Digital Business University of Applied Sciences

Cybersecurity & Management (MBA)

Modulhandbuch

Version: 06.2023

I. Vorwort

Der Masterstudiengang Cybersecurity & Management (Master of Business Administration) umfasst drei Studiensemester in Vollzeit mit insgesamt 90 ECTS-Kreditpunkten. Dieser Studiengang kann nach individueller Vereinbarung auch in Teilzeit studiert werden. Die Regelstudiendauer verlängert sich dabei nach Maßgabe der Studien- und Prüfungsordnung für den Studiengang.

Forschung, wissenschaftlich fundierte Theorien und deren Transfer für die Berufspraxis sind handlungsleitend für die inhaltliche Ausgestaltung wie auch das semi-virtuelle Lehr- und Lernkonzept. Das Anspruchsniveau entspricht in allen Modulen internationalen Standards.

Die Zugangsvoraussetzungen zum Studium sind in der Zulassungsordnung sowie in der Studien- und Prüfungsordnung in der jeweils gültigen Fassung festgelegt. Da es sich um einen weiterbildenden Masterstudiengang handelt, ist zusätzlich zum berufsqualifizierenden Abschluss eines Hochschulstudiums eine daran anschließende qualifizierte berufspraktische Erfahrung von mindestens einem Jahr nachzuweisen. Näheres regelt die jeweilige Studien- und Prüfungsordnung.

II. Berufsprofil

Im Zeitalter der digitalen Transformation nehmen Cyber-Angriffe immer mehr zu. Je vernetzter die Welt und je mehr Gerätschaften mit dem Internet verbunden sind, umso größer auch die Gefahren und Risiken. Dies bringt neue Herausforderungen mit sich, mit denen Unternehmen, aber auch NGOs und die öffentliche Verwaltung konfrontiert werden. Die Herausforderungen sind dabei nicht nur technischer Natur. Vielmehr gilt es, den Themenkomplex auch aus prozessualer sowie Management-Sicht, zu beurteilen. Damit gehen u.a. folgende Aufgaben einher:

- Cyber-Risiken ermitteln
- Maßnahmen planen und umsetzen
- Prozesse zur kontinuierlichen Überwachung und Verbesserung aufsetzen und administrieren

Insgesamt sollen also Cyber-Risiken minimiert und gleichzeitig Mitarbeitende sensibilisiert werden. Für diese Aufgaben bedarf es eines qualifizierten Nachwuchses, der Unternehmen dabei unterstützt, insbesondere den Bereich der Cybersecurity umfassend zu betrachten.

Der MBA-Studiengang Cybersecurity & Management hat sich die Ausbildung von Expert:innen zum Ziel gesetzt, die leitende, beratende oder selbständige Tätigkeiten im Bereich der Cybersecurity übernehmen. Der Studiengang fokussiert dabei auf den Bereich des Informationsmanagements mit Teilaspekten wie bspw. Audits, Informationssicherheits-Managementsysteme (ISMS) und InfoSec-Standards.

Nach dem Studium bieten sich den Absolvent:innen mit dem in diesem MBA-Studiengang erworbenen Kompetenzen zahlreiche Möglichkeiten für einen Karriereeinstieg oder -aufstieg im Bereich der Cybersecurity. Absolvent:innen des Masterstudiengangs Cybersecurity & Management (MBA) sind unter anderem in folgenden Positionen tätig:

- Chief Information Security Officer (CISO)
- Mitarbeiter:in / Leiter:in von Cybersecurity Projekten oder Abteilungen
- Enterprise Security Analyst
- Unternehmensberater:in mit Schwerpunkt Cybersecurity
- Produktmanager:in für IT-Sicherheitslösungen
- Gutachter:in für Cybersecurity

III. Studienziel

Der Cybersecurity kommt eine wesentliche Rolle bei Digitalisierungsvorhaben zu. Die Frequenz von Cyber-Angriffen, deren Intensität und Gefährdungspotenzial steigen mit dramatischer Geschwindigkeit. Aber auch die Regulierung für Cybersicherheit und Anforderungen von Gesetzgeber, Kund:innen, Lieferant:innen und Geschäftspartner:innen nehmen zu. Um diesen Anforderungen gerecht werden zu können, benötigen Organisationen zunehmend Spezialist:innen auf dem Gebiet der Cybersecurity.

Reine Informatikfachkenntnisse und technische Expertise reichen dafür nicht mehr aus. Vielmehr ist dediziertes Cybersecurity Spezial- und Querschnittswissen notwendig, um den sicheren digitalen Wandel in Unternehmen konstruktiv zu begleiten. Genau dieser Aspekt wird im MBA-Studiengang Cybersecurity & Management aufgegriffen, der neben der organisatorischen und juristischen Betrachtung von Cybersecurity auch verschiedene Managementaspekte verbindet. Der Studiengang bereitet somit ideal auf eine Übernahme verantwortungsvoller Aufgaben in der Cybersecurity vor.

Der MBA-Studiengang Cybersecurity & Privacy vermittelt eine umfassende Ausbildung mit hohem Praxisbezug. Neben Pflichtmodulen haben die Studierenden die Möglichkeit, durch Wahlmodule einzelne Themen in den folgenden Bereichen (Auszug) zu vertiefen:

- Einführung in die Kryptografie
- IT-Forensik
- IT-Management: TILv4
- Systemanalyse

Studierende sind nach dem Abschluss des Masterstudiengangs u.a. befähigt, mittels geeigneter Methoden und Instrumente strategische Entscheidungen in der Cybersecurity zu treffen und Transformationsprojekte in diesem Kontext umzusetzen.

