Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modulhandbuch

Fakultät Informatik
Studiengang Business and Security Analytics

StuPO 18.2
ab Wintersemester 2021/22
Ersteller: Prof. Dr. German Nemirovski, Studiendekan
Verantwortlich: Prof. Dr. German Nemirovski, Studiendekan

Inhaltsverzeichnis

1 Vorwort 3
2 Qualifikationsziel-Modul-Matrix 5
3 Studiengangs-Kompetenzmatrix 7
4 Modulbeschreibungen 8
4.1 1. Semester 8
4.1.1 51200 – Data and Web Mining 8
4.1.2 51300 – Large Scale Data Analysis and Parallelization 10
4.1.3 51500 – Strategic IT Management 12
4.1.4 51700 – Incident Response und Malware Defence 16
4.1.5 xxxxx – Wahlpflichtmodul 1a / Wahlpflichtmodul 1b 19
4.2 2. Semester 21
4.2.1 52100 – Business Process Management and Data Compliance 21
4.2.2 52200 – Advanced Statistic 25
4.2.3 52500 – Innovation and Transfer Competence 27
4.2.4 52700 – Security Analytics 29
4.2.5 xxxxx – Wahlpflichtmodul 2a / Wahlpflichtmodul 2b 31
4.3 3. Semester 33
4.3.1 60100 – Master-Thesis 33
4.3.2 60200 – Mündliche Masterprüfung 35

1 Vorwort

Der Masterstudiengang Systems Engineering ist ein praxisorientierter Master-Studiengang. Die Inhalte Werden auf wissenschaftlichem Niveau bei einer ausgeprägten Anwendungsorientierung vermittelt. Die Studierenden erlangen Qualifikationen, die sie befähigen als technische Fach- und Führungskräfte, weltweit aber auch für die regionale mittelständische Industrie tätig zu sein. Die Fähigkeiten, Fertigkeiten und Kenntnisse der Absolventen ermöglichen die folgenden Tätigkeitsfelder:

- Business Intelligence und Digitalisierung bei Beratungen sowie in Unternehmensabteilungen
- Analyst-Referent(in) direkt zugeordnet zum Direktorium oder Vorstand
- Risikomanagement bei Finanz-Unternehmen
- (IT-)Sicherheitsbeauftragte
- Security Information and Event Management

Folgende Qualifikationsziele werden in der Lehre gesetzt:

Konzeptionelle Fähigkeiten
Die Studierenden sind in der Lage, eigenständig Konzepte für Business Analytics-Werkzeuge und deren wirtschaftlichen Einsatz im Unternehmensumfeld zu entwickeln. Besondere Bedeutung hat in diesem Zusammenhang die Fähigkeit, theoretische Konzepte auf die konkreten Anwendungsfälle zu übertragen.
Vernetztes Denken
Die Studierenden können Zusammenhänge aus unterschiedlichen Anwendungsgebieten innerhalb des Fachgebiets und in deren Umfeld herleiten. Sie sind in der Lage, fachübergreifend zu analysieren und Konzepte zu entwickeln.
Führungskompetenz
Die Studierenden entwickeln sich in ihrer Führungsfähigkeit weiter. Sie sind in der Lage, Zielvereinbarungen zu treffen und deren Umsetzung zu steuern. Sie können ein Team motivieren und die Erfahrung von Personen unterschiedlicher Kompetenzen zielgerichtet zum Erfolg eines Teamprojekts einsetzen und nutzen.
Methodenkompetenz
Die Studierenden verfügen nicht nur über die Kenntnis von Methoden und Verfahren unterschiedlicher Fachgebiete der Informatik, sondern sind auch in der Lage, diese im jeweiligen Anwendungskontext anzuwenden.
Forschungskompetenz
Im Bereich Wissenschaft und Forschung sind die Studierenden in der Lage, wissenschaftliche Methoden einzusetzen und diese managementgerecht aufzubereiten.
Prozesskompetenz
Die Studierenden sind in der Lage, Konzepte und Strategien im Unternehmensumfeld erfolgreich umzusetzen. Sie haben das Rüstzeug, auch große Projekte von hoher Komplexität erfolgreich zu managen.
Analytische Kompetenz
Die Studierenden sind in der Lage, die für deren Problembereich relevanten Datenquellen zu identifizieren, die Daten formal zu beschreiben und diese für analytische Zwecke aufzubereiten. Sie sind darüber hinaus in der Lage, analytische Untersuchungen der Daten unter der Zielsetzung der Beantwortung komplexer Fragestellungen und des Generierens neuen, nicht trivialen Wissens selbstständig durchzuführen.

Sicherheitskompetenz
Die Studierenden sind in der Lage, im Rahmen einer eigenständigen Arbeit komplexe IT - Sicherheits und -Bedrohungs-relevanten Fragen und Problemstellungen zu formulieren. Sie sind in der Lage mit analytischen Mitteln aus Vorgangsdaten relevante Informationen zu Bedrohungen und Angriffen abzuleiten.

Ethische Kompetenz
Die Studierenden sind in der Lage ihr Vorgehen im rechtlich zulässigen, ethischen und moralischen Rahmen einzuordnen und kritisch zu hinterfragen. Insbesondere sind sie in der Lage Datenerhebungs- und Datenverarbeitungsprozesse bezüglich Konflikten mit Datenschutz- und Persönlichkeitsrechten zu prüfen.

