**Gültig ab** 2027.FS

# Modulbeschreibung: Advanced IT Security Management

| | |
|---|---|
| **Modulkürzel** | w.MA.XX.AISM.26HS |
| **ECTS Credits** | 3 |
| **Unterrichts- und Prüfungssprache** | Deutsch |
| **Beschreibung des Moduls** | Wie wird aus einer Sicherheitsanforderung eine überprüfbare Kontrolle und eine überzeugende Managemententscheidung? In diesem Modul verbinden Sie technische Analyse mit der Steuerung von Cyberrisiken. An einem durchgängigen Fall aus der Finanzbranche, der Diagnostik oder einem Cloud-Softwareunternehmen entwickeln Sie ein Sicherheitsprogramm: Sie prüfen Zugriffsrechte, analysieren verdächtige Logs, beurteilen Backups und priorisieren Verbesserungen unter einem begrenzten Budget. In einer Cybervorfall-Simulation treffen Sie Entscheidungen unter Unsicherheit und passen diese an neue Informationen an. So üben Sie, technische Befunde in umsetzbare Empfehlungen für Fach- und Führungskräfte zu übersetzen. |
| **Verantwortliche OE** | Institut für Wirtschaftsinformatik |
| **Modulverantwortung** | Christian Weber |
| **Studiengang und Vertiefungsrichtung** | Wirtschaftsinformatik |
| **Rechtliche Grundlagen** | Studienordnung für den Masterstudiengang Wirtschaftsinformatik vom 22.08.2019, Anhang zur Studienordnung für den Masterstudiengang Wirtschaftsinformatik erstmals beschlossen am 10.07.2012 |
| **Modulkategorie** | **Modultyp**<br>Wahlpflichtmodul |
| **Spezifische Vorkenntnisse** | Das Modul nutzt Inhalte von IT Security Management. Erwartet werden Grundlagen zu ISMS, Risikoanalyse, Netzwerken und Zugriffssteuerung. Einstiegsdiagnose und gezielte Selbstlernaufträge aktivieren das Vorwissen. Umfangreiche Programmier- oder Systemadministrationskenntnisse werden nicht vorausgesetzt. |
| **Beitrag des Moduls für Learning Objectives des Studiengangs (durch das Modul betroffene)** | • Fachkompetenz<br>• Methodenkompetenz<br>• Sozialkompetenz<br>• Selbstkompetenz |
| **Beitrag des Moduls für Learning Objectives des Studiengangs** | **Fachkompetenz**<br>• Theorie- & Praxisrelevante Fachinhalte wissen & verstehen<br>• Theorie- & Praxisrelevante Fachinhalte anwenden, analysieren und verknüpfen<br>• Theorie- & Praxisrelevante Fachinhalte evaluieren<br>**Methodenkompetenz**<br>• Problemlösung & Kritisches Denken<br>• Wissenschaftliche Methoden<br>• Arbeitsmethoden, -techniken & -verfahren<br>• Nutzung von Informationen<br>• Kreativität & Innovation<br>**Sozialkompetenz**<br>• Schriftliche Kommunikation<br>• Mündliche Kommunikation<br>• Kooperation im Team & Umgang mit Konflikten<br>• Interkulturalität & Perspektivenübernahme<br>**Selbstkompetenz**<br>• Selbstmanagement & Selbstreflexion<br>• Ethische & Soziale Verantwortung<br>• Lernen & Veränderung |
| **Lernziele des Moduls** | Die Studierenden...<br>• können Geschäftsprozesse, IT-Architektur und Dienstabhängigkeiten analysieren und daraus Schutzbedarf, Datenflüsse und Vertrauensgrenzen ableiten. |