Im anwendungsorientierten Studiengang Cybersecurity & Management (MBA) wird die Vermittlung von Fach- und Methodenkompetenzen im Bereich Cybersecurity ergänzt um die Vermittlung spezifischer Fach- und Methodenkompetenzen im Bereich Prozessmanagement sowie managementspezifischer Kompetenzen wie Projektmanagement und Mitarbeiterführung. Außerdem erwerben die Studierenden ein breites Spektrum an Selbst- und Sozialkompetenzen.

Die Absolventinnen und Absolventen des Studiengangs können u.a.

- geeignete Methoden und Instrumente für strategische Entscheidungen in der Cybersecurity beurteilen, auswählen und anwenden;
- sichere Informations-Architekturen entwickeln und beurteilen;
- Transformationsprojekte im Kontext der Cybersecurity begleiten und umsetzen;
- ethische und juristische Aspekte der Cybersicherheit identifizieren, geeignete Lösungskonzepte und -strategien auswählen und umsetzen;
- wissenschaftliche Erkenntnisse und Verfahren aus dem Bereich Cybersecurity & Management selbstständig anwenden und (weiter-)entwickeln;

- zentrale Herausforderungen der sicheren digitalen Transformation wissenschaftlich analysieren und kritisch reflektieren;
- komplexe und interdisziplinär angelegte Projekte unter Anwendung klassischer, hybrider und agiler Methoden erfolgsorientiert planen, organisieren und durchführen;
- (virtuelle) interdisziplinäre Teams verantwortungsvoll und effektiv führen sowie zielorientiert mit Personen aus verschiedenen Fachrichtungen, auch über digitale Medien, kommunizieren.

Der Studiengang eignet sich für Absolvent:innen mit einem ersten berufsqualifizierenden Hochschulabschluss einer beliebigen Fachrichtung im Umfang von mindestens 180 ECTS sowie einer mindestens einjährigen qualifizierten berufspraktischen Erfahrung. Insbesondere richtet sich der Studiengang auch an Berufstätige unterschiedlicher Branchen, die ihr Wissen im Bereich Cybersecurity & Management aufbauen und erweitern möchten.

IV. Übersicht über Module und Leistungsnachweise

vgl. Anlage 1 Studien- und Prüfungsordnung

Lfd. NR	Modul	Art der Lehr-veran-staltung	Zugangs-voraus-setzung	Art der Prüfungs-leistung	ECTS-Kredit-punkte
(PLAN-)SEMESTER 1					
01	Einführung in die Grundlagen der In-formationssicherheit	SK	Keine	ST	6
02	Rechtliche und ethische Aspekte der Cybersicherheit	SK	Keine	ST	6
03	Einführung in die Grundlagen von Audits, Reviews und Assessments	SK	Keine	K (120)	6
04	Enterprise Security Architecture	SK	03	ST	6
05	Cloud Computing & Cloud Security	SK	01	ST	6
(PLAN-)SEMESTER 2					
06	Grundlagen des IT-Managements	SK	Keine	SL/ST	6
07	Digital Leadership: Mitarbeitenden-führung im digitalen Zeitalter	SK	Keine	K (120)	6
08	Einführung Managementsysteme und InfoSec-Standards	SK	Keine	K (120)	6
09	Implementierung von Informationssi-cherheits- Managementsystemen (ISMS)	SK	05	SL/ST	6
10	Agiles Projektmanagement	SK	Keine	SL/ST	6
(PLAN-)SEMESTER 3					
11	Wahlpflichtmodul	s.u.	s.u.	s.u.	6
12	Advanced Research Methods	SK	Keine	SL/ST	6
13	Masterarbeit	M	Keine	MA	18
Gesamt					**90**

Art der Lehrveranstaltung:

M Masterarbeitsprojekt

L Lab (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativen Lernen)

PR Projekt (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf problemorientiertem Lernen anhand eines konkreten realen oder fiktiven Projektauftrages)

SK Semi-virtueller Kurs (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen)

Art der Leistung:

MA	Masterarbeit
K(xx)	Klausur mit Dauer in Minuten
SL	Studienbegleitende Leistungsnachweise
ST	Studienarbeit
uSL	unbenotete Studienleistung

WAHLPFLICHTMODULE

mögliche Wahlpflichtmodule im Studiengang Cybersecurity & Management (MBA)

vgl. Anlage 3 Studien- und Prüfungsordnung

Lfd. NR	Modul	Art der Lehr-veran-staltung	Zugangs-voraus-setzung	Art der Prüfungs-leistung	ECTS-Kredit-punkte
WP1	Einführung in die Kryptografie	SK	Keine	K (120)	6
WP2	IT-Forensik	SK	Keine	ST	6
WP3	IT-Management: TILv4	SK	Keine	ST	6
WP4	Systemanalyse	SK	Keine	ST	6

Art der Lehrveranstaltung:

M Masterarbeitsprojekt

L Lab (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf Wissensanwendung bzw. anwendungsorientiertem, situativen Lernen)

PR Projekt (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen mit besonderem Fokus auf problemorientiertem Lernen anhand eines konkreten realen oder fiktiven Projektauftrages)

SK Semi-virtueller Kurs (virtuelle Lehrveranstaltungen mit optionalen Präsenzphasen)

Art der Leistung:

MA Masterarbeit

K(xx) Klausur mit Dauer in Minuten

SL Studienbegleitende Leistungsnachweise

ST Studienarbeit

uSL unbenotete Studienleistung

V. Modulbeschreibungen

Die Studieninhalte sind übersichtlich in Module gebündelt; diese sind in ihrer Größe einheitlich (6 CP/ECTS) und auf Mindestgröße gebracht (vgl. European Communities: ECTS User´s Guide, Brussels 2015). Gemäß Musterrechtsverordnung §7 (Beschluss der Kultusministerkonferenz vom 07.12.2017) beinhalten die Modulbeschreibungen folgende Angaben

