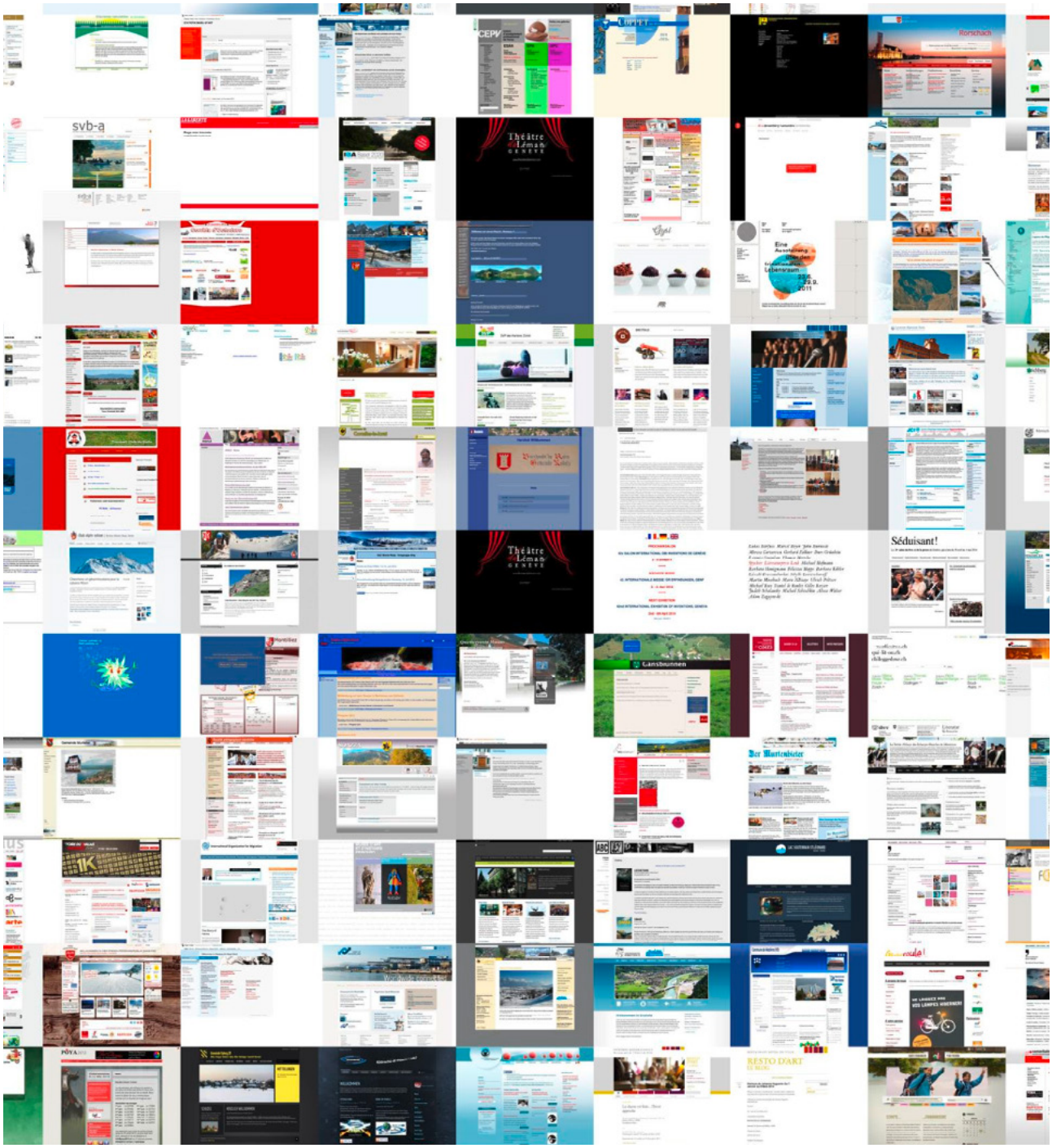
Minimum standard for the information and communication technology (ICT) security of digital cultural property



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Office for Civil Protection FOCP

As at 19.02.2025

Cover picture:
Web Archive Switzerland, Swiss National Library (NL). Landing page as a collage.
https://www.e-helvetica.nb.admin.ch/collage/

Author:
Tobias Wildi, University of Applied Sciences of Graubünden, docuteam AG

Publisher:
Federal Office for Civil Protection (FOCP)
Civil Protection and Training Unit
Civil Protection and Training Fundamentals Section
Protection of Cultural Property Group 2024
kulturgueterschutz@babs.admin.ch
www.kgs.admin.ch

All links were last checked on 8 July 2024.

Foreword

In its Digital Switzerland Strategy[1], the Federal Council emphasises its desire to make the most of the opportunities offered by Switzerland's digital transformation. Today, operating archives without the use of information and communication technologies (ICT) is almost inconceivable. The Minimum ICT Standard presented here focuses on the security of digital long-term archiving, in particular on securing 'data at rest' for digital cultural property (see glossary), and is intended as a recommendation for organisations in the field of cultural heritage management.

The Federal Commission for the Protection of Cultural Property (FCPCP) is working together with the Federal Office for Civil Protection (FOCP) and external experts to increase the resilience of digital cultural property. This standard also depends on the support of the institutions concerned, however. This first version of the Minimum ICT Standard will therefore be regularly updated and, where necessary, made more specific and expanded.

With the increasing digitalisation of the administration (electronic records and process management GEVER, specialist applications), the volume of digital archive records has increased significantly in recent years. At the same time, the digitalisation of business processes entails new risks that must be addressed. The risk of cyberattacks on IT infrastructure affects not only government offices, but also operators of critical infrastructure and organisations in the field of cultural heritage management (museums, libraries). Nowadays, the preservation of analogue cultural heritage also uses digital data such as inventory and catalogue databases, digitised representations, and electronic documentation on preservation and archaeological finds.

Digital cultural property becomes particularly important when physical originals of cultural property are no longer available or when they are 'born digital', i.e. produced directly in digital form. The long-term archiving of these digital objects raises the key question of what 'long-term' really means. The aim is to keep data usable across many generations of processor architectures, operating systems and file formats. The necessary measures go beyond simple data protection and backups. Archival thinking operates over periods of decades and centuries. The following sectoral standard takes this special challenge into account.

1 See https://digital.swiss/de/strategie/strategie.html

Summary

This Minimum ICT Standard serves as a recommendation and guideline for improving ICT resilience in organisations involved in the management and preservation of digital cultural property. It is aimed primarily at operators of critical infrastructures, in particular the managers and ICT officers of those operators. However, the minimum standard should in principle be useful for any organisation involved in the preservation of cultural property. The goal is to recognise risks and reduce them to an acceptable level.

The Minimum ICT Standard provides a framework focusing on the long-term security of digital cultural property and the aim of achieving an appropriate level of security against cyberattacks and other dangers. After an incident, normal operation should be restored as quickly as possible. For planning purposes, the NIST Cybersecurity Framework[2] is used, with which organisations can systematically assess their risks and determine the effectiveness of their measures. The core recommendation is to implement a defence-in-depth strategy, i.e. a multi-level strategy against cyberthreats.

The minimum standard also outlines specific modules for improving resilience, relating to the categories of security management, processes, systems and physical security. These modules help both large and small cultural heritage organisations.

The structure of this standard is based on the model of the general Minimum ICT Standard – 2023[3] of the Federal Office for National Economic Supply (FONES).

2 Standard of the US National Institute of Standards and Technology: https://www.nist.gov/cyberframework.

3 The document is available at: https://www.bwl.admin.ch/bwl/en/home/bereiche/ikt/ikt_minimalstandard.html.

Contents

1 Background and objectives

Many items of cultural property are now created in digital form and are archived and used accordingly. Digital cultural heritage includes, for example, public archives (such as the Federal Archives and state archives), collections in libraries (including image archives, authors' estates, research data) and museums with their video and digital artworks or photo collections. The use and protection of this cultural property require digital tools such as preservation documentation, inventories, catalogues and digital representations.

Managing digital cultural property is essential, and in Switzerland some of this property is part of systemically critical infrastructures. These infrastructures are indispensable for the functioning of society and the maintenance of order and security. Archives make an important contribution to legal certainty by preserving important documents such as legal texts, contracts, deeds and court judgments.

This report focuses on the situation of archives, but the principles also apply to other institutions that are responsible for digital cultural heritage, including libraries, museums, monument preservation sites, archaeological services and documentation centres, regardless of their legal organisation. Like all sectors, digital cultural property is exposed to a wide range of risks. The Minimum ICT Standard aims to help cultural heritage organisations to make their IT infrastructure more resilient. This standard follows a risk-based approach that enables different levels of protection, adapted to the specific needs of organisations.

The Minimum ICT Standard provides an overview of critical systems and processes to be protected in section 3 and introduces the concept of 'defence in depth' – a multi-level defence against cyberthreats – in section 4. Section 5 then introduces the NIST Cybersecurity Framework, a risk-based approach to analysing and managing cyber risks. Finally, specific security measures are proposed in section 6, divided into the categories of security management, process modules, system modules and physical modules.

1.1 Background and overview

In 2021, the Federal Office for Civil Protection (FOCP) updated its report on resilience in the cultural heritage critical sub-sector[4]. That report discusses the strong dependence of today's archiving and library processes on information and communication technologies (ICT). Against this backdrop, cyberattacks on archives and libraries represent a risk that extends far beyond the institutions affected and that can have repercussions for society as a whole.

In future, a significant increase in digital holdings in archives and libraries is to be expected, along with increasingly centralised data storage. This can be seen in the establishment of archive networks and cooperations, and in the joint operation of data centres, such as DIMAG[5] Switzerland, a consortium of several cantons. These digital networks offer advantages through synergies in the operation of high-maintenance infrastructures, but they also harbour an increased risk in the event of targeted cyberattacks or ICT system failures.

4 Internal report. A summary factsheet is available at: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/21/1209e420-c585-43d9-b9bb-297d4e7b87b2.pdf

5 DIMAG (short for Digital Magazine) is a package of software solutions for the digital long-term archiving of official documents. DIMAG was developed by the archive administrations of the German federal states of Baden-Württemberg and Hesse and the Free State of Bavaria. The cantons of Solothurn, Schaffhausen and Aargau founded the DIMAG Switzerland archive network in 2019. See also: https://www.eoperations.ch/service/geschaeftsstelle-dimag/.

A detailed risk analysis carried out in the aforementioned report examines the potential for archive processes to be impaired by targeted cyberattacks on state archives or cantonal ICT systems. The report makes it clear that such attacks and the resulting failures of the ICT infrastructure can impair the accessibility and availability of archive holdings and archive networks for longer periods. Additionally, there is a risk of irreversible destruction or theft, as well as intentional or unintentional publication of sensitive information.

1.2 Scope and boundaries

The responsibility for protecting digital cultural property lies in principle with the preserving institutions, which act on the basis of a legal or voluntary mandate. Wherever the functioning of critical infrastructures can be affected, the state also has a responsibility based on its remit as laid down in the Federal Constitution and the National Economic Supply Act (NESA).[6] This Minimum ICT Standard is an expression of this responsibility of the state to protect society, the economy, institutions and public administration.

