Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Modulkatalog Wahlpflichtfächer M. Sc. Security Management (SPO 2015)

März 2016

Impressum

Autor:	Max Luber
Redaktion:	Prof. Dr. Ivo Keller
Druck:	Druckerei der Technischen Hochschule Brandenburg
Kontakt:	Technische Hochschule Brandenburg
	University of Applied Sciences
	Magdeburger Str. 50
	14770 Brandenburg an der Havel
	T +49 3381 355 - 278
	F +49 3381 355 - 199
	E ivo.keller@th-brandenburg.de
	www.th-brandenburg.de
Stand:	Montag, 21. März 2016

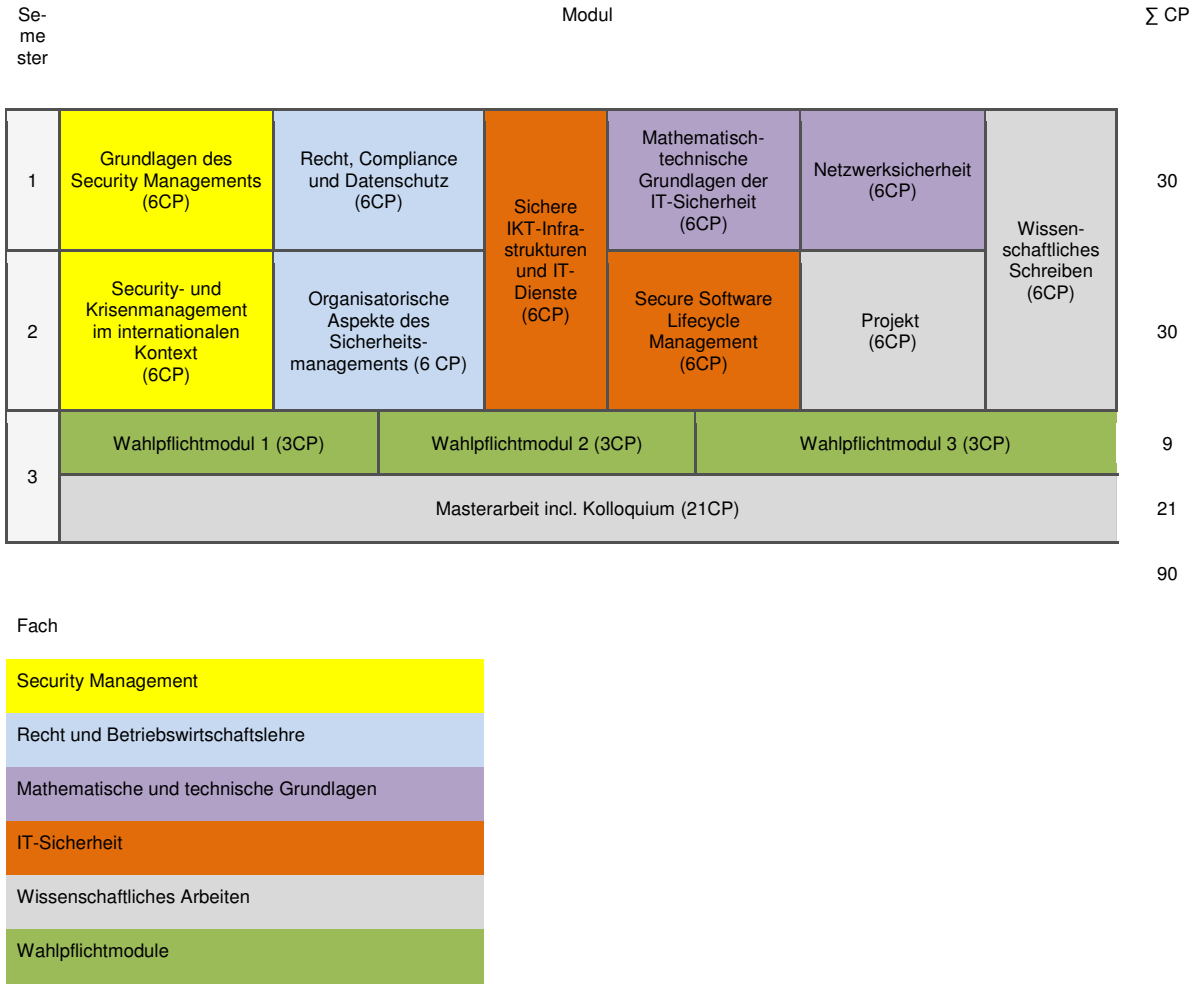
Inhaltsverzeichnis

Einleitung

Dieses Dokument enthält die Beschreibungen der Wahlpflichtfächer des Masterstudiengangs *Security Management* der Technischen Hochschule Brandenburg in der Version der Studien- und Prüfungsordnung von 2014 und 2015.

Nach dem Regelstudienplan (siehe Abb.1) sind die drei vorgeschriebenen Wahlpflichtmodule (WPM) im dritten Fachsemester begleitend zur Masterarbeit zu absolvieren. Die Studierenden können die Wahlpflichtfächer aber auch in den früheren Semestern belegen. Ein Wahlpflichtmodul geht über 2 SWS (22,5 Zeitstunden) und hat jeweils 3 CP; insgesamt sind 3 WPM zu belegen. Wahlpflichtmodule dienen der Vertiefung und Spezialisierung, sie sind jeweils einem oder mehreren Vertiefungsbereichen des Studiums zugeordnet.

Abbildung 1 Modulübersicht des Masterstudiengang Security Management



Angebotene Wahlpflichtfächer und Vertiefungsfächer

Im jedem Semester werden mindestens 3, in der Regel 6, Wahlpflichtfächer angeboten, wobei jedes Semester geringfügige Änderungen im Angebot vorgenommen werden. Auf diese Weise kann die

Verfügbarkeit der Dozenten berücksichtigt werden, auf aktuelle Entwicklungen eingegangen werden und das Lehrangebot weiterentwickelt werden. Die Tabelle 1 unten zeigt, welche WPF in welchem Semester angeboten werden. Der Tabelle 2 auf der Folgeseite ist zu entnehmen, welchen Vertiefungsfächern die WPF zugeordnet sind.