Credit Points/Workload	Benennung des Gesamtarbeitsaufwands und der Anzahl der zu erwerbenden Leistungspunkte für jedes Modul; Jedem Modul ist in Abhängigkeit vom Arbeitsaufwand für die Studierenden eine bestimmte Anzahl von ECTS-Leistungspunkten zuzuordnen.
Zeitrahmen	Mit dem Zeitrahmen ist festgelegt, in welchem Semester das Modul in den Studiengang eingeplant ist.
Dauer des Moduls	1 Semester
Häufigkeit	Festlegung, ob das Modul jedes Semester, jedes Studienjahr oder nur in größeren Abständen angeboten wird;

Qualifikationsziele: Lern- und Qualifikationsziele, die sich an der definierten Gesamtqualifikation (angestrebter Abschluss) ausrichten; Qualifikationsziele beschreiben das Wissen, die Fähigkeiten und Fertigkeiten der Studierenden, die sie zum berufsbezogenen Handeln befähigen.

Inhalte: Fachliche, methodische, fachpraktische und fächerübergreifende Inhalte dem betreffenden Modul bearbeitet werden.

Voraussetzungen für die Teilnahme: Unter den Voraussetzungen für die Teilnahme sind die Kenntnisse, Fähigkeiten und Fertigkeiten für eine erfolgreiche Teilnahme und Hinweise für die geeignete Vorbereitung durch die Studierenden zu benennen.

Verwendbarkeit: Es wird dargestellt, welcher Zusammenhang mit anderen Modulen desselben Studiengangs besteht und inwieweit es zum Einsatz in anderen Studiengängen geeignet ist.

Lehr- und Lernformen: Die Umsetzung des semi-virtuellen Studienkonzeptes in Bezug auf das Modul wird beschrieben.

Basisliteratur: Die Basisliteratur ist als Einstiegsempfehlung genannt und wird regelmäßig aktualisiert.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten: Prüfungsart, -dauer, -umfang werden beschrieben; sie können auf Antrag der bzw. des Lehrenden an den Prüfungsausschuss mit dessen Zustimmung geändert werden.

01 Einführung in die Grundlagen der Informationssicherheit

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die Grundlagen der Informationssicherheit und deren Einführung.
- Sie haben ein grundsätzliches Verständnis davon, was zur Einführung von Informationssicherheit auf Basis des internationalen Standards für Informationssicherheitsmanagementsysteme, ISO/IEC 27001, notwendig ist.
- Sie können auftretende Herausforderungen bei der Einführung von Informationssicherheit erkennen.

Inhalte

- Überblick zu den normativen Elementen des ISO/IEC 27001
- Der Managementsystemzyklus auf Basis des P-D-C-A
- Diskussion und Abgrenzung des Begriffs “Asset” aus Sicht der Informationsverarbeitung / Informationssicherheit
- Informationssicherheit, Sicherheitsziele und -strategien, Informationssicherheitsmanagementprozess
- Abgrenzung IT-Sicherheit vs. Informationssicherheit
- Gegenüberstellung der Standards ISO/IEC 27001 auf Basis von IT-Grundschutz (BSI, Bonn) vs. ISO/IEC 27001
- Stand und Entwicklung der Normenfamilie ISO/IEC 270XX (XX= 1,2,3,4,5..)
- Abgrenzung: Informationsmanagementsystem (IMS), Informationssicherheitsmanagementsystem (ISMS), IT Service Management (ITSM)
- Analysen von Schwachstellen und Bedrohungen in Abhängigkeit von Assets

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)

- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Kersten, H., Klett, G., Reuter, J. & Schröder, K. W. (2019). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Publishing.
- Humphreys, E. & Plate, A. (2013). *Are You Ready for an ISMS Audit Based on 27001?* BSI British Standards Institution.
- Benner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H. & Schaaf, T. (2019). *Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm DIN ISO/IEC 27001:2017*. Carl Hanser Verlag.
- Sowa, A. (2017). *Management Der Informationssicherheit: Kontrolle Und Optimierung*. Springer Vieweg.
- Schneier, B. (2009). *Schneier on Security*. Wiley.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienarbeit (100%)

02 Rechtliche und ethische Aspekte der Cybersicherheit

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen ausgewählte Gesetze, die maßgeblich das Arbeitsumfeld der Cybersicherheit prägen.
- Die Studierenden können selbständig Arbeitskonflikte in der Cybersicherheit erkennen und thematisch zuordnen.
- Die Studierenden sind in der Lage, grundlegende ethische Aspekte der Cybersicherheit zu identifizieren und zu diskutieren.

Inhalte

- Datenschutzgrundverordnung
- §202 StGB (“Hackerparagraf”)
- Telekommunikationsgesetze
- Sozialgesetzbuch
- IT Sicherheitsgesetz / BSI Gesetz
- SEC Disclosure Guidance No 7
- Ethische Aspekte der Cybersicherheit (z.B. Überwachung versus Datenfreiheit)
- FDA und andere internationale Regularien

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Christen, M., Gordijn, B. & Loi, M. (2020). *The Ethics of Cybersecurity (The International Library of Ethics, Law and Technology (21))* (1st ed. 2020 Aufl.). Springer.
- Vedder, A., Schroers, J., Ducuing, C. & Valcke, P. (2019). *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security (7) (KU Leuven Centre for IT & IP Law Series)* (First Aufl.). Intersentia.
- Schneier, B. (2009). *Schneier on Security*. Wiley.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienarbeit (100%)

03 Einführung in die Grundlagen von Audits, Reviews und Assessments

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die grundlegenden Auditprinzipien sowie die ethischen und fachlichen Anforderungen an Auditor:innen.
- Sie können zwischen den verschiedenen Auditarten und Reviews unterscheiden und wissen, wann welche Auditart von Relevanz ist.
- Sie können sowohl interne wie externe Audit Programme planen, erstellen und koordinieren.
- Sie sind in der Lage, selbständig Audits durchzuführen.
- Sie kennen die Dokumentationsanforderungen im Rahmen von Audits sowohl aus Sicht von Auditierenden als auch aus Sicht von Auditierten.
- Sie sind in der Lage, einen Auditbericht zu strukturieren und zu verfassen.
- Sie sind mit der Fragetechnik im Rahmen von Audits vertraut und können diese bewusst und selbständig anwenden.