This standard is primarily directed at operators and those responsible for critical infrastructures in the cultural property sub-sector, which are listed in the critical infrastructure protection inventory (CIP Inventory)[7]. All objects in the CIP inventory are also listed in the PCP inventory as objects of national importance (A-objects)[8]. The sectoral recommendation focuses on institutions with digital archive holdings (archives, libraries, museums), but it may also cover other institutions within the cultural property sub-sector that have digital holdings. Operators of critical infrastructures are advised to implement the Minimum ICT Standard. In principle, the standard offers assistance and specific modules for improving ICT resilience to every stakeholder involved in the preservation of cultural property.

A distinction is often made between digital cultural property that is 'born digital' (material that was created in digital form) and material that was originally created in physical form and has subsequently been digitised. This minimum standard does not differentiate between these two types of material; it treats them as equivalent. This is due to the fact that the boundary between these concepts, which were originally clearly defined, has become increasingly blurred in recent years. In addition to analogue-to-digital conversion, the process of digitisation today usually also involves datafication steps. Examples include text or speech recognition, named-entity recognition (NER) for converting text into structured data, vectorisation of plans, and 3D scans in archaeology or for museum objects. In addition, digitised representations are used as backup copies of the original analogue materials and take on the status of originals if the physical objects are lost. The value of digital cultural property therefore does not depend on how it was created, i.e. whether it has been created through digitisation or is born digital.

Several internationally recognised standards already exist for IT security (for an overview, see section 7, Literature). The Minimum ICT Standard is compatible with these existing standards, albeit with a reduced scope; it is not intended to compete with them. It aims to provide an easier introduction to the topic and help with the most important measures for achieving an appropriate level of protection. The sectoral recommendation focuses on processes with a direct impact on the security of digital cultural property and the safeguarding of data at rest. The security of the administrative IT infrastructure is only addressed in a subordinate manner.

6 Federal Act of 17 June 2016 on National Economic Supply (National Economic Supply Act, NESA; SR 531) (status as of 1 July 2023).

7 The CIP Inventory identifies individual critical infrastructure elements that are of strategic importance. The inventory of these buildings and facilities was compiled for the first time in 2012 in collaboration with the cantons. It is a classified document and is not available to the public. It provides the authorised parties (federal and cantonal authorities, operators) with a basis for planning and setting priorities for both risk management and incident response.

8 The PCP Inventory 2021 is available at https://www.babs.admin.ch/en/inventory-of-cultural-property-of-national-and-regional-importance.

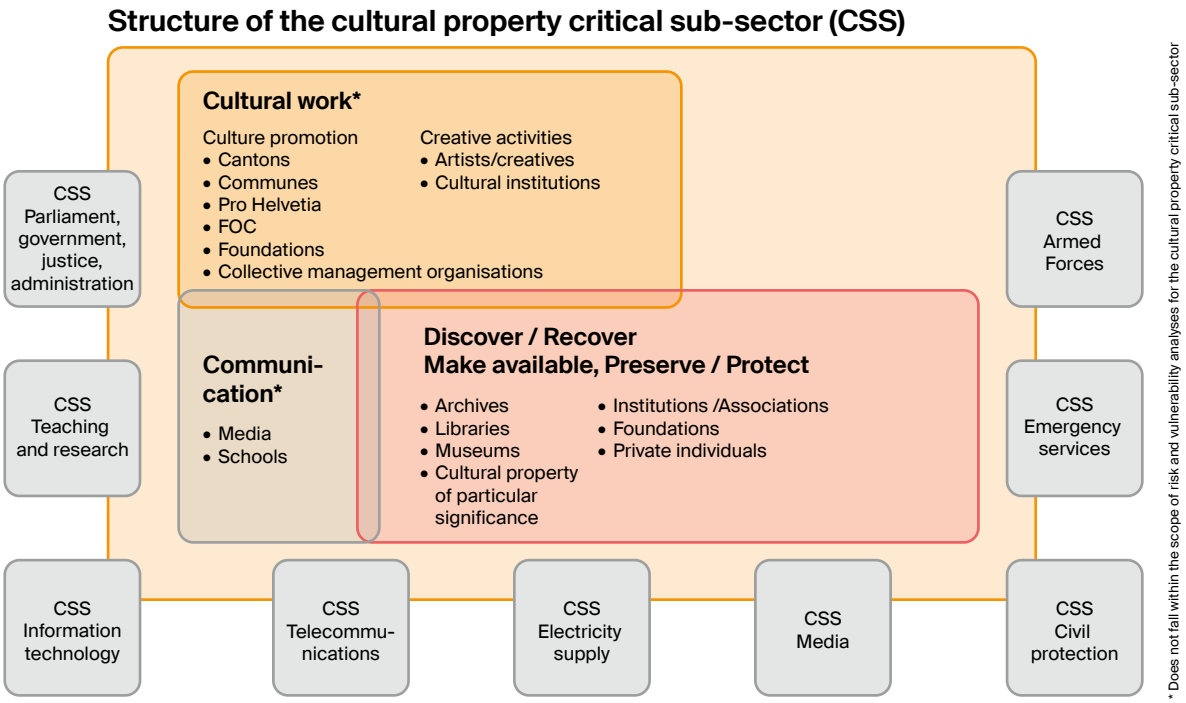


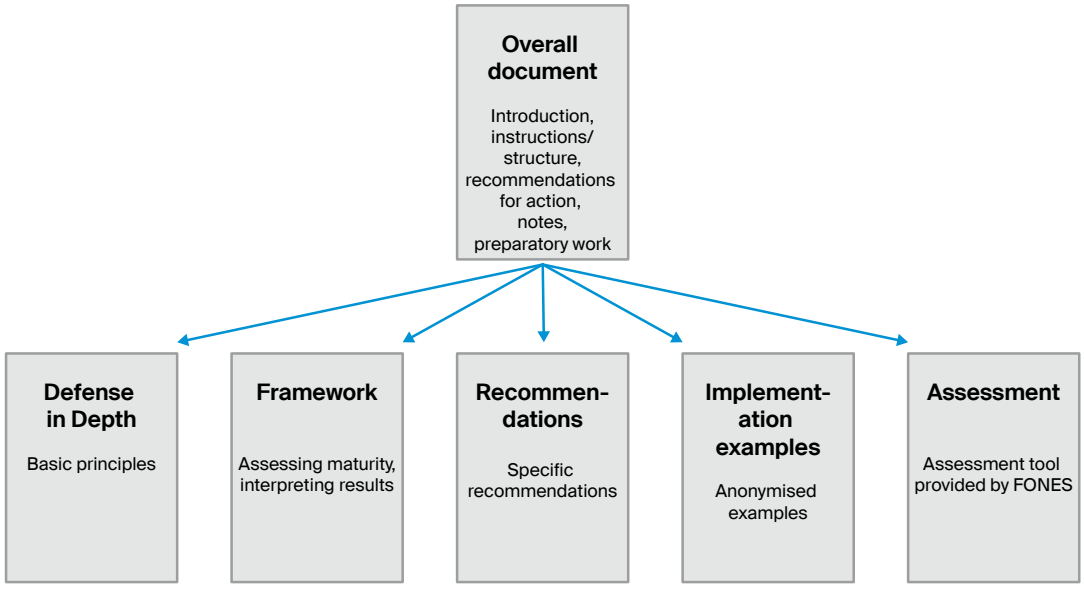
Figure: System boundaries of the critical sub-sector cultural property

1.3 Objectives and structure of the Minimum ICT Standard

This Minimum ICT Standard is intended as a preventive measure and formulated as a sectoral recommendation.

This document is structured into the following sections:

- Sections 1 and 2 provide an introduction to the main areas of protection of cultural property
- Section 3 describes the critical systems and processes
- Section 4 explains the defence-in-depth approach
- Section 5 provides a framework for reviewing and planning resilience
- Section 6 contains specific recommendations for improving resilience in the form of organisational and technical modules.



Overview of the documents of the Minimum ICT Standard

An assessment tool[9] is available from the FONES to assess the maturity level of a company or organisation. The Minimum ICT Standard is deemed to have been implemented if the maturity – according to the assessment tool's categorisation – corresponds at least to the minimum requirements in the overall rating, in accordance with the institution's own risk-based approach. In general, a process-based approach is recommended in order to guarantee regular, continuous review and improvement.

1.4 Implementation of the Minimum ICT Standard

The institutional landscape of cultural property preservation is very heterogeneous, particularly in terms of size, mandate and type of funding. Not every institution will be able to fully implement the Minimum ICT Standard. Smaller and financially weaker institutions will concentrate on a few centralised protective measures. The implementation proposals in section 6 are structured as modular building blocks. Each institution can prioritise the modules relevant to it based on its collection and risk profile. Depending on the size of the institution, the following general guidelines for implementation apply:

Type of institution	Examples	Implementation recommendation
Small, limited resources, low level of professionalisation	Small communal archive, specialist archive with focused collection profile	Focus on the most important modules as set out in section 6
Medium-sized to large, secured resources, high degree of professionalisation	Large communal archive, state archive, Federal Archives, specialist archive with a broad collection profile	Prioritisation of the modules in section 6 according to the risk profile, use of the assessment tool

The process model below can be used to implement the Minimum ICT Standard. If the archive's IT system is part of a larger IT organisation (e.g. city, canton or federal government), the implementation can take place at a higher level and also include other infrastructures. If this is not the case or if the archive is to be secured independently according to this standard, the next step is to assess the size of the institution. Small institutions implement the modules prioritised for them in section 6. Medium-sized and large institutions implement the Minimum ICT Standard in full.

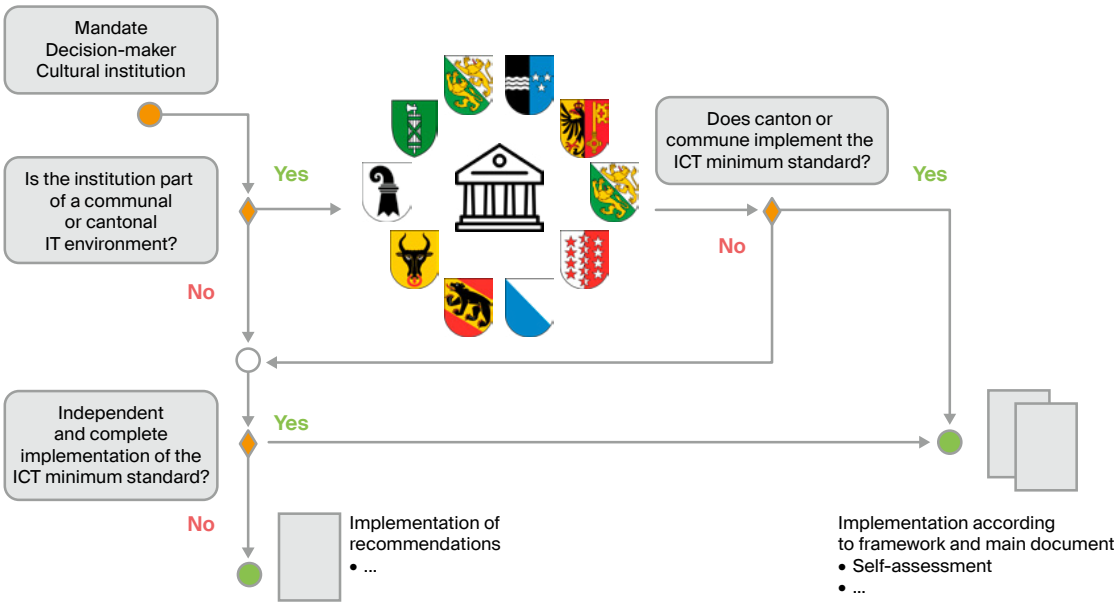


Figure: Visualisation of the process for implementing the Minimum ICT Standard

9 The assessment tool is available as an Excel document: https://www.bwl.admin.ch/en/ict-minimum-standards

A process-based approach is recommended in general, especially for large organisations. This means that cybersecurity is not a static state, but rather must be understood as a process that is put into practice and continually reviewed. ICT security can never be fully achieved, but must be constantly strived for and regularly updated.