2 Qualifikationsziel-Modul-Matrix

Modul-Nr.	Modulbezeichnung	Summe der Unterstützungspunkte	Strategisches Denken	Konzeptionelle Fähigkeiten	Vernetztes Denken	Führungskompetenz	Methodenkompetenz	Forschungskompetenz	Prozesskompetenz	Analythische Kompetenz	Sicherheitskompetenz	Ethische Kompetenz
	Qualifikationsziel (QuZ)											
51100	Business Intelligence	8		2	1		2		1	2		
52200	Advanced Statistics	8		2			2	2		2		
52300	Distributed Enterprise Applications	9	2	2	1		2	1	1			
52700	Security Analytics	13		1	2		2	2		2	2	2
51500	Strategic IT-Management	13	2	1	2	2		2	2			2
52100	Business Process Management & Data Compliance	11	1	2	1	1	2	1	2	1		
51200	Data- and Webmining	8		2			2	2		2		
51300	Large-Scale Data Analysis & Parallelization	11	1	2	2		2		2	2		
51400	Semantic Web	6		2			1	1		2		
52500	Innovations- und Transferkompetenz	11	2	1	1	2	1	2		1		1
51600	Open Source Intelligence	10		1			1	2		2	2	2
51700	Incident Response and Malware Defence	8					2			2	2	2
52600	Advanced Network and Internet Security	8					2			2	2	2
52400	Finance Risk Management	8	1		1		1	1		2	1	1
60100	Master Thesis	11	1	2			2	2	1	1	1	1
52400	Mündliche Masterprüfung	6	1	2	1		1			1		

Unterstützung der Qualifikationsziele in den Modulen (0=keine Unterstützung, 1=indirekte Unterstützung, 2=direkte Unterstützung)

Strategisches Denken
Die Studierenden verfügen über Verständnis zur Analyse der für die Geschäftsabläufe relevanten Informationen, verstehen daraus Wissensstrukturen zu formen und auf der Grundlage des resultierenden Wissens die Strategien für einen qualifizierten Entscheidungsfindungsprozess abzuleiten.

3 Studiengangs-Kompetenzmatrix

Kompetenzen		Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
Ausprägung		Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit/ Verantwortung	Reflexivität	Lernkompetenz
51100	Business Intelligence	7	7	7				7			7	
52200	Advanced Statistics	7		7					7	7		
52300	Distributed Enterprise Applications	7		7						7		
52700	Security Analytics	7	7	7	7		7			7		7
51500	Strategic IT-Management		7	7	7		7		7	7		
52100	Business Process Management & Data Compliance	7		7			7		7	7		
51200	Data- and Webmining	7	7	7	7				7	7		
51300	Large-Scale Data Analysis & Parallelization	7	7	7			6			7		
51400	Semantic Web	7		6	7				7			7
52500	Innovations- und Transferkompetenz		7	7	7		7			7		
51600	Open Source Intelligence	6	7		7	7			7	7		7
51700	Incident Response and Malware Defence	7			7				7	7		
52600	Advanced Network and Internet Security	7		7	7					7		
52400	Finance Risk Management	7		7			7		7	7		7
60100	Master Thesis				7					7		
52400	Mü. Masterprüfung				7							7

4 Modulbeschreibungen

4.1 1. Semester

4.1.1 51200 – Data and Web Mining

Studiengang: Business and Security Analytics M.Sc.
StuPO-Version: 18.2

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

Modul: Data and Web Mining					
Kennnummer 52200	**Workload** 180 h	**Modulart** P	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung Data- and Web-Mining Praktikum Semantic Web	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt -zeit** 4 SWS / 60 h	**Selbst-studium** 120	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS Praktikum: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die grundlegenden Methoden des Data- und Web-Mining. Sie verstehen die Konzepte, kennen die Funktionsmechanismen der Methoden sowie die Rahmenbedingungen für deren Einsatz. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage die Methoden des Data- und Web-Mining in realen Anwendungssituationen sinnvoll einzusetzen. Sie sind in der Lage aus eine Menge von in Frage kommenden Methoden die geeigneten auszuwählen und diese einzusetzen. *[Instrumentelle Fertigkeiten, 7]* Die Ergebnisse aus der Anwendung der Methoden können eingeordnet und kritisch bewertet werden. *[Beurteilungsfähigkeit, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage die Ergebnisse ihrer Analysen einem Fachkundigen zu erläutern. *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden sind in der Lage, eigenständig Datenanalysen zu konzipieren, auszuführen und die Ergebnisse verständlich darzustellen. *[Eigenständigkeit/Verantwortung, 7]*				

