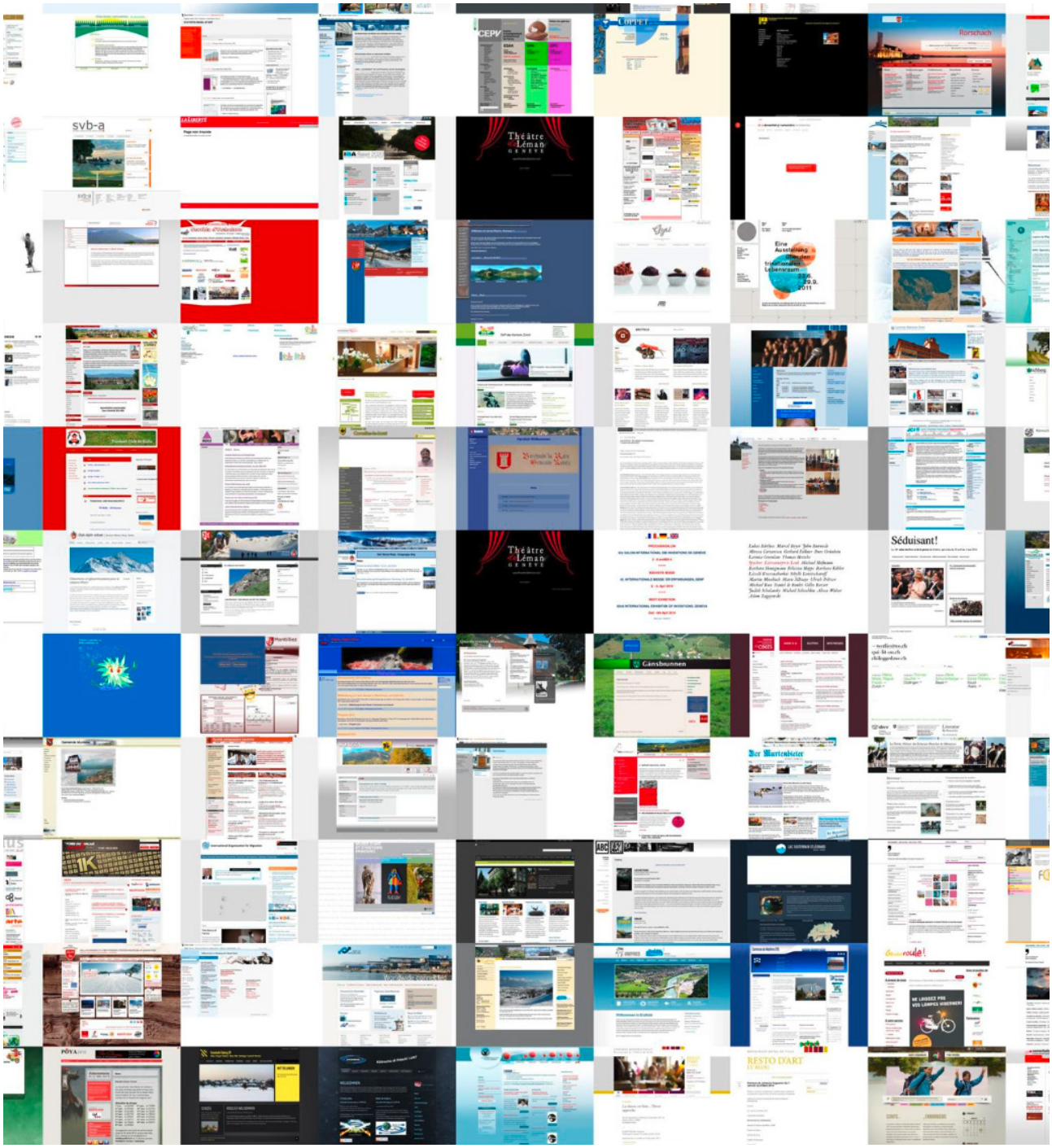
Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) digitaler Kulturgüter



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Bevölkerungsschutz BABS

Stand 17.08.2026

Titelbild:
Webarchiv Schweiz, Schweizerische Nationalbibliothek (NB). Einstiegsseite als Collage.
https://www.e-helvetica.nb.admin.ch/collage/

Autor:
Tobias Wildi, Fachhochschule Graubünden, docuteam AG

Herausgeber:
Bundesamt für Bevölkerungsschutz BABS,
Geschäftsbereich Zivilschutz und Ausbildung,
Fachbereich Grundlagen Zivilschutz und Ausbildung,
Gruppe Kulturgüterschutz
kulturgueterschutz@babs.admin.ch
www.kgs.admin.ch

Alle Links wurden am 29.7.2026 letztmals überprüft.

Vorwort

In seiner «Strategie Digitale Schweiz»[1] unterstreicht der Bundesrat seinen Willen, die Chancen, die der digitale Wandel der Schweiz bietet, optimal zu nutzen. Heute ist der Betrieb von Archiven ohne den Einsatz von Informations- und Kommunikationstechnologie (IKT) kaum noch vorstellbar. Der hier vorgestellte IKT-Minimalstandard konzentriert sich auf die Sicherheit der digitalen Langzeitarchivierung, insbesondere auf die Sicherung von Data at Rest im Bereich der digitalen Kulturgüter (siehe Glossar), und ist als Empfehlung für Organisationen im Bereich der Kulturerbepflege gedacht.

Die Eidgenössische Kommission für Kulturgüterschutz (EKKGS) arbeitet gemeinsam mit dem Bundesamt für Bevölkerungsschutz (BABS) und externen Fachleuten daran, die Resilienz digitaler Kulturgüter zu erhöhen. Der vorliegende Standard braucht allerdings auch Rückhalt in den betroffenen Institutionen. Diese erste Fassung des IKT-Minimalstandards soll deshalb regelmässig aktualisiert und wo nötig konkretisiert und erweitert werden.

Mit der zunehmenden Digitalisierung der Verwaltung (elektronische Geschäftsverwaltung GEVER, Fachanwendungen) hat die Menge des digitalen Archivguts in den letzten Jahren deutlich zugenommen. Zugleich führt die Digitalisierung von Geschäftsprozessen zu neuen Gefahren, auf die reagiert werden muss. Die Gefahr von Cyberangriffen auf die IT-Infrastruktur betrifft nicht nur staatliche Stellen, sondern auch Betreiber kritischer Infrastrukturen und Organisationen im Bereich der Kulturerbepflege (Museen, Bibliotheken). Heutzutage beruht auch der Erhalt des analogen Kulturerbes auf digitalen Daten wie Inventar- und Katalogdatenbanken, Digitalisaten sowie digitalen Sicherstellungs- und archäologischen Funddokumentationen.

Digitale Kulturgüter gewinnen besonders an Bedeutung, wenn von den Kulturgütern keine physischen Originale mehr vorhanden sind oder diese *born-digital*, also direkt in digitaler Form erzeugt wurden. Bei der Langzeitarchivierung dieser digitalen Objekte stellt sich die zentrale Frage, was «lange Zeit» wirklich bedeutet. Es geht darum, Daten über viele Generationen von Prozessorarchitekturen, Betriebssystemen und Dateiformaten hinweg nutzbar zu halten. Die notwendigen Massnahmen dafür gehen über einfache Datensicherungen und Backups hinaus. Archivarisches Denken bewegt sich in Zeiträumen von Jahrzehnten und Jahrhunderten. Dieser speziellen Herausforderung wird im folgenden Branchenstandard Rechnung getragen.

1 Siehe dazu https://digital.swiss/de/strategie/strategie.html

Zusammenfassung

Der vorliegende IKT-Minimalstandard dient als Empfehlung und Richtschnur zur Verbesserung der IKT-Resilienz in Organisationen, die sich mit der Pflege und dem Erhalt digitaler Kulturgüter befassen. Er richtet sich primär an Betreiber kritischer Infrastrukturen, insbesondere an deren Geschäftsleitungsmitglieder und IKT-Verantwortliche. Der Minimalstandard soll jedoch grundsätzlich für jede Organisation nützlich sein, die sich mit der Bewahrung von Kulturgütern beschäftigt. Ziel ist es, Risiken zu erkennen und auf ein akzeptables Mass zu reduzieren.

Der IKT-Minimalstandard bietet ein Rahmenwerk mit dem Fokus auf der langfristigen Sicherung digitaler Kulturgüter und dem Ziel, ein angemessenes Sicherheitsniveau gegen Cyber-Angriffe sowie andere Gefahren zu erreichen. Nach einem Vorfall soll möglichst rasch wieder ein Normalbetrieb möglich sein. Für die Planung wird das «NIST Cybersecurity Framework»[2] verwendet, mit dem Organisationen ihre Risiken systematisch einschätzen und so einstufen können, wie weit ihre Massnahmen dagegen gediehen sind. Kern der Empfehlung ist die Implementierung einer sogenannten Defense-in-Depth-Strategie, also einer mehrstufigen Strategie gegenüber Cyber-Bedrohungen.

Weiter umreisst der Minimalstandard konkrete Bausteine zur Verbesserung der Resilienz, welche die Kategorien Sicherheitsmanagement, Prozesse, Systeme und physische Sicherheit betreffen. Diese Bausteine helfen sowohl grossen als auch kleinen Organisationen der Kulturerbepflege.

Die Struktur des vorliegenden Standards richtet sich nach dem Modell des allgemeinen «IKT-Minimalstandards – 2023»[3] des Bundesamtes für wirtschaftliche Landesversorgung (BWL).

2 Standard des National Institute of Standards and Technology (USA): https://www.nist.gov/cyberframework.

3 Das Dokument ist abrufbar unter: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html.

Inhaltsverzeichnis

Vorwort 3

Zusammenfassung 4

Inhaltsverzeichnis 5

1 Ausgangslage und Zielsetzung 7
1.1 Hintergrund und Überblick 7
1.2 Geltungsbereich und Abgrenzungen 8
1.3 Ziele und Struktur des IKT-Minimalstandards 9
1.4 Umsetzung des IKT-Minimalstandards 10
1.5 Vorarbeiten und gesetzliche Grundlagen 11

2 Das digitale Kulturerbe der Schweiz 12
2.1 Übersicht und Stakeholder 13
2.2 Archive und Archivstruktur in der Schweiz 14

3 Übersicht über die systemkritischen Systeme und Prozesse 15
3.1 Systemkritische Archive 15
Bundesarchiv (BAR) 15
Staatsarchive und Kommunalarchive 15
Spezialarchive 15
3.2 Leistungen der Archive im Teilsektor Kulturgüter 15
3.3 Übersicht der kritischen Prozesse 16
Sammeln 16
Inventarisieren und kontextualisieren 16
Schützen und erhalten 16
Zugänglichmachen 16
Valorisieren 16
3.4 Gegen welche Gefahren schützen? 17

4 Defense in Depth 18
4.1 Das Defense in Depth-Konzept 18
4.2 Organisatorische Massnahmen (Prozesse) 18
4.3 Technische Massnahmen (Systeme) 19
4.4 Physische Massnahmen 19
4.5 Trennung von Büroinformatik und Archivsystem 19

5 NIST Framework Core-Massnahmen 21
5.1 Übersicht 21
NIST Framework Core 21
NIST Framework und Branchenstandard ISO 16363:2012 22
5.2 Identifizieren (Identify) 24
Inventar-Management (Asset Management) 24
Geschäftsumfeld (Business Environment) 25
Vorgaben (Governance) 26
Risikoanalyse (Risk Assessment) 27
Risikomanagementstrategie (Risk Management Strategy) 28
Lieferketten-Risikomanagement (Supply Chain Risk Management) 29
5.3 Schützen (Protect) 30
Zugriffsmanagement und -steuerung (Access Control) 30
Sensibilisierung und Ausbildung (Awareness and Training) 31
Datensicherheit (Data Security) 32
Informationsschutzrichtlinien (Information Protection Processes and Procedures) 33
Unterhalt (Maintenance) 34
Einsatz von Schutztechnologie (Protective Technology) 35
5.4 Erkennen (Detect) 36
Auffälligkeiten und Vorfälle (Anomalies and Events) 36
Überwachung (Security Continous Monitoring) 37
Detektionsprozess (Detection Processes) 38
5.5 Reagieren (Respond) 39
Reaktionsplanung (Response Planning) 39
Kommunikation (Communications) 40
Analyse (Analysis) 41
Schadensminderung (Mitigation) 42
Verbesserungen (Improvements) 43
5.6 Wiederherstellen (Recover) 44
Wiederherstellungsplanung (Recovery Planning) 44
Verbesserungen (Improvements) 45
Kommunikation (Communications) 46

6 Bausteine zur Verbesserung der Informationssicherheit 47
6.1 Sicherheitsmanagement 48
6.2 Prozess-Bausteine 48
Organisation 48
Personal 48
Sensibilisierung und Schulung 49
Identitäts- und Berechtigungsmanagement 49
Compliance Management (Anforderungsmanagement) 49
Datenschutz 50
Datensicherungskonzept 50
Löschen und Vernichten 51
Eigener Betrieb 51
Betrieb durch Dritte (Cloud) 51
6.3 System-Bausteine 52
Server 52
Speicherlösungen 52
Desktop-Systeme 52
Wechseldatenträger 53
Netzwerk 53
6.4 Physische Bausteine 53
Allgemeines Gebäude 53
Rechenzentrum, Serverraum 54
Datenträgerarchiv 54
7 Literatur 55
8 Glossar und Abkürzungsverzeichnis 56

1 Ausgangslage und Zielsetzung

Heutzutage entstehen viele Kulturgüter in digitaler Form und werden entsprechend archiviert und genutzt. Zum digitalen Kulturerbe zählen beispielsweise öffentliche Archive (wie das Bundesarchiv, Staats- und Kommunalarchive), Sammlungen in Bibliotheken (darunter Bildarchive, Nachlässe von Autorinnen und Autoren, Forschungsdaten) sowie Museen mit ihren Video- und Netzkunstwerken oder Fotobeständen. Die Nutzung und der Schutz dieser Kulturgüter erfordern digitale Hilfsmittel wie Sicherstellungsdokumentationen, Inventare, Kataloge und Digitalisate.

Die Pflege digitaler Kulturgüter ist essentiell, in der Schweiz gehören einige davon zu den systemkritischen Infrastrukturen. Diese Infrastrukturen sind für das gesellschaftliche Funktionieren sowie die Aufrechterhaltung von Ordnung und Sicherheit unverzichtbar. Archive leisten hierbei einen wichtigen Beitrag zur Rechtssicherheit, indem sie wichtige Dokumente wie Gesetzestexte, Verträge, Urkunden und Gerichtsurteile aufbewahren.

Der vorliegende Bericht konzentriert sich auf die Situation der Archive, aber die Grundsätze gelten auch für andere Einrichtungen, die sich um digitale Kulturgüter kümmern, einschliesslich Bibliotheken, Museen, Denkmalpflegestellen, archäologische Dienste und Dokumentationszentren, unabhängig von ihrer rechtlichen Organisation. Wie alle Branchen sind auch die digitalen Kulturgüter verschiedenen Gefahren ausgesetzt. Der IKT-Minimalstandard soll Kulturerbe-Organisationen helfen, ihre IT-Infrastruktur widerstandsfähiger zu machen. Dieser Standard verfolgt einen risikobasierten Ansatz, der unterschiedliche Schutzniveaus ermöglicht, angepasst an die spezifischen Bedürfnisse der Organisationen.

Der IKT-Minimalstandard bietet in Kap. 3 einen Überblick über zu schützende kritische Systeme und Prozesse und stellt in Kap. 4 das Konzept der «Defense in Depth» vor – eine mehrstufige Verteidigung gegen Cyber-Gefahren. Anschliessend führt Kap. 5 das «NIST Cybersecurity Framework» ein, einen risikobasierten Ansatz, um Cyber-Risiken zu analysieren und zu bewältigen. Abschliessend werden in Kap. 6 konkrete Sicherheitsmassnahmen vorgeschlagen, unterteilt in die Kategorien Sicherheitsmanagement, Prozess-, System- und physische Bausteine.

1.1 Hintergrund und Überblick

Im Jahr 2021 hat das Bundesamt für Bevölkerungsschutz (BABS) den «Bericht zur Resilienz im kritischen Teilsektor Kulturgüter»[4] aktualisiert. Dieser Bericht führt aus, dass die heutigen Archivierungs- und Bibliotheksprozesse eine grosse Abhängigkeit von Informations- und Kommunikationstechnologie (IKT) zeigen. Vor diesem Hintergrund stellen Cyber-Angriffe auf Archive und Bibliotheken ein Risiko dar, das weit über die betroffenen Institutionen hinausreicht und gesamtgesellschaftliche Auswirkungen haben kann.

Für die Zukunft ist nicht nur ein markanter Anstieg digitaler Bestände in Archiven und Bibliotheken zu erwarten, sondern auch eine fortschreitende Zentralisierung der Datenhaltung. Dies manifestiert sich in der Bildung von Archiv-Verbünden, Kooperationen und dem gemeinsamen Betrieb von Rechenzentren, wie beispielsweise beim DIMAG[5] Schweiz, einem Zusammenschluss mehrerer Kantone. Derartige digitale Netzwerke bieten zwar Vorteile durch Synergien im Betrieb wartungsintensiver Infrastrukturen, bergen jedoch gleichzeitig ein erhöhtes Risiko bei gezielten Cyberangriffen oder Ausfällen der IKT-Systeme.

4 Interner Bericht. Ein zusammenfassendes Factsheet ist abrufbar unter: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/21/1209e420-c585-43d9-b9bb-297d4e7b87b2.pdf

5 DIMAG (Kurzform für Digitales Magazin) ist ein Paket von Software-Lösungen für die digitale Langzeitarchivierung behördlicher Unterlagen. DIMAG wurde von den Archivverwaltungen der deutschen Bundesländer Baden-Württemberg und Hessen sowie des Freistaats Bayern entwickelt. Die Kantone Solothurn, Schaffhausen und Aargau gründeten 2019 den Archivverbund DIMAG Schweiz. Siehe auch: https://www.eoperations.ch/service/geschaeftsstelle-dimag/.

Eine detaillierte Risikoanalyse, die im besagten Bericht durchgeführt wurde, untersucht das Potenzial von Beeinträchtigungen der Archivprozesse durch zielgerichtete Cyber-Angriffe auf Staatsarchive oder kantonale IKT-Systeme. Der Bericht verdeutlicht, dass solche Angriffe und die daraus resultierenden Ausfälle der IKT-Infrastruktur die Zugänglichkeit und Verfügbarkeit der Archivbestände und der Archivverbünde langfristig beeinträchtigen können. Hinzu kommt das Risiko einer irreversiblen Zerstörung oder Entwendung sowie der beabsichtigten oder unbeabsichtigten Veröffentlichung sensibler Informationen.

1.2 Geltungsbereich und Abgrenzungen

Die Verantwortung zum Schutz digitaler Kulturgüter liegt grundsätzlich bei den bewahrenden Institutionen, die auf der Basis eines gesetzlichen oder freiwilligen Auftrags handeln. Überall da wo das Funktionieren von kritischen Infrastrukturen betroffen sein kann besteht zusätzlich eine staatliche Verantwortung, basierend auf dem Auftrag der Bundesverfassung sowie dem Landesversorgungsgesetz (LVG)[6]. Der vorliegende IKT-Minimalstandard ist Ausdruck dieser Schutzverantwortung des Staates gegenüber der Gesellschaft, der Wirtschaft, den Institutionen und der öffentlichen Verwaltung.

Dieser Standard richtet sich primär an die Betreiber und Verantwortlichen kritischer Infrastrukturen im Teilbereich Kulturgüter, welche im Inventar Schutz kritischer Infrastrukturen (SKI-Inventar)[7] aufgeführt sind. Alle Objekte im SKI-Inventar sind ebenfalls im KGS-Inventar als Objekte von nationaler Bedeutung (sogenannte A-Objekte)[8] aufgeführt. Die Branchenempfehlung richtet ihren Fokus auf Institutionen (Archive, Bibliotheken, Museen) mit digitalen Archivbeständen, es können jedoch auch andere Institutionen innerhalb des Teilbereichs Kulturgüter betroffen sein, welche über digitale Bestände verfügen. Betreibern von kritischen Infrastrukturen wird empfohlen, den IKT-Minimalstandard umzusetzen. Der Standard bietet grundsätzlich jedem Akteur, der sich mit der Erhaltung von Kulturgütern beschäftigt, eine Hilfestellung und konkrete Bausteine zur Verbesserung der IKT-Resilienz.

Oftmals werden digitale Kulturgüter unterteilt in die Kategorien «born digital» und «retrodigitalisiert». Der vorliegende Minimalstandard differenziert jedoch nicht zwischen diesen beiden Kategorien, sondern betrachtet sie als gleichwertig. Dies ist darauf zurückzuführen, dass die Grenze zwischen den ursprünglich klar abgegrenzten Konzepten in den letzten Jahren zunehmend verschwommen ist. Mit der Retrodigitalisierung sind heute neben der Analog-Digital-Wandlung zumeist auch Schritte der Datafizierung verbunden. Beispiele dafür sind Text- oder Spracherkennung, "Named Entity Recognition" (NER) zur Überführung von Text in strukturierte Daten, Vektorisierung von Plänen, 3D-Scans in der Archäologie oder bei Museumsobjekten. Darüber hinaus dienen Retrodigitalisate als Sicherheitskopien der analogen Originalmaterialien und erhalten bei deren Verlust einen Originalcharakter. Folglich hängt der Wert digitaler Kulturgüter nicht von ihrer Entstehungsweise ab, sei diese retrodigitalisiert oder «born digital».

Es existieren bereits mehrere international anerkannte Standards zur IT-Sicherheit (Überblick siehe Kap. 7 Literatur). Der IKT-Minimalstandard versteht sich nicht als Konkurrenz zu diesen bestehenden Standards, sondern ist mit ihnen kompatibel, allerdings verfügt er über einen reduzierten Umfang. Er soll einen einfacheren Einstieg in die Thematik ermöglichen und bei den wichtigsten Massnahmen zur Erreichung eines angemessenen Schutzniveaus helfen. Die Branchenempfehlung fokussiert auf jene Prozesse, welche einen direkten Einfluss auf die Sicherheit digitaler Kulturgüter, respektive die Sicherung sogenannter Data at Rest haben. Die Sicherheit der administrativen IT-Infrastruktur wird dabei nicht oder nur in untergeordneter Weise behandelt.

6 Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG; SR 531) vom 17. Juni 2016 (Stand am 1. Juli 2023).

7 Das SKI-Inventar bezeichnet einzelne kritische Infrastruktur-Elemente, die von strategisch wichtiger Bedeutung sind. Das Inventar dieser Bauten und Anlagen wurde in Zusammenarbeit mit den Kantonen 2012 zum ersten Mal erstellt. Es ist klassifiziert und nicht öffentlich zugänglich. Es dient den zugriffsberechtigten Stellen (Bund, Kantone und Betreiber) als Planungs- und Priorisierungsgrundlage im Risikomanagement und in der Ereignisbewältigung.

8 Das KGS-Inventar 2021 ist abrufbar unter: https://www.babs.admin.ch/de/aufgabenbabs/kgs/inventar.html.

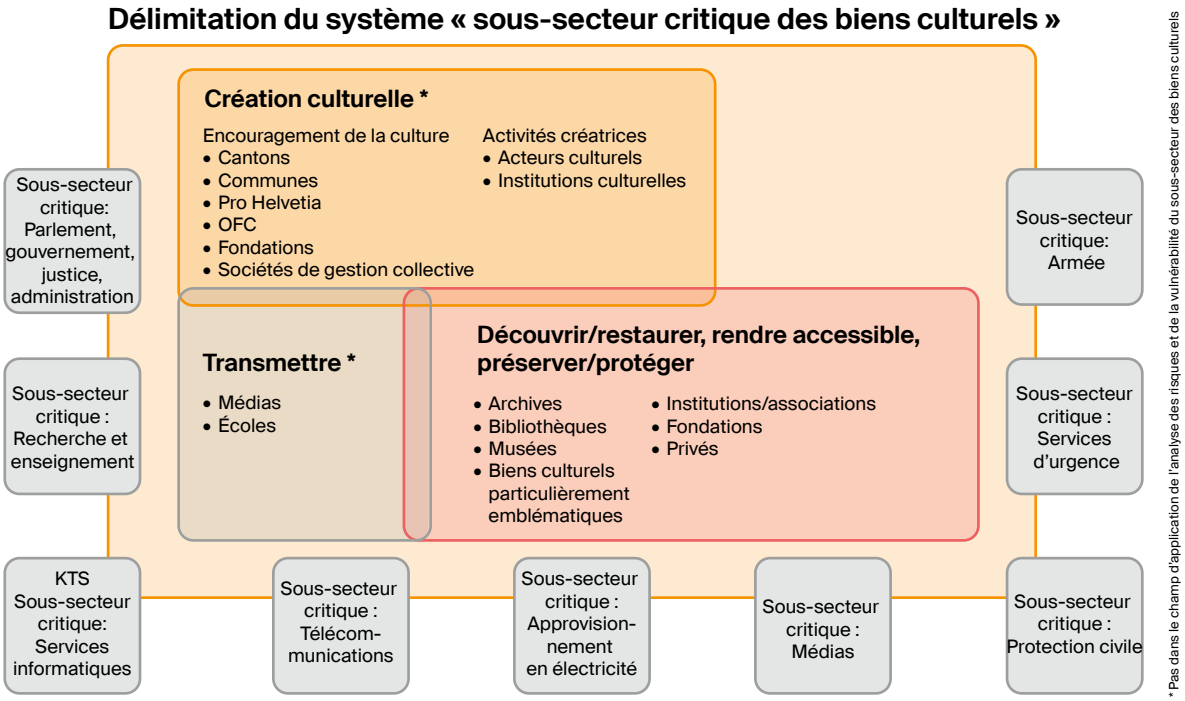


Abbildung: Systemgrenze des kritischen Teilsektors Kulturgüter

1.3 Ziele und Struktur des IKT-Minimalstandards

Dieser IKT-Minimalstandard ist als präventive Massnahme gedacht und als Branchenempfehlung formuliert.

Das Dokument gliedert sich in folgende Kapitel:

- Kapitel 1 und 2 bieten eine Einführung in die im Fokus stehenden Bereiche des Kulturgüterschutzes
- Kapitel 3 beschreibt die kritischen Systeme und Prozesse
- Kapitel 4 erläutert den Defense in Depth-Ansatz
- Kapitel 5 beschreibt ein Framework zur Überprüfung und Planung der Resilienz
- Kapitel 6 enthält konkrete Empfehlungen zur Verbesserung der Resilienz in Form von organisatorischen und technischen Bausteinen.

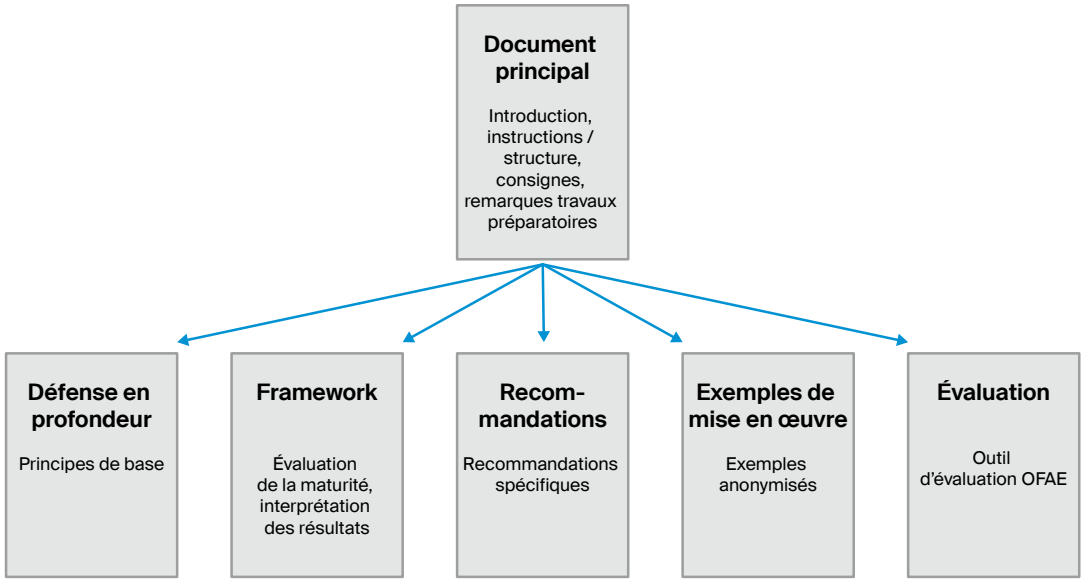


Abbildung: Übersicht der Dokumente des IKT-Minimalstandards

Zur Einschätzung des Maturitätsniveaus des Unternehmens oder der Organisation steht vom BWL ein Assessment-Tool[9] zur Verfügung. Der IKT-Minimalstandard gilt dann als umgesetzt, wenn die Maturität – gemäss Einstufung des Assessment-Tools – entsprechend dem eigenen risikobasierten Ansatz mindestens den Minimalvorgaben im Overall-Rating entspricht. Es wird prinzipiell ein prozessbasiertes Vorgehen empfohlen, damit eine regelmässige, ständige Überprüfung und Verbesserung garantiert werden kann.

1.4 Umsetzung des IKT-Minimalstandards

Die institutionelle Landschaft der Kulturgüterbewahrung ist sehr heterogen ausgestaltet, gerade was die Grösse, den Auftrag und die Art der Finanzierung betrifft. Nicht jede Institution wird in der Lage sein, den IKT Minimalstandard komplett umzusetzen. Kleinere und finanzschwächere Institutionen werden sich auf wenige zentrale Schutzmassnahmen konzentrieren. Die Umsetzungsvorschläge in Kap. 6 sind modular als Bausteine aufgebaut. Jede Institution kann basierend auf ihrem Sammlungs- und Risikoprofil die für sie relevanten Bausteine priorisieren. Je nach Grösse der Institution gilt die folgende generelle Richtschnur für die Umsetzung:

Art der Institution	Beispiele	Umsetzungsempfehlung
Klein, beschränkte Ressourcen, tiefer Professionalisierungsgrad	Kleines Kommunalarchiv, Spezialarchiv mit fokussiertem Sammlungsprofil	Konzentration auf ausgewählte Bausteine aus Kap. 6
Mittel bis gross, gesicherte Ressourcen, hoher Professionalisierungsgrad	Grosses Kommunalarchiv, Staatsarchiv, Bundesarchiv, Spezialarchiv mit breitem Sammlungsprofil	IKT-Minimalstandard vollumfänglich, inklusive Assessment-Tool

Für die Umsetzung des IKT-Minimalstandards steht das untenstehende Prozessmodell zur Verfügung. Falls die IT des Archivs Teil einer grösseren IT-Organisation ist (bspw. Stadt, Kanton oder Bund), kann die Umsetzung übergeordnet erfolgen und auch weitere Infrastrukturen umfassen. Falls dies nicht der Fall ist oder das Archiv eigenständig nach diesem Standard gesichert werden soll, wird als Nächstes eine Grösseneinstufung durchgeführt. Kleine Institutionen setzen die für sie prioritären Bausteine in Kap. 6 um. Mittlere und grosse Institutionen setzen den IKT-Minimalstandard vollumfänglich um.

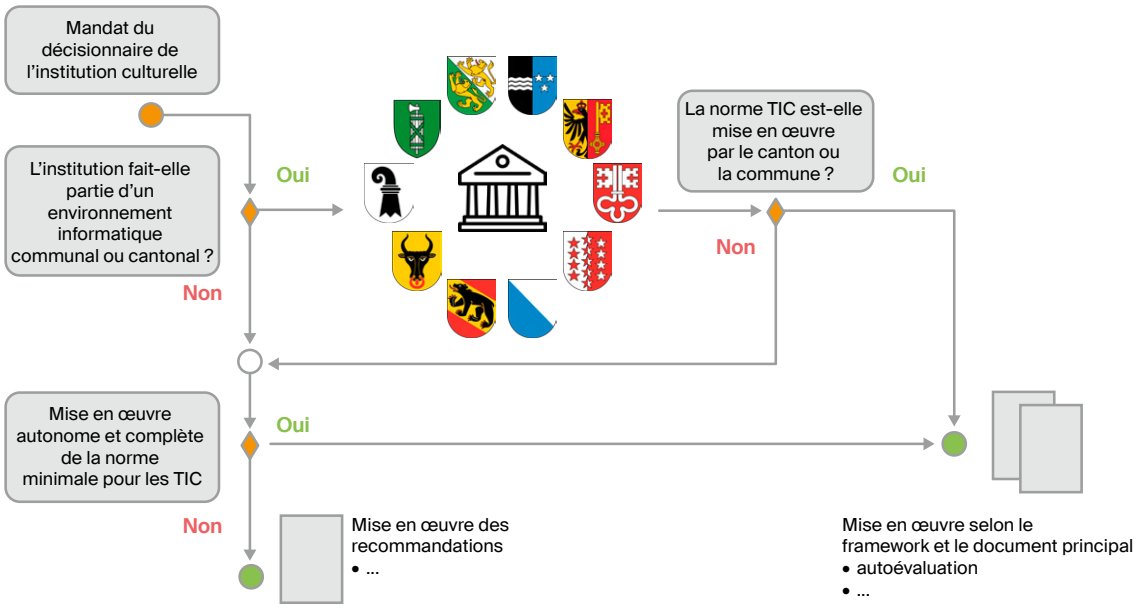


Abbildung: Visualisierung des Prozesses zur Umsetzung des IKT-Minimalstandards

9 Das Assessment-Tool steht unter https://www.bwl.admin.ch/de/ikt-minimalstandards

Grundsätzlich wird insbesondere für grosse Einrichtungen ein prozessbasierter Ansatz empfohlen. Dies bedeutet, dass Cybersecurity kein Zustand ist, sondern als Prozess verstanden, gelebt und immer wieder überprüft wird. Sicherheit im Umgang mit IKT kann nie erzielt werden, sondern muss ständig angestrebt und periodisch aktualisiert werden.

1.5 Vorarbeiten und gesetzliche Grundlagen

Basierend auf der Bundesverfassung besitzen die Kantone die Kulturhoheit. Zudem sind sie, gemäss den Archivgesetzen, verantwortlich für die öffentlich-rechtlichen Archive. Der Bund kann die Kantone subsidiär unterstützen. Insbesondere kann das BABS beim Schutz von Kulturgütern die Kantone[10] unterstützen und beraten.

Der Bundesrat hat am 16. Juni 2023 die nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) verabschiedet.[11] Dabei handelt es sich um eine Weiterentwicklung der ersten beiden Strategien aus den Jahren 2012 und 2017. Das BABS ist mit der Koordination der Aufgaben im SKI-Bereich beauftragt. Die SKI-Strategie bezeichnet 17 Massnahmen, mit denen die Resilienz sowohl sektorspezifisch als auch sektorübergreifend verbessert wird. In der «Nationalen Strategie zum Schutz vor Cyberrisiken»[12] wird deutlich, dass sich die Schweiz aus wirtschafts- und gesellschaftspolitischer Sicht vor Cyber-Gefahren unbedingt schützen muss, um die Chancen der Digitalisierung konsequent nutzen zu können und den Standortvorteil als sicheres Land zu erhalten. Die Arbeiten in den Bereichen SKI und Cyber werden zwischen Bund und Kantonen koordiniert. Im Zuge der Umsetzung ist das Nationale Zentrum für Cybersicherheit (NCSC) entstanden, das eng mit dem Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei zusammenarbeitet. Ebenfalls hat das BWL zu diesem Zwecke einen Minimalstandard zur Verbesserung der IKT-Resilienz herausgegeben.

Die EKKGS hat 2020 eine Strategie 2021–2025 in den Bereichen Prävention/Vorsorge – Einsatz – Nachsorge im Kulturgüterschutz[13] verabschiedet. In dieser werden die wichtigsten Leitlinien für einen möglichst hohen Schutz der Kulturgüter festgehalten. Der Digitalisierung und der Cybersicherheit von digitalen Kulturgütern wird darin ein wichtiger Stellenwert beigemessen. Die notwendige begriffliche Präzisierung und die Erarbeitung einer Bewertungsmatrix für die systematische Aufnahme ins KGS-Inventar wurden vorgenommen. Der langfristige und nachhaltige Erhalt digitaler Objekte ist Teil dieser KGS-Strategie.

Das Digital Humanities Lab (DH Lab) der Universität Basel führte im Auftrag der EKKGS und des BABS KGS Online-Umfragen zu digitalen Kulturgütern durch und wertete diese aus.[14] Die Resultate beider Umfragen des DH Lab von 2016 und 2020 zur Ermittlung von Mengengerüsten digitaler Kulturgüter und die daraus abgeleiteten Bedürfnisse im Bereich Sicherheit flossen als Grundlage in den IKT-Minimalstandard ein.

10 Art. 4 Abs. b Bundesgesetz über den Schutz der Kulturgüter bei bewaffneten Konflikten, bei Katastrophen und in Notlagen (KGSG; SR 520.3) vom 20. Juni 2014.

11 Nationale Strategie zum Schutz kritischer Infrastrukturen 2023. Bereits im Juni 2012 und 2017 hat der Bundesrat Vorgängerstrategien zum Schutz kritischer Infrastrukturen verabschiedet, um die Resilienz (Widerstands-, Anpassungs- und Regenerationsfähigkeit) der Schweiz im Hinblick auf die kritischen Infrastrukturen weiter zu verbessern: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/3159c04b-ffc8-4f4e-b72f-ccba6b6a800e.pdf

12 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken: https://www.ncsc.admin.ch/ncsc/de/home/strategie/strategie-ncss-2018-2022.html

13 Das Strategiepapier ist abrufbar unter: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/732d8094-52f3-49dd-965f-3debd139c8cd.pdf

14 Der Bericht «Auswertung der Umfrage Digitale Kulturgüter» vom Februar 2017 kann beim BABS KGS bezogen werden.

2 Das digitale Kulturerbe der Schweiz

Der Begriff des Kulturerbes umfasst gemäss den UNESCO-Übereinkommen[15] die Gesamtheit der mobilen und immobilen Kulturgüter sowie das immaterielle Kulturerbe.

- Zu den **mobilen (beweglichen)** Kulturgütern zählen Sammlungen in Archiven, Bibliotheken und Museen. In diese Kategorie fällt auch das digitale Kulturerbe in Form digitaler Bestände in den Verwaltungsarchiven und in den genannten Institutionen. Beispiele dafür sind Video- und Netzkunst, Autorinnen- und Autorennachlässe, Archive audiovisueller Medien (AV-Archive), Datensammlungen, Forschungsdaten usw.
- Zu den **immobilen (unbeweglichen)** Kulturgütern zählen Bauten, Denkmäler und archäologische Stätten. Zu diesen Kulturgütern existieren Sicherstellungsdokumentationen in Form von Plänen, Fotografien und Inventaren. Heute wird diese Dokumentation ebenfalls in digitaler Form angelegt.
- Zum **immateriellen Kulturerbe** zählen Traditionen, Brauchtümer, Feste und die darstellenden Künste.[16] Immaterielles Kulturerbe ist flüchtig und kann nicht archiviert, sehr wohl aber dokumentiert werden. Die Dokumentation erfolgt in der Regel in Form audiovisueller oder schriftlicher Aufzeichnungen, welche heute grundsätzlich digital angelegt und archiviert werden.

Diese Übersicht zeigt, dass schützenswerte digitale Objekte in allen drei Bereichen anzutreffen sind. Der Schwerpunkt liegt allerdings bei den mobilen Kulturgütern mit ihren digitalen Sammlungen und Archiven. Solche Sammlungen sind heute sowohl bei öffentlichen als auch privaten Akteuren der Kulturerbepflege anzutreffen. Primär fokussiert der vorliegende IKT-Minimalstandard auf den Schutz der Archive, da diese wegen ihrer rechtssichernden Funktion als besonders kritisch angesehen werden.

15 Die von der Schweiz ratifizierten UNESCO-Übereinkommen sind unter https://www.unesco.ch/culture/conventions/ abrufbar.

16 Art. 2 Übereinkommen zur Bewahrung des immateriellen Kulturerbes (SR 0.440.6), abgeschlossen in Paris am 17. Oktober 2003.

2.1 Übersicht und Stakeholder

In der Schweiz liegt die Bewahrung und Pflege von Kulturgütern auf Grund der traditionell stark föderalistisch geprägten Kulturpolitik nicht in den Händen weniger zentralisierter Gedächtnisinstitutionen, sondern erfolgt durch eine Vielzahl regional, kantonal und national ausgerichteter Organisationen unterschiedlicher Rechtsformen. Die Erhaltung des Kulturerbes in der Schweiz wird nicht zentral gesteuert.