1.5 Preliminary work and legal bases

Pursuant to the Federal Constitution, the cantons have cultural sovereignty. Under the archive laws, they are also responsible for archives governed by public law. The federal government may support cantons on a subsidiary basis. In particular, the FOCP can support and advise the cantons on the protection of cultural property.[10]

On 16 June 2023, the Federal Council adopted the National Critical Infrastructure Protection (CIP) Strategy.[11] The CIP Strategy is a further development of the first two strategies from 2012 and 2017. The FOCP is responsible for coordinating the tasks relating to CIP. The CIP Strategy describes 17 measures to improve resilience within and across sectors. The national strategy for the protection against cyber risks[12] makes it clear that Switzerland must protect itself against cyberthreats from an economic and socio-political perspective in order to consistently exploit the opportunities of digitalisation and maintain its locational advantage as a secure country. Work relating to CIP and cybersecurity is coordinated between the federal government and the cantons. The National Cyber Security Centre (NCSC), which works closely with the Federal Chancellery's Digital Transformation and ICT Steering Sector (DTI), was established as part of the implementation process. The FONES has also published a minimum standard for improving ICT resilience for this purpose.

In 2020, the FCPCP adopted a 2021–2025 strategy focusing on prevention/precaution, deployment and recovery in the protection of cultural property.[13] This strategy sets out the most important guidelines for maximising the protection of cultural property. Digitalisation and the cybersecurity of digital cultural property are given a high priority. The necessary conceptual clarification and the development of an evaluation matrix for systematic inclusion in the PCP inventory were undertaken. The long-term and sustainable preservation of digital objects is part of this PCP strategy.

The Digital Humanities Lab (DH Lab) at the University of Basel conducted and analysed online surveys on digital cultural property on behalf of the FCPCP and the FOCP PCP.[14] The Minimum ICT Standard has drawn on the results of the 2016 and 2020 DH Lab surveys to determine the quantitative structures of digital cultural property and the resulting security needs.

10 Art. 4 para. b of the Federal Act of 20 June 2014 on the Protection of Cultural Property during Armed Conflicts, Disasters and Emergencies (CPPA; SR 520.3).

11 National Critical Infrastructure Protection Strategy 2023. Already in June 2012 and 2017, the Federal Council adopted predecessor strategies for critical infrastructure protection in order to further improve Switzerland's resilience (robustness, adaptability and regenerative capacity) with regard to critical infrastructures: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/3159c04b-ffc8-4f4e-b72f-ccba-6b6a800e.pdf

12 National strategy for the protection of Switzerland against cyber risks (NCS): https://www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html

13 The strategy paper is available at: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/732d8094-52f3-49dd-965f-3debd139c8cd.pdf

14 The evaluation report from February 2017 on the digital cultural property survey can be obtained from the FOCP PCP.

2 Switzerland's digital cultural heritage

According to the UNESCO conventions[15], the term 'cultural heritage' encompasses all movable and immovable cultural property as well as intangible cultural heritage.

- **Movable** cultural property includes collections in archives, libraries and museums. This category includes not only cultural property on analogue information carriers, but also digital cultural heritage in the form of digital holdings in the administrative archives and in the aforementioned institutions. Examples include video and net art, authors' estates, archives of audiovisual media (AV archives), data collections, research data, etc.
- **Immovable** cultural property includes buildings, monuments and archaeological sites. These items of cultural property are secured by documentation in the form of plans, photographs and inventories. Today, this documentation is also created in digital form.
- **Intangible** cultural heritage includes traditions, customs, festive events and the performing arts.[16] Intangible cultural heritage is ephemeral and cannot be archived, but it can be documented. Documentation usually takes the form of audiovisual or written recordings, which are now generally created and archived digitally.

This overview shows that digital objects worthy of protection can be found in all three areas. However, the focus is on movable cultural property with its digital collections and archives. Such collections can now be found in both public and private cultural heritage organisations. This Minimum ICT Standard focuses primarily on the protection of archives, given that they are considered to be especially critical due to their role in protecting legal certainty.

15 The UNESCO conventions ratified by Switzerland are available at https://www.unesco.ch/culture/conventions/.

16 Art. 2 of the Convention for the Safeguarding of the Intangible Cultural Heritage (SR 0.440.6), adopted in Paris on 17 October 2003.

2.1 Overview and stakeholders

Due to Switzerland's traditionally strongly federalist cultural policy, the preservation and maintenance of cultural property is not in the hands of a few centralised memory institutions, but rather is carried out by a large number of regional, cantonal and national organisations with a range of legal forms. The preservation of cultural heritage in Switzerland is not centrally managed.

The stakeholders are organised under either public or private law and can be assigned to the federal (national) – cantonal – city/communal/regional levels. Sometimes they are also active on several levels. The following figure shows the diversity of the stakeholders:

		Legal form		
		Governed by public law Public/legal mandate	**Private** Public/legal mandate	**Private** Own mandate
Main source of funding	**Public sector**	**Public stakeholder** • Organised under public law • Public/legal mandate • Funding mainly from public sources (may also receive private funding)	**Hybrid stakeholder** • Organised under private law • Public/legal mandate • Funding mainly from public sources (may also receive private funding)	**Hybrid stakeholder** • Organised under private law • Public/legal mandate • Funding mainly from public sources (may also receive private funding)
	Private	Does not occur	Does not occur	**Private stakeholder** • Organised under private law • Private/own mandate • Funding mainly from private sources (may also receive public funding)

Haupttypen:

Public	**Hybrid**	**Private**

The following organisational forms of the stakeholders are typical:

- **Public stakeholders (governmental):** Authorities, foundations at federal, cantonal, city/communal levels
- **Hybrid stakeholders (private/public):** Foundations, associations at international, national, cantonal and regional levels
- **Private stakeholders:** Foundations, associations, companies at international, national, cantonal and regional levels

This overview shows that cultural heritage management is characterised by a marked heterogeneity with stakeholders of different sizes, financial strength and operating scope.

Most of these stakeholders involved in cultural heritage preservation are located at cantonal and communal level. The federal government supports them on a subsidiary basis and takes on coordinating tasks. At national level, the Federal Office of Culture (FOC) is responsible for the preservation and classification of cultural property, and the FOCP is responsible for the protection of cultural property in the event of war and disasters. At cantonal and communal level, the cantonal and communal offices are responsible for culture, protection of cultural property, protection of sites of local character, monument preservation and archaeology. In addition, numerous private stakeholders are committed to the preservation and protection of cultural property in Switzerland, most of which are organised either as private foundations or associations. A wide range of hybrid stakeholders have a public mandate but are organised under private law. [17]

17 Edzard Schade, Tobias Wildi (2022). Übersicht / Bestandesaufnahme Kulturerbe der Schweiz. Report commissioned by the Federal Office of Culture.

The federal government and the cantons are responsible for the cultural property in their possession. The responsibilities for the preservation and classification of cultural property are generally regulated at federal level in the Federal Act on the Protection of Nature and Cultural Heritage (NCHA)[18]. In addition, extensive special cantonal legislation contains relevant provisions (e.g. archive law, monument preservation and archaeology). Responsibility for cultural property during armed conflicts, disasters and emergencies is regulated in the Federal Act on the Protection of Cultural Property during Armed Conflicts, Disasters and Emergencies (CPPA)[19].

2.2 Archives and archive structure in Switzerland

This Minimum ICT Standard focuses primarily on archives, as some of the archives in our country are categorised as critical infrastructure.[20] These archives are considered critical infrastructures because of their contribution to legal certainty. In this report, the term 'archive' does not refer to a specific type of memory organisation; it is used more generally to encompass functions and systems for storing and preserving digital objects of cultural value. The task of an archive is to accept items of cultural property and guarantee that they remain usable over long periods of time. The integrity (unchanged state) and authenticity (trustworthiness) of the documents must be preserved. A different type of stakeholder, such as a library or a museum, can also take on this function.

Switzerland has a multi-layered public archive landscape with the Federal Archives, 26 state and cantonal archives, city and communal archives. There are also important ecclesiastical archives, company and specialist archives, as well as archival holdings in libraries, museums and documentation centres. The 26 state archives and the Federal Archives have been categorised as systemically relevant objects in the CIP inventory.

In Switzerland, there is no centralised archive structure managed by the federal government, cantons and communes. The right of use and storage and notification obligations are not defined by any constitutional provision. In Switzerland, archive law has a federalist structure: each canton has its own archives act or archives ordinance. The 26 state archives accordingly have their own historical-legal tradition.

Data protection legislation significantly influenced the development of archive law in the 1990s. The main issues to be regulated were the obligation to offer documents to archives, the right to use and the protection of privacy (data protection). In addition to the federal government, the majority of the cantons have meanwhile also enacted archive legislation. In principle, every person in Switzerland has the right to inspect official files, provided that doing so does not conflict with overriding public or private interests.

The Federal Act on Archiving (ArchA)[21] regulates the archiving of federal files in the Federal Archives. Federal documents that are valuable for legal, political, economic, historical, social or cultural reasons must be archived. However, the ArchA has no direct impact on the cantons and communes.

18 Federal Act of 1 July 1966 on the Protection of Nature and Cultural Heritage (NCHA; SR 451).

19 Art. 3 and 5 of the Federal Act of 20 June 2014 on the Protection of Cultural Property during Armed Conflicts, Disasters and Emergencies (CPPA; SR 520.3).

20 See https://www.babs.admin.ch/en/critical-infrastructures.

21 Federal Act of 26 June 1998 on Archiving (Archiving Act, ArchA; SR 152.1).

3 Overview of system-critical systems and processes

3.1 System-critical archives

System-critical archives include the Federal Archives, the state archives and selected communal and specialist archives.

Federal Archives (SFA)

The Swiss Federal Archives (SFA) have the legal mandate[22] to keep relevant federal information permanently available. This makes the administration accountable for its activities and supports it in its work. The SFA supports and advises the Federal Administration in the creation, organisation and management of data and documents. The SFA also works with the administrative offices to select the documents worthy of archiving and guarantees that they remain available and preserved in the long term. The evaluation is based on systematic criteria, and the decisions are published regularly.[23] The SFA also digitises analogue archive documents and makes them available to the public. The SFA participates in historical research on selected topics and makes it accessible to a broad public.

State archives and communal archives

The state archives and communal archives essentially fulfil the same tasks at cantonal and communal level as the SFA at national level. They accept, classify and preserve the archive-worthy documents of the authorities obliged to offer them and are responsible for preservation measures and accessibility. They contribute to the communication of historical knowledge and historical research for the needs of the canton, science and culture. They evaluate documents according to their archival value, advise authorities as well as private individuals and institutions and in some cases also issue instructions on the delivery of documents and finding aids.