4	**Inhalte*:*** Grundlagen das Data- und Web Mining Prozessuale Sicht auf das Data Mining (Crisp-DM) Data Preprocessing (Data Cleansing, Missing Values, Dimensionsreduzierung…) Clusteranalyse (hierarchisch, partitionierend) Klassifikation (Entscheidungsbäume, einfache Neuronale Netze, Support Vector Machines,… Assoziations Daten (A-Priori, FP-Growth) Sequenzanalyse Web Mining (Web Content Analyse)
	Empfohlene Literaturangaben: Han, J et al. – Data Mining – Concepts and Techniques, Elsevier – Morgan Kaufmann, 3rd edit., 2012 Thomas A. Runkler, Data Mining –Methoden und Algorithmen intelligenter Datenanalyse, Springer Vieweg, 2010 Ian H. Witten, Eibe Frank, Mark A. Hall, Data Mining: Practical Machine Learning Tools and Techniques, 3rd edit., Elsevier, 2011; Florin Gorunescu, Data Mining: Concepts, Models and Techniques, Springer, 2011, Markus Hofmann, Ralf Klinkenberg, Rapidminer: Data Mining Use Cases and Business Analytics Applications, Productivity Pr Inc, 2013, Bing Liu, Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data (Data-Centric Systems and Applications), Springer; 2. Auflage, 2011, Beierle, C., Kern-Isberner, G. – Methoden wissensbasierter Systeme – Grundlagen, Algorithmen, Anwendungen, Vieweg+Teubner, 5. Aufl. 2014
5	**Teilnahmevoraussetzungen:** Es existieren keine Teilnahmevoraussetzungen.
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Die erfolgreiche praktische Arbeit im Praktikum wird durch Semesteraufgaben, die eigenständig zu bearbeiten sind, nachgewiesen.
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: Prof. Dr. Bernd Stauß, N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.2 51300 – Large Scale Data Analysis and Parallelization

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="8">Modul: Large-Scale Data Analysis and Parallelization</td></tr>
<tr><td colspan="2">Kennnummer
51300</td><td>Workload
180 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Large-Scale Data Analysis and Parallelization
Praktikum Large-Scale Data Analysis and Parallelization</td><td colspan="2">Sprache
Deutsch oder Englisch, wenn von den Modulteil-nehmern gewünscht (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt -zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
- kennen Systeme und Techniken für die parallele Datenverarbeitung
- kennen die Aufgabenstellungen aus dem Themengebiet von Big Data [Wissen, 7]

Kompetenz Fertigkeiten
Lernergebnisse (Kompetenzen) bei:
Die Studierenden
- sind in der Lage die Problem- und Aufgabenstellungen mit Bezug auf das Themengebiet Big Data zu erkennen, diese, basierend auf eigenem Wissen und durch die gezielte Recherche zu beschreiben, Lösungsansätze zu entwickeln und diese allein oder im Team umzusetzen.
- sind in der Lage, eine anwendungsbezogeneEvaluation von Daten, –Zugriffs- und –Verwaltungstechniken sowie von den diese Techniken implementierenden Systemen auszuführen, und darauf basierend eine zielgerechte Auswahl zu treffen.
- sind in der Lage wissenschaftliche Beiträge im Themenbereich Big Data eigenständig zu lesen und qualitative Vergleiche der gelesenen Beiträge systematisch zu präsentieren. [Instrumentelle Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen Big Data Prozess mit konkreter Aufgabenstellung entwickeln [Team-/Führungsfähigkeit, 7]</td></tr>
</table>

	Selbstständigkeit Die Studierenden sind in der Lage komplexe Aufgaben verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** Vorlesung: - Überblick zu No-SQL-Datenbanken - Überblick zu Graphendatenbanken - Architekturen für verteiltes und paralleles Datenmanagement und Datenverteilung - Verteilte Anfragebearbeitung - Clustering, Map Reduce, YARN, Tez - Verteilte Datenbanken - Vertikale/horizontale Fragmentierung - Fragmentierungstransparenz - Transaktionskontrolle - Frameworks für Skalierung und Parallelisierung der Datenzugriffe am Beispiel von Apache Hadoop, Spark und verteilten RDBMS Praktikum: Arbeiten mit Apache Hadoop, Spark Clustern, IBM Cloud, Azure, IBM Data Warehouse Arbeiten mit MongoDB, Apache Cassandra, Neo4J Arbeiten mit Injectiontools wie Apache Nifi, Talend, IBM NodeRed
	Empfohlene Literaturangaben: keine
5	**Teilnahmevoraussetzungen:** keine
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, 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:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Thomas Eppler Dozenten: Prof. Dr. Thomas Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.3 51500 – Strategic IT Management

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="7">Modul: Strategic IT Management</td></tr>
<tr><td colspan="2">Kennnummer
51500</td><td>Workload
180 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Strategic IT-Management
Fallstudie Strategic IT-Management</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Fallstudie: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
• kennen Zielstellung, Zielgruppen und den Aufbau von IT-Strategien
• kennen Instrumente zur Planung, Steuerung und Kontrolle von IT-Bereichen
• kennen die strategischen Herausforderungen der IT-Sicherheit im digitalen Zeitalter
• kennen die strategische Bedeutung von IT Governance, Risk and Compliance Management (IT-GRC) für Unternehmen, IT-Organisation und CIO
• kennen innovative Geschäftsmodelle der digitalen Plattformökonomie aus Sicht der IT
[Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden
• können den Einsatz der Informationstechnologie im Kontext der strategischen Ausrichtung des Unternehmens bewerten und einordnen
• können die Herausforderungen, Aufgaben und methodisches Vorgehen des IT-Management beschreiben
• können die Auswirkungen von Digitalisierung und speziell der digitalen 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, 7]

Die Studierenden
• können in umfangreichen, realitätsnahen Fallstudien die Unternehmenssituation analysieren, strategische Aspekte vor dem Hintergrund von Branche sowie</td></tr>
</table>

