# CAS Cybersecurity und Information Risk Management (CISSP/BSI/ISO)

Zertifizierte Kompetenz, um Angriffe abzuwehren und Werte zu schützen

**Safety first! Cyberangriffe, Informationssicherheit und Risikomanagement sind Topthemen für das Management. Der Schutz von digitalen Werten (Informationen, Unternehmens- und Personendaten) ist heute geschäftskritisch. Daher sind Cybersecurity-Strategien, Security Awareness-Kampagnen und ein umfassendes Information Security Management notwendiges Rüstzeug für Führungskräfte im IT-Umfeld, u.a. IT-Leitende, RevisorInnen, RechtsanwältInnen.**

In diesem Lehrgang erhalten Sie eine komplette Vorlage für ein Security Framework. Das systematische Vorgehen, die rechtlichen Rahmenbedingungen und die praktische Umsetzung werden strukturiert und ganzheitlich aufgezeigt. Kurz: Das Programm befähigt Sie, Cybersecurity ganzheitlich zu managen. Die erworbenen Kenntnisse werden an einem Beispielunternehmen umgesetzt.

Darüber hinaus erlangen Sie das Zertifikat IT-Sicherheitsbeauftragter BSI (zweistufige Prüfung) und sind vorbereitet auf die Zertifizierung zum CISSP.

**Ziele**

Die Absolventinnen und Absolventen des Zertifikatslehrgangs:
- beurteilen die rechtliche Verantwortung der Informationssicherheit
- kennen relevante Sicherheitsfaktoren im Zeitalter von Cybersecurity
- gestalten den Aufbau eines professionellen Information Risk Managements
- beurteilen die verschiedenen Stufen des Schutzbedarfs
- kennen Arten der Sicherheitsorganisation und der Sicherheitsarchitektur
- planen Awareness-Kampagnen gegen Cyber-Attacken
- kennen die Anforderungen bezüglich Datenschutz (DSGVO)

| | |
|---|---|
| **Inhalt** | - BSI Information Security Framework, inklusive Audit-Methodik<br>- Cybercrime: Bedrohungen und Gefahren, Sicherheitsrichtlinien und Standards<br>- Physische Sicherheit und Business-Continuity-Strategien<br>- Risiko-Analysen nach CISSP, Werksspionage, Social-Engineering<br>- Mobile Kommunikation, VoIP und CISSP, WLAN/Telefon/Blutooth Security<br>- Vorbereitung auf die internationale CISSP Zertifizierungsprüfung<br>- Security Models, System Security Architecture, Identity & Access Control<br>- Applikationssicherheit: Geschäftsprozesse, Websicherheit, Webarchitektur<br>- Infrastruktur: Perimeter Security, TCP/IP-Protokoll Architektur<br>- Kryptologie: Kryptoanalyse, Steganographie, Anwendungen<br>- Krisenbewältigung, Desaster-Recovery-Konzepte<br>- Security Awareness: Schulungskonzepte, Kampagnen, Kultur<br>- Vertragsrecht im IT-Umfeld, Datenschutz und DSGVO<br>- Ausbildung zum IT-Sicherheitsbeauftragten nach BSI<br>- Systematik nach ISO/IEC 27001 und ISO/IEC 19011 (ISO/IEC Foundation Prüfung) |
| **Besonderheiten** | Der Leistungsnachweis für das FHNW-Zertifikat ist gleichzeitig die Prüfung zum IT-Sicherheitsbeauftragten BSI. Darüber hinaus wird die ISO 27001 Foundation Prüfung angeboten und auf die CISSP-Prüfung vorbereitet. |
| **Zielpublikum** | - IT-Fachkräfte, IT-Leitende<br>- IT-Sicherheitsbeauftragte und Datenschutzbeauftragte<br>- Revisoren, Controller, Rechtsanwälte Schwerpunkt IT<br>- IT-Unternehmensberater, IT-Verkaufsberater Schwerpunkt Security |
| **Abschluss** | Certificate of Advanced Studies FHNW Cybersecurity und Information Risk Management, 15 ECTS-Punkte<br>Dieser CAS ist ein Wahlfach im MAS Information Systems Management und Teil des DAS Digital Leadership in IT. |
| **Daten** | Startdaten : 4. April und 13. Oktober 2022 |
| **Ort** | Online und Campus Brugg-Windisch |
| **Kosten** | (inkl. Unterlagen und die BSI-Prüfung, exkl. CISSP-Prüfung) 7'500 CHF |
| **Programmleitung** | Prof. Martina Dalla Vecchia T +41 61 279 17 62<br>martina.dallavecchia@fhnw.ch |
| **Koordination** | Dominique Ongaro T +41 61 279 18 65<br>dominique.ongaro@fhnw.ch |