Specialist archives

Specialist archives are archives that focus on certain topics or subject areas. They collect, preserve and make available documents on a specific topic. Specialist archives include archives for art, music, history, natural history, technology, science, medicine and others. They are used for research, education and culture and are important sources for scientists, historians, journalists, artists and the general public. Specialist archives fulfil an important social function because they document the work of civil society and non-state actors in a way that complements state records. These include social movements, political parties, religious communities, associations, non-governmental organisations (NGOs), etc.

3.2 Services provided by the archives in the cultural property sub-sector

Public archives are important stakeholders in ensuring legal certainty in Switzerland. They safeguard documents that are of vital importance for the protection and enforcement of rights and obligations, such as legislative texts, contracts, deeds, court judgments and evidence of land ownership. The archives ensure that the documents are archived in accordance with applicable laws, norms and standards in order to guarantee the integrity and authenticity of the archive material.

By permanently storing administrative documents, archives ensure the traceability of decisions and actions, especially in the public sector. This contributes to the transparency and accountability of government and administrative processes, promoting citizens' trust in their institutions and the rule of law. The Federal Archives aptly summarise this in their claim: **No democracy without archives.**

22 See Federal Act on Archiving (ArchA, SR 152.1).

23 The SFA's evaluation decisions are available at : https://www.bar.admin.ch/bar/de/home/informationsmanagement/archivwuerdigkeit/bewertungsentscheide.html

Complementing the public archives, the overall social benefit of specialist archives lies in the preservation and usability of items of movable cultural property that were not created directly in connection with public administration. Specialist archives focus on specific topics and subject areas such as social history, economic history or women's history. Specialist archives have a high value for forging the cultural identity of our country and therefore fall (at least partially) under critical infrastructures.

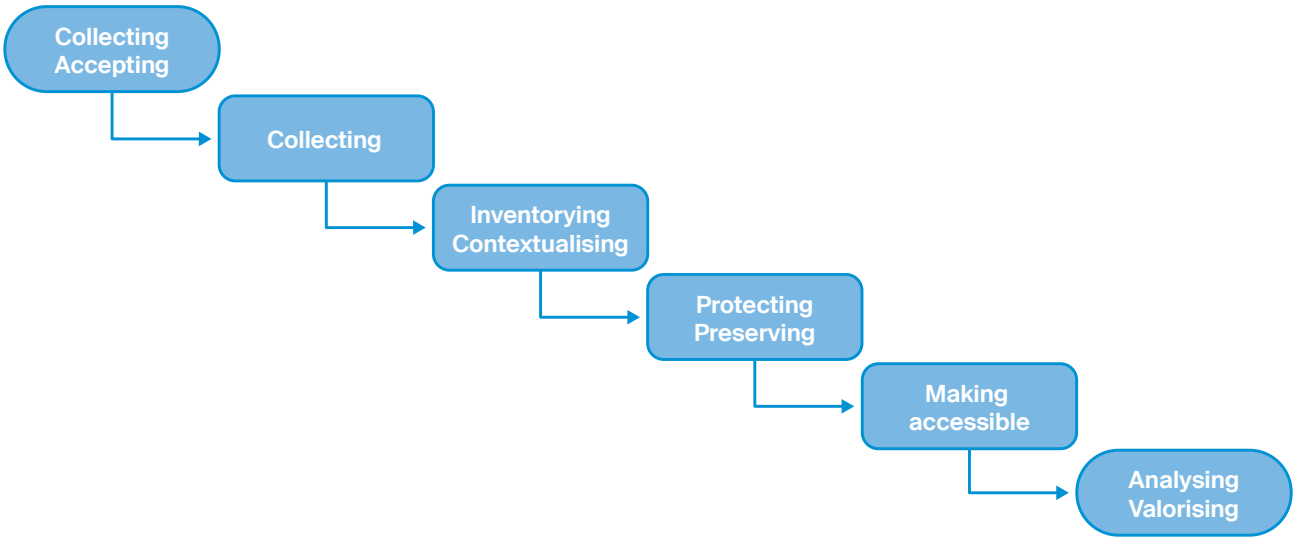
3.3 Overview of critical processes

In principle, the business processes of all stakeholders involved in the preservation and maintenance of cultural heritage can be described with the help of the process model below. Terms as general as possible are used to describe the fields of action; the phases are named differently depending on the type of stakeholder (archive, library, museum, documentation centre, monument preservation) and cultural property (movable, immovable, intangible). The model shows that the cultural property critical sub-sector is highly dependent on ICT systems, particularly for inventory, research and protection/preservation.

Within the scope of this Minimum ICT Standard, some fields of action are not taken into account or are part of critical infrastructures of other sub-sectors:

- Upstream systems such as GEVER, document management, records management, specialist applications
- Evaluation, selection, choice of cultural property for archiving
- Downstream systems such as analysis systems, research infrastructures

The acceptance, preservation and making accessible of digital cultural property consists of the following process stages:



Collecting
Acceptance and preparation of data and metadata, also referred to as ingest. Supported by workflow-based systems that automate and orchestrate tasks such as virus checks, validation, metadata extraction, file format migration, integrity (writing checksums), etc.

Inventory and contextualisation
Classifying, recording and organising, documenting, cataloguing. Depending on the type of organisation, this task is supported by archive information systems, library systems or collection management systems. In addition, contextual knowledge and information on provenance, context of origin and utilisation are collected.

Protecting and preserving
Saving (initial process), securing (permanent task: maintenance, checking the storage). Preservation planning, implementation of conservation measures if necessary.

Making accessible
Enabling research (OPAC, digital reading room, web access), delivery (outputting data for machine analysis or further use via technical interfaces).

Analysing and valorising
Transmission and updating in the form of didactic and media-based communication, and through practice.

3.4 Which dangers to protect against

The 2022 FOCP report on threats and resilience in the cultural property sub-sector analyses the risks caused by the failure or disruption of this critical infrastructure. Four main danger areas were identified for cultural property:

- A **cyberattack** and/or ICT failure is likely to affect the availability of a cultural heritage preservation organisation's digital holdings for several weeks. In addition, irreversible destruction, theft or (un) intentional publication of sensitive information may occur. The archive holdings can be restored only if appropriate measures have been taken in advance. Publication of confidential documents can cause considerable reputational damage to individuals and organisations. The danger of a cyberattack exists not least because cultural heritage institutions often have to make do with limited resources and are unable to keep pace with rapid technological progress.
  Threatened process stages: All process stages are threatened by cyberattacks.
- In the case of **natural hazards** such as earthquakes and floods, considerable coping and restoration costs are to be expected. The two threats impair several items of cultural property in the affected region. The availability of the archive records is impaired for months or even years. This leads to considerable follow-up costs for the public, authorities and research.
  Threatened process stages: The «Protecting and preserving» stage in particular is jeopardised by natural hazards.
- A **conventional attack** on an archive or cultural property is considered an attack on the identity of the canton or the country and leads to major damage due to the uncertainty among the public and in the economy. A conventional attack on a data centre can lead to considerable data loss.
  Threatened process stages: The "Protecting and preserving" stage in particular is jeopardised by conventional attacks.
- A **pandemic** leads to a loss of specialised personnel who are needed to operate the digital archive and secure the data. This danger is especially acute in smaller cultural property institutions, where the relevant specialised knowledge is concentrated in a single individual or a few individuals.
  Threatened process stages: If specialised personnel are unable to work, process knowledge is jeopardised in all areas. The «Protecting and preserving» stage in particular is jeopardised.

As in other sub-sectors, cyber risks also pose a considerable risk for cultural property due to the increasing digitalisation of business processes and the centralisation of IT infrastructures. Moreover, the frequency of such attacks has increased considerably in recent years. The emerging regional and supra-regional networks for digital archiving and the larger volume of digital objects being accepted into archives are also increasing the potential for damage.

4 Defense in Depth

The defence-in-depth approach is introduced here to protect against the dangers mentioned above. This approach is based on the principle that no security measure is sufficient on its own to fully protect systems or networks. Instead, a holistic approach should be pursued, consisting of various security measures that are implemented in several layers or levels. The aim of this chapter is to explain the defence-in-depth approach to cybersecurity in more detail and to show which categories of measures organisations can use to implement it. Building on these principles, section 6 then lists specific modules for improving information security.

4.1 The defence-in-depth concept

An organisation's ICT security strategy must be geared towards protecting the systems and applications required for its fields of activity and processes. This requires a multi-layered approach known as defence in depth. The approach involves the coordinated deployment of several layers of protection, based on the principle that it is more difficult to overcome a layered, multi-tiered defence system than a single barrier. At the same time, the methods and modus operandi of potential attackers are observed as a basis for the corresponding defence plan. In a cybersecurity context, a defence-in-depth concept is designed to recognise breaches in ICT security, to respond to them, and to minimise or mitigate the consequences of those security breaches. Defence in depth takes a holistic approach which seeks to protect all (ICT) assets against all types of risk. An organisation's resources should be deployed to ensure effective protection against known risks, as well as comprehensive monitoring of potential future risks. This includes people, processes, properties, data and devices. An attacker only poses a threat to an ICT system if they succeed in exploiting a vulnerability in one of these elements. Organisations and businesses must monitor their security measures continuously, and adapt them to new threats where necessary.

Roughly speaking, elements of a defence-in-depth approach can be divided into organisational, technical and physical measures.

4.2 Organisational measures (processes)

This group of measures includes the following modules:

- Defence as a permanent task of an organisation within the framework of security management. Regulation of responsibilities within the organisation
- Creating a risk profile, identifying security risks
- Organisational and personnel security aspects
- Standardised concepts and procedures, such as regarding data protection, deletion and destruction of data and data carriers, exchange of information internally or with third parties
- Inventory management of ICT assets (asset management)
- Overview of the archived digital objects
- Operational security aspects, both for in-house operation and for operation by third parties (external data centre, cloud). This also includes separating administrative IT and archive systems
- Ensuring patch and vulnerability management
- Processes for creating and reviewing the implemented security measures, the detection of security incidents and the incident management processes
- Organisation of business continuity management
- Documentation

4.3 Technical measures (systems)

This group of measures includes the following modules:

- Securing applications and services, including in the areas of communication, storage, and business and client applications
- Securing individual IT systems such as servers and desktops
- Securing the network, network connections and components and communication via the network. Subdividing the network into segments and security zones.
- Securing active network components (firewalls, routers, switches, etc.)

4.4 Physical measures

The physical protection of archive holdings is relevant especially for analogue material, in light of the need to secure storage rooms against fire, water or vandalism. The following areas play a role in digital archives:

- Access security for server rooms and data centres
- Protection of server rooms and data centres against natural hazards
- Geographically distributed storage and backup systems
- Backup to offline or cold storage. With this type of storage – as with all other types of storage – it is important to carry out a periodic integrity check.

4.5 Separation of office systems and archive systems

A key point of the defence-in-depth strategy is the systematic and systemic separation of administrative IT and the digital archive holdings, or the archive system. An 'archive system' in principle comprises the tasks described in the ISO 14721 standard, Open Archival Information System (OAIS).

The following table uses examples to explain how these two areas function according to different logics and planning processes and must therefore be considered differently. This minimum standard and in particular the modules for improving information security in section 6 relate primarily to the protection of digital cultural property and not to office systems.

