Fachhochschule Graubünden
University of Applied Sciences

Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) digitaler Kulturgüter

Memoriav Fachtagung 26.6.2024

Tobias Wildi, tobias.wildi@fhgr.ch

Kulturgüter gehören zu den „kritischen Infrastrukturen“

- Als „kritische Infrastrukturen“ werden Prozesse, Systeme und Einrichtungen bezeichnet, die essentiell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.

- Die „kritischen Infrastrukturen“ in der Schweiz wurden in 28 Teilsektoren unterteilt. Diese Teilsektoren umfassen die verschiedenen Branchen, Industrien, Wirtschaftssektoren und sonstige wirtschaftliche Unterteilungen.

- Sektor Behörden
  - Teilsektor Forschung und Lehre
  - Teilsektor Kulturgüter
  - Teilsektor Parlament, Regierung, Justiz, Verwaltung

- Ein SKI-Inventar definiert die Objekte, die für die Schweiz eine strategisch wichtige Bedeutung haben. Dies, weil sie entweder eine wichtige Versorgungsfunktion haben oder ein grosses Gefahrenpotenzial aufweisen.

FH GR

https://www.babs.admin.ch/de/die-kritischen-infrastrukturen

Schutz kritische Infrastrukturen (SKI)

- Nationale Strategie zum Schutz kritischer Infrastrukturen, verabschiedet durch Bundesrat am 16. Juni 2023.

- Das Bundesamt für Bevölkerungsschutz (BABS), Gruppe SKI, stellt die übergeordnete Koordination bei der Umsetzung dieser Strategie sicher.

- Der Fachbereich Kulturgüterschutz (BABS) und die Eidgenössische Kommission für Kulturgüterschutz (EKKGS) stehen im Austausch mit der Gruppe SKI. Daraus resultierten:

  - 2017 „Risiko- und Verwundbarkeitsanalyse des kritischen Teilsektors Kulturgüter“
  - 2022 „Bericht zur Resilienz im kritischen Teilsektor Kulturgüter“

- In beiden Berichten wurden primär die Cyberrisiken analysiert. Ziel ist es, die Cybersicherheit der kritischen Infrastrukturen zu verbessern.

FH GR

https://www.babs.admin.ch/de/ski

Heterogene Akteurslandschaft bei den kulturgüterbewahrenden Organisationen

		Rechtsform		
		Öffentlich-rechtlich verwaltet mit öffentlichem/gesetzlichem Auftrag	**Privat** mit öffentlichem/gesetzlichem Auftrag	**Privat** mit eigenem Auftrag
Hauptfinanzierungsträger	**Öffentliche Hand**	**Öffentlicher Akteur** • Öffentlich-rechtlich organisiert • mit einem öffentlichen/gesetzlichen Auftrag • Hauptfinanzierung durch öffentliche Hand (private Teilfinanzierung möglich)	**Hybrider Akteur** • privatrechtlich organisiert • mit einem öffentlichen/gesetzlichen Auftrag • Hauptfinanzierung durch öffentliche Hand (private Teilfinanzierung möglich)	**Hybrider Akteur** • privatrechtlich organisiert • mit einem privaten/eigenen Auftrag • Hauptfinanzierung durch öffentliche Hand (private Teilfinanzierung möglich)
	Privat	Unplausibler Fall	Unplausibler Fall	**Privater Akteur** • privatrechtlich organisiert • mit einem privaten/eigenen Auftrag • private Hauptfinanzierung (Teilfinanzierung durch öffentliche Hand möglich)

Haupttypen:

öffentlich	hybrid	privat

BWL IKT-Minimalstandard 2018, 2023
OFAE Norme minimale pour les TIC

- Herausgegeben vom Bundesamt für wirtschaftliche Landesversorgung BWL / Office fédéral pour l'approvisionnement économique du pays OFAE

- Die grundsätzliche Verantwortung zum Eigenschutz liegt bei den jeweiligen Unternehmen und Organisationen.

- Überall da jedoch, wo das Funktionieren von kritischen Infrastrukturen betroffen ist, besteht eine staatliche Verantwortung, basierend auf dem Auftrag der Bundesverfassung sowie dem Landesversorgungsgesetz.

- Betreibern von kritischen Infrastrukturen wird empfohlen, den IKT-Minimalstandard umzusetzen.

https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html

Branchenstandards Normes minimales par secteur

- Basieren auf dem IKT-Minimalstandard, konkretisieren diesen Standard für die verschiedenen Bereiche kritischer Infrastrukturen

- Folgende Branchenstandards existieren bereits:
  - Wasserversorgung, Abwasser, Abfallentsorgung, Lebensmittel, Gasversorgung, Öffentlicher Verkehr, Strom, Fernwärme- und Fernkälteversorgung
  - Eau, Eaux usées, Denrées alimentaires, Gaz, Transports publics, Electricité, Elimination des déchets, Chauffage et froid à distance

- Die Kulturgüter fehlen auf dieser Liste (noch)

https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard/ikt_branchenstandards.html

Erarbeitung Minimalstandard digitale Kulturgüter

- Für den Teilsektor (digitale) Kulturgüter begannen die 2020 Diskussionen für einen Branchenstandard. Beteiligt waren das BWL, Gruppe SKI, Fachbereich KGS und die EKKGS

- Es dauerte aber, bis das notwendige Domänen- und Cybersecurity-Wissen zusammengebracht werden konnte

- 2022/2023 Erarbeitung des Branchenstandards im Rahmen eines Projekt an der Fachhochschule Graubünden

- 2023/2024 Vernehmlassung bei bundesnahen Stellen und bei den Kantonen

- Sommer 2024: Überarbeitung, Layout, Übersetzungen

- Herbst 2024 Publikation

FH GR

Minimalstandard digitale Kulturgüter

- Autor: Tobias Wildi (FHGR)
- Review: Peter Fornaro (DH Lab), Stefanie Müller (FHGR)
- BABS, Fachbereich KGS: Laura Albisetti, Agata Guirard, Olivier Melchior, Julian Miguez, Carine Simoes.
- Richtet sich primär an die Betreiber kritischer Infrastrukturen, soll aber alle kulturgüterbewahrenden Organisationen unterstützen.

FH GR

Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) digitaler Kulturgüter

Stand 24.6.2024
Version 1.0

Gliederung des Minimalstandards

1. Ausgangslage und Zielsetzung
2. Das digitale Kulturerbe der Schweiz
3. Übersicht über die systemkritischen Systeme und Prozesse
4. Defense in Depth
5. NIST Framework Core-Massnahmen **(WAS muss getan werden? Prozesse)**
6. Bausteine zur Verbesserung der Informationssicherheit **(WIE soll man vorgehen? Technik)**
7. Literatur und Ressourcen

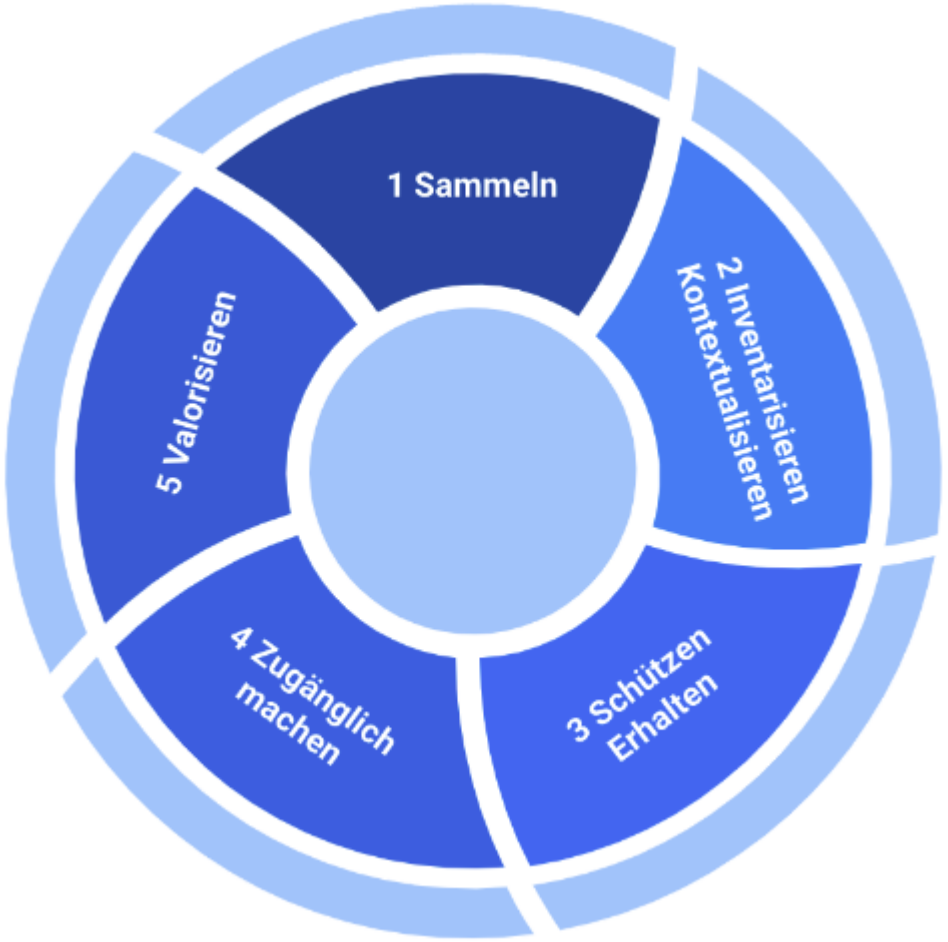
FH GR

3. Übersicht über die systemkritischen Systeme und Prozesse

- Was soll geschützt werden? Die zentralen Aufgaben und Prozesse müssen bekannt sein.

- Generisches Lebensphasenmodell (bzw. Handlungsfelder) für die Bewahrung und Pflege von Kulturerbe

- Ausgeklammert wurden:
  - Vorgelagerte Systeme wie GEVER, Dokumentenmanagement, Records Management, Fachanwendungen
  - Bewertung, Selektion, Auswahl von Kulturgütern für die Archivierung
  - Nachgelagerte Systeme wie Systeme zur Auswertung, Forschungsinfrastrukturen



4 Defense in Depth

- Wichtigstes Prinzip: Es gibt keine Sicherheitsmassnahme, die für sich alleine ausreichend ist, Systeme oder Netzwerke vollständig zu schützen.

- Stattdessen verschiedene Sicherheitsmassnahmen, die in mehreren Schichten oder Ebenen implementiert werden
  - Organisatorische Massnahmen (Prozesse, Verantwortlichkeiten)
  - Technische Massnahmen (Systeme, Netzwerke)
  - Physische Massnahmen

FH GR

5 Strategische Sicht: NIST-Framework

- Ein freiwilliges Rahmenwerk, entwickelt vom National Institute of Standards and Technology (NIST) der USA.
- Besteht aus fünf Funktionen. Diese fünf Funktionen bilden gemeinsam eine strategische Sicht auf das Management von Cyber-Risiken einer Organisation.
- Orientiert sich an einem Risikokreislauf
- Schaffung eines einheitlichen Ansatzes zur Analyse von Cybersicherheitsrisiken. Die Anwendung des NIST-Frameworks gibt Aufschluss darüber, **was** gemacht werden muss zur Reduzierung der Risiken.

https://www.nist.gov/cyberframework

6 Bausteine zur Verbesserung der Informationssicherheit

- Die Kulturerbepflege zeichnet sich aus durch eine sehr heterogene Akteurslandschaft
  - Bezüglich Grösse (Anzahl Mitarbeitende und verfügbare Ressourcen für die Informationssicherheit)
  - Bezüglich den zu schützenden Werten
  - Bezüglich Auftrag (öffentlich/gesetzlicher Auftrag oder eigener Auftrag)
  - Bezüglich Art der Finanzierung (öffentliche Hand oder privat)

- Es ist nicht möglich, generische Vorgaben für alle Typen von Akteuren zu machen.

- Wir haben uns entschieden, mit Bausteinen zu arbeiten, die die Akteure je nach ihren Anforderungen zu einer Defense in Depth kombinieren können

- Das NIST-Framework sagt, **was** gemacht werden muss, im Sinne eines Assessments. Die IT-Grundschutz-Bausteinen liefern Ideen, **wie** es gemacht werden kann.

FH GR

Übersicht über die Bausteine

6 Bausteine zur Verbesserung der Informationssicherheit

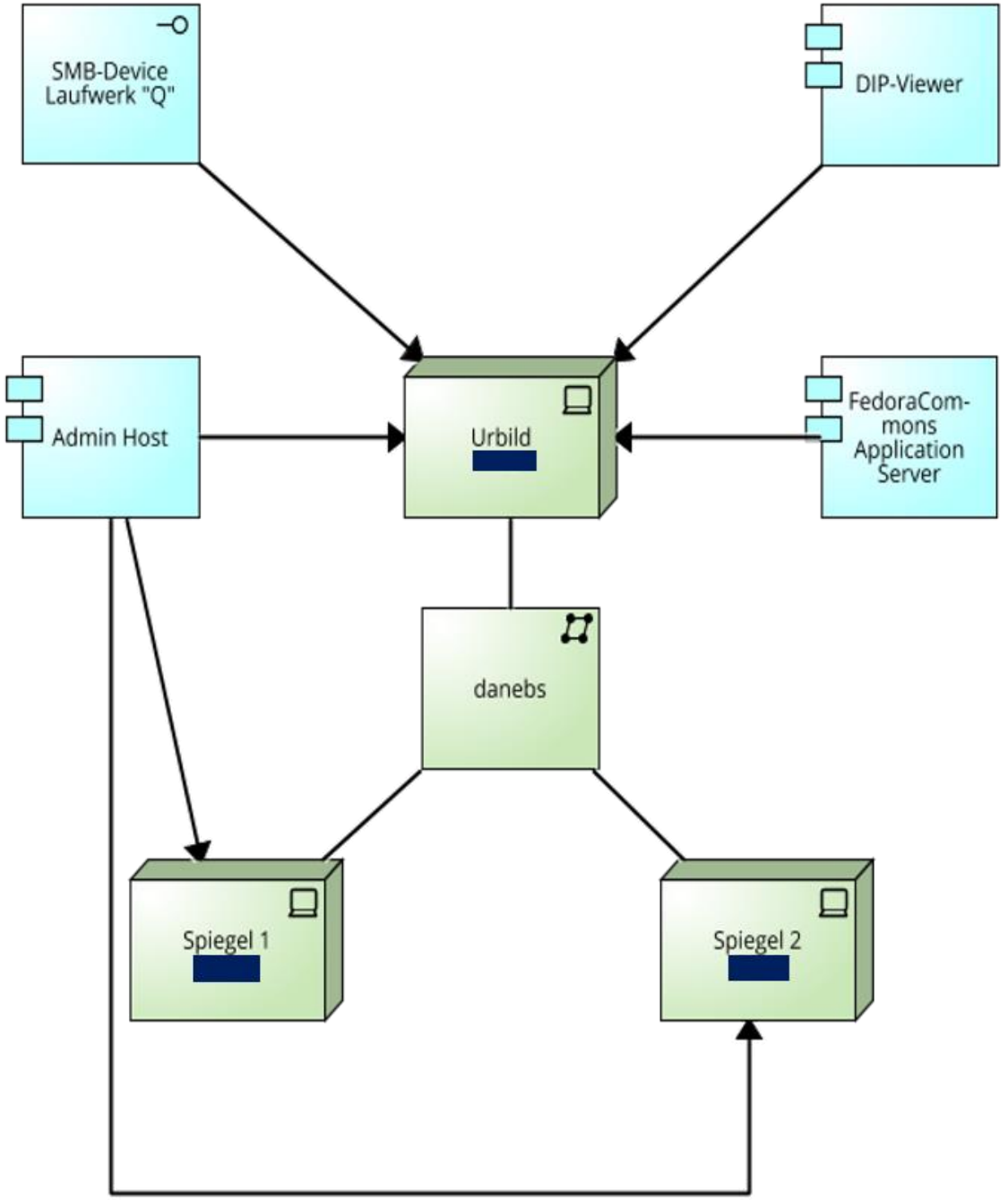
- 6.1 Sicherheitsmanagement
- 6.2 Prozess-Bausteine
  - Organisation
  - Personal
  - Sensibilisierung und Schulung
  - Identitäts- und Berechtigungsmanagement
  - Compliance Management (Anforderungsmanagement)
  - Datenschutz
  - Datensicherungskonzept
  - Löschen und Vernichten
  - Eigener Betrieb
  - Betrieb durch Dritte (Cloud)
- 6.3 System-Bausteine
  - Server
  - Speicherlösungen
  - Desktop-Systeme
  - Wechseldatenträger
  - Netzwerk
- 6.4 Physische Bausteine
  - Allgemeines Gebäude
  - Rechenzentrum, Serverraum
  - Datenträgerarchiv

FH GR

Baustein „Speicherlösungen“

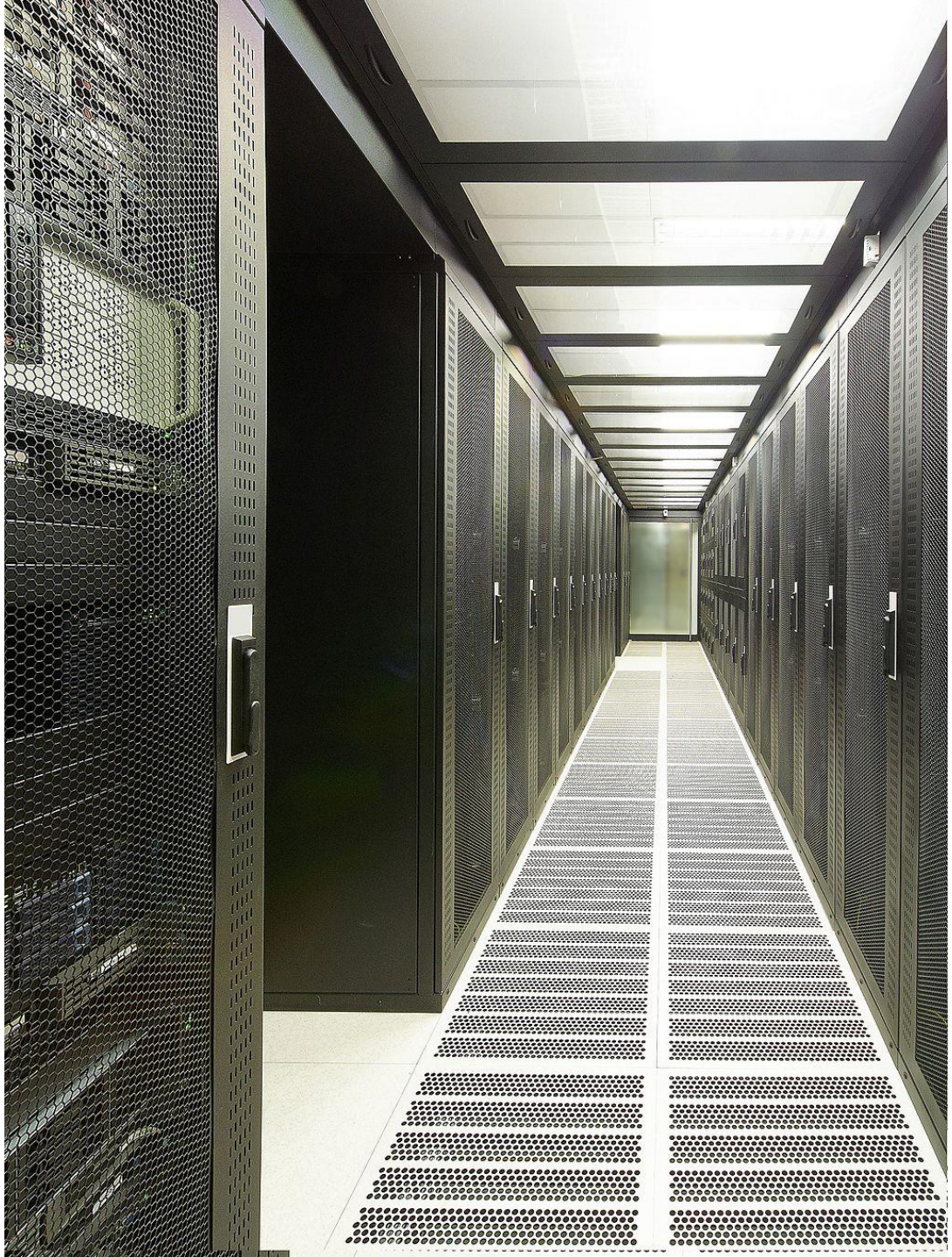
Spezifisch für die Archivierung ist wichtig, dass

- mindestens drei voneinander unabhängige Kopien der Daten gehalten werden,
- wovon eine geographisch getrennt ist.
- Die Speicherlösung unterstützt die regelmässige Überprüfung der Integrität der Daten
- und verfügt über Self-Healing-Mechanismen, um alfällige Fehler zu korrigieren.



Baustein „Rechenzentrum, Serverraum“

- Sicherung von Zugängen zu Rechenzentren und Serverräumen
- Kontrolle von Besuchern und Gästen
- Installation von Sicherheitsanlagen wie Überwachungskameras, Alarmanlagen und Zugangskontrollsystemen
- Klimatisierung
- Unterbruchsfreie Stromversorgung
- Feuerlöschsysteme



FH GR

Nächste Schritte – Ausblick

- Übersetzung, Layout und dann Publikation des Berichts im Herbst 2024

- Herunterbrechen der Bausteine auf konkrete Massnahmen und Checklisten

- Zielgruppengerichtete Aus- und Weiterbildungsangebote erarbeiten und durchführen
  - Informatikdienste
  - Fachpersonen in Gedächtnisinstitutionen
  - Kleine Institutionen, die grösstenteils mit Freiwilligen arbeiten

- Diskussion um den „Digitalen Bergungsort“ als Ablösung der Mikroverfilmung muss wieder aufgenommen werden.

FH GR

Fachhochschule Graubünden
Pulvermühlestrasse 57
7000 Chur
T +41 81 286 24 24
info@fhgr.ch

Vielen Dank für Ihre Aufmerksamkeit.

Fachhochschule Graubünden
Scuola universitaria professionale dei Grigioni
Scola universitara professiunala dal Grischun
University of Applied Sciences of the Grisons

swissuniversities

SCHWEIZERISCHER AKKREDITIERUNGSRAT
CONSEIL SUISSE D'ACCRÉDITATION
CONSIGLIO SVIZZERO DI ACCREDITAMENTO
SWISS ACCREDITATION COUNCIL
Institutionell akkreditiert nach HFKG 2018-2025