Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

AACSB ACCREDITED

Storyboard

Certificate of Advanced Studies
Cybersecurity und Information Risk Management
IT-Sicherheitsbeauftragter BSI. ISO 27001 Foundation. NIST. CISSP Vorbereitung.

Prof. Martina Dalla Vecchia

Editorial

Cybersecurity gehört zu den grossen Herausforderungen in der Geschäftswelt. Es braucht die Zusammenarbeit vom Management, Business, HRM und der IT, um den aktiven Schutz von Daten, Unternehmenswerte und Menschen zu ermöglichen und Krisen zu bewältigen.

2004 fand dieser Lehrgang «NDK Informationssicherheit» zum ersten Mal statt. Damals lag der Fokus auf der **Vorbereitung zum CISSP** und dem Management der Informationssicherheit.

Im Laufe der Jahre haben sich die Inhalte den aktuellen Anforderungen und Security-Standards angepasst. So konnten wir – in Zusammenarbeit mit dem Deutschen Bundesministerium - die Zertifizierung zum **IT-Sicherheitsverantwortlichen nach BSI** integrieren.

Seit 2021 ist zusätzlich die Zertifizierungsprüfung **ISO/IEC 27001 Foundation** (ISFS) Bestandteil des Lehrgangs und ab 2022 haben wir auch das **NIST Cyber Security Framework** integriert.

Es ist eine intensive Ausbildungszeit, mit vielen anspruchsvollen Themen, welche laufend aktualisiert werden. Gemeinsam mit unserem eingespielten und praxiserfahrenen Dozententeam ist es eine spannende Lern-Reise.

Ich freue mich Sie, bei unserem Zertifikatslehrgang
«CAS Cybersecurity und Information Risk Management» persönlich kennenzulernen!

Ihre
Martina Dalla Vecchia
Programmleiterin

Modul 1: Big Picture zu BSI, ISO, NIST, CISSP, ISMS

1. Tag

Kick-off: Zertifikatslehrgang CSIRM
Martina Dalla Vecchia

- Begrüssung und Warm-up
- Leitfaden zum Lehrgang
- Leistungsnachweis und Zertifikate
- Organisatorisches

BSI Framework & Audit-Methodik
Dozent: Andreas Wisler

BSI – Einführung und Übersicht

- Informationssicherheitsmanagement
  Standards und Normen
  BSI 200-x, IT-Grundschutz-Kompendium
- Informationssicherheitsorganisation
  Leitlinie zur Informationssicherheit
- Massnahmen zur Informationssicherheit
- Sicherheitskonzept

2. Tag

ISO 27001 – Einführung und Übersicht
Dozent: Andreas Wisler

ISO 27001 Deep Dive

- Übersicht über die ISO-Normen
- Wichtige Begriffe gemäss ISO 27000
- Anforderungen an ein Management-System
- Ziele der Informationssicherheit
- Zusammenhang Risiken, Massnahmen, Kontrollen
- Definition des Anwendungsbereichs
- Vorgehen Internes Audit
- Inhalt des Management Reviews
- KVP-Prozess
- Übersicht über die Controls
- Ablauf Zertifizierungsaudit
- Schritte und Anforderungen eines Audits
- Überblick über weitere ISO-Normen

CISSP Prüfung

- Grundlagen, Vorgehen, Anmeldung
- Strategien, Aktuelle Informationen ISC2
- Erfahrungsberichte

3. Tag

NIST CSF – Einführung, Übersicht & Projekt
Dozent: Rainer Kessler

Kritische Infrastruktur

- Definition im engeren und im weiteren Sinn
- Sicherheit, Schutz und Abhängigkeit

National Institute of Standards and Technology

- Genereller Auftrag des NIST
- Engagement für die Cybersicherheit

NIST CSF

- Entwicklung und globale Verbreitung, inkl. IKT-Minimalstandard und FINMA
- Übersicht der Elemente (IPDRR, Core, Tiers, etc.)
- NIST CSF für KMU (Small Business Cyber-security)
- Nutzung des NIST CSF (mit Praxisbeispielen)

Projektarbeit

- Unternehmung und Aufgabenstellung
- Anforderungen an die Lösung, inkl. Zeitplan und Rahmenbedingungen
- Templates, Gruppenarbeit und Kick-off