Tabelle 1: Verteilung der WPM über die Semester

Kursname	Dozent	WiSe 14/15	SoSe 2015	WiSe 15/16	SoSe 2016	WiSe 16/17	SoSe 2017
Predictive Analytics	Prof. Dr. I. Keller				X		
Datenschutz in der vernetzten Welt	Prof. Dr. I. Keller Prof. Dr. F. Holl	X		X	X		
Penetration Testing	Wilhelm Dolle, n.n.				X		
Sicherheitsanforderungen Kerntechnischer Anlagen	Prof. Dr. Mertins	X					
IT-Sicherheit im BOS-Umfeld	Rolf Lambertz	X		X			
Systemkompetenz und sicherheitsbewusstes Handeln	Dieter Skrobotz						
Sicherheitsheuristik	Dieter Skrobotz				X		
Working for Life	Dr. Manuel Burkert	X		X			
PCI DSS (Payment Card Industry Data Security Standard)	Patrick Sauer	X		X			
Informationssicherheitsmanagementsysteme (ISMS)	Jörn Mayer & Tobias Goldschmidt, n.n.	X		X			
Technische Aspekte der IT-Forensik	Prof. Dr. I. Podebrad	X			X		
Sicherheitsveranstaltungen	Prof. Dr. I. Keller	X					
Know How Schutz	Peter Mnich & Jörg Treffke, n.n.		X				
Sicherheit von Rechenzentren	Ralph Wölpert		X		X		
Cyber War	Ingo Ruhmann		X		X		
Risikoanalyse und Risikomanagement	Carsten Baeck, n.n.		X				
Social Engineering	Stephan Humer						
ITIL	Prof. Dr. J. Scheeg, Ralf Grasedyck		x		X		
Business Continuity Management (BCM)	Prof. Dr. O. Weissmann			X			
Globale Risiken und lokale Handlungsoptionen	Thomas Wandinger			X	X		

Tabelle 2: Zuordnung der WPM zu den Vertiefungsrichtungen

Kursname	Dozent	Bankensicherheit	Gebäude & Personensicherheit	BCM & Krisenmanagement	Cyber War & Cyber Security	Informations-sicherheit	Forensik	Anlagen & Reaktorsicherheit
Predictive Analytics	Prof. Dr. I. Keller	X		X	X	X	X	
Datenschutz in der vernetzten Welt	Prof. Dr. I. Keller Prof. Dr. F. Holl	X			X	X	X	
Penetration Testing	Wilhelm Dolle	X			X	X	X	
Sicherheitsanforderungen Kerntechnischer Anlagen	Prof. Dr. Mertins		X	X		X		X
IT-Sicherheit im BOS-Umfeld	Rolf Lambertz			X	X	X	X	X
Systemkompetenz und sicherheitsbewusstes Handeln	Dieter Skrobotz	X	X	X	X	X	X	X
Sicherheitsheuristiken	Dieter Skrobotz	X	X	X	X	X	X	X
Working for Life	Dr. Manuel Burkert		X	X		X		x
PCI DSS (Payment Card Industry Data Security Standard)	Patrick Sauer	X			X	X	X	
Informationssicherheits-managementsysteme (ISMS)	Jörn Mayer, Tobias Goldschmitt, n.n.	X		X	X	X	X	X
Technische Aspekte der IT-Forensik	Prof. Dr. I. Podebrad	X		X	X	X	X	X
Sicherheitsveranstaltungen	Prof. Dr. I. Keller	X	X	X	X	X	X	X
Know How Schutz in der Wirtschaft	Peter Mnich & Dr. Jörg Treffke, n.n.	X	X	X	X	X	X	X
Sicherheit von Rechenzentren	Ralph Wölpert	X	X	X	X	X	X	X
Cyber War	Ingo Ruhmann	X		X	X	X	X	X
Risikoanalyse und Risikomanagement	Carsten Baeck	X	X	X	X	X	X	X
ITIL (IT Infrastructure Library)	Prof. Dr. J. Scheeg, Ralf Grasedyck, n.n.	X	X	X	X	X	X	X
BCM (Business Continuity Management)	Prof. Dr. O. Weissmann, n.n.	X	X	X	X	X	X	X
Globale Risiken und lokale Handlungsoptionen	Thomas Wandinger		X	X		X		X

1 Predictive Analytics

WPF-Kurzkennzeichen:	MA_SM_Analytics
WPF-Bezeichnung:	Predictive Analytics
ggf. Aufteilung in Lehrveranstaltungen:	Nein
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	• SecMan-Master, 1./2./3. Semester, WPF • Wirtschaftsinformatik-Master als Teil des WPFs „Predictive Analytics und Privatheit"
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller
Lehrsprache:	Deutsch
Voraussetzungen:	Grundlagen der Statistik, Data Warehousing, XML/HTML
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 30 Stunden
Studien-/ Prüfungsleistungen:	Hausarbeit oder Referat/Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	2,5% der Abschlussnote
Lernergebnisse:	Kompetenz im Umgang mit • Tools zur Textindexierung (z.B. Solr/Lucene) • Methoden zur Verarbeitung von Prozessdaten, Benutzerverhalten und Meinungen • Visualisierungstools (z.B. Rapid Miner)
Inhalte:	Den Studierenden werden hierbei Kenntnisse zu folgenden grundlegenden Themenbereichen vermittelt: • Aufbereitung nicht-numerischer Daten aus heterogenen Quellen (Big Data) • Maschinelles Lernen, Clusterung und Visualisierung

	• Predictive Modelling, ggf. Empfehlungssysteme
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	Wird in der Veranstaltung bekannt gegeben.

