Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 21.09.2020

Modulnummer:
MCSM 101, MCSMT 101

Modulbezeichnung:
Theoretische Grundlagen zu forensischen Methoden

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Meuser

Studiengang:
MCSM, MCSMT

Semester:
1. Fachsemester

Angebotsturnus:
jedes Semester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- Aspekte aus den Bereichen der Netzwerkforensik, Mobilfunkforensik, elektronische Forensik sowie Compliance-Themen anzuwenden und diese den jeweiligen Bereichen der IT-Landschaft der Organisationen zuordnen.
- die Besonderheiten und Herausforderungen bei der forensischen Analyse in den Bereichen der Analyse, Präsentation und Dokumentation zu verstehen und diese ggfls. im Kontext der forensischen Methodik berücksichtigen.
- mit Hilfe der Methoden zur digitalen Forensik Grundverständnisse zu entwickeln, um mit spezifischen Werkzeugen Gefahrenabwehrpläne zu entwickeln und Handlungsmaßnahmen, Rückschlüsse auf Angriffsvektoren zu konzipieren sowie deren langfristige Bekämpfung zu erzielen.

Inhalte des Moduls:
Anwendungsszenarien, Maßnahmen und die prinzipiellen Vorgehensweisen und Möglichkeiten der Computer Forensik werden dargestellt, um die die Möglichkeiten und Erfolgsaussichten der Computer Forensik insb. auch auf mobilen Geräten abschätzen zu können. Es wird vermittelt, wie die forensisch erfassten Daten als Beweismittel in Form eines Reports gerichtsverwertbar zu sichern und zu dokumentieren sind. Die Unterschiede und Grenzen der ‚mobilen' Forensik zur traditionellen PC-Forensik werden deutlich gemacht.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Überblick über die IT-Forensik
- Grundsätze, Ziele und Vorgehensweise bei einer IT-Forensischen Untersuchung
- Zu berücksichtigende rechtliche Aspekte
- Forensische Modelle zur Analyse, Präsentation und Dokumentation der IT-Angriffe
- Identifizierung und Datensicherung von relevanten Datenquellen
- Wiederherstellung von gelöschten und geänderten Daten
- Dateianalyse: Allocated, Unallocated, Carving
- Parallelen und Gemeinsamkeiten der Forensik zur Mobilfunkforensik
- der Analyse und der Sicherung von Daten von mobilen Geräten und der Erfassung der forensischen Daten
- Car Forensics (IoT und vernetzen Computer Technologie)
- Kennenlernen von IT-Forensik-Werkzeugen
- Zeitstempel Informationen einbinden (Timelines und Supertimelines)
- Anforderungen an ein Gutachten bzw. an einen Sachverständigenvertrag

Verwendete Literatur:
Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press
Geschonneck, A.: Computer Forensik. dpunkt Verlag

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 102, MCSMT 102

Modulbezeichnung:
Weiterführende Aspekte der ISM-Systeme und KRITIS

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
1. Fachsemester

Angebotsturnus:
jedes Semester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- Vulnerability der IT-Systeme zu erkennen und diese im Rahmen des Cyber Security Managements mit dem präventiven und detektiven IS-Einsatz zu bekämpfen.
- Managementsysteme nach einschlägigen Qualitäts- und Sicherheitsmerkmalen (QS + IT-Sicherheit) unter Verwendung des PDCA-Zyklus und KVP einführen, zu leiten und zu auditieren.
- Als second and third line of defense Sicherheitsprozesse und Projekte, die zur langfristigen Erhöhung der Resilienz der IT-Systeme führen, zu konzipieren.

- eine Implementierung von Informations-Sicherheits-Management-Systemen gemäß ISO/IEC 27001 / B3S und IT- Sicherheitsgesetz zu leiten.

Inhalte des Moduls:
Das Modul thematisiert die Abwicklung bzw. Organisation von ISMS-Projekten insbesondere in kritischen Infrastrukturen zur Umsetzung technischer und organisatorischer Anforderungen. Schwerpunkmäßig werden hierbei der Reporting-Prozess und Auditverfahren betrachtet.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Projektorganisation und Projektkommunikation
- technische und organisatorische Implementierung
- Durchführung von Workshops
- Wissensmanagement
- Reporting
- Durchführung von internen und externen Audits
- IS0/IEC 27001 / 27006
- ISMS-Projektorganisation
- Aufbau eines DMS zum Thema Wissensmanagement
- Durchführung, Koordination und Problembewältigung bei derartigen ISMS-Projekten
- Reporting-Prozesse (Management Review) und Auditverfahren

Verwendete Literatur:
- ISO/IEC 27001 / 27006 / IT-Grundschutz
- ISO 9001
- Thomas W. Harich; IT – Sicherheitsmanagement (Praxiswissen für IT Security Manager)

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 18.09.2020

Modulnummer:
MCSM 103, MCSMT 103

Modulbezeichnung:
Einführung in die Cyberkriminalität

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
1. Fachsemester

Angebotsturnus:
jedes Semester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- die nationale juristische Fachterminologie sowie die gesetzlichen Aspekte der IKT-Kriminalität im Sinne der Computerkriminalität zu erkennen und diese im Rahmen der Untersuchungen zu benutzen.
- die Aspekte der Beweismittelführung und des Computerbetrugs juristisch zu verstehen und diese einordnen.
- die rechtlichen Aspekte der EU – Legislative und Regelungen in Vereinigten Staaten sowie zwischenstaatliche Vereinbarungen G8, UN, ITU zu verstehen und diese differenziert zu betrachten.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 18.09.2020

Inhalte des Moduls:
In dem Modul werden die Grundlagen zu Kriminalität und Strafbarkeit allgemein vermittelt und darauf aufbauend ausgewählte Formen der Cyberkriminalität, unter Berücksichtigung der nationalen rechtlichen Grundlagen, betrachtet. Darüber hinaus wird der internationale Kontext der Cyberkriminalität anhand von Richtlinien und zwischenstaatlichen Vereinbarungen beleuchtet.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Internet und Kommunikation - Kriminalität (IuK und Computerkriminalität)
- Computerbetrug (§ 263a StGB)
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei
- Datenverarbeitung (§§ 269, 270 StGB)
- Datenveränderung (§ 303a)
- Computersabotage (§ 303b StGB)
- Ausspähen von Daten (§ 202a StGB)
- Abfangen von Daten (§ 202b StGB)
- Softwarepiraterie: Herstellen, Überlassen, Verbreiten oder Verschaffen von sog. "Hacker-Werkzeugen", die illegalen Zwecken dienen (§202c StGB)
- Cybercrime im internationalen Kontext
- Die EU-Cybercrime Richtlinie
- Computer Fraud and Abuse Act und nachfolgende Regelungen in Vereinigten Staaten
- Zwischenstaatliche Vereinbarungen, G8, UN, ITU

