

Modulkatalog Pflichtfächer M. Sc. Security Management (SPO 2016)

Januar 2017

Impressum

Autor: 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, 30. Januar 2017
© Technische Hochschule Brandenburg

Inhaltsverzeichnis

1.	Einleitung	4
2.	Grundlagen des Security Managements	6
3.	Security- und Krisenmanagement im internationalen Kontext.....	9
4.	Recht, Compliance und Datenschutz	11
5.	Organisatorische Aspekte des Sicherheitsmanagements	14
6.	Netzwerksicherheit.....	18
7.	Mathematisch-technische Grundlagen der IT-Sicherheit.....	20
8.	Sichere IKT-Infrastrukturen und IT-Dienste	22
9.	Secure Systems Lifecycle Management.....	25
10.	Wissenschaftliches Schreiben.....	27
11.	Projekt	29
12.	Masterarbeit	31

1. Einleitung

Dieses Dokument beschreibt die Pflichtfächer¹ des Masterstudiengangs *Security Management* der Technischen Hochschule Brandenburg in der Version der Studien- und Prüfungsordnung von 2016².

Modulübersicht (Regelstudienplan Vollzeit)

Sem.	Module						Σ CP
1	Grundlagen des Security Managements (6 CP)	Recht, Compliance und Datenschutz (6 CP)	Sichere IKT-Infrastrukturen und IT-Dienste (6 CP)	Mathematisch-technische Grundlagen der IT-Sicherheit (6 CP)	Netzwerksicherheit (6 CP)	Wissenschaftliches Schreiben (6 CP)	30
2	Security- und Krisenmanagement im internationalen Kontext (6 CP)	Organisatorische Aspekte des Sicherheitsmanagements (6 CP)		Secure Software Lifecycle Management (6CP)	Projekt (6 CP)		30
3	Wahlpflichtmodul 1 (3CP)		Wahlpflichtmodul 2 (3 CP)		Wahlpflichtmodul 3 (3 CP)		9
	Masterarbeit inkl. Kolloquium (21 CP)						21
							90

Fach

Security Management
Recht und Betriebswirtschaftslehre
Mathematische und technische Grundlagen
IT-Sicherheit
Wissenschaftliches Arbeiten
Wahlpflichtfach

¹ *Fächer* sind Gruppen von *Modulen*. Module werden jeweils mit *einer* Prüfungsnote benotet und können aus mehreren Lehrveranstaltungen bestehen.

² SPO 2016 vom 19.11.2016, veröffentlicht am 10.01.2017

Modulübersicht (Regelstudienplan Teilzeit)

Sem. Module

1	Grundlagen des Security Managements (6 CP)	Mathematisch-technische Grundlagen der IT-Sicherheit (6 CP)	Sichere IKT-Infrastrukturen und IT-Dienste (6 CP)	15
2	Security- und Krisenmanagement im internationalen Kontext (6 CP)	Organisatorische Aspekte des Sicherheitsmanagements (6 CP)		15
3	Netzwerksicherheit (6 CP)	Recht, Compliance und Datenschutz (6 CP)	Wissenschaftliches Schreiben (6CP)	15
4	Secure Software Lifecycle Management (6 CP)	Projekt (6CP)		15
5	Wahlpflichtmodul 1 (3 CP)	Wahlpflichtmodul 2 (3 CP)		6
	Masterarbeit incl. Kolloquium (21 CP)			
6	Wahlpflichtmodul 3 (3 CP)			24
				90

Fach

Security Management
Recht und Betriebswirtschaftslehre
Mathematische und technische Grundlagen
IT-Sicherheit
Wissenschaftliches Arbeiten
Wahlpflichtmodule

2. Grundlagen des Security Managements

Modul-Kurzkennzeichen	SM_MA_GrundlagenSecurityManagement
Modulbezeichnung	Grundlagen des Security Managements
ggf. Aufteilung in Lehrveranstaltungen	
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SM Ma, 1. Semester, Pflichtmodul
Verwendbarkeit des Moduls	Das Modul wird auch als Pflichtvorlesung des Master-Studiengangs Wirtschaftsinformatik angeboten. Das Modul kann auch für Master Informatik angeboten werden.
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Heinz-Dieter Schmelling
Dozent/in	Prof. Dr. Heinz-Dieter Schmelling
Lehrsprache	Deutsch
Voraussetzungen	Keine
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS	Vorlesung: 30 Stunden (2 SWS), Praktische Anwendung und Übung an Fallbeispielen: 30 Stunden (2 SWS)
Studien-/Prüfungsleistungen	Hausarbeit + Referat, alternativ mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote

Lernergebnisse	<p>Die Lernenden sollen in die Lage versetzt werden, die folgenden grundsätzlichen Kenntnisse und Fertigkeiten zu erlangen:</p> <ul style="list-style-type: none"> • Erstellen von Sicherheitsuntersuchungen • Durchführen von Risikobewertungen • Analysieren von Sicherheitslagen und der Sinnhaftigkeit von Gegenmaßnahmen • Verständnis entwickeln für die Bedeutung der Sicherheit im Entscheidungsprozess bei Unternehmern • Sicherheitsorganisationen im Unternehmen beurteilen • Beispielhaft Sicherheitsprozesse unter Zuhilfenahme von IT-Werkzeugen abbilden • Sicherheitsmaßnahmen erarbeiten und vor einem Entscheidungsgremium erfolgreich durchsetzen <p>Zusätzlich sollen die folgenden Lernergebnisse erreicht werden:</p> <ul style="list-style-type: none"> • Etablieren einer Sicherheitsorganisation in einem Unternehmen • Erstellen eines Qualifikationsprofils für einen Sicherheitsverantwortlichen • Integrieren von IT- und nicht-IT-Sicherheits-relevanten Aspekten • Einführen eines Sicherheitsmanagementsystems in einer Organisation • Erarbeiten einer Strategie für einen Teilbereich der IT-, Informations- oder Unternehmenssicherheit
Inhalte	<p>Wesentliche Aspekte der Unternehmenssicherheit:</p> <ul style="list-style-type: none"> • Security Governance und Sicherheitsmanagementsystem • Security Organisation • Security Policy • Risikomanagement • Sicherheitsanalysen • Sicherheitsprozesse • Normen und Standards für Informationssicherheit • Return-on-Security-Investment-Berechnungen • Krisenmanagement • Business Continuity Management <p>Zudem:</p> <ul style="list-style-type: none"> • Ausgewählte Vertiefungsbereiche der IT- und der Unternehmenssicherheit
Lehr- und Lernmethoden	<p>Interaktiver Mix aus Vorlesung, Erarbeiten und Vortragen von Inhalten, Demonstration von Konzepten, praktischen Aufgaben in Gruppen, Erarbeiten von eigenen Inhalten und Rollenspiel.</p>
Literatur	<ul style="list-style-type: none"> • Security Management 2011: Handbuch für Informationsschutz, IT-Sicherheit, Standortsicherheit, Wirtschaftskriminalität und Managerhaftung von Guido Birkner, 2011. • Handbuch Unternehmenssicherheit: Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System von Klaus-Rainer Müller, 2010. • Unternehmenssicherheit von Stephan Gundel, und Lars Mülli, 2009. • Security Risk Management Body of Knowledge von Julian Talbot, Miles Jakeman, Wiley 2009.

Besonderes	
------------	--

3. Security- und Krisenmanagement im internationalen Kontext

Modul-Kurzzeichen	SM_MA_SecurityKrisenManagementInternational
Modulbezeichnung	Security- und Krisenmanagement im internationalen Kontext
ggf. Aufteilung in Lehrveranstaltungen	
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SM Ma, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls	
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Heinz-Dieter Schmelling
Dozent/in	Prof. Dr. Heinz-Dieter Schmelling
Lehrsprache	Deutsch, z. T. Englisch (10%)
Voraussetzungen	Keine
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS	Vorlesung: 30 Stunden, Übung: 30 Stunden
Studien-/ Prüfungsleistungen	Hausarbeit und Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	<p>Die Lernenden sollen in die Lage versetzt werden, die folgenden grundsätzlichen Kenntnisse und Fertigkeiten zu erlangen:</p> <ul style="list-style-type: none"> • Analysieren von Sicherheitslagen im internationalen Kontext unter Berücksichtigung kultureller, politischer und geographischer Gegebenheiten • Führen einer Sicherheitsorganisation in internationalen Konzernen • Erarbeiten von Sicherheitsmaßnahmen bei Reisen oder Entsendung von Mitarbeitern ins Ausland • Einführen eines Krisenmanagements • Reagieren in internationalen Krisensituationen • Steuern der globalen Krisenkommunikation • Beeinflussen der öffentlichen Wahrnehmung zu Sicherheitsthemen

Inhalte	<ul style="list-style-type: none"> • Sicherheitsmanagement in globalen Organisationen • Travel Security • Sicherheit bei Entsendung von Mitarbeitern • Krisenmanagement im internationalen Umfeld • Krisenkommunikation: Prinzipien und Vorgehensweisen bei der Kommunikation in Krisenfällen • Interne und externe Krisenkommunikation • Message House • Umgang mit den Medien in Krisensituationen • Außenwirkung von Sicherheit • Kampagnen für Sicherheitsthemen
Lehr- und Lernmethoden	<p>Interaktiver Mix aus Vorlesung, Erarbeiten und Vortragen von Inhalten, Demonstration von Konzepten, praktischen Aufgaben in Gruppen, Erarbeiten von eigenen Inhalten und Rollenspiel.</p>
Literatur	<ul style="list-style-type: none"> • Notfall- und Krisenmanagement im Unternehmen von Axel Bédé, 2009. • Unternehmenskrisen und Krisenmanagement von Ronny Scharschmidt, 2009. • Führen in Krisensituationen von Markus Klaus, 2008. • Global Threat: Target-Centered Assessment and Management von Robert Mandel, 2008. • Security Risk Management Body of Knowledge von Julian Talbot und Miles Jakeman, 2009.
Besonderes	

4. Recht, Compliance und Datenschutz

Modul-Kurzzeichen	SM_MA_RechtComplianceDatenschutz
Modulbezeichnung	Recht, Compliance und Datenschutz
ggf. Aufteilung in Lehrveranstaltungen	
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SecMan Master, 1. Semester, Pflichtmodul
Verwendbarkeit des Moduls	
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Michaela Schröter
Dozent/in	Prof. Dr. Michaela Schröter, Dr. Raoul Kirmes M. Sc., CISA, QMA
Lehrsprache	Deutsch
Voraussetzungen	
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 Stunden Vorlesung inklusive Arbeit an Fallbeispielen, 90 h Eigenstudium und 30 h Prüfungsvorbereitung
Lehrform/SWS	Vorlesung: 60 Stunden
Studien-/ Prüfungsleistungen	Klausur und/oder Hausarbeit + Referat oder mündliche Prüfung.
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	<p>Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen:</p> <ul style="list-style-type: none"> • Erlangung von Fertigkeiten zum Erkennen der relevanten Rechtslage für die wesentlichen sicherheitsbezogenen Aktivitäten in Unternehmen • Anwenden von nationalen , europäischen und internationalen Rechtsvorschriften zur Erfüllung von Compliance-Vorgaben für Unternehmen • Befähigung zur kritischen Auseinandersetzung mit rechtlichen Zielkonflikten und zur Abgabe einer angemessenen Beurteilung der Risikosituation für Unternehmen als Regelungsbetroffene

Inhalte	<ul style="list-style-type: none"> • Einführung in die juristische Methodik • Europäisches und Int. Sicherheitsrecht • Einführung in das WTO-Recht (schw. int. Produktsicherheitsrecht) • System der Grundfreiheiten und nationale Sicherheitsinteressen • Technische Handelshemmnisse im Sicherheitsrecht • Compliance im Int. Kontext • Intern, europäisches und nat. Akkreditierungsrecht • Grundlagen vertraglicher Haftung (§§280 BGB) • Grundlagen deliktischer Haftung (§§823ff BGB, ProdHaftG) • Recht des privaten Sicherheitsgewerbes • Überblick zum deutschen Waffenrecht • Grundzüge Strafverfahrensrechts • elektronischer Rechtsverkehr (eCommerce/Signaturrecht) • Int. Bezüge und Grundlagen des Datenschutzrechtes
Lehr- und Lernmethoden	Vorlesung

Literatur	<ul style="list-style-type: none"> • Harald Jele, Wissenschaftliches Arbeiten: Zitieren, Kohlhammer, 3. Aufl., 2012 • Calliess/Ruffert, EUV/AEUV 4. Auflage 2011. • Röhl, Akkreditierung und Zertifizierung im Produktsicherheitsrecht, Springer Verlag 2000. • Ensthaler, Zertifizierung und Akkreditierung technischer Produkte, Springer Verlag 2007. • Martin Schulte, Handbuch des Technikrechts, 2. Aufl. Springer Verlag, 2010. • bbott/ Kirchner/ et.al., International Standards and the Law, Stämpfli Verlag AG, 2005. • Kurt Schellhammer, Schuldrecht nach Anspruchsgrundlagen, Auflage: 8., 2011. • Martin Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, BWV Verlag, 2006. • olf Stober, Sven Eisenmenger, Besonderes Wirtschaftsverwaltungsrecht, 15 Aufl., Verlag Kohlhammer, 2011 • Knemeyer: Polizei- und Ordnungsrecht, Beck, 2007 • Busche: Waffenrecht 2012, Kiel 2012 • Hoeren: Internet- und Kommunikationsrecht, Otto Schmidt Köln 2012 • Schade: Arbeitsrecht, Kohlhammer 2010 • Martin T. Biegelman, Building World-Class Compliance Program: Best Practices and Strategies for Success, John Wiley & Sons; 2008. • Acquisti/ Gritzalis/Lambrinouidakis, Digital Privacy: Theory, Technologies, and Practices, Auerbach Pubn, 2007 • Sanjay Anand, Essentials of Sarbanes-Oxley, John Wiley & Sons, 2007. • CCH Incorporated, SEC Compliance and Disclosure Interpretations, Harcourt Professional Publishing, 2009. • Reyes, Carla, WTO-compliant Protection of Fundamental Rights: Lessons from the EU 'Privacy Directive, Melbourne Journal of International Law, Vol. 12, No. 1, Jun 2011: 141-176. • Spiros Simitis, Bundesdatenschutzgesetz, Nomos, Aufl. 8, 2014 • Aktuelle Gesetzestexte
Besonderes	Intensives Lesepensum

5. Organisatorische Aspekte des Sicherheitsmanagements

Modul-Kurzkennzeichen	SM_MA_OrgAsp_Sicherheitsmanagement
Modulbezeichnung	Organisatorische Aspekte des Sicherheitsmanagements
ggf. Aufteilung in Lehrveranstaltungen	<ul style="list-style-type: none"> • Unternehmensführung und Sicherheitsstrategie • Physische Sicherheit
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SecMan Master, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls	
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Ivo Keller
Dozent/in	Prof. Dr. Oliver Weissmann, Prof. Dr. Ivo Keller Holger Könnecke, Gerhard Reinhardt
Lehrsprache	Deutsch
Voraussetzungen	
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS	Vorlesung: 30 h, Übung mit Bearbeitung von Fallbeispielen: 30 h
Studien-/ Prüfungsleistungen	Praktische Arbeit + Referat und/oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote

<p>Lernergebnisse</p>	<p>Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen:</p> <ul style="list-style-type: none"> • Kennen der Prinzipien erfolgreicher Unternehmensführung • Beeinflussen von Unternehmenslenkern hin zur Beachtung von Sicherheitsaspekten und zum konstruktiven Umgang mit Krisensituationen • Ableiten einer Sicherheitsstrategie und von Sicherheitszielen aus der Unternehmensstrategie • Entwickeln einer Strategie zur Stärkung der ethischen Aspekte der Unternehmensführung • Lösen von Konflikten • Kennen der Methoden der Schutz- und Sicherheitstechnik • Analysieren der Einsatzmöglichkeiten und Wirkungsweisen von Schutzmechanismen gegen Elementarschäden, mechanischen Sicherheitseinrichtungen, Gefahrenmeldeanlagen und Beobachtungseinrichtungen • Planen eines Sicherheitssystemverbunds • Bewerten von am Markt angebotenen Lösungen • Einschätzen der rechtlichen Grundlagen für den Einsatz der einzelnen Sicherheitsmechanismen
-----------------------	---

<p>Inhalte</p>	<ul style="list-style-type: none"> • Funktionen der Unternehmensführung (Entwicklung von Unternehmensziele, -grundsätze, -kultur; Formulierung von Strategien; Personal- und Verhandlungsführung; internationale Aspekte im globalen Wettbewerb) • Integration von Sicherheitszielen in die Unternehmensstrategie • Ethische Aspekte der Unternehmensführung (Anti-Korruptionsstrategien, Code of Conduct etc.) • Konfliktmanagement (Konfliktdiagnose, Typologie von Konflikten, Eskalationen, Strategien zur Konfliktbehandlung) • Grundlagen der Gebäudesicherheit • Begriffe und Überblick über Aufgabengebiete und Möglichkeiten • technische Grundlagen • Physische Angriffe und ihre Wirkung • Elementarschäden • Angreifer, Ziele und Angriffsmethoden • Waffen und ihre Wirkung • Abstrahlung elektronischer Geräte • Mechanische Sicherheitseinrichtungen und Zutrittskontrolle • Schlösser, Schließanlagen und ihre Sicherheit • Angriffssicherung an Türen und Fenstern und Zaunanlagen • Wertbehältnisse und Datensicherungsschränke • technische und rechtliche Vorschriften und Richtlinien • Gefahrenmeldeanlagen • Grundlagen • Einbruchmeldeanlagen • Überfallmeldeanlagen • technische Störungsmeldeanlagen • Brandmelde- und Brandbekämpfungsanlagen • technische und rechtliche Vorschriften und Richtlinien • Beobachtungseinrichtungen • technische Möglichkeiten • offene und verdeckte Überwachung • technische und rechtliche Vorschriften und Richtlinien • Notfallplanung und betriebliche Sicherheit • Folgeschädenanalyse • Handhabung von Vorfällen
<p>Lehr- und Lernmethoden</p>	<p>Vorlesung, Bearbeitung von Fallbeispielen in Kleingruppen, Vorstellung von Praxisbeispielen, Rollenspiele.</p>