2 Datenschutz in der vernetzten Welt

WPF-Kurzkennzeichen:	MA_SM_WPM_Datenschutz_vernetzt
WPF-Bezeichnung:	Datenschutz in der vernetzten Welt
ggf. Aufteilung in Lehrveranstaltungen:	---
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	• SecMan Master, 1./2./3. Semester, WPF • Wirtschaftsinformatik Master als Teil des WPFs „Predictive Analytics und Privatheit"
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller, Prof. Dr. Friedrich Holl
Lehrsprache:	Deutsch
Voraussetzungen:	Grundlagen des Datenschutzes, möglichst Predictive Analytics
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 30 Stunden
Studien-/ Prüfungsleistungen:	Hausarbeit oder Referat/Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	2,5% der Abschlussnote

Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, vernetzte Medien und Dienste in einer konstruktiven Herangehensweise nutzen zu können. Dabei soll eine grundsätzliche Sensibilisierung für persönlichkeitsrechtliche Grundwerte und eine nachhaltige unternehmerische Compliance erreicht werden. Damit sollen die Studierenden in die Lage versetzt werden, moderne Technologien wie Big Data und Data Mining/Predictive Analytics sicher und im Einklang mit ethischen und normenrechtlichen Anforderungen des Daten- und Persönlichkeitsschutzes auszuwählen und einzusetzen.
Inhalte:	Den Studierenden werden hierbei zu folgenden Themen Informationen vermittelt: • Verantwortung der Datenverarbeitung gg. den Quellen, Persönlichkeitsschutz als Grundrecht • Datensicherheit als Voraussetzung für unternehmerische Existenz • Sicheres Agieren in Cloud und Web 2.0 • Nachhaltige Compliance, serviceorientierte Organisation und Datensouveränität, technische Umsetzung von 80-/20-Prinzipien
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Bernhard C. Witt: Datenschutz kompakt • Michael Helisch: Security Awareness • Thorsten Logemann: Datenschutz in Unternehmen Weitere Literatur wird in der Vorlesung bekannt gegeben.
Besonderes:	

3 Penetration Testing

WPF-Kurzkennzeichen:	MA_SM_Pen-Test
WPF-Bezeichnung:	Penetration Testing
ggf. Aufteilung in Lehrveranstaltungen:	Nein
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyberwar & Cybersecurity • Informationssicherheit • Forensik
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Dipl.-Chem. Wilhelm Dolle
Dozent/in:	Dipl.-Chem. Wilhelm Dolle, Marco Murch, n. n.
Lehrsprache:	Deutsch
Voraussetzungen:	Es sind keinerlei Vorkenntnisse notwendig.
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 30 Stunden
Studien-/ Prüfungsleistungen:	Hausarbeit oder Referat/Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	2,5% der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Studierenden zu befähigen, einen Penetrationstest mithilfe gängiger Hacking Tools nach Best-Practice-Vorgehensweise durchzuführen und zu dokumentieren. Gleichermaßen soll ein Verständnis dafür geschaffen werden, wie Ergebnisse eines Penetrationstest zu bewerten sind und welche Handlungsempfehlungen daraus resultieren.
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Kenntnisse über potenzielle Cyber-Risiken

	• Angreifertypen: Von Script Kiddies bis Advanced Persistant Threats • Vorstellung von Standards und Best-Practice-Ansätzen zur Durchführung von Penetrationstests • Rechtliche Rahmenbedingungen • Testverfahren und Aggressivität • Vorstellung gängiger Hacking Tools (Nmap, OWASP Zed, Metasploit, Nessus u.a.) • Live-Hacking • Durchführung eines Penetrationstests • Fundierte Einschätzung der Ergebnisse • Dokumentation und Handlungsempfehlungen • Advanced Cyber Defense
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	Wird in der Veranstaltung bekannt gegeben.
Besonderes:	

4 Sicherheitsanforderungen an kerntechnische Anlagen

Modul-Kurzkennzeichen:	MA_SM_Sich_KTA
Modulbezeichnung:	Sicherheitsanforderungen an kerntechnische Anlagen
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Anlagen- und Reaktorsicherheit • Gebäude- und Personensicherheit • Informationssicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Friedrich Holl
Dozent/in:	Prof. Dr. Manfred Mertins, n. n.
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit
Gewichtung der Note in der Gesamtnote:	2,5% der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Anforderungen an kerntechnische Anlagen verstehen und anwenden

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt:
	• integriertes Managementsystem (Zusammenwirken von Mensch-Technik-Organisation (MTO-Konzept))
	• Sicherheitsziele (radiologische und technische Ziele)
	• Defence in Depth Konzept, Unabhängigkeit der Sicherheitsebenen
	• Barrierenkonzept
	• Ereignisse und Zustände auf den Sicherheitsebenen
	• Anlageninternes Notfallschutzkonzept
	• Schutz gegen übergreifende Einwirkungen
	• Grundsätze der Sicherheitsnachweise (deterministische und probabilistische Ansätze)
	• Klassifizierungskonzept
	• Konzept zum praktischen Ausschluss von Ereignissen
	• Auslegungsgrundsätze
	  • Diversitätsprinzip - Vermeidung von GVA
	  • Einzelfehlerkonzept
	  • 30-Minuten Konzept
	  • Inhärente Sicherheit, fail-safe Prinzip
	  • Passive Wirkungsprinzipien
	  • Basissicherheit, Bruchausschlusskonzept - Sicherheitsanforderungen an zukünftige Kernkraftwerke

Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Borlein, M.: Kerntechnik, Vogel Business Media, 2011 • Smidt, D.: Reaktor-Sicherheitstechnik, Springer-Verlag, Berlin, 1979 • IAEA: http://www-ns.iaea.org/standards/default.asp?s=11&l=90 • WENRA: http://www.wenra.org/extra/pod/?id=20&module_instance=1&action=pod_show • KTA: http://www.kta-gs.de/ • GRS: http://www.grs.de/content/kerntechnisches-regelwerk • Handbuch für Reaktorsicherheit und Strahlenschutz, http://www.bfs.de/de/bfs/recht/RSH • BMU: Sicherheitskriterien für Kernkraftwerke, http://www.bmu.de/atomenergie_sicherheit/rechtsvorschriften_technische_regeln/doc/40327.php
Besonderes:	

5 IT-Sicherheit im BOS Umfeld

Modul-Kurzkennzeichen:	MA_SM_ITSich_BOS
Modulbezeichnung:	IT-Sicherheit im BOS-Umfeld
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Rolf Lambertz
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Anforderungen an die IT-Sicherheit in Behörden und Organisationen mit Sicherheitsaufgaben