Die Akteure sind entweder öffentlich-rechtlich oder privatrechtlich organisiert und lassen sich den Ebenen Bund (national) – Kanton – Stadt/Gemeinde/Region zuordnen. Zuweilen sind sie auch auf mehreren Ebenen aktiv. Die folgende Grafik zeigt die Vielfältigkeit der Akteure auf:

		Statut juridique		
		De droit public avec mandat public / légal	**Privé** avec mandat public / légal	**Privé** avec mandat propre
Principaux acteurs de financement	**Secteur public**	**Acteur public** • Relevant du droit public • Avec mandat public / légal • Financement principal par les pouvoirs publics (financement partiel par le secteur privé possible)	**Acteur hybride** • Relevant du droit privé • Avec mandat public / légal • Financement principal par les pouvoirs publics (financement partiel par le secteur privé possible)	**Acteur hybride** • Relevant du droit privé • Avec mandat privé / propre • Financement principal par les pouvoirs publics (financement partiel par le secteur privé possible)
	Secteur privé	N/A	N/A	**Privater Akteur** • Relevant du droit privé • Avec mandat privé / propre • Financement principal par le secteur privé (financement partiel par le secteur public possible)

Types principaux :

Public	**Hybride**	**Privé**

Folgende typische Organisationsformen der Akteure sind anzutreffen:

- **Öffentliche Akteure (staatlich):** Behörden, Stiftungen auf den Ebenen Bund, Kanton, Stadt/Gemeinde
- **Hybrider Akteure (privat/öffentlich):** Stiftung, Verein auf den Ebenen national, kantonal, regional
- **Private Akteure:** Stiftung, Verein, Unternehmen auf den Ebenen national, kantonal, regional

Diese Übersicht zeigt, dass sich der Bereich der Kulturerbepflege durch eine ausgesprochene Heterogenität mit Akteuren unterschiedlicher Grösse, Finanzkraft und unterschiedlichem Aktionsradius auszeichnet.

Die meisten dieser Akteure, die sich mit dem Erhalt von Kulturerbe befassen, sind auf Stufe Kantone und Gemeinden angesiedelt. Der Bund unterstützt sie subsidiär und übernimmt koordinative Aufgaben. Auf nationaler Ebene ist das Bundesamt für Kultur (BAK) für Erhaltung und Erschliessung von Kulturgütern und das BABS für den Kulturgüterschutz im Kriegs- und Katastrophenfall zuständig. Auf kantonaler und kommunaler Ebene sind die jeweiligen kantonalen und kommunalen Fachstellen für Kultur, Kulturgüterschutz, Ortsbildschutz, Denkmalpflege und Archäologie zuständig. Zudem setzen sich zahlreiche private Akteure für die Erhaltung und den Schutz von Kulturgütern in der Schweiz ein, diese sind zumeist entweder als privatrechtliche Stiftungen oder Vereine organisiert. Eine ganze Reihe hybrider Akteure haben einen öffentlichen Auftrag, sind aber privatrechtlich organisiert.[17]

17 Edzard Schade, Tobias Wildi (2022). Übersicht / Bestandesaufnahme Kulturerbe der Schweiz. Bericht im Auftrag des Bundesamtes für Kultur.

Der Bund und die Kantone sind verantwortlich für diejenigen Kulturgüter, die sich in ihrem Besitz befinden. Die Verantwortlichkeiten für Erhaltung und Erschliessung der Kulturgüter sind generell auf Stufe Bund im Bundesgesetz über den Natur- und Heimatschutz (NHG)[18] geregelt. Daneben existiert eine weitreichende kantonale Spezialgesetzgebung mit einschlägigen Bestimmungen (bspw. Archivrecht, Denkmalpflege und Archäologie). Die Verantwortung für die Kulturgüter bei bewaffneten Konflikten, bei Katastrophen und in Notlagen wird im entsprechenden Bundesgesetz über den Schutz der Kulturgüter bei bewaffneten Konflikten, bei Katastrophen und in Notlagen (KGSG)[19] geregelt.

2.2 Archive und Archivstruktur in der Schweiz

Der vorliegende IKT-Minimalstandard konzentriert sich primär auf die Archive, da ein Teil der Archive in unserem Land als kritische Infrastruktur[20] eingestuft ist. Diese Archive zählen wegen ihrem Beitrag zur Rechtssicherheit zu den kritischen Infrastrukturen. Der Begriff **Archiv** bezeichnet im vorliegenden Bericht allerdings nicht nur einen Typ von Gedächtnisorganisation, sondern ganz allgemein Funktionen und Systeme zur Speicherung und Erhaltung digitaler Objekte von kulturellem Wert. Die Aufgabe eines Archivs besteht darin, Kulturgüter zu übernehmen und zu garantieren, dass diese über lange Zeiträume hinweg nutzbar bleiben. Dabei sollen die Integrität (Unveränderthеit) und die Authentizität (Vertrauenswürdigkeit) der Unterlagen erhalten bleiben. Auch ein anderer Akteurstyp, wie eine Bibliothek oder ein Museum, kann diese Funktion übernehmen.

Die Schweiz verfügt über eine mehrschichtige öffentliche Archivlandschaft mit dem Bundesarchiv, 26 Staats- und Kantonsarchiven, Stadt- und Gemeindearchiven. Hinzu kommen bedeutende geistliche Archive, Firmen- und Spezialarchive, sowie archivische Bestände in Bibliotheken, Museen und Dokumentationszentren.

In der Schweiz existiert keine zentral gesteuerte Archivstruktur von Bund, Kantonen und Gemeinden. Benutzungsrecht, Aufbewahrungs- und Mitteilungspflicht sind durch keine Verfassungsbestimmung festgelegt. In der Schweiz ist das Archivrecht föderalistisch geregelt: Jeder Kanton hat ein eigenes Archivgesetz oder eine eigene Archivverordnung. Die 26 Staatsarchive stehen somit in einer eigenen historisch-rechtlichen Tradition.

Die Entwicklung im Archivrecht wurde durch die Datenschutzgesetzgebung in den 1990er Jahren massgeblich beeinflusst. Zu regeln waren in erster Linie die Anbietpflicht, das Recht zur Benützung und der Schutz der Persönlichkeit (Datenschutz). Aktuell hat neben dem Bund auch ein Grossteil der Kantone ein Archivgesetz erlassen. Im Grundsatz hat jede Person in der Schweiz ein Recht auf Einsicht in amtliche Akten, soweit nicht überwiegende öffentliche oder private Interessen dem entgegenstehen.

Das Bundesgesetz über die Archivierung (BGA)[21] regelt die Archivierung der Akten des Bundes im Bundesarchiv. Rechtlich, politisch, wirtschaftlich, historisch, sozial oder kulturell wertvolle Unterlagen des Bundes werden archiviert. Das BGA hat jedoch keine direkten Auswirkungen auf die Kantone und die Gemeinden.

18 Bundesgesetz über den Natur- und Heimatschutz (NHG; SR 451) vom 1. Juli 1966.

19 Art. 3 und 5 Bundesgesetz über den Schutz der Kulturgüter bei bewaffneten Konflikten, bei Katastrophen und in Notlagen (KGSG; SR 520.3) vom 20. Juni 2014.

20 Siehe dazu https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html.

21 Bundesgesetz über die Archivierung (Archivierungsgesetz, BGA; SR 152.1) vom 26. Juni 1998.

3 Übersicht über die systemkritischen Systeme und Prozesse

3.1 Systemkritische Archive

Zu den systemkritischen Archiven zählen das Bundesarchiv, die Staatsarchive und ausgewählte Kommunal- und Spezialarchive.

Bundesarchiv (BAR)

Das Schweizerische Bundesarchiv (BAR) hat den gesetzlichen Auftrag[22], relevante Informationen des Bundes dauerhaft verfügbar zu halten. Dadurch legt die Verwaltung Rechenschaft über ihre Tätigkeiten ab und wird in ihrer Arbeit unterstützt. Das BAR unterstützt und berät die Bundesverwaltung beim Erstellen, Organisieren und Verwalten von Daten und Unterlagen. Weiter wählt das BAR mit den Verwaltungsstellen die archivwürdigen Unterlagen aus und garantiert, dass diese langfristig verfügbar und erhalten bleiben. Die Bewertung basiert auf systematischen Kriterien und die Entscheide werden regelmässig publiziert.[23] Das BAR stellt zudem Digitalisate von analogen Archivunterlagen her und stellt diese der Öffentlichkeit zur Verfügung. Bei ausgewählten Themen beteiligt sich das BAR an historischen Forschungen und macht diese einem breiten Publikum zugänglich.

Staatsarchive und Kommunalarchive

Die Staatsarchive und Kommunalarchive erfüllen auf kantonaler, respektive kommunaler Ebene im Wesentlichen die gleichen Aufgaben wie das BAR auf nationaler Ebene. Sie übernehmen, erschliessen und bewahren die archivwürdigen Unterlagen der anbietepflichtigen Behörden und sind verantwortlich für bestandserhaltende Massnahmen und die Zugänglichkeit. Sie leisten einen Beitrag zur Vermittlung historischen Wissens und zur historischen Forschung für die Bedürfnisse des Kantons, der Wissenschaft und der Kultur. Sie bewerten Unterlagen nach ihrer Archivwürdigkeit, beraten Behörden ebenso wie Private und erlassen teilweise auch Weisungen über die Ablieferung der Unterlagen und der Findmittel.

Spezialarchive

Spezialarchive sind Archive, die sich auf bestimmte Themen oder Sachgebiete spezialisiert haben. Sie sammeln, bewahren und stellen Unterlagen zu einem spezifischen Thema zur Verfügung. Spezialarchive können beispielsweise Archive für Kunst, Musik, Geschichte, Naturkunde, Technik, Wissenschaft oder Medizin sein. Sie dienen der Forschung, Bildung und Kultur und sind wichtige Quellen für Wissenschaftler, Historiker, Journalisten, Künstler und die breite Öffentlichkeit. Spezialarchive nehmen eine wichtige gesellschaftliche Funktion ein, weil sie komplementär zur staatlichen Überlieferung das Wirken von zivilgesellschaftlichen und nicht-staatlichen Akteuren dokumentieren. Dazu gehören soziale Bewegungen, politische Parteien, Religionsgemeinschaften, Vereine, Nichtregierungsorganisationen (NGO) etc.

3.2 Leistungen der Archive im Teilsektor Kulturgüter

Die öffentlichen Archive sind wichtige Akteure für die Sicherstellung der Rechtssicherheit in der Schweiz. Sie bewahren Unterlagen auf, die für die Wahrung und Durchsetzung von Rechten und Pflichten von zentraler Bedeutung sind, wie beispielsweise Gesetzestexte, Verträge, Urkunden, Gerichtsurteile oder Belege über Grundeigentumsverhältnisse. Die Archive stellen sicher, dass die Unterlagen im Einklang mit geltenden Gesetzen, Normen und Standards archiviert werden, um die Integrität und Authentizität des Archivguts zu gewährleisten.

Durch die dauerhafte Aufbewahrung von Unterlagen aus der Verwaltung gewährleisten Archive die Nachvollziehbarkeit von Entscheidungen und Handlungen, insbesondere im öffentlichen Bereich. Dies trägt zur Transparenz und Verantwortlichkeit von Regierungs- und Verwaltungsprozessen bei und fördert somit das Vertrauen der Bürgerinnen und Bürger in ihre Institutionen und die Rechtsstaatlichkeit des Landes. Das Bundesarchiv fasst dies in seinem Claim **Keine Demokratie ohne Archive** treffend zusammen.

22 Siehe Bundesgesetz über die Archivierung (BGA, SR 152.1)

23 Die Bewertungsentscheide des BAR sind abrufbar unter: https://www.bar.admin.ch/bar/de/home/informationsmanagement/archivwuerdigkeit/bewertungsentscheide.html

Komplementär zu den öffentlichen Archiven liegt der gesamtgesellschaftliche Nutzen von Spezialarchiven in der Bewahrung und Nutzbarhaltung von mobilem Kulturgut, das nicht direkt im Zusammenhang mit öffentlicher Verwaltung entstanden ist. Spezialarchive fokussieren auf bestimmte Themen und Fachgebiete wie beispielsweise Sozialgeschichte, Wirtschaftsgeschichte oder Frauengeschichte. Spezialarchive haben einen hohen Wert für die kulturelle Identifikationsbildung unseres Landes und fallen deshalb (zumindest teilweise) unter die kritischen Infrastrukturen.

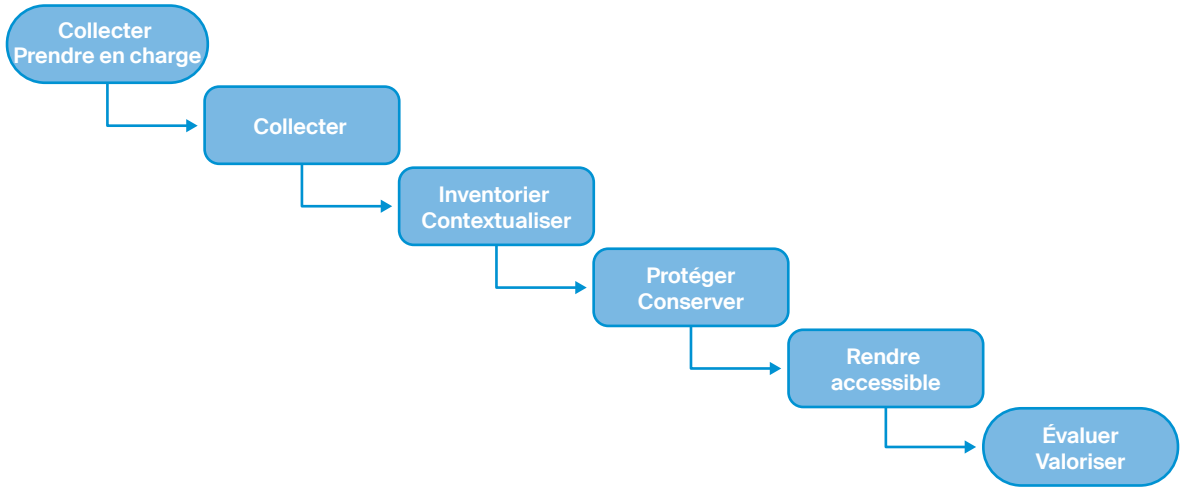
3.3 Übersicht der kritischen Prozesse

Die Geschäftsprozesse grundsätzlich aller Akteure, die sich mit der Bewahrung und Pflege von Kulturerbe beschäftigen, können mit Hilfe des untenstehenden Prozess-Modells beschrieben werden. Für die Benennung der Handlungsfelder werden möglichst allgemeine Begriffe verwendet, je nach Typ des Akteurs (Archiv, Bibliothek, Museum, Dokumentationsstelle, Denkmalpflege) und Kulturgut (mobil, immobil, immateriell) werden die Phasen unterschiedlich benannt. Im Modell zeigt sich, dass der kritische Teilsektor Kulturgüter insbesondere bei der Inventarisierung, der Erforschung und dem Schützen/Erhalten eine hohe Abhängigkeit von IKT-Systemen aufweist.

Im Rahmen dieses IKT-Minimalstandards werden einige Handlungsfelder nicht berücksichtigt, respektive sind sie Teil von anderen Teilsektoren kritischer Infrastrukturen:

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

Die Übernahme, Pflege und Vermittlung digitaler Kulturgüter setzt sich aus folgenden Prozessabschnitten zusammen:



Sammeln
Übernahme und Aufbereitung von Daten und Metadaten, auch Ingest genannt. Wird unterstützt durch workflowbasierte Systeme, die Aufgaben wie Virenprüfung, Validierung, Metadatenextraktion, Dateiformat-Migration, Integrität (Checksummen schreiben) etc. automatisieren und orchestrieren.

Inventarisieren und kontextualisieren
Erschliessen, verzeichnen und ordnen, dokumentieren, katalogisieren. Je nach Typ von Organisation wird diese Aufgabe unterstützt durch Archivinformationssysteme, Bibliothekssysteme oder Sammlungsmanagementsysteme. Zudem werden Kontextwissen und Angaben zu Provenienz, Entstehungs- und Nutzungszusammenhang erhoben.

Schützen und erhalten
Speichern (initialer Vorgang), Sichern (Daueraufgabe: Pflege, Überprüfung des Speichers). Preservation Planning (Erhaltungsplanung), gegebenenfalls Durchführung bestandeserhaltender Massnahmen.

Zugänglichmachen
Recherche ermöglichen (OPAC, digitaler Lesesaal, Webzugang), Ausliefern (Daten ausgeben für die maschinelle Auswertung oder Weiterverwendung über technische Schnittstellen).

Valorisieren
Weitergabe und Reaktualisierung in Form von didaktischer und medialer Vermittlung und durch Praktizieren.

3.4 Gegen welche Gefahren schützen?

Der Bericht des BABS zu Gefährdungen und Resilienz im Teilsektor Kulturgüter aus dem Jahr 2022 analysiert die Risiken, die durch den Ausfall oder Störungen dieser kritischen Infrastruktur verursacht werden. Dabei wurden für die Kulturgüter die folgenden vier Haupt-Gefahrenbereiche ausgemacht:

- Ein **Cyber-Angriff** und/oder Ausfall der IKT beeinträchtigen die Verfügbarkeit der digitalen Bestände einer kulturgüterbewahrenden Organisation voraussichtlich für mehrere Wochen. Darüber hinaus ist auch eine irreversible Zerstörung, eine Entwendung oder eine (un-)absichtliche Veröffentlichung sensibler Informationen möglich. Die Archivbestände können nur wiederhergestellt werden, wenn vorgängig entsprechende Massnahmen getroffen wurden. Bei einer Veröffentlichung vertraulicher Unterlagen kann es zu beachtlichen Reputationsschäden bei Personen und Organisationen kommen. Die Gefahr eines Cyber-Angriffs besteht nicht zuletzt auch deswegen, weil Kulturgüter-Institutionen oft mit knappen Ressourcen auskommen müssen und mit dem schnellen technischen Fortschritt nicht Schritt halten können.
  Bedrohte Prozessabschnitte: Alle Prozessabschnitte sind durch Cyber-Angriffe bedroht.
- Bei den **Naturgefahren** Erdbeben und Hochwasser ist mit erheblichen Bewältigungs- und Wiederherstellungskosten zu rechnen. Die beiden Gefährdungen beeinträchtigen mehrere Kulturgüter in der betroffenen Region. Die Verfügbarkeit der Archivalien wird über Monate bis Jahre beeinträchtigt. Dies führt zu beachtlichen Folgekosten für Bevölkerung, Behörden und Forschung.
  Bedrohte Prozessabschnitte: Insbesondere der Abschnitt «Schützen und Erhalten» ist durch Naturgefahren gefährdet.
- Ein **konventioneller Anschlag** auf ein Archiv oder ein Kulturgut gilt als Angriff auf die Identität des Kantons bzw. des Landes und führt aufgrund der Verunsicherung in Bevölkerung und Wirtschaft zu grossen Schäden. Ein konventioneller Anschlag auf ein Rechenzentrum kann zu erheblichem Datenverlust führen.
  Bedrohte Prozessabschnitte: Insbesondere der Abschnitt «Schützen und Erhalten» ist durch konventionelle Anschläge gefährdet.
- Eine **Pandemie** führt zu einem Ausfall von Spezialpersonal, das für den Betrieb des digitalen Archivs und die Sicherung der Datenbestände notwendig ist. Diese Gefahr akzentuiert sich insbesondere bei kleineren Kulturgüter-Institutionen, wo das entsprechende Spezialwissen auf eine einzige oder einige wenige Personen konzentriert ist.
  Bedrohte Prozessabschnitte: Bei einem Ausfall von Spezialpersonal ist das Prozesswissen in allen Abschnitten gefährdet. Besonders gefährdet ist der Abschnitt «Schützen und Erhalten».

Wie in anderen Teilsektoren stellen auch bei den Kulturgütern die Cyber-Risiken aufgrund der zunehmenden Digitalisierung von Geschäftsprozessen und der Zentralisierung von IT-Infrastrukturen ein beträchtliches Risiko dar. Zudem hat sich in den letzten Jahren die Frequenz solcher Angriffe beträchtlich erhöht. Ein höheres Schadenspotential zeichnet sich auch durch die entstehenden regionalen und überregionalen Verbünde für digitale Archivierung ab, ebenso wie durch die grössere Menge an digitalen Objekten, die in die Archive übernommen werden.

4 Defense in Depth

Um sich vor den oben genannten Gefahren zu schützen, wird hier der sogenannte Defense-in-Depth-Ansatz eingeführt. Dieser basiert auf dem Prinzip, dass es keine Sicherheitsmassnahme gibt, die für sich alleine ausreichend ist, Systeme oder Netzwerke vollständig zu schützen. Stattdessen sollte ein ganzheitlicher Ansatz verfolgt werden, der aus verschiedenen Sicherheitsmassnahmen besteht, die in mehreren Schichten oder Ebenen implementiert werden. Ziel dieses Kapitels ist es, den Defense-in-Depth-Ansatz in der Cybersecurity genauer zu erläutern und zu zeigen, mit welchen Massnahmenkategorien Organisationen diesen Ansatz umsetzen können. Aufbauend auf diesen Grundsätzen werden dann in Kapitel 6 konkrete Bausteine zur Verbesserung der Informationssicherheit genannt.