	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, 7]*
	Sozialkompetenz Die Studierenden sind in der Lage, die komplexen Fallstudien zum IT-Management – im Kontext aktueller Trends und Entwicklungen in IT und Digitalisierung – in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren [Team-/Führungsfähigkeit, 7] Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken auf Management-Niveau *[Kommunikation, 7]*
	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, 7]*
4	**Inhalte*:*** • IT-Strategieentwicklung • Rolle und Aufgaben der IT im Unternehmen • Rolle, Aufgaben und Pflichten des Chief Information Officer (CIO) im Unternehmen • Aufgaben, Rollen und Gremien im IT-Management • Aufbau von IT-Organisationen und internationale Koordination • Business-IT-Alignment mit internen und externen Kunden • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC) • IT-Service- und Prozessmanagement • IT-Ressourcenmanagement • Management des IT-Applikationsportfolios • IT-Partnermanagement: Relationship Management und Sourcing-Strategien • Sourcing Strategien: Business Process Outsourcing, Application Outsourcing, IT-Infrastruktur Outsourcing und Cloud Computing • IT-Projekt- und Projektportfoliomanagement • IT-Planung und IT-Controlling • IT-Management Cockpits • Umgang mit Schatten-IT • Digitalisierung, Digitale Transformation und Digitale Plattformökonomie • Industrie 4.0 im Kontext von Industrieunternehmen • IT-Unterstützung innovativer Geschäftsmodelle in der Plattformökonomie
	Empfohlene Literaturangaben: Porter, M. E.: Wettbewerbsstrategie: Methoden zur Analyse von Branchen und Konkurrenten, 12. Auflage, campus, 2013 Porter, M. E.: Wettbewerbsvorteile: Spitzenleistungen erreichen und behaupten, 8. Auflage, campus, 2014 Malik, F.: Strategie des Managements komplexer Systeme: Ein Beitrag zur Management-Kybernetik evolutionärer Systeme, 11. Auflage, 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 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 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 Mangiapane, M./Büchler, R.: Modernes IT-Management: Methodische Kombination von IT- Strategie und IT-Reifegrademodell, Springer Vieweg, 2015 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 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 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:** Kenntnisse auf den folgenden Lehrgebieten sind hilfreich: • IT-Management, IT-Consulting und E-Business • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC)

6	**Prüfungsformen***:* Seminararbeit, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreich bearbeitete Seminararbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.4 51700 – Incident Response und Malware Defence

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="8">Modul: Incident Response und Malware Defence</td></tr>
<tr><td colspan="2">Kennnummer
51700</td><td>Workload
180 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Incident Response und Malware Defense
Praktikum Incident Response und Malware Defense</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
60 SWS / 4 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können Methoden entwickeln und anwenden um IT-Angriffe zu erkennen, zu analysieren, einzudämmen und zu beseitigen [Systemische Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen [Kommunikation, 7]

Selbstständigkeit
Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
1. Der Incident Response Prozess: Preparation, Detection, Analysis, Containment, Recovery, Post Incident Activity
Veranschaulichung und Vertiefung der Phasen an Beispielen
2. Klassifikation und Taxonomie von Incidents
3. Systemsicherung: Sicherung systemwichtiger Daten
4. Spurensicherung: Netzbasierte Spuren (Netzwerkmitschnitte und Netzwerk-Komponenten), Host-basierte Spuren (persistente und nicht persistente Spuren, Arbeitsspeicher)
5. Spurenanalyse: Netzbasierte Spuren (Netzwerkmitschnitte, Log-Dateien), Host-basierte Spuren (Arbeitsspeicher, Log-Dateien, Dateisysteme)</td></tr>
</table>

	6. Detektion: Signatur-basierte und Regel-basierte Methoden 7. Methoden zur Einschränkung der Schadwirkung: Sandbox, Zugriffsschutz, Rechteüberwachung, Firewall, Proxy, Netzwerksegmentierung 8. Wiederherstellung: Backup und Systemsicherung anwenden 9. Statische Malware-Analyse: Aufbau der Malware, verwendete Bibliotheken, maliziöse Funktionen und Strukturen 10. Dynamische Malware-Analyse: Wirkungsweise der Malware, Schadwirkung lokalisieren 11. Reporting zur Malware-Analyse: Wirkungsweise, Schadenspotential, potentielle Quellen 12. Reporting zum Incident Response-Prozess 13. Post Incident Aktivitäten: Maßnahmen zur Verbesserung der Sicherheit treffen; Training von Incidents Beispiele für Projekte • Aufsetzen einer Signaturbasierten Detektion in einem System. Angriff auf das System. Incident behandeln • Aufsetzen eines Systems mit Schwachstellen (z. B. offene USB-Anschlüsse oder Mail-Clients ohne Makrovirenschutz); Eintragen einer Malware; Incident Response Prozess ausführen • Entwicklung einer Malware, die vermutete Systemschwächen ausnutzt (z. B. Keylogger, DLL-Injektor); Erproben der Malware an einem System mit Malware-Schutz; Incident Respons anwenden
	Empfohlene Literaturangaben: Alan J White (Autor), Ben Clark: Blue Team Field Manual. Create Space Independent Publishing Platform (2017) Gerard Johansen: Digital Forensics and Incident Response.Packt (2012 Johansen, Gerard. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents (Kindle-Positionen14-15). Packt Publishing. Kindle-Version. Cameron H. Malin, Eoghan Casey, James M. Aquilina: Malware Forensics Guide for Windows Systems, Digital Forensics Field Guides. Elsevier (2012) Weitere Literatur, insbesondere aktuelle wissenschaftliche Artikel, werden in der Vorlesung bekannt gegeben.
5	Teilnahmevoraussetzungen: Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Praktische Arbeit mit Präsentation 20 min. und Handout, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat und bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics M.Sc.