Security topic	ICT (e.g. office systems)	OAIS-based archive system
Normative bases	Norms and standards	National and cantonal archive legislation, UNESCO Convention for the Protection of Cultural Property, norms and standards
Anti-virus	Widespread. Easily deployed and updated. Users have control over customisation. Anti-virus protection can be asset-based or enterprise-based.	Viruses pose a double challenge: The archive system servers must be protected, and virus-infected files must be prevented from entering the long-term archive via ingest.
Security updates (update management)	Clearly defined, company-wide, remote and automated.	Long lead and planning time to successful patch installation; OEM-specific; may (temporarily) halt OAIS functionality. The acceptable risk in this regard must be defined.
Technology support life cycle	2–3 years, multiple providers, ongoing development and upgrades.	10–20 years, usually same vendor/service provider over the entire life cycle, product end-of-life creates new security threats.
Testing and audit methods	Use modern (poss. automated) methods. Systems are usually resilient and reliable enough to handle assessments during normal operation.	Automated assessment may be unsuitable, e.g. owing to the high degree of individual development. There is a greater probability of failure during testing, so assessments during normal operation tend to be more difficult.

Security topic	ICT (e.g. office systems)	OAIS-based archive system
Change management	Regular and scheduled. Geared to the organisation's requirements, to minimum/maximum period of use.	A complex procedure with a potential impact on the archive's business activities. Strategic, individual planning required.
Asset classification	Common and performed annually. Results drive expenditure/investment.	Data classification is a particular issue in relation to archiving. Without an inventory and knowledge of the data's worthiness of protection, it is difficult to plan effective countermeasures.
Incident response and forensics	Easily developed and deployed. There may be regulatory requirements (data protection) that must be observed.	Primary focus on resumption of the system as part of data recovery and disaster recovery.
Physical security	Ranges from poor (office systems) to excellent (secure data centres).	Physical security is typically excellent. In state archives, OAIS is usually operated in cantonal data centres.
Secure software development	An integral part of the development process.	Early digital long-term archives were often designed as physically isolated systems and formed a foreign element in the IT infrastructure. Modern OAIS are planned and implemented as an integral part of the cantonal IT infrastructure, also in terms of security.
Security compliance	General regulatory requirements, depending on sector (and not in all sectors).	The security requirements of the sectoral standards focus on the long-term preservation of data and metadata and do not address broader security-specific issues. General standards such as NIST or ISO 27001 should be used for this purpose.

Table 1: Differences between office systems and OAIS-based archive systems

5 NIST Framework Core measures

5.1 Overview

NIST Framework Core

The aim of the Cybersecurity Framework[24] developed by the US National Institute of Standards and Technology is to provide operators of critical infrastructures with a tool to proactively increase their resilience to cyber risks. It also takes into account the pursuit of cost-effectiveness and efficiency as well as confidentiality and data protection. The Framework is based on a selection of existing standards, guidelines, and best practice specifications, and is technology-neutral.

The NIST Framework Core is a risk-based approach to address and consciously manage cyber risks. It consists of five functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Together, these five functions form the basis for the security concept.

The NIST Framework has four implementation tiers. These describe the practices or level of protection that a business has instituted. They range from partial (tier 1) to adaptive (tier 4). To determine its desired level of protection (tier level), an organisation should gain an overview of its risk management practices, the threat situation, legal and regulatory requirements, business objectives and organisational guidelines. Only then will it become clear what the organisation is trying to protect itself against.

The following chapter is organised according to the five functions of the NIST Framework Core. The tasks to be performed are categorised as follows:

- In each case, the first two letters (e.g. 'ID' = 'Identify) refer to one of the five functions.
- The second pair of letters then refers to the category (e.g. 'AM' = 'Asset Management').
- Finally, the number designates the individual task. They are numbered sequentially within the category. Example: 'ID.AM-1' corresponds to the first task in the asset management category under the Identify function.

The following table provides an overview of the functions and categories of the NIST framework:

Abbreviation	German	English
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 measures

Abbreviation	German	English
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

Table 2: Overview of the NIST framework functions and categories

An additional table of references to other international ICT standards has been added to each table listing tasks from the NIST Framework Core. These tables each reference a particular category, such as asset management. They are intended to make it easier for users who organise their ICT security according to other standards to map the present standard against their own. Sector-specific reference is also made to the ISO 16363 standard for digital cultural property (see next section).

NIST Framework and industry standard ISO 16363:2012

ISO 16363:2012, Audit and certification of trustworthy digital repositories, is an important industry standard for assessing the trustworthiness of digital archives. It is divided into the following three parts:

- Organizational infrastructure
- Digital object management
- Infrastructure and security risk management

The following table shows how the functions and categories of the NIST Framework and ISO 16363 relate to each other:

5 NIST Framework Core measures

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	

Table 3: Relationship between NIST framework categories and ISO 16363:2012

The industry standard ISO 16363:2012 largely covers the NIST functions Identify and Protect, and awareness of the importance of these two areas is generally high in the industry. However, it is also clear that it does not cover the Detect, Respond and Recover functions. The same conclusion can be drawn by comparing the NIST categories with 'nestor criteria, Catalogue of Criteria for Trusted Digital Repositories'[25], a widely used tool in German-speaking countries that covers the same areas as ISO 16363:2012.

25 nestor Working Group Trusted Repositories – Certification. (2008). Catalogue of Criteria for Trusted Digital Repositories. http://nbn-resolving.de/urn:nbn:de:0008-2008021802

5.2 Identify

Asset management

The data, individuals, devices, systems and facilities of an organisation are identified, catalogued and rated. Their rating should correspond to their criticality in the business processes that must be completed, and the organisation's risk strategy.

The creation of inventories is a key measure for the protection of digital cultural property. Inventories not only provide an overview and control of the cultural property to be protected, they also document their provenance and history of origin, and help to ensure authenticity. There are inventories both at an overarching level, such as the PCP inventory, but also within the institutions, such as archive information systems, library catalogues or databases for collection management.

Designation	Task
ID.AM-1	Draw up an inventory-taking process which ensures that you have a complete inventory of all your ICT assets at all times.
ID.AM-2	Produce an inventory of all of the software platforms/licences and applications within your organisation.
ID.AM-3	Catalogue all internal communication and data flows.
ID.AM-4	Catalogue all external ICT systems that are relevant to your organisation.
ID.AM-5	Prioritise the inventoried resources (devices, applications, data) according to their criticality.
ID.AM-6	Define clear roles and responsibilities in cybersecurity.

Table 4: ID.AM tasks

Standard	Reference
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

Table 5: ID.AM references

Business environment
The company's objectives, tasks and activities are rated and prioritised. This information is used as a basis for allocating responsibilities.

Designation	Task
ID.BE-1	Identify, document and communicate the exact role of your business within the (critical) supply chain.
ID.BE-2	Identify and communicate the importance of the organisation as a critical infrastructure operator, and its position within the critical sector.
ID.BE-3	Rate and prioritise objectives, tasks and activities within the organisation.
ID.BE-4	Define all dependencies and critical functions for the provision of critical services.
ID.BE-5	Define resilience requirements to support the provision of critical services for all operating states (e.g. under constraint/attack, during recovery, in normal operation).

Table 6: ID.AM references

Standard	Reference
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

Table 7: ID.BE tasks

Governance
Governance determines responsibilities, monitors, and ensures compliance with regulatory, legal and operational requirements from the business environment.

Designation	Task
ID.GV-1	Establish and communicate an organisational cybersecurity policy.
ID.GV-2	Coordinate information security roles and responsibilities with internal roles (e.g. those in risk management) and external partners.
ID.GV-3	Ensure that your organisation complies with all legal and regulatory cybersecurity requirements, including those applicable to data protection.
ID.GV-4	Ensure that cybersecurity risks are embedded in company-wide risk management structures.

Table 8: ID.GV tasks

Standard	Reference
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

Table 9: ID.GV references

Risk Assessment
The organisation understands the effects of cybersecurity risks on business operations, assets and individuals, including reputational risks.

Designation	Task
ID.RA-1	Identify the (technical) vulnerabilities of your assets, and document them.
ID.RA-2	Share intelligence regularly in fora and other bodies to stay up to date about cybersecurity threats.
ID.RA-3	Identify and document internal and external cybersecurity threats.
ID.RA-4	Identify the possible business impacts of cybersecurity threats, and calculate the probability of their occurrence.
ID.RA-5	Rate the risks to your organisation based on threats, vulnerabilities, impacts (on business activity) and probabilities.
ID.RA-6	Define possible immediate responses should a risk occur, and prioritise these measures.

Table 10: ID.RA tasks

Standard	Reference
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

Table 11: ID.RA references

Risk Management Strategy
The organisation's priorities, restrictions and maximum acceptable risks are defined. Operational risks are assessed on this basis.

Designation	Task
ID.RM-1	Establish risk management processes, manage them actively and have them confirmed by the persons/stakeholders concerned.
ID.RM-2	Define and communicate your organisation's maximum risk tolerance.
ID.RM-3	Ensure that maximum risk tolerance is calculated taking into account your organisation's importance as an operator of a critical infrastructure. This calculation should also be informed by sector-specific risk analyses.

Table 12: ID.RM tasks

Standard	Reference
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

Table 13: ID.RM references

Supply Chain Risk Management
Determine priorities, constraints, and the maximum risks that your organisation is willing to accept in connection with supplier-related risks.

Designation	Task
ID.SC-1	Identify, establish, evaluate and manage risk management processes in the cyber supply chain. Have the stakeholders involved agree on the selected processes.
ID.SC-2	Identify and prioritise suppliers and third-party partners of information systems, components, and services, and assess them using a cyber supply chain risk assessment process (see ID.SC-1).
ID.SC-3	Routinely check suppliers and third-party providers through audits, tests or other forms of assessment to ensure that they are fulfilling their contractual obligations.
ID.SC-4	Establish a system of monitoring to ensure that all of your suppliers and service providers are fulfilling their obligations as required. Have this confirmed on a regular basis by audit reports or technical test results.
ID.SC-5	Work with your suppliers and service providers to define response and recovery procedures following cybersecurity incidents. Conduct drills to test these procedures.

Table 14: ID.SC tasks

Standard	Reference
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

Table 15: ID.SC references

5.3 Protect

Access Control

Physical and logical access to ICT assets and facilities is possible only for authorised individuals, processes and devices. Access is also only possible for authorised activities.

Designation	Task
PR.AC-1	Establish a clearly defined procedure for granting and managing permissions and access data for users, devices and processes.
PR.AC-2	Ensure that only authorised individuals have physical access to ICT assets. Take action (on building security, for example) to ensure that ICT assets are protected from unauthorised physical access.
PR.AC-3	Establish procedures to manage remote access.
PR.AC-4	Define permission levels according to the principle of least privilege, as well as separation of functions.
PR.AC-5	Ensure that the integrity of your network is protected. Segregate your network both logically and physically where necessary and sensible.
PR.AC-6	Ensure that digital identities are allocated to unambiguously authenticated individuals or processes.
PR.AC-7	Authenticate users, devices, and other assets (e.g. using single-factor or multi-factor authentication) commensurate with the risk of the transaction (e.g. individuals' security and privacy risks and other organisational risks).