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Welche Behörden sind "BOS"? • Zuordnung zu Gebietskörperschaften (Bund, Land, Kommunen) • Welchen Status haben Werksfeuerwehren (z.B. Flughafen BER, wichtig für die Zusammenarbeit mit öffentlichen Feuerwehren • Sicherheitsarchitektur Deutschland (Polizeien des Bundes und der Länder, Zollverwaltung, Feldjäger) • Einbindung im Schengen-Raum (SIS, VIS, EURODAC, Rolle von EUROPOL und FRONTEX, EU Kommission - DG Home Affairs) • Zentralstellenfunktion des BKA, BKA-Gesetz • Zusammenarbeit mit "den Diensten" (polizeilicher Staatsschutz, Legalitätsprinzip, Anti-Terror-Datei) • IT-Systeme der dt. Polizei (Übersicht, INPOL, extrapol) • Typische Anwendungen der Polizeien (Vorgangsbearbeitung, Fahndung, Fall-Analyse-Systeme, AFIS, Ausblick PIAV und xPolizei) • Sicherheitsüberprüfungsgesetz • Rolle der Industrie
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	Wird in der Veranstaltung bekannt gegeben
Besonderes:	

6 Systemkompetenz und sicherheitsbewusstes Handeln

Modul-Kurzkennzeichen:	MA_SM_Systemkompetenz
Modulbezeichnung:	Systemkompetenz und sicherheitsbewusstes Handeln
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Personen und Gebäudesicherheit • Anlagen- und Reaktorsicherheit • Business Continuity und Krisenmanagement
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Dipl.-Ing. Dieter Skrobotz
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit und/oder mündliche Prüfung und/oder Klausur (wird zu Beginn des Semesters bekannt gegeben)
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Verständnis für die Einflüsse der Komplexität von Systemen auf die Sicherheit des Systems und der Komponenten / Akteure im System

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Ganzheitliches Sicherheitsmanagement • Der moderne Sicherheitsbegriff • Beispiel: ganzheitliche Gebäudesicherheit • Hidden Management Funktion • Building Information Modeling • Systemkompetenz • Sicherheitsbewusstes Handeln • Kybernetik
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Literatur zu Kybernetik und vernetztem Denken • Wird in der Veranstaltung bekannt gegeben
Besonderes:	

7 Sicherheitsheuristik

WPF-Kurzkennzeichen:	MA_SM_Sicherheitsheuristik
WPF-Bezeichnung:	Sicherheitsheuristik
ggf. Aufteilung in Lehrveranstaltungen:	Vorlesung (Präsenzstudium) und Übungen/Projektarbeit in Kleingruppen im Eigenstudium/Gemeinsame Auswertung
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Personen- und Gebäudesicherheit • Business Continuity und Krisenmanagement • Cyber War & Cyber Security • Informationssicherheit • Forensik • Anlagen- und Reaktorsicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Dipl.-Ing. Dieter Skrobotz
Dozent/in:	Dipl.-Ing. Dieter Skrobotz
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Präsentation (empfohlen)
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Anwendungsfähiges Wissen und Fähigkeiten zum Handeln in sicherheitsrelevanten Ausnahmesituationen
Inhalte:	Den Studierenden werden vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Neue Aspekte des Sicherheitsbegriffs • Was ist Ganzheitliches Sicherheitsmanagement? • Systemkompetenz als Wissensbasis • Prinzipien sicherheitsbewussten Handelns • Systeme und der Umgang mit ihnen • Der Kompetenzbegriff • Komplexität und ihre Beherrschbarkeit • Besonderheiten im sicherheitsorientierten Teammanagement • Besonderheiten im sicherheitsorientierten Projektmanagement

	• Sicherheitsbewusstes Handeln in Ausnahmesituationen • Heuristiken - Entstehung, Aufbau, Eigenschaften, Anwendungsgebiete • Metaheuristiken und Heuristische Regeln • Heuristiken als methodische Grundlage für die Lösung von Problemen • Prinzipien einer Sicherheits-Heuristik (SIH) • SIH-Regeln und Handlungsstrukturen • Praktische Übungen zur Anwendung einer Sicherheitsheuristik
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Literatur zum Problemlösen und vernetzten Denken und zum Handeln in Ausnahmesituationen wird in der Veranstaltung bekannt gegeben
Besonderes:	Das Spezialwissen zur Sicherheitsheuristik und ihrer Anwendung beruht auf aktuellen Forschungsergebnissen und wird 2016 erstmals in einer Vorlesung angeboten.

8 Working for Life

Modul-Kurzkennzeichen:	MA_SM_Working_for_Life
Modulbezeichnung:	Working for Life
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Personen und Gebäudesicherheit • Business Continuity und Krisenmanagement • Informationssicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Friedrich Holl
Dozent/in:	Dr. Manuel Burkert
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Grundkompetenzen im Bereich von Gesundheitsmanagement und Arbeitsmedizin im Unternehmenskontext

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Arbeitsmedizin • Gesundheitsmanagement • Entsendung von Mitarbeitern in Regionen mit gesundheitlichen Risiken • Medizinische Versorgung bei Großveranstaltungen • Work-Life-Balance • Fokussierter Einblick in die Welt der Medizin • Verständnis für unterschiedliche Denkweisen • Juristische Implikationen paramedizinischer Entscheidungen • Anwendung von Grundsätzen aus dem Security-Umfeld im medizinischen Setting
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	Wird in der Veranstaltung bekannt gegeben.
Besonderes:	

9 PCI DSS

Modul-Kurzkennzeichen:	MA_SM_PCI_DSS
Modulbezeichnung:	PCI DSS (Payment Card Industry Data Security Standard)
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Friedrich Holl
Dozent/in:	Patrick Sauer M. Sc.
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Sicherheitsanforderungen an Webshops und Portale, die Finanztransaktionen durchführen
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Sicherheitsanforderungen der Kreditkartenfirmen • Technische Umsetzungsmöglichkeiten • Zertifizierungsprozess

Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	Wird in der Veranstaltung bekannt gegeben.
Besonderes:	

10 Informationssicherheitsmanagementsysteme

Modul-Kurzkennzeichen:	MA_SM_ISMS
Modulbezeichnung:	Informationssicherheitsmanagementsysteme (ISMS)
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Business Continuity und Krisenmanagement • Anlagen und Reaktorsicherheit
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Ronny Frankenstein und Jörn Maier
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Implementieren eines ISMS in einem Unternehmen

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • ISO 27001 und ff. • IT-Grundschutz des BSI • Unterschiede und Gemeinsamkeiten • Erfolgsfaktoren bei der Umsetzung
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	Wird in der Lehrveranstaltung bekannt gegeben.
Besonderes:	

11 Technische Aspekte der IT-Forensik

Modul-Kurzkennzeichen:	MA_SM_Tech_Forensik
Modulbezeichnung:	Technische Aspekte der IT-Forensik
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Igor Podebrad
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Erlernen IT-forensischer Vorgehensweisen und technischer Analysemethoden • Durchführung IT-forensischer Untersuchungen am Beispiel zweier unterschiedlicher Filesysteme

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt:
	• Grundsätze und Anforderungen, speziell im internationalen Kontext und vor dem Hintergrund unterschiedlicher rechtlicher Situationen:
	• Datenträgeranalyse
	  • Übersicht Typen von Festplatten (SCSI, xATA, xIDE, etc.)
	  • Übersicht physische Aufteilung einer Platte (cylinder, head, sector)
	  • Übersicht logische Aufteilung einer Platte (partitions, raw data)
	  • Übersicht Dateisysteme (FAT, NTFS als Schwerpunkt, ggfls. ext2, ext3)
	  • Übersicht Dateiverwaltung (Cluster, slack space [drive slack, RAM slack])
	  • Details Festplattenanalyse (Sicherheitsmaßnahmen, tools, hands on)
	  • Dateien und ihre Eigenschaften (Metadaten)
	  • Arten von Dateien (normal, hidden, deleted, encrypted, alternate datastream, ...)
	  • string search (logisch vs. physisch, Kodierung)
	  • Details FAT
	  • Historische FAT-Systeme (FAT 12, FAT 16)
	  • FAT32 (Strukturen, Namenskonvention)
	• Betriebssystemanalyse
	  • Server vs. Workstation
	  • Lokation OS auf Platte
	  • Prozessanalyse
	  • Netzwerkverbindungen
	  • Registry
	  • NTFS (Metadaten und Details)
	  • Details Alternate Datastreams
	  • Details Filetypen
	  • Windows-Artefakte (cookies, temporary files, MRU, print jobs, ...)
	  • timelining
	  • Details Registry
	  • Email-Analyse
	• Netzwerkanalyse
	  • Grundlagen
	  • Protokolle
	  • Detail-Analyse
	  • Anomalien
	  • verdeckte Kommunikation
	  • Angriffstypen

Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.

Literatur:	• File System Forensic Analysis, Brian Carrier, Taschenbuch: 600 Seiten, Verlag: Addison-Wesley Longman, Amsterdam (17. März 2005), Sprache: Englisch, ISBN-10: 0321268172, ISBN-13: 978-0321268174 • Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, Alexander Geschonneck, Broschiert: 342 Seiten, Verlag: dpunkt Verlag; Auflage: 4., aktualisierte Auflage (22. Februar 2010), Sprache: Deutsch, ISBN-10: 3898646580, ISBN-13: 978-3898646581 • Windows® Internals, Fifth Edition (PRO-Developer), Mark Russinovich & David A. Solomon, Gebundene Ausgabe: 1232 Seiten, Verlag: Microsoft Press; Auflage: Fifth Edition. (17. Juni 2009), Sprache: Englisch, ISBN-10: 9780735625303, ISBN-13: 978-0735625303, ASIN: 0735625301 • Harlan Carvey, Windows Forensic Analysis, Verlag: Syngress Media; Auflage: 2nd edition. (13. Juli 2009), ISBN-13: 978-1597494229 • Sammes; Jenkinson, Forensic Computing: A Practitioner's Guide, Verlag: Springer, Berlin; Auflage: 2nd ed. (30. Juli 2007), ISBN-13: 978-1846283970
Besonderes:	

12 Sicherheitsveranstaltungen

Modul-Kurzkennzeichen:	SM_MA_WPM_Sicherheitsveranstaltungen
Modulbezeichnung:	Sicherheitsveranstaltungen
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Personen und Gebäudesicherheit • Anlagen- und Reaktorsicherheit • Business Continuity und Krisenmanagement (Je nach Wahl der Veranstaltung)
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr (in der Regel)
Autor/in:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Exkursionen zu Sicherheitsveranstaltungen; Mitwirken an einer Sicherheitsveranstaltung des Studiengangs, Erstellen von Exkursionsberichten
Studien-/ Prüfungsleistungen:	Hausarbeit (50%) und Projekt
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote

Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Analyse des Inhaltes von Konferenzen und Messen mit Sicherheitsfokus • Bewerten des Mehrwerts von verschiedenen Konferenzen und Messen • Erstellen von Zusammenfassungen von Vorträgen, Konferenzen und Messen
Inhalte:	Je nach Angebot. Typischerweise eine Exkursion zu einer kommerziellen Identitätsmanagement- und Cloud-Konferenz, eine Exkursion zu einer Messe zu physischer Sicherheit, und eine Exkursion zu einer sicherheitsrelevanten Veranstaltung eines börsennotierten Konzerns.
Lehr- und Lernmethoden:	Besuch von Veranstaltungen.
Literatur:	Keine
Besonderes:	Exkursionen, Reisekosten sind durch die Studierenden selbst zu tragen.