Rot markierte Titel sind CISSP relevant

Modul 2: Identity / Access Management, Security Models, Risiko- und Security-Governance

4. Tag

IAM Identity & Access Management
Dozent: Andreas Wisler

CISSP Schwerpunkttag

- Access Control Principles
  - Classification, Categories, Types
- Identifcation
- Authentification
  - Weak, Strong, Single-Sign-On (SSO)
- Authorisation
  - Kerberos, Radius, 802.1x, NAC/NAP
  - NTLM, SESAME, TACACS. SSO, OTP
- Models
  - Security Models
- System Evaluationsmethoden
  - TCSEC & ITSEC
  - Common Criteria, ISO 15408

Workshop «Access Management»

5. Tag

Security Models
Dozent: Andreas Wisler

CISSP Schwerpunkttag

- System Security Architecture
  - Motherboard
  - CPU, ALU, RAM
  - Prozesse, Threads
  - Schnittstellen, BIOS/UEFI
  - Kernel & Reference Monitor
- Cloud Security
  - Dienstmodelle, Architekturen
  - Sicherheitsrisiken nach Gartner, CSA, ENISA
  - Kriterienkatalog C5 des BSI

Workshop «Cloud Security»

6. Tag

Risiko- und Security-Governance
Dozent: Rainer Kessler

Mechanismen, Prozesse und Kontext

- Risk Assessment gem. CISSP
- Risikomanagement in verschiedenen Umfeldern
- Umgang mit Risiken
- Information Security Management System

Risikomanagement: Anwendung und Beispiele

- Spezifische Bedrohungslage: Cyber-Threat
- Data-Loss, Data-Leakage, Data-Breach, etc.
- Cyber-Verteidigungsdispositiv CH/Global
- Informations- und Technologierisiken

Struktur: Institutionalisierung der «Security»

- Three-Lines-of-Defense und Sicherheits-zusammenarbeit in der Organisation
- Struktur Informations-, IT- und Cybersicherheit
- Aufbau und Betrieb einer Sicherheitsfunktion
- Sicherheit als Teil des Asset-Managements
- Das betriebliche «Informationsuniversum»

Modul 3: IT-Forensik, Infrastruktur- und Perimetersicherheit, Eskalation und Business Continuity Mgt.

7. Tag

IT-Forensik
Dozent: Andreas Wisler

IT-Forensik
- Inhalt
- Einsatzgebiete

Forensische Datensicherung
- Schritte
- Datenquellen
- Desktop, Laptop, RAM, Online

Datenanalyse
- Ort und Form
- Dateianalyse
- Datenbanken

8. Tag

Infrastruktur
Dozent: Andreas Wisler

CISSP Schwerpunkttag

- Grundlagen
  - Schichtenmodel
  - UKV, Kabel, Glasfaser

- TCP/IP-Protokoll Architektur
  - IPv4, IPv6
  - TCP/UDP
  - Protokolle: DHCP, DNS, FTP, HTTP, SMTP, POP3, IMAP4, SNMP

- Perimeter Security
  - Zonenkonzept (DMZ)
  - Firewalls & Proxies
  - Intrusion Detection / Prevention
  - Datenbanken

9. Tag

Eskalation und Business Continuity Management
Dozent: Rainer Kessler

Business Continuity Management
- Incidents, Problems, Taskforces, Crisis
- BCM-Komponenten gem. ISO 22301 (ITSCM & BPCM) sowie Disaster Response Strategien
- Cold, Warm, Hot Recovery, etc.
- BCM-Test, Education, Controlling / Maintenance

Normen und Standardisierung
- Standards und Best Practices
- Gesetze, Verordnungen, Regulationen und Compliance versus Assurance versus Security

Weitere Spezialgebiete
- FDPS (Fraud Detection & Prevention)
- IT Forensics & Investigation, etc.

Workshop «Notfallplan»

Zwischen Modul 3 und 4 erhalten alle Teilnehmenden einen Voucher für die Online-Prüfung.
Die Kosten für die Prüfung (Wert 250 CHF) sind im Kursgeld enthalten.