Table 16: PR.AC tasks

Standard	Reference
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

Table 17: PR.AC references

Awareness and Training
Regular, appropriate training of staff and external partners on all aspects of cybersecurity is ensured. It is ensured that staff and external partners perform their security-related tasks in accordance with the related requirements and procedures.

Designation	Task
PR.AT-1	Ensure that all members of staff receive information and training on cybersecurity.
PR.AT-2	Ensure that higher-level users are particularly aware of their role and responsibility.
PR.AT-3	Ensure that all third-party stakeholders (suppliers, customers and partners) are aware of their role and responsibility.
PR.AT-4	Ensure that all managers are aware of their particular role and responsibility.
PR.AT-5	Ensure that those in charge of physical security and information security are aware of their particular role and responsibility.

Table 18: PR.AT tasks

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

Table 19: PR.AT references

Data Security
It is ensured that information, data and data carriers are managed in a way which protects the confidentiality, integrity and availability of the data in accordance with the organisation's risk strategy.

Designation	Task
PR.DS-1	Ensure that stored data is protected (against violations of confidentiality, integrity and availability).
PR.DS-2	Ensure that data is protected while in transit (against violations of confidentiality, integrity and availability).
PR.DS-3	Ensure that you have a formal procedure in place for your ICT assets which protects data upon the removal, transfer or replacement of those assets.
PR.DS-4	Ensure that your ICT assets have sufficient capacity to ensure data availability is maintained.
PR.DS-5	Ensure that appropriate action has been taken to prevent data leaks.
PR.DS-6	Establish a procedure to check the integrity of firmware, operating systems, application software and data.
PR.DS-7	Provide a development and testing IT environment which is completely separate from productive systems.
PR.DS-8	Establish a procedure to check the integrity of the hardware you use.

Table 20: PR.DS tasks

Standard	Reference
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

Table 21: PR.DS references

Information protection processes and procedures
Policies exist to protect information systems and assets. It is ensured that these policies include as a minimum the purpose, scope, roles and responsibilities and regulate coordination within the organisation. Apply these policies to protect those information systems and assets.

Designation	Task
PR.IP-1	Draw up a baseline configuration for your information and communication infrastructure, as well as for industrial control systems. Ensure that this baseline configuration complies with typical security principles (e.g. N-1 redundancy, least-functionality configuration).
PR.IP-2	Establish a life cycle procedure for the use of ICT assets.
PR.IP-3	Establish a procedure to monitor configuration changes.
PR.IP-4	Ensure that copies (backups or synchronisations) of your information are conducted, maintained and tested on a regular basis (check that you are able to revert to your copies).
PR.IP-5	Ensure that you comply with all (regulatory) requirements and policies concerning your physical assets.
PR.IP-6	Ensure that data is destroyed according to requirements.
PR.IP-7	Ensure that your information security procedures are enhanced and improved continuously.
PR.IP-8	Share information about the effectiveness of various protection technologies with your partners.
PR.IP-9	Establish response procedures for any cyberincidents that may occur (incident response planning, business continuity management, incident recovery, disaster recovery).
PR.IP-10	Test your response and recovery plans.
PR.IP-11	Embed aspects of cybersecurity in the staff recruitment process at an early stage (e.g. by conducting background checks and individual security checks).
PR.IP-12	Develop and implement a procedure for dealing with identified vulnerabilities.

Table 22: PR.IP tasks

Standard	Reference
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

Table 23: PR.IP references

Maintenance
It is ensured that maintenance and repair work is carried out on ICT system components in accordance with the applicable guidelines and processes.

Designation	Task
PR.MA-1	Ensure that the operation and maintenance of assets are logged, as well as any repairs. Ensure that such work is conducted promptly and uses only those means which have been tested and approved.
PR.MA-2	Ensure that any maintenance work on your systems that is carried out via remote access is logged and documented. Ensure that no unauthorised access is possible.

Table 24: PR.MA tasks

Standard	Reference
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

Table 25: PR.MA references

Protective technology
Install technical security solutions in accordance with requirements and procedures to ensure the security and resilience of your ICT systems and their data.

Designation	Task
PR.PT-1	Define requirements for audits and log records. Produce and check the regular logs in accordance with those requirements and policies.
PR.PT-2	Ensure that removable media are protected, and that they are used only in accordance with policy.
PR.PT-3	Ensure that your system is configured so that a minimum level of functionality is guaranteed at all times.
PR.PT-4	Ensure that your communications and control networks are protected.
PR.PT-5	Ensure that mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Table 26: PR.PT tasks

Standard	Reference
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

Table 27: PR.PT references

5.4 Detect

Anomalies and events

It is ensured that anomalies (abnormal behaviours) and security-related events are detected swiftly and that the potential impact of incidents is understood.

Designation	Task
DE.AE-1	Define a baseline for permitted network operations and expected data flows for users and systems. Manage these values continuously.
DE.AE-2	Ensure that detected cybersecurity incidents are analysed to understand their targets and methods.
DE.AE-3	Ensure that information on cybersecurity incidents is aggregated and correlated from multiple sources and sensors.
DE.AE-4	Determine the impact of possible events.
DE.AE-5	Define threshold values for incident alerts.

Table 28: DE.AE tasks

Standard	Reference
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

Table 29: DE.AE references

Security continuous monitoring
It is ensured that ICT systems, including all assets, are monitored at regular intervals to detect cybersecurity incidents, and also to verify the effectiveness of protective measures.

Designation	Task
DE.CM-1	Establish continuous network monitoring to detect potential cybersecurity incidents.
DE.CM-2	Establish continuous monitoring/surveillance of all physical assets and buildings to detect cybersecurity incidents.
DE.CM-3	Monitor staff activities to identify potential cybersecurity incidents.
DE.CM-4	Ensure that malware can be detected.
DE.CM-5	Ensure that malware can be detected on mobile devices.
DE.CM-6	Ensure that the activities of external service providers are monitored so that cybersecurity incidents can be detected.
DE.CM-7	Monitor your system continuously to ensure that activities/access by unauthorised persons, devices and software are detected.
DE.CM-8	Perform vulnerability scans.

Table 30: DE.CM tasks

Standard	Reference
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

Table 31: DE.CM references

Detection processes
Processes and instructions for detecting cybersecurity incidents are cultivated, maintained and tested.

Designation	Task
DE.DP-1	Define clear roles and responsibilities so that there is no doubt about who is responsible for what, and who holds what authority.
DE.DP-2	Ensure that detection processes comply with all requirements and conditions.
DE.DP-3	Test your detection processes.
DE.DP-4	Communicate detected incidents to the relevant actors (suppliers, customers, partners, authorities, etc.).
DE.DP-5	Improve your detection processes continuously.

Table 32: DE.DP tasks

Standard	Reference
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

Table 33: DE.DP references

5.5 Respond

Response planning

A response plan is in place to address detected cybersecurity incidents. The necessary measures have been taken to ensure that this response plan is implemented correctly and on time in the event of an incident.

Designation	Task
RS.RP-1	Ensure that the response plan is executed promptly and correctly during or after a detected cybersecurity incident.

Table 34: RS.RP tasks

Standard	Reference
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

Table 35: RS.RP references

Communications
Ensure that your response procedures are coordinated with internal and external stakeholders. Ensure that, should an event occur, you receive support from public-sector bodies if necessary and appropriate.

Designation	Task
RS.CO-1	Ensure that all individuals are familiar with their response and the sequence of their actions if and when a cybersecurity incident occurs.
RS.CO-2	Define reporting criteria and ensure that cybersecurity incidents are reported and processed in accordance with these criteria.
RS.CO-3	Share information and findings about detected cybersecurity incidents in accordance with the defined criteria.
RS.CO-4	Coordinate with stakeholders in a way that is consistent with response plans and in accordance with the defined criteria.
RS.CO-5	Raise awareness of the current cybersecurity situation through the voluntary sharing of information with external stakeholders.

Table 36: RS.CO events

Standard	Reference
COBIT 2019	none
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

Table 37: RS.CO references

Analysis
It is ensured that regular analyses are conducted to permit an effective response to cybersecurity incidents.

Designation	Task
RS.AN-1	Ensure that notifications from detection systems are noted and investigated.
RS.AN-2	Ensure that the impact of a cybersecurity incident is properly understood.
RS.AN-3	Conduct a forensic analysis after any incident that occurs.
RS.AN-4	Establish processes to receive, analyse and respond to vulnerabilities that become known to the organisation from internal and external sources.

Table 38: RS.AN tasks

Standard	Reference
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

Table 29: RS.AN references

Mitigation
Act to prevent the further spread of a cybersecurity incident and to limit the potential damage.

Designation	Task
RS.MI-1	Ensure that cybersecurity incidents can be contained and their further spread blocked.
RS.MI-2	Ensure that the impact of cybersecurity incidents can be mitigated.
RS.MI-3	Ensure that newly identified vulnerabilities are reduced or documented as accepted risks.

Table 40: RS.MI tasks

Standard	Reference
COBIT 2019	none
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

Table 41: RS.MI references

Improvements
It is ensured that the organisation's capacity to respond to cybersecurity incidents improves continuously by learning lessons from previous incidents.

Designation	Task
RS.IM-1	Ensure that the findings and lessons of previous cybersecurity incidents are incorporated into your response plans.
RS.IM-2	Update your response strategies.

Table 42: RS.IM tasks

Standard	Reference
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

Table 43: RS.IM references

5.6 Recover

Recovery planning

It is ensured that the recovery processes can be prepared and then carried out in such a way that the systems can be recovered promptly.

Designation	Task
RC.RP-1	Ensure that recovery plans can be executed properly after any cybersecurity incident.

Table 44: RC.RP tasks

Standard	Reference
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

Table 45: RC.RP references

Improvements
It is ensured that recovery procedures improve continuously by learning lessons from previous recoveries.

Designation	Task
RC.IM-1	Ensure that the findings and lessons of previous cybersecurity incidents are incorporated into your response plans.
RC.IM-2	Update your recovery strategy.

Table 46: RC.IM tasks

Standard	Reference
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

Table 47: RC.IM references

Communications
Coordinate your recovery activities with internal and external partners, e.g. internet service providers, CERT, authorities, system integrators, etc.

Designation	Task
RC.CO-1	A prior communication plan exists for public relations work in connection with the cybersecurity incident.
RC.CO-2	Following a cybersecurity incident, the organisation works to restore its good reputation.
RC.CO-3	Communication of recovery activities to internal and external stakeholders, in particular to management and the executive board.

Table 48: RC.CO tasks

Standard	Reference
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

Table 49: RC.CO references

6 Modules for improving information security

The assessment framework used in section 5 provides comprehensive support for surveying and planning the improvement of cybersecurity in memory institutions. Larger organisations with the appropriate resources and trained staff (e.g. at cantonal or federal level) will be able to implement this recommendation in full. It is possible that these stakeholders are already using the framework proposed in this document or a similar one. However, cultural heritage management is made up of very heterogeneous stakeholders. Some critical infrastructures are more similar to a small or micro-enterprise in terms of staff numbers and the resources they have available for information security. Comprehensive implementation of the framework will pose major challenges for such institutions. To take this fact into account and still implement an effective defence-in-depth strategy, we recommend that smaller institutions focus on the key modules for improving information security enumerated in the following section.