10. Sicherheit von Rechenzentren

Modul-Kurzkennzeichen:	MA_SM_Sicherheit_von_Rechenzentren
Modulbezeichnung:	Sicherheit von Rechenzentren
ggf. Aufteilung in Lehrveranstaltungen:	--
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Personen und Gebäudesicherheit • Anlagen- und Reaktorsicherheit • Business Continuity und Krisenmanagement
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Ralph Wölpert
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Besondere Anforderungen an die Sicherheit und Verfügbarkeit von Rechenzentren

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt: • Auswirkung von organisatorischer, technischer, physischer und logischer IT-Sicherheit • Planung, Konzeption und Auslegung von Rechenzentren und IT-Umgebungen inkl. der Verfügbarkeit und Sicherheit der einzelnen Infrastrukturbereiche wie: Racksystem, Klimatisierung, Sicherheitsraum unter besonderer Berücksichtigung von o Lage und Architektur o Kühlungsoptionen o Aktivem und passivem Brandschutz o Mehrpfadiger Stromversorgung o Anbindung der Datenleitungen o Zutrittsschutz und Einbruchschutz o Redundanzkonzepten o Datensicherung z.B. Raid, Spiegelung etc. Enthalten sind zudem Themen wie BSI Grundschutz, Risikoanalysen von Rechenzentren und Bitkom-Leitfäden, Geheimschutz der Wirtschaft sowie Zertifizierungen (BSI, TÜV, ECB-S, eco) von RZ.
Lehr- und Lernmethoden:	• Vorlesung/ Vorträge mit wechselnden Medien • Übungen in Kleingruppen
Literatur:	• BSI Grundschutzkataloge, Ausgabe 2013/2014 • BITKOM Leitfaden, Betriebssicheres Rechenzentrum, 2013 • BITKOM Leitfaden, Energieeffizienz im Rechenzentrum, 2010 • BITKOM Leitfaden, Prozesse und KPI für Rechenzentren, 2012 • Bernd Dürr, IT-Räume und Rechenzentren planen und betreiben: Handbuch der Bautechnik und Technischen Gebäudeausrüstung", Verlag Bau + Technik, 2013 • Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben
Besonderes:	Die Exkursion zu einem RZ ist Teil des Seminars

11. Risikoanalysen und Risikomanagement

Modul-Kurzkennzeichen:	MA_SM_Risiko
Modulbezeichnung:	Risikoanalyse und Risikomanagement
ggf. Aufteilung in Lehrveranstaltungen:	--
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Personen und Gebäudesicherheit • Anlagen- und Reaktorsicherheit • Business Continuity und Krisenmanagement
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Friedrich Holl
Dozent/in:	Carsten Baeck
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Methodenkompetenz in der Analyse von Risiken • Methodenkompetenz im Management von Risiken
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt:

	• Verschiedene Ansätze der Risikoanalyse • Probabilistische und deterministische Ansätze • Retrospektive und prospektive Analysen • Qualitative und quantitative Ansätze • Umgang mit Unsicherheiten • Ansätze aus dem Qualitätsmanagement bzw. der Sicherheitsbewertung technischer Systeme • Management von Risiken in verschiedenen Umgebungen • Etablierte Frameworks des Risikomanagement
Lehr- und Lernmethoden:	• Vorlesung/ Vorträge mit wechselnden Medien (Beamer, Flipchart, Whiteboard) • Übungen in Kleingruppen und zusammen.
Literatur:	• British Standard - 25999: Business Continuity Management [Buch]. - London : [s.n.], 2006. • Brühwiler Bruno - Risikomanagement als Führungsaufgabe: ISO 31000 mit ONR 49000 wirksam umsetzen [Buch]. - [s.l.] : Haupt, 2011. • Brühwiler Bruno und Romeike Frank - Strategische Früherkennung [Buch]. - 2010. • http://www.controllingwiki.com/de/index.php/Risikoanalyse_FMEA. • Dornes Nadeshda - Alternative Risikomodellierungs-, Risikoanalyse- und Bewertungsmethode: Risikomanagement ohne komplexe mathematische Modelle [Buch]. - Hamburg : disserta Verlag, 2014. • eurorisk.ch [Online]. - 2015. - http://www.eurorisk.ch/.fh-hannover.de [Online]. - 2015. http://transfer.tr.fhhannover.de/projekte/norma/pix/glossar/risikowahrnehmung.htm. • http://www.es.hsmannheim.de/sps/Uebungen/Kapitel8/Uebung8_2.html. • maschinenrichtlinie-2006-42-eg.de [Online]. - 2015. - http://www.maschinenrichtlinie-2006-42-eg.de/grunds%C3%A4tze-der-risikobeurteilung-von-maschinen. • ONR 49000 - 2010. • ONR 49002-1 - 2010. • ONR 49002-2 - 2010. • orghandbuch.de [Online]. - 2015. http://www.orghandbuch.de/OHB/DE/Organisationshandbuch/6_MethodenTechniken/63_Analysetechniken/633_FehlermoeglichkeitUndEinflussanalyse/fehlermoeglichkeitundeinflussanalysenode.html. • pwc.de [Online]. - 2015. - http://www.pwc.de/de/risiko-management/studie-offenbart-maengel-imrisikomanagement-deutscher-unternehmen.jhtml . • risikomanager.org [Online]. - 2015. - http://risikomanager.org/methodenassistent/fehlerbaumanalyse/.risknet.de [Online]. - 2015. – • Romeike Frank und Hager Peter - Erfolgsfaktor Risiko-

	Management 3.0: Methoden, Beispiele, Checklisten Praxishandbuch für Industrie und Handel [Buch]. - Wiesbaden : Springer Gabler, 2013. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben
Besonderes:	

12. Cyber War

Modul-Kurzkennzeichen:	MA_SM_CyberWar
Modulbezeichnung:	Cyber War
ggf. Aufteilung in Lehrveranstaltungen:	--
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Anlagen- und Reaktorsicherheit • Business Continuity und Krisenmanagement
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Ingo Ruhmann
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit Details werden zu Beginn des Kurses bekannt gegeben
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Die Studierenden sollen in die Lage versetzt werden, die Bedrohungen durch Cyber War und die Wirksamkeit von Gegenmaßnahmen einschätzen zu können.

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt: • Spezifika des Cyber War im Vergleich zu anderen Manipulationsformen • Cyber War als Herausforderung für das Sicherheitsmanagement • Cyber War und der Schutz von KRITIS • Cyber War aktuelle Fälle und Angriffstechniken • Cyberdefence-Strategien im Vergleich und Gegenstrategien
Lehr- und Lernmethoden:	• Vorlesung/ Vorträge mit wechselnden Medien (Beamer, Flipchart, Whiteboard) • Übungen in Kleingruppen und zusammen.
Literatur:	• https://ccdcoe.org/publication-library.html • Ingo Ruhmann: Cyber War: Will it define the Limits to IT Security? In: IRIE - International Review of Information Ethics, Vol 20, 12/2013, S. 4-15 • Ingo Ruhmann, Ute Bernhardt: Information Warfare und Informationsgesellschaft. Zivile und sicherheitspolitische Kosten des Informationskriegs. In: Wissenschaft und Frieden, Heft 1/2014, Dossier Nr. 74 • Ingo Ruhmann: NSA, IT-Sicherheit und die Folgen. Eine Schadensanalyse ; in: Datenschutz und Datensicherheit, Heft 1, 2014, S. 40-46 • Ingo Ruhmann, Christiane Schulzki-Haddouti: Kryptodebatten. Der Kampf um die Informationshoheit; in: Christiane Schulzki-Haddouti (Hg.): Bürgerrechte im Netz, Bundeszentrale für politische Bildung, / Leske & Budrich, Bonn, 2003, S. 162-177 • Ingo Ruhmann: Rüstungskontrolle gegen den Cyberkrieg? In: Telepolis, 4.01.2010 • Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann, Dieter Wöhrle: Naturwissenschaft - Rüstung - Frieden: Basiswissen für die Friedensforschung, VS-Verlag, 2007 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
Besonderes:	

13. ITIL (IT Infrastructure Library)

Modul-Kurzkennzeichen:	MA_SM_ITIL
Modulbezeichnung:	ITIL (IT Infrastructure Library)
ggf. Aufteilung in Lehrveranstaltungen:	--
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Business Continuity und Krisenmanagement
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Friedrich Holl
Dozent/in:	Prof. Dr. J. Scheeg, Ralf Grasedyck, n.n.
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit und/oder mündliche Prüfung und/oder Klausur und/oder Präsentation
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Anwenden des ITIL-Modells • Bewerten von Unternehmens- und Sicherheitsprozessen bezüglich der Umsetzung des ITIL-Modells

Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt:
	
	Die Studierenden erhalten eine Einführung in ITIL (IT Infrastructure Library „v3") und IT Service Management. Hierzu zählen:
	• ITIL-Modell
	• 5 Phasen des ITIL-Lebenszyklus'
	  ○ Service Strategy
	  ○ Service Design
	  ○ Service Transition
	  ○ Service Operation und
	  ○ Continual Service Improvement
	und ihre einzelnen Prozesse.
	
	Ergänzend zur theoretischen Einführung werden verschiedene Praxisszenarien vorgestellt und praktisch erarbeitet. Es werden verschiedene Situationen von ITIL-Einführungen vorgestellt und die Bedeutung von ITIL an Beispielen durchgespielt. In Vorträgen werden einzelne Themen vertieft.

Lehr- und Lernmethoden:	• Vorlesung/Vorträge mit wechselnden Medien (Beamer, Flipchart, Whiteboard) • Übungen in Kleingruppen und zusammen.
Literatur:	• Jan van Bon, et al., Foundations in IT Service Management basierend auf ITIL v3, Van Haren Publishing, Zaltbommel 2008 • Jan van Bon, et al., Foundations in IT Service Management basierend auf ITIL, Zaltbommel 2006 • David Cannon, et al., ITIL Service Strategy 2011 Edition, TSO, London, 2011 • Lou Hunnebeck, et al., ITIL Service Design 2011 Edition, TSO, London, 2011 • Stuart Rance, et al., ITIL Service Transition 2011 Edition, TSO, London, 2011 • Randy Steinberg, et al. ITIL Service Operation 2011 Edition, TSO, London, 2011 • Vernon Lloyd, et al., ITIL Continual Service Improvement 2011 Edition, TSO, London, 2011
Besonderes:	Im Anschluss an die Lehrveranstaltung ist es möglich, das „ITIL Foundation"-Zertifikat zu erwerben.

14. Globale Risiken und lokale Handlungsoptionen

Modul-Kurzkennzeichen:	MA_SM__Glob_Risk_lokale_Handlung
Modulbezeichnung:	Globale Risiken und lokale Handlungsoptionen
ggf. Aufteilung in Lehrveranstaltungen:	Nein
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Personen und Gebäudesicherheit • Informationssicherheit • Anlagen- und Reaktorsicherheit • Business Continuity und Krisenmanagement
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Thomas Wandiger
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2SWS
Studien-/ Prüfungsleistungen:	Hausarbeit oder Referat/Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform vor Beginn der Lehrveranstaltung bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	2,5% der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Auslandsinformationen aus verschiedenen Quellen ermitteln und bewerten / einen Überblick über die Anbieter und Arbeitsweise von Informationslieferanten erhalten. • Einen Überblick über internationale/regionale Sicherheitsregime erlangen. • Die besonderen Problemstellungen für Reisesicherheit, Standortsicherheit und Unternehmenssicherheit in einer globalisierten Welt kennen und bewerten.