9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.5 xxxxx – Wahlpflichtmodul 1a / Wahlpflichtmodul 1b

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="7">Modul: Wahlpflichtmodule 1a / 1b</td></tr>
<tr><td colspan="2">Kennummer</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog (extra Liste)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Wird definiert durch jeweiligen Modulverantwortlichen</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen [Systemische Fertigkeiten, 7]
Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Für die hier Wahlpflichtmodulteile existieren jeweils gesonderte Modulteilbeschreibungen in diesem Modulhandbuch. Wenn Modulteile aus anderen Masterstudiengängen gewählt werden gelten die Inhaltsangaben der dort definierten Modulteilbeschreibungen. Sofern in diesen Fällen grundlegende Vorkenntnisse erforderlich sind die im bisherigen Studienverlauf der Studierenden nicht zwangsläufig erworben wurden, obliegt es dem Kandidaten diese Vorkenntnisse gesondert zu erwerben

Empfohlene Literaturangaben:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
</table>

5	**Teilnahmevoraussetzungen:** Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)
6	**Prüfungsformen***:* Siehe jeweilige Modulteilbeschreibungen
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Es gelten die Ausführungen in den Beschreibungen des WPM
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Systems Engineering M.Eng., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozenten: s. Modulbeschreibungen der jeweiligen WPM
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2 2. Semester

4.2.1 52100 – Business Process Management and Data Compliance

Studiengang: Business and Secvurity Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="7">Modul: Business Process Management and Data Compliance</td></tr>
<tr><td colspan="2">Kennnummer
52100</td><td>Workload
180 h</td><td>Modulart
P</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Business Process Management and Data Compliance
Fallstudie Business Process Management and Data Compliance</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Fallstudie: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen

Die Studierenden
• kennen Merkmale, Aufbau und Prinzipien von Prozessen und Geschäftsprozesse im Kontext der betrieblichen Ablauforganisationen
• kennen betriebliche Wertschöpfungsstrukturen und Anforderungen an das unternehmensweite Prozessmanagement
• kennen die gängigen Modellierungsmethoden und können diese auf Meta-Modellebene systematisieren
• kennen Kennzahlen und Kennzahlensysteme für das Monitoring von Geschäftsprozessen
• kennen den Datenbegriff und Methodiken zum Master Data Management
• kennen die Herausforderungen zum Datenschutz im Kontext der betrieblichen Erfassung, Verarbeitung und Speicherung personenbezogener Daten
• kennen Zielstellung, methodisches Vorgehen und Kontrollmechanismen zu Data Compliance, auch im digitalen Kontext [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden
• können betriebliche Ablaufstrukturen in gängigen Modellierungsnotationen modellieren und beherrschen den Einsatz von Abstraktionstechniken
• können betriebliche Prozesse auf Automationspotenzial und Resilienzfähigkeit hin analysieren und optimieren
• können Prozesse auf Basis von Kennzahlen und Kennzahlensystemen systematisieren und vergleichen sowie Monitoring- und Reporting-Strukturen aufbauen</td></tr>
</table>

	• können den betrieblichen Datenschutz und Data Compliance-Strukturen beschreiben und systematisieren *[Instrumentelle Fertigkeiten, 7]*
	Sozialkompetenz Die Studierenden sind in der Lage, die komplexen Fallstudien zu Business Process Management and Data Compliance – im Kontext aktueller Trends und Entwicklungen in IT und Digitalisierung – in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren [Team-/Führungsfähigkeit, 7] Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken auf Management-Niveau *[Kommunikation, 7]*
	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, 7]*
4	**Inhalte*:*** • Prozesse und Geschäftsprozesse • Betriebliche Kernkompetenzen und unternehmensweite Kernprozesse • Betriebliche Wertschöpfung, Wertschöpfungsstufen und Wertschöpfungsketten • Prozessmanagement und Prozessportfolio • Operatives versus strategisches Prozessmanagement • Enterprise Architecture Management und Business Architecture Management • Aufbau und Vergleich von Modellierungsmethoden für den betrieblichen Einsatz • Meta-Modelle und Meta-Meta-Modelle • Referenzmodelle und Prozesslandkarten • Kennzahlen und Kennzahlensysteme für das Monitoring von Geschäftsprozessen • Daten und Master Data Management • Datenschutz im Kontext der betrieblichen Unternehmung • Erfassung, Verarbeitung und Speicherung von Daten im Kontext gesetzlicher Vorgaben (Bundesdatenschutzgesetz und Datenschutz-Grundverordnung) • Zielstellung, methodisches Vorgehen und Kontrollmechanismen zu Data Compliance • Data Compliance im Kontext von Digitalisierung und digitaler Plattformökonomie
	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 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 Schmelzer, Herrmann J./Sesselmann, Wolfgang: Geschäftsprozessmanagement in der

	Praxis: Kunden zufrieden stellen, Produktivität steigern und Wert erhöhen, Hanser, 2013 Keuper, Frank/Neumann, Fritz: Corporate Governance, Risk Management und Compliance: Innovative Konzepte und Strategien,Gabler, 2010 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.: „Management der Informationssicherheit: Kontrolle und Optimierung“, Springer Vieweg, 2017 Sowa, A./Duscha, P./Schreiber, S.: IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die IT-Prüfung, Springer Vieweg, 2019 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 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 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:** Kenntnisse auf den folgenden Lehrgebieten sind hilfreich: • IT-Management, IT-Consulting und E-Business • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC)
6	**Prüfungsformen***:* Mündliche Prüfung (20 min.), benotet Referat, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreich bearbeitete Seminararbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.

9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozenten: Prof. Dr. Nils Herda, Prof. Dr. Bernd Stauß
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.2 52200 – Advanced Statistic

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="7">Modul: Advanced Statistics</td></tr>
<tr><td colspan="2">Kennnummer
52200</td><td>Workload
180 h</td><td>Modulart
P</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Seminar Advanced Statistics
Übungen Advanced Statistics</td><td>Sprache
Deutsch und Englisch (deutsches und englisches Litaratur-studium erforderlich)</td><td>Kontakt -zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Seminar: 2 SWS
Übungen: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierende kennen die grundlegenden Begriffe der Wahrscheinlichkeitstheorie und können diese anwenden [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können den Stoff praktisch in der Programmiersprache R für Analysen umsetzen [Instrumentelle Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden können statistische Sachverhalte anderen vermitteln. [Kommunikation, 6]

Selbstständigkeit
Die Studierenden können selbstständig Analysen mittels der Programmiersprache R durchführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
R-Grundlagen.

Stochastische Grundlagen (Wahrscheinlichkeit, Bedingte Wahrscheinlichkeit, Satz von Bayes)
Zufallsvariablen, Erwartungswert, Varianz, Stichproben, Lage- und Streumaße

Bootstrapping, Konfidenzintervalle, Verteilungen (Binomialverteilung, Poisson-Verteilung, Geometrische Verteilung, Exponentialverteilung, Normalverteilung, Betaverteilung)</td></tr>
</table>

	Signifikanz- und Hypothesentests (A/B-Tests, Permutationstests, ANOVA), Korrelationen, Maximum-Likelihood, Lineare Regression.
	Empfohlene Literaturangaben: Introduction to Statistical Thought☐ISBN: 978-1616100483 http://people.math.umass.edu/~lavine/Book/book.html Introduction to Probability and Statistics UsingR ISBN: 978-0-557-24979-4 http://cran.r-project.org/web/packages/IPSUR/vignettes/IPSUR.pdfAn Introduction to Statistical Learning: with Applications in R Gareth James, Daniela Witten, Trevor Hastie, Robert TibshiraniSpringer Texts in Statistics, 11. Juli 2016, ISBN-10: 1461471370 Die "'offizielle"' R-Einführung☐ISBN: 978-0954612085 cran.r-project.org/doc/manuals/R-intro.pdf R-Kurs der Uni Augsburg: stats.math.uni-augsburg.de/~theus/r-kurs.pdf
5	**Teilnahmevoraussetzungen:** Grundlegende Programmierkenntnisse müssen da sein.
6	**Prüfungsformen***:* Klausur 90 min., benotet Referat, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur und Referat
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Tobias Häberlein Dozenten: Prof. Dr. Tobias Häberlein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.3 52500 – Innovation and Transfer Competence

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="8">Modul: Innovation and Transfer Competence</td></tr>
<tr><td colspan="2">Kennnummer
52500</td><td>Workload
180</td><td>Modulart
PM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. 52305 In. and Transfer Competence
b. 52320 Proj. In. and Transfer Competence</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
a. 15
b. 45</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, Seminar b. Projektarbeit</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Methoden zur Integration einen betrieblichen Innovationsmangements in bestehende Betriebe [Wissen, 7]
Planungs-, Organisations-und Qualitätsmanagementsmethoden aus Theorie und Praxis [Wissen, 7]

Kompetenz Fertigkeiten
Wissenschaftliche Grundlagen-und neuere Forschungsergebnisse erfassen, auf deren praktischen Einsatz hin prüfen, ergänzen und zum Einsatz bringen. [Systemische Fertigkeiten, 7]

Zusammenhänge zwischen diversen Theorien und Konzepten zu sehen, diese zu umfassenderen integrierenden praxisorientierten Konzeptionen weiterzuentwickeln und in konkreten entwickelten Anwendungen zum Einsatz zu bringen [Instrumentelle Fertigkeiten, 7]

Geschäftsideen entwickeln, diese bezügliche Realisierbarkeit prüfen und Strategien entwickeln, Forschungsergebnisse zu transferieren und als Innovation umzusetzen [Systemische Fertigkeiten, 7]

Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. [Team-/Führungsfähigkeit, 7]

Selbstständigkeit
Sind in der Lage in einem konkurrierendem Kontext, eigene Ideen zu reflektieren, diese gegeben Falls anzupassen und durchzusetzen, oder sich Argumenten zu beugen und die Ideen der Wettbewerber zu akzeptieren
[Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

4	**Inhalte*:*** Vorlesung: - Ideenmanagement - Betriebliches Innovationsmanagement - Transfer Wissenschaft -Praxis Projekt - Entwicklung eines ausführlichen Geschäftsszenarios, eines Qualitätsmanagementplans und einer Risikoabschätzung - Bestimmung, Suche und Auswahl der einzusetzenden wissenschaftlichen Forschungsergebnisse - Entwicklung einer Vermarktungsstrategie - Durchführen der Organisations-und Qualitätsplanung - Vornahme der Projektplanung (Aufgaben, Netzplan, Meilensteine) und Festlegung der Arbeitsverteilung (Rollen, Verantwortlichkeiten, Mitarbeit, Personalführung) - Leitung und Durchführung des Projekts - Betreiben des Projekt-und Risikomanagements - Durchführung von Produkttest, Endfertigung und Qualitätskontrolle
	Empfohlene Literaturangaben: Al-Laham, Andreas. Organisationales Wissensmanagement: Eine strategische Perspektive. Vahlen, 2016. Mertins, Kai, Ina Kohl, and Ronald Orth. "Ein Referenzmodell für Wissensmanagement." Wissensmanagement im Mittelstand. Springer Gabler, Berlin, Heidelberg, 2016. 31-40. Kamiske, Gerd F., and Jörg-Peter Brauer. Qualitätsmanagement von A-Z: Wichtige Begriffe des Qualitätsmanagements und ihre Bedeutung. Carl Hanser Verlag GmbH Co KG, 2016. Neumann, Alexander. Führungsorientiertes Qualitätsmanagement. Carl Hanser Verlag GmbH Co KG, 2017.
5	**Teilnahmevoraussetzungen:** Wissenschaftliches Arbeiten (DQR 6), Projektmanagement (DQR 5)
6	**Prüfungsformen***:* Praktische Arbeit (benotet) als Modulprüfung
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business und Security Analysis MSc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.4 52700 – Security Analytics

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="8">Modul: Security Analytics</td></tr>
<tr><td colspan="2">Kennnummer
52700</td><td>Workload
180</td><td>Modulart
PM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. 52705 Security Analytics
b. 52720 Proj. Security Analytics</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
a. 30
b. 30</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, b. Projektarbeit</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den aktuellen Forschungsstand zu den Themenbereichen Security Analytics wie Malware Analytics or/and Security Network Package and Profess Analytics. [Wissen, 7]
Vertieftes Verstehen von Semantic Web -Technologien als Instrument für interoperable Wissensbeschreibung [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können den Analytischen Prozesse auf konkrete Aufgabenstellungen anwenden und mit spezifischen Methoden und Tools umsetzen. [Instrumentelle Fertigkeiten, 7]

Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen Security Analytics Prozess mit konkreter Aufgabenstellung entwickeln. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Sind in der Lage komplexe Aufgaben in einem Team zu bearbeiten, die Teamarbeit zu organisieren und die Rollen effektiv zu verteilen. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Sind in der Lage komplexe Aufgaben verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Definition und Begriffsklärung,
Security Analytics Use Cases,
Data Souesess und Methoden der Datensammlung ,
Real time Datensammeln,
Anwendung der Security Analytics Ergebnissen und ihr Impact,
Basic security analytics Costs,
Advanced persistent threats,
Security Analytics und Digitale Forensics,</td></tr>
</table>

	Übersicht der security analytics tools and services, u.a.: Blue Coat Security Analytics Platform, Lancope Stealth Watch System, Juniper Networks JSA Series Secure Analytics, EMC RSA Security Analytics NetWitness, FireEye Threat Analytics Platform, Arbor Networks Security Analytics, Click Security Click Commander, Hexis Cyber Solutions' NeatBeat MON, Sumo Logics' cloud service., Security Onion.
	Empfohlene Literaturangaben: Hitzler, P., Krötzsch, M., Rudolph, S., & Sure, Y. (2007). Semantic Web: Grundlagen. Springer-Verlag. Dengel, Andreas, ed. Semantische Technologien: Grundlagen. Konzepte. Anwendungen. Springer-Verlag, 2011. Ege, Börteçin, Bernhard Humm, and Anatol Reibold, eds. Corporate Semantic Web: Wie semantische Anwendungen in Unternehmen Nutzen stiften. Springer-Verlag, 2015.
5	**Teilnahmevoraussetzungen:** Grundkenntnisse in formalen Logiken (DQR 3), Kenntnisse in Web Technologien und auszeichnungssprachen (DQR 5)
6	**Prüfungsformen***:* Klausur 90 Min. (Modulprüfung), Praktische Arbeit (Projekt-Prüfung).
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur und die praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business und Security Analysis MSc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.5 xxxxx – Wahlpflichtmodul 2a / Wahlpflichtmodul 2b