Literatur	<ul style="list-style-type: none"> • K. Macharzina: Unternehmensführung: Das internationale Managementwissen Konzepte - Methoden – Praxis. 9. Aufl. 2015 • T. Hutzschenreuther: Krisenmanagement 2007 • F. Glasl:Konfliktmanagement: Ein Handbuch für Führungskräfte, Beraterinnen und Berater. 11. Aufl. 2013 • B. Stackpole, E. Osendahl: Security Strategy: From Requirements to Reality. 2010 • Physical Security Systems Handbook von Michael Kairallah, 2005. • Aktuelle Journale und Zeitschriften zum Thema: kes, • Der Sicherheitsberater, S&I
Besonderes	

6. Netzwerksicherheit

Modul-Kurzkennzeichen	SM_Ma_Netzwerksicherheit
Modulbezeichnung	Netzwerksicherheit
ggf. Aufteilung in Lehrveranstaltungen	
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SecMan Master, 1. Semester, Pflichtmodul
Verwendbarkeit des Moduls	
Häufigkeit des Angebots von Modulen	jedes Studienjahr
Autor/in	Prof. Dr. Eberhard von Faber
Dozent/in	Prof. Dr. Eberhard von Faber, Dipl.-Ing. Dietmar Hausmann
Lehrsprache	Deutsch
Voraussetzungen	Bedeutung der IT-Sicherheit und deren Rolle in der Praxis; technische und physikalische Grundkenntnisse; Kenntnisse zu den Grundlagen von Internet-Netzwerken, Betriebssystemen und kryptographiebasierten Techniken
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS	Vorlesung im Umfang von mindestens 30 Stunden sowie Übungen von bis zu 30 Stunden
Studien-/ Prüfungsleistungen	Praktische Arbeit + Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	<ul style="list-style-type: none"> • Kennenlernen der Bedrohungen und Herausforderungen in Netzwerken sowie wichtiger Gegenmaßnahmen in Form von Protokollen und diversen Sicherheitslösungen • Kennenlernen der Funktionsweise dieser Lösungen, Verständnis ihres Einsatzes, Betriebes und Zusammenwirkens; Fähigkeit, einige dieser Lösungen selbst zu integrieren und einzusetzen; Kennenlernen ergänzender Maßnahmen und Lösungen • Entwicklung der Fähigkeit, Anforderungen und industrielle Praxisfaktoren zu analysieren und Lösungen am praktischen Beispiel einer Branchenlösung zu integrieren • Kennenlernen von Sicherheitsmodulen und eingebetteten Systemen als Kernkomponenten für verteilte Systeme; Eigenschaften, Herausforderungen und Einsatz

Inhalte	<ul style="list-style-type: none"> • Erweiterte Grundlagen von Internet-Netzwerken (TCP/IP-Protokoll, ISO/OSI, Routing, aktive Komponenten, Kryptographie) • Gefahren beim Einsatz von IT, Kategorien von Bedrohungen, Schwachstellen und Gefährdungen • Sicherheitsmanagement, Sicherheitsaudits mit Tools, Netzwerkmonitoring und Netzwerklogging • Attacken und Gegenmaßnahmen • Kryptographieanwendungen (verschlüsselte Kommunikation, VPN-Protokolle, Zertifikate) • Web-Server-Sicherheit, E-Mail-Sicherheit • Vertiefung und praktische Anwendung in Projektthemen zu Firewalls, Honeypots und Intrusion-Detection-Systems, WLAN-Sicherheit und VPN
Lehr- und Lernmethoden	Kombination aus Vorlesung, Übungen am eigenen Computer und Übungen im Labor; Vorlesung mit gemischten Medien; Aufgaben und Übungsbeispiele; Kontrollfragen/Repetitorium
Literatur	<ul style="list-style-type: none"> • Cisco Networking Academy: CCNA Exploration Companion Guide, Bnd. 1-4, Cisco Press, 2008 • Alexander Michael: Netzwerke und Netzwerksicherheit - Das Lehrbuch, Hüthing Verlag, 2006. • Plötner Johannes, Wendzel Steffen: Praxishandbuch Netzwerk-Sicherheit, Galileo Computing, 2007. • Projektthemen (VPN, IPSec, IPv6, IDS, WLAN, Angriffe, u.a.m) <p>Skripte und andere Lehrmaterialien werden während der Vorlesung direkt an die Studierenden verteilt bzw. stehen auf der Lernplattform der Hochschule zur Verfügung.</p>
Besonderes	