Verwendete Literatur:
- Strafgesetzbuch
- EU-Cybercrime Richtlinie

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 104, MCSMT 104

Modulbezeichnung:
Weiterführende Aspekte zum Entwurf sicherer IT-Systeme

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Stockmanns

Studiengang:
MCSM, MCSMT

Semester:
1. Fachsemester

Angebotsturnus:
jedes Semester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- die Integrationsfähigkeit neuer Lösungskonzepte in die existierende Architektur und Verifizierung Security-relevanter Features zu prüfen.
- Infrastrukturen und Systemlandschaften (Clients, Windows-/Linux-Server, Netzwerk, Firewalls, Storage, etc.) zu bewerten (beispielsweise für Embedded Systems).
- durch den Einsatz von sicherheitsspezifischen Methoden und Techniken die IT-Systeme unter Berücksichtigung der Prinzipien wie "Security by Design, Defense in Depth, Multilevel Security, Multilateral Security und Attack Surface Reduction, " zu gestalten.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Inhalte des Moduls:
Es erfolgt die Auseinandersetzung mit ausgewählten Entwurfsprinzipien und Entwurfsmustern für sichere IT-Systeme. Darüber hinaus werden Schwachstellen-Analysen und Angriffssimulation thematisiert und somit die Sicherheit von IT-System bzw. Security Policies und Sicherheitsmechanismen bewertet.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Internet und Kommunikation - Kriminalität (IuK und Computerkriminalität)
- Design - Prinzipien und Verfahren
- Objektorientierte Modellierung und Entwurf, Designpattern
- Security by Design
- Defense in Depth, Multilevel Security
- Bedrohungsanalysen
- Multilateral Security
- Attack Surface Reduction
- Least Privilege
- Design for Evil
- Security through Diversity
- Design und Bewertung von Security Policies, Sicherheitsmechanismen
- Schwachstellen-Analyse und Angriffssimulation

Verwendete Literatur:
Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle. 7. Auflage, Oldenbourg-Verlag, 2012.
Skriha, Walter, Schmitz, Roland: Sichere Systeme: Konzepte, Architekturen und Frameworks. Springer Verlag, 2009.

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 105, MCSMT 403

Modulbezeichnung:
Führungskompetenz

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Stockmanns

Studiengang:
MCSM, MCSMT

Semester:
1. Fachsemester

Angebotsturnus:
jedes Semester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Projektarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
Das Modul wird in folgenden Studiengängen angeboten: MBM, MWI Vollzeit, Dual, Teilzeit

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- innerhalb der Prozesse zur Personalgewinnung, - Entwicklung, -Motivation und -Führung durch gewonnene Kenntnisse mitzuwirken und die organisatorischen Prozesse effizient zu gestalten.

Inhalte des Moduls:
Die Studierenden lernen zunächst Führungsaufgaben, -eigenschaften, -qualifikationen und -kompetenzen kennen.
Sie lernen zudem den Stellenwert der Kommunikation in der Personalführung kennen. Von besonderer Bedeutung sind dabei Gespräche. Sie haben generell mehr Erfolg, wenn man die Regeln

sachlicher Gesprächsführung beachtet, die ebenso vermittelt werden wie die Spielregeln auf der Beziehungsebene.
Den Studierenden werden die Erkenntnisse aus der Motivationsforschung nahe gebracht. Beschäftigte können nur dann motiviert ihrer Arbeit nachgehen, wenn sie eine Chance auf Selbstbestätigung, Leistungserfolg, Anerkennung, Verantwortung, Beförderung und Aufstieg haben.
Die Studierenden lernen, dass Führung der Festlegung von Zielen dient, und zwar nicht nur rein sach- prozess- und strukturbezogen, sondern auch und gerade personenbezogen. Letztere sollen den Beschäftigten die Möglichkeit geben, sich zu entfalten.
Sie lernen die Planungsaufgaben von Führungskräften ebenso kennen wie die Notwendigkeit und die Abläufe der Festlegung und Koordination von Aufgabenbereichen, also der Delegation.
Es macht nur dann Sinn, per Delegation zu fordern, wenn man die Beschäftigten in die Lage versetzt, die anstehenden Aufgaben zu lösen. Insofern werden die Grundlagen der Personalentwicklung vermittelt.
Ferner werden die Studierenden als künftige Führungskräfte damit vertraut gemacht, wie man in und mit Gruppen kooperiert. Dazu tragen Führungskräfte mit ihrem Führungsstil bei, aber auch mit Ansätzen, Konflikte zu schlichten. Wenn einzelne zermürbt werden, nennt man das Mobbing, eine spezielle Form von Konflikten.
Weder Anerkennung noch Kritik sind ohne eine Meinungsbildung über Leistung und Arbeitsverhalten des Einzelnen, anders gesagt ohne Beurteilungen möglich, deren Abläufe die Studierenden abschließend erlernen.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Grundlagen, Techniken und Prozessen zur:
- Personalgewinnung,
- Personalentwicklung,
- Personalmotivation,
- Personalführung und
- Durchführung von Deeskalationsstrategien, Verhandlungsgeschick,
- Soziologischen Aspekte im Bereich der Führungskompetenzen

Verwendete Literatur:
Pflicht:
ein Fachbuch zur Personalführung
Empfehlungen für die Pflichtlektüre:
Blessin, B. u. Wick, A., Führen und führen lassen, 8. A., Konstanz 2017
Bröckermann, R., Führungskompetenz, Stuttgart 2011
Domsch, M. E., Regnet, E. u. Rosenstiel, L. v., Führung von Mitarbeitern, 3. A., Stuttgart 2012
Felfe, J., Mitarbeiterführung, Göttingen u. a. 2009
Hentze, J., Graf, A., Kammel, A. u. Lindert, K., Personalführungslehre, 4. A., Bern 2005
Hintz, A. J., Erfolgreiche Mitarbeiterführung durch soziale Kompetenz, 2. A., Wiesbaden 2013
Kets de Vries, M. F. R., Führer, Narren und Hochstapler, Stuttgart 2009
Lang, R. u. Rybnokova, I., Aktuelle Führungstheorien und -konzepte, Wiesbaden 2014
Lieber, B., Personalführung, 3. A., Konstanz 2017
Lohaus, D. u. Habermann, W., Führung im Mittelstand, München 2012
Niermeyer, R. u. Postall, N., Führen, 2. A., Freiburg 2008