4.1 Das Defense in Depth-Konzept

Die IKT-Sicherheitsstrategie einer Organisation ist darauf auszurichten, die für ihre Handlungsfelder und Prozesse notwendigen Systeme und Anwendungen zu schützen. Dazu braucht es einen mehrschichtigen Ansatz, welcher als Defense in Depth bekannt ist. Darunter versteht man einen koordinierten Einsatz mehrerer Schutzebenen, nach dem Prinzip, dass es schwieriger ist, ein gestaffeltes, mehrschichtiges Abwehrsystem zu überwinden als eine einzige Barriere. Gleichzeitig werden die Methoden und Vorgehensweisen der potenziellen Angreifer beobachtet, um darauf basierend entsprechende Abwehrdispositive vorzubereiten. Im IKT-Sicherheitsumfeld zielt ein Defense-in-Depth-Konzept darauf ab, Verletzungen der IKT-Sicherheit zu erkennen, darauf zu reagieren, sowie die Konsequenzen der Sicherheitsverletzung zu minimieren, bzw. zu mildern. Defense in Depth verfolgt einen holistischen Ansatz, welcher alle (IKT-)Betriebsmittel gegen beliebige Risiken zu schützen versucht. Die Ressourcen einer Organisation sollten so eingesetzt werden, dass ein effektiver Schutz vor bekannten Risiken sowie eine umfassende Überwachung potenzieller zukünftiger Risiken gewährleistet ist. Dazu gehören Personen, Prozesse, Objekte, Daten und Geräte. Ein Angreifer stellt erst dann eine Bedrohung für ein IKT-System dar, wenn es ihm gelingt, eine existierende Schwachstelle in einem dieser Elemente auszunutzen. Organisationen und Unternehmen sind gehalten, die Massnahmen laufend zu überwachen und, wo nötig, an neue Bedrohungen anzupassen.

Grob können Elemente eines Defense-in-Depth-Ansatzes in organisatorische, technische und physische Massnahmen unterteilt werden.

4.2 Organisatorische Massnahmen (Prozesse)

Zu dieser Gruppe von Massnahmen gehören folgende Bausteine:

- Defense als Daueraufgabe einer Organisation im Rahmen des Sicherheitsmanagements. Regelung der Verantwortlichkeiten innerhalb der Organisation.
- Erstellen eines Risikoprofils, Identifizieren von Sicherheitsrisiken
- Organisatorische und personelle Sicherheitsaspekte
- Standardisierte Konzepte und Vorgehensweisen, etwa betreffend Datenschutz, Löschen und Vernichten von Daten und Datenträgern, Informationsaustausch intern oder mit Dritten
- Bestandsverwaltung der IKT-Betriebsmittel (Asset-Management)
- Übersicht über die archivierten digitalen Objekte
- Betriebliche Sicherheitsaspekte im operativen Betrieb, sowohl bei einem Betrieb im Haus, wie auch beim Betrieb durch Dritte (externes Rechenzentrum, Cloud). In diesen Bereich gehört auch die Trennung von administrativer IT und dem Archivsystem.
- Sicherstellung des Patch- und Schwachstellen-Managements
- Prozesse zur Erstellung und Überprüfung der umgesetzten Sicherheitsmassnahmen, der Detektion von Sicherheitsvorfällen sowie der Incident Management-Prozesse
- Organisation des Business Continuity Managements
- Dokumentation

4.3 Technische Massnahmen (Systeme)

Zu dieser Gruppe von Massnahmen gehören folgende Bausteine:

- Absicherung von Anwendungen und Diensten, unter anderem in den Bereichen Kommunikation, Speicher, sowie Business- und Client-Anwendungen
- Absicherung der einzelnen IT-Systeme wie Server und Desktops
- Absicherung des Netzwerks, Netzwerkverbindungen und -komponenten und der Kommunikation über das Netzwerk. Unterteilung des Netzwerks in Segmente und Sicherheitszonen.
- Absicherung aktiver Netzwerkkomponenten (Firewalls, Router, Switches etc.)

4.4 Physische Massnahmen

Die physische Sicherung von Archivbeständen ist vor allem bei analogem Material ein Thema durch Sicherung von Magazinräumen gegen Feuer, Wasser oder Vandalismus. Bei digitalen Archiven spielen die folgenden Bereiche eine Rolle:

- Zugangssicherung von Serverräumen und Rechenzentren
- Schutz von Serverräumen und Rechenzentren vor Elementargefahren
- Geographisch verteilte Speicher- und Backupsysteme
- Backup auf Offline-, respektive Cold-Speicher. Bei dieser Art von Speicher gilt es – wie bei allen anderen Speicherarten auch – darauf zu achten, dass eine periodische Integritätsprüfung vorgenommen wird.

4.5 Trennung von Büroinformatik und Archivsystem

Ein zentraler Punkt der Defense-in-Depth-Strategie betrifft die systematische und systemische Trennung von administrativer IT und den digitalen Archivbeständen, respektive dem Archivsystem. Ein «Archivsystem» umfasst grundsätzlich die Aufgaben, die im Standard ISO 14721, «Open Archival Information System» (OAIS) beschrieben werden.

Die folgende Tabelle erläutert an Beispielen, wie diese zwei Bereiche nach unterschiedlichen Logiken und Planungsprozessen funktionieren und deshalb unterschiedlich betrachtet werden müssen. Der vorliegende Minimalstandard und insbesondere die Bausteine zur Verbesserung der Informationssicherheit in Kap. 6 beziehen sich primär auf den Schutz der digitalen Kulturgüter und nicht der Büroinformatik.

Sicherheitsthema	IKT (z. B. Büroinformatik)	OAIS, Archivsystem
Normative Grundlagen	Normen und Standards	Nationale und kantonale Archivgesetzgebung, UNESCO-Übereinkommen Kulturgüterschutz, Normen und Standards.
Antivirus	Weit verbreitet. Einfach zu verteilen und zu aktualisieren. Anwender haben die Möglichkeit zur Personalisierung. Antiviren-Schutz kann auf Geräte- oder Unternehmensebene konfiguriert werden.	Viren bilden eine doppelte Herausforderung: Die Server des Archivsystems müssen geschützt werden, zudem muss vermieden werden, dass virenverseuchte Dateien via Ingest ins Langzeitarchiv gelangen.
Sicherheitsaktualisierungen (Update Management)	Klar definiert, unternehmensweit ausgeführt, automatisiert über Fernzugriff.	Lange Vorlauf- und Planungszeit bis zur erfolgreichen Patch-Installation; immer herstellerspezifisch; kann im OAIS (temporär) zu Unterbrüchen führen. Notwendigkeit, das diesbezüglich akzeptable Risiko zu definieren.
Technologielebenszyklus (Technology Support Lifecycle)	2–3 Jahre, mehrere Anbieter, laufende Weiterentwicklung und Upgrades.	10–20 Jahre, typischerweise derselbe Lieferant/Dienstleister über den gesamten Lebenszyklus, Ende des Lebenszyklus verursacht neue Sicherheitsgefährdungen.

Sicherheitsthema	IKT (z. B. Büroinformatik)	OAIS, Archivsystem
Methoden zum Testen und Auditieren (Testing and Audit Methods)	Einsatz von zeitgemässen (ev. automatisierten) Methoden. Die Systeme sind üblicherweise resilient und zuverlässig genug, um Assessments im laufenden Betrieb zu ermöglichen.	Z. B. aufgrund des hohen Grades an Individualentwicklungen sind automatisierte Assessmentmethoden möglicherweise nicht geeignet. Es besteht eine höhere Wahrscheinlichkeit für Fehleranfälligkeit während eines Assessments. Assessments im laufenden Betrieb sind deswegen tendenziell schwieriger.
Change Management	Regulär und in regelmässigem Rhythmus geplant. Abgestimmt auf die Vorgaben der Organisation, zur minimalen/maximalen Einsatzdauer.	Komplexer Prozess mit potenziellen Auswirkungen auf die Geschäftstätigkeit des Archivs. Strategische, individuelle Planung notwendig.
Asset Klassifikation (Asset Classification)	Üblich und jährlich ausgeführt. Ausgaben/Investitionen werden gemäss den Ergebnissen geplant.	In Bezug auf die Archivierung ist v.a. die Datenklassifizierung ein Thema. Ohne Inventar und Kenntnis über die Schutzwürdigkeit der Daten ist die Planung wirksamer Gegenmassnahmen schwierig.
Vorfallreaktion/-analyse (Incident Response and Forensics)	Einfach zu entwickeln und umzusetzen. U.U. regulatorische Vorschriften (Datenschutz) zu beachten.	Fokussiert primär auf die Wiederaufnahme des Systems im Rahmen der Wiederherstellung der Daten und Disaster Recovery.
Physische Sicherheit (Physical Security)	Variiert zwischen schwach (Büro-IT) bis stark (gehärtete Rechenzentren).	Typischerweise sehr gute physische Sicherheit. Bei Staatsarchiven wird das OAIS in der Regel in kantonalen Rechenzentren betrieben.
Sichere Systementwicklung (Secure Software Development)	Integraler Teil des Entwicklungsprozesses.	Frühe digitale Langzeitarchive wurden oft noch als physisch isolierte Systeme konzipiert und bildeten einen Fremdkörper in der IT-Infrastruktur. Moderne OAIS werden auch bez. Sicherheit als integraler Bestandteil der kantonalen IT-Infrastruktur geplant und umgesetzt.
Sicherheitsvorgaben	Allgemeine regulatorische Vorgaben, abhängig vom Sektor (nicht alle Sektoren).	Die Sicherheitsvorgaben der Branchenstandards konzentrieren sich auf den langfristigen Erhalt von Daten und Metadaten und gehen nicht auf breiter gefasste sicherheitsspezifische Themen ein. Hierfür ist die Nutzung allgemeiner Standards wie NIST oder ISO 27001 angezeigt.

Tabelle 1: Unterschiede zwischen Büroinformatik und OAIS

5 NIST Framework Core-Massnahmen

5.1 Übersicht

NIST Framework Core

Ziel des «Cybersecurity Frameworks»[24] des «National Institute of Standards and Technology (USA)» ist es, den Betreibern kritischer Infrastrukturen ein Instrument zur Verfügung zu stellen, mit dem sie proaktiv ihre Resilienz gegenüber Cyber-Risiken erhöhen können. Dabei berücksichtigt es auch das Streben nach Wirtschaftlichkeit und Effizienz sowie Vertraulichkeit und Datenschutz. Das Framework basiert auf einer Auswahl an existierenden Standards, Richtlinien und Best-Practice-Vorgaben und ist technologieneutral.

Das NIST Framework Core ist ein risikobasierter Ansatz, um Cyber-Risiken anzugehen und bewusst zu managen. Es besteht aus fünf Funktionen:

1. Identifizieren (Identify)
2. Schützen (Protect)
3. Erkennen (Detect)
4. Reagieren (Respond)
5. Wiederherstellen (Recover)

Diese fünf Funktionen bilden gemeinsam die Basis für die Sicherheitskonzipierung.

Das NIST Framework kennt vier Implementation Tiers (Implementierungs-Stufen). Diese beschreiben die Ausbaustufe oder das Schutzniveau, welche/s ein Unternehmen umgesetzt hat. Sie reichen von teilweise (partial, Tier 1) bis auf die Gefahr angepasst (adaptive, Tier 4). Zur Festlegung des eigenen angestrebten Schutzniveaus (Tier Level) sollte sich eine Organisation einen Überblick verschaffen über ihre Praktiken zum Risikomanagement, die Bedrohungslage sowie rechtliche und regulatorische Anforderungen, Geschäftsziele und organisatorischen Vorgaben. Nur so wird klar, wogegen sie sich überhaupt schützen will.

Das folgende Kapitel ist nach den fünf Funktionen des NIST Framework Core gegliedert. Die auszuführenden Aufgaben werden wie folgt kategorisiert:

- Die ersten beiden Buchstaben (z. B. ID = Identify) bezeichnen jeweils eine der fünf Funktionen.
- Das zweite Buchstabenpaar bezeichnet die Kategorie (z. B. AM = Asset Management).
- Die Nummer bezeichnet schliesslich die einzelne Aufgabe. Sie sind innerhalb der Kategorie fortlaufend nummeriert. Lesebeispiel: ID.AM-1 entspricht der ersten Aufgabe in der Kategorie Asset Management der Funktion Identify.

Die folgende Tabelle gibt einen Überblick über die Funktionen und Kategorien des NISTFrameworks:

Abkürzung	Deutsch	Englisch
ID	**Identifizieren**	**Identify**
ID.AM	Inventar Management	Asset Management
ID.BE	Geschäftsumfeld	Business Environment
ID.GV	Vorgaben	Governance
ID.RA	Risikoanalyse	Risk Assessment
ID.RM	Risikomanagementstrategie	Risk Management Strategy
ID.SC	Lieferketten-Risikomanagement	Supply Chain Riskmanagement

24 https://www.nist.gov/cyberframework

5 NIST Framework Core-Massnahmen

Abkürzung	Deutsch	Englisch
PR	**Schützen**	**Protect**
PR.AC	Zugriffsmanagement und -steuerung	Access Control
PR.AT	Sensibilisierung und Ausbildung	Awareness and Training
PR.DS	Datensicherheit	Data Security
PR.IP	Informationsschutzrichtlinien	Information Protection Processes and Procedures
PR.MA	Unterhalt	Maintenance
PR.PT	Einsatz von Schutztechnologie	Protective Technology
DE	**Erkennen**	**Detect**
DE.AE	Auffälligkeiten und Vorfälle	Anomalies and Events
DE.CM	Überwachung	Security Continous Monitoring
DE.DP	Detektionsprozess	Detection Processes
RS	**Reagieren**	**Respond**
RS.RP	Reaktionsplanung	Response Planning
RS.CO	Kommunikation	Communications
RS.AN	Analyse	Analysis
RS.MI	Schadensminderung	Mitigation
RS.IM	Verbesserungen	Improvements
RC	**Wiederherstellen**	**Recover**
RC.RP	Wiederherstellungsplan	Recovery Planning
RC.IM	Verbesserungen	Improvements
RC.CO	Kommunikation	Communications

Tabelle 2: Überblick über die NIST-Framework-Funktionen und -Kategorien

Jeder Tabelle mit Aufgaben aus dem NIST Framework Core folgt eine zusätzliche Tabelle mit Referenzen zu anderen internationalen Standards. Die Tabellen referenzieren jeweils auf die Kategorie, z. B. Asset Management. Dies soll Anwendern, die ihre IKT-Sicherheitsaufgaben nach anderen Standards organisieren, die Zuordnung erleichtern. Branchenspezifisch für den Bereich der digitalen Kulturgüter wird jeweils auch auf den Standard ISO 16363 verwiesen, siehe nächster Abschnitt.

NIST Framework und Branchenstandard ISO 16363:2012

Ein wichtiger Branchenstandard zur Beurteilung der Vertrauenswürdigkeit digitaler Archive ist ISO 16363:2012 «Audit and certification of trustworthy digital repositories». Dieser Standard gliedert sich in die folgenden drei Teile:

- Organisatorischer Rahmen
- Management von digitalen Objekten
- Management der Infrastruktur- und Sicherheitsrisiken

Die folgende Tabelle zeigt auf, wie sich Funktionen und Kategorien des NIST Frameworks und ISO 16363 aufeinander beziehen:

5 NIST Framework Core-Massnahmen

Function	NIST Framework Core	ISO 16363
Identify	Asset Management	5.1 Technical Infrastructure Risk Management
	Business Environment	3.3 Procedural Accountability and Preservation Policy Framework
	Governance	3.1 Governance and Organizational Viability 3.3 Procedural Accountability and Preservation Policy Framework 3.4 Financial Sustainability
	Risk Assessment	5.1 Technical Infrastructure Risk Management 5.2 Security Risk Management
	Risk Management Strategy	5.1 Technical Infrastructure Risk Management 5.2 Security Risk Management
	Supply Chain Management	3.5 Contracts, Licenses, and Liabilities
Protect	Identity management and access control	4.6 Access management
	Awareness and Training	3.2 Organizational Structure and Staffing
	Data Security	5.1 Technical Infrastructure Risk Management
	Information Protection	3.3 Procedural Accountability and Preservation Policy Framework 4.1 Ingest: Acquisition of Content 4.2 Ingest: Creation of the AIP 4.5 Information Management
	Maintenance	4.3 Preservation Planning
	Protective Technology	4.4 AIP Preservation
Detect	Anomalies and Events	
	Security continuous monitoring	
	Detection Processes	
Respond	Response Planning	
	Communications	
	Analysis	
	Mitigation	
	Improvements	
Recover	Recovery Planning	
	Improvements	
	Communications	

Tabelle 3: Bezug zwischen NIST-Framework-Kategorien und ISO 16363:2012

Es zeigt sich, dass der Branchenstandard ISO 16363:2012 die NIST-Funktionen Identify und Protect weitgehend abdeckt, und es kann generell festgehalten werden, dass das Bewusstsein für die Wichtigkeit dieser beiden Bereiche in der Branche hoch ist. Ganz klar zeigt sich aber auch, dass die Funktionen Detect, Respond und Recover nicht abgedeckt sind. Das gleiche Fazit ergibt sich bei einem Vergleich der NIST-Kategorien mit dem «nestor-Kriterien, Kriterienkatalog vertrauenswürdige digitale Langzeitarchive»[25], einem zumindest im deutschsprachigen Raum breit rezipierten Hilfsmittel. Dieser Kriterienkatalog deckt die gleichen Bereiche wie ISO 16363:2012 ab.

25 nestor-Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung. (2008). Kriterienkatalog vertrauenswürdige digitale Langzeitarchive. http://nbn-resolving.de/urn:nbn:de:0008-2008021802

5.2 Identifizieren (Identify)

Inventar-Management (Asset Management)
Die Daten, Personen, Geräte, Systeme und Anlagen einer Organisation sind identifiziert, katalogisiert und bewertet. Die Bewertung soll ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse sowie der Risikostrategie der Organisation entsprechen.

Für den Schutz digitaler Kulturgüter ist die Erstellung von Inventaren eine zentrale Massnahme. Inventare bieten nicht nur eine Übersicht und Kontrolle über die zu schützenden Kulturgüter, sie dokumentieren auch deren Herkunft (Provenienz), Entstehungsgeschichte und tragen zur Sicherung der Authentizität bei. Es gibt Inventare sowohl auf übergreifender Ebene, wie beispielsweise das KGS-Inventar, aber auch innerhalb der Institutionen, wie Archivinformationssysteme, Bibliothekskataloge oder Datenbanken für das Sammlungsmanagement.

Bezeichnung	Aufgabe
ID.AM-1	Erarbeiten Sie einen Inventarisierungsprozess, welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar Ihrer IKT-Betriebsmittel (Assets) vorhanden ist.
ID.AM-2	Inventarisieren Sie all Ihre Softwareplattformen, -lizenzen und -applikationen innerhalb Ihrer Organisation.
ID.AM-3	Katalogisieren Sie alle internen Kommunikations- und Datenflüsse.
ID.AM-4	Katalogisieren Sie alle externen IKT-Systeme, die für Ihre Organisation relevant sind.
ID.AM-5	Priorisieren Sie die inventarisierten Ressourcen (Geräte, Anwendungen, Daten) hinsichtlich ihrer Kritikalität.
ID.AM-6	Definieren Sie klare Rollen und Verantwortlichkeiten im Bereich der Cybersecurity.

Tabelle 4: Aufgaben ID.AM

Standard	Referenz
CCS CSC 1	1, 2
COBIT 2019	BAI09.01, BAI09.02, BAI09.05, Dss05.02, APO02.02, APO03.03, APO03.04, PO01.02, Dss06.03
ISO 27001:2013	A.5.2, A.5.3, A.5.9, A.7.9, A.5.12, A.5.14 A.5.32, Clause 7.1, Clause 7.2
NIST-SP-800-53 Rev. 5	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-20, PS-7, PM-2, PM-5, PM-29, SA-17, SC-6, RA-9
BSI 100-2	M 2.225, M 2.393, B 2.10, M 2.193
ISO 16363	5.1

Tabelle 5: Referenzen ID.AM

Geschäftsumfeld (Business Environment)
Die Ziele, Aufgaben und Aktivitäten des Unternehmens sind priorisiert und bewertet. Diese Informationen dienen als Grundlage für die Zuweisung der Verantwortlichkeiten.

Bezeichnung	Aufgabe
ID.BE-1	Die Rolle ihres Unternehmens innerhalb der (kritischen) Versorgungskette ist identifiziert, dokumentiert und kommuniziert.
ID.BE-2	Die Bedeutung der Organisation als kritische Infrastruktur und ihre Position innerhalb des kritischen Sektors sind identifiziert und kommuniziert.
ID.BE-3	Die Ziele, Aufgaben und Aktivitäten innerhalb der Organisation sind bewertet und priorisiert.
ID.BE-4	Abhängigkeiten und kritische Funktionen für die Bereitstellung kritischer Dienste sind festgelegt.
ID.BE-5	Für alle Betriebszustände (z. B. unter Zwang/Angriff, während der Wiederherstellung, im Normalbe- trieb) sind die Anforderungen an die Widerstandsfähigkeit zur Unterstützung der Erbringung kritischer Dienste festgelegt.

Tabelle 6: Aufgaben ID.BE

Standard	Referenz
CCS CSC 1	1, 2
COBIT 2019	BAI09.01, BAI09.02, BAI09.05, Dss05.02, APO02.02, APO03.03, APO03.04, PO01.02, Dss06.03
ISO 27001:2013	A.5.19, A.5.21, A.5.23, A.5.24, A.5.28, A.5.29, A.5.30, A.5.31, A.5.33, A.5.37, A.6.2, A.7.11, A.7.12, A.7.5, A.8.14, A.8.6, A.8.30, Clause 4.1
NIST-SP-800-53 Rev. 5	CP-2, CP-8, PM-8, PM-11, PE-9, PE-11, RA-9, SA-20, SR-1, SR-2, SR-3
BSI 100-2	B 1.11, M 2.256, B 2.2, B 2.12, M 2.214
ISO 16363	3.3

Tabelle 7: Referenzen ID.BE

Vorgaben (Governance)
Die Governance regelt Zuständigkeiten, überwacht und stellt sicher, dass regulatorische, rechtliche und operationelle Anforderungen aus dem Geschäftsumfeld eingehalten werden.

Bezeichnung	Aufgabe
ID.GV-1	Vorgaben zur Informationssicherheit sind im Unternehmen festgelegt und kommuniziert.
ID.GV-2	Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit sind mit internen Rollen (z. B. aus dem Riskmanagement) sowie externen Partnern koordiniert.
ID.GV-3	Stellen Sie sicher, dass Ihre Organisation alle gesetzlichen und regulatorischen Vorgaben im Bereich der Cybersecurity erfüllt, inkl. Vorgaben zum Datenschutz.
ID.GV-4	Stellen Sie sicher, dass Cyberrisiken Teil des unternehmensweiten Risikomanagements sind.

Tabelle 8: Aufgaben ID.GV

Standard	Referenz
COBIT 2019	APO01.03, EDM01.01, EDM01.02, APO13.02, MEA03.01, MEA03.04, Dss04.02
ISO 27001:2013	A.5.1, A.5.19, A.5.30, A5.31, A.6.2, A.6.6, A.8.27, A.8.30, A15.1.1, Clause 6
NIST-SP-800-53 Rev. 5	PM-1, PS-7, PM-9, PM-11
BSI 100-2	M 2.192, M 2.193, M 2.336, B 1.16
ISO 16363	3.1, 3.3, 3.4

Tabelle 9: Referenzen ID.GV

Risikoanalyse (Risk Assessment)
Die Organisation kennt die Auswirkungen von Cyber-Risiken auf die Geschäftstätigkeit, auf Betriebsmittel und Individuen, inklusive Reputationsrisiken.

Bezeichnung	Aufgabe
ID.RA-1	Identifizieren Sie die (technischen) Verwundbarkeiten Ihrer Betriebsmittel und dokumentieren Sie diese.
ID.RA-2	Aktuelle Informationen über Cyber-Bedrohungen werden durch regelmässigen Austausch in Foren und Gremien erhalten.
ID.RA-3	Identifizieren und dokumentieren Sie interne und externe Cyber-Bedrohungen.
ID.RA-4	Identifizieren Sie mögliche Auswirkungen der Cyber-Bedrohungen auf die Geschäftstätigkeit und bewerten Sie ihre Eintretenswahrscheinlichkeit.
ID.RA-5	Bewerten Sie die Risiken für Ihre Organisation, basierend auf den Bedrohungen, Verwundbarkeiten, Auswirkungen (auf die Geschäftstätigkeit) und Eintretenswahrscheinlichkeiten.
ID.RA-6	Definieren Sie mögliche Sofortmassnahmen bei Eintritt eines Risikos und priorisieren Sie diese.

Tabelle 10: Aufgaben ID.RA

Standard	Referenz
COBIT 2019	APO12.01, APO12.02, APO12.03, APO12.04, APO 12.05, APO 13.02, Dss04.02
ISO 27001:2013	A.5.37, A.5.6, A.5.7, A.6.1, A.8.12, A8.14, A.8.16, A,8.2, A.8.3, A.8.7, A.8.8, Clause 6.1.2, Clause 6.1.3, Clause 8, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 5	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, RA-3, PM-12, RA-2, PM-9, PM-11, SA-14
BSI 100-2	M 2.35, M 2.199, M 2.546
ISO 16363	3.4.3 (financial risks), 5.1, 5.2

Tabelle 11: Referenzen ID.RA

Risikomanagementstrategie
(Risk Management Strategy)
Die Prioritäten, Einschränkungen und maximal tragbaren Risiken der Organisation sind festgelegt. Die Beurteilung der operativen Risiken ist auf dieser Grundlage erfolgt.

Bezeichnung	Aufgabe
ID.RM-1	Etablieren Sie Risikomanagementprozesse, bewirtschaften Sie diese aktiv und lassen Sie sich diese von den beteiligten Personen/ Anspruchsgruppen bestätigen.
ID.RM-2	Definieren und kommunizieren Sie die maximal tragbaren Risiken Ihrer Organisation.
ID.RM-3	Stellen Sie sicher, dass die maximal tragbaren Risiken unter Berücksichtigung der Bedeutung Ihrer Organisation als Betreiber einer kritischen Infrastruktur bewertet werden. Berücksichtigen Sie dazu auch die sektorspezifischen Risikoanalysen.

Tabelle 12: Aufgaben ID.RM

Standard	Referenz
COBIT 2019	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06
ISO 27001:2013	A.6.1, A.8.2, A.8.3, Clause 6.1.3, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 5	PM-8, PM-9, PM-11, PM-28, RA-9
ISO 16363	3.4.3 (financial risk management), 5.1, 5.2

Tabelle 13: Referenzen ID.RM

Lieferketten-Risikomanagement (Supply Chain Risk Management)
Die Prioritäten, Einschränkungen und maximalen Risiken, die die Organisation in Zusammenhang mit Lieferantenrisiken zu tragen gewillt ist, sind festgelegt.

Bezeichnung	Aufgabe
ID.SC-1	Prozesse für das Risikomanagement in der Cyber-Supply-Chain sind identifiziert, etabliert, bewertet und verwaltet. Die involvierten Stakeholder sind sich einig über die gewählten Prozesse.
ID.SC-2	Lieferanten und Dienstleister von Informationssystemen, Komponenten und Leistungen werden identifiziert, nach Prioritäten geordnet und anhand eines Risikobewertungsprozesses für die Cyber-Lieferkette bewertet, siehe ID.SC-1
ID.SC-3	Lieferanten und Drittanbieter werden routinemässig durch Audits, Tests oder andere Bewertungsformen geprüft, um sicherzustellen, dass sie ihren vertraglichen Verpflichtungen nachkommen.
ID.SC-4	Etablieren Sie ein Monitoring, um sicherzustellen, dass all Ihre Lieferanten und Dienstleister ihre Verpflichtungen gemäss den Vorgaben erfüllen. Lassen Sie sich dies regelmässig in Audit-Berichten oder technischen Prüfergebnissen bestätigen.
ID.SC-5	Definieren Sie mit Ihren Lieferanten und Dienstleistern Reaktions- und Widerherstellungsprozesse nach Cybersecurity-Vorfällen. Testen Sie diese Prozesse in Übungen.

Tabelle 14: Aufgaben ID.SC

Standard	Referenz
COBIT 2019	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05
ISO 27001:2013	A.5.19, A.5.20, A.5.21, A.5.22, A.5.29, A.6.6, A.8.30, Clause 8.3
NIST-SP-800-53 Rev. 5	SA-9, SA-12, PM-9, RA-2, RA-3, SA-14, SA-15, SA-11, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
BSI	B 1.11, B 1.17, M 2.256, B 1.3
ISO 16363	3.5

Tabelle 15: Referenzen ID.SC

5.3 Schützen (Protect)

Zugriffsmanagement und -steuerung (Access Control)

Der physische und logische Zugriff auf IKT-Betriebsmittel und -Anlagen ist nur für autorisierte Personen, Prozesse und Geräte möglich. Ebenfalls ist der Zugriff nur für zulässige Aktivitäten möglich.

Bezeichnung	Aufgabe
PR.AC-1	Etablieren Sie einen klar definierten Prozess zur Erteilung und Verwaltung von Berechtigungen und Zugangsdaten für Benutzer, Geräte und Prozesse.
PR.AC-2	Stellen Sie sicher, dass nur autorisierte Personen physischen Zugriff auf die IKT-Betriebsmittel haben. Sorgen Sie mit (baulichen) Massnahmen dafür, dass die IKT-Betriebsmittel vor unautorisiertem physischem Zugriff geschützt sind.
PR.AC-3	Etablieren Sie Prozesse zur Verwaltung der Fernzugriffe.
PR.AC-4	Definieren Sie Zugriffsberechtigungen und Autorisierungen unter Berücksichtigung der Grundsätze der geringsten Rechte und der Aufgabentrennung.
PR.AC-5	Stellen Sie sicher, dass die Integrität Ihres Netzwerks geschützt ist. Segregieren Sie Ihr Netzwerk logisch und physisch, wo notwendig und sinnvoll.
PR.AC-6	Stellen Sie sicher, dass digitale Identitäten eindeutig verifizierten Personen oder Prozessen zugeordnet sind.
PR.AC-7	Die Authentifizierung von Benutzern, Geräten und anderen Vermögenswerten (z. B. Ein-Faktor- oder Mehr-Faktor-Authentifizierung) erfolgt entsprechend dem Risiko der Transaktion (z. B. Sicherheits- und Datenschutzrisiken für Einzelpersonen und andere Unternehmensrisiken).

Tabelle 16: Aufgaben PR.AC

Standard	Referenz
COBIT 2019	Dss05.04, Dss06.03, Dss01.04, Dss05.05, APO13.01, Dss01.04, Dss05.03, Dss05.04, Dss05.07, BAI08.03
ISO 27001:2013	A.5.14, A.5.15, A.5.16, A.5.17, A.5.18, A.5.21, A.5.22, A.5.23, A.5.3, A.5.34, A.6.1, A.6.7, A.7.1, A.7.2. A.7.3, A.7.4, A.7.5, A.7.6, A.7.9, A.8.1, A.8.5, A.8.11, A.15, A.8.16, A.8.18, A.8.2, A.8.3, A.8.5, A.8.20, A.8.22, A.8.27, A.8.31
NIST-SP-800-53 Rev. 5	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-10, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-15, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9, SC-7, SC-10, SC-20, PS-3
BSI	M 2.30, M 2.220, M 2.11, M 4.15, M 1.79, M 2.17, B 2.2, B 2.12, B 5.8, B 4.1, M 2.393, M 2.5, B 1.18, M 2.8, M 4.135, B 4.1, M 5.77, M 2.393, M 3.33, M 2.31, M 2.586
ISO 16363	4.6

Tabelle 17: Referenzen PR.AC

Sensibilisierung und Ausbildung (Awareness and Training)
Die regelmässige, angemessene Schulung und Ausbildung der Mitarbeitenden und externen Partner bezüglich aller Belange der Cybersecurity ist sichergestellt. Es ist sichergestellt, dass die Mitarbeitenden und externen Partner ihre sicherheitsrelevanten Aufgaben gemäss den zugehörigen Vorgaben und Prozessen ausführen.

Bezeichnung	Aufgabe
PR.AT-1	Stellen Sie sicher, dass alle Mitarbeitenden bezüglich Cybersecurity informiert und geschult sind.
PR.AT-2	Stellen Sie sicher, dass Anwender mit höheren Berechtigungsstufen sich ihrer Rolle und Verantwortung besonders bewusst sind.
PR.AT-3	Stellen Sie sicher, dass sich alle beteiligten Akteure ausserhalb Ihres Unternehmens (Lieferanten, Kunden, Partner) ihrer Rolle und Verantwortung bewusst sind.
PR.AT-4	Stellen Sie sicher, dass sich alle Führungskräfte ihrer besonderen Rolle und Verantwortung bewusst sind.
PR.AT-5	Stellen Sie sicher, dass die Verantwortlichen für physische Sicherheit und Informationssicherheit sich ihrer besonderen Rolle und Verantwortung bewusst sind.

Tabelle 18: Aufgaben PR.AT

Standard	Referenz
COBIT 2019	APO07.03, BAI05.07, APO07.02, Dss06.03, APO07.03, APO10.04, APO10.05
ISO 27001:2013	A.5.19, A.5.2, A.5.4, A.6.2, A.6.3, A.6.6, A.7.2, A.7.3, A.7.6, A.8.18, A.8.2, A.8.3, A.8.30, Clause 5.1, Clause 5.3
NIST-SP-800-53 Rev. 5	AT-2, AT-3, PM-13, PS-7, SA-9, PM-7
BSI	M 2.193, B 1.13
ISO 16363	3.2

Tabelle 19: Referenzen PR.AT

Datensicherheit (Data Security)
Es ist sichergestellt, dass Informationen, Daten und Datenträger so gemanaged werden, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gemäss der Risikostrategie der Organisation geschützt sind.

Bezeichnung	Aufgabe
PR.DS-1	Stellen Sie sicher, dass gespeicherte Daten geschützt sind (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit).
PR.DS-2	Stellen Sie sicher, dass Daten während der Übertragung (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit) geschützt sind.
PR.DS-3	Stellen Sie sicher, dass für Ihre IKT-Betriebsmittel ein formaler Prozess etabliert ist, welcher die Daten bei Entfernung, Verschiebung oder Ersatz der Betriebsmittel schützt.
PR.DS-4	Stellen Sie sicher, dass Ihre IKT-Betriebsmittel bezüglich der Verfügbarkeit der Daten über ausreichende Kapazitätsreserven verfügen.
PR.DS-5	Stellen Sie sicher, dass adäquate Massnahmen gegen den Abfluss von Daten (Datenlecks) implementiert sind.
PR.DS-6	Etablieren Sie einen Prozess, um Firmware, Betriebssysteme, Anwendungssoftware und Daten hinsichtlich ihrer Integrität zu verifizieren.
PR.DS-7	Stellen Sie eine IT-Umgebung für das Entwickeln und Testen zur Verfügung, welche komplett unabhängig von den produktiven Systemen ist.
PR.DS-8	Etablieren Sie einen Prozess, um die eingesetzte Hardware hinsichtlich ihrer Integrität zu verifizieren.

Tabelle 20: Aufgaben PR.DS

Standard	Referenz
COBIT 2019	APO01.06, BAI02.01, BAI06.01, Dss06.06, BAI09.03, APO13.01, BAI07.04, BAI03.05.4
ISO 27001:2013	A.5.7, A.5.10, A.5.13, A.5.14, A.5.15, A.5.23, A.5.24, A.5.29, A.5.33, A.5.34, A.6.1, A.6.2, A.6.5, A.6.6, A.7.5, A.7.8, A.7.9, A.7.10, A.7.14, A.8.1, A.8.11, A.8.12, A.8.13, A.8.14, A.8.16, A.8.18, A.8.19, A.8.2, A.8.20, A.8.22, A.8.23, A.8.24, A.8.26, A.8.28, A.8.29, A.8.31, A.8.34, A.8.3, A.8.4, A.8.6, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-4, AC-5, AC-6, AU-4, AU-13, CM-2, CM-8, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, CP-2, PE-11, PE-16, PE-19, PE-20, PS-6, SA-10, SC-5, SC-7, SC-8, SC-11, SC-28, SI-4, SI-7, SI-10
BSI	M 2.217, B 4.1, M 2.393, B 5.3, B 5.4, B 5.21, B 5.24, B 1.7, M 2.3, B 1.15, M 5.23, M 3.33, M 2.226, M 3.2, M 3.6, B 1.18, M 2.220, M 2.8, M 4.135, M 4.494, M 5.77, M 2.393, B 5.3, M 3.55, B 5.4, B 5.21, B 5.24, B 1.6, B 1.9, M 2.62, M 2.4
ISO 16363	5.1

Tabelle 21: Referenzen PR.DS

Informationsschutzrichtlinien (Information Protection Processes and Procedures)
Richtlinien zum Schutz von Informationssystemen und Betriebsmitteln liegen vor. Es ist sichergestellt, dass diese Richtlinien im Minimum den Zweck, den Umfang, die Rollen und die Verantwortlichkeiten umfassen sowie die Koordination innerhalb der Organisation regeln. Nutzen Sie diese Richtlinien, um die Informationssysteme und Betriebsmittel zu schützen.

Bezeichnung	Aufgabe
PR.IP-1	Erstellen Sie eine Standardkonfiguration für die Informations- und Kommunikationsinfrastruktur sowie für die industriellen Kontrollsysteme. Stellen Sie sicher, dass diese Standardkonfiguration typische Security-Prinzipien (z. B. N-1-Redundanz, Minimalkonfiguration etc.) einhält.
PR.IP-2	Etablieren Sie einen Lebenszyklus-Prozess für den Einsatz von IKT-Betriebsmitteln.
PR.IP-3	Etablieren Sie einen Prozess zur Kontrolle von Konfigurationsänderungen.
PR.IP-4	Stellen Sie sicher, dass Sicherungen (Backups oder Synchronisation) Ihrer Daten regelmässig durchgeführt, bewirtschaftet und getestet werden (Rückspielbarkeit der Kopien testen).
PR.IP-5	Stellen Sie sicher, dass Sie alle (regulatorischen) Vorgaben und Richtlinien hinsichtlich der physischen Betriebsmittel erfüllen.
PR.IP-6	Stellen Sie sicher, dass Daten gemäss den Vorgaben vernichtet werden.
PR.IP-7	Stellen Sie sicher, dass Ihre Prozesse zur Informationssicherheit kontinuierlich weiterentwickelt und verbessert werden.
PR.IP-8	Tauschen Sie sich bezüglich der Effektivität verschiedener Schutztechnologien mit Ihren Partnern aus.
PR.IP-9	Etablieren Sie Prozesse zur Reaktion auf eingetretene Cyber-Vorfälle (Incident Response-Planning, Business Continuity Management, Incident Recovery, Disaster Recovery).
PR.IP-10	Testen Sie die Reaktions- und Wiederherstellungspläne.
PR.IP-11	Etablieren Sie Aspekte der Cybersecurity bereits in den Personalrekrutierungsprozess (z. B. durch die Etablierung von Background-Checks / Personensicherheitsprüfungen).
PR.IP-12	Entwickeln und implementieren Sie einen Prozess zum Umgang mit erkannten Schwachstellen.

Tabelle 22: Aufgaben PR.IP

Standard	Referenz
COBIT 2019	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI06.01, BAI01.06, APO13.01, Dss01.04, Dss05.05, BAI09.03, APO11.06, Dss04.05, Dss04.03, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
ISO 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.16.1.6, A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3, A.12.6.1, A.18.2.2
NIST-SP-800-53 Rev. 5	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, A-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, CA-7, SI-4, CP-2, IR-8, IR-3, PM-14, RA-3, RA-5, SI-2
BSI	B 1.4, B 1.3, M 2.217, B 1.14, B 1.9, M 2.62, B 5.27, M 4.78, M 2.9, B 1.0, M 2.80, M 2.546, B 5.27, B 5.21, B 5.24
ISO 16363	3.3, 4.1, 4.2, 4.5

Tabelle 23: Referenzen PR.IP

Unterhalt (Maintenance)
Es ist sichergestellt, dass Unterhalts- und Reparaturarbeiten an Komponenten des IKT-Systems und den geltenden Richtlinien und Prozessen durchgeführt werden.

Bezeichnung	Aufgabe
PR.MA-1	Stellen Sie sicher, dass der Betrieb, die Wartung und allfällige Reparaturen an den Betriebsmitteln aufgezeichnet und dokumentiert werden (Logging). Stellen Sie sicher, dass diese zeitnah durchgeführt werden und nur unter Einsatz von geprüften und freigegebenen Mitteln erfolgen.
PR.MA-2	Stellen Sie sicher, dass Unterhaltsarbeiten an Ihren Systemen, die über Fernzugriffe erfolgen, aufgezeichnet und dokumentiert werden. Stellen Sie sicher, dass kein unautorisierter Zugriff möglich ist.

Tabelle 24: Aufgaben PR.MA

Standard	Referenz
COBIT 2019	BAI09.03, Dss05.04, APO11.04, Dss05.02, APO13.01
ISO 27001:2013	A.5.14, A.5.15, A.5.19, A.5.22, A.6.7, A.7.13, A.8.2, A.8.9, A.8.15, A.8.16
NIST-SP-800-53 Rev. 5	MA-1, MA-2, MA-3, MA-4, MA-5, MA-6
BSI	M 2.17, M 2.4, M 2.218, B 1.11, B 1.17, M 2.256
ISO 16363	4.3, 5.2.1

Tabelle 25: Referenzen PR.MA

Einsatz von Schutztechnologie (Protective Technology)
Installieren Sie technische Security-Lösungen, um die Sicherheit und Resilienz Ihrer IKT-Systeme und Ihrer Daten gemäss den Vorgaben und Prozessen zu garantieren.

Bezeichnung	Aufgabe
PR.PT-1	Definieren Sie Vorgaben zu Audits und Log-Aufzeichnungen. Erstellen und prüfen Sie die regelmässigen Logs gemäss den Vorgaben und Richtlinien.
PR.PT-2	Stellen Sie sicher, dass Wechseldatenträger geschützt sind und dass sie nur gemäss den Richtlinien eingesetzt werden.
PR.PT-3	Stellen Sie sicher, dass Ihr System so konfiguriert ist, dass jederzeit eine Minimalfunktionalität gewährleistet wird.
PR.PT-4	Stellen Sie sicher, dass Ihre Kommunikations- und Steuernetzwerke geschützt sind.
PR.PT-5	Stellen Sie sicher, dass Mechanismen (z.B. Ausfallsicherheit, Lastenausgleich, Hot-Swap) implementiert sind, um die Anforderungen an die Ausfallsicherheit in normalen und ungünstigen Situationen zu erfüllen.

Tabelle 26: Aufgaben PR.PT

Standard	Referenz
COBIT 2019	APO11.04, Dss05.02, APO13.01, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, Dss01.05
ISO 27001:2013	A.5.14, A.5.15, A.5.18, A.5.29, A.5.30, A.5.34, A.5.37, A.8.11, A.8.13, A.8.14, A.8.15, A.8.16, A.8.20, A.8.21, A.8.22, A.8.2, A.8.3, A.8.34, A.8.5, A.8.6, A.8.9, A.9.2, A.5.10, A.6.7, A.7.10, A.7.14, A.8.24
NIST-SP-800-53 Rev. 5	AC-3, AC-4, AC-17, AC-18, AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16, CM-7, CP-7, CP-8, CP-11, CP-12, CP-13, MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, PE-11, PL-8, SC-6, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
BSI	B 5.22, M 2.500, M 2.220, M 2.64, M 4.227, M 2.64, B 1.18, B 4.1, M 2.393, B 1.3, B 2.4, B 2.9
ISO 16363	4.4

Tabelle 27: Referenzen PR.PT

5.4 Erkennen (Detect)

Auffälligkeiten und Vorfälle (Anomalies and Events)
Es ist sichergestellt, dass Auffälligkeiten (abnormes Verhalten) und sicherheitsrelevante Ereignisse zeitgerecht erkannt und potenzielle Auswirkungen des Vorfalls verstanden werden.

Bezeichnung	Aufgabe
DE.AE-1	Definieren Sie Standardwerte für zulässige Netzwerkoperationen und die zu erwartenden Datenflüsse für Anwender und Systeme. Managen Sie diese Werte fortlaufend.
DE.AE-2	Stellen Sie sicher, dass entdeckte Cybersecurity-Vorfälle hinsichtlich ihrer Ziele und ihrer Methoden analysiert werden.
DE.AE-3	Stellen Sie sicher, dass Informationen zu Cybersecurity-Vorfällen aus verschiedenen Quellen und Sensoren aggregiert und aufbereitet werden.
DE.AE-4	Bestimmen Sie die Auswirkungen möglicher Ereignisse.
DE.AE-5	Definieren Sie Schwellenwerte für Vorfallswarnungen.

Tabelle 28: Aufgaben DE.AE

Standard	Referenz
COBIT 2019	Dss03.01, APO12.06
ISO 27001:2013	A.5.24, A.5.25, A.5.27, A.5.28, A.5.37, A.8.1, A.8.12, A.8.15, A.8.16, A.8.20, A.8.21, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-4, AU-6, CA-3, CA-7, CM-2, CP-2, SI-4, IR-4, IR-5, IR-8, SC-16, SI-4, RA-3, RA-5
BSI	B 1.8

Tabelle 29: Referenzen DE.AE

Überwachung (Security Continous Monitoring)
Es ist sichergestellt, dass das IKT-System inkl. aller Betriebsmittel in regelmässigen Intervallen überwacht wird, um einerseits Cybersecurity-Vorfälle zu entdecken und anderseits die Effektivität der Schutzmassnahmen überprüfen zu können.

Bezeichnung	Aufgabe
DE.CM-1	Etablieren Sie ein kontinuierliches Netzwerkmonitoring, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-2	Etablieren Sie ein kontinuierliches Monitoring / eine kontinuierliche Überwachung aller physischen Betriebsmittel und Gebäude, um Cybersecurity-Vorfälle entdecken zu können.
DE.CM-3	Die Aktivitäten der Mitarbeitetenden werden überwacht, um potenzielle Cybersicherheitsvorfälle zu erkennen.
DE.CM-4	Stellen Sie sicher, dass Schadsoftware entdeckt werden kann.
DE.CM-5	Stellen Sie sicher, dass Schadsoftware auf Mobilgeräten entdeckt werden kann.
DE.CM-6	Stellen Sie sicher, dass die Aktivitäten von externen Dienstleistern überwacht werden, so dass Cybersecurity-Vorfälle entdeckt werden können.
DE.CM-7	Überwachen Sie Ihr System laufend, um sicherzustellen, dass Aktivitäten/Zugriffe von unberechtigten Personen, Geräten und Software erkannt werden.
DE.CM-8	Führen Sie Verwundbarkeitsscans durch.

Tabelle 30: Aufgaben DE.CM

Standard	Referenz
COBIT 2019	Dss05.01, Dss05.07, APO07.06, BAI03.10
ISO 27001:2013	A.5.14, A.5.15, A.5.18, A.5.19, A.5.21, A.5.23, A.5.7, A.6.7, A.7.1, A.7.2, A.7.4, A.7.8, A.7.9, A.8.1, A.8.11, A.8.12, A.8.15, A.8.16, A.8.19, A.8.2, A.8.20, A.8.21, A.8.23, A.8.28, A.8.3, A.8.30, A.8.5, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-6, PE-20, PS-7, RA-5, SA-4, SA-9, SC-5, SC-7, SC-18, SC-44, SI-3, SI-4, SI-8
BSI	B 5.22, M 2.500, B 1.6, B 2.9, B 1.9, B 5.25, B 1.11, M 2.256, M 2.35

Tabelle 31: Referenzen DE.CM

Detektionsprozess (Detection Processes)
Prozesse und Handlungsanweisungen zur Detektion von Cybersecurity-Vorfällen werden gepflegt, getestet und unterhalten.

Bezeichnung	Aufgabe
DE.DP-1	Definieren Sie eindeutige Rollen und Verantwortlichkeiten, so dass klar ist, wer wofür zuständig ist und wer welche Kompetenzen hat.
DE.DP-2	Stellen Sie sicher, dass die Detektionsprozesse alle Vorgaben und Bedingungen erfüllen.
DE.DP-3	Testen Sie Ihre Detektionsprozesse.
DE.DP-4	Kommunizieren Sie detektierte Vorfälle an die zuständigen Stellen (Lieferanten, Kunden, Partner, Behörden etc.).
DE.DP-5	Verbessern Sie Ihre Detektionsprozesse kontinuierlich.

Tabelle 32: Aufgaben DE.DP

Standard	Referenz
COBIT 2019	Dss05.01, APO13.02, APO12.06, APO11.06, Dss04.05
ISO 27001:2013	A.5.2, A.5.26, A.5.27, A.5.3, A.5.35, A.5.4, A.6.3, A.6.8, A.7.4, A.8.12, A.8.15, A.8.16, A.8.17, A.8.27, A.8.6, A.8.7, A.8.8, A.8.9, Clause 5.3, Clause 7.2, Clause 9.2, Clause 10.1
NIST-SP-800-53 Rev. 5	AC-1, AT-1, AU-1, AU-6, CA-1, CA-2, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-1, PM-14, PS-1, PT-1, RA-1, RA-5, SA-1, SC-1, SI-1, SI-3, SI-4, SR-1, SR-9, SR-10
BSI	M 2.193, M 2.568, B 1.8

Tabelle 33: Referenzen DE.DP

5.5 Reagieren (Respond)

Reaktionsplanung (Response Planning)

Ein Reaktionsplan zur Adressierung erkannter Cybersecurity-Vorfälle ist vorhanden. Es sind die notwendigen Massnahmen ergriffen worden, damit dieser Reaktionsplan im Ereignisfall korrekt und zeitgerecht ausgeführt wird.

Bezeichnung	Aufgabe
RS.RP-1	Stellen Sie sicher, dass der Reaktionsplan während oder nach einem detektierten Cybersecurity-Vorfall korrekt und zeitnah durchgeführt wird.

Tabelle 34: Aufgaben RS.RP

Standard	Referenz
COBIT 2019	BAI01.10
ISO 27001:2013	A.5.26, A.5.28, A.5.29
NIST-SP-800-53 Rev. 5	CP-2, CP-10, IR-4, IR-8
BSI	B 1.8

Tabelle 35: Referenzen RS.RP

Kommunikation (Communications)
Stellen Sie sicher, dass Ihre Reaktionsprozesse mit den internen und externen Anspruchsgruppen abgestimmt sind. Stellen Sie sicher, dass Sie im Ereignisfall Unterstützung durch staatliche Stellen erhalten, falls notwendig und angemessen.

Bezeichnung	Aufgabe
RS.CO-1	Stellen Sie sicher, dass alle Personen ihre Aufgaben bezüglich der Reaktion und der Reihenfolge ihrer Handlungen auf eingetretene Cybersecurity-Vorfälle kennen.
RS.CO-2	Definieren Sie Kriterien für Meldungen und stellen Sie sicher, dass Cybersecurity-Vorfälle gemäss diesen Kriterien gemeldet und bearbeitet werden.
RS.CO-3	Teilen Sie Informationen und Erkenntnisse zu detektierten Cybersecurity-Vorfällen gemäss den definierten Kriterien.
RS.CO-4	Die Koordinierung mit allen Beteiligten und den Anspruchsgruppen erfolgt im Einklang mit den Reaktionsplänen gemäss den vordefinierten Kriterien.
RS.CO-5	Es werden regelmässig freiwillig Informationen mit externen Akteuren ausgetauscht, um das Bewusstsein hinsichtlich der aktuellen Cybersicherheitssituation zu steigern.

Tabelle 36: Aufgaben RS.CO

Standard	Referenz
COBIT 2019	keine
ISO 27001:2013	A.5.2, A.5.24, A.5.26, A.5.3, A.5.30, A.5.37, A.5.5, A.5.6, A.6.3, A.6.8, A.7.4
NIST-SP-800-53 Rev. 5	AU-6, CP-2, CP-3, IR-3, IR-4, IR-6, IR-8, PM-15, SI-5
BSI	B 1.3, B 1.8, M 2.193

Tabelle 37: Referenzen RS.CO

Analyse (Analysis)
Es ist sichergestellt, dass regelmässig Analysen durchgeführt werden, die eine adäquate Reaktion auf Cybersecurity-Vorfälle ermöglichen.

Bezeichnung	Aufgabe
RS.AN-1	Stellen Sie sicher, dass Benachrichtigungen aus Detektionssystemen berücksichtigt und Nachforschungen ausgelöst werden.
RS.AN-2	Stellen Sie sicher, dass die Auswirkungen eines Cybersecurityvorfalls bekannt sind und verstanden werden.
RS.AN-3	Führen Sie nach einem eingetretenen Vorfall forensische Analysen durch.
RS.AN-4	Richten Sie Prozesse ein, um Schwachstellen, die der Organisation aus internen und externen Quellen bekannt werden, zu empfangen, zu analysieren und darauf zu reagieren.

Tabelle 38: Aufgaben RS.AN

Standard	Referenz
COBIT 2019	Dss02.07
ISO 27001:2013	A.5.19, A.5.25, A.5.26, A.5.27, A.5.28, A.5.35, A.5.5, A.5.6, A.6.3, A.8.15, A.8.16, A.10.2
NIST-SP-800-53 Rev. 5	AU-6, AU-7, CA-1, CA-2, CA-7, CP-2, IR-4, IR-5, IR-8, PE-6, PM-4, PM-15, RA-1, RA-3, RA-5, RA-7, SI-4, SI-5, SR-6
BSI	B 5.22, M 2.500, M 2.64, B 1.8

Tabelle 39: Referenzen RS.AN

Schadensminderung (Mitigation)
Handeln Sie so, dass die weitere Ausbreitung eines Cybersecurity-Vorfalls verhindert und der mögliche Schaden verringert werden.

Bezeichnung	Aufgabe
RS.MI-1	Stellen Sie sicher, dass Cybersecurity-Vorfälle eingegrenzt werden können und die weitere Ausbreitung unterbrochen wird.
RS.MI-2	Stellen Sie sicher, dass die Auswirkungen von Cybersecurity-Vorfällen gemindert werden können.
RS.MI-3	Stellen Sie sicher, dass neu identifizierte Verwundbarkeiten reduziert oder als akzeptierte Risiken dokumentiert werden.

Tabelle 40: Aufgaben RS.MI

Standard	Referenz
COBIT 2019	keine
ISO 27001:2013	A.5.26, A.8.23, A.8.8
NIST-SP-800-53 Rev. 5	IR-4, CA-2, CA-7, RA-3, RA-5, RA-7
BSI	B 1.6, B 1.8, M 2.35

Tabelle 41: Referenzen RS.MI

Verbesserungen (Improvements)
Es ist sichergestellt, dass die Reaktionsfähigkeit der Organisation auf Cybersecurity-Vorfälle laufend verbessert wird, indem die Lehren aus vorangegangenen Vorfällen gezogen werden.

Bezeichnung	Aufgabe
RS.IM-1	Stellen Sie sicher, dass Erkenntnisse und Lehren aus vorangegangenen Cybersecurity-Vorfällen in Ihre Reaktionspläne einfliessen.
RS.IM-2	Aktualisieren Sie Ihre Reaktionsstrategien.

Tabelle 42: Aufgaben RS.IM

Standard	Referenz
COBIT 2019	BAI01.13
ISO 27001:2013	A.5.27, A.10.1, Clause 10
NIST-SP-800-53 Rev. 5	CP-2, IR-4, IR-8
BSI	B 1.8

Tabelle 43: Referenzen RS.IM

5.6 Wiederherstellen (Recover)

Wiederherstellungsplanung (Recovery Planning)
Es ist sichergestellt, dass die Wiederherstellungsprozesse so vorbereitet und dann durchgeführt werden können, dass eine zeitnahe Wiederherstellung der Systeme möglich ist.

Bezeichnung	Aufgabe
RC.RP-1	Stellen Sie sicher, dass der Wiederherstellungsplan nach einem eingetretenen Cybersecurity-Vorfall korrekt durchgeführt werden kann.

Tabelle 44: Aufgaben RC.PR

Standard	Referenz
COBIT 2019	Dss02.05, Dss03.04
ISO 27001:2013	A.5.29, A.5.30, A.5.37
NIST-SP-800-53 Rev. 5	CP-10, IR-4, IR-8

Tabelle 45: Referenzen RC.PR

Verbesserungen (Improvements)
Es ist sichergestellt, dass Wiederherstellungsprozesse laufend verbessert werden, indem Lehren aus vorangegangenen Wiederherstellungen gezogen werden.

Bezeichnung	Aufgabe
RC.IM-1	Stellen Sie sicher, dass Erkenntnisse und Lehren aus früheren Cybersecurity-Vorfällen in Ihre Wiederherstellungspläne einfliessen.
RC.IM-2	Aktualisieren Sie Ihre Wiederherstellungsstrategie.

Tabelle 46: Aufgaben RC.IM

Standard	Referenz
COBIT 2019	BAI05.07
ISO 27001:2013	A.5.27, A.10.1, Clause 10
NIST-SP-800-53 Rev. 5	CP-2, IR-4, IR-8

Tabelle 47: Referenzen RC.IM

Kommunikation (Communications)
Koordinieren Sie Ihre Wiederherstellungsaktivitäten mit internen und externen Partnern, z. B. Internet Service Providern, CERT, Behörden, Systemintegratoren etc.

Bezeichnung	Aufgabe
RC.CO-1	Für die Öffentlichkeitsarbeit im Zusammenhang mit dem Cybersecurity-Vorfall besteht ein vorgängiger Kommunikationsplan.
RC.CO-2	Nach einem eingetretenen Cybersecurity-Vorfall arbeitet die Organisation an der Wiederherstellung ihres guten Rufs.
RC.CO-3	Kommunikation der Wiederherstellungsaktivitäten an interne und externe Anspruchsgruppen, insbesondere auch an das Management und die Geschäftsleitung.

Tabelle 48: Aufgaben RC.CO

Standard	Referenz
COBIT 2019	EDM03.02
ISO 27001:2013	A.5.24, A.5.26, A.5.5, A.6.3, Clause 7.4
NIST-SP-800-53 Rev. 5	CP-2, IR-4

Tabelle 49: Referenzen RC.CO

6 Bausteine zur Verbesserung der Informationssicherheit

Das in Kap. 5 verwendete Assessment Framework bietet eine umfassende Unterstützung zur Erhebung und Planung der Verbesserung der Cybersicherheit in Gedächtnisinstitutionen. Grössere Organisationen mit entsprechenden Ressourcen und ausgebildeten Mitarbeitenden (z. B. auf Stufe Kanton oder Bund) werden diese Empfehlung integral umsetzen können. Möglicherweise werden diese Akteure bereits das in diesem Dokument vorgeschlagene oder ein ähnliches Framework verwenden. Die Kulturerbepflege besteht jedoch aus sehr heterogen aufgestellten Akteuren. Einige durchaus kritische Infrastrukturen sind in ihrer Grösse (Anzahl Mitarbeitende und verfügbare Ressourcen für die Informationssicherheit) eher mit einem Klein- oder Kleinstunternehmen vergleichbar. Eine umfassende Umsetzung des Frameworks wird solche Institutionen vor grosse Herausforderungen stellen. Um diesem Umstand Rechnung zu tragen und trotzdem eine wirkungsvolle Defense-in-Depth-Strategie umzusetzen, wird empfohlen, dass sich kleinere Institutionen auf die im folgenden Kapitel genannten zentralen Bausteine zur Verbesserung der Informationssicherheit konzentrieren.

Eine kleine Institution hat in der Regel wenig umfangreiche digitale Sammlungsbestände, wenig Publikumsverkehr und beschränkte personelle und finanzielle Ressourcen. Man könnte sich darunter das Kommunalarchiv einer Kleinstadt oder ein Spezialarchiv vorstellen, das Bestände und Nachlässe zu einem bestimmten Themengebiet sammelt. In diesem Kapitel soll dargelegt werden, wie eine derartige Institution mit minimalen Ressourcen die zentralen Punkte einer Defense-in-Depth-Strategie (Kap. 4) umsetzen kann. Kleine Gedächtnisinstitutionen sind oft in grössere IT-Organisationen eingebunden (bspw. städtische, kantonale, universitäre IT-Dienste). Hier ist alles daranzusetzen, Synergien zu nutzen und sich in die grössere, übergeordnete Einheit einzugliedern.

Nicht jede Institution muss also zwingend alle Massnahmen umsetzen, sondern nur diejenigen, die nötig sind, um die eigenen kritischen Prozesse und IT-Systeme zu schützen. Eine Sammlung von Massnahmen und Empfehlungen zur Erhöhung der Informationssicherheit bilden die IT-Grundschutz-Bausteine des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Deutschland.[26] Die Bausteine sind in die drei Kategorien unterteilt, die bereits in Kap. 4, Defense in Depth, beschrieben wurden:

- Organisatorische Massnahmen (Sicherheitsmanagement, Organisation und Prozesse)
- Technische Massnahmen (Systeme)
- Physische Massnahmen (Gebäude, Räume)

Das NIST-Framework sagt, **was** gemacht werden muss, im Sinne eines Assessments. Das folgende Kapitel mit den IT-Grundschutz-Bausteinen liefert Ideen, **wie** es gemacht werden kann.

26 Die Bausteine sind abrufbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

6.1 Sicherheitsmanagement

Ziel dieses Bausteins ist es, ein umfassendes Sicherheitsmanagement in der Institution zu etablieren, um Informationssicherheit als kontinuierlichen Prozess zu verankern.

Zu den Massnahmen des Bausteins gehören die Definition von Sicherheitszielen und -anforderungen, die Einführung von Sicherheitsprozessen, die Festlegung von Verantwortlichkeiten und Zuständigkeiten, die Schulung und Sensibilisierung der Mitarbeitenden sowie die Einrichtung von Notfallplänen.

Mit diesem Baustein soll in der Organisation eine Kultur zur systematischen und kontinuierlichen Verbesserung der Informationssicherheit etabliert werden. Durch ein umfassendes Sicherheitsmanagement sollen Risiken minimiert und ein angemessenes Sicherheitsniveau für IT-Systeme und Daten erreicht werden.

Standard	Referenz
BSI IT-G 2023	ISMS.1

6.2 Prozess-Bausteine

Organisation

Das Ziel des Bausteins **Organisation** ist es, eine effektive und effiziente Organisation zu schaffen, die in der Lage ist, Risiken im Bereich der IT-Sicherheit proaktiv zu erkennen und zu minimieren.

Zu den Massnahmen des Bausteins gehören unter anderem die Festlegung von Organisationsstrukturen und -prozessen im Hinblick auf die Informationssicherheit, die Zuweisung von Zuständigkeiten und Verantwortlichkeiten sowie die Erstellung von Sicherheitsrichtlinien. Da die meisten Archive in eine übergeordnete behördliche IT-Struktur eingebettet sind, ist die Klärung der fachlichen und technischen Zuständigkeiten von hoher Bedeutung.

Der Baustein **Organisation** legt auch Wert auf eine enge Zusammenarbeit und Kommunikation zwischen den verschiedenen Abteilungen und Mitarbeitenden eines Unternehmens oder einer Behörde. Ziel ist es, ein gemeinsames Verständnis für die Bedeutung von Informationssicherheit zu schaffen und alle Beteiligten in die Sicherheitsprozesse einzubeziehen. Dies ist, wie gesagt, von hoher Bedeutung bei der Abstimmung der fachlichen und technischen Bedürfnisse zwischen Archiv und IT-Dienst.

Mit der Umsetzung der Massnahmen des Bausteins **Organisation** kann eine Institution ihre Organisationsform so weiterentwickeln, dass Informationssicherheit zu einem integralen Bestandteil des Geschäftsbetriebs wird.

Standard	Referenz
BSI IT-G 2023	ORP.1

Personal

Dieser Baustein befasst sich mit dem Thema Informationssicherheit im Zusammenhang mit den Mitarbeitenden einer Institution. Das Ziel ist es, sicherzustellen, dass die Mitarbeitenden ausreichend sensibilisiert und geschult sind, um zur Sicherheit der IT-Systeme und Daten beizutragen.

Zu den Massnahmen des Bausteins gehören unter anderem die Festlegung von Sicherheitsanforderungen für Mitarbeitende, die Sensibilisierung und Schulung in Bezug auf Informationssicherheit und die Einhaltung von Sicherheitsvorschriften. Es sind Vorkehrungen zu treffen, um den Know-how-Verlust bei einem Personalausfall z. B. im Fall einer Pandemie zu minimieren. Zudem gilt es, die Qualifikation ausgewählter Mitarbeitender im Bereich der Informationssicherheit gezielt weiterzuentwickeln.

Eine weitere Massnahme für Institutionen mit sensiblen und sicherheitsrelevanten Daten bildet die Durchführung einer Personensicherheitsprüfung bei der Einstellung von neuem Personal.[27]

Standard	Referenz
BSI IT-G 2023	ORP.2

27 Beim Bund ist dafür die Fachstelle Personensicherheitsprüfungen (PSP) im VBS zuständig: https://www.vbs.admin.ch/de/sicherheit/integrale-sicherheit/personensicherheitspruefung.html

Sensibilisierung und Schulung
Dieser Baustein hat das Ziel, Mitarbeitende von Unternehmen und Behörden im Bereich Informationssicherheit zu sensibilisieren und zu schulen. Nur so können sie ihre Aufgaben im Hinblick auf Informationssicherheit angemessen wahrnehmen und zur Minimierung von Risiken beitragen.

Zu den Massnahmen des Bausteins gehören unter anderem die Definition von Schulungs- und Sensibilisierungszielen, die Auswahl von geeigneten Schulungsformaten und -methoden sowie die Planung und Durchführung von Schulungen und Sensibilisierungsmassnahmen.

Die Schulungs- und Sensibilisierungsmassnahmen sollten auf die spezifischen Bedürfnisse und Anforderungen der Mitarbeitenden abgestimmt sein, auch in Bezug auf die spezifischen Gefahren, denen eine Institution ausgesetzt ist. Die Massnahmen sollen regelmässig durchgeführt werden, insbesondere auch mit neu eintretenden Mitarbeitenden, die Führungsebene ist ebenfalls einzubeziehen, um die Bedeutung von Informationssicherheit in der Institution zu betonen.

Standard	Referenz
BSI IT-G 2023	ORP.3

Identitäts- und Berechtigungsmanagement
Dieser Baustein befasst sich mit dem Management von Identitäten und Berechtigungen innerhalb einer Institution. Das Ziel des Bausteins ist es, sicherzustellen, dass nur berechtigte Personen Zugriff auf IT-Systeme und Daten haben.

Zu den Massnahmen des Bausteins gehören unter anderem die Festlegung von Rollen und Berechtigungen für Mitarbeitende, die Implementierung von Zugriffskontrollmechanismen, die Überprüfung von Identitäten und Berechtigungen sowie die Durchführung von Zugriffskontrollaudits. Eine zentrale Massnahme ist die Trennung des Identitäts- und Berechtigungsmanagements von Büroinformatik und digitalem Archiv.

Der Baustein «Identitäts- und Berechtigungsmanagement» umfasst weiter die angemessene Verwaltung von Zugangsdaten und die Nutzung der Zwei-Faktor-Authentifizierung, um die Sicherheit von Zugängen zu erhöhen.

Standard	Referenz
BSI IT-G 2023	ORP.4

Compliance Management (Anforderungsmanagement)
Dieser Baustein befasst sich mit der Einhaltung von gesetzlichen, regulatorischen und vertraglichen Anforderungen im Bereich der Informationssicherheit. Das Ziel des Bausteins ist es, sicherzustellen, dass die Institution die relevanten Anforderungen erfüllt und somit rechtliche und regulatorische Risiken minimiert.

Zu den Massnahmen des Bausteins gehören unter anderem die Identifizierung und Überwachung von gesetzlichen, regulatorischen und vertraglichen Anforderungen, die Integration von Compliance-Anforderungen in das IT-Sicherheitskonzept, die Dokumentation von Compliance-Anforderungen sowie die Durchführung von Compliance-Checks. Zu diesen Anforderungen gehören insbesondere auch die archivischen Normen und Standards sowie Best Practices.

Der Baustein **Compliance Management** umfasst auch eine regelmässige Überprüfung der Einhaltung von Anforderungen sowie die Einbindung von Compliance-Aspekten in die Planung und Durchführung von IT-Projekten. Hier finden sich Schnittstellen zum kritischen Teilsektor Verwaltung, indem bei der Planung und Einführung neuer Systeme bereits die Archivierung berücksichtigt werden muss.

Standard	Referenz
BSI IT-G 2023	ORP.5

Datenschutz
Dieser Baustein befasst sich mit dem Schutz personenbezogener Daten innerhalb einer Organisation. Das Ziel des Bausteins ist es, sicherzustellen, dass personenbezogene Daten entsprechend den gesetzlichen Anforderungen verarbeitet und geschützt werden.

Zu den Massnahmen des Bausteins gehören unter anderem die Durchführung von Datenschutz-Folgeabschätzungen, die Implementierung von technischen und organisatorischen Massnahmen zum Schutz personenbezogener Daten, die Schulung von Mitarbeitenden im Umgang mit personenbezogenen Daten sowie die Überprüfung der Einhaltung von Datenschutzanforderungen.

Der Baustein **Datenschutz** fokussiert auf die Einhaltung von Datenschutzprinzipien wie Datensparsamkeit, Zweckbindung und Transparenz sowie die Sicherstellung der Rechte betroffener Personen, wie z. B. das Recht auf Auskunft, Löschung oder Berichtigung.

Durch die Umsetzung der Massnahmen dieses Bausteins stellt eine Institution sicher, dass personenbezogene Daten entsprechend den gesetzlichen Anforderungen verarbeitet und geschützt werden, was das Vertrauen von abliefernden Stellen wie auch von Benutzerinnen und Benutzern stärkt und rechtliche Risiken minimiert.

Standard	Referenz
BSI IT-G 2023	CON.2

Datensicherungskonzept
Dieser Baustein befasst sich mit der Erstellung und Umsetzung eines Konzepts zur Sicherung der Archivdaten und der Metadaten. Das Ziel des Bausteins ist es, die Verfügbarkeit und Integrität dieser Daten zu gewährleisten und das Risiko von Datenverlusten zu minimieren.

Zu den Massnahmen des Bausteins gehören unter anderem die Erstellung eines Datensicherungskonzepts, das die Häufigkeit und Art der Datensicherungen, die Speicherung der Sicherungskopien und die Überprüfung der Sicherungen umfasst. Darüber hinaus werden auch die Wiederherstellung und Integritätsprüfung von Daten nach einem Datenverlust sowie die Implementierung von Sicherungsverfahren geregelt.

Für digitales Archivgut ist ein Datensicherungskonzept zu wählen, das auf mindestens drei unabhängigen Kopien beruht, die synchronisiert werden. Bei einem Fehler auf einer der Kopien werden die Daten von einer anderen Kopie zurückgespielt. Bei der Konzipierung zu berücksichtigen sind insbesondere:

- Geographisch verteilte Speichersysteme,
- Nutzung unterschiedlicher Brandabschnitte für Produktiv- und Backupsysteme
- Offline-Speicher
- Speichersysteme mit Self-Healing-Mechanismen, um allfällige Fehler zu korrigieren
- Die manuelle statt automatische Auslösung von Backup- und Replikationsprozessen, um die Ausbreitung von Ransomware zu verhindern.

Der Baustein **Datensicherungskonzept** umfasst zudem die Identifikation und Bewertung von Risiken im Zusammenhang mit der Datensicherung sowie die Anpassung des Datensicherungskonzepts an die sich ändernden Anforderungen und Risiken im Laufe der Zeit.

Standard	Referenz
BSI IT-G 2023	CON.3

Löschen und Vernichten

Es gibt durchaus Fälle, wo Archivdaten gelöscht werden müssen. Beispielsweise, weil ihre Formate obsolet geworden sind und sie in neue Formate überführt wurden oder weil eine Nachbewertung ergeben hat, dass sie nicht mehr als archivtauglich eingestuft werden.

Dieser Baustein befasst sich mit der sicheren und endgültigen Löschung von Daten und der Vernichtung von Datenträgern einer Institution. Das Ziel des Bausteins ist es, sicherzustellen, dass Archivdaten (insb. vertrauliche oder personenbezogene) nicht in falsche Hände geraten und unautorisiert verwendet werden können.

Zu den Massnahmen des Bausteins gehören unter anderem die Erstellung von Richtlinien und Verfahren für die sichere Löschung von Daten, die genaue Identifizierung der Daten und Metadaten, die gelöscht werden müssen, und die Festlegung von Verfahren zur Vernichtung von Datenträgern. Dazu gehört die Dokumentation des Löschvorgangs. Darüber hinaus werden auch die Schulung von Mitarbeitenden im Umgang mit der sicheren Löschung von Daten sowie die Überprüfung der Einhaltung von Lösch- und Vernichtungsverfahren behandelt.

Standard	Referenz
BSI IT-G 2023	CON.6

Eigener Betrieb

Dieser Baustein befasst sich mit der Absicherung von IT-Systemen und -Infrastrukturen, die von einer Institution selbst betrieben werden. Das Ziel des Bausteins ist es, die Verfügbarkeit, Integrität und Vertraulichkeit der Daten und IT-Systeme zu gewährleisten und somit das Risiko von Störungen und Angriffen zu minimieren.

Zu den Massnahmen des Bausteins gehören unter anderem die Erstellung von IT-Sicherheitsrichtlinien, die Implementierung von Zugangs- und Berechtigungskontrollen, die Überwachung von IT-Systemen und Netzwerken sowie die Durchführung von regelmässigen IT-Sicherheitsaudits. Darüber hinaus werden die physische Absicherung von Serverräumen und die Notfallplanung behandelt. Der Baustein umfasst die Planung dieser Massnahmen und verweist auf die notwendigen System-Bausteine.

Der Baustein **Eigener Betrieb** berücksichtigt auch neue Entwicklungen und Technologien sowie die Anpassung der IT-Sicherheitsmassnahmen an sich ändernde Risiken und Bedrohungen.

Kleine, manchmal auf Freiwilligenarbeit basierende Institutionen fallen oft in diese Kategorie. Die Anforderungen an den eigenen Betrieb sind hoch und diesen Institutionen wird empfohlen, den «Betrieb durch Dritte (Cloud)» vertieft zu prüfen.

Standard	Referenz
BSI IT-G 2023	OPS.1

Betrieb durch Dritte (Cloud)

Dieser Baustein befasst sich mit der Absicherung von IT-Systemen und -Infrastrukturen, die von einem externen Dienstleister betrieben werden. Das Ziel des Bausteins ist es, die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und IT-Systemen zu gewährleisten und somit das Risiko von Störungen und Angriffen zu minimieren.

Zu den Massnahmen des Bausteins gehören unter anderem die Festlegung von Sicherheitsanforderungen an den Dienstleister, die Durchführung von Sicherheitsüberprüfungen des Dienstleisters, die Festlegung von Verantwortlichkeiten und Pflichten im Rahmen des Outsourcing-Vertrags sowie die Durchführung von regelmässigen IT-Sicherheitsaudits. Darüber hinaus werden auch die Überwachung von Service-Level-Agreements (SLAs) und die Notfallplanung behandelt.

Ein wichtiger Aspekt dieses Bausteins bildet die Auswahl geeigneter Dienstleister und die Berücksichtigung von Sicherheitsaspekten bei der Vertragsgestaltung.

Standard	Referenz
BSI IT-G 2023	OPS.2

6.3 System-Bausteine

Server

Dieser Baustein befasst sich mit der Absicherung von Servern und Serverumgebungen in IT-Systemen. Das Ziel des Bausteins ist es, die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und IT-Systemen zu gewährleisten und somit das Risiko von Störungen und Angriffen zu minimieren.

Zu den Massnahmen des Bausteins gehören unter anderem die physische Absicherung von Serverräumen, die Implementierung von Zugangs- und Berechtigungskontrollen, die Verwendung von verschlüsselter Kommunikation, die Durchführung von regelmässigen Sicherheitsupdates sowie die Implementierung von Backup- und Recovery-Mechanismen. Darüber hinaus werden auch die Überwachung von Servern und die Notfallplanung behandelt.

Ein wichtiger Aspekt dieses Bausteins bildet die Berücksichtigung neuer Entwicklungen und Technologien sowie die Anpassung der IT-Sicherheitsmassnahmen an sich ändernde Risiken und Bedrohungen.

Standard	Referenz
BSI IT-G 2023	SYS.1

Speicherlösungen

Dieser Baustein befasst sich mit der Absicherung von Speicherlösungen in IT-Systemen. Das Ziel des Bausteins ist es, die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und IT-Systemen zu gewährleisten und somit das Risiko von Störungen und Angriffen zu minimieren. Dieser Baustein setzt im Wesentlichen das Datensicherungskonzept des Bausteins CON.3 um.

Zu den Massnahmen des Bausteins gehören unter anderem die physische Absicherung von Speichersystemen, die Implementierung von Zugangs- und Berechtigungskontrollen, die Verwendung von verschlüsselter Kommunikation, die Durchführung von regelmässigen Sicherheitsupdates sowie die Implementierung von Synchronisations- und Backup-Mechanismen.

Durch die Umsetzung der Massnahmen soll sichergestellt werden, dass Speicherlösungen angemessen geschützt sind und Ausfälle oder Angriffe schnell erkannt werden können und darauf reagiert werden kann.

Standard	Referenz
BSI IT-G 2023	SYS.1.8

Desktop-Systeme

Dieser Baustein befasst sich mit der Absicherung von Desktopsystemen in IT-Umgebungen. Das Ziel des Bausteins ist es, die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und IT-Systemen zu gewährleisten und somit das Risiko von Störungen und Angriffen zu minimieren.

Zu den Massnahmen des Bausteins gehören unter anderem die physische Absicherung von Arbeitsplätzen, die Implementierung von Zugangs- und Berechtigungskontrollen, die Verwendung von verschlüsselter Kommunikation, die Durchführung von regelmässigen Sicherheitsupdates sowie die Implementierung von Backup- und Recovery-Mechanismen. Es ist darauf zu achten, dass das Betriebssystem und die installierte Software aktuell gehalten werden und ein ebenfalls aktuell gehaltener Virenschutz installiert ist. Veraltete oder nicht mehr benötigte Software ist zu deinstallieren. Darüber hinaus werden auch die Überwachung von Desktopsystemen und die Notfallplanung behandelt.

Ein wichtiger Aspekt dieses Bausteins bildet die Berücksichtigung von neuen Entwicklungen und Technologien sowie die Anpassung der IT-Sicherheitsmassnahmen an sich ändernde Risiken und Bedrohungen.

Standard	Referenz
BSI IT-G 2023	SYS.2

Wechseldatenträger
Dieser Baustein befasst sich mit der sicheren Nutzung von USB-Sticks, externen Festplatten und anderen mobilen Speichermedien in IT-Systemen. Das Ziel des Bausteins ist es, das Risiko von Datenverlust, Diebstahl oder Manipulation durch den Einsatz von Wechseldatenträgern zu minimieren und die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

Zu den Massnahmen des Bausteins gehören die Definition von Richtlinien zur Nutzung von Wechseldatenträgern, die Implementierung von Mechanismen zur Erkennung und Abwehr von Schadsoftware auf Wechseldatenträgern sowie die Schulung und Sensibilisierung von Mitarbeitenden zur sicheren Nutzung von Wechseldatenträgern. Ein Verlust oder Diebstahl eines Datenträgers kann vorkommen, durch geeignete Massnahmen wie Verschlüsselung sind die Auswirkungen jedoch minimal. Wechseldatenträger können Defekte erleiden. Sie können als Teil einer Backup-Strategie eingesetzt werden, aber nie als einzige Kopie der Daten.

Wichtig im Baustein **Wechseldatenträger** ist die Überwachung und Protokollierung von Aktivitäten im Zusammenhang mit Wechseldatenträgern sowie die regelmässige Überprüfung und Aktualisierung der Sicherheitsmassnahmen.

Standard	Referenz
BSI IT-G 2023	SYS 4.5

Netzwerk
Dieser Baustein befasst sich mit der Sicherheit von Netzwerken in IT-Systemen. Das Ziel des Bausteins ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten in Netzwerken zu gewährleisten und das Risiko von Angriffen und Datenverlusten zu minimieren.

Zu den Massnahmen des Bausteins gehören unter anderem die Definition von Richtlinien und Prozessen zur Netzwerkarchitektur, Netzwerksegmentierung und Netzwerkverwaltung. Weitere Massnahmen umfassen die Implementierung von Firewalls, Intrusion-Detection-Systemen und Verschlüsselung von Netzwerkverbindungen. Eine zentrale Massnahme ist die Trennung von Büroinformatik und digitalem Archiv auf Netzwerkebene. Zudem sind auf der Firewall nicht nur für den eingehenden, sondern auch für den ausgehenden Datenfluss Regeln zu erstellen, um unkontrollierten Datenabfluss zu verhindern. Grundsätzlich sind sämtliche Netzwerkverbindungen zwischen den Bereichen und einzelnen Rechnern zu verschlüsseln. Bei der Übertragung von Archivdaten ist die transaktionale Integrität sicherzustellen, indem Checksummen vor- und nach der Übertragung miteinander verglichen werden.

Der Baustein **Netzwerk** legt auch Wert auf die Überwachung und Protokollierung von Netzwerkaktivitäten, die regelmässige Überprüfung und Aktualisierung von Netzwerkgeräten und -systemen sowie die Schulung und Sensibilisierung von Mitarbeitenden zur sicheren Nutzung von Netzwerken.

Standard	Referenz
BSI IT-G 2023	NET.1

6.4 Physische Bausteine

Allgemeines Gebäude
Dieser Baustein befasst sich mit den physischen Aspekten der Sicherheit von Gebäuden, in denen IT-Systeme betrieben werden. Ziel des Bausteins ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von IT-Systemen und Daten durch geeignete Sicherheitsmassnahmen am Gebäude zu gewährleisten. Unbefugter physischer Zutritt zu sensiblen Orten wie Serverräumen oder Rechenzentren soll verhindert werden.

Zu den Massnahmen des Bausteins gehören die Sicherung von Eingängen, Fenstern und anderen Zugängen zum Gebäude, die Kontrolle von Besuchern und Gästen sowie die Installation von Sicherheitsanlagen wie Überwachungskameras, Alarmanlagen und Zugangskontrollsystemen.

Zu diesem Baustein gehören auch die Verfügbarkeit von Notfallplänen und die Schulung von Mitarbeitenden zur Handhabung von Notfällen wie Bränden, Überschwemmungen oder anderen Naturkatastrophen.

Standard	Referenz
BSI IT-G 2023	INF.1

Rechenzentrum, Serverraum
Dieser Baustein befasst sich mit den spezifischen Anforderungen an die Sicherheit von Rechenzentren und Serverräumen, in denen IT-Systeme betrieben werden. Ziel des Bausteins ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von IT-Systemen und Daten durch geeignete Sicherheitsmassnahmen zu gewährleisten.

Zu den Massnahmen des Bausteins gehören die Sicherung von Zugängen zu Rechenzentren und Serverräumen, die Kontrolle von Besuchern und Gästen sowie die Installation von Sicherheitsanlagen wie Überwachungskameras, Alarmanlagen und Zugangskontrollsystemen. Zu diesem Baustein gehören auch eine geeignete Klimatisierung und Feuerlöschsysteme im Rechenzentrum oder Serverraum, um Schäden durch Überhitzung oder Brände zu vermeiden.

Neben diesen allgemeinen Massnahmen gelten spezifische Massnahmen für digitales Archivgut. Es sind vom Archivgut mindestens drei Kopien an mindestens zwei Standorten zu halten. Die Standorte liegen in verschiedenen Erdbebenzonen. Werden nur zwei Standorte für die drei Kopien gewählt, so muss die an einem Standort doppelt vorhandene Hardware in verschiedenen Feuerschutzzonen liegen.

Darüber hinaus umfasst der Baustein **Rechenzentrum, Serverraum** auch Empfehlungen für die Gestaltung der technischen Infrastruktur, wie etwa die Stromversorgung, Netzwerkarchitektur und Server-Infrastruktur.

Standard	Referenz
BSI IT-G 2023	INF.2

Datenträgerarchiv
Dieser Baustein befasst sich mit der sicheren Aufbewahrung und Archivierung von Datenträgern in IT-Systemen. Das Ziel des Bausteins ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten auf Datenträgern zu gewährleisten, um das Risiko von Verlust, Diebstahl oder Manipulation zu minimieren. Die Massnahmen der beiden Bausteine Wechseldatenträger und Datenträgerarchiv schützen die Daten auch bei Stromausfall und bilden im Rahmen des Disaster Recovery ein wichtiges Sicherheitsnetz.

Zu den Massnahmen des Bausteins gehören unter anderem die Definition von Prozessen zur physischen und logischen Zugangskontrolle zu den Räumlichkeiten des Datenträgerarchivs, die Implementierung von Sicherheitsmassnahmen für die Datenträger selbst wie Verschlüsselung und Labeling sowie die Definition von Verfahren für die sichere Vernichtung von Datenträgern am Ende ihrer Lebensdauer.

Der Baustein **Datenträgerarchiv** umfasst auch die regelmässige Überprüfung und Aktualisierung der Sicherheitsmassnahmen sowie die Schulung und Sensibilisierung des Personals, das Zugang zum Datenträgerarchiv hat.

Standard	Referenz
BSI IT-G 2023	INF.6

7 Literatur

BSI
Bundesamt für Sicherheit in der Informationstechnik (Deutschland). BSI 100-2.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.html

BSI IT-G (2023)
Bundesamt für Sicherheit in der Informationstechnik (Deutschland). IT-Grundschutz-Bausteine.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

CoreTrustSeal
Die CoreTrustSeal-Stiftung bietet eine Zertifizierung digitaler Archive und Repositorien auf der Grundlage der «Core Trustworthy Data Repositories Requirements» an.
https://www.coretrustseal.org/why-certification/requirements/

COBIT
Control Objectives for Information and related Technology (COBIT).
https://www.isaca.org/resources/cobit

ENISA
EU Agency for Cybersecurity. Good Practice Guide on National Cyber Security Strategies.
https://www.enisa.europa.eu/topics/national-cyber-security-strategies

ISO 14721
Open archival information system (OAIS) — Reference model
https://www.iso.org/standard/57284.html

Identischer Text:
https://public.ccsds.org/pubs/650x0m2.pdf

ISO 16363
Audit and certification of trustworthy digital repositories.
https://www.iso.org/standard/56510.html
Identischer Text:
https://public.ccsds.org/pubs/652x0m1.pdf

ISO 2700x
Die International Organization for Standardization (ISO) veröffentlicht rund ein Dutzend sich gegenseitig ergänzende Standards zur Informationssicherheit, welche als «2700x-Familie» bezeichnet werden. Der bekannteste Standard darunter ist der Standard ISO 27001. Er spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation.
https://www.iso.org/standard/73906.html

Leitfaden Schutz kritische Infrastrukturen
Bundesamt für Bevölkerungsschutz (Hg.) (2018).
https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/27228b5a-2d7c-4c17-9df6-42e105197465.pdf

nestor-Kriterienkatalog
nestor-Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung (2008). Kriterienkatalog vertrauenswürdige digitale Langzeitarchive.
https://d-nb.info/1000083241/34

NIST Framework
National Institute of Standards and Technology (USA). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST-SP-800-53 Rev. 5
National Institute of Standards and Technology (USA). Security and Privacy Controls for Information Systems and Organizations, Revision 5.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

8 Glossar und Abkürzungsverzeichnis

Asset	In diesem Zusammenhang: Daten, Personen, Geräte, Systeme und Anlagen einer Organisation.
Authentizität	Im Bereich der digitalen Archivierung wird der Begriff so verwendet, dass eine Datei tatsächlich das beinhaltet, was sie vorgibt zu sein. Wird weitgehend synonym mit Vertrauenswürdigkeit verwendet.
AV-Archiv	Archiv audiovisueller Medien
BABS	Bundesamt für Bevölkerungsschutz
Backup	Ein Backup ist eine Kopie von Daten, die erstellt wird, um im Falle eines Datenverlustes oder einer Datenbeschädigung eine Wiederherstellung zu ermöglichen. Diese Kopien werden regelmäßig angefertigt und an einem sicheren Ort gespeichert.
BAK	Bundesamt für Kultur
BAR	Schweizerisches Bundesarchiv
Bitstream Preservation	Bezeichnet den Prozess des langfristigen Erhalts und der Wiederherstellung von digitalen Bitströmen, um die Integrität und Wiedergabefähigkeit von digitalen Inhalten zu gewährleisten.
BGA	Bundesgesetz über die Archivierung (Archivierungsgesetz, BGA; SR 152.1) vom 26. Juni 1998
BWL	Bundesamt für wirtschaftliche Landesversorgung
Compliance	Compliance ist die betriebswirtschaftliche und rechtswissenschaftliche Umschreibung für die Regeltreue von Unternehmen, also die Einhaltung von Gesetzen, Richtlinien und freiwilligen Kodizes.
Cybersicherheit	Cybersicherheit bezieht sich auf den Schutz von Computern, Netzwerken und Daten vor Angriffen aus dem Internet oder anderen Netzwerken. Sie umfasst Massnahmen zur Abwehr von Cyberbedrohungen (--> Gefährdungen), um digitale Infrastrukturen zu sichern.
Data at Rest	Data at Rest bezieht sich auf gespeicherte oder ruhende Daten, die sich auf physischen oder elektronischen Speichermedien befinden.
Data in Transit	Data in Transit bezieht sich auf Daten während der Übertragung in Netzwerken oder Kommunikationskanälen.
Defense in Depth	Ein Cybersicherheitsansatz, der mehrere Schichten von Sicherheitsmassnahmen implementiert, um Systeme und Daten zu schützen. Ziel ist es, redundante Sicherheitsbarrieren zu schaffen, so dass ein einzelnes Versagen einer Schutzmassnahme nicht zur Kompromittierung der gesamten Sicherheit führt.
DH Lab	Digital Humanities Lab, Universität Basel

8 Glossar und Abkürzungsverzeichnis

Digitales Kulturgut	Der Begriff des Kulturguts, so wie er im Art. 1 des Haager Abkommens zum Schutz des Kulturguts im bewaffneten Konflikt von 1954 festgehalten ist, dient als zentrales Kriterium für die Auswahl der digitalen Objekte. Unter digitalem Kulturgut verstehen wir sowohl digital erstellte (born digital), wie auch digitalisierte Objekte (Retrodigitalisierung). Der Begriff „Sammlung" in diesem Zusammenhang versteht sich hier analog zu dem in Archiven, Bibliotheken und Museen. Es handelt sich hierbei um eine Sammlung von digitalen Archivalien. Diese digital erstellten Kulturgüter umfassen neben digitalen Archivbeständen (z. B. digitalisierten Tageszeitungen und audiovisuellen Sendungsarchiven einer Kantonsbibliothek) auch digitale Kunst (z. B. digital erstellte Sammlung von Fotografien in einem Museum), digitale Kunstreproduktion und Forschungsdaten (Fundstellendokumentation eines kantonalen archäologischen Dienstes in Form von Drohnenaufnahmen oder 3D-Modellen), digital erstellte Sicherstellungsdokumentationen usw.
DIMAG	Digitales Magazin. Verbundslösung für digitale Archivierung in öffentlichen Archiven.
DTI	Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei
Eintrittswahrscheinlichkeit	Als Eintrittswahrscheinlichkeit wird das geschätzte bzw. auf Statistikwerten beruhende Eintreten eines Ereignisses innerhalb einer bestimmten Zeitspanne bezeichnet (z. B. innerhalb von 10 Jahren).
EKKGS	Eidgenössische Kommission für Kulturgüterschutz
Gefährdung	Als Gefährdung wird eine konkrete Gefahr bezeichnet, die für ein konkretes Schutzgut besteht. Die Gefährdung entspricht daher einem potentiellen Ereignis oder einer potentiellen Entwicklung mit möglichen Auswirkungen für ein Schutzgut.
Informationssicherheit	Informationssicherheit schützt Informationen und Informationssysteme vor unbefugtem Zugriff, Verwendung, Offenlegung, Veränderung oder Zerstörung. Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.
GEVER	(elektronische) Geschäftsverwaltung
IKT	Informations- und Kommunikationstechnologie
Integrität	Nachweis, dass Daten korrekt und unverändert sind. Ein wichtiges Hilfsmittel dazu sind Checksummen.
Immaterielles Kulturerbe	Das immaterielle Kulturerbe umfasst (nach Definition der UNESCO-Konvention) «Praktiken, Darbietungen, Ausdrucksweisen, Kenntnisse und Fähigkeiten – sowie die damit verbundenen Instrumente, Objekte, Artefakte und Kulturräume [...], die Gemeinschaften, Gruppen und gegebenenfalls Individuen als Bestandteil ihres Kulturerbes ansehen.» Die UNESCO-Konvention benennt fünf Bereiche: A.mündlich überlieferte Traditionen und Ausdrucksweisen, einschliesslich der Sprache als Träger immateriellen Kulturerbes; B. darstellende Künste; C. gesellschaftliche Praktiken, Rituale und Feste; D. Wissen und Praktiken im Umgang mit der Natur und dem Universum; E. Fachwissen über traditionelle Handwerkstechniken.
KGS	Kulturgüterschutz
KGSG	Bundesgesetz über den Schutz der Kulturgüter bei bewaffneten Konflikten, bei Katastrophen und in Notlagen vom 20. Juni 2014 (KGSG; SR 520.3)
Kritische Infrastrukturen	Als kritische Infrastrukturen werden Prozesse, Systeme und Einrichtungen bezeichnet, die essentiell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.

8 Glossar und Abkürzungsverzeichnis

Kritische Prozesse	Im Rahmen des Schutzes kritischer Infrastrukturen wird unter kritischem Prozess ein Prozess verstanden, welcher für die Funktionsfähigkeit der kritischen Infrastruktur existenziell wichtig ist und bei dessen Ausfall die Bevölkerung und deren Lebensgrundlagen in einem schweren Masse betroffen wären.
Kulturerbe	Das Kulturerbe wird als Oberbegriff genutzt und umfasst die Gesamtheit der immobilen und mobilen Kulturgüter sowie das immaterielle Kulturerbe.
Kulturgut	Das «Haager Abkommen für den Schutz von Kulturgut bei bewaffneten Konflikten» von 1954 definiert den Begriff wie folgt: «bewegliches oder unbewegliches Gut, das für das kulturelle Erbe der Völker von grosser Bedeutung ist, wie z. B. Bau-, Kunst- oder geschichtliche Denkmäler kirchlicher oder weltlicher Art, archäologische Stätten, Gruppen von Bauten, die als Ganzes von historischem oder künstlerischem Interesse sind, Kunstwerke, Manuskripte, Bücher und andere Gegenstände von künstlerischem, historischem oder archäologischem Interesse sowie wissenschaftliche Sammlungen und bedeutende Sammlungen von Büchern, von Archivalien oder von Reproduktionen des oben umschriebenen Kulturguts;»[29] Hervorzuheben ist die Unterteilung in mobile (bewegliche) und immobile (unbewegliche) Kulturgüter.
LVG	Landesversorgungsgesetz
NB	Schweizerische Nationalbibliothek (NB)
NCSC	Nationales Zentrum für Cybersicherheit
NHG	Bundesgesetz über den Natur- und Heimatschutz (SR 451) vom 1. Juli 1966
NIST	Das National Institute of Standards and Technology (NIST, Nationales Institut für Standards und Technologie) ist eine Bundesbehörde der Vereinigten Staaten und hat ein Cyberrisiko-Management-Framework herausgegeben.
OAIS	Open Archival Information System, ISO 14721. Referenzmodell für digitale Archive
OPAC	Open Public Access Catalog
Preservation Planning	Das Preservation Planning (deutsch: Erhaltungsplanung) in der Langzeitarchivierung verfolgt das Ziel, die archivierten Inhalte langfristig verfügbar zu halten.
Records Management	Records Management umfasst die systematische Verwaltung von Aufzeichnungen und Informationen über deren gesamten Lebenszyklus hinweg, von der Erstellung oder Erfassung, über die Ablage, Aufbewahrung, bis zur endgültigen Archivierung oder Vernichtung.
Resilienz	Die Resilienz beschreibt die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und die Funktionsfähigkeit möglichst zu erhalten respektive wieder zu erlangen. Die Resilienz setzt sich aus vier Bestandteilen zusammen: 1) die Robustheit der Systeme (z. B. → kritische Infrastrukturen, Staat, Wirtschaft und Gesellschaft) an sich; 2) die Verfügbarkeit von Redundanzen; 3) die Fähigkeit, wirksame Hilfsmassnahmen zu mobilisieren; 4) die Schnelligkeit und Effizienz der Hilfsmassnahmen.
Risiko	Das Risiko ist ein Mass für die Grösse einer → Gefährdung und beinhaltet die → Eintrittswahrscheinlichkeit und das → Schadensausmass eines unerwünschten Ereignisses.

29 Art. 1 Haager Abkommen für den Schutz von Kulturgut bei bewaffneten Konflikten (SR 0.520.3), abgeschlossen in Den Haag am 14. Mai 1954.

Schadensausmass	Als Schadensausmass werden die geschätzten Auswirkungen auf die Bevölkerung und deren Lebensgrundlagen bezeichnet, die durch den Ausfall eines oder mehrerer → kritischen/kritischer Prozesse/s bei Eintritt der → Gefährdung entstehen. Es besteht aus der Summe des Schadens zum Zeitpunkt des Eintritts eines Ereignisses und des Schadens, der während der ganzen Wiederherstellungszeit entstehen kann.
Schutz kritischer Infrastrukturen	Der Schutz kritischer Infrastrukturen umfasst Massnahmen, die die → Eintrittswahrscheinlichkeit und/oder das → Schadensausmass einer Störung, eines Ausfalls oder einer Zerstörung von → kritischen Infrastrukturen reduzieren beziehungsweise die Ausfallzeit minimieren.
SR	Schweizer Recht
Synchronisation	Synchronisation ist das Verfahren, bei dem Daten zwischen zwei oder mehr Systemen in Einklang gebracht werden, um sicherzustellen, dass alle beteiligten Systeme denselben Datenstand haben. Dies erfolgt entweder in Echtzeit oder in regelmässigen Intervallen, um Konsistenz und Aktualität der Daten zu gewährleisten.
Teilsektor	Die → kritischen Infrastrukturen in der Schweiz wurden in 28 Teilsektoren unterteilt. Diese Teilsektoren umfassen die verschiedenen Branchen, Industrien, Wirtschaftssektoren und sonstige wirtschaftliche Unterteilungen. Folgende Teilsektoren existieren im Bereich der kritischen Infrastrukturen in der Schweiz: Abfälle, Abwasser, Armee, Ärztliche Betreuung und Spitäler, Diplomatische Vertretungen und Sitze internationaler Organisationen, Banken, Blaulichtorganisationen, Chemie- und Heilmittelindustrie, Erdgasversorgung, Erdölversorgung, Forschung und Lehre, Informationstechnologien, Kulturgüter, Labors, Lebensmittelversorgung, Luftverkehr, Maschinen-, Elektro- und Metallindustrie, Medien, Parlament – Regierung – Justiz – Verwaltung, Postverkehr, Schienenverkehr, Schiffsverkehr, Strassenverkehr, Stromversorgung, Telekommunikation, Versicherungen, Wasserversorgung und Zivilschutz.

Für weiterführende Glossare und Begriffsdefinitionen siehe auch:

- Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013. https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/6e53cc48-dfd0-496e-8516-54bd2f227e76.pdf

- Glossar im Leitfaden Schutz kritischer Infrastrukturen, 2018. https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/27228b5a-2d7c-4c17-9df6-42e105197465.pdf

8 Glossar und Abkürzungsverzeichnis

Autoren/-innen und Fachexperten/-innen der Erstausgabe

Name	Vorname	Organisation	Funktion
Wildi	Tobias	EKKGS Fachhochschule Graubünden	PL / Hauptautor
Fornaro	Peter	Digital Humanities Lab, Universität Basel	Review
Müller	Stefanie	Fachhochschule Graubünden	Review

Chronologie

Datum	Kurzbeschreibung
2018	Beschluss EKKGS zur Erarbeitung eines IKT-Minimalstandards
Jan – Jul 2023	Erarbeitung 1. Entwurf
Aug – Nov 2023	Konsultation Ämter und Kantone
Dez 2023	Überarbeitung und 2.Entwurf
Jan – März 2024	Konsultation Kantone
April – Juli 2024	Überarbeitung und definitive Version
November 2024	Abnahme durch EKKGS
Aug – Dez 2024	Übersetzung und Veröffentlichung

Lizenz

Das vorliegende Dokument wurde unter einer Creative Commons BY Lizenz erstellt. Gültig ist die Version 4.0. Sie dürfen:

- Teilen: das Material in jeglichem Format oder Medium vervielfältigen und weiterverbreiten.
- Bearbeiten: das Material verändern und darauf aufbauen, und zwar für beliebige Zwecke, auch kommerziell.

Voraussetzung dafür ist die Einhaltung der unten beschriebenen Bedingungen:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.
  Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technischen Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Es werden keine Garantien gegeben und auch keine Gewähr geleistet. Für allfällige Schäden, die sich aus der Anwendung des vorliegenden Standards ergeben, wird jede Haftung abgelehnt. Die Lizenz verschafft Ihnen möglicherweise nicht alle Erlaubnisse, die Sie für die jeweilige Nutzung brauchen. Es können beispielsweise andere Rechte wie Persönlichkeits- und Datenschutzrechte zu beachten sein, die Ihre Nutzung des Materials entsprechend beschränken.

Bitte zitieren Sie das Dokument wie folgt:

Bundesamt für Bevölkerungsschutz BABS;
«Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) digitaler Kulturgüter», Bern, 2024.

Rechtsverbindlich ist einzig der vollständige Lizenztext. Dieser kann online eingesehen werden unter:
https://creativecommons.org/licenses/by/4.0/legalcode.de