Sollte man die Prüfung wiederholen müssen/wollen, werden die Kosten in Rechnung gestellt.

Modul 4: Kryptologie, Hacking / Angriffsmethoden, Cybersecurity und Emerging Technology

10. Tag

Kryptologie
Dozent: Andreas Wisler

CISSP Schwerpunkttag

Kryptographie
- Bedrohungen
- Begriffe
- Geschichte
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Digitale Signatur, Hash-Verfahren

Kryptoanalyse

Steganographie

Anwendungen
- SSL
- PKI
- Secure Messaging
- Secure Remote Access

Workshop «Kryptographie»

11. Tag

Hacking Day / Angriffsmethoden
Dozent: Raphael Rietmann

CISSP Schwerpunkttag

Angriffsmethoden
- Bedrohungen
  - Methoden & Strategien
  - Hacker & Cracker
  - Angriffsszenarien
  - Windows Security
- Web-Sicherheit
  - Web-Angriffe (SQL-Injection…), OWASP
  - Schutz von Webservern
- Schwachstellen
  - Werkzeuge, Assessment, Manual Hacking
  - Kali

Workshop «Angriffe»

12. Tag

Cybersecurity & Emerging Technology
Fokus A.I.
Dozent: Rainer Kessler

Emerging Technology (EmTech)
- Stand der Technik in verschiedenen Bereichen und zu verschiedenen Zeitpunkten (Industrie 1.0 - 4.0)
- Digitale «Game Changer» und Blick in die Zukunft: Podularisierung, A.I. und QIS)

Vertrauen in Emerging Technology
- Strategische und taktische vertrauensbildende Massnahmen in neue Technologien
- Cybersicherheit im Kontext neuer Technologien
- Standards und Gesetze für neue Technologien

Emerging-Technology-Ethik
- Neue Ethikgebiete und deren Nutzen/Nutzung (Digital Ethics, Data Ethics, Algorithm Ethics, Machine Learning Ethics, Artificial Intelligence Ethics, Robot Ethics, Machine Ethics, etc.)
- Wichtigkeit der eigenen Meinung und Einflussnahme

Modul 5: Recht, DSGVO, Outsourcing, Mobile Kommunikation, Security Awareness Kampagnen

13. Tag

Recht und Informationssicherheit
Dozent: Lukas Fässler, RA

Recht, DSG/DSGVO und Sicherheit

- Sicherheit, Risiko und Recht
- Code of Ethics
- Strafrecht
- Ermittlungen / Investigation
- Grundlagen des Datenschutzrechts CH & EU
- Haftungsausschluss
- Durchsetzbarkeit von Sicherheitsrichtlinien
- Besondere Schutzklauseln für Verträge mit Providern und Beratern
- Möglichkeiten und Grenzen von Datenüberwachung
- Grenzen von Outsourcing
- Werksspionage, Social-Engineering

Workshop «Recht /Policy»

14. Tag

Mobile Kommunikation und physische Sicherheit
Dozent: Andreas Wisler

WLAN Security

- Grundlagen, Angriffspunkte
- Konzepte

VoIP Security

- Grundlagen, Angriffspunkte
- Konzepte, Multiplex-Verfahren
- Satellitenkommunikation, GSM, UTMS, LTE

Bluetooth

- Technik, Möglichkeiten

Physische Sicherheit

- Zonenkonzept
- Verbindung physische und logische Sicherheit
- Spezielle Überwachungssysteme (Video, etc.)

15. Tag

Security Awareness
Dozent: Rainer Kessler

Security Awareness

- Grundlagen zur Wahrnehmung von Sicherheitsaspekten
- Unternehmenskultur als „Awareness-Trigger“
- Psychologische Ansätze und Hintergründe – Warum Mitarbeitende Risiken eingehen
- Schulungskonzepte für Mitarbeiter, Kunden, Partner / Lieferanten
- Best Cases – Beispiele von Awareness Kampagnen von Unternehmen und Verwaltungen
- Explorative Massnahmen und Kommunikationsbeschleuniger

Workshop «Security Awareness»

Die Kosten (Wert 160 CHF) für die Prüfung sind im Kursgeld enthalten.