Stippler, M., Moore, S., Rosenthal, S. u. Dörffer, T., Führung, 2. A., Gütersloh, 2011
Wagner, K., Rex, B. F. u. Eichler, M., Praktische Personalführung, 3. A., Wiesbaden 2003
Walenta, C. u. Kirchler, E., Führung, Wien 2011
Weibler, J., Personalführung, 3. A., München 2016
Withauer, K. F., Führungskompetenz und Karriere, Wiesbaden 2011
Wunderer, R., Führung und Zusammenarbeit, 8. A., München 2009
Wunderer, R. u. Grunwald, W., Führungslehre, Band 1 und 2, Berlin 1980
Ergänzend:
Bröckermann, R., Führung und Angst, Frankfurt 1989
Brooks, I., Organisational Behaviour, 4th Ed., Harlow 2009
Comelli, G., Rosenstiel, L. v. u. Nerdinger, F. W., Führung durch Motivation, 5. A., München 2014
Franken, S., Verhaltensorientierte Führung, 3. A., Wiesbaden 2010
Glasl, F., Konfliktmanagement, 11. A., Bern, Stuttgart 2013
Kanning, U. P., Diagnostik für Führungspositionen, Göttingen 2018
Kirchler, E. u. Walenta, C., Motivation, Wien 2010
Küpers, W. u. Weibler, J., Emotionen in Organisationen, Stuttgart 2005
Nerdinger, F. W., Motivation von Mitarbeitern, Göttingen u. a. 2003
Nerdinger, F. W., Blickle, G. u. Schaper, N. (Hrsg.), Arbeits- und Organisationspsychologie, 3. A., Berlin 2014
Regnet, E., Konflikt und Kooperation, Göttingen u. a. 2007
Sievers, B., Work, Death and Life Itself, Berlin 1994
Stürmer, S. u. Siem, B., Sozialpsychologie der Gruppe, München u. a. 2013
Stührenberg, L., Professionelle betriebliche Kommunikation, Wiesbaden 2003
Treier, M., Personalpsychologie im Unternehmen, München 2009
Watzlawick, P., Anleitung zum Unglücklichsein, 28. A., München, Zürich 1989

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 106, MCSMT 501

Modulbezeichnung:
IT-Governance und IT-Controlling

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Stockmanns

Studiengang:
MCSM, MCSMT

Semester:
1. Fachsemester

Angebotsturnus:
jedes Wintersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Klausurarbeit

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- Fach- und Methodenkompetenz zur Konzeption und Umsetzung von IT- Controlling-Strategien anzuwenden.
- die Wirkungsketten und Wirkungsnetze zu verstehen und diese umzusetzen.
- verschiedene IT-Controlling-Konzepte zu verstehen und strategische und operative IT-Controlling-Werkzeuge anzuwenden.
- ein allgemeines Controlling-Verständnis zu entwickeln.
- die wichtigen Konzepte und Methoden in den Bereichen IT-Strategie, IT-Projekte, IT-Betrieb zu verstehen.
- die Entwicklung einer IT-Strategie als Voraussetzung des IT-Controllings zu entwickeln und

Chancen und Risiken des IT-Controllings einzuordnen.
- Werkzeuge des IT-Controllings (Kennzahlensysteme, Portfolioanalyse, Benchmarking und Berichtswesen) anzuwenden und kritisch zu beurteilen und die gewonnenen Erkenntnisse am Beispiel von Fallstudien in die Praxis umzusetzen.

Inhalte des Moduls:
Es werden die Grundlagen in den Bereichen IT-Governance und IT-Compliance vermittelt: Im Teil IT-Governance werden die Aspekte Führung, Organisationsstrukturen und Prozesse betrachtet, wohingegen im Teil IT-Compliance die Einhaltung geltender Regelung in Anbetracht aktueller Themen, wie beispielsweise IT-Outsourcing, im Fokus steht.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung

Lehrsprache:
Deutsch

Inhalt:
- Grundlagen des IT-Controllings
- Strategisches und operatives IT-Controlling
- IT-Nutzenbewertung
- Portfolio-Controlling, Projekt-Controlling, Produkt-Controlling, Infrastruktur-Controlling
- Organisation des IT-Controllings
- Entwicklungstrends
- IT-Risikomanagement
- Organisatorische Gestaltung des Risikomanagements
- IT-Kosten- und Leistungsrechnung
- Service Level Agreements
- IT-Prozessmanagement
- IT-Outsourcing
- Moderation als IT-Controllingaufgabe
- Kostenrechnung für IT-Controller
- Deckungsbeitragsrechnung für IT-Controller
- Anwendungssysteme zur Unterstützung des IT-Controllings

Verwendete Literatur:
Pflicht:
Gadatsch, A./Mayer, E.: Masterkurs IT-Controlling, aktuelle Auflage
Frick, D./Gadatsch, A./ Schäffer-Külz, U.: Grundkurs SAP ERP. Geschäftsprozessorientierte Einführung mit durchgehendem Fallbeispiel, aktuelle Auflage

Ergänzend:
Kargl, H./Kütz, M.: IV-Controlling, aktuelle Auflage Krcmar, H.: Informationsmanagement, aktuelle Auflage Kütz, M.: IT-Controlling für die Praxis, aktuelle Auflage

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 20101, MCSMT 20101

Modulbezeichnung:
Social Engineering

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Wahlpflicht

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- menschliche Aspekte der Mensch-Maschinen-Interaktion (MMI) mit dem Fokus auf die informationstechnischen Fragestellungen und Handlungsfelder zusammenbringen.
- den Faktor „Mensch“ in den Bereichen der Informationssicherheit als Anwender, Beobachter, Regulierer und Angreifer zu erkennen.
- zielgerichtete Maßnahmen zur Sensibilisierung und Schulung sowie Akzeptanzerhöhung zu konzipieren.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Inhalte des Moduls:
Anhand der Herausstellung des Faktors Mensch als mögliche Schwachstelle in sozio-technischen Systemen werden die Grundlagen des Social Engineerings vermittelt. Hierbei werden die Perspektiven von Anwendern sowie Angreifern eingenommen, um so zielgerichtete organisatorische und technische Maßnahmen abzuleiten.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Übung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Grundlagen des Social Engineering
- Reziprozität
- Konsistenz
- Commitment
- Phishing
- Dumpster Diving
- Abwehrstrategien gegen Social Engineering

Verwendete Literatur:
Kevin D. Mitnick, William L. Simon: Die Kunst der Täuschung. Risikofaktor Mensch. mitp, Heidelberg 2006.
Cialdini, R. B.: Die Psychologie des Überzeugens. Verlag Hans Huber, 2007.
Stefan Schumacher: Psychologische Grundlagen des Social Engineering. In: Die Datenschleuder. 94, 2010.

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.09.2020

Modulnummer:
MCSM 20102, MCSMT 20102

Modulbezeichnung:
OSINT

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Wahlpflicht

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- menschliche Aspekte der Mensch-Maschinen-Interaktion (MMI) mit dem Fokus auf die informationstechnischen Fragestellungen und Handlungsfelder zusammenbringen.
- Den Faktor „Mensch“ in den Bereichen der Informationssicherheit als Anwender, Beobachter, Regulierer und Angreifer zu erkennen und heraus zielgerichtete Maßnahmen zur Sensibilisierung und Schulung sowie Akzeptanzerhöhung zu konzipieren.

Inhalte des Moduls:
Die Grundlagen des Bereiches Open Source Intelligence (OSINT) werden praxisnah vermittelt, indem die Arten von offenen Quellen und Vorgehensweisen zur Auswertung vorgestellt werden. Im Kontext

der automatisierten Erhebung und Auswertung von Informationen werden Aspekte des Themenfeldes Big Data betrachtet.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Übung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Grundlagen von OSINT
- Arten von offenen Quellen
- Automatisiertes Sammeln von Informationen
- Zusammenführen von Informationen
- Auswertung offener Quellen
- Big Data

Verwendete Literatur:
Arthuer S. Hulnick: 'The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?', pages 229-241, The Oxford Handbook of National Security Intelligence, 2010.

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 20201, MCSMT 20201

Modulbezeichnung:
Informationssysteme und Anwendungssysteme der Kritischen Infrastrukturen

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Wahlpflicht

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:

./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- Informationssysteme und Anwendungssysteme der Kritischen Infrastrukturen (z.B. KIS / NLT etc.) = Prozessnetzwerke zu verstehen
- Managen von externen Service Providern (insbesondere Security Operation Center) zu organisieren.
- Informationssysteme nach einschlägigen Qualitäts- und Sicherheitsmerkmalen (QS + IT-Sicherheit) unter Verwendung des PDCA-Zyklus und KVP einzuführen, zu leiten und zu auditieren.

- als second and third line of defense Sicherheitsprozesse und Projekte zu konzipieren, die zur langfristigen Erhöhung der Resilienz der IT-Systeme führen.

Inhalte des Moduls:
In diesem Modul werden die Informationssysteme und Anwendungssysteme der Kritischen Infrastrukturen anhand von Qualitäts- und Sicherheitsmerkmalen thematisiert. Hierzu werden beispielhaft branchen- bzw. sektorspezifische Systeme, wie Krankenhausinformationssysteme oder Netzleittechnik, betrachtet.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung

Lehrsprache:
Deutsch

Inhalt:
- Informationssysteme und Anwendungssysteme der Kritischen Infrastrukturen
- Krankenhausinformationssysteme / Laborinformationssysteme etc.
- Netzleittechnik und SCADA Systeme
- Prozessleittechnik, Überwachungs- und Monitoringsysteme

Verwendete Literatur:
B3S
BSI-ICS-Security-Kompendium

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 20202, MCSMT 20202

Modulbezeichnung:
Informationssysteme und Anwendungssysteme der Verwaltung, Behörden und KMU

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Wahlpflicht

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- Informationssysteme und Anwendungssysteme der Verwaltung, Behörden und KMU zu verstehen,
- externe Service Providern (insbesondere Security Operation Center) zu organisieren.
- Informationssysteme nach einschlägigen Qualitäts- und Sicherheitsmerkmalen (QS + IT-Sicherheit) unter Verwendung des PDCA-Zyklus und KVP einzuführen und zu auditieren.
- als second and third line of defense Sicherheitsprozesse und Projekte zu konzipieren, die zur langfristigen Erhöhung der Resilienz der IT-Systeme führen.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Inhalte des Moduls:
In diesem Modul werden die Informationssysteme und Anwendungssysteme der Verwaltung, Behörden und KMU anhand von Qualitäts- und Sicherheitsmerkmalen thematisiert. Hierzu werden beispielhaft Systeme und mögliche Sicherheitsprozesse zur Erhöhung der Resilienz betrachtet.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung

Lehrsprache:
Deutsch

Inhalt:
- Informationssysteme und Anwendungssysteme der Verwaltung, Behörden und KMU
- Betriebliche Anwendungssysteme
- Archivierungssysteme
- Systeme der öffentlichen Verwaltung

Verwendete Literatur:
Alpar, P., Alt, R., Bensberg, F., Grob, H.L., Weimann, P., Winter, R. (2016), Anwendungsorientierte Wirtschaftsinformatik - Strategische Planung, Entwicklung und Nutzung von Informationssystemen, 8. Aufl., Wiesbaden.
Mertens, P. (2013), Integrierte Informationsverarbeitung 1 - Operative Systeme in der Industrie, Wiesbaden.

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 20301, MCSMT 20301

Modulbezeichnung:
Weiterführende Aspekte der Computerkriminalität: Thematik 1

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Wahlpflicht

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- weiterführende Aspekte der Computerkriminalität in unterschiedlichen Kontexten wie bspw. Internetdelikte zu verstehen und diese in ihrer Allgemeinheit mit den Angriffsvektoren, Angriffsarten und Angriffsmotiven zusammenbringen, um daraus entsprechende Kenntnisse im Bereich der präventiven und reaktiven Informationssicherheit zu konzipieren.

Inhalte des Moduls:
Aufbauend auf den bereits gelegten Grundlagen im Bereich Cyberkriminalität werden spezifische Unterthemen im Detail beleuchtet. So werden u. a. die Verbreitung von illegalen Inhalten, politische motivierte Internetdelikte sowie Urheberrechtsdelikte als mögliche Ausprägungsformen hervorgehoben.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Verbreitung pornographischer Schriften (Kinderpornographie) über das Internet
- Verbreitung von Gewaltdarstellungen im Internet
- Onlinemarktplätze (Drogenhandel, Waffenhandel, Menschenhandel)
- Urheberrechtsdelikte Cybercrime im Staatsschutz
- Internetdelikte PMK Rechts
- Internetdelikte PMK Links
- Internetdelikte PMK Islamismus

Verwendete Literatur:
- Strafgesetzbuch
- EU-Cybercrime Richtlinie

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 20302, MCSMT 20302

Modulbezeichnung:
Weiterführende Aspekte der Computerkriminalität: Thematik 2

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Wahlpflicht

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.
Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- weiterführende Aspekte der Computerkriminalität in unterschiedlichen Kontexten wie bspw. Internetdelikte zu verstehen und diese in ihrer Allgemeinheit mit den Angriffsvektoren, Angriffsarten und Angriffsmotiven zusammenbringen, um daraus entsprechende Kenntnisse im Bereich der präventiven und reaktiven Informationssicherheit zu konzipieren.

Inhalte des Moduls:
Aufbauend auf den bereits gelegten Grundlagen im Bereich Cyberkriminalität werden spezifische Unterthemen im Detail beleuchtet. Schwerpunkt dieses Moduls stellt die IuK-Kriminalität dar, insbesondere im Kontext der organisierten Kriminalität.

Stand: 19.06.2020

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Einsatz von IuK in der Organisierten Kriminalität
- Geldwäsche im Internet
- Bedeutung von IuK für grenzüberschreitende Kriminalität
- Fälschungen
- IuK im Strafverfahren
- IuK als falsche Beweise

Verwendete Literatur:
- Strafgesetzbuch
- EU-Cybercrime Richtlinie
- Kochheim, D. (2018), Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik: Cybercrime und IuK-Strafrecht, München.

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 20401, MCSMT 20401

Modulbezeichnung:
Vernetze Computertechnologie und Connectivity

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Stockmanns

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Wahlpflicht

Art der Prüfung:
Klausurarbeit

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- neue Technologien im Bereich der IoT und vernetzten Computertechnologie sowie der Connectivity zu verstehen und diese im Rahmen der sicherheitstechnischen Handlungsfelder der Cyber-physischen Systeme einzuordnen.
- aus der technischen Sicht die Systeme und deren Vernetzungstechnologien zu erkennen und diese mit den informationstechnischen Sicherheitskomponenten zusammen zu bringen.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Inhalte des Moduls:
In diesem Modul werden ausgewählte vernetzte Computertechnologien, inkl. Protokolle, vorgestellt. Es erfolgt die Vermittlung der Grundlagen in den Bereichen Internet der Dinge, Aktorik und Sensorik, sowie RFID: Ausgehend von einzelnen Komponenten wird die vernetzte Kommunikation über das Internet demonstriert.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung

Lehrsprache:
Deutsch

Inhalt:
- Vermittlung von Kenntnissen über die differenzierten Technologien
- Vernetze Computertechnologie und Connectivity
- Einführung in das Internet der Dinge (IoT)
- Protokolle und Technologien
- Sensoren, Aktoren und deren Funktionsprinzip und Anschluss
- RFID-Systeme in Hard- und Software
- Mikrocontroller und TCP/IP Stack als Kommunikationsendpunkte
- Datenkommunikation über das Internet mit embedded Systemen und angeschlossenen
- Wireless Sensor Network Technologie-Funksensoren IEEE 802.15.4

Verwendete Literatur:
Tanenbaum, A.: Computernetzwerke, International Edition 2011.
Meyer, Martin: Kommunikationstechnik: Vieweg +Teubner Verlag GmbH, 2011.
John Catsoulis: Designing Embedded Hardware. O'Reilly, 2005.
Klaus Finkenzeller: RFID Handbuch.Hanser 2008.

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 20402, MCSMT 20402

Modulbezeichnung:
Blockchain

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Stockmanns

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Wahlpflicht

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
Das Modul wird in folgenden Studiengängen angeboten: Informatik Master Vollzeit, Dual, Teilzeit

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- neue Technologien im Bereich Blockchain und der virtuellen Währung zu verstehen und diese im Rahmen der sicherheitstechnischen Handlungsfelder einzuordnen.
- aus der technischen Sicht eine eigene Kryptowährung zu konzipieren und diese durch gezielte Cyber-Angriffe zu untersuchen.

Inhalte des Moduls:
Es werden die Grundlagen der digitalen Technologie Blockchain vermittelt sowie die Auswirkungen und mögliche Regulierungsbedarfe offengelegt. Im Allgemeinen werden die Anwendungsfälle von und der Umgang mit Kryptowährungen demonstriert und unter kryptografischen Aspekten eingeordnet.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung

Lehrsprache:
Deutsch

Inhalt:
- Grundlagen Blockchain-Technologie
- Grundlagen / Grundlagen Kryptografie und Kryptowährungen
- Dezentralisierung durch die Blockchain, Konsensfindung
- Erzeugen einer eigenen BTC-Adresse, Umgang mit Wallets, Erzeugen von
- Transaktionen, Verfolgen von Transaktionen im Netzwerk, Anonymität im Netzwerk,
- Alternative Mining Puzzles
- Aufsetzen eines eigenen Altcoin-Clients
- Umsetzung einer Miningsoftware für die Altcoin
- Durchführung von Angriffsszenarien innerhalb der Altcoin
- Gesellschaftliche Einordnung von Bitcoin / Regulierung / Geschichte/ Community

Verwendete Literatur:
Andreas M. Antonopoulos: Mastering Bitcoin. O"Reilly Media, 2013.
Melanie Swan: Blockchain: Blueprint for a New Economy. O'Reilly and Associates, 2015.

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 205, MCSMT 401

Modulbezeichnung:
Projektmanagement

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Stockmanns

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
Das Modul wird in folgenden Studiengängen angeboten: MWI, Vollzeit, Dual, Teilzeit

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- die Rolle des Projektleiters zu verstehen und zu bekleiden.

Freiwillig können die Teilnehmer auch das Basiszertifikat der Deutschen Gesellschaft für Projektmanagement (GPM) erwerben.

Inhalte des Moduls:
In diesem Modul werden Best Practices für die Projektführung vermittelt und die erworbenen Kenntnisse anhand von praxisnahen Fallstudien eingeübt und vertieft.

Stand: 19.06.2020

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Best Practices für die Projektführung
- praxisnahe Fallstudien

Verwendete Literatur:
Pflicht:
Wallmüller, E. Software-Qualitätssicherung in der Praxis, aktuelle Auflage
Balzert, H.: Lehrbuch der Softwaretechnik. Softwaremanagement, aktuelle Auflage
Romeike, F./Finke, R.: Erfolgsfaktor Risiko-Management. Chance für Industrie und Handel. Methoden, Beispiele, Checklisten, aktuelle Auflage

Ergänzend:
Abts, D./Mülder, W. (Hrsg.): Masterkurs Wirtschaftsinformatik. Kompakt, praxisnah, verständlich. 12 Lern- und Arbeitsmodule, aktuelle Auflage
Meyers, G. J.: The Art of Software Testing, aktuelle Auflage
Mellis, W./Herzwurm, G./Stelzer, D.: TQM der Softwareentwicklung, aktuelle Auflage
Jalote, P.: CMM in Practise. Processes for Executing Software Projects at Infosys, aktuelle Auflage
Königs, H.-P.: IT-Risiko-Management mit System. Von den Grundlagen bis zur Realisierung. Ein praxisorientierter Leitfaden, aktuelle Auflage
Lichtenberg, G.: Risiko-Management bei EDV- Projekten. Technische und vertragliche Aspekte, aktuelle Auflage
Dreger, W.: Erfolgreiches Risiko-Management bei Projekten, aktuelle Auflage

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 206, MCSMT 402

Modulbezeichnung:
Methoden der Unternehmens- und IT-Beratung

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Stockmanns

Studiengang:
MCSM, MCSMT

Semester:
2. Fachsemester

Angebotsturnus:
jedes Sommersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
Das Modul wird in folgenden Studiengängen angeboten: MWI Vollzeit, Dual, Teilzeit

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- die Besonderheiten der Unternehmens- und IT-Beratung als professionelle, extern oder intern zu erbringender Dienstleistung zu benennen.
- die Beratungsfähigkeiten sowohl auf der Ebene sozialer Kompetenzen als auch auf der Ebene konzeptioneller Problemlösungsansätze, wodurch sie in Zusammenarbeit mit Geschäftspartnern Probleme erkennen und definieren, zu strukturieren sowie kreative Lösungen zu entwickeln.
- Interviews zu führen.
- Instrumente des Konfliktmanagements anzuwenden.

- Kenntnisse des Beratungsmarkts zu benutzen und darauf basierend Aufbau und Kernprozesse von Beratungsorganisationen zu analysieren und zu bewerten.

Inhalte des Moduls:
Das Modul behandelt Methoden und Instrumente für zentrale Themen im Beratungsgeschäft. Die Spanne reicht von der Strategie und Top-Management-Beratung bis hin zur Unterstützung im Umfeld operativer Kostensenkungsprogramme. Es werden allgemeine Problemlösungskonzepte vorgestellt und diskutiert. Darüber hinaus werden Akquisitionsprozesse von Beratungsmandaten behandelt. Notwendige generelle persönliche Eigenschaften und Fähigkeiten für eine erfolgreiche Beratung werden ebenso thematisiert wie ethische Herausforderungen. Fallbeispiele werden zur Unterstützung der Praxisnähe und zum Zweck des Praxistransfers herangezogen. Das Geschäft der Unternehmensberatung wird auch aus der Perspektive des Auftraggebers transparent gemacht, wodurch einerseits die Tätigkeit des Beraters effektiv unterstützt, andererseits auch nichtproduktive Begleiterscheinungen erkannt und eingeordnet werden können.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Methoden und Instrumente für zentrale Themen im Beratungsgeschäft
- Strategie und Top-Management-Beratung
- operative Kostensenkungsprogramme
- Problemlösungskonzepte
- Akquisitionsprozesse von Beratungsmandaten
- persönliche Eigenschaften und Fähigkeiten für eine erfolgreiche Beratung
- ethische Herausforderungen
- Geschäft der Unternehmensberatung aus der Perspektive des Auftraggebers
- Einsatz von IT-Beratern
- Strategieorientierte Methoden
- Wettbewerbs- und innovationsorientierte Methoden
- Prozess- und effizienzorientierte Ansätze
- Informationsorientierte Ansätze
- Ausgewählte Methoden des Business Process Reengineering - Akquisition und Durchführung von Beratungsmandaten
- Fallbeispiele

Verwendete Literatur:
Pflicht:
Scheer, A.-W./Köppen, A. (Hrsg.): Consulting. Wissen für die Strategie-, Prozess- und IT-Beratung, aktuelle Auflage
Niedereichholz, C./Niedereichholz, J.: Consulting Wissen. Modulares Trainingskonzept für Berater mit Fallstudienhinweisen, aktuelle Auflage
Kerth, K./Asum, H./Stich, V.: Die besten Strategietools in der Praxis. Welche Werkzeuge brauche ich wann? Wie wende ich sie an? Wo liegen die Grenzen?, aktuelle Auflage

Ergänzend:
Simon, H./von der Gathen, A.: Das grosse Handbuch der Strategieinstrumente. Alle Werkzeuge für

eine erfolgreiche Unternehmensführung, aktuelle Auflage
Simon, H. (Hrsg.): Das grosse Handbuch der Strategiekonzepte. Ideen, die die Businesswelt verändert haben, aktuelle Auflage

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 301, MCSMT 301

Modulbezeichnung:
Security Information and Event Management (SIEM)

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Meuser

Studiengang:
MCSM, MCSMT

Semester:
3. Fachsemester

Angebotsturnus:
jedes Wintersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- die Fähigkeit von Produkten, die Daten von Netzwerk- und Sicherheitskomponenten zu sammeln, zu analysieren und zu präsentieren.
- den Umgang mit Sicherheitslücken zu verstehen und diese langfristig zu beseitigen.
- Logdateien von Betriebssystemen, Datenbanken und Anwendungen zu analysieren.
- externe Gefahren zu erkennen.
- Echtzeit-Warnungen zu konzipieren und Systeme in Echtzeit zu überwachen.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Inhalte des Moduls:
Mit Unterstützung eines Security Information and Event Management (SIEM) wird ein ganzheitlicher Blick auf die IT-Sicherheit ermöglicht. Dazu sind Meldungen und Logfiles verschiedener Systeme zu sammeln und auszuwerten. Verdächtige Ereignisse oder gefährliche Trends müssen sich in Echtzeit erkennen lassen. Auswahl, Implementierung und Betrieb dieser software-basierten Managementplattform werden vorgestellt..

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Konzeption vonSecurity Information and Event Management (SIEM)
- Security Information Management (SIM) und Security Event Management (SEM)
- Echtzeitanalyse von Sicherheitsalarmen
- Speicherung, Normalisierung, Strukturierung und Auswertung der Daten
- Regeln, Korrelations-Modelle, maschinelles Lernen und Künstliche Intelligenz, um Beziehungen zwischen den Meldungen herzustellen und Auffälligkeiten zu identifizieren
- Einhaltung gesetzlicher Vorgaben oder Richtlinien und Compliance-Regularien der IT-Sicherheit
- nachträglicher Nachweis von Sicherheitsereignissen
- SIEM Tools

Verwendete Literatur:
David R. Miller, Shon Harris, Allen Harper; Security Information and Event Management (SIEM) Implementation; McGrow-Hill, 2010.
Security Information and Event Management Systems Monitoring Auto; Juho Frigård; Universität Tampere, 2019

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 302, MCSMT 302

Modulbezeichnung:
Weiterführende Aspekte der IT-Frameworks

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
3. Fachsemester

Angebotsturnus:
jedes Wintersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- eine Implementierung von Informations-Sicherheits-Management-Systemen- und Frameworks gemäß ISO/IEC 27001, IT-Sicherheitsgesetz, COBIT, NIST, ITIL zu leiten.
- externe Service Provider (insbesondere Security Operation Center) zu managen.

Inhalte des Moduls:
Basierend auf den bereits gelegten Grundlagen zu den verbreiteten IT-Rahmenwerke erfolgt in diesem Modul eine Detailbetrachtung, welche zudem Zusammenhänge bzw. Überschneidungen hervorhebt. Insbesondere die Information Technology Infrastructure Library (ITIL) und die Control Objectives for Information and Related Technology (COBIT) werden anhand ihrer Anwendungsfälle thematisiert.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung

Lehrsprache:
Deutsch

Inhalt:
- Wissensvertiefung im Bereich der allgemeinen und fachspezifischen IT-Frameworks
- ITIL
- COBIT
- KPI
- Kennzahlentwicklung zur Quantifizierung der IT-Sicherheitsprozesse

Verwendete Literatur:
Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle. 7. Auflage, OldenbourgVerlag, 2012.
ITIL V2 und V3
COBIT
ISO/IEC 27000 / 27001 / 27002 / 27005

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Modulnummer:
MCSM 303, MCSMT 303

Modulbezeichnung:
IT-Netzwerk & Cloud Forensik

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Meuser

Studiengang:
MCSM, MCSMT

Semester:
3. Fachsemester

Angebotsturnus:
jedes Wintersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Klausurarbeit

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- die sicherheitstechnischen Konzepte aus den Bereichen der Netzwerkforensik, Mobilfunkforensik, elektronische Forensik adäquat umzusetzen.
- forensische Analysen in den jeweiligen dedizierten Bereichen aufzusetzen und diese fachgerecht durchzuführen.
- mit Hilfe der Methoden zur digitalen Forensik Gefahrenabwehrpläne sowie konkrete Vorgehensmodelle und Handlungsanweisungen für die Untersuchung von Cloud-Storage-Lösungen, Verschlüsselung von Cloud-Daten zu entwickeln und Handlungsmaßnahmen, Rückschlüsse auf Angriffsvektoren zu konzipieren.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 19.06.2020

Inhalte des Moduls:
Besonderheiten des forensischen Untersuchungsprozesses in Cloudumgebungen, technische und rechtliche Aspekte, konkrete Vorgehensmodelle und Handlungsanweisungen für die Untersuchung von Cloud-Storage-Lösungen.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung / Seminaristische Lehrveranstaltung

Lehrsprache:
Deutsch

Inhalt:
- Cloud Computing Stack, Cloud Security and Privacy, Internet-fähige Endgeräte, Smartphones und Cloud Computing,
- Besonderheiten des forensischen Untersuchungsprozesses in Cloudumgebungen, technische und rechtliche Aspekte,
- Konkrete Vorgehensmodelle und Handlungsanweisungen für die Untersuchungvon Cloud-Storage-Lösungen, Verschlüsselung von Cloud-Daten,
- Forenische Analyse aktueller Cloud-Anwendungen (Dropbox, Micosoft Azure, Cloudflare, Amazon Cloud, Front, Amazone S3, Google Drive etc.)
- IT-Sicherheit und Forensikzur Mobilfunkforensik:
- Mobile Betriebssysteme: insbesondere Android, iOS, WindowsPhone
- Architektur von Mobilfunkendgeräten: insbesondere Speichertechnologien, Forensische Tools

Verwendete Literatur:
Raymond Choo, Darren Quick, Ben Martini : Cloud Storage Forensics. 1. Edition. Elsevier LTD, Oxford (2014).
Keyun Ruan: Cybercrime and Cloud Forensics Applications for Investigation Processes (2013).

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 21.09.2020

Modulnummer:
MCSM 304, MCSMT 304

Modulbezeichnung:
Integrierte Managementsysteme

Modulumfang:
4 SWS

Credits:
5 CP

Gewichtung der Note in der Gesamtnote:
(5 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
3. Fachsemester

Angebotsturnus:
jedes Wintersemester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.
Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Nach erfolgreichem Absolvieren des Moduls sind die Absolvent*innen in der Lage…

- Aspekte der übergeordneten Managementsystem-Prinzipien mit dem Schwerpunkt auf „High Level Structure“ zu verstehen.
- eine Synchronisierung (Harmonisierung) sowie Orchestrierung der differenzierten Managementsysteme zu konzipieren.
- anderweitige Managementsysteme wie bspw. Technisches Sicherheitsmanagement (TSM), QMS, UMS und etc. zu verstehen.
- die bestehenden Managementsysteme und die zukünftigen Managementsysteme in den Institutionen unter den Aspekten und Prinzipien der IS und IT-Sicherheit einheitlich zu implementieren und diese fortlaufend zu harmonisieren.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 21.09.2020

Inhalte des Moduls:
Es erfolgt die Vermittlung von weiterführenden Kenntnissen zu integrierten Managementsystemen und kontinuierlichen Verbesserungsprozessen. Hierbei werden konzeptionelle Anforderungen an integrierte Managementsysteme abgeleitet und die unterstützende Funktion im Dienstleistungsbereich aufgezeigt.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 30 h Vorbereitung / 60 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Vorlesung

Lehrsprache:
Deutsch

Inhalt:
- Wissensvertiefung im Bereich der kontinuierlichen Verbesserungsprozesse
- KVP-Aspekte (Deming-Kreis)
- GRC – Ansatz
- Three Lines of Defense - Prinzip
- High Level Structure
- Technisches Sicherheitsmanag. / Umweltmanag. etc. (TSM, QSM, UMS, EMS, …)
- Managementsystem Harmonisierung und Orchestrierung

Verwendete Literatur:
Stefanie Schwendt, Dirk Funck: Integrierte Managementsysteme - Konzepte, Werkzeuge, Erfahrungen, Heidelberg (2002).

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 21.09.2020

Modulnummer:
MCSM 305, MCSMT 502

Modulbezeichnung:
Forschungsprojekt

Modulumfang:
4 SWS

Credits:
10 CP

Gewichtung der Note in der Gesamtnote:
(10 CP / 90 CP)*0,75

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
3. Fachsemester

Angebotsturnus:
jedes Semester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Hausarbeit und Präsentation

Voraussetzungen für die Teilnahme:
Keine

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Die Studierenden erwerben praktische soziale Kompetenzen und Projektkompetenzen durch die Möglichkeit, selbstständig ein Forschungsprojekt in einer Gruppe zu bearbeiten und einen gemeinsamen Bericht zu verfassen sowie Ergebnisse zu präsentieren. Im Rahmen dieses Moduls sollen die Studierenden Kenntnisse im Projektmanagement (z.B. Projekt- und Zeitplanung, Fortschrittskontrolle, etc.) durch direkte Anwendung erwerben und einüben.
Darüber hinaus sollen methodische und analytische Fähigkeiten sowie weitere Schlüsselkompetenzen wie z.B. Teamfähigkeit ausgebildet werden. Die erworbenen Fähigkeiten können in individueller Weise in der Master-Thesis angewandt und erweitert werden.
Ein Forschungs- bzw. Entwicklungsprojekt wird im Regelfall in Kooperation mit dem Forschungsinstitut CLAVIS und mehreren Unternehmen durchgeführt. Die Studierenden können aus einer Reihe von