Inhalte

- Begriffsbestimmungen und Abgrenzungen im Kontext Audit, Review und Assessment
- Auditmethoden
- Umgang mit Feststellungen/Abweichungen
- Leiten und Lenken eines Auditprogramms
- Auditdurchführung
- Abschließen des Audits
- Durchführung von Auditfolgemaßnahmen
- Kompetenzen von und Bewertungen durch Auditor:innen

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)

- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- DIN EN ISO 17021:-1:2015-11
- DIN EN ISO 19011:2018-10
- DIN EN ISO/IEC 27000:2020-06
- Kersten, H., Klett, G., Reuter, J. & Schröder, K. W. (2019). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Publishing.
- Humphreys, E. & Plate, A. (2013). *Are You Ready for an ISMS Audit Based on 27001?* BSI British Standards Institution.
- Benner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H. & Schaaf, T. (2019). *Praxis-buch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm DIN ISO/IEC 27001:2017*. Carl Hanser Verlag.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

Klausur (120 Minuten)

04 Enterprise Security Architecture (ESA)

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden können Enterprise (Security) Architecture Management auf die Zusammenhänge von Software- und Organisationsentwicklung anwenden.
- Die Studierenden können IT Sicherheits-Systemlösungen entwickeln und auf sich verändernde Geschäftsprozesse anwenden.
- Die Studierenden haben ein Verständnis dafür, wie technologische Fortschritte in Sicherheitsarchitekturen umgesetzt werden können.
- Sie können den Einfluss von Sicherheitsarchitekturen auf diverse Stakeholder, wie Mitarbeiter, Kunden und Lieferanten beurteilen.
- Die Studierenden sind in der Lage, die erworbenen Kenntnisse in Form von methodischen Ansätzen zur Weiterentwicklung von Organisationen und Architekturen einzusetzen.
- Die Studierenden sind in der Lage, Funktionen und die entsprechende Governance von ESA zu beschreiben und anzuwenden.
- Sie kennen verschiedene Rahmenwerke und sind in der Lage, für die jeweilige Aufgabenstellung das jeweils angemessene Rahmenwerk zu selektieren und anzuwenden.

Inhalte

- Grundlagen von Enterprise Security Architecture als integraler Bestandteil der Enterprise Architecture
- Grundlagen und Einsatz von ESA/ EA Frameworks: Vorstellung zentraler Grundideen von Rahmenwerken und Diskussion an Beispielen
- IT-Anwendungsportfoliomanagement
- Architektur-Governance
- Modellierung von Unternehmenssicherheitsarchitekturen
- Querschnittsaufgaben und Zusammenhänge zur Unternehmensarchitektur
    - IT Service Management
    - IT Governance mit Hilfe von COBIT®

Voraussetzungen für die Teilnahme

Modul 03

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Dern, G. (2009). *Management Von It Architekturen: Leitlinien für die Ausrichtung, Planung und Gestaltung von Informationssystemen* (3. Aufl.). Springer Vieweg.
- Weill, P. & Ross, J. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Review Press.
- Hanschke, I. (2010). *Strategisches Management der IT-Landschaft. Ein praktischer Leitfaden für das Enterprise Architecture Management.* (2. Aufl.). Carl Hanser Verlag.
- Keller, W. (2012. *IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung.* (2. Aufl.). (2012). dpunkt.verlag.
- Keuntje, J. H. & Barkow, R. (2010). *Enterprise-architecture-Management in der Praxis. Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen.* Symposion.
- Ross, J. W., Weill, P. & Robertson, D. (2006). *Enterprise Architecture As Strategy: Creating a Foundation for Business Execution*. Harvard Business Review Press.
- Schwarzer, B. (2009). *Einführung in das Enterprise Architecture Management. Verstehen - Planen - Umsetzen*. Books on Demand.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Studienarbeit (100%)

05 Cloud Computing & Cloud Security

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden sind in der Lage, unterschiedliche Cloud Service Modelle zu differenzieren (PaaS, SaaS, IaaS).
- Sie verstehen die Differenzierung zwischen Public Cloud, Private Cloud und Hybrid Cloud.
- Sie sind in der Lage, wesentliche Elemente der Cloud Security für vorliegende Liefer-Situationen selbständig zu erkennen, auf die jeweilige Liefersituation anzupassen und zu designen.
- Die Studierenden kennen wesentliche technische Komponenten der Cloud Security, wie z.B. CASBs, Klassifizierungstechnologien, Verschlüsselungstechnologien, Cloud-based Directory Services.
- Sie kennen wesentliche Standards in der Auditierung von Cloud Services (z.B. Star Audit, ISO/IEC 27018, …).

