IT-Consulting II (W3WI_SC306)

IT Consulting II

FORMALE ANGABEN ZUM MODUL

MODULNUMMER	VERORTUNG IM STUDIENVERLAUF	MODULDAUER (SEMESTER)	MODULVERANTWORTUNG	SPRACHE
W3WI_SC306	3. Studienjahr	2	Prof. Dr.-Ing. Clemens Martin	Deutsch/Englisch

EINGESETZTE LEHRFORMEN

Vorlesung, Seminar, Übung, Case Study

EINGESETZTE PRÜFUNGSFORMEN

PRÜFUNGSLEISTUNG	PRÜFUNGSUMFANG (IN MINUTEN)	BENOTUNG
Klausur oder Portfolio	120	ja

WORKLOAD UND ECTS-LEISTUNGSPUNKTE

WORKLOAD INSGESAMT (IN H)	DAVON PRÄSENZZEIT (IN H)	DAVON SELBSTSTUDIUM (IN H)	ECTS-LEISTUNGSPUNKTE
150	50	100	5

QUALIFIKATIONSZIELE UND KOMPETENZEN

FACHKOMPETENZ

Die Studierenden kennen die Grundlagen der Informationssicherheit und deren Konzepte zu diskutieren. Sie können diese vergleichend diskutieren und ihre Anwendbarkeit beurteilen. Sie kennen aktuelle Entwicklungen im IT-Consulting-Umfeld und diese grundlegend einschätzen.

METHODENKOMPETENZ

Die Studierenden können Methoden und Verfahren zur Datensicherheit und Datenschutz anwenden, einfache Sicherheitsrichtlinien konzipieren und diese implementieren. Sie können Methoden aus dem Bereich „Neue Aspekte“ in den Consulting Kontext einordnen und anwenden.

PERSONALE UND SOZIALE KOMPETENZ

Die Studierenden sind sich der Verantwortung im Umgang mit sensiblen Daten sowie den durch die IT-Sicherheit adressierten Risiken bewusst. Sie haben erkannt, inwiefern der kontinuierliche Wandel der Informationstechnologie Arbeitswelt und Gesellschaft verändert.

ÜBERGREIFENDE HANDLUNGSKOMPETENZ

Die Studierenden können die Aspekte der Informationssicherheit und aktuelle Entwicklungen in wirtschaftsinformatischen Fragestellungen berücksichtigen.

LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM
IT-Security	25	50

Einführung in Informationssicherheit: Common Criteria, BSI IT-Grundschutz, Auditing und Assessment, Bedrohungsszenarien, Risiken – Designprinzipien und Evaluierungskriterien im Designprozess – Evaluation und Vertrauen, Zusicherung von Eigenschaften der Informationsysteme – Systeme zur Sicherstellung von Datenintegrität, Authentifizierung und Autorisierung – Containment und Recovery.

Grundlagen der Kryptographie, symmetrische und asymmetrische Verschlüsselung, Public Key Verfahren, digitale Signaturen – Sicherheitssyteme (z. B. Firewalls, IDS/IPS, Virenscanner).

LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM
Neue Aspekte des IT-Consultings	25	50

IT Security, Privacy und Trust in neuen Aspekten des IT-Consultings.
Grundlegende Prinzipien der Datenanalyse: Sammeln, Bereinigen, Bearbeiten, Visualisieren und Auswerten von Daten unter Berücksichtigung des Datenschutzes und -sicherheit.

Besonderheiten wie soziale Graphen und deren Eigenschaften sowie Auswirkungen auf Geschäftsmodelle – Auswahl von essenziellen Tools und Algorithmen der Datenanalyse (auch im Fokus von BigData und IT-Sicherheit), wie bspw. MapReduce in verteilten Systemen.

Implementierung von beispielhaften Analyseszenarien auf Basis vorgegebener oder simulierter Daten (z. B. Risikobetrachtung, Sicherheitsvorfälle, etc.).

BESONDERHEITEN

Die Prüfungsdauer gilt nur für die Klausur.

VORAUSSETZUNGEN

-

LITERATUR

- Bishop, M.: Computer Security, Boston: Art and Science
- BSI: IT-Grundschutz-Standards. http://www.bsi.bund.de
- BSI: Leitfaden Informationssicherheit. http://www.bsi.bund.de
- Ferguson, N.; Schneier, B.: Practical Cryptography. Indianapolis: Wiley
- Pfleeger, C. P.; Pfleeger, S. L.: Security in Computing. Upper Saddle River (N.J.).