Projektvorschlägen wählen. Pro Projektthema werden Teams von ca. 2-4 Studierenden gebildet, die von einem Professor betreut werden.
Zu Beginn werden Zielsetzung, Problemstellung, Vorgehensweise, Methoden, Tools und mögliche Projektergebnisse gemeinsam formuliert. Gemeinsam mit dem betreuenden Professor wird ein detaillierter Projektplan mit Meilensteinen und Zwischenergebnissen aufgestellt. Die Studierenden sollen in dem Forschungs- bzw. Entwicklungsprojekt in starkem Maße eigenständig die Arbeiten durchführen und sich auch intern abstimmen bzw. organisieren. Das Projekt findet nicht in Form einer „klassischen" Lehrveranstaltung statt. Vielmehr kann es in den Räumlichkeiten des kooperierenden Unternehmens oder in einem Labor der Hochschule durchgeführt werden. Die Rolle des Professors ist vordringlich die eines Beraters und Controllers. Die Forschungsergebnisse sind zu dokumentieren, vor den Sponsoren in den Unternehmen zu präsentieren sowie abschließend in geeigneten Foren (z.B. wissenschaftliche Tagungen, Fachzeitschriften, Messen) auch einer breiten Öffentlichkeit vorzustellen.

Inhalte des Moduls:
Bearbeitung eines Forschungsprojektes in einer Gruppe unter Anwendung von Projektmanagement-kompetenzen und wissenschaftlichen Methoden innerhalb eines vorgegebenen Zeitraums.

Gesamtworkload und seine Zusammensetzung
60 h Präsenzzeit / 60 h Vorbereitung / 180 h Nachbereitung und Prüfungsvorbereitung

---

Dozent:
N.N.

Art der Lehrveranstaltung:
Projektseminar

Lehrsprache:
Deutsch

Inhalt:
- Analyse der wissenschaftlichen Problemstellung
- Auswahl und Begründung der wissenschaftlichen Methoden
- Durchführung des Projekts
- Dokumentation und Abschlusspräsentation

Verwendete Literatur:
Die Literatur ist abhängig von dem konkreten Thema des jeweiligen Forschungsprojekts.

Besonderes:
./.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 21.09.2020

Modulnummer:
MCSM 401, MCSMT 601

Modulbezeichnung:
Masterarbeit und Kolloquium

Modulumfang:
900 Stunden

Credits:
30 CP

Gewichtung der Note in der Gesamtnote:
Masterarbeit 20 % der Gesamtnote; Kolloquium 5 % der Gesamtnote

Modulverantwortlicher:
Prof. Dr. Treibert

Studiengang:
MCSM, MCSMT

Semester:
4. Fachsemester

Angebotsturnus:
jedes Semester

Dauer des Moduls:
1 Semester

Art des Moduls:
Pflichtmodul

Art der Prüfung:
Masterarbeit und mündliche Prüfungsleistung (Kolloquium)

Voraussetzungen für die Teilnahme:
80 CP

Verwendbarkeit des Moduls innerhalb desselben Studiengangs:
./.

Verwendbarkeit des Moduls für andere Studiengänge:
./.

Zu erwerbende Kompetenzen:
Die Studierenden sollen die erlernten Fachkenntnisse und wissenschaftliche Methoden im Rahmen einer konkreten anwendungsorientierten Themenstellung selbstständig anwenden und umsetzen. Ferner soll die Selbstkompetenz durch die Beurteilung der eigenen Arbeitsergebnisse und durch eigenverantwortliches Handeln auf Grundlage einer selbständigen Projektorganisation gefördert werden. Die wissenschaftliche Aufarbeitung bzw. systematische Dokumentation und Präsentation eines komplexen Themas erfordert eine fachspezifische Methodenkompetenz. Im wissenschaftlichen Diskurs der Arbeitsergebnisse zeigt der Student seine Kritik- und Argumentationsfähigkeit.

Inhalte des Moduls:
Die Masterarbeit soll zeigen, dass der Prüfling befähigt ist, innerhalb einer vorgegebenen Frist eine praxisorientierte Aufgabenstellung aus einem Fachgebiet des Studiengangs sowohl in fachlichen Ein-

zelheiten als auch in fachübergreifenden Zusammenhängen nach wissenschaftlichen und anwendungsorientierten Methoden selbständig zu bearbeiten.
Das Kolloquium dient der Feststellung, ob der Prüfling befähigt ist, die Ergebnisse der Masterarbeit, ihre fachlichen Zusammenhänge und außerfachlichen Bezüge mündlich darzustellen, selbständig zu begründen und ihre Bedeutung für die Praxis einzuschätzen.

Gesamtworkload und seine Zusammensetzung
800 h Erstellung Masterarbeit / 100 h Vorbereitung Kolloquium

---

Modulteil a:
Masterarbeit

Dozent:
zwei Prüfer, i. d. R. Professoren am Fachbereich

Art der Lehrveranstaltung:
Masterarbeit

Lehrsprache:
Deutsch (mit Zustimmung des Prüfungsausschusses auch eine Fremdsprache)

Inhalt:
Selbständige Bearbeitung einer Aufgabenstellung aus der Forschung und/oder Praxis nach wissenschaftlichen Methoden innerhalb eines Zeitraums von höchstens vier Monaten.

Verwendete Literatur:
Die relevante Literatur ist abhängig von der konkreten Aufgabenstellung.

Besonderes:
./.

Modulteil b:
Kolloquium

Dozent:
zwei Prüfer, i. d. R. Professoren am Fachbereich

Art der Lehrveranstaltung:
Masterarbeit

Lehrsprache:
Deutsch (mit Zustimmung des Prüfungsausschusses auch eine Fremdsprache)

Inhalt:
Das Kolloquium ergänzt die Masterarbeit. Erörtert und begründet werden die Ergebnisse der Masterarbeit, ihre fachlichen Zusammenhänge und außerfachlichen Bezüge, die Bearbeitung des Themas und die Bedeutung der Ergebnisse für die Praxis. Im Verlauf des Studiums behandelte Inhalte können durch die Prüfer zur Feststellung ausreichender Fachkompetenz thematisiert werden.
In Absprache mit den Prüfern kann der Studierende als Ausgangsbasis eine Präsentation bezüglich der Vorgehensweise und der Kernaussagen der Masterarbeit erstellen.

Verwendete Literatur:
Die relevante Literatur ist abhängig von der konkreten Aufgabenstellung.

Modulbeschreibung

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Stand: 21.09.2020

Besonderes:
./.