Inhalte

- Grundlagen und Begriffe zu Cloud Services
- Cloud Service Modelle:
  - IaaS
  - PaaS
  - SaaS
- Cloud Delivery Modelle:
  - Public
  - Hybrid
  - Private
- Cloud Security Komponenten
- Audit Standards für Cloud Computing
- Security Controls für Cloud Computing
- Cloud Access Security Broker
- Directory Technologien
- Verschlüsselungssoftware für die Cloud

Voraussetzungen für die Teilnahme

Modul 01

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Krcmar, H., Leimeister, J. M., Roßnagel, A. & Sunyaev, A. (2016). *Cloud-Services aus der Geschäftsperspektive*. Springer Publishing.
- Jr., M. G. B. & Jackson, K. L. (2016). *Practical Cloud Security: A Cross-Industry View*. CRC Press.
- Dotson, C. (2019). *Practical Cloud Security: A Guide for Secure Design and Deployment*. O'Reilly Media.
- Information Resources Management Association. (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications*. IGI Global.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

Studienarbeit (100%)

06 Grundlagen des IT Managements

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden erlangen einen grundlegenden Einblick in das IT Management als Grundlage für den IT Betrieb. Sie verstehen die sich daraus ableitenden Anforderungen an die Cybersicherheit.
- Die Studierenden sind in der Lage, die IT Infrastructure Library (ITIL) als Grundlage von allgemeinen Management- und Service-Management-Praktiken anzuwenden.
- Sie können eigenständig einfache IT Management Aufgaben identifizieren, klassifizieren und Lösungen ableiten.

Inhalte

- Aufbau von ITIL
- Allgemeine Management-Praktiken
- Service-Management-Praktiken
- SLA und OLA Definition
- Problem Management und Incident Management
- CMDB und DHL
- IT Accounting und Auswirkung auf Transfer Pricing

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Urbach, N. & Ahlemann, F. (2016). *IT-Management im Zeitalter der Digitalisierung*. Springer Publishing.
- Hoch, D. J., Klimmer, M. & Leukert, P. (2005). *Erfolgreiches IT-Management im öffentlichen Sektor: Managen statt verwalten*. Gabler Verlag.
- Tiemeyer, E. (2020). *Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis*. Carl Hanser Verlag.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)

- studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)

07 Digital Leadership: Mitarbeitendenführung im digitalen Zeitalter

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die Unterschiede und Zusammenhänge der Konzepte Management, Führung und Leadership im digitalen Zeitalter.
- Sie haben einen Überblick über Anforderungen an Führungskräfte, insbesondere im Bereich der Personalentwicklung im digitalen Zeitalter und kennen Ansätze, Methoden und Tools zu deren Bewältigung.
- Sie kennen im Kontext der Digitalisierung relevante Führungstheorien (wie z.B. Full Range Leadership, Emergent Leadership) und können diese auf konkrete Führungssituationen anwenden.
- Die Studierenden sind mit den Grundlagen und wichtigen Instrumenten der Teamführung vertraut und können insbesondere die Herausforderungen der Führung virtueller Teams reflektieren und diesen mit konkreten Lösungsansätzen begegnen.
- Sie kennen grundlegende Prinzipien, Elemente und Instrumente von agilen Führungsansätzen und können diese für die Führung von Mitarbeitenden nutzen.
- Die Studierenden erfassen die Bedeutung von Emotionen im Führungskontext und können das Konzept der Emotionalen Intelligenz auf Führungssituationen anwenden.

Inhalte

- Definition und Abgrenzung von Management, Führung und Leadership
- Wissenschaftliche Führungstheorien und ihre Relevanz für Führung im Zeitalter der Digitalisierung
    - Leadership Mindset im Licht eigenschaftsorientierter Führungstheorien
    - Transaktionale, Transformationale Führung und das Full Range Leadership Modell
    - Emergent Leadership
    - Situative Führungsansätze und das Konzept des Ambidextrous Leadership
- Personenentwicklungsmaßnahmen im digitalen Zeitalter
    - Herausforderungen und Chancen
    - Einfluss von Technologien
    - Tools und Methoden
- Führung von (virtuellen) Teams
    - Grundlagen und aktuelle Erkenntnisse der Team-Führung
    - Besonderheit und Herausforderungen bei der Führung virtueller Teams
    - Techniken und Instrumente zur Führung virtueller Teams
- Mitarbeiterführung in agilen Arbeitswelten
    - Rolle der Führungskraft im agilen Management

    - Coaching und Steuerung autonomer Teams
    - Techniken und Instrumente der agilen Mitarbeiterführung
- Grundlagen von Emotional Leadership
    - Bedeutung von Emotionen in der Mitarbeitendenführung
    - Konzept der emotionalen Intelligenz inkl. kritischer Reflektion der Grundlagen und Grenzen
    - Implikationen für die Führung von Mitarbeitenden

Voraussetzungen für die Teilnahme
Keine

Verwendbarkeit
- Cybersecurity & Management (MBA)
- Digital Business Management (M.Sc.)
- Data Science & Management (M.Sc.)

Lehr- und Lernformen: semi-virtueller Kurs
- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Übungen auf der Online-Lernplattform (z.B. Quizzes, individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Bass, B.M. & Bass, R. (2008). *The Bass Handbook of Leadership: Theory, Research, and Managerial Applications* (4. Auflage). New York: Free Press
- Bergiel, B.J., Bergiel, E.B. & PW Balsmeier (2008). Nature of virtual teams: A summary of their advantages and disadvantages. *Management Research News*, 3, 99-110.
- Bartol, Kathryn & Liu, Wei. (2002). Information technology and human resources management: Harnessing the power and potential of netcentricity. *Research in Personnel and Human Resources Management*, 21, 215-242. Doi 10.1016/S0742-7301(02)21005-1.
- Cortellazzo, L., Bruni, E., Zampieri, R. (2019). The Role of Leadership in a Digitalized World: A Review. *Frontiers in Psychology, 10*, 1938 Doi 10.3389/fpsyg.2019.01938
- Domsch, M., Regnet, E., Rosenstiel, L v. (2018). *Führung von Mitarbeitern: Fallstudien zum Personalmanagement*. 4. Aufl., Schäffer-Poeschl: Stuttgart
- Holtbrügge, D. (2018). *Personalmanagement* (7. Auflage). Berlin, Heidelberg: Springer
- Goleman, D. (1998). What Makes A Leader. *Harvard Business Review*, 76 (6), 93-102.
- Google (2018). *Understand team effectiveness.* (Abrufbar unter: https://rework.withgoogle.com/guides/understanding-team-effectiveness)
- Petry, T. (2016). *Digital Leadership: Erfolgreich Führen in Zeiten der Digital Economy.* Freiburg: Haufe.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Klausur (120 Minuten) (100%)

08 Einführung Managementsysteme und InfoSec-Standards

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	1. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen verschiedene Managementsystem- und Sicherheitsstandards.
- Sie können, je nach Anwendungssituation, einen angemessenen Sicherheitsstandard auswählen und einsetzen.
- Die Studierenden sind in der Lage eigene Managemenstsysteme zu implementieren und zu betreiben.
- Sie können Synergieeffekte durch den Einsatz der unterschiedlichen Managementsystemen erkennen und nutzen.
- Die Studierenden sind in der Lage, Sicherheitsstandards in etablierten Managementsystemen zu verwenden.

Inhalte

- ISO/IEC 27000 Familie
- ISO/IEC 22301
- ISO/IEC 20000
- ISO/IEC 9000
- ISO/IEC 14000
- ISO/IEC 15000
- BSI Grundschutz auf Basis ISO/IEC 27001

Voraussetzungen für die Teilnahme

keine

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Kersten, H., Klett, G., Reuter, J. & Schröder, K. W. (2019). IT-Sicherheitsmanagement nach der neuen ISO 27001. Springer Publishing.
- Benner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H. & Schaaf, T. (2019). Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm DIN ISO/IEC 27001:2017. Carl Hanser Verlag.
- Sowa, A. (2017). Management Der Informationssicherheit: Kontrolle Und Optimierung. Springer Vieweg.
- Eckert, C. (2018). IT-Sicherheit. De Gruyter.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Klausur (120 Minuten)

09 Implementierung von Informationssicherheits-Managementsystemen (ISMS)

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen Good Practices, Risiken sowie die kritischen Erfolgsfaktoren für die Implementierung von Managementsystemen.
- Sie kennen die gängigen Schritte bei der Einführung von Managementsystemen und können einen konkreten Plan zur Implementierung eines Managementsystems entwerfen.
- Die Studierenden sind in der Lage, ein Managementsystem mit seinen Prozessen und Strukturen unter Berücksichtigung der jeweiligen Gegebenheiten und Anforderungen von Organisationen zu planen.
- Sie können eigenständig das Managementsystem mit seinen Prozessen und Strukturen in einer Organisation implementieren und betreiben.
- Sie sind befähigt, die Performance des Managementsystems zu messen, zu bewerten und kontinuierlich zu verbessern.

Inhalte

- Grundlagen der Implementierung von Managementsystemen anhand von Praxisbeispielen (Good Practices, Risiken und Fallstricke, kritische Erfolgsfaktoren, etc.)
- Projektplanung zur Implementierung eines Managementsystems am Beispiel eines ausgewählten Managementsystems wie z.B. Informationssicherheits-Managementsystem (ISMS)
- Planung der Prozesse und Strukturen eines Managementsystems am Beispiel eines ausgewählten Managementsystems
- Implementierung und Betrieb von Prozessen und Strukturen eines Managementsystems am Beispiel eines ausgewählten Managementsystems
- Messung, Bewertung und Verbesserung der Performance eines Managementsystems am Beispiel eines ausgewählten Managementsystems

Voraussetzungen für die Teilnahme

Modul 05

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform

- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- BSI Grundschutzkatalog (in der jeweils aktuellsten Version. Online)
- Kersten, H., Klett, G., Reuter, J. & Schröder, K. W. (2019). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Publishing.
- Benner, M., Felde, N., Hommel, W., Metzger, S., Reiser, H. & Schaaf, T. (2019). *Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm DIN ISO/IEC 27001:2017*. Carl Hanser Verlag.
- Sowa, A. (2017). *Management Der Informationssicherheit: Kontrolle Und Optimierung*. Springer Vieweg.
- Clader, A. (2016). *Nine Steps to Success: An ISO 27001 Implementation Overview*. IT Governance Limited.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

- studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)

10 Agiles Projektmanagement

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	2. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden kennen die Grundlagen und Begriffe des klassischen und des agilen Projektmanagements. Sie kennen zentrale agile Methoden und deren Vorgehensweise sowie korrespondierende agile Tools und Techniken.
- Sie sind in der Lage, klassische und agile Projektmanagementmethoden in der Praxis anzuwenden.
- Die Studierenden haben ein Grundverständnis von Agilität und damit zusammenhängenden Werten und Prinzipien. Sie verstehen, wie Agilität im Projektmanagement förderlich eingesetzt werden kann.
- Die Studierenden kennen die Rollen und Verantwortlichkeiten in der agilen Projektarbeit (insb. Scrum) und können diese aktiv in der Praxis anwenden. Sie sind in der Lage, Projekte erfolgreich zu leiten und entsprechende Arbeitspakete zu übernehmen.
- Die Studierenden kennen hybride Formen des Projektmanagements. Sie sind in der Lage, klassische Projektmanagement-Ansätze auch in komplexen Umwelten zu nutzen und sie mit agilen Techniken zu verknüpfen.
- Die Studierenden kennen agile Veranstaltungsformate. Sie sind dazu fähig, die Transformation einer Organisation zu mehr Agilität und Dynamik erfolgreich mitzugestalten.

Inhalte

- Grundlagen und klassisches Projektmanagement
- Agiles Projektmanagement
  - Agilität im Kontext des Projektmanagements, agile Werte und Prinzipien
  - Agile Methoden und Vorgehensweisen (z.B. Scrum, Kanban, Lean-Startup)
  - Rollenverständnisse und korrespondierende Verantwortungsbereiche in agilen Methoden (insb. Scrum)
  - Agile Tools und Arbeitstechniken (z.B. User Stories, Epics, Persona, Planungspoker, Story- und Valuepoint Schätzung, Timeboxing, Daily Standup, Taskboarding, Definition of Done, Burn Down Charts)
  - Agiles Controlling und Qualitätsmanagement
- Hybrides Projektmanagement
  - Begriffsklärung
  - Formen und Vorgehensweisen
- Agile Veranstaltungsformate (z.B. Google Design Sprint, Hackathon, FedEx days, Rotation Days, FedEx Meetings, Barcamp, ThinkTank)

- Umsetzung konkreter Projektaufgaben an Hand agiler und hybrider Ansätze

Voraussetzungen für die Teilnahme
keine

Verwendbarkeit
- Digital Business Management (M.Sc.)
- Data Science & Management (M. Sc.)
- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs
- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Adkins, L. (2010). Coaching Agile Teams: A Companion for ScrumMasters, Agile Coaches, and Project Managers in Transition. Addison-Wesley Professional.
- Graf, N., Gramß, D. & Edelkraut, F. (2019). Agiles Lernen: Neue Rollen, Kompetenzen und Methoden im Unternehmenskontext (2. Aufl.). Haufe.
- Kuster, J., Bachmann, C., Huber, E., Hubmann, M., Lippmann, R., Schneider, E., Schneider, P., Witschi, U. & Wüst, R. (2019). Handbuch Projektmanagement: Agil – Klassisch – Hybrid (4. Aufl.). Springer.
- Poguntke, S. (2014). Corporate Think Tanks: Zukunftsgerichtete Denkfabriken, Innovation Labs, Kreativforen & Co. Springer.
- Timinger, H. (2017). Modernes Projektmanagement: Mit Traditionellem, Agilem Und Hybridem Vorgehen Zum Erfolg. Wiley.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
- Studienbegleitende Leistungsnachweise (50%)
- Studienarbeit (50%)

11 Wahlpflichtmodul

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Siehe Beschreibung der Wahlpflichtmodule

12 Advanced Research Methods

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden haben ein fundiertes Verständnis von gängigen und fortgeschrittenen Methoden der empirischen Sozialforschung. Sie können qualitative und quantitativer Methoden entsprechend der wissenschaftlichen Fragestellung auswählen.
- Sie können geeignete Methoden der empirischen Sozialforschung, der Befragung, Beobachtung, quantitativ und qualitativer Methoden im Feld und im Labor, sowie der experimentellen Methoden auswählen und anwenden.

Inhalte

- Relevanz und Güte wissenschaftlicher Methoden
- Qualitative versus quantitative Methoden der Sozial- und Wirtschaftsforschung
- Erstellung von Studiendesigns, Skalenbildung, Methoden der Stichprobenauswahl
- Qualitative Forschungsmethoden (Tiefen- und Experteninterviews, Gruppendiskussionen, Ethnografische Beobachtungsstudien)
- Qualitative Analysemethoden (Inhaltsanalyse nach Mayring)
- Quantitative Forschungsmethoden (Befragungen, Beobachtungen, Experiment)
- Univariate und multivariate Analysemethoden (Regressionsanalyse, Einfaktorielle und multifaktorielle Varianzanalyse, Cluster- und Faktorenanalyse)
- Kritische Reflexion von Studienergebnissen und Integration in den bestehenden wissenschaftlichen Diskurs

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Data Science & Management (M.Sc.)
- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden

- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Backhaus, K. Erichson, B., Plinke, W. & Weiber, R. (1994). *Multivariate Analysemethoden. Eine anwendungsorientierte Einführung* (11. überarbeitete Auflage). Berlin: Springer.
- Baur, N. & Blasius, J. (2019). *Handbuch Methoden der empirischen Sozialforschung.* Wiesbaden: Springer Vieweg.
- Fahrmeir, L., Heumann, C., Künstler, R., Pigeot, I. & Tutz, G. (2016). *Statistik.* Springer Berlin Heidelberg.
- Mayring, P. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12. Auflage). Weinheim: Julius Beltz.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)

- studienbegleitende Leistungsnachweise (40%)
- Studienarbeit (60%)

13 Masterarbeit

Credit Points/Workload	18 CP (ECTS) / 450 Stunden Selbstlernzeit: 450 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden können das im Masterstudiengang erworbene Wissen für die Bearbeitung einer ausgewählten Problemstellung nutzen.
- Sie können eine wissenschaftliche Fragestellung aus dem gewählten Themenbereich selbstständig unter Berücksichtigung des aktuellen Forschungsstandes und unter Berücksichtigung der Regeln wissenschaftlichen Arbeitens innerhalb einer vorgeschriebenen Zeit bearbeiten.
- Die Studierenden sind dazu in der Lage zu beurteilen, welche methodologischen Zugänge bzw. wissenschaftlichen Forschungsmethoden für die Bearbeitung einer selbst gewählten Fragestellung geeignet sind. Sie können diese praxisbezogen anwenden.
- Sie können die gewonnenen Erkenntnisse beschreiben und bewerten, sie in den Forschungsstand einordnen und den Forschungsprozess kritisch reflektieren.
- Sie können den gewählten wissenschaftlichen Standpunkt sowie die verwendeten Methoden und gewonnenen Ergebnisse logisch ableiten, schriftlich darlegen und argumentativ verteidigen.
- Die Studierenden sind dazu in der Lage, einen Beitrag zum Theorie-Praxis-Transfer zu leisten und das während des Studiums erworbene disziplinäre Wissen in die berufliche Praxis zu integrieren.