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="8">Modul: Wahlpflichtmodule 2a / 2b</td></tr>
<tr><td colspan="2">Kennnummer</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog (extra Liste)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Wird definiert durch den jeweiligen Modulverantwortlichen</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten [Wissen, 7]</td></tr>
<tr><td></td><td colspan="7">Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen [Systemische Fertigkeiten, 7]</td></tr>
<tr><td></td><td colspan="7">Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. [Team-/Führungsfähigkeit, 7]</td></tr>
<tr><td></td><td colspan="7">Selbstständigkeit
Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Für die hier Wahlpflichtmodulteile existieren jeweils gesonderte Modulteilbeschreibungen in diesem Modulhandbuch. Wenn Modulteile aus anderen Masterstudiengängen gewählt werden gelten die Inhaltsangaben der dort definierten Modulteilbeschreibungen. Sofern in diesen Fällen grundlegende Vorkenntnisse erforderlich sind die im bisherigen Studienverlauf der Studierenden nicht zwangsläufig erworben wurden, obliegt es dem Kandidaten diese Vorkenntnisse gesondert zu erwerben</td></tr>
<tr><td></td><td colspan="7">Empfohlene Literaturangaben:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
</table>

5	**Teilnahmevoraussetzungen:** Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)
6	**Prüfungsformen***:* Siehe jeweilige Modulteilbeschreibungen
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Es gelten die Ausführungen in den Beschreibungen des WPM
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc.. Systems Engineering M.Eng., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozenten: s. Modulbeschreibungen der jeweiligen WPM
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.3 3. Semester

4.3.1 60100 – Master-Thesis

Studiengang: Business and Security Analytics M.Sc. **Semester**: WS 2021/22
StuPO-Version: 18.2 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="7">Modul: Master-Thesis</td></tr>
<tr><td colspan="2">Kennnummer
60100</td><td>Workload
750 h</td><td>Modulart
P</td><td>Studiensemester
3</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Projekt Master-Thesis</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
--</td><td>Selbst-studium
750 (Präsenz & Selbst-studium)</td><td>Credits (ECTS)
25</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Projekt, betreute selbständige wissenschaftliche Arbeit</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Abhängig vom Thema der Masterarbeit [Wissen, 7]</td></tr>
<tr><td></td><td colspan="6">Kompetenz Fertigkeiten
Mit der Master – Thesis zeigt der Student, dass er unter Anleitung selbständig umfangreiche wissenschaftliche Themen bearbeiten kann. Er wird praxisorientierte oder theoretische Themenstellungen nach wissenschaftlichen Kriterien analysieren, strukturieren und ergebnisorientiert bearbeiten. Die Master – Thesis dokumentiert seine Arbeit und erfüllt die Kriterien eines wissenschaftlichen Berichts. [Systemische Fertigkeiten, 7]</td></tr>
<tr><td></td><td colspan="6">Sozialkompetenz
Abhängig vom Thema und Ort der Ausarbeitung (z.B. ein externes Unternehmen) 7]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit
Master-Thesis ist das größte Projekt im gesamten Master-Studiums, das die Studierenden nachweislich selbständig und verantwortlich ausführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
abhängig von Thema und Inhalt der Master-Thesis</td></tr>
<tr><td></td><td colspan="6">Empfohlene Literaturangaben:
Abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
</table>

5	**Teilnahmevoraussetzungen:** Ggf. formal geregelt in der Prüfungsordnung
6	**Prüfungsformen***:* Master-Thesis (Ma.), benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Thesis (Positive Bewertung)
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: abhängig vom Thema und Inhalt der Master-Thesis
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.3.2 60200 – Mündliche Masterprüfung

Studiengang: Business and Security Analytics
StuPO-Version: 18.2

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Mündliche Masterprüfung</td></tr>
<tr><td colspan="2">Kennnummer
60200</td><td>Workload
180 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
3</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
60210 Mastervortrag
60220 Masterprüfung</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
---</td><td>Selbst-studium
180 (Präsenz & Selbst-studium)</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Projekt, betreute selbständige wissenschaftliche Arbeit</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Wissen in Abhängigkeit vom Thema der Masterarbeit [Wissen, 7]</td></tr>
<tr><td></td><td colspan="7">Kompetenz Fertigkeiten
Mit dem Master – Vortrag sollen die Studierenden die Ergebnisse ihrer Tätigkeit in eine anschaulichen Art einem fachlich kompetenten Hörerkreis vermitteln. Die Verteidigung soll nicht nur eine Präsentation der wissenschaftlichen Ergebnisse der Masterarbeit, sondern auch eine Präsentation der Persönlichkeit des Vortragenden sein. [Systemische Fertigkeiten, 7]</td></tr>
<tr><td></td><td colspan="7">Sozialkompetenz
Studierende sind in der Lage, sehr komplexe Inhalte in einer plausiblen und transparenten, jedoch aussagekräftigen Form in Kürzester Zeit darzustellen. [Kommunikation, 7]</td></tr>
<tr><td></td><td colspan="7">Selbstständigkeit
Insbesondere in der dem Vortrag folgenden Diskussion sollen die Studierenden Beweis von der Tiefgründigkeit und Sicherheit ihrer Kenntnisse abgeben. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Ist abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
<tr><td></td><td colspan="7">Empfohlene Literaturangaben:
Anleitung zurwissenschaftlichen Arbeit. Vom Kandidaten selber vorzuschlagende vertiefende Literatur.</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Ggf. formal beschrieben in Prüfungsordnung</td></tr>
</table>

6	**Prüfungsformen***:* Referat 30 min., benotet Mündliche Prüfung 30 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Referat, Bestandene mündliche Prüfung
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: abhängig vom Thema und Inhalt der Master-Thesis
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul