Certificate of Advanced Studies

IT Security Management

Die globale Vernetzung erlaubt uns, jederzeit und überall miteinander verbunden zu sein. Die dauernde Verfügbarkeit stellt jedoch höchste Ansprüche an den Umgang und die Sicherheit der Privatsphäre, Zugangskontrolle und des Datenschutzes.

Im CAS IT Security Management erwerben Sie die Fachkompetenzen, um in einer integralen Sicherheitsorganisation aktiv mitzuarbeiten. Sie lernen, IT-Security-Prozesse zu definieren, um diese in den laufenden IT-Security-Tätigkeiten zu nutzen.

Berner
Fachhochschule

Inhaltsverzeichnis

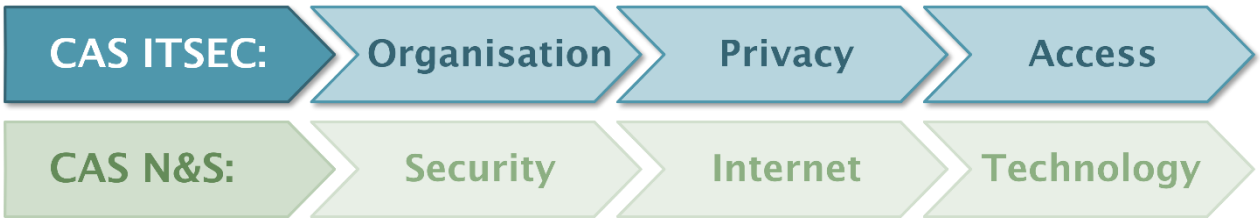
Stand: 05. Februar 2024

1 Umfeld

Die Vernetzung verschiedenster IT-Systeme ermöglicht den Abgleich und die Verknüpfung von zuvor isolierten Daten für viele neue Anwendungen in Logistik, Marketing, Monitoring und Steuerung von Systemen in Medizin, Energieversorgung, Infrastruktur und anderem. Diese Anwendungen bergen aber auch neue Gefahren, insbesondere jene des unberechtigten Zugriffs auf Firmendaten oder bösartige Eingriffe. Das CAS vermittelt Ihnen Methoden, wie Risiken in der Informationssicherheit eines Unternehmens erkannt, analysiert, bewertet und gesenkt werden können, so dass die Datensicherheit nachhaltig gewährleistet ist.

Das CAS IT Security Management (ITSEC) ist Teil des MAS Cyber Security. Zusammen mit den CAS N&S (Networking & Security) bildet es einen wesentlichen Teil der Cyber-Security-Weiterbildung und ergibt eine ideale Voraussetzung für den erfolgreichen Abschluss in MAS Cyber Security.

Die ideale Kombination für eine erfolgreiche Weiterbildung in Cyber Security



2 Zielpublikum

- Sie sind für die Planung, den Auf- und Ausbau von Netzwerken oder Serverplattformen im Intranet und Internet sowie für den Unterhalt und Betrieb aller dazu notwendigen Kommunikationskomponenten verantwortlich.
- Sie arbeiten innerhalb eines Security-Teams und sind für Compliance, Governance sowie für die integrale IT-Sicherheit Ihrer Organisation verantwortlich.
- Sie sind Software-Architekt*in oder Applikationsentwickler*in und wollen sich fundiert in die Datensicherheit einarbeiten.

3 Ausbildungsziele

- Sie sind mit den Aufgaben des Security-Managements und der Betreuung der Security-Technologie vertraut und können diese umfassend wahrnehmen.
- Sie kennen Strategien, Compliance und Risikomanagement in der IT-Security.
- Sie verstehen die Grundlagen der Kryptographie sowie darauf aufbauende Sicherheits- und Kommunikationsprotokolle; Sie können diese analysieren, bewerten und effizient einsetzen.
- Sie kennen Verfahren und Technologien zum Schutz der Privacy und die Grundzüge der schweizerischen Gesetzgebung zur Erfassung, Haltung, Bearbeitung und Archivierung von personenbezogenen Daten.

4 Voraussetzungen

- Ausbildung in Informatik / Wirtschaftsinformatik oder entsprechende Berufserfahrung
- Gute Kenntnisse von IP-Netzwerken und Internettechnologien
- Motivation für die Vertiefung der Lehrinhalte in Labs und Praktika

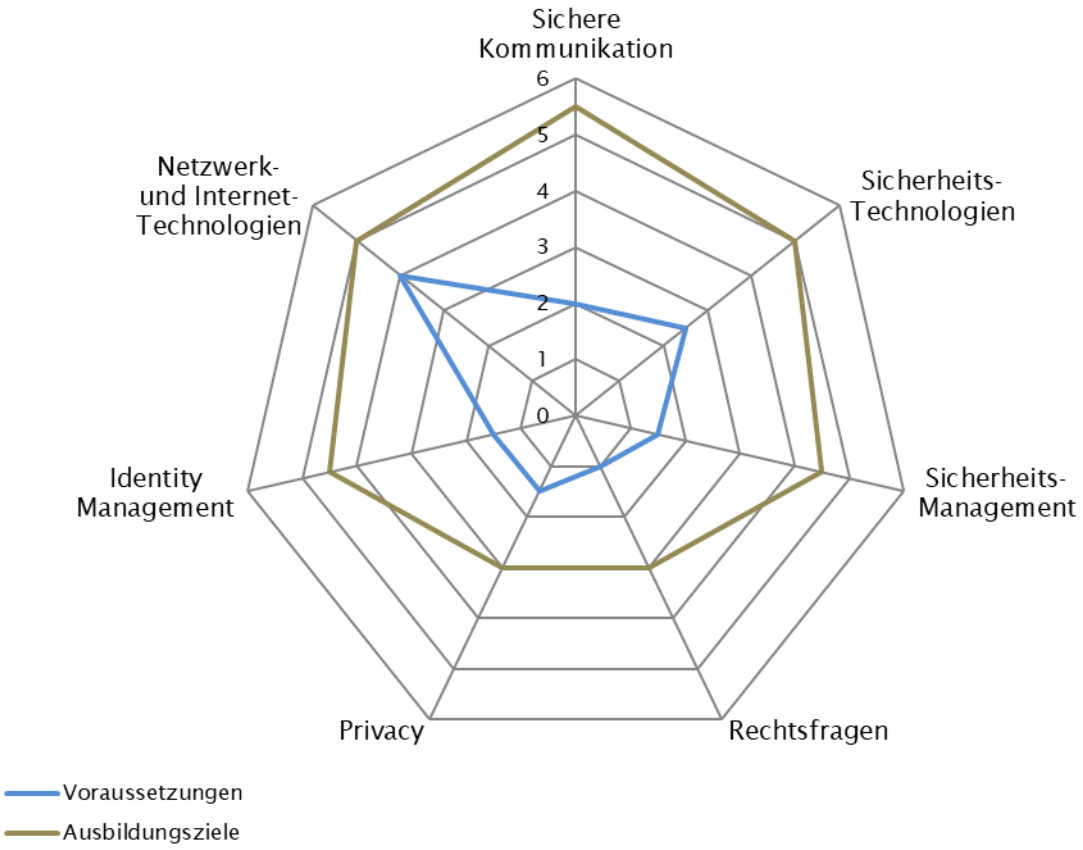
5 Unterrichtssprache

Die Unterrichtssprache ist Deutsch, die Unterlagen sind teilweise in Englisch.

6 Durchführungsort

Berner Fachhochschule, Weiterbildung, Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne), 2503 Biel,
Telefon +41 31 848 31 11, E-Mail weiterbildung.ti@bfh.ch.

7 Kompetenzprofil



Kompetenzstufen

1. Kenntnisse/Wissen
2. Verstehen
3. Anwenden
4. Analyse
5. Synthese
6. Beurteilung

8 Kursübersicht

Kurs / Lehreinheit	Lektionen	Stunden	Dozierende
Information Security Technologies	58		Pascal Mainini
Information Security Management	40		Anton Brunner, Hans-Peter Käser
Identity und Access Management	24		Dominik Kuhn
Rechtsfragen	18		Muriel Künzi
Organisation und Meilensteine der Semesterarbeit	12		Anton Brunner
Semesterarbeit		90	Dozierende des MAS Cyber Security
Total	152	90	

Das CAS umfasst insgesamt 12 ECTS-Credits. Für die einzelnen Kurse ist entsprechend Zeit für Selbststudium, Prüfungsvorbereitung, etc. einzurechnen.

9 Kursbeschreibungen

Nachfolgend sind die einzelnen Kurse dieses Studienganges beschrieben.

Der Begriff Kurs schliesst alle Veranstaltungstypen ein, es ist ein zusammenfassender Begriff für verschiedene Veranstaltungstypen wie Vorlesung, Lehrveranstaltung, Fallstudie, Living Case, Semesterarbeiten usw.

9.1 Information Security Technologies

Der Kurs bietet eine Einführung in die Kryptographie, welche als Basis für Sicherheitsmechanismen in heute verwendeten Konzepten und Anwendungen dient. Er besteht aus zwei Hauptteilen: einer Einführung in grundlegende kryptographische Verfahren sowie die Betrachtung typischer kryptographischer Protokolle und darauf aufbauender Anwendungen.

Lernziele	Die Teilnehmenden – lernen die Grundlagen der Kryptographie und deren Anwendungen kennen. – können Sicherheitsaspekte und Einsatzgebiete kryptographischer Verfahren allgemein beurteilen. – erhalten grundlegende Kenntnisse über PKI und Zertifikate. – haben detaillierte Kenntnisse einiger heute am häufigsten angewendeten Sicherheitsprotokolle und können deren Einbettung in typische Anwendungen und Umgebungen verstehen, selbstständig analysieren, bewerten und deren Einsatz planen. – kennen die gängigsten Authentisierungsverfahren/-technologien und können diese bezüglich Missbrauchspotenzial und Sicherheit einordnen. – kennen heutige Verfahren, Anforderungen und Lösungen für die Erzeugung von elektronischen Signaturen.
Themen und Inhalte	Die folgende Zusammenstellung umfasst einige Teile der behandelten Themen: – Einführung und Übersicht der Kryptographie – Symmetrische und asymmetrische Verschlüsselung – Schlüsselaustauschverfahren – Datenauthentizität und -integrität: Hashfunktionen, Authenticated Encryption – Public-Key-Infrastrukturen und Zertifikate – Elektronische Signaturen und Identitäten – End-to-End-Verschlüsselung: Transport Layer Security und andere, angewandte Protokolle – Authentisierung, 2FA + MFA Login – Zertifikatsklassen und gesetzliche Grundlagen – Post-Quantum Kryptographie
Lehrmittel und Lehrmethode	– Folien/Skript – Persönliche Übungen/Laborarbeiten – Literaturempfehlungen Nr. 1 und 2

9.2 Information Security Management

Eine gute Informationssicherheit berücksichtigt technische und organisatorische Aspekte sowie auch den Faktor Mensch. Das Information Security Management charakterisiert dabei die systematische Einführung, den risikogerechten Betrieb und die kontinuierliche Optimierung der Informationssicherheit. Mittels theoretischer Grundlagen und Praxisbeispielen werden im Kurs die Möglichkeiten und Massnahmen des Information Security Managements strukturiert und ganzheitlich vermittelt.

Lernziele	Die Teilnehmenden – beherrschen die Grundsätze der Informationssicherheit, – kennen Vorgaben, Inhalte sowie gebräuchliche Vorgehensweisen eines Information Security Managements Systems (ISMS), – können potenzielle Risiken eines Unternehmens im Umgang mit Informationen erkennen, analysieren und bewerten, – kennen personelle, organisatorische und technische Massnahmen zur Reduktion der Risiken – wissen, wie Mitarbeitende für die Informationssicherheit sensibilisiert werden können (Awareness) – und verfügen damit über das nötige Fachwissen, um in einer integralen Sicherheitsorganisation aktiv mitzuarbeiten.
Themen und Inhalte	– Einführung in die Informationssicherheit – Sicherheitseigenschaften, Grundsätze und Prinzipien – Gefahren, Schadenspotentiale und Schutzbedarf – Abgrenzung Information Security Management System (ISMS) – Compliance – Informationssicherheit und Governance – Rechtliche Grundlagen und internationale Richtlinien – Standards und Rahmenwerke – ISO/IEC 27000-Familie, IT-Grundschutz – NIST Cybersecurity Framework – Risikomanagement – Grundlagen und Methoden der Risikobewertung – Risikomanagement-Prozess, ISO/IEC 27005 – Strategien zur Risikobewältigung, Kosten-Nutzen-Verhältnis – Ebenen des Sicherheitsmanagements, Sicherheitsorganisation – Informationssicherheitspolitik und -konzept – Planung und Aufbau eines ISMS – Zertifizierungen nach ISO/IEC 27001 und IT-Grundschutz – Sicherheit in der Softwareentwicklung – Technische und organisatorische Lösungsansätze, betriebliche Aspekte – Dokumentation, Change- und Release-Management – Monitoring, Aufzeichnen und Auswerten von Logs – Erkennen, Behandeln und Eskalieren von Sicherheitsvorfällen – Notfall- und Krisenmanagement – Erhöhung der Sicherheit – Audits, Assessments – Awareness, Ausbildung
Lehrmittel	– Folien/Skript – Gruppenarbeiten

9.3 Identity und Access Management

Identity und Access Management ist in der digitalen Welt eine Querschnittfunktion, mit der wir täglich auf vielfältige Weise in Berührung kommen. Wenn wir uns im Internet bewegen, Geräte konfigurieren oder während der Arbeit Applikationen benutzen – jedes Mal geht es dabei auch um Identity und Access Management. Für unsere Sicherheit und die Sicherheit der eigenen und der uns anvertrauten Daten leisten Identity und Access Management einen wichtigen Beitrag.

Dieser Kurs vermittelt einen Überblick über das Thema. Einerseits werden die technischen Aspekte, wie z.B. die Architektur von Identity- und Access-Management-Systemen oder die zugrunde liegenden Standards behandelt. Andererseits kommt auch die organisatorische Seite, wie z.B. Prozesse im Firmenumfeld oder rechtliche Rahmenbedingungen zur Sprache. Ebenfalls wichtig sind hier die Unterschiede zwischen Identity und Access Management im Firmenumfeld und im Privatbereich.

Lernziele	Die Teilnehmenden – haben Kenntnisse, wie sich Identitäten und Autorisierungsinformationen zuverlässig und sicher erfassen und verwalten lassen – wissen, wie Identitäten zur Authentisierung in einem Authentisierungsprozess genutzt werden – kennen die Gefahren, die sich aus der Verknüpfung von persönlichen Informationen mit Identitäten ergeben – kennen die Prinzipien der attribut- bzw. rollenbasierten Berechtigungsverwaltung – kennen die Prozesse und organisatorischen Voraussetzungen für Identity und Access Management – lernen die aktuellen Standards kennen – sind in der Lage, die Vor- und Nachteile sowie die Risiken, die sich durch die Nutzung eines IAM-Systems ergeben, abzuschätzen – können die Sicherheit/Architektur von IAM-Systemen beurteilen – sind in der Lage, an der Architektur/Konzeption neuer IAM-Systeme mitzuarbeiten
Themen und Inhalte	– IAM-Grundlagen und generische IAM-Architektur – Digitale Identität (Verwaltung, Lifecycle Management, Sicherheitsanforderungen) – Speicherung von digitalen Identitäten (Directory Services, Datenbanken) – Provisionierung von digitalen Identitäten und Ressourcen – Berechtigungsmodelle (RBAC, ABAC) – Föderierung / Single Sign On (SAML und OpenID Connect) – Session Management und Umgang mit Logout – API-Autorisierung (OAuth 2.0) – Prozesse und Organisation – Rechtliche Rahmenbedingungen – Ausblick auf zukünftig wichtige Technologien, wie z.B. Privacy Enhanced Identity Management, UMA – Laborübung: Praktische Anwendung einiger Themen in einem CTF- (Capture the Flag) Spiel
Lehrmittel	– Folien/Skript – Literaturempfehlungen Nr. 3 und 4 – Verweise auf wichtige Dokumente und Standards im Skript

9.4 Rechtsfragen

Daten sind schnell erfasst und lassen sich heute ohne grossen Aufwand speichern und verknüpfen. Auch ist es dem IT-Personal jederzeit möglich, aus Logdateien und der für einen sicheren Betrieb notwendigen Netzwerküberwachungs-Software Rückschlüsse auf das Verhalten einzelner Personen zu ziehen. Dieser Kurs soll zeigen, was unter welchen Voraussetzungen vom Gesetzgeber erlaubt ist und wie mit den erfassten Daten umgegangen werden muss resp. darf.

Im IT-Bereich kommt man um Fragen der rechtlichen Qualifikation konkreter IT-Leistungen nicht herum. Auch stellen sich regelmässig Fragen im Zusammenhang mit geistigem Eigentum (insbesondere Urheberrechtsschutz von Software), resp. im Zusammenhang mit Lizenzen (Nutzungsrechten). In diesem Kurs sollen Grundzüge zu diesen Themen vermittelt werden.

Lernziele	Die Teilnehmenden – wissen, welche Daten unter welchen Voraussetzungen erfasst, bearbeitet und archiviert werden dürfen – kennen die zentralen Punkte der schweizerischen Gesetzgebung zur Bearbeitung von personenbezogenen Daten und die Grundzüge relevanter Vorgaben in der EU – wissen, welche gesetzlichen Anforderungen an eine digitale Signatur gestellt werden – kennen zentrale Punkte der gesetzlichen Vorschriften im Zusammenhang mit Verträgen im IT-Bereich – kennen die Grundzüge der gesetzlichen Vorschriften im Bereich des Urheberrechtsschutzes von Software (insb. im Zusammenhang mit Lizenzen)
Themen und Inhalte	– Datenschutz und massgebliche Erlasse – Aufgaben im Kontext Datenschutz – Digitale Signatur (ZertES) – Gesetzliche Grundlagen im Zusammenhang mit IT-Verträgen Gestaltungsmöglichkeiten und gängige Fallstricke – Gesetzliche Grundlagen im Zusammenhang mit Softwareschutz
Lehrmittel	Folien/Skript

9.5 Projektarbeit

Die Projektarbeiten sind Einzel- oder Gruppen-Arbeiten aus dem Arbeitsumfeld der Studierenden. Gruppenarbeiten sind – wo immer möglich – erwünscht und je nach Rahmenbedingungen meist von Vorteil. Der nominelle Aufwand liegt bei 90 Arbeitsstunden pro Gruppenmitglied, kann je nach Vorbereitungsphase und Komplexität der Aufgabenstellung aber auch leicht höher sein.

Falls aus Sicht der Auftraggebenden notwendig, können Semesterprojekte vertraulich behandelt werden. Massgebend für die Rahmenbedingungen ist das Studienreglement. Die Vertraulichkeit darf den didaktischen Rahmen nicht behindern: Präsentationen und Diskussionen über das gewählte Thema müssen im Rahmen der Klasse möglich sein.

Zielsetzung und Thema	In der Semesterarbeit befassen sich die Teilnehmenden idealerweise mit einem Security-Projekt (ev. Teilprojekt) oder einer Fragestellung aus ihrer Firma. Mit dem gewählten Thema vertiefen die Studierenden die im Studium erlernten Methoden und lernen diese in der Praxis anzuwenden. Sie nutzen geeignete Vorgehensweisen, um mit vertretbarem Aufwand die für ihren Betrieb notwendigen Security- und Privacy-Aspekte einzuführen und durchzusetzen.
Ablauf	Die Semesterarbeit beinhaltet die folgenden Meilensteine (siehe auch Zeitplan): 1. In der Firma ein Thema suchen und finden sowie eine*n Ansprechpartner*in/Betreuer*in in der Firma definieren. 2. Erstellen einer Projektskizze (Wordvorlage vorhanden) und Eingabe (hochladen) an die Schule. 3. Die Projektskizze umfasst eine ein- bis maximal zweiseitige Aufgabenstellung mit folgenden Elementen: 1. Titel 2. Umfeld 3. Problemstellung 4. Lösungsansatz (Vorgehen, Methoden) 5. Angestrebte Ergebnisse und Ziele 6. Name und Kontaktadressen aller Gruppenmitglieder, und der Ansprechpartner*in/Betreuer*in der Firma 4. Individuelle Kurzpräsentation (10'–15') und Diskussion (10') des Themas an der Schule vor einem Expert*innen- und Dozierenden-Gremium. 5. Eventuell Ergänzung oder Überarbeitung der Projektskizze gemäss Feedback an der Präsentation. 6. Zuordnung von Expert*innen durch die Schule für die Begleitung der Semesterarbeit. 7. Durchführung der Arbeit in eigener Terminplanung. 8. Ca. 2-3 Meetings mit der Expertin / dem Experten. • Projektskizze besprechen / Kick-Off. • Ev. bei Bedarf: Zwischenreview / Beratung. • Schlusspräsentation vor Expert*innen- und Dozierenden-Gremium. • Dauer: 10'–15' und Diskussion: 10'–12' pro Semesterarbeit. 9. Abgabe des Berichtes auf der Studienplattform oder nach Absprache per E-Mail an die Expert*innen. 10. Beurteilung durch die Expert*innen.

Ergebnis und Bewertung	Der Bericht ist in elektronischer Form, als PDF-Dokument, an die bewertenden Expert*innen und die CAS-Leitung über die aktuelle Studienplattform (Moodle) abzugeben. Der Bericht umfasst ca. 20 Seiten. Der Source Code ist (sofern für die Projektbeurteilung notwendig) als Anhang mitzuliefern. Die Semesterarbeit wird nach folgenden Kriterien bewertet: – Themeneingabe Projektskizze rechtzeitig und vollständig eingereicht. Themenpräsentation sorgfältig vorbereitet. Idee oder Aufgabe durchdacht und abgegrenzt, Quellen recherchiert, Rahmenbedingungen definiert, Teilziele priorisiert. – Methodik und Ausführung Gewählte Methode(n) systematisch und korrekt angewendet. Kreativ und agil in der Ausführung. Entscheidungen präzis begründet. – Ergebnis Nachvollziehbares und dokumentiertes Ergebnis. Aufgabenstellung erfüllt. Ergebnisse validiert, getestet, verifiziert. Vergleich von Zielsetzung und Ergebnis vorgenommen. Learnings und Ausblick vorhanden. – Bericht und Dokumentation Vollständig und verständlich. Rechtschreibung korrekt. Kapiteleinteilung sinnvoll. Angemessene Darstellung. Grafiken auf das Wesentliche reduziert und beschriftet. – Schlusspräsentation Roter Faden, logisches Vorgehen, klare Aussagen. Identifikation mit dem Thema spür- und erkennbar. Professionelle Präsentationstechnik, Zeitvorgaben genutzt und eingehalten. Fragen präzis und sicher beantwortet. Die aufgeführten Kriterien sind durch die Expert*innen entsprechend dem bearbeiteten Thema und dem Ablauf der Arbeit in ihrem Gewicht anpassbar.

10 Kompetenznachweis

Für die Anrechnung der 12 ECTS-Credits ist das erfolgreiche Bestehen der Qualifikationsnachweise (Prüfungen, Projektarbeiten) erforderlich, gemäss folgender Aufstellung:

Kompetenznachweis	Gewicht	Art der Qualifikation	Erfolgsquote Studierende
Information Security Technologies	2	Gruppenarbeit & Prüfung	0 – 100 %
Information Security Management	2	Schriftliche Prüfung	0 – 100 %
Identity und Access Management	1	Schriftliche Prüfung	0 – 100 %
Rechtsfragen	1	Schriftliche Prüfung	0 – 100 %
Semesterarbeit	4	Einzel- oder Gruppenarbeit	0 – 100 %
Gesamtgewicht / Erfolgsquote	**10**		3 - 6

Jede*r Student*in kann in einem Kompetenznachweis eine Erfolgsquote von 0 bis 100% erreichen. Die gewichtete Summe aus den Erfolgsquoten pro Thema und dem Gewicht des Themas ergibt eine Gesamterfolgsquote zwischen 0 und 100%. Der gewichtete Mittelwert der Erfolgsquoten der einzelnen Kompetenznachweise wird in eine Note zwischen 3 und 6 umgerechnet. Die Note 3 (gemittelte Erfolgsquote weniger als 50%) ist ungenügend. Die Noten 4, 4.5, 5, 5.5 und 6 (gemittelte Erfolgsquote zwischen 50% und 100%) sind genügend.

11 Lehrmittel

Ergänzende Lehrmittel sind Empfehlungen, um den Stoff zu vertiefen oder zu erweitern. Die Beschaffung liegt im Ermessen der Studierenden:

Nr.	Titel	Autoren	Verlag	Jahr	ISBN-Nr.
1	Serious Cryptography – A Practical Introduction to Modern Encryption	Jean-Philippe Aumasson	no starch press	2017	ISBN: 9781593278267
2	Bulletproof TLS and PKI, Second Edition	Ivan Ristić	Feisty Duck	2022	ISBN: 9781907117091
3	Rollen und Berechtigungs-konzepte, Identity- und Access Management im Unternehmen	Alexander Tsolkas, Klaus Schmidt	Springer Vieweg	2017	ISBN: 978-3658179861
4	Solving Identity Management in Modern Applications, Second Edition	Yvonne Wilson, Abhishek Hingnikar	Apress	2022	ISBN: 9781484282618

12 Dozierende

Vorname Name	Firma	E-Mail
Anton Brunner	SNF	anton.brunner@bfh.ch
Pascal Mainini	BFH	pascal.mainini@bfh.ch
Hans-Peter Käser	BACS	hans-peter.kaeser@bfh.ch
Dominik Kuhn	BIT	dominik.kuhn@bfh.ch
Muriel Künzi	BKS Rechtsanwälte AG	muriel.kuenzi@bfh.ch
Rolf Lanz	BFH	rolf.lanz@bfh.ch

+ Weitere Expert*innen und Betreuer*innen für die Fallstudie / Projektarbeit

13 Organisation

CAS-Leitung:
Anton Brunner
Tel: +41 79 388 77 55
E-Mail: anton.brunner@bfh.ch

CAS-Administration:
Andrea Moser
Tel: +41 31 848 32 11
E-Mail: andrea.moser@bfh.ch

Für die praktischen Übungen wird **zwingend** ein Laptop/Notebook mit >=8GB RAM und >50GB freiem Platz auf der SSD, sowie Administrations- resp. Root-Rechten auf dem OS und auch auf der BIOS- oder UEFI-Ebene benötigt. Als Betriebssysteme sind Windows, Linux oder MAC OS-X geeignet. Während der Durchführung des CAS können sich Anpassungen bezüglich Inhalte, Lernziele, Dozierende und Kompetenznachweise ergeben. Es liegt in der Kompetenz der Dozierenden und der Studienleitung, aufgrund der aktuellen Entwicklungen in einem Fachgebiet, aufgrund der Vorkenntnisse und Interessenslage der Teilnehmenden sowie aus didaktischen und organisatorischen Gründen Anpassungen im Ablauf eines CAS vorzunehmen.

Berner Fachhochschule
Technik und Informatik
Weiterbildung
Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne)
2503 Biel

Telefon +41 31 848 31 11
E-Mail: weiterbildung.ti@bfh.ch

bfh.ch/ti/weiterbildung
bfh.ch/cas-itsec
bfh.ch/mas-cs