# Modulbeschreibung: Advanced IT Security Management

| | |
|---|---|
| | • können Sicherheitskontrollen anhand von Risiken, Betriebsanforderungen und Kosten vergleichen und ihre Auswahl mit Bezug auf ISMS und etablierte Rahmenwerke begründen.<br>• können die Wirksamkeit ausgewählter Kontrollen mit reproduzierbaren Prüfungen untersuchen und Ergebnisse sowie Nachweisgrenzen kritisch beurteilen.<br>• können Cyberrisiken unter Unsicherheit bewerten und Massnahmen anhand von Wirkung, Ressourcen und wirtschaftlichen Annahmen priorisieren.<br>• können Detektion, Incident Response und Wiederherstellung koordinieren und Entscheidungen bei veränderter Lage nachvollziehbar revidieren.<br>• können ein konsistentes Sicherheitsprogramm mit Verantwortlichkeiten, Roadmap und Restrisiken adressatengerecht vertreten und eigene Fachbeiträge auf neue Situationen übertragen. |
| **Inhalte des Moduls** | **W01–W03: Sicherheitskontext, Bedrohungsszenarien und Evidenzqualität; ISMS-Ausschnitt und Zielprofil mit NIST CSF 2.0 und ISO/IEC 27001**<br><br>**W04–W06: Netzwerksegmentierung, sichere Betriebszugänge, Identity and Access Management sowie Cloud- und Lieferantensicherheit**<br><br>**W07–W10: Schwachstellenmanagement und Hardening, Monitoring und Detection, Incident Response, Business Continuity und vertrauenswürdige Wiederherstellung**<br><br>**W11–W12: Investitionsentscheidungen und Roadmap; nutzbare Sicherheitsprozesse, Verhalten und organisationsbezogene Rechts- und Meldepflichten im Schweizer Kontext**<br><br>**W13–W14: Kontrollreview, Management Summary und Abschluss des Sicherheitsprogramms; Entscheidungssimulation und Transfer** |
| **Verknüpfung zu anderen Modulen** | **Verknüpftes Modul**<br>w.MA.XX.ITIS.26HS / IT Infrastructure Security<br><br>**Vorausgesetztes Modul**<br>w.MA.XX.ITSM.26HS / IT Security Management |
| **Digitale Lernressourcen** | • Reader<br>• Lehrvideos<br>• Übungs- und Anwendungsaufgaben (inkl. Lösungen)<br>• Fallstudien (inkl. Lösungen) |
| **Unterrichtsmethoden** | • Lehrgespräch<br>• Forschendes Lernen<br>• Projektarbeit<br>• Literaturstudium<br>• Übungen<br>• Fallstudien<br>• Fachinputs, Diskussionen und angeleitete Fallarbeit wechseln sich ab.<br>• In festen Teams entwickeln Sie ein Security-Portfolio und erhalten Rückmeldungen auf Zwischenstände.<br>• Fünf technische Übungen vertiefen Segmentierung, Berechtigungen, Hardening, Detection und Restore anhand synthetischer Daten.<br>• Sie beurteilen Befunde und deren Grenzen. Rollenwechsel und Peer-Review verbinden Technik, Governance und Betrieb.<br><br>**Eingesetzte Sozialformen**<br>• Gruppenarbeit<br>• Einzelarbeit |

# Modulbeschreibung: Advanced IT Security Management

**Unterrichtsgliederung**

| | Kontaktstudium | Begleitetes Studium | Autonomes Selbststudium |
|---|---|---|---|
| Vorlesung | 14 h | - | |
| Übung | 14 h | - | |
| Projektarbeit | - | 14 h | |
| Seminar | - | - | |
| **Total 90** | **28 h** | **14 h** | **48 h** |

**Leistungsnachweise**

| Modulendprüfung | Form | Dauer (Min.) | Gewichtung |
|---|---|---|---|
| - | | | |
| **Hilfsmittel** | | | |

| Andere | Bewertung | Format | Dauer (Min.) | Gewichtung |
|---|---|---|---|---|
| Security-Portfolio *Gruppenleistung: Architektur, Risiko und Kontrollen, fünf Prüfnachweise, Response und Recovery, Roadmap mit Management Summary. Richtumfang 18–22 Seiten.* | Note | Gruppenarbeit | 0 | 50.00% |
| Entscheidungsbeitrag zur Simulation (wird näher definiert in SW01) *Individuell: persönliches Log aus der 70-minütigen Simulation in SW14 und anschliessendes Memo von höchstens zwei Seiten.* | Note | Einzelarbeit | 0 | 30.00% |
| Fachverteidigung *Individuell, mündlich und separat terminiert: technischer Befund, Entscheidungsbegründung und Transfer. Dauer 6 Minuten.* | Note | Einzelarbeit | 0 | 20.00% |

**Präsenzverpflichtung**

80%

Aufgrund des Vorlesungssettings als "inter"aktive Workshop Veranstaltung ist eine hohe Anwesenheitsquote erforderlich Typische Lehr- und Lernformen sind: Fachinputs, Diskussionen und angeleitete Fallarbeit wechseln sich ab. In festen Teams entwickeln Sie ein Security-Portfolio und erhalten Rückmeldungen auf Zwischenstände. Fünf technische Übungen vertiefen Segmentierung, Berechtigungen, Hardening, Detection und Restore anhand synthetischer Daten. Sie beurteilen Befunde und deren Grenzen. Rollenwechsel und Peer-Review verbinden Technik, Governance und Betrieb.

**Pflichtliteratur**

- Wird zu Semesterbeginn bekanntgegeben

**Ergänzende Literatur**

- Wird bei Bedarf bekanntgegeben

**Bemerkungen**

Eine Nachbesserung bzw. Nachbearbeitung von Leistungsnachweisen ist nicht möglich.