7. Mathematisch-technische Grundlagen der IT-Sicherheit

Modul-Kurzzeichen	SM_MA_MathTechGrundlagen
Modulbezeichnung	Mathematisch-technische Grundlagen der IT-Sicherheit
ggf. Aufteilung in Lehrveranstaltungen	Grundlagen von Forensik und Auditing, Grundlagen technischer Sicherheit: Kryptographie
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SecMan Master, 1. Semester, Pflichtmodul
Verwendbarkeit des Moduls	Das Modul ist in dem Masterstudiengang Wirtschaftsinformatik als Vertiefungsfach für die Spezialisierungsrichtung „Informationssicherheit“ verwendbar.
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Igor Podebrad
Dozent/in	Prof. Dr. Igor Podebrad, Prof. Dr. Michael Syrjakow
Lehrsprache	Deutsch
Voraussetzungen	
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS	Vorlesung: 60 Stunden
Studien-/ Prüfungsleistungen	Hausarbeit/Klausur/mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	<p>Im Bereich von „Forensik und Auditing“ ist es das Ziel der Lehrveranstaltung, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen:</p> <ul style="list-style-type: none"> • Sichere Anwendung der mathematischen und technischen Grundlagen der Sicherheit, insbesondere • Organisieren von IT-forensischen Analysen und IT-Audits • Betreiben von IT-Systemen unter Berücksichtigung der Anforderungen an IT-Forensik und IT-Audit • Entwickeln und Durchsetzen von IT-Forensik-bezogenen Sicherheitsrichtlinien • Bewerten der Verwendbarkeit von IT-Audit-Ergebnissen für Forensik <p>Im Kontext der „technischen Sicherheit“ ist es das Ziel der Lehrveranstaltung, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen:</p>

	<ul style="list-style-type: none"> • Symmetrische Verschlüsselung: informations-theoretisch sichere Verschlüsselung, klassische Verschlüsselungsverfahren, Blockchiffren (DES, AES), Stromchiffren, Verschlüsselungsmodi (z.B. CBC), Angriffe • Asymmetrische Verschlüsselung: RSA, Diffie-Hellman-Schlüsselaustausch, zahlentheoretische Grundlagen (Euklidischer Algorithmus, modulare Arithmetik, etc.), Angriffe • Nachrichtenauthentifizierung, digitale Signaturen, Public-Key-Infrastruktur (PKI), Angriffe • Aktuelle Trends in der Kryptographie (Quantenkryptographie, etc.)
Inhalte	<ul style="list-style-type: none"> • Gesetzliche Voraussetzungen für IT-Forensik • Prinzipien von IT-Audit • Organisation von IT-forensischen Analysen • Grundlagen kryptografischer Verfahren
Lehr- und Lernmethoden	Vorlesung und Übungen in Kleingruppen.
Literatur	<ul style="list-style-type: none"> • IT-Forensik von Alexander Geschonnek, 2011 • The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons, 2012 • Wolfgang Ertel: Angewandte Kryptographie; Fachbuchverlag Leipzig im Carl Hanser Verlag, 2003. • Klaus Schmech: Kryptografie: Verfahren, Protokolle, Infrastrukturen; dpunkt Verlag, 2009.
Besonderes	Im Bereich der Kryptographie: Verwendung des Werkzeugs „CrypTool“ zum Experimentieren mit kryptographischen Verfahren

8. Sichere IKT-Infrastrukturen und IT-Dienste

Modul-Kurzzeichen	SM_MA_SichereIKTInf_ITDienste
Modulbezeichnung	Sichere IKT-Infrastrukturen und IT-Dienste
ggf. Aufteilung in Lehrveranstaltungen	Teil A (WiSe), „Grundlagen und Anwendungen der Kryptographie und des Identitäts- und Zugriffsmanagements (IAM)“ Teil B (SoSe), „Sicherheitslösungen, IT Outsourcing, Cloud, industrielle IT-Produktion und sichere IT-Dienste“
Dauer des Moduls	Zweimestrig
Zuordnung zum Curriculum	SM Ma, 1. und 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls	Die beiden Lehrveranstaltungen des Moduls sind soweit in sich abgeschlossen, dass sie in beliebiger Reihenfolge belegt werden können.
Häufigkeit des Angebots von Modulen	jedes Studienjahr
Autor/in	Prof. Dr. Eberhard von Faber
Dozent/in	Prof. Dr. Eberhard von Faber
Lehrsprache	Deutsch
Voraussetzungen	Bedeutung der IT-Sicherheit und deren Rolle in der Praxis, technische und physikalische Grundkenntnisse, Kenntnisse zur Informations- und Kommunikationstechnologie: Anwendungen, Systeme und Netze sowie zugrundeliegende Technologien.
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS	2 x 2 SWS in Blöcken von vier Lehrveranstaltungen je Semester, insgesamt 60 Stunden. Vorlesung mit gemischten Medien, Angebot von Selbststudium und Hausaufgabe zur Vertiefung und Selbstkontrolle sowie Kontrollfragen/Repetitorium.
Studien-/ Prüfungsleistungen	Klausur oder mündliche Prüfung jeweils über Teil A und B (zwei Prüfungen)
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote

<p>Lernergebnisse</p>	<p>Die Lernenden sollen in die Lage versetzt werden, die folgenden grundsätzlichen Kenntnisse und Fertigkeiten zu erlangen:</p> <p>Teil A - Grundlagen und Anwendungen der Kryptographie und des Identitäts- und Zugriffsmanagements (IAM):</p> <ul style="list-style-type: none"> • Entwicklung der Fähigkeit, Anforderungen und industrielle Praxisfaktoren zu analysieren und Lösungen auch in Branchenlösungen zu integrieren • Erlernen von Grundlagen der Kryptografie und ihrer praktischen Anwendung sowie den Grenzen bzw. den Aufgaben für das Schlüsselmanagement • Gewinnen von detaillierten Kenntnissen auf dem Gebiet „Identity and Access Management (IAM)“. Grundbegriffe sowie Architekturen und Technologien für Unternehmen und in komplexen Wertschöpfungsketten. <p>Teil B - Sicherheitslösungen, IT Outsourcing, Cloud, industrielle IT-Produktion und sichere IT-Dienste:</p> <ul style="list-style-type: none"> • Verstehen, wie Anforderungen systematisch analysiert und umgesetzt werden; Entwicklung der Fähigkeit, selbst Sicherheit zu konzipieren und zu bewerten • Prüfschemata als internationale Infrastruktur für das Risikomanagement • Entwicklung der Fähigkeit, benötigte Lösungen adäquat in verschiedenen ITK-Infrastrukturen und Nutzungsszenarien zu integrieren • Kenntnisse und Fertigkeiten erlangen zu Technik und Organisation moderner (industrieller) ICT-Produktion und diesbezüglicher Sicherheitsfragen sowie zur Nutzung und Einbindung von IT-Diensten in Geschäftsprozesse (Sicherheit, Bewertung und Auswahl von IT-Diensten)
<p>Inhalte</p>	<p>Teil A - Grundlagen und Anwendungen der Kryptographie und des Identitäts- und Zugriffsmanagements (IAM):</p> <ul style="list-style-type: none"> • Lernbeispiel der speziellen Branchen-Anwendung „Bezahlsysteme“: Anforderungen und Lösungen; Praxisfaktoren und Auswirkungen, industrielle Praxis • Grundlagen der Kryptografie; Schlüsselmanagement • Absicherung von Geschäftsprozessen; Grundbegriffe IAM (alles von Administration bis Accounting), • Autorisierung: Leistungen und Grenzen; Strategien (DAC, MAC, RBAC, IF); Realisierung (Gruppen, Rollen, ACL, Capabilities); Alternativen; Trends und Ausblick, • Authentisierung: Arten, Methoden, Technologien; Probleme und Lösungen; Architekturen und verteilte Systeme (z.B. LDAP, RADIUS, Kerberos, ESSO, Single Sign-On, Federation), • IAM-Architekturen (das ganze Bild) <p>Teil B - Sicherheitslösungen, IT-Outsourcing, Cloud, industrielle IT-Produktion und sichere IT-Dienste:</p>

	<ul style="list-style-type: none"> • Grundbegriffe der Informationssicherheit; Design-Ziele und Methoden zur Entwicklung adäquater Sicherheitsmaßnahmen • Assurance: eine Infrastruktur für „Vertrauen“ und „Sicherheit“ bei (globaler) Arbeitsteilung in industriellen Wertschöpfungsketten • Integration der verschiedenen Lösungen im ITK-Verbund • Vorteile und Probleme beim Outsourcing; Methoden zur Aufgliederung der Risiken und ihrer Bewertung • Risikomanagement für Anwenderunternehmen bei Nutzung von Fremdleistungen • Herausforderungen und Lösungen für IT-Dienstleister: Komplexität großtechnischer IT-Produktion und Herausforderungen der IT-Security; Rolle von Prozessen und Automation; ESARIS
Lehr- und Lernmethoden	Kombination aus Vorlesung, Aufgaben und Übungsbeispielen, Vorlesung mit gemischten Medien, Kontrollfragen/ Repetitorium sowie Hausaufgaben.
Literatur	<p>Teil A:</p> <ul style="list-style-type: none"> • Anderson, Ross: Security Engineering, A Guide to Building Dependable Distributed Systems; John Wiley & Sons • Alexander Tsolkas und Klaus Schmidt: Rollen und Berechtigungskonzepte, Ansätze für das Identity- und Access Management im Unternehmen; 2010, Vieweg+Teubner • Claudia Eckert: IT-Sicherheit, Konzepte - Verfahren – Protokolle; Oldenbourg-Verlag, 2013 <p>Teil B:</p> <ul style="list-style-type: none"> • Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond; Springer-Vieweg. 2013 • Datenschutz und Datensicherheit, DuD, Heft 10/2016: Schwerpunkt „Informationssicherheit beim IT-Outsourcing“, Herausgegeben von Eberhard von Faber; diverse Beiträge auf ca. 40 Seiten, Springer, ISSN 1614-0702 • Open Enterprise Security Architecture (O-ESA); The Open Group, Van Haren Publ., 2011, ISBN 978 90 8753 672 5 • Martin Kappes: Netzwerk- und Datensicherheit, Eine praktische Einführung; Vieweg+Teubner • Common Criteria for Information Technology Security Evaluation; www.commoncriteriaportal.org oder ISO 15408 • www.ital.org <p>Skripte und andere Lehrmaterialien werden während der Vorlesung direkt an die Studierenden verteilt.</p>
Besonderes	

9. Secure Systems Lifecycle Management

Modul-Kurzzeichen	SM_MA_SecureSystems
Modulbezeichnung	Secure Systems Lifecycle Management (SSLM)
ggf. Aufteilung in Lehrveranstaltungen	
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SecMan Master, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls	Das Modul kann auch als WPF für WI und Informatik Master angeboten werden.
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Ivo Keller
Dozent/in	Prof. Dr. Ivo Keller, Sandro Hartenstein, Marcel Niefindt
Lehrsprache	80% Deutsch, 20% Englisch
Voraussetzungen	Erste Erfahrungen im Programmieren von Web-Anwendungen für das Beispiel-Szenario. Dies sollte i.d.R. durch das bis zu diesem Zeitpunkt absolvierte Studium sichergestellt sein. Ansonsten: Selbststudium, z.B. mit PHP 5.3: Dynamische Websites professionell programmieren von Christian Wenz und Tobias Hauser (Dezember 2009)
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)
Lehrform/SWS	30 h Vorlesung, 30 h Übungen
Studien-/ Prüfungsleistungen	Praktische Arbeit und Referat oder mündliche Prüfung
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote

Lernergebnisse	<p>Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen:</p> <ul style="list-style-type: none"> • Kennen und Anwenden der vermittelten Best Practices während der Entwicklung von IT-basierten Systemen für sichere Software • Entwickeln von Akzeptanzkriterien für nicht-funktionale Sicherheitsanforderungen • Durchführen von Bedrohungsmodellierungen • Vermeiden von Schwachstellen während der Entwicklung • Durchführen von Sicherheitstests • Sicheres Installieren und Betreiben von Software • Etablieren eines Security Response Programms • Analysieren von bestehender Software auf Sicherheitsschwachstellen • Entwickeln und umsetzen eines Schutzprogramms für Software während der Systementwicklung • Etablieren eines Management-Systems für Sicherheit im Entwicklungsprozess, Integrieren dieses Management-Systems in einen eventuell vorhandenen Qualitätsprozess • Durchführen von Sicherheitsanalysen („Hacking“) • Darstellen von Untersuchungsergebnissen
Inhalte	<p>Grundsätze der sicheren Software-Entwicklung:</p> <ul style="list-style-type: none"> • Sicherheitsanforderungen • Sicheres Design und Bedrohungsmodellierung • Architekturanalysen • Sicheres Kodieren • Sicherheitstests • Sichere Einrichtung • Security Response • Schutz der eigenen Software vor Manipulation und Know-how-Diebstahl • Common Criteria/ISO 15408
Lehr- und Lernmethoden	<p>Interaktiver Mix aus Vorlesung, Übungen am eigenen Computer, Übungen im Labor, Erarbeiten und Vortragen von Inhalten, Demonstration von Konzepten, praktischen Aufgaben in Gruppen.</p>
Literatur	<p>Basiswissen sichere Software von Friedrich Holl, dpunkt 2011. Software-Qualität, Testen, Analysieren und Verifizieren von Software von Peter Liggesmeyer, Spektrum Akademischer Verlag, 2002. Writing Secure Code von Michael Howard & David LeBlanc, 2003 www.owasp.org</p>
Besonderes	<p>Anwendung des Wissens u.a. in Pflichtfach „Wissenschaftliches Arbeiten“, Modul „Projekt“. Wird begleitet durch das Fraunhofer-Projekt „Weiterbildungsprogramm von Fachkräften in der IT-Sicherheit“</p>

10. Wissenschaftliches Schreiben

Modul-Kurzkennzeichen	SM_MA_WissSchreiben
Modulbezeichnung	Wissenschaftliches Schreiben
ggf. Aufteilung in Lehrveranstaltungen	Semesterarbeit 1 Semesterarbeit 2
Dauer des Moduls	Zweisemestrig
Zuordnung zum Curriculum	SecMan Master, 1. und 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls	
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Ivo Keller
Dozent/in	Prof. Dr. Ivo Keller
Lehrsprache	Deutsch
Voraussetzungen	
ECTS-Credits	6
Gesamtworkload und ihre Zusammensetzung	180 h = 60 h Präsenzstudium, Konsultationen und 120 h betreutes Erstellen einer Ausarbeitung
Lehrform/SWS	Vorlesung und Seminar mit Referat: 60 Stunden; 2 x 2 SWS
Studien-/ Prüfungsleistungen	Schriftliche Arbeit
Gewichtung der Note in der Gesamtnote	6,25% der Abschlussnote
Lernergebnisse	Erstellen von wissenschaftlichen Arbeiten unter Anleitung im Themenfeld der Sicherheit
Inhalte	<ul style="list-style-type: none"> • Erhebungsmethoden (Statistik, Interview, primär/sekundär Quellen) • Quellendiskussion: recherchieren, lesen, bewerten • Kreativtechniken und Selbstorganisation • situationsbezogene Anforderungen an Schreibstile (Werbung, Pressemitteilung, wiss. Arbeit ...) • Erstellung eines Exposés • Methodischer Aufbau wiss. Arbeiten • Phasen des wissenschaftlichen Arbeitens • Materialsammlung und Recherche • Materialbewertung und -Auswahl • Material- und Themenbearbeitung • Zitiersysteme
Lehr- und Lernmethoden	Vorlesung, Diskussion, Vorstellen der eigenen Ergebnisse.

Literatur	<ul style="list-style-type: none"> • DIN 1421 (Gliederung und Benummerung in Texten) • Eco, U. (2005) • ZBW, gesis, Rat SWD (Hg.): Auffinden – Zitieren - Dokumentieren. 2014 (www.auffinden-zitieren-dokumentieren.de) • Wie man eine wissenschaftliche Abschlussarbeit schreibt - Doktor-, Diplom- und Magisterarbeit in den Geistes- und Sozialwissenschaften, Müller, Heidelberg • Theisen, Manuel R.: Wissenschaftliches Arbeiten - Technik Methodik, Form, 2000. • Peterßen, Wilhelm H.: Wissenschaftliche(s) Arbeiten - Eine Einführung für Schule und Studium, 1999.
Besonderes	

11. Projekt

Modul-Kurzkennzeichen:	SM_MA_Projekt
Modulbezeichnung:	Projekt
ggf. Aufteilung in Lehrveranstaltungen:	
Dauer des Moduls:	Einsemestrig
Zuordnung zum Curriculum:	SecMan Master, 2. Semester, Pflichtmodul
Verwendbarkeit des Moduls:	
Häufigkeit des Angebots von Modulen:	Jedes Studienjahr
Autor/in:	Prof. Dr. Ivo Keller
Dozent/in:	Prof. Dr. Ivo Keller
Lehrsprache:	Deutsch
Voraussetzungen:	
ECTS-Credits:	6
Gesamtworkload und ihre Zusammensetzung:	180 h = 60 h Präsenz-, 90 h Eigenstudium und 30 h Referatsvorbereitung („Verteidigung“)
Lehrform/SWS:	Vorlesung, Seminar und Betreuung der Projektgruppen: 60 Stunden
Studien-/ Prüfungsleistungen:	Praktische Arbeit + Referat
Gewichtung der Note in der Gesamtnote:	6,25% der Abschlussnote
Lernergebnisse:	<p>Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen:</p> <ul style="list-style-type: none"> • Durchführen von Sicherheitsprojekten • Planen eines sicherheitsbezogenen Projekts unter ganzheitlicher Beachtung der Anforderungen • Anwenden von Projektmanagement-Methoden

Inhalte:	<ul style="list-style-type: none"> • Problemerkennung: <ul style="list-style-type: none"> - wissenschaftliche Erarbeitung des „State of the Art“ - Einbindung in den vorhandenen praktischen Kontext - Rahmenbedingungen des Einsatzes • Nutzung unterschiedlicher Analysetechniken wie bspw. Interviewmethode, Fragebogen Delphi-Methode, Erarbeitung der Kontextes über Dokumente usw. • Sollkonzeptentwicklung: <ul style="list-style-type: none"> - wissenschaftlich fundierte Entwicklung eines praxisorientierten Lösungsansatzes - Nutzung von Kreativmethoden - Kosten-/Nutzen-Analysen - Entwicklung von Rahmenbedingungen des Einsatzes • Prototypische Umsetzung <ul style="list-style-type: none"> - die prototypische Umsetzung erfolgt durch Entwicklung eines Software-Prototypen - Umsetzung im Unternehmen/Organisation oder Entwicklung bspw. eines Antrags auf Forschungs- und Entwicklungsförderung
Lehr- und Lernmethoden:	Vorlesung, praktisches Arbeiten in Gruppen bis maximal 7 Teilnehmer, Vorstellen der eigenen Ergebnisse.
Literatur:	<p>A Guide to the Project Management Body of Knowledge, PMI, 2008</p> <p>Krallmann (Hrsg.): Systemanalyse im Unternehmen - Prozessorientierte Methoden der Wirtschaftsinformatik, Oldenburg, 2007</p> <p>Office of Government Commerce: Erfolgreiche Projekte managen mit PRINCE2, The Stationery Office, 2009</p> <p>Jan Friedrich: Das V-Modell XT: Für Projektleiter und QS-Verantwortliche kompakt und übersichtlich, Springer 2009</p> <p>App, S.: Virtuelle Teams (Haufe TaschenGuide), 2013</p> <p>Bobikiewicz, L.: Virtual Meeting [Vting]: Ein Praxisbuch für verteilte Teams, Loop-2, 2014</p> <p>Literatur zum Projektthema wird im Rahmen der LV benannt.</p>
Besonderes:	Die Bereitschaft zu praktischem Arbeiten bei Kooperationspartnern und zur Zusammenarbeit mit den Projektmitgliedern wird vorausgesetzt.

12. Masterarbeit

Modul-Kurzkennzeichen	Masterarbeit
Modulbezeichnung	Masterarbeit incl. Masterseminar
ggf. Aufteilung in Lehrveranstaltungen	Masterarbeit Master-Kolloquium
Dauer des Moduls	Einsemestrig
Zuordnung zum Curriculum	SecMan Master, 3. Semester, Pflichtmodul
Verwendbarkeit des Moduls	Das Modul dient dem Abschluss des Studiums
Häufigkeit des Angebots von Modulen	Jedes Studienjahr
Autor/in	Prof. Dr. Ivo Keller
Dozent/in	Der Erstgutachter einer Master-Arbeit muss ein Professor der Technischen Hochschule Brandenburg sein. Der Zweitgutachter wird in Abstimmung mit dem Erstgutachter ausgewählt
Lehrsprache	Deutsch/Englisch (nach Wahl des Studenten)
Voraussetzungen	Zur Master-Arbeit kann sich grundsätzlich nur anmelden, wer alle Prüfungsleistungen bis auf die Wahlpflichtmodule erfolgreich absolviert hat.
ECTS-Credits	21
Gesamtworkload und ihre Zusammensetzung	600 h Erarbeitung der Thesis inkl. Konsultationen
Lehrform/SWS	Betreute Erarbeitung der Thesis
Studien-/Prüfungsleistungen	Master-Arbeit (87,5%) Kolloquium (12,5%)
Gewichtung der Note in der Gesamtnote	30 % der Abschlussnote
Lernergebnisse	<p>Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen:</p> <p>Erstellen einer wissenschaftlichen Arbeit unter Anleitung mit eigenen kreativen und/oder konstruktiven Anteilen im Themenfeld des „Security Management“ in einem Zeitraum von 4 Monaten (in Teilzeit von 8 Monaten).</p> <p>Das Master-Kolloquium dient der Präsentation der Masterarbeit; im Rahmen dieser mündlichen Prüfung stellt der Kandidat die Ergebnisse seiner Masterarbeit vor und verteidigt diese vor dem Plenum.</p>

Inhalte	<p>Die Masterarbeit dient der zusammenhängenden Beschäftigung mit einem umfassenden Thema und der daraus resultierenden Lösung einer theoretischen oder praktischen Problemstellung.</p> <p>Im Rahmen des Kolloquiums findet eine mündliche Prüfung und Diskussion statt.</p>
Lehr- und Lernmethoden	<p>Selbststudium unter Anleitung.</p> <p>Masterarbeit: Eigene wissenschaftliche Arbeit</p> <p>Kolloquium: Vorbereiten eines Vortrags und einer Diskussion, Erstellen von Präsentationsmedien</p>
Literatur	<p>Booth, W. C. et a. (1995). The draft of research. Chicago London</p> <p>Brown, S. R. et al. (1990) Experimental Design and Analysis. London</p> <p>Cialdini, R. B. (2001). Influence, Science and Practice. Bosten, M.A.</p> <p>Hussley, J., Hussley, R. (1997). Business Research. A practical guide for undergraduate and postgraduate students</p> <p>Karmasin, M. et al. (1999). Die Gestaltung wissenschaftlicher Arbeiten: ein Leitfaden für Haus-, Seminar- und Diplomarbeiten sowie Dissertationen. Wien</p> <p>Pyrzack, S. et. Al. (1998). Writing empirical Research Reports. Los Angeles. C.A.</p> <p>Seale, C. (1999). The quality of quantitative research. London</p> <p>Trachim, W. M. K. (2000). The Research Knowledge Base. Cincinatti. Ohio</p>
Besonderes	