IT-Compliance, Prozesse und Architekturen

Allgemeine Angaben

Kürzel	ITCO
Modulverantwortliche	Prof. Dr. E. Koch, Prof. Dr. Schumann
Dozenten	Prof. Dr. Koch, Prof. Dr. Schumann, Prof. Dr. Stehr
Lehrsprache	Deutsch
Semester	6
ECTS	5
Kontaktstunden	40
Selbststudium	85
Dauer	1 Semester
Art	Pflicht in der Spezialisierung „Cyber Security“
Häufigkeit	Jedes Studienjahr
Gewichtung	5/180
Prüfungsleistung	K**R**S90

Stichwörter

- IT Compliance
- IT-Governance
- BSI, ISACA, ISF, NIST
- Datenschutzgesetze, EU Datenschutzgrundverordnung
- Telekommunikationsgesetz, Telemediengesetz etc.
- Signaturgesetz, DE-Mail-Gesetz
- MA-Risk, BAIT
- IT Grundschutz (BSI)
- ISO 27001
- ISO 9001
- IEC 61508
- Prüf- und Zertifizierungsstandards
- Sicherheits-Architekturen
- Identity und Access Management
- Patch Management
- Security information and event Management (SIEM)
- Security Operations Center (SOC)
- Business Continuity Management

Zugangsvoraussetzungen

- Technical Security
- Securing Digital Transformation

Verwendbarkeit

- Konsekutive Master-Studiengänge

Qualifikations- und Kompetenzziele

Rechtkonforme IT Systeme sind ein immer wichtiger werdender Faktor für Unternehmen. Das Modul IT Compliance, Prozesse und Architekturen vermittelt Kenntnisse über wichtige Gesetzesvorgaben, Regulierungswerke und Standards.

Studierende erlernen die Grundbegriffe und Regelwerke der IT Compliance. Diese steht in engen Zusammenhang mit der IT-Governance und bildet einen wichtigen Aspekt der IT Sicherheit. Darüber hinaus wird ein übergreifendes Verständnis im Bereich IT-Sicherheitsmanagement geschaffen, welches die relevanten Managementprozesse, deren Organisation und die Kenntnisse über die erforderlichen Architekturen und Systeme vermittelt.

Lehr- und Lernmethoden

Klassischer Vortrag, Durchführung von Übungen mit Präsentation der Ergebnisse, Fallstudienarbeit, praktische Übungen

Inhalte

- Begriffe und Grundlagen
    - Compliance und Governance
    - IT Compliance
    - IT-Governance
- Gesetze, Regelwerke und Organisationen
    - Organisationen (BSI, ISACA, ISF, NIST, …)
    - Datenschutzgesetze, EU Datenschutzgrundverordnung, etc.
    - Telekommunikationsgesetz, Telemediengesetz, etc.
    - Signaturgesetz, DE-Mail-Gesetz
    - MA-Risk, BAIT, etc.
- Standards und Frameworks
    - IT Grundschutz (BSI)
    - ISO 27001
    - ISO 9001
    - IEC 61508
    - Prüf- und Zertifizierungsstandards
- Sicherheitsmanagement
    - Sicherheits-Architekturen
    - Identity und Access Management
    - Patch Management
    - Security information and event Management (SIEM)
    - Security Operations Center (SOC)
    - Business Continuity Management

Grundlegende Literatur

ECKERT, Claudia: *IT-Sicherheit: Konzepte - Verfahren – Protokolle*, De Gruyter Oldenbourg; 9. Auflage, 2014

HARICH, Thomas: *IT-Sicherheit im Unternehmen*, mitp Verlag, 2015

Ergänzende Literatur

BARTSCH, Michael: *Cyberstrategien für Unternehmen und Behörden: Maßnahmen zur Erhöhung der Cyberresilienz*, Springer, 2017