	• Auswirkungen von Krisen- und Konflikte auf Unternehmens- und Reisesicherheit einschätzen
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Bewertung und Erschließung von Internationalen Informationsquellen • Marktübersicht und Dienstleistungen privater Auslandsinformationsanbieter • Sicherheitsregime der VN-Charta / Handlungsrahmen der int. Staatengemeinschaft • Sicherheit im Umfeld entgrenzter/erodierender Staatlichkeit • Staatliche und Nicht-Staatliche Akteure in der Sicherheitspolitik • Das Ringen um regionale Vorherrschaft / Regionale Konflikte / Nationale Interessen und Nationale Sicherheit im Wandel
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• CIA world-fact-book • www.swp.de • Le monde diplomatique Weitere Literatur wird zu Beginn des Kurses bekannt gegeben
Besonderes:	

15. Business Continuity Management (BCM)

Modul-Kurzkennzeichen:	MA_SM__BCM
Modulbezeichnung:	Business Continuity Management (BCM)
ggf. Aufteilung in Lehrveranstaltungen:	Nein
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Personen und Gebäudesicherheit • Anlagen- und Reaktorsicherheit • Business Continuity- und Krisenmanagement
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Ivo Keller
Dozent/in:	Dr. Oliver Weissmann
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 30 h Präsenz- und 60 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS
Studien-/ Prüfungsleistungen:	Hausarbeit oder Referat/Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.
Gewichtung der Note in der Gesamtnote:	2,5% der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Aufbau eines BCM nach ISO 22301, Einbettung in die Unternehmensorganisation, Verzahnung des BCM mit dem (Informations-)Sicherheitsmanagement • Identifizieren kritischer Geschäftsprozesse und

	Infrastrukturen • Minimieren der Auswirkungen von Vorfällen, Minimieren der Ausfallzeiten und verkürzen der Wiederherstellungszeit
Inhalte:	Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt: • Aufbau eines BCM nach ISO 22301 • Einbinden des BCM in Unternehmensorganisation allgemein und die Sicherheitsorganisation in speziellen. • Schnittstellen zum Informationssicherheitsmanagement, zum Risikomanagement, zur Notfallplanung und weiteren Bereichen der Unternehmenssicherheit. • Kernbegriffe und Grundkonzepte im BCM • Prozessmodellierung und Identifikation kritischer Geschäftsprozesse, kritischer Infrastrukturen, Versorgungsketten und Zulieferer • Modellierung von (und Umgang) mit Interdependenzen
Lehr- und Lernmethoden:	Vorlesung, Übungen in Kleingruppen.
Literatur:	• Disaster Recovery, Crisis Response, and Business Continuity A Management Desk Reference //by: Watters, Jamie Berkeley, CA ; s.l., Apress, 2014 Volltext: https://ezproxy.th-brandenburg.de/login?url=http://dx.doi.org/10.1007/978-1-4302-6407-1 • Business Continuity: Notfallplanung für Geschäftsprozesse (Xpert.press) // von: Martin Wieczorek, Uwe Naujoks und Bob Bartlett (Hrsg.); Berlin / Heidelberg; Springer 2003 • http://www.bcm-institute.org/ • Business Continuity Management by Patrick Woodman 2007 • International Journal of Business Continuity and Risk Management: http://www.inderscience.com/jhome.php?jcode=ijbcrm
Besonderes:	

16. Know How Schutz

Modul-Kurzkennzeichen:	MA_SM_
Modulbezeichnung:	Know How-Schutz
ggf. Aufteilung in Lehrveranstaltungen:	--
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 1./2./3. Semester, Wahlpflichtmodul
Verwendbarkeit des Moduls:	Dieses Modul kann für folgende Profilrichtungen verwendet werden: • Bankensicherheit • Cyber War & Cyber Security • Informationssicherheit • Forensik • Personen und Gebäudesicherheit • Anlagen- und Reaktorsicherheit • Business Continuity und Krisenmanagement
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Verantwortlich:	Prof. Dr. Friedrich Holl
Dozent/in:	Peter Mnich & Dr. Jörg Treffke
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	3
Gesamtworkload und ihre Zusammensetzung:	90 h = 24 h Präsenz- und 66 h Eigenstudium
Lehrform/SWS:	Vorlesung: 2 SWS in Blockform innerhalb von 3 Tagen
Studien-/ Prüfungsleistungen:	Hausarbeit oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote:	2,5 % der Abschlussnote
Lernergebnisse:	Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen: • Bewerten von Unternehmensrisiken bzgl. Know-How-Schutzes • Methoden zum Schutz von Know-How

Inhalte:	Den Studierenden werden hierbei vertiefte zu folgenden Informationen vermittelt: • Erläuterung von Know-how- und Produktschutz • Definitionen und Unterschiede von Informationsabfluss und Spionage • Aktuellen Lage der Spionage weltweit • Risiken für deutsche Unternehmen • Täter, Tätermodelle und modus operandi • Schutzmaßnahmen, Prozesse und aktuelle Handlungsfelder im Bereich des Know-How-Schutzes
Lehr- und Lernmethoden:	• Vorlesung, Übungen in Kleingruppen.
Literatur:	• Lindemann U. at all.: Know-How-Schutz im Wettbewerb: Gegen Produktpiraterie und unerwünschten Wissenstransfer, Springer Berlin Heidelberg, 2012 • Kochmann, K.: Schutz des „Know-How" gegen ausspähende Produktanalysen, De Gruyter, 2009 • Abele, E. at all.: Schutz vor Produktpiraterie: Ein Handbuch für den Maschinen- und Anlagenbau, Springer Berlin Heidelberg, 2011 • Kahle/Merkel: Fall- und Schadensanalyse bzg. Know-how-/Informationsverlusten in Baden-Württemberg ab 1995, Uni Lüneburg, 2004 • Wurzer/Kaiser: Praxishandbuch Internationaler Know-how-Schutz, Bundesanzeiger Verlag, 2010 • Lux/Peske: Competitive Intelligence und Wirtschaftsspionage, Gabler Verlag, 2002 • Michaeli, Competitive Intelligence, Springer Verlag, 2004 • Schaaf, Industriespionage, Boorberg, 2009 • Fussan: Managementmaßnahmen gegen Produktpiraterie und Industriespionage, Gabler Verlag, 2010 • Fink, Lauschziel Wirtschaft, Boorberg, 1996 • Kenan, Vertrag versus Vertrauen, VDM, 2008 • Liman: Bewertung des irregulären Verlustes von Know-how, Wirtschaftsverlag Bachem, 1999 • Westermann: Handbuch Know-how-Schutz, Verlag C.H. Beck, 2007 • http://www.sicherheitsforum-bw.de/ • http://www.verfassungsschutz.de/ • http://www.verfassungsschutz-bw.de • http://www.verfassungsschutz.bayern.de/
Besonderes:	