Inhalte

- Eigenständige Bearbeitung einer wissenschaftlichen Problemstellung
- Kritische Reflexion des Forschungsstandes.

Voraussetzungen für die Teilnahme

Keine

Verwendbarkeit

- Digital Business Management (M.Sc.)
- Data Science & Management (M.Sc.)
- Cybersecurity & Management (MBA)

Lehr- und Lernformen:

- eigenständiges Verfassen einer Masterarbeit
- individuelle Begleitung bei Themenauswahl und methodischem Vorgehen durch Fachbetreuer:innen

Basisliteratur

- Themenspezifische Fachliteratur wird in der Lehrveranstaltung bekannt gegeben.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten
(Prüfungsart, -dauer, -umfang)
Masterarbeit (100%)

Wahlpflichtmodule (Auszug)

WP1 Einführung in die Kryptografie

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

Qualifikationsziele

- Die Studierenden verstehen die mathematischen Grundlagen der Kryptographie.
- Sie verstehen die Prinzipien von Public und Secret-Key-Verschlüsselung sowie der relevanten Verfahren einschließlich ihrer Sicherheit und Effizienz.
- Die Studierenden kennen die Prinzipien digitaler Signaturen und der relevanten Verfahren einschließlich ihre Sicherheit und Effizienz.
- Die Studierenden kennen die grundlegenden symmetrischen Verschlüsselungssystemen in der Praxis, sowie die Grundlagen der asymmetrischen Kryptographie insbesondere das weitverbreitete RSA-Kryptosystem und die wichtigsten Ersätze der asymmetrischen Methoden (Diffie-Hellman und elliptische Kurven).
- Sie können die Grundlagen den Quantenkryptografie erklären.

Inhalte

- Mathematische Grundlagen:
  Berechnungen in Kongruenz- und Restklassenringen; Faktorisierung großer Zahlen; Wahrscheinlichkeit; Modulare Arithmetik; Euklidischer Algorithmus; Endliche Felder; Faktorisierung großer Zahlen; Diskrete Logarithmen; Chinesischer Restsatz; Quadratischer Rest; Elliptische Kurven
- Grundlagen der Verschlüsselung:
  Geschichte der Kryptologie; Symmetrische vs. Asymmetrische Kryptosysteme; Block- und Stromchiffren; Kryptanalyse; Verschlüsselung mit öffentlichen Schlüsseln; RSA, Diffie-Hellman, ElGamal; Message Authentication Codes bzw.kryptographische Prüfsummen; Digitale Signaturen; Identifikation; Monoalphabetische Substitution; Struktur des Restklassenrings Z/mZ; Randomisierte Homophonie; Vigenere-Verschlüsselung, Kappa- und Phi-Index; Zweifache klassische Vigenere-Verschlüsselung; Zylinder und Rotoren; Vernam-Chiffrierung, One-Time-Pad; Pseudo-Zufalls-Generatoren; Data-Encryption-Standard (DES); Advanced-Encryption-Standard (AES); IDEA-Algorithmus; Huffman-Codes; Lempel-Ziv-Kompression; Kryptographie-Verfahren; Primzahltests; Faktorisierungs-Algorithmen; Message Digests, RSA-Signatur; RC5-Algorithmus, RSA-Challenge 1997; Diffie-Hellman Schlüssel-Vereinbarung; ElGamal-Signatur, DSS (Digital Signature Standard)

Empfohlene Voraussetzungen für die Teilnahme:
keine

Verwendbarkeit

- Cybersecurity & Management (MBA)

Lehr- und Lernformen: semi-virtueller Kurs

- Lernvideos, (digitale) Arbeitsmaterialien und wissenschaftliche Literatur (eBooks, e-Journals) auf der Online-Lernplattform
- studienbegleitende Anleitungen und Unterstützung auf der Online-Lernplattform (z.B. individuelle Aufgabenbearbeitung, Beiträge in Gruppenforen)
- Virtuelle Kommunikation & Kollaboration (synchron, asynchron) in Foren, Chats und virtuellen Konferenzen und Online-Sprechstunden
- eine zwei-tägige Präsenzphase: Interaktive individuelle und kollektive Aufarbeitung und Vertiefung von Lerninhalten

Basisliteratur

- Buchmann, J. (2010). *Einführung in die Kryptographie* (5. Aufl.). Springer.
- Paar, C. & Pelzl, J. (2016). *Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender*. Springer Vieweg.
- Rogaway, P. & Bellare, M. (2005). *Introduction to Modern Cryptography*. Lecture Notes. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf
- Buchmann, J. (2010). *Einführung in die Kryptographie* (5. Aufl.). Springer.
- Schneier, B. (2015). *Secrets and Lies: Digital Security in a Networked World*. Wiley.

Voraussetzungen für die Vergabe von ECTS-Leistungspunkten

(Prüfungsart, -dauer, -umfang)
Klausur (120 Minuten) (100%)

WP2 IT-Forensik

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

WP3 IT-Management: TILv4

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr

WP4 Systemanalyse

Credit Points/Workload	6 CP (ECTS) / 150 Stunden Lehrveranstaltungsstunden: 30 Stunden Selbstlernzeit: 120 Stunden
Zeitrahmen	3. Semester
Dauer des Moduls	1 Semester
Häufigkeit	Mindestens einmal pro Studienjahr