Modul 6: Pitch Cybersecurity und Information Risk Mgt. Framework (ISMS, Strategy, Tasks, Roadmap)

16. Tag

Abschlusspräsentationen MoneyMaker
Martin Dalla Vecchia (CEO)
Rainer Kessler (COO)
Andreas Wisler (CIO)
Martina Dalla Vecchia (CMO)

1. **Präsentationen des Projekts Security Frameworks**
   GL der MoneyMaker
   - ISMS Ist-Zustand
   - Information Security Strategie
   - Prioritäten, Risiken/Vorgehen
   - Kosten/Nutzen, Zeitplan
2. **Präsentationen des Security Frameworks nach BSI vor der IT-Abteilung der MoneyMaker**
   - Summary GL-Präsentation
   - Information Security Strategie, Scope, Gesetze, Funktionen/Rollen
   - Roadmap
   - Technische Massnahmen
   - Kommunikation/Awareness
3. Feedback zu den Präsentationen und Frameworks

Abschluss-Apéro

Tagesablauf (Grobstruktur):

08.45 Uhr	Start Unterrichtsblock I
12.15 Uhr	Mittagspause
13.30 Uhr	Unterrichtsblock II
16.30 Uhr	Feedback und Round up
16.45 Uhr	Abschluss

Die Räumlichkeiten stehen am Abend für freies Arbeiten (Projektgruppen) bis 20 Uhr zur Verfügung.

Projekt «MoneyMaker»

MoneyMaker ist der Titel der begleitenden Praxisarbeit der Teilnehmenden. Die Teilnehmenden werden in Gruppen über die gesamten 14 Tage ein Praxisprojekt ausarbeiten. Hierbei geht es darum ein Security-Framework (Policy, Risk Management, IT-Security) zu erarbeiten. Am Abschlusstag werden die Gruppen vor der Geschäftsleitung ihre Ergebnisse präsentieren. Ziel ist es, die GL (mit IT-Wissen) für das Projekt zu begeistern und eine Freigabe des Investitionsantrages zu erreichen!
Diese Praxisarbeit ist gleichzeitig der praktische Prüfungsteil zur BSI-Zertifizierung

Präsentation am Abschlusstag (2 Präsentationen)

15 Minuten Präsentation mit PPT vor GL
20 Minuten Präsentation mit PPT vor Fachgruppe
(Hinweis: Die Präsentationen sind Teil der BSI-Prüfung)

CAS-Abschluss:

15 ECTS Punkte
Plus Note für Security Framework & Präsentation

ISO 27001:

Die ISO-Prüfung ist im Kursgeld enthalten.

BSI:

Prüfung besteht aus zwei Teilen:
Teil A) Computergestützte Prüfung (MC)
Teil B) MoneyMaker-Präsentation (PPT)
und Security Framework (Word)
Info: Die BSI-Prüfung ist im Kursgeld enthalten.

CISSP:

Vorbereitung auf die Prüfung CISSP:
CISSP-Übungsbuch und Testprüfungen sind im Kursgeld enthalten. Die CISSP-Prüfung selbst ist im Kursgeld **nicht** enthalten (Stand 6.12.2021 = 665 €)
Aktuelle Gebührenordnung siehe www.ISC2.org

Leistungsnachweis:

80 % Anwesenheit im Unterricht
Teilnahme an der BSI und ISO-Prüfung
Erfolgreiche Abschlussarbeit „MoneyMaker“

«MoneyMaker»

Security Framework, Management Summary
und Antrag an GL (PDF)
Abgabe siehe Stundenplan
Präsentationen (PDF)
Abgabe am Abschlusstag

Dozententeam:

Lukas Fässler | FSDZ Rechtsanwälte & Notariat AG

Rainer Kessler | SWISS-TECH-ACADEMY

Andreas Wisler | goSecurity AG

Raphael Rietmann | goSecurity AG

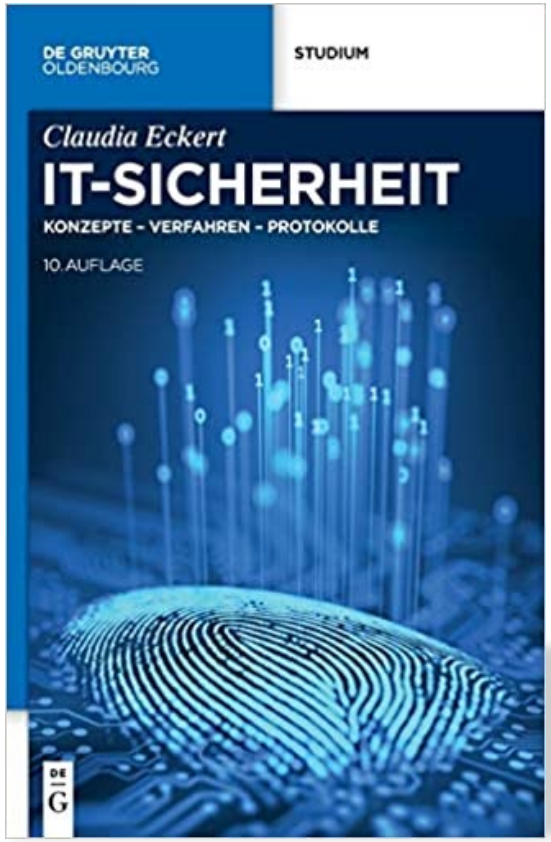
Prof. Martina Dalla Vecchia | FHNW

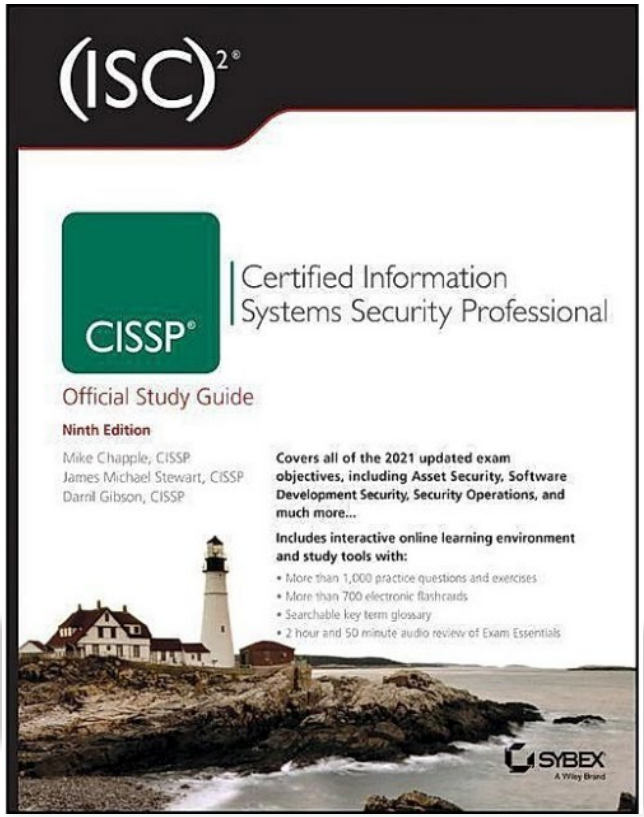
Kontaktdaten für Abwesenheiten oder Fragen:

Dominique Ongaro
061 279 18 65
dominique.ongaro@fhnw.ch

Prof. Martina DallaVecchia
061 279 17 62
martina.dallavecchia@fhnw.ch

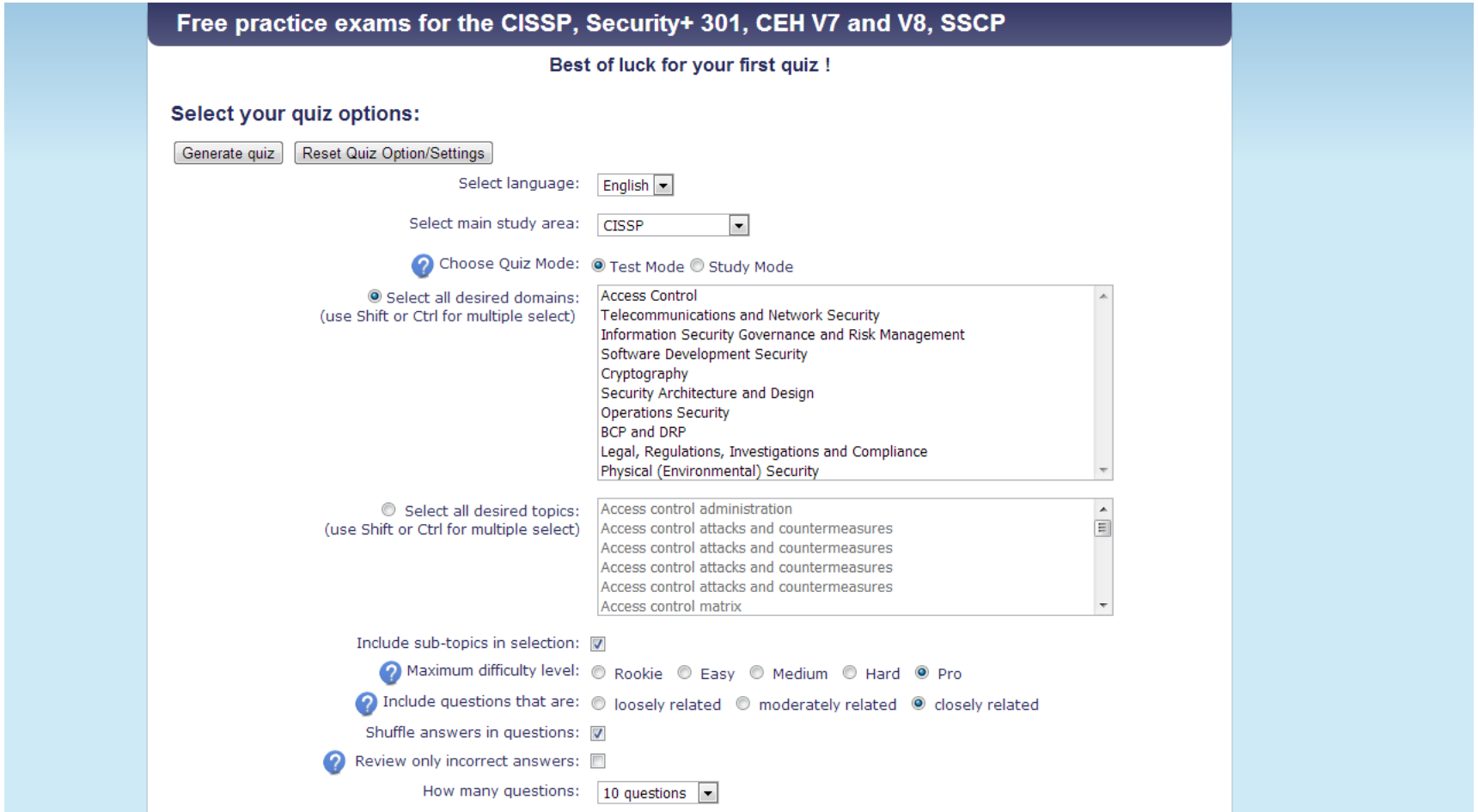
Bücher zum CAS Cybersecurity und Information Risk Management





Diese Bücher erhalten Sie digital vor dem Start als PDF und als Link.

Zur Vorbereitung auf die CISSP-Prüfung erhalten Sie Zugang zur Online-Plattform mit Testfragen



Dozententeam

Andreas Wisler
Sicherheitsarchitektur, Sicherheitstechnologie und Prüfungstechnik

goSecurity AG
www.gosecurity.ch
Linkedin

Raphael Rietmann
Pentesting, Hacking

goSecurity AG
www.gosecurity.ch

Rainer Kessler
Sicherheitsstrategie und Sicherheitsmanagement

SWISS-TECH-ACADEMY
Linkedin

Lukas Fässler
RA, Recht im Security-Umfeld

FSDZ Rechtsanwälte & Notariat AG
www.fsdz.ch
Linkedin

Impression aus dem CAS:

Unsere Absolventinnen und Absolventen sind engagiert und kreativ!

Im Bild die Security Awareness die Kampagne für die MoneyMaker AG

Ich freue mich, wenn Sie beim nächsten **CAS Cybersecurity und Information Risk Management** dabei sind!

Ihre
Martina Dalla Vecchia

Fragen? Just mail to martina.dallavecchia@fhnw.ch