A small institution usually has a small digital collection, little public traffic and limited human and financial resources. This could be the communal archive of a small town or a specialist archive that collects holdings and bequests on a specific subject area. This section will explain how such an institution can implement the key points of a defence-in-depth strategy (section 4) with minimal resources. Small memory institutions are often integrated into larger IT organisations (e.g. city, cantonal or university IT services). Every effort must be made in such cases to utilise synergies and integrate into the larger, overarching unit.

Accordingly, it will not be necessary for every institution to implement all measures, but rather focus on those that are necessary to protect its own critical processes and IT systems. A collection of measures and recommendations for increasing information security is provided by the IT baseline security modules of the German Federal Office for Information Security (BSI).[26] The modules are divided into the three categories already described in section 4, Defence in depth:

- Organisational measures (security management, organisation and processes)
- Technical measures (systems)
- Physical measures (buildings, rooms)

The NIST Framework says **what** needs to be done, in the sense of an assessment. The following section with the IT baseline security modules provides ideas on **how** this can be done.

26 The modules are available at: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

6.1 Security management

The aim of this module is to establish comprehensive security management in the institution in order to anchor information security as a continuous process.

The measures in this module include the definition of security objectives and requirements, the introduction of security processes, the definition of roles and responsibilities, training and awareness of employees and the establishment of emergency plans.

This module is intended to establish a culture of systematic and continuous improvement in information security within the organisation. Comprehensive security management aims to minimise risks and achieve an appropriate level of security for IT systems and data.

Standard	Reference
BSI IT-G 2023	ISMS.1

6.2 Process modules

Organisation

The aim of the organisation module is to create an effective and efficient organisation that is able to proactively identify and minimise IT security risks.

The measures in this module include the definition of organisational structures and processes with regard to information security, the assignment of roles and responsibilities and the creation of security guidelines. Given that most archives are embedded in a higher-level official IT structure, functional and technical responsibilities must be clarified.

The organisation module also emphasises close cooperation and communication between the various departments and employees of a company or authority. The aim is to create a common understanding of the importance of information security and to involve all stakeholders in the security processes. As mentioned, this is very important when harmonising the field-specific and technical requirements between the archive and the IT service.

By implementing the measures in the organisation module, an institution can develop its organisational structure in such a way that information security becomes an integral part of its business operations.

Standard	Reference
BSI IT-G 2023	ORP.1

Staff

This module deals with information security in connection with the staff of an institution. The aim is to ensure that employees are sufficiently aware of and trained to contribute to the security of IT systems and data.

The measures in this module include defining security requirements for employees, raising awareness and training in relation to information security, and compliance with security regulations. Precautions must be taken to minimise the loss of expertise in the event of staff absences, e.g. in the event of a pandemic. In addition, the qualifications of selected information security employees must be further developed in a targeted manner.

A further measure for institutions with sensitive and security-relevant data is to carry out a personnel security screening when hiring new staff.[27]

Standard	Reference
BSI IT-G 2023	ORP.2

27 At the federal level, this is the responsibility of the Personnel Security Screening Unit (PSS Unit) in the DDPS: https://www.vbs.admin.ch/de/sicherheit/integrale-sicherheit/personensicherheitspruefung.html

Awareness and training

This module aims to raise the awareness and train employees of companies and authorities with regard to information security. This is essential if they are to adequately perform their information security tasks and contribute to minimising risks.

The measures in this module include defining training and awareness objectives, selecting suitable training formats and methods, and planning and implementing training and awareness measures.

Training and awareness measures should be tailored to the specific needs and requirements of staff, including in relation to the specific risks to which an institution is exposed. The measures should be implemented regularly, especially with new employees, and the management level should also be involved in order to emphasise the importance of information security in the institution.

Standard	Reference
BSI IT-G 2023	ORP.3

Identity and authorisation management

This module deals with the management of identities and authorisations within an institution. The aim of the module is to ensure that only authorised persons have access to IT systems and data.

The measures in this module include defining roles and authorisations for employees, implementing access control mechanisms, checking identities and authorisations and carrying out access control audits. A key measure is the separation of identity and authorisation management of office systems and the digital archive.

The identity and authorisation management module also includes appropriate management of access data and the use of two-factor authentication to increase access security.

Standard	Reference
BSI IT-G 2023	ORP.4

Compliance management

This module deals with compliance with legal, regulatory and contractual requirements in the area of information security. The aim of the module is to ensure that the institution fulfils the relevant requirements, thereby minimising legal and regulatory risks.

The measures in this module include identifying and monitoring legal, regulatory and contractual requirements, integrating compliance requirements into the IT security concept, documenting compliance requirements and performing compliance checks. Archiving norms and standards as well as best practices are of particular importance in this context.

The compliance management module also includes a regular review of compliance with requirements and the integration of compliance aspects into the planning and implementation of IT projects. This includes interfaces to the critical sub-sector of administration, in that archiving must already be taken into account when planning and introducing new systems.

Standard	Reference
BSI IT-G 2023	ORP.5

Data protection

This module deals with the protection of personal data within an organisation. The aim of the module is to ensure that personal data is processed and protected in accordance with legal requirements.

The measures in the module include carrying out data protection impact assessments, implementing technical and organisational measures to protect personal data, training employees in the handling of personal data and checking compliance with data protection requirements.

The data protection module focuses on compliance with data protection principles such as data minimisation, purpose limitation and transparency, as well as safeguarding the rights of data subjects, such as the right to information, erasure or rectification.

By implementing the measures in this module, an institution ensures that personal data is processed and protected in accordance with legal requirements, which strengthens the trust of users and the entities transferring data and minimises legal risks.

Standard	Reference
BSI IT-G 2023	CON.2

Data backup concept

This module deals with the creation and implementation of a concept for backing up archive data and metadata. The aim of the module is to ensure the availability and integrity of this data and to minimise the risk of data loss.

The measures in the module include the creation of a data backup concept that covers the frequency and type of data backups, the storage of backup copies and the verification of backups. In addition, the recovery and integrity check of data after a data loss and the implementation of backup procedures are also set out.

For digital archive records, the data backup concept should be based on at least three independent, synchronised copies. If an error occurs on one of the copies, the data is restored from another copy. The concept design should take the following points into account:

- Geographically distributed storage systems
- Use of different fire compartments for productive and backup systems
- Offline storage
- Storage systems with self-healing mechanisms to correct any errors
- Manual (rather than automatic) triggering of backup and replication processes to prevent the spread of ransomware.

The data backup concept module also includes identifying and assessing risks in connection with data backup and adapting the data backup concept to changing requirements and risks over time.

Standard	Reference
BSI IT-G 2023	CON.3

Deletion and destruction

There are certainly cases where archive data must be deleted. For example, because their formats have become obsolete and they have been converted into new formats or because a re-evaluation has shown that they are no longer classified as suitable for archiving.

This module deals with the secure and final deletion of data and the destruction of an institution's data carriers. The aim of the module is to ensure that archive data (especially confidential or personal data) does not fall into the wrong hands and cannot be used without authorisation.

The measures in the module include the creation of guidelines and procedures for the secure deletion of data, the precise identification of the data and metadata that must be deleted and the definition of procedures for the destruction of data carriers. This includes documentation of the deletion process. In addition, training of staff in handling the secure deletion of data and verification of compliance with deletion and destruction procedures are also covered.

Standard	Referenz
BSI IT-G 2023	CON.6

Own operation

This module deals with securing IT systems and infrastructures that an institution operates itself. The aim of the module is to ensure the availability, integrity and confidentiality of the data and IT systems, thereby minimising the risk of disruptions and attacks.

The measures in this module include creating IT security guidelines, implementing access and authorisation controls, monitoring IT systems and networks and performing regular IT security audits. The physical protection of server rooms and emergency planning are also covered. The module includes the planning of these measures and refers to the necessary system modules.

The own operation module also takes into account new developments and technologies as well as adaptation of IT security measures to changing risks and threats.

Small institutions, some of which rely on volunteers, often fall into this category. The demands on own operation are high, and these institutions are advised to examine operation by third parties (cloud) in depth.

Standard	Referenz
BSI IT-G 2023	OPS.1

Operation by third parties (cloud)

This module deals with securing IT systems and infrastructures operated by an external service provider. The aim of the module is to ensure the availability, integrity and confidentiality of the data and IT systems, thereby minimising the risk of disruptions and attacks.

The measures in this module include defining security requirements for the service provider, carrying out security audits of the service provider, defining responsibilities and obligations as part of the outsourcing contract and conducting regular IT security audits. Monitoring of service level agreements (SLAs) and emergency planning are also covered.

An important aspect of this module is the selection of suitable service providers and the consideration of security aspects when drawing up contracts.

Standard	Referenz
BSI IT-G 2023	OPS.2

6.3 System modules

Servers

This module deals with securing servers and server environments in IT systems. The aim of the module is to ensure the availability, integrity and confidentiality of the data and IT systems, thereby minimising the risk of disruptions and attacks.

The measures in this module include physical protection of server rooms, implementation of access and authorisation controls, use of encrypted communication, regular security updates and backup and recovery mechanisms. Server monitoring and emergency planning are also covered.

An important aspect of this module is the consideration of new developments and technologies as well as the adaptation of IT security measures to changing risks and threats.

Standard	Reference
BSI IT-G 2023	SYS.1

Storage solutions

This module deals with securing storage solutions in IT systems. The aim of the module is to ensure the availability, integrity and confidentiality of the data and IT systems, thereby minimising the risk of disruptions and attacks. This module essentially implements the data backup concept of module CON.3.

The measures in this module include physical protection of storage solutions, implementation of access and authorisation controls, use of encrypted communication, regular security updates and synchronisation and backup mechanisms.

Implementation of the measures is intended to ensure that storage solutions are adequately protected and that failures or attacks can be quickly recognised and responded to.

Standard	Reference
BSI IT-G 2023	SYS.1.8

Desktop systems

This module deals with securing desktop systems in IT environments. The aim of the module is to ensure the availability, integrity and confidentiality of the data and IT systems, thereby minimising the risk of disruptions and attacks.

The measures in this module include physical protection of workstations, implementation of access and authorisation controls, use of encrypted communication, regular security updates and backup and recovery mechanisms. The operating system, installed software and virus protection must be kept up to date. Software that is outdated or no longer required must be uninstalled. Desktop system monitoring and emergency planning are also covered.

An important aspect of this module is the consideration of new developments and technologies as well as the adaptation of IT security measures to changing risks and threats.

Standard	Reference
BSI IT-G 2023	SYS.2

Removable media
This module deals with the secure use of USB sticks, external hard drives and other mobile storage media in IT systems. The aim of the module is to minimise the risk of data loss, theft or manipulation through the use of removable media and to ensure the confidentiality, integrity and availability of data.

The measures in this module include defining guidelines for the use of removable media, implementing mechanisms to detect and defend against malware on removable media, and training and raising the awareness of employees with regard to the secure use of removable media. Loss or theft of a data carrier can occur, but with suitable measures such as encryption, the impact is minimal. Removable media can suffer defects. They can be used as part of a backup strategy, but never as the only copy of the data.

The monitoring and logging of activities in connection with removable media and the regular review and updating of security measures are important in the removable media module.

Standard	Reference
BSI IT-G 2023	SYS 4.5

Network
This module deals with the security of networks in IT systems. The aim of the module is to ensure the confidentiality, integrity and availability of the data in networks, thereby minimising the risk of attacks and data loss.

The measures in this module include defining guidelines and processes for network architecture, network segmentation and network management. Other measures include implementation of firewalls, intrusion detection systems and encryption of network connections. One key measure is the separation of office systems and digital archives at network level. Rules must also be created on the firewall not only for incoming but also for outgoing data flow so as to prevent uncontrolled data leaks. In principle, all network connections between the areas and individual computers must be encrypted. When archive data is transferred, transactional integrity must be ensured by comparing checksums before and after the transfer.

The network module also emphasises monitoring and logging of network activities, regular checking and updating of network devices and systems, and training and raising the awareness of employees with regard to the secure use of networks.

Standard	Reference
BSI IT-G 2023	NET.1

6.4 Physical modules

Buildings in general
This module deals with the physical aspects of the security of buildings in which IT systems are operated. The aim of the module is to ensure the confidentiality, integrity and availability of IT systems and data through suitable building security measures. Unauthorised physical access to sensitive locations such as server rooms and data centres should be prevented.

The measures in the module include securing entrances, windows and other building access points, monitoring visitors and guests, and installing security systems such as surveillance cameras, alarm systems and access control systems.

This module also includes the availability of emergency plans and the training of staff in handling emergencies such as fires, floods and other natural disasters.

Standard	Reference
BSI IT-G 2023	INF.1

Data centre, server room

This module deals with the specific requirements for the security of data centres and server rooms in which IT systems are operated. The aim of the module is to ensure the confidentiality, integrity and availability of IT systems and data through suitable security measures.

The measures in the module include securing access points to data centres, monitoring visitors and guests, and installing security systems such as surveillance cameras, alarm systems and access control systems. This module also includes suitable air conditioning and fire extinguishing systems in the data centre or server room to prevent damage caused by overheating or fires.

In addition to these general measures, specific measures apply to digital archive records. At least three copies of the archive records must be kept in at least two locations. The locations must be located in different earthquake zones. If only two locations are selected for the three copies, the duplicate hardware at one location must be located in different fire protection zones.

In addition, the data centre and server room module also includes recommendations for the design of the technical infrastructure, such as the power supply, network architecture and server infrastructure.

Standard	Reference
BSI IT-G 2023	INF.2

Data carrier archive

This module deals with the secure storage and archiving of data carriers in IT systems. The aim of the module is to ensure the confidentiality, integrity and availability of the data stored on data carriers to minimise the risk of loss, theft or manipulation. The measures set out in the removable media and data carrier archive modules protect the data even in the event of a power failure and form an important safety net in the context of disaster recovery.

The measures in the module include defining processes for physical and logical access control to premises of the data carrier archive, implementing security measures such as encryption and labelling for the data carriers themselves, and defining procedures for the secure destruction of data carriers at the end of their life.

The data carrier archive module also includes the regular review and updating of security measures and training and raising awareness among staff who have access to the data carrier archive.

Standard	Reference
BSI IT-G 2023	INF.6

7 Literature and resources

BSI
Federal Office for Information Security (Germany).
BSI 100-2.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.html

BSI IT-G (2023)
Federal Office for Information Security (Germany).
IT baseline security modules.
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
The CoreTrustSeal foundation offers certification of digital archives and repositories on the basis of the Core Trustworthy Data Repositories Requirements.
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
Same text:
https://public.ccsds.org/pubs/650x0m2.pdf

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

ISO 2700x
The International Organization for Standardization (ISO) publishes around a dozen mutually complementary standards on cybersecurity. These are referred to as the '2700x family'. The best-known of these is ISO 27001. It specifies the requirements for setting up, implementing, maintaining and continuously improving a documented information security management system compatible with the context of the organisation concerned.
https://www.iso.org/standard/73906.html

Critical infrastructure protection guide
Federal Office for Civil Protection (ed.) (2018).
https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/27228b5a-2d7c-4c17-9df6-42e105197465.pdf

nestor Catalogue of Criteria
nestor Working Group Trusted Repositories – Certification (2008). Catalogue of Criteria for Trusted Digital Repositories.
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 Glossary and list of abbreviations

Asset	In this context: data, people, devices, systems and facilities of an organisation.
Authenticity	In the field of digital archiving, the term means that a file actually contains what it claims to be. Largely used synonymously with trustworthiness.
AV archive	Archive of audiovisual media
FOCP	Federal Office for Civil Protection
Backup	A backup is a copy of data that is created to enable recovery in the event of data loss or data corruption. These copies are made regularly and stored in a secure location.
FOC	Federal Office of Culture
SFA	Swiss Federal Archives
Bitstream preservation	Refers to the process of long-term preservation and recovery of digital bitstreams to ensure the integrity and continued usability of digital content.
ArchA	Federal Act of 26 June 1998 on Archiving (Archiving Act, ArchA; SR 152.1)
FONES	Federal Office for National Economic Supply
Compliance	Compliance is the business and legal term for a company's adherence to rules, i.e. compliance with laws, guidelines and voluntary codes.
Cybersecurity	Cybersecurity refers to the protection of computers, networks and data against attacks from the internet or other networks. It includes measures to defend against cyberthreats (--> threats) in order to secure digital infrastructures.
Data at rest	Data at rest refers to stored or dormant data located on physical or electronic storage media.
Data in transit	Data in transit refers to data during transmission in networks or communication channels.
Defence in depth	A cybersecurity approach that implements multiple layers of security measures to protect systems and data. The aim is to create redundant security barriers so that a single failure of a protective measure does not lead to compromising of the entire security.
DH Lab	Digital Humanities Lab, University of Basel

8 Glossary and list of abbreviations

Digital cultural property	The concept of cultural property, as defined in Art. 1 of the 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, serves as the main criterion for the selection of digital objects. Digital cultural property includes both digitally created (born digital) and digitised objects. The term 'collection' in this context is analogous to that used in archives, libraries and museums. It refers to a collection of digital archive records. In addition to digital archive holdings (e.g. digitised daily newspapers and audiovisual programme archives of a cantonal library), these digitally created items of cultural property also include digital art (e.g. digitally created collection of photographs in a museum), digital art reproduction and research data (site documentation of a cantonal archaeological service in the form of drone images or 3D models), digitally created preservation documentation, etc. Digital PCP objects are recorded and categorised as collections for inclusion in the PCP inventory.
DIMAG	Digital Magazine. Consortium for digital archiving in public archives.
DTI	Digital Transformation and ICT Steering Sector of the Federal Chancellery
Probability of occurrence	Probability of occurrence is the estimated occurrence of an event within a certain period of time (e.g. ten years) based on statistical values.
FCPCP	Federal Commission for the Protection of Cultural Property
Threat	A threat is defined as a specific danger that exists for a specific protected good. A threat corresponds to a potential event or a potential development with possible impacts on a protected good.
Information security	Information security protects information and information systems from unauthorised access, use, disclosure, modification or destruction. The aim is to guarantee the confidentiality, integrity and availability of data.
GEVER	(Electronic) records and process management
ICT	Information and communication technology
Integrity	Proof that data is correct and unchanged. Checksums are an important tool for this purpose.
Intangible cultural heritage	Intangible cultural heritage (as defined by the UNESCO Convention) means 'practices, representations, expressions, knowledge, skills – as well as the instruments, objects, artefacts and cultural spaces associated therewith – that communities, groups and, in some cases, individuals recognise as part of their cultural heritage.'[28] The UNESCO Convention identifies five domains: A. oral traditions and expressions, including language as a vehicle of the intangible cultural heritage; B. performing arts; C. social practices, rituals and festive events; D. knowledge and practices concerning nature and the universe; E. traditional craftsmanship.
PCP	Protection of cultural property
CPPA	Federal Act of 20 June 2014 on the Protection of Cultural Property during Armed Conflicts, Disasters and Emergencies (SR 520.3)
Critical infrastructures	Critical infrastructures are processes, systems and facilities that are essential for the functioning of the economy or the well-being of the population.

28 Art. 2 of the Convention for the Safeguarding of the Intangible Cultural Heritage (SR 0.440.6), adopted in Paris on 17 October 2003.

8 Glossary and list of abbreviations

Critical processes	In the context of critical infrastructure protection, a critical process is a process that is vital to the functioning of the critical infrastructure and whose failure would severely affect the population and its basic needs.
Cultural heritage	Cultural heritage is used as an umbrella term encompassing all immovable and movable cultural property as well as intangible cultural heritage.
Cultural property	The 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict defines the term as 'movable or immovable property of great importance to the cultural heritage of every people, such as monuments of architecture, art or history, whether religious or secular; archaeological sites; groups of buildings which, as a whole, are of historical or artistic interest; works of art; manuscripts, books and other objects of artistic, historical or archaeological interest; as well as scientific collections and important collections of books or archives or of reproductions of the property defined above'.[29] The distinction between movable and immovable cultural property must be emphasised.
NESA	National Economic Supply Act
NL	Swiss National Library
NCSC	National Cyber Security Centre
NCHA	Federal Act of 1 July 1966 on the Protection of Nature and Cultural Heritage (SR 451)
NIST	The National Institute of Standards and Technology (NIST) is a US federal agency which has published a cyber risk management framework.
OAIS	Open Archival Information System, ISO 14721. Reference model for digital archives
OPAC	Open Public Access Catalogue
Preservation planning	Preservation planning in long-term archiving pursues the goal of keeping archived content available in the long term.
Records management	Records management encompasses the systematic administration of records and information throughout their entire life cycle, from creation or capture, through filing and storage, to final archiving or destruction.
Resilience	Resilience describes the ability of a system, organisation or society to withstand internal or external disruptions and to maintain or regain functionality as far as possible. Resilience is made up of four components: 1. the robustness of the systems themselves (e.g. critical infrastructures, state, economy and society); 2. the availability of redundancies; 3. the ability to mobilise effective aid measures; 4. the speed and efficiency of the aid measures.
Risk	Risk is a measure of the magnitude of a threat and includes the probability of occurrence and the extent of the damage caused by an undesirable event.
Extent of damage	The extent of damage is defined as the estimated impact on the population and their basic needs resulting from the failure of one or more critical processes when the threat materialises. It consists of the sum of the damage at the time of the occurrence of an event and the damage that may occur during the entire recovery period.

29 Art. 1 of the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict (SR 0.520.3), adopted in The Hague on 14 May 1954.

8 Glossary and list of abbreviations

Critical infrastructure protection	Critical infrastructure protection includes measures that reduce the probability of occurrence and/or the extent of damage caused by the disruption, failure or destruction of critical infrastructures, or that minimise the resulting downtime.
SR	Swiss law
Synchronisation	Synchronisation is the process of reconciling data between two or more systems to ensure that all systems involved have the same data status. This is done either in real time or at regular intervals to ensure that the data is consistent and up to date.
Sub-sector	The critical infrastructures in Switzerland are divided into 28 sub-sectors. These sub-sectors include the various industries, economic sectors and other economic subdivisions. The following critical infrastructure sub-sectors exist in Switzerland: refuse, sewage, armed forces, medical care and hospitals, diplomatic missions and headquarters of international organisations, banks, emergency services, chemical and pharmaceutical industry, natural gas supply, oil supply, research and teaching, information technologies, cultural property, laboratories, food supply, air transport, mechanical, electrical and metal industry, media, parliament – government – justice – administration, postal service, rail transport, water transport, road transport, power supply, telecommunications, insurance, water supply and civil defence.

Further glossaries and definