrumentelle Fertigkeiten, 6]
Sozialkompetenz
Der Studierende ist in der Lage technische Probleme bei der Umsetzung zu kommunizieren und Hilfestellungen zu erfragen. [Kommunikation, 6]
Selbstständigkeit
Aufgaben werden vergeben und diese werden bis Semesterende bearbeitet. [Eigenständigkeit/Verantwortung, 6]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung & Übungen
Clouddienste: SaaS, PaaS, IaaS
Verteilte Software: REST, SOAP, OPCUA, MQTT etc.
Softwareorchestrierung: Docker
Dienste: Namensdienst, Transaktionsdienst, Zeitdienst und Sicherheitsdienst
Softwaremuster für verteilte Systeme: Einsatz, Struktur, Verhalten, Entwurf, Konstruktion, Varianten der Muster Client-Dispatcher-Server, Forward-Receiver, Proxy, Observer, Layers, Broker, Model-View-Controller.
Vernetzte Systeme in Fahrzeugen:
CAN: Protokoll, Kommunikationsmatrix
LIN: Protokoll, Architektur, Botschaften, Schedule
FlexRay: Protokoll, Architektur

Praktikum
Realisierung eines REST Servers
Realisierung einer MQTT Applikation
Einsatz von Docker beim REST Server und MQTT Applikation</td></tr>
</table>

	Empfohlene Literaturangaben: Buschmann, F. u.a.: Pattern - Oriented Software Architecture: A System of Patterns; Zimmermann, W.; Schmidgall, R.: Bussysteme in der Fahrzeugtechnik, Protokolle und Standards, 2. Vieweg. Reißenweber, B.: Feldbussysteme zur industriellen Kommunikation, Oldenbourg Industrieverlag München.
5	**Teilnahmevoraussetzungen:** Programmierkenntnisse in Python oder C++.
6	**Prüfungsformen***:* Verteilte Systeme (Technik): Klausur 90 min., benotet Prakt. Verteilte Systeme (Technik): Laborarbeit unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Der Studierende muss in der Lage sein, verteilte Software Produkte und ihre Einsatzgebiete zu benennen. Er soll Softwaremuster kennen, und verteilte Software selbst programmieren. Busprotokolle, eingesetzt in Fahrzeugen, müssen benannt und erklärt werden können.
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: Cyber-Physical Systems
9	***Modulverantwortliche(r):*** Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Derk Rembold
10	***Optionale Informationen:*** keine
11	***Bearbeitungsstand:*** 23.01.2023

3.4 23600 – Advanced Database Technology

<table>
<tr><td colspan="8">Modul: Advanced Database Technology</td></tr>
<tr><td colspan="2">Kennnummer
23600</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung & Übungen Datenbanken 2</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung & Übungen: 4 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen
die Implementierungstechniken zur Formulierung hoch komplexer Anfragen auf Basis eines objekt-relationalen Datenbanksystems in SQL, die wichtigsten Verfahrensweise des „ETL“ (Extract, Transform, Load),die Rolle der Dimension „Zeit“ im Hinblick auf die langfristige Speicherung in einem Data-Warehouse, den Separationsprozess von Daten des operativen Geschäfts gegenüber den (verdichteten) Daten von Data Warehouse-Anfragen, die „Themenorientierung“ im Hinblick auf die Auswertung komplexer Auswertungen sowie deren Abgrenzung zur Prozessorientiertheit operativer Aufgaben [Wissen, 6]
Kompetenz Fertigkeiten
Fertigkeiten
Die Studierenden sind in der Lage
ein Datenmodell für Datawarehouse-Anwendungen zu konzipieren,
komplexe Datenbankanfragen auf Basis des (objekt-) relationalen Datenmodells zur Entscheidungs-unterstützung in Bereichen des Controlling oder der Strategischen Unternehmensführung zu formulieren,
mehrdimensionale Wissensbasen im Sinne einer OLAP -Architektur aufzubauen,
einfache und komplexe Zusammenhänge zu Unternehmensdaten im Sinne eines Business Analytics zu bewerten
[Instrumentelle Fertigkeiten, 6]

Die Studierenden sind fähig Zusammenhänge zwischen nicht antizipierten Daten durch Data Mining-Techniken zu erkennen, Analysen über zeitliche Veränderungen und Entwicklungen in einem Data-Warehouse anzustellen, Data Marts als anwendungsspezifische Data Warehouse-Bereiche aufzubauen, den Integrationsprozess für große, unterschiedlich strukturierte und verteilte Datenbasen hin zu einer vereinheitlichten Datenbasis für komplexe, mehrdimensionale Auswertungen vorzunehmen geeignete Patterns in den verschiedenen Phasen der Software-entwicklung zu erkennen und umzusetzen [Systemische Fertigkeiten, 6]
Sozialkompetenz
Nicht relevant
/Kompetenzausprägung wählen: nicht relevant
Selbstständigkeit
Die Studierenden sind fähig Zusammenhänge zwischen nicht antizipierten Daten durch Data Mining-Techniken zu erkennen, Analysen über zeitliche Veränderungen und</td></tr>
</table>

	Entwicklungen in einem Data-Warehouse anzustellen, Data Marts als anwendungsspezifische Data Warehouse-Bereiche aufzubauen, den Integrationsprozess für große, unterschiedlich strukturierte und verteilte Datenbasen hin zu einer vereinheitlichten Datenbasis für komplexe, mehrdimensionale Auswertungen vorzunehmen geeignete Patterns in den verschiedenen Phasen der Softwareentwicklung zu erkennen und umzusetzen *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte***:* Bewertung operativer und analytischer Datenbanken Konzeption von Datenmodellen für Data Warehouses Anwendung von Optimierungstechniken für sehr große Datenbanken Anwendung multidimensionaler Auswertungen Implementierung verteilter Transaktionen auf Basis eines TP-Monitor-basierenden Applikationsservers Aufbau und Arbeitsweise von In-memory-Datenbanken am Beispiel SAP/HANA bzw. Oracle 18g
	Empfohlene Literaturangaben: https://docs.oracle.com/cd/B28359_01/server.111/b28310/ds_txns001.htm#ADMIN12211 https://docs.oracle.com/cd/B19306_01/server.102/b14231/ds_txns.htm Farkisch, Kiumars: Data-Warehouse-Systeme kompakt, Xpers.press, 2011 Bauer, A.; Günzel, H.: Data-Warehouse-Systeme: Architektur, Entwicklung, Anwendung, dpunkt, 2008 Holten, R.: Entwicklung einer Modellierungstechnik für Data Warehouse -Fachkonzepte, Proc. MobIS Fachtagung, Münster, 2000 Kempfer, H.-G.; Mehanna, W., Unger, C.: Business Intelligence – Grundlagen und praktische Anwendungen, Vieweg, 2. Auflage, 2006 https://2bm.com/sap-s-4hana-always-on-business-functions/ Müller, R.M, Lenz, H.-J.: Business Analytics, Springer Vieweg 2013 Kaiser, C.: Business Intelligence 2.0, Springer Gabler, 2012 Kemper, H.-G., Baars, H., Mehanna, W.: Business Intelligence -Grundlagen und praktische Anwendungen, 3. Ausgabe, Springer Vieweg 2010Klein, A., Gräf, J.: Reporting und Business Intelligence, Haufe 2014 http://www.oracle.com/technetwork/database/features/storage/database-11gr2-managing-storage-whi-131523.pdf
5	**Teilnahmevoraussetzungen:** Zulassung zu einem der Informatik-Studiengänge BSc. an der HS Albstadt Sigmaringen Profunde Kenntnisse auf in vorbereitenden Veranstaltungen des Grundstudiums der Studiengänge Wirtschaftsinformatik/IT-Security bzw. Technische Informatik, beispielsweise 12000 Programmierung 1,14500 Programmierung 2, 15000 Betriebssysteme und Netzwerke 1, 21000 Datenbanken 1
6	**Prüfungsformen***:* Mündliche Prüfung, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der mündlichen Prüfung

8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: Application Development
9	***Modulverantwortliche(r):*** Prof. Dr. J. Röhrle Dozent: Prof. Dr. J. Röhrle
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.5 23700 – GUI-Development (Graphical User Interface-Development)

<table>
<tr><td colspan="7">Modul: GUI-Development (Graphical User Interface-Development)</td></tr>
<tr><td colspan="2">Kennnummer
23700</td><td>Work-load
150 h</td><td>Modulart
P</td><td>Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Übungen GUI-Development
Praktikum GUI-Development</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Übungen: 3 SWS
Praktikum: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen die unterschiedlichen Entwurfs-paradigmen für Desktop-, Web- und Mobile GUIs (ergonomische Sicht). Sie kennen die verschiedenen MVC-Architekturen für Desktop- und mobile Applikationen, sowie Event-Verarbeitungsmechanismen. Sie kennen Aufbau und Funktionsweise typischer Widgets für Desktop-Anwendungen, sowie für für mobile Anwendungen (beispielsweise Android) [Wissen, 6]
Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, eigenständig komplexere Workflows in Form von Desktop-GUIs und in Form mobiler GUIs auf Basis von gegebenen Nutzer-Anforderungen zu entwickeln.

Sie können gängige Prozessmodelle in der Softwareentwicklung für die GUI-Entwicklung anwenden und andere Regelwerke (z. B. StyleGuides) im Software-entwicklungsprozess adäquat an die gegebene Situation anpassen und anwenden

Sie können geeignete Patterns in den verschiedenen Phasen der Software-entwicklung erkennen und umsetzen
[Instrumentelle Fertigkeiten, 6]
Die Studierenden sind in der Lage, auch für sie neue Problemstellungen in Workflows abzubilden und als Desktop-GUI oder mobile GUI umzusetzen. [Systemische Fertigkeiten, 6]
Die Studierenden können softwaretechnische Lösungen im Umfeld der GUI-Entwicklung architektonisch und codetechnisch beurteilen und einordnen. [Beurteilungsfähigkeit, 6]
Sozialkompetenz
Die Studierenden können in Absprache mit Kunden GUIs mit ansprechender Usability und UX für bestimmte Zielgruppen umsetzen. [Kommunikation, 6]</td></tr>
</table>

	Selbstständigkeit Die Studierenden sind in der Lage, sich im sehr schnelllebigen Umfeld der GUI-Entwicklung selbstständig auf neue Technologien und Frameworks einzustellen und sich diese rasch und selbstständig anzueignen. [Reflexivität, 6] Sie sind in der Lage, sich auch weitere Frameworks im GUI-Umfeld, sowie weitere Widget-Sets eigenständig anzueignen. [Lernkompetenz, 6]
4	**Inhalte*:*** Ergonomische Sicht / Anwendersicht der GUI-Entwicklung: Usability und User-Experience Arten von GUIs Entwurfsparadigmen für GUIs (Ergonomische Sicht) Verschiedene aktuelle StyleGuides Unterschiede Desktop-Oberflächen, Web-Oberflächen, Mobile Anwendungen Widgets, Widget-Sets Weiterführung und Verallgemeinerung von GUI-Architekturen: verschiedene MVC-Umsetzungen, Thread-Aufteilung, Eventmodelle Entwicklung von Desktop-GUIs mit einem ausgewählten Widget-Set/Framework Entwicklung mobiler GUIs mit einem ausgewählten Framework
	Empfohlene Literaturangaben: Eclipse rcp (rich client platform) - tutorial. L. Vogel, https://www.vogella.com/tutorials/EclipseRCP/article.html, 2020. UX-Methoden praxisnah erklärt. J. Jacobsen et al., Rheinwerk, 2019 Android Studio 3.5 Development Essentials - Java Edition: Developing Android 10 (Q) Apps Using Android Studio 3.5, Java and Android Jetpack. N. Smyth, Payload-Verlag, 2019 Material design. developer.android.com, https://material.io/design/introduction/, 2020 Homepage der eclipse foundation. Eclipse Foundation, http://www.eclipse.org, 2020. Mobile Design Patterns Gallery: UI Patterns for Smartphone Apps, T. Neil, O'Reilly, 2014 Designing the User Interface, B. Shneiderman, Addison-Wesley, 2013 Lehrbuch der Softwaretechnik: Entwurf, Implementierung, Installation und Betrieb. H. Balzert, Spektrum Akademischer Verlag, 3. Aufl., 2012.
5	**Teilnahmevoraussetzungen:** Empfohlen: Programmierung 1 und 2

6	**Prüfungsformen***:* GUI-Development: Klausur Praktikum GUI-Development: Laborarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur, Bestandenes Praktikum
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: Application Development Wahlpflichtfach für die anderen Vertiefungsrichtungen
9	***Modulverantwortliche(r):*** Prof. Dr. Ute Matecki Dozent: Prof. Dr. Ute Matecki
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.6 23800 – Softwarearchitektur

<table>
<tr><td colspan="7">Modul: Softwarearchitektur</td></tr>
<tr><td colspan="2">Kennnummer
23800</td><td>Work-load
150 h</td><td>Modulart
P</td><td>Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Software-Architektur
Praktikum Software-Architektur</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Übungen: 3 SWS
Praktikum: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen die Bedeutung und Notwendigkeit der Betrachtung und Entwicklung von Software-Architekturen für komplexe Software-Produkte, wichtige Architekturmuster und –Stile, Techniken zur Implementierung komponentenbasierter Software-Entwicklung auf Basis von Applikationsservern [Wissen, 6]</td></tr>
<tr><td></td><td colspan="6">Kompetenz Fertigkeiten
Die Studierenden sind in der Lage
Komponenten im Sinne einer Applikationsserver-orientierten Architektur zu entwerfen und zu implementieren,
verteilte Transaktionsarchitekturen zu entwerfen und zu implementieren,
verschiedene Frontend- und Backend-Architekturen zu entwickeln und zu implementieren [Instrumentelle Fertigkeiten, 6]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit
Die Studierenden sind fähig selbständig
komplexere Aufgabenstellungen im Sinne einer komponentenorientierten Software-Architektur zu modellieren und umzusetzen [Eigenständigkeit/Verantwortung, 6]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Aufbau eines komponentenorientierten, TP-Monitor-basierten Applikationsservers
Implementierung komplexer (Datenbank-) Anwendungen auf Basis der Java Persistence Architektur</td></tr>
<tr><td></td><td colspan="6">Empfohlene Literaturangaben:
https://www.tutorialspoint.com/software_architecture_design/component_based_architecture.htm
Syperski, C.: Component Software: Beyond Object-Oriented Programming (Addison-Wesley Component Software), 2011
Andresen, A.: Komponentenbasierte Softwareentwicklung mit MDA, UML 2 und XML. Hanser, 2. Auflage, 2004,ISBN-13: 978-3446229150
Eilebrecht, K., Starke, G.: Patterns kompakt: Entwurfsmuster für effektive Software-Entwicklung. Spektrum Akademischer Verlag, 3. Auflage, 2010, ISBN-13: 978-3827425256
Erl, T.: SOA: Design Patterns. Prentice Hall International, 2008, ISBN-13: 978-</td></tr>
</table>

	0136135166Erl, T.: SOA: Entwurfsprinzipien für service-orientierte Architektur. Addison-Wesley, 2008, ISBN-13: 978-3827326515 Fowler, M. et al.: Patterns of Enterprise Application Architecture. mitp, 2003, ISBN-13: 978-3826613784 Gamma et al.: Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software. Addison-Wesley, Neuauflage, 2010, ISBN-13: 978-3827330437 Gharbi, M.: Basiswissen für Softwarearchitekten: Aus- und Weiterbildung nach iSAQB-Standard zum Certified Professional for Software Architecture - Foundation Level. dpunkt.verlag, 1. Auflage, 2012, ISBN-13: 978-3898647915
5	Teilnahmevoraussetzungen: Zulassung zu einem der Informatik-Studiengänge BSc. an der HS Albstadt Sigmaringen Profunde Kenntnisse auf in vorbereitenden Veranstaltungen des Grundstudiums der Studiengänge Wirtschaftsinformatik/IT-Security bzw. Technische Informatik, beispielsweise 12000 Programmierung 1,14500 Programmierung 2, 15000 Betriebssysteme und Netzwerke 1, 21000 Datenbanken 1
6	**Prüfungsformen***:* Mündliche Prüfung, Dauer 20 min., benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der mündlichen Prüfung
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: Application Development
9	***Modulverantwortliche(r):*** Prof. Dr. Jörg Röhrle Dozent: Prof. Dr. Jörg Röhrle
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.7 24000 – IT-Management

<table>
<tr><td colspan="7">Modul: IT-Management</td></tr>
<tr><td colspan="2">Kennnummer
24000</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung & Übungen IT-Management</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung & Übungen: 4 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
• kennen die Historie und Prinzipien von Unternehmensstrategien
• kennen Zielstellung, Zielgruppen und den Aufbau von IT-Strategien
• kennen Methoden und Verfahren der IT-Planung und das Zusammenwirken mit den Interessengruppen der Unternehmung (interne und externe Stakeholder)
• kennen Instrumente zur Planung, Steuerung und Kontrolle von IT-Bereichen im Unternehmen
• kennen innovative Geschäftsmodelle der Plattformökonomie aus Sicht der IT
[Wissen, 6]
Kompetenz Fertigkeiten
Die Studierenden
• können den Einsatz der Informationstechnologie im Kontext der strategischen Ausrichtung des Unternehmens bewerten und einordnen
• sind in der Lage, systematisch und methodisch Geschäftsmodelle und Unternehmensstrategien zu konzipieren
• können IT-Strategien systematisch und methodisch – im Kontext der Unternehmensstrategie – entwickeln
• können die Herausforderungen des IT-Management auf der gesamten organisatorischen Unternehmensebene beschreiben
• können die Auswirkungen von Digitalisierung und speziell der Plattformökonomie auf das IT-Management skizzieren
• beherrschen die differenzierte Einordnung von IT-Sicherheit und IT-Governance, Risk and Compliance Management (IT-GRC) in den Kontext des IT-Managements
[Instrumentelle Fertigkeiten, 6]

Die Studierenden
• können in umfangreichen, realitätsnahen Fallstudien die Unternehmenssituation analysieren, strategische Aspekte vor dem Hintergrund von Branche sowie Unternehmensumwelt bewerten, die Herausforderungen für IT-Organisationen und das IT-Management systematisieren
• können weiterhin – durch zielgerichtete Abstraktionstechniken – Grundzüge von IT-Strategien und Maßnahmenkataloge für das IT-Management entwickeln
[Systemische Fertigkeiten, 6]</td></tr>
</table>

	Sozialkompetenz Die Studierenden sind in der Lage, die komplexen Fallstudien zum IT-Management in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren [Team-/Führungsfähigkeit, 6] Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken [Kommunikation, 6]
	Selbstständigkeit Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen [Eigenständigkeit/Verantwortung, 6]
4	**Inhalte*:*** Die Vorlesung vermittelt Kenntnisse in der Entwicklung von IT-Strategien im Kontext von Unternehmensstrategien und dem IT-Management in der Bandbreite organisatorischer, technologischer, personeller und kaufmännischer Aspekte: • Begriffssysteme für Strategie- und Managementlehre • Entwicklung von Unternehmensstrategien • Konzeption von IT-Strategien • Referenzmodelle für das IT-Management • IT-Reifegradmodelle • Interessengruppen (Stakeholder) und interne sowie externe Kunden • Aufgaben und Verantwortung des Chief Information Officer (CIO) und des IT-Managements • Business Alignment und Business Enabling • IT-Sicherheit • IT Governance, Risk and Compliance Management (IT-GRC) • IT-Service- und Prozessmanagement • IT-Ressourcenmanagement • IT-Partnermanagement: Relationship Management und Sourcing-Strategien • IT-Projekt- und Projektportfoliomanagement • IT-Planung und IT-Controlling • Umgang mit Schatten-IT • Innovative Geschäftsmodelle in der Plattformökonomie aus Sicht der IT
	Empfohlene Literaturangaben: Hofmann, J./Schmidt, W.: Masterkurs IT-Management - Grundlagen,Umsetzung und erfolgreiche Praxis für Studenten und Praktiker. 2. Auflage, Vieweg und Teubner, 2010 Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 7. Auflage, Hanser Verlag, 2020 Friedrich, K./Malik, F./Seiwert, L.: Das große 1x1 der Erfolgsstrategie: EKS® – Die Strategie für die neue Wirtschaft, 25. Auflage, Gabal, 2009 Oswald G./Krcmar, H.: Digitale Transformation: Fallbeispiele und Branchenanalysen (Informationsmanagement und digitale Transformation), Springer Gabler, 2018 Krcmar, H.: Informationsmanagement, 6. Auflage, Springer, 2015 Resch, O.: Einführung in das IT-Management - Grundlagen, Umsetzung, Best Practice, 4. Auflage, Erich Schmidt Verlag, 2016 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen

	Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 Zimmermann, S.: Der Umgang mit Schatten-IT in Unternehmen: Eine Methode zum Management intransparenter Informationstechnologie Hanschke, I.: Strategisches Management der IT-Landschaft: Ein praktischer Leitfacen für das Enterprise Architecture Management, 3. Auflage, Hanser Verlag, 2013 Kersten, H./Klett, G./Reuter, J./Schröder, K.-W.: IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, 4. Auflage, Springer Vieweg, 2019 Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung", Springer Vieweg, 2017
5	**Teilnahmevoraussetzungen:** Entweder Wahl der Studienwahlrichtung „IT-Management" im Rahmen der Studiengänge Wirtschaftsinformatik, IT Security und Technische Informatik oder Wahl als Wahlpflichtmodul
6	**Prüfungsformen***:* Seminararbeit (Sa), benotet, und ein mündliches Referat von 15 min (R15), benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend benotete Seminararbeit, ausreichend benotetes mündliches Referat.
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: IT-Management
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand***: 23.01.2023

3.8 24100 – IT-Consulting

<table>
<tr><td colspan="8">Modul: IT-Consulting</td></tr>
<tr><td colspan="2">Kennnummer
24100</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung & Übungen IT-Consulting</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung & Übungen: 4 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
• kennen Zielstellung und Aufgaben der Unternehmensberatung
• kennen die Beratungsleistung im Kontext strategischer Initiativen im Unternehmen
• kennen die Problemlösung als originäre Beratungsleistung, speziell im Kontext der Informationstechnologie
• kennen Strategieberatung auf Unternehmens- sowie Geschäftsbereichsebene
• kennen typische Fragestellungen des IT-Consulting
• beherrschen den Lösungsansatz über ein umfangreiches Portfolio an betriebswirtschaftlichen sowie informationstechnischen Methoden und Lösungsansätzen
• kennen Methoden zur Analyse und Definition von Geschäftsmodellen sowie bewährte Geschäftsmodellmuster
• kennen die Herausforderungen der digitalen Transformation für Unternehmen und die relevanten Fragestellungen im Zeitalter der Digitalisierung
• kennen moderne Technologien und Arbeitsformen
• kennen betriebswirtschaftliche Analyse-, Bewertungs- und Entscheidungsverfahren [Wissen, 6]
Kompetenz Fertigkeiten

Die Studierenden
• können das IT-Consulting systematisieren und den Einsatz der Informationstechnologie im Kontext der strategischen Ausrichtung des Unternehmens bewerten und einordnen
• sind in der Lage, systematisch und methodisch Geschäftsmodelle zu analysieren, bewerten und zu konzipieren
• können die relevanten Grundkonzepte für die Durchführung von Beratungsprojekten (wie Lernkurven, Business Rengineering, ABC-Analysen, Produktlebenszyklus, Just-In-Time etc.) auswählen und systematisch anwenden
• können die relevanten Methoden und Analysewerkzeuge für die Durchführung von Beratungsprojekten (4C-Konzept, Five-Forces-Modell, SWOT-Analyse, Marketing-Mix, Portfolioanalyse: Boston-Consulting-Group-Matrix, Wertschöpfungskette, Businessplan etc.) auswählen und systematisch anwenden
• können die relevanten Analyse- und Beschreibungskonzepte für Geschäftsmodelle im digitalen Kontext der Plattformökonomie (Business Model Canvas, Value</td></tr>
</table>

	Proposition Canvas, Persona Design, Lean Startup: Lean Canvas) auswählen und systematisch anwenden • beherrschen das grundlegende Instrumentarium des IT-Consulting (Strategisches IT-Architekturmanagement, strategisches IT-Prozessmanagement, Auswahl von Anwendungssystemen, Optimierung von IT-Organisationsstrukturen, IT-Projekt- und Portfoliomanagement, IT-Anforderungsmanagement, IT-Servicemanagement, Identifikation von Schatten-IT etc.) *[Instrumentelle Fertigkeiten, 6]* Die Studierenden • können in umfangreichen, realitätsnahen Fallstudien die Problemstellungen identifizieren, analysieren und bewerten sowie methodische Lösungsansätze umsetzen • können weiterhin – durch zielgerichtete Abstraktionstechniken – die methodischen Lösungsansätze strukturiert systematisieren und den Lösungsweg vor einer definierten Zielgruppe verteidigen [Systemische Fertigkeiten, 6]
	Sozialkompetenz Die Studierenden sind in der Lage, die in Form einer Fallstudie definierten Aufgaben des IT-Consulting in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren [Team-/Führungsfähigkeit, 6] Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken [Kommunikation, 6]
	Selbstständigkeit Die Studierenden können Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren, zielgerichtet lösen und präsentieren [Eigenständigkeit/Verantwortung, 6]
4	**Inhalte*:*** Die Vorlesung vermittelt Kenntnisse in der Unternehmensberatung, speziell im Kontext der Informationstechnologie und neuerer Entwicklungen der Digitalisierung: • Grundlagen der Unternehmensberatung • Systematisierung von Unternehmensberatungen • Beratungsleistungen im Kontext strategischer Initiativen • Problemlösung als originäre Beratungsleistung • Sinnstiftung als derivative Beratungsleistung • Strategieberatung auf Unternehmens- und Geschäftsbereichsebene • Grundlagen des IT-Consulting • Einsatz moderner Technologien und Technikfolgenabschätzung • Digitalisierung: Prinzipien, Erfolgsfaktoren und Technikeinsatz • Digitale Plattformökonomie • Ökonomische, organisatorische und technologische Grundkonzepte • Fortgeschrittene Methoden und Analysewerkzeuge • Vernetztes Problemlösen • Bearbeitung realitätsnaher Fallstudien

	Empfohlene Literaturangaben: Fink, D.: Strategische Unternehmensberatung, 1. Auflage, Vahlen, 2009 Hartenstein, M./Billing, F./Schawel, C./Grein, M.: Der Weg in die Unternehmensberatung: Consulting Case Studies erfolgreich bearbeiten, 12. Auflage, Springer Gabler, 2015 Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 6. Auflage, Hanser, 2017 Niedereichholz, C.: Unternehmensberatung: Band 1: Beratungsmarketing und Auftragsakquisition, 5. Auflage, Oldenbourg, 2010 Niedereichholz, C.: Unternehmensberatung: Band 2: Auftragsdurchführung und Qualitätssicherung, 6. Auflage, Oldenbourg, 2012 Mangiapane, M./Büchler, R.: Modernes IT-Management: Methodische Kombination von IT-Strategie und IT-Reifegrademodell, Springer Vieweg, 2015 Camenzind, A./Fueglistaller, U.: Strategisches Denken in KMU und die Lehren von Clausewitz, Verlag Neue Zürcher Zeitung, 2014 Simon, H./Von der Gathen, A.: Das große Handbuch der Strategieinstrumente: Werkzeuge für eine erfolgreiche Unternehmensführung, 2. Auflage, Campus, 2010 Dörner, D.: Die Logik des Misslingens: Strategisches Denken in komplexen Situationen, 11. Auflage, rororo, 2012 Vester, F.: Die Kunst vernetzt zu denken: Ideen und Werkzeuge für einen neuen Umgang mit Komplexität: Ein Bericht an den Club of Rome, DVA, 2019 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 Osterwald, A./Pigneur, Y.: Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer, campus, 2011 Osterwald, A./Pigneur, Y./Bernarda, G./Smith, A.: Value Proposition Design: Entwickeln Sie Produkte und Services, die Ihre Kunden wirklich wollen, campus, 2015 Maurya, A.: Running Lean: Das How-to für erfolgreiche Innovstionen, O'Reilly, 2013 Gärtner, C./Heinrich. C. (Hrsg.): Fallstudien zur Digitalen Transformation: Case Studies für die Lehre und praktische Anwendung, Springer Gabler, 2017 Von Engelhardt, S./Petzold, S. (Hrsg.): Das Geschäftsmodell-Toolbox für digitale Ökosysteme, Campus, 2019 Gassmann, O./Frankenberger, K./Csik, M.: Geschäftsmodelle entwickeln: 55 innovative Konzepte mit dem St. Galler Business Model Navigator, 2. Auflage, 2017 Hoffmeister, C.: Digitale Geschäftsmodelle richtig einschätzen, Hanser, 2013 Srnicek, N.: Plattform-Kapitalismus, Hamburger Edition, 2018 Jaekel: Die Macht der digitalen Plattformen: Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz, Springer Vieweg, 2017 Parker, G. G./Van Alstyne, M.W./Choudary, S. P.: Die Plattform-Revolution im E-Commerce: Von Airbnb, Uber, PayPal und Co. lernen: Wie neue Plattform-Geschäftsmodelle die Wirtschaft verändern, mitp, 2017 Clement, R./Schreiber, D./Bossauer, P./Pakusch, C.: Internet-Ökonomie: Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, 4. Auflage, Springer Gabler, 2020
5	**Teilnahmevoraussetzungen:** Entweder Wahl der Studienwahlrichtung „IT-Management" im Rahmen der Studiengänge Wirtschaftsinformatik, IT Security und Technische Informatik oder Wahl als Wahlpflichtmodul
6	**Prüfungsformen***:* Seminararbeit (Sa), benotet, und ein mündliches Referat von 15 min. (R15), benotet.

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Seminararbeit, ausreichend bewertetes mündliches Referat.
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: IT-Management
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.9 24400 – Offensive Sicherheitsmethoden

<table>
<tr><td colspan="7">Modul: Offensive Sicherheitsmethoden</td></tr>
<tr><td colspan="2">Kennnummer
24400</td><td>Workload
225 h</td><td>Modulart
KM</td><td colspan="2">Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Übungen Offensive Sicherheitsmethoden
Praktikum Offensive Sicherheitsmethoden</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
6 SWS / 90 h</td><td>Selbst-studium
135 h</td><td>Credits (ECTS)
7,5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Übungen: 4 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Breites Wissen über offensive Methoden der IT Sicherheit inkl. PEN Tests, CIA Angriffe auf Systeme, Netzwerke und Kommunikationskanäle [Wissen, 6]
Tiefe Kenntnisse aktueller offensiver Werkzeuge und Frameworks, u.a. aktuelles Metasploit [Wissen, 6]
Kompetenz Fertigkeiten
Sind in der Lage mittels umfangreicher und vielfältiger offensiver Methoden und Werkzeuge in geschützte IT Systeme einzudringen [Instrumentelle Fertigkeiten, 6]
Sind in der Lage neue offensive Werkzeuge und Skripte zu entwickeln und anzuwenden [Systemische Fertigkeiten, 6]
Studierende sind in der Lage das Sicherheitsniveaus aus den Ergebnissen offensiver Sicherheitstests zu beurteilen [Beurteilungsfähigkeit, 6]
Sozialkompetenz
Neue Methoden und Techniken im Bereich offensiver Sicherheitsmethoden werden mit einem Fachpublikum diskutiert [Kommunikation, 6]
Selbstständigkeit
Reflexion und Bewusstsein über rechtliche und ethische Rahmenbedingungen und Auswirkungen offensiver Methoden [Reflexivität, 6]</td></tr>
</table>

4	**Inhalte*:*** Vorlesung & Übungen • Offensive Methoden und ihre Ziele im Kontext der IT Sicherheit • Rechtliche und Ethische Rahmenbedingungen • Grundlagen, Rahmenbedingungen und Ziele von Penetrationstests • Angriffe auf die Vertraulichkeit, Integrität oder Verfügbarkeit von • Übertragungskanälen • Netzwerken • Betriebssystemen • Anwendungen • Hardwarekomponenten • Web-Anwendungen • Funksystemen • Finden von Schwachstellen durch Fuzzing und Codeanalyse Praktikum Die in der Vorlesung behandelten Punkte werden im Praktikum innerhalb eines isolierten Netzwerks praktisch erprobt. Dabei werden aktuelle Werkzeuge und Systeme aus dem Penetrationstest- und Systemanalysebereich wie z.B. Burp Suite, Nmap und das Metasploit Framework angewandt.
	Empfohlene Literaturangaben: Kim, P.: The Hacker Playbook 2, A practical Guide to Penetration Testing, Secure Planet LLC, 2015 Hadnagy, C.: Social Engineering, The Art of Human Hacking, Wiley Publishing Inc., 2011 Stuttard D.: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Auflage 2, John Wiley & Sons, 2011 Erickson, J.: Hacking, The Art of Exploitation, No Starch Press, 2008 Messner, M.: Metasploit: Das Handbuch zum Penetration-Testing Framework, dpunkt.Verlag, 2015
5	**Teilnahmevoraussetzungen:** keine empfohlen: Inhalte der Module Einführung ITS, Betriebssysteme, Netzwerke, Web-basierte Anwendungen
6	**Prüfungsformen*:*** Referat 15 min. incl. schriftlicher Ausarbeitung Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: Applied IT Security
9	***Modulverantwortliche(r):*** Prof. Dr. Jungk Dozent: Herr Koplin, Herr Schwarz
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:***

	24.01.2023

3.10 32000 - Simulationstechnik

Modul: Simulationstechnik						
Kennnummer 32000	**Workload** 150	**Modulart** P	**Studiensemester** 7. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung 3 SWS Praktikum: 1 SWS	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS/ 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung & Übungen Simulationstechnik Praktikum Simulationstechnik					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen: - die grundlegende Vorgehensweise und die Parameter zur Planung der Fertigungsressourcen in realen und in virtuellen Systemen. - die Analyse von Prozessen für Simulationszwecke und Methoden der Prozessmodellierung. - die Informationsmodelle der Simulation. - grundelemente und Algorithmen zur Modellbildung der objekt- und ereignisorientierten Simulation. - Störgrößenverarbeitung in Simulationssystemen. - Bewertungsverfahren für Simulationsmodelle [Wissen, 6]					
	Kompetenz Fertigkeiten Die Studierenden können: - Betriebs- und Produktionsstrukturen analysieren und die zur Simulation erforderlichen Parameter erfassen. - die Methoden der Modellbildung anwenden und Simulationsmodelle entwerfen, erstellen, erweiterte Algorithmen hinzufügen. ☐Simulationsmodelle optimieren nach den Kriterien: minimale Durchlaufzeit, maximale Kapazitätsauslastung, minimale Puffergrößen, maximale Flexibilität - Verfahren und Algorithmen anwenden die geeignet sind um Simulationsaufgaben in komplexe Modelle zu überführen und damit zielgerichtet ingenieurmäßig zu arbeiten. ☐Modellierverfahren bewerten und evaluieren und die geeigneten Methoden zur Lösung der Probleme auswählen und anwenden. Dazu gehört auch die Analyse von Simulationsaufgaben nach technischen und ökonomischen Gesichtspunkten. [Systemische Fertigkeiten, 6]					
	Sozialkompetenz Nicht relevant					
	Selbstständigkeit Die Studierenden sind fähig: - logisch und abstrakt zu denken. - technisch/organisatorische Prozesse in Simulationsmodelle zu überführen und daraus Vorhersagen für die Praxis abzuleiten. - die Praxisrelevanz der erlernten Methoden und Prinzipien zu erkennen und diese					

	zielgerichtet zur Lösung von Ingenieurproblemen anzuwenden. [Eigenständigkeit/Verantwortung, 6]
4	**Inhalte***:* Die grundlegende Vorgehensweise und die Parameter zur Planung der Fertigungsressourcen in realen und in virtuellen Systemen Analyse von Prozessen und Abläufen Parameterermittlung und -erfassung zur Modellierung für die Simulation. Methoden der Prozessmodellierung, Grundelemente, Algorithmen und Modellbildung zur objekt- und ereignisorientierten Simulation Störgrößenverarbeitung (Verteilfunktionen) in Simulationssystemen Modellbildungstheorie, Systemarchitekturen, Informationsmodelle der Simulation virtuelle Erprobung, Rapid Prototyping (Verfahren, Schnittstellen), virtuelle und reale Prozessketten, Managementkonzepte für virtuelle Entwicklungs- und Produktionsstrukturen. ☐ Bewertung von Simulationsmodellen (technisch und ökonomisch).
	Empfohlene Literaturangaben: Spur, G., Krause, F.-L.: Das virtuelle Produkt, Hanser Verlag, München. Bangsow, S.: Fertigungssimulationen mit Plant Simulation und SimTalk. Anwendung und Programmierung mit Beispielen und Lösungen, Hanser Verlag, München. Eley, M.: Simulation in der Logistik. Eine Einführung in die Erstellung ereignisdiskreter Modelle unter Verwendung des Werkzeuges "Plant Simulation", Springer Verlag, Berlin,New York Hehenberger, P.: Computerunterstützte Fertigung. Eine kompakte Einführung. 1. Aufl.,: Springer Verlag, Berlin, New York. Kramer, U.; Neculau, M.: Simulationstechnik. Hanser Verlag, München. Liebl, F.: Simulation. Problemorientierte Einführung, 2. Aufl., Oldenburg Verlag, München, Wien. Sauerbier, T.: Theorie und Praxis von Simulationssystemen. Eine Einführung für Ingenieure und Informatiker, mit Programmbeispielen und Projekten aus der Technik. Vieweg Verlag, Braunschweig, Wiesbaden
5	**Teilnahmevoraussetzungen:** keine

6	**Prüfungsformen***:* Klausur, 90 min., benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Am Ende des Semesters ist eine 90 minütige schriftliche Prüfung zu schreiben. Während des Semesters sind mehrere Praktikumsaufgaben zu bearbeiten.
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik, Wahlrichtung Cyber-Physical Systems
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Eppler Dozent(in):
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.11 32100 – Mobile Systeme und Cloud

<table>
<tr><td colspan="7">Modul: Mobile Systeme und Cloud</td></tr>
<tr><td colspan="2">32100</td><td>Workload
150 h</td><td>Modulart
P</td><td>Studiensemester
7</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Übungen Mobile Systeme und Cloud.
Praktikum Mobile Systeme und Cloud</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Übungen: 3 SWS
Praktikum: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen die Besonderheiten mobiler Endgeräte (incl. Sensoren), Netzwerke und Protokolle. Sie kennen aktuelle Architekturen, APIs und Deploymentmöglichkeiten mobiler Applikationen (beispielsweise unter Android)
Sie kennen Cloud-Einsatzszenarien und Service-Modelle aus Kundensicht, sowie Betriebsszenarien von Cloud-Services aus Anbietersicht. Sie kennen Cloud-Architekturen und Softwarelösungen für Cloud-Einsatzszenarien [Wissen, 6]

Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, eigenständig mobile Applikationen (incl. anzusprechender Sensoren) zu spezifizieren. Sie sind in der Lage, mobile Systeme nach vorgegebener/selbst erstellter Spezifikation zu entwickeln und zu testen. Sie können mobile Systeme für den Endanwender bereitstellen (Deployment). Sie können außerdem Einsatzszenarien für Cloud Anwendungen verstehen und für Kunden entwickeln. Die Studierenden können Cloud-Service-Modelle (aus Anbietersicht) spezifizieren und entwickeln. [Instrumentelle Fertigkeiten, 6]

Die Studierenden sind in der Lage, auch für sie neue Problemstellungen im Umfeld mobiler Anwendungen und Cloud-Servicemodelle zu lösen.
[Systemische Fertigkeiten, 6]

Die Studierenden im Umfeld Mobile & Cloud architektonisch und codetechnisch beurteilen und einordnen. [Beurteilungsfähigkeit, 6]

Sozialkompetenz
Die Studierenden können bei der Entwicklung von Cloud-Lösungen und mobilen Apps Kunden aktiv mit einbeziehen, ihre Anforderungen berücksichtigen und die Machbarkeit kommunizieren, mit dem Ziel, hohe Usability und Benutzerfreundlichkeit der Anwendung zu erreichen.

[Kommunikation, 6]

Selbstständigkeit
Die Studierenden sind in der Lage, sich im sehr schnelllebigen Umfeld mobiler Systeme und Cloud-Systeme selbstständig auf neue Technologien und Frameworks einzustellen und sich diese rasch und selbstständig anzueignen.
[Eigenständigkeit/Verantwortung, 6]</td></tr>
</table>

	Sie sind in der Lage, sich auch weitere Frameworks im Cloud-Umfeld, sowie im Bereich mobiler Anwendungen eigenständig anzueignen. *[Lernkompetenz, 6]*
4	**Inhalte*:*** - Besondere Anforderungen an mobile Anwendungen (Kundensicht und Anbietersicht) - Mobile Endgeräte, Sensoren mobiler Endgeräte - Arten Mobiler Anwendungen (Apps) - Aktuelle mobile Betriebssysteme - Aktuelle Entwicklungswerkzeuge, Frameworks und APIs für mobile Applikationen - Architekturparadigmen für die Entwicklung mobiler Anwendungen - Besondere Anforderungen an Cloud-Einsatzszenarien und Betriebsszenarien (Kundensicht und Anbietersicht) - Cloud-Einsatz-Arten, Cloud-Service-Modelle und Cloud-Architekturen (Private, Public, Hybrid Clouds, SaaS, PaaS, IaaS, HaaS) - Cloud-Management (Service Level Agreements, LifeCycle, Betrieb, Kosten- und Risikomanagement) Exemplarische Betrachtung aktueller Cloud-Lösungen
	Empfohlene Literaturangaben: *Mobile Computing. K. Zeppenfeld et al., W3L GmbH* Android 7. T. Künneth, Rheinwerk Verlag IaaS mit OpenStack. T. Beiter et al., d.punkt Verlag Die Logik des Mißlingens, D. Dörner, rororo Das E-Commerce-Buch, A. Graf et al., dfv-Mediengruppe
5	**Teilnahmevoraussetzungen:** Empfohlen: Programmierung 1 und 2
6	**Prüfungsformen***:* Vorlesung: Klausur 90min Praktikum: Laborarbeit unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur, Bestandenes Praktikum
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Application Development Wahlpflichtfach für die anderen Vertiefungsrichtungen
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozent: Herr Inan
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.12 32300 – IT-GRC

<table>
<tr><td colspan="7">Modul: IT-GRC (IT-Governance, Risk & compliance)</td></tr>
<tr><td colspan="2">Kennnummer
32300</td><td>Workload
150 h</td><td>Modulart
P</td><td>Studiensemester
7</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Übungen IT-GRC</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Übungen: 4 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
• kennen die wirtschaftliche, rechtliche und ethische Motivation für Governance, Risk and Compliance Management (GRC)
• können GRC systematisieren und jeweils die Disziplinen Corporate Governance, Risikomanagement und Compliance Management systematisieren und beschreiben
• kennen methodische Modelle für GRC
• kennen den methodischen Zusammenhang zwischen GRC und IT-GRC
• kennen Aufgaben, Zielstellung und Pflichten von Wirtschaftsprüfung, IT-Prüfung und IT-Revision im Kontext von IT-GRC
• kennen Aufgaben, Zielstellung und Pflichten des Chief Information Officer (CIO) sowie des IT-Managements im Kontext von IT-GRC
• kennen die Herausforderungen betrieblicher Unternehmen im Kontext der Digitalisierung, Industrie 4.0 und Plattformökonomie im Kontext von IT-GRC
• kennen aktuelle Forschungsprojekte
[Wissen, 6]

Kompetenz Fertigkeiten
Die Studierenden
• können in umfangreichen, realitätsnahen Fallstudien die Unternehmenssituation analysieren, Herausforderungen in Bezug auf IT-GRC vor dem Hintergrund von Branche sowie Unternehmensumwelt bewerten sowie die Herausforderungen für IT-Organisationen und das IT-Management systematisieren
• können weiterhin – durch zielgerichtete Abstraktionstechniken – Grundzüge von IT-GRC-Reifegraden sowie -Maßnahmenkatalogen für das IT-Management entwickeln
[Instrumentelle Fertigkeiten, 6]</td></tr>
</table>

	Sozialkompetenz Sind in der Lage, die komplexen Fallstudien zu IT-GRC in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren [Team-/Führungsfähigkeit, 6]
	Selbstständigkeit Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen *[Eigenständigkeit/Verantwortung, 6]* Die Studierenden erlernen die Fähigkeit, aus Sicht unterschiedlicher Stakeholder und in unterschiedlichen Rollen eine konkrete Unternehmenssituation zu analysieren, zu reflektieren und zu bewerten. Der informationstechnologische Hintergrund der Studierenden wird ergänzt um rechtliche, organisatorische, technologische Aspekte, so dass sie die richtigen Schlussfolgerungen aus einer kritischen Prüfungsperspektive ziehen und zielgerichtete Maßnahmen entwickeln können. [Reflexivität, 6]
4	**Inhalte*:*** Die Vorlesung vermittelt Kenntnisse in der Entwicklung von IT-Strategien im Kontext von Unternehmensstrategien und dem IT-Management in der Bandbreite rechtlicher, organisatorischer, technologischer und personeller Aspekte: • Begriffssystem für IT Governance, Risk and Compliance Management • Zusammenhang zwischen GRC und IT-GRC • Unternehmerische Fallbeispiele für Bedeutung und Motivation • Corporate Governance und Corporate Governance-Systeme • Risikomanagement und Risikomanagementsysteme • Compliance und Compliance-Management-Systeme • Reifegradmodelle für den betrieblichen Einsatz • IT-GRC als ganzheitlicher methodischer Ansatz • IT-GRC aus Sicht von Wirtschaftsprüfung • IT-GRC aus Sicht der IT-Revision und IT-Prüfung • IT-GRC im Kontext von IT Security und Cyber Security • IT-GRC im Kontext betrieblicher Resilienz • IT-GRC im Kontext von Daten, Datenschutz und Cloud Computing • IT-GRC im Kontext der Forschung (Industrial Data Space) • IT-GRC im Kontext von Digitalisierung, Industrie 4.0 und digitaler Plattformökonomie
	Empfohlene Literaturangaben: *Knoll, M.: Praxisorientiertes IT-Risikomanagement: Konzeption, Implementierung und Überprüfung, 2. Auflage, dpunkt, 2019* *Nestler, D./Modi, J. (Hrsg.: Institut der Wirtschaftsprüfer in Deutschland e.V.): Leitfaden IT-Compliance: Anforderungen, Chancen und Umsetzungsmöglichkeiten, IDW, 2020.* *Klotz, M.: IT-Compliance: Ein Überblick, 1. Auflage, dpunkt, 2009* *Rath, M.; Sponholz, R.: IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen, o. A., Erich Schmidt, 2009* *Sowa, A./Duscha, P./Schreiber, S.: IT-Revision, IT-Audit und IT-Compliance: Neue*

	Ansätze für die IT-Prüfung, Springer Vieweg, 2019 *Kersten, H.; Klett, G.: Der IT Security Manager: Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden, 4. Auflage, Springer Vieweg, 2015* *Johannsen, W./Goeken, M.: Referenzmodelle für IT-Governance: Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co, dpunkt., 2010* *Pohlmann, N.: Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, Springer Vieweg, 2019* *Schulz, T: Cybersicherheit: für vernetzte Anwendungen in der Industrie 4.0, Vogel, 2019*
5	**Teilnahmevoraussetzungen:** Entweder Wahl der Studienwahlrichtungen „IT-Management" oder „Application Management" im Rahmen der Studiengänge Wirtschaftsinformatik, IT Security und Technische Informatik oder Wahl als Wahlpflichtmodul
6	**Prüfungsformen***:* Klausur, 90 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiches Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: Application Development, IT-Management
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.13 32400 – IT-Sicherheitsmanagement

<table>
<tr><td colspan="7">Modul: IT-Sicherheitsmanagement</td></tr>
<tr><td colspan="2">Kennnummer
32400</td><td>Workload
75 h</td><td>Modulart
P</td><td>Studiensemester
7</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Übungen IT-Sicherheitsmanagement</td><td>Sprache
Deutsch (deutsches und englisches Literaturstudium erforderlich)</td><td>Kontakt-zeit
2 SWS / 30 h</td><td>Selbst-studium
45 h</td><td>Credits (ECTS)
2,5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Übungen: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Breites Wissen über Grundlagen und Bedeutung des IT Sicherheitsmanagements [Wissen, 6]
Tiefe Kenntnis relevanter Normen und Regulatorien im Bereich IT Sicherheitsmanagement [Wissen, 6]
Kompetenz Fertigkeiten
Studierende beherrschen ein breites Spektrum an Methoden und Werkzeugen für die Konzeption und Implementierung eines ISM [Instrumentelle Fertigkeiten, 6]
Studierende sind in der Lage das IT Sicherheitsniveau einer Organisation auf organisatorischer Ebene zu bewerten und mittels ISM zu verbessern [Beurteilungsfähigkeit, 6]
Sozialkompetenz
Fachspezifika und aktuelle Regulatorien können sowohl einem Fachpublikum diskutiert als auch den Fachabteilungen verständlich vermittelt werden [Kommunikation, 6]
Selbstständigkeit
Das Sicherheitsniveau und Sicherheitsrisiken der Unternehmens IT können hinsichtlich des rechtlichen und ethischen Rahmens kritisch reflektiert werden. [Reflexivität, 6]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung & Übungen:
• Grundlagen und Bedeutung des ITSicherheitsmanagements
• Gesetzliche Anforderungen
• IT-Sicherheitsstandards
• Prozess „IT-Sicherheitsmanagement“
• IT-Sicherheitsmanagement nach BSI-Grundschutzbe
• Normen und Zertifizierung
• Organisatorische Aspekte</td></tr>
</table>

	Empfohlene Literaturangaben: Hofmann, Schmidt: Masterkurs IT-Management, 2. Auflage, Springer, 2010 Grünendahl, Steinbacher u.a.: Das IT-Gesetz: Compliance in der IT-Sicherheit, 2. Auflage, Springer, 2012 Kersten, Reuter u.a.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, 4. Auflage, Springer, 2013 Müller, K.-R.: IT-Sicherheit mit System, 4. Auflage, Springer, 2011 Pelzl, J.: e-security 4.0 – Sicherheitsmanagement für das Internet der Dinge, aus: Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing - Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT-Sicherheit, Springer, 2014 Kersten, H.; Klett, G.: Der IT Security Manager: Expertenwissen für jeden IT Security Manager - Von namhaften Autoren praxisnah vermittelt, 2. Auflage, Springer, 2012
5	**Teilnahmevoraussetzungen:** keine empfohlen: Inhalte der Module Einführung ITS, Betriebswirtschaftslehre und Management
6	**Prüfungsformen***:* Klausur, 60 min.,benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik Wahlrichtung: Applied IT-Security
9	***Modulverantwortliche(r):*** (n.n.), Prof. Holger Morgenstern Dozent: LB
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.14 32500 – Mobile und Cloud Forensik

<table>
<tr><td colspan="7">Modul: Mobile und Cloud Forensik</td></tr>
<tr><td colspan="2">Kennnummer
32500</td><td>Workload
75</td><td>Modulart
P</td><td>Studiensemester
7. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS (falls Wahlrichtung Applied IT-Security zustande kommt)</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Mobile und Cloud Forensik</td><td>Sprache
Deutsch und Englisch</td><td>Kontakt-zeit
2 SWS/ 30 h</td><td>Selbst-studium
45 h</td><td>Credits (ECTS)
2,5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Übungen, Seminar: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden erhalten breite Kenntnis forensischer Methoden, spezialisiert im Mobile- und Cloud-Bereich. [Wissen, 6]

Kompetenz Fertigkeiten
Die Studierenden erlernen ein breites Spektrum an forenstischen Methoden zur Sicherung und Analyse digitaler Spuren im Mobile- und Cloud-Bereich. [Instrumentelle Fertigkeiten, 6]

Die Studierenden sind in der Lage Möglichkeiten und Grenzen der erlernten forensischen Methoden und Werkzeuge einzuschätzen und diese zu erweitern bzw. neue Skripte/Werkzeuge zu entwickeln. [Systemische Fertigkeiten, 6]

Die Studierende können die Relevanz und Sicherheit gesicherter und analysierte digitaler Spuren beurteilen. [Beurteilungsfähigkeit, 6]

Sozialkompetenz
Die Studierenden können die Ergebnisse eine forensischen Untersuchung schriftlich darlegen [Kommunikation, 6]

Selbstständigkeit
Die Studierenden können forensische Aufgabenstellungen eigenständig analysieren und ihre Untersuchungsprozesse entsprechend gestalten. [Eigenständigkeit/Verantwortung, 6]

Die Studiereden können notwendige neue / angepasste forensische Methoden und Werkzeuge eigenständig erschließen. [Lernkompetenz, 6]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
• Digitale Forensik im Kontext mobiler Endgeräte (Smartphones, Navigationsgeräte, etc.)
• Besonderheiten im Bereich der forensischen Sicherung und Analyse von mobilen Endgeräten (Betriebssysteme, Dateisysteme, Datenformate, Zugriffsmöglichkeiten und Einschränkungen)</td></tr>
</table>

	• Digitale Forensik im Kontext des Cloudcomputings • Besonderheiten im Bereich der forensischen Sicherung und Analyse von Cloud-Systemen (Architekturen, Service- und Organisationsmodelle, Vertrauensmodelle, Zugriffsmöglichkeiten und Einschränkungen) • Praktische Anwendungen und Übungen im Bereich Digitalen Forensik mobiler Endgeräte und Cloud-Systeme
	Empfohlene Literaturangaben: Dewald und Freiling (2015): Forensische Informatik, 2. Auflage, Books on Demand Casey (2011): Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3. Auflage, Academic Press Carrier (2005): File System Forensic Analysis, Addison Wesley Tamma, Skulkin, Mahalik und Bommisetty (2020): Practical Mobile Forensics, Packt Publishing, 4. Auflage
5	**Teilnahmevoraussetzungen:** Keine (empfohlen: Inhalte der Module Einführung ITS, Betriebssysteme, Netzwerke, Digitale Forensik)
6	**Prüfungsformen***:* Klausur 60 min.
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik, Wahlrichtung Applied IT-Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Holger Morgenstern, Prof. Dr. Christofer Fein Dozent(in): Prof. Dr. Christofer Fein
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 27.02.2023

3.15 32248 – SAP Application Development

Modul: SAP Application Development						
Kennnummer 32248	**Workload** 75	**Modulart** KM	**Studiensemester** 5. und 7. Semester	**Dauer** 1 Semester		**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung mit praktischen Übungen	**Sprache** Deutsch und Englisch	**Kontakt-zeit** 2 SWS/ 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5	
2	**Lehrform(en) / SWS:** Vorlesung und Übungen: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die Erweiterungskonzepte im Digital Core S4HANA und sind mit den Entwicklungswerkzeugen von SAP vertraut. . [Wissen, 6] /Niveaustufe wählen *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, Datenstrukturen zu definieren und diese zu verwenden. Sie können die grundlegenden Modularisierungskonzepte in der ABAP-Programmierung anwenden und einfache Backend-Applikationen implementieren [Instrumentelle Fertigkeiten, 6] Sie sind in der Lage, Lösungskonzepte für konkrete Anforderungen zu erarbeiten [Systemische Fertigkeiten, 6] Die Studierende können die Relevanz und Sicherheit gesicherter und analysierte digitaler Spuren beurteilen. [Beurteilungsfähigkeit, 6] *Sozialkompetenz* Die Studierenden sind in der Lage Anforderungen mit den Auftraggebern abzustimmen und diese strukturiert zusammenzufassen. [Kommunikation, 6] *Selbstständigkeit* Die Studierenden sind in der Lage, Lösungskonzepte aus konkreten Anforderungen zu entwickeln und diese umzusetzen. [Eigenständigkeit/Verantwortung, 6] Sie können sich kritisch mit Lösungen auseinandersetzen und Schwachstellen in der Umsetzung identifizieren [Reflexivität, 6]					
4	**Inhalte*:*** - Architektur von SAP-Systemen - Systemmonitore und IDEs - Datenstrukturen in SAP - Einführung in die Programmierung mit ABAP - Erweiterungskonzepte für Standardapplikationen - Sicherheitsaspekte in der ABAP-Entwicklung (Berechtigungskonzepte, Changemanagement,…) - Aufbau und Anwendung von Micro-Services - Bereitstellen von Micro-Services über RFC/Web/ bzw.					

	- ODATA-Services oder IoT-Protokolle wie MQTT - Front-End-Entwicklung (Reports / Fiori-Apps)
	Empfohlene Literaturangaben: ABAP Objects: Die Werkzeuge des ABAP-Entwicklers: Das umfassende Handbuch zu Konzepten, Sprachelementen und Werkzeugen in ABAP OO – Ausgabe 2020 (SAP PRESS) Einstieg in ABAP: Die Einführung für ABAP-Einsteiger – Topaktuell zu SAP S/4HANA (SAP PRESS)
5	**Teilnahmevoraussetzungen:** Grundkenntnisse zu Architektur, Funktionen und Einsatzbereichen von ERP-Systemen sind von Vorteil aber nicht zwingend erforderlich.
6	**Prüfungsformen***:* Mündliche Prüfung 15 minütig (M15)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Voraussetzung für einen erfolgreichen Modulabschluss ist ausschließlich die bestandene mündliche Prüfung. Praktische Aufgaben, die in der Vorlesung bearbeitet werden, dienen lediglich zur Festigung des Stoffes und gehen nicht in die Bewertung ein.
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Bernd Stauß Dozent(in): Prof. Dr.Bernd Stauß
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.16 xxxxx – Digitaler Schaltungsentwurf

<table>
<tr><td colspan="7">Modul: Digitaler Schaltungsentwurf</td></tr>
<tr><td colspan="2">Kennnummer
xxxxx</td><td>Workload
75</td><td>Modulart
KM</td><td>Studiensemester
5. und 7. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung und Übung Digitaler Schaltungsentwurf</td><td>Sprache
Deutsch oder Englisch</td><td>Kontakt-zeit
2 SWS/ 30 h</td><td>Selbst-studium
45 h</td><td>Credits (ECTS)
2,5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung und Übung Digitaler Schaltungsentwurf: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verstehen die Grundzüge und Konzepte von Hardwarebeschreibungssprachen und können diese anwenden. [Wissen, 6]

Kompetenz Fertigkeiten
Die Studierenden können Hardware-Implementierungen von Algorithmen und einfachen Microcontrollern erstellen. [Instrumentelle Fertigkeiten, 6]

Sozialkompetenz
Die Studierenden können die Eigenschaften von Hardware-Implementierungen mit anderen Experten diskutieren. [Kommunikation, 6]

Selbstständigkeit
Die Studierenden können selbstständig komplexe Problemstellungen mit Hardware-Implementierungen lösen. [Eigenständigkeit/Verantwortung, 6]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung
- Einführung RTL-Programmierung mit VHDL oder Verilog
- Einführung Programmierung von FPGAs und ASICs
- Ansteuerung von externer Peripherie (Schalter, LEDs, 7-Segment-Anzeige) und Kommunikation über serielle Schnittstellen.
- Synchronisation von unterschiedlichen Clock-Domains
- Funktionsweise einfacher Microcontroller

Übung
- FPGA-Programmierung mit VHDL oder Verilog
- Implementierung von Beispielanwendungen in VHDL oder Verilog

Empfohlene Literaturangaben:
Ashenden, J. P. - The Designer's Guide to VHDL, Morgan Kaufmann, 2010

Ashenden, J. P. - The Student's Guide to VHDL, Morgan Kaufmann, 2008

LaMeres, Brock J. - Quick Start Guide to Verilog, Springer Verlag, 2021</td></tr>
</table>

	Harris, D. M., Harris, S. L., Digital Design and Computer Architecture, Morgan Kaufmann, 2013
5	**Teilnahmevoraussetzungen:** Programmierkenntnisse (C, Assembler), Digitale Logik, Rechnertechnik
6	**Prüfungsformen***:* Klausur 60 min
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Klausur
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Bernhard Jungk Dozent(in): Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.16 xxxxx – Cybersecurity Awareness and Behavior

Modul: Cybersecurity Awareness and Bahavior						
Kennnummer xxxxx	**Workload** 150	**Modulart** KM	**Studiensemester** 5. + 7. Semester		**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung / Seminar Cybersecurity Awareness and Behavior Übung Cybersecurity Awareness and Behavior	**Sprache** Deutsch oder Englisch	**Kontakt-zeit** Vorlesung / Seminar 2 SWS/ 30 h Übung 2 SWS/30 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung / Seminar Cybersecurity Awareness and Behavior: 2 SWS Übung Cybersecurity Awareness and Behavior: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden verstehen die Grundzüge und Konzepte von Cybersecurity Trainings in Unternehmen und Organisationen [Wissen, 6] *Kompetenz Fertigkeiten* Die Studierenden können Trainings und Bildungsmaßnahmen mit dem Ziel der Cybersecurity Awareness kritisch beurteilen, effizient gestalten, und statistisch evaluieren. [Beurteilungsfähigkeit, 6] *Sozialkompetenz* Die Studierenden können Schulungskonzepte präsentieren und kritisch diskutieren. [Kommunikation, 6] *Selbstständigkeit* Die Studierenden können sich selbstständig in internationale Fachliteratur einlesen und diese auf deutsch oder englisch präsentieren. [Eigenständigkeit/Verantwortung, 6]				
4	**Inhalte*:*** Vorlesung & Seminar - Formats and course designs of cybersecurity awareness trainings in companies and organizations - Evaluations of training and education effects - Methodological designs and statistical approaches - Employee-centered and adaptive interventions - Cybersecurity culture and cyberhygiene - Self-report assessments, design of surveys and questionnaires - Factors of success of sensibilization efforts - Behavior change models and sustainability of training effects				

	Empfohlene Literaturangaben: Weber, K., Schütz, A.E., & Fertig, T. (2019). Grundlagen und Anwendung von Information Security Awareness. Springer: Wiesbaden.
5	**Teilnahmevoraussetzungen:** keine
6	**Prüfungsformen***:* Hausarbeit
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Als mindestens ausreichend benotete Hausarbeit sowie ein erfolgreich absolviertes Kurzreferat
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Stefan Sütterlin Dozent(in): Prof. Dr. Stefan Sütterlin
10	***Optionale Informationen:*** -----
11	***Bearbeitungsstand:*** 23.01.2023

3.17 23474 – Hardware-orientierte IT-Sicherheit

Modul: Hardware-orientierte IT-Sicherheit						
Kennnummer 23474	**Workload** 75	**Modulart** KM	**Studiensemester** 5. + 7. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung / Seminar Einführung Hardware-orientierte IT-Sicherheit	**Sprache** Deutsch oder Englisch	**Kontakt-zeit** Vorlesung und Seminar 2 SWS/ 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5	
2	**Lehrform(en) / SWS:** Vorlesung & Seminar Einführung Hardware-orientierte IT-Sicherheit: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden verstehen die Grundzüge und Konzepte von Hardware-orientierter IT-Sicherheit [Wissen, 6] *Kompetenz Fertigkeiten* Die Studierenden können das Bedrohungspotential von Hardware-orientierten Angriffen einschätzen, sowie geeignete Gegenmaßnahmen beurteilen. [Beurteilungsfähigkeit, 6] *Sozialkompetenz* Die Studierenden können Schwachstellen von Hardware-Komponenten aufzeigen und kommunizieren [Kommunikation, 6] *Selbstständigkeit* Die Studierenden können sich selbständig komplexe Problemstellungen der Hardware-orientierten IT-sicherheit erarbeiten [Eigenständigkeit/Verantwortung, 6]					

4	**Inhalte*:***
	Vorlesung & Seminar
	- Grundlagen der hardware-orientierten IT-Sicherheit
	- Einführung in Angriffsvektoren und Gegenmaßnahmen auf Hardware:
	  - Angriffe auf Kommunikationsschnittstellen
	  - Seitenkanal-Angriffe
	  - Fehler-Angriffe
	  - Hardwaretrojaner
	- Vorträge zu ausgewählten Themen der hardware-orientierten Sicherheit
	
	Empfohlene Literaturangaben:
	Ross Anderson, "Security Engineering - A Guide to Building Dependable Distributed Systems", Wiley Publishing, Inc., 2021
	
	Aaron Blum, Kevin Dillon, Brendan Egan, John Shegerian, Tammy Shegerian, "The Insecurity of Everything: How Hardware Data Security is Becoming the Most Important Topic in the World", Independently published, 2021					

5	**Teilnahmevoraussetzungen:** Programmierkenntnisse (C, optional Assembler), Digitale Logik, Rechnertechnik
6	**Prüfungsformen***:* Referat, 15 min.
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Bernhard Jungk Dozent(in): Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.18 xxxxx – Hardware-Sicherheitsmethoden

<table>
<tr><td colspan="7">Modul: Hardware-Sicherheits-Methoden</td></tr>
<tr><td colspan="2">Kennnummer
xxxxx</td><td>Work-load
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
5. + 7. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Hardware-Sicherheitsmethoden
Praktikum Hardware-Sicherheitsmethoden</td><td>Sprache
Deutsch oder Englisch</td><td>Kontakt-zeit
Vorlesung 2 SWS / 30h
Praktikum 2 SWS / 30h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung Hardware-Sicherheits-Methoden
Praktikum Hardware-Sicherheits-Methoden</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verstehen das Bedrohungspotenzial von hardware-orientierten Angriffen und verstehen die Notwendigkeit von entsprechenden Schutzmaßnahmen. [Wissen, 6]
Kompetenz Fertigkeiten
Die Studierenden können offensive Methoden der IT-Sicherheit auf Hardware-Komponenten anwenden und geeignete Gegenmaßnahmen identifizieren. [Instrumentelle Fertigkeiten, 6]
Die Studierenden können das Risiko von Angriffen auf Hardware-Komponenten im gesamtheitlichen Kontext der IT-Sicherheit betrachten und einordnen. [Systemische Fertigkeiten, 6]
Sozialkompetenz
Die Studierenden können in einem Team von IT-Sicherheitsexperten die hardware-orientierten IT-Sicherheitsthemen einbringen und sinnvoll ausgestalten. [Mitgestaltung, 6]
Selbstständigkeit
Die Studierenden können selbstständig Angriffsoberflächen erkennen, die aus methodischen und systematischen Fehlern entstehen. [Eigenständigkeit/Verantwortung, 6]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Vorlesung:
- Vertiefung der hardware-orientierten Angriffe und Gegenmaßnahmen
- Vorgehen zum Pentesting von Hardware-Komponenten
- Ausnutzung verschiedener Schwachstellen anhand von Prototypen-Hardware:
- Debugging-Schnittstellen
- Extraktion und Analyse des Binärcodes
- Angriffe auf Kommunikationsschnittstellen
- Seitenkanal-Angriffe</td></tr>
</table>

	- Fehler-Angriffe - Hardwaretrojaner - Gegenmaßnahmen: - Schutz gegen Reverse-Engineering-Maßnahmen - Verschlüsselung von Kommunikationsschnittstellen - Pairing von Hardware-Komponenten - Masking und Hiding-Grundzüge gegen Seitenkanal-Angriffe - Erkennung von und Umgang mit Fehler-Angriffen - Vertrauenswürdige Zulieferketten
	Empfohlene Literaturangaben: Jean-Georges Valle, "Practical Hardware Pentesting", Packt Publishing, 2021 Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods, "Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things", No Starch Press, 2021 Swarup Bhunia , "Hardware Security: A Hands-on Learning Approach", Morgan Kaufmann, 2018 Stefan Mangard, Elisabeth Oswald, Thomas Popp, "Power Analysis Attacks - Revealing the Secrets of Smartcards", Springer-Verlag, 2007 Cetin Kaya Koc, "Cryptographic Engineering", Springer-Verlag, 2008
5	**Teilnahmevoraussetzungen:** Programmierkenntnisse (C, Assembler), Digitale Logik, Rechnerarchitektur, Rechnertechnik
6	**Prüfungsformen***:* Klausur 90 min Praktikum unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Klausur erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik
9	***Modulverantwortliche(r):*** Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023

3.19 xxxxx – Sichere Digitale Schaltkreise

<table>
<tr><td colspan="8">Modul: Sichere Digitale Schaltkreise</td></tr>
<tr><td colspan="2">Kennnummer
xxxxx</td><td>Workload
150</td><td>Modulart
KM</td><td colspan="2">Studiensemester
5. + 7. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Sichere Digitale Schaltkreise
Praktikum Sichere Digitale Schaltkreise</td><td>Sprache
Deutsch oder Englisch</td><td>Kontakt-zeit
Vorlesung 2 SWS/ 30 h
Praktikum 2 SWS/30 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung Sichere Digitale Schaltkreise 2 SWS
Praktikum Sichere Digitale Schaltkreise 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verstehen die Grundzüge und Konzepte von Hardwarebeschreibungssprachen, von sicherem Hardwareentwurf und können übliche Schwachstellen erkennen und Gegenmaßnahmen entwerfen. [Wissen, 6]

Kompetenz Fertigkeiten
Die Studierenden können Hardwarebeschreibungssprachen nutzen, um kryptografische Verfahren und einfache Microcontroller zu implementieren. [Instrumentelle Fertigkeiten, 6]

Die Studierenden können ihr Wissen zur Hardwareentwicklung anwenden, um die Wirkweise von komplexen mikroarchitekturellen und ähnlichen hardware-orientierten Angriffen zu verstehen und entsprechende Angriffe in einen Gesamtkontext im Bereich IT-sicherheit einzuordnen [Systemische Fertigkeiten, 6]

Sozialkompetenz
Die Studierenden können komplexe Zusammenhänge der Hardware-Sicherheit zielgruppengerecht kommunizieren und die Problemstellungen kompetent erläutern. [Kommunikation, 6]

Selbstständigkeit
Die Studierenden können selbständig ihr erlerntes Wissen auf neue Themenfelder wie die Hardware-Entwicklung mittels Hardwarebeschreibungssprachen anwenden und dadurch sich neue Themenfelder erschließen. [Lernkompetenz, 6]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Vorlesung:
- Wiederholung von Basis-Wissen zu Hardwarebeschreibungssprachen, wie effiziente Kommunikationsprotokolle, Clock-Domain-Crossing, effiziente Hardware-Schnittstellen.
- Optimierungsverfahren: Pipelining, Sprungvorhersagen, Out-of-Order-Architekturen,Superskalare Architekturen, Serialisierung
- Effiziente Umsetzung von Krypto-Algorithmen in Hardware.
- Entstehung von Seitenkanal-Angriffsoberflächen durch Optimierungen und Cache-Hierarchien</td></tr>
</table>

	- Schutz vor Seitenkanal-Angriffen auf Hardware-Ebene Praktikum: - Entwicklung von integrierten Schaltkreisen zur Begleitung der Vorlesung. - Praktische Umsetzung auf einem FPGA-Entwicklungsboard.
	Empfohlene Literaturangaben: John Hennessy, David Patterson, "Computer Architecture - A Quantitative Approach", Morgan Kaufmann, 2017 David Patterson, John Hennessy, "Computer Organization and Design RISC-V Edition: The Hardware Software Interface", Morgan Kaufmann, 2021 Sarah Harris, David Harris, "Digital Design and Computer Architecture RISC-V Edition", Morgan Kaufmann, 2021 Donald Thomas, Philip Moorby, "The Verilog® Hardware Description Language", Springer-Verlag, 2008 Stefan Mangard, Elisabeth Oswald, Thomas Popp, "Power Analysis Attacks - Revealing the Secrets of Smartcards", Springer-Verlag, 2007 Cetin Kaya Koc, "Cryptographic Engineering", Springer-Verlag, 2008
5	**Teilnahmevoraussetzungen:** Einführung Chipdesign, Programmierkenntnisse (VHDL/Verilog, C, Assembler), Digitale Logik, Rechnertechnik
6	**Prüfungsformen***:* Klausur 90 min. Praktikum unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Klausur Erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Bernhard Jungk Dozent(in): Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** *2*3.01.2023

3.20 23422 – Social Engineering

Modul: Social Engineering						
Kennnummer 23422	**Workload** 150	**Modulart** KM	**Studiensemester** 5. + 7. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung / Seminar Social Engineering Übung Social Engineering	**Sprache** Deutsch oder Englisch	**Kontakt-zeit** Vorlesung / Seminar 2 SWS/30h Übung 2 SWS/30h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung & Seminar Social Engineering: 2 SWS Übung Social Engineering: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden verstehen die Grundzüge und Konzepte von Social Engineering und Ansätze zur Verteidigung dagegen [Wissen, 6] *Kompetenz Fertigkeiten* Die Studierenden können Cyberkriminalität unter Verwendung von Social Engineering Techniken erkennen und mit höherer Wahrscheinlichkeit vermeiden oder abwehren [Beurteilungsfähigkeit, 6] *Sozialkompetenz* Die Studierenden können komplexe Zusammenhänge aus der Fachliteratur zielgruppengerecht aufbereiten und auf deutsch oder englisch präsentieren [Kommunikation, 6] *Selbstständigkeit* Die Studierenden können sich selbstständig in internationale Fachliteratur einlesen und diese auf deutsch oder englisch präsentieren. [Eigenständigkeit/Verantwortung, 6]						
4	**Inhalte*:*** Vorlesung & Seminar - Basics of personality psychology - Building interpersonal trust and exploiting individual weakness - Principles and strategies in physical penetration testing - Success factors of phishing attacks, cognitive processes of phishing detection - Defence strategies against Social Engineering - Remote social engineering and IoT - Strategies and effect mechanisms of disinformation in cyberspace - Deep fake recognition - Microtargeting and decision-making - Conspiracy theories, disinformatin, extremism in cyberspace - Cognitive inoculation						

	- Insider threats: types, causes and detection
	Empfohlene Literaturangaben: D. Drechsler (Ed.) (2019). Schutz vor Social Engineering. Angriffspunkte und Abwehrmöglichkeiten in digitalwirtschaftlichen Ökosystemen. Erich Schmidt Verlag.
5	**Teilnahmevoraussetzungen:** keine
6	**Prüfungsformen***:* Hausarbeit
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Als mindestens ausreichend benotete Hausarbeit sowie ein erfolgreich absolviertes Kurzreferat
8	***Verwendbarkeit des Moduls:*** Bachelor Informatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Stefan Sütterlin Dozent(in): Prof. Dr. Stefan Sütterlin
10	***Optionale Informationen:*** -
11	***Bearbeitungsstand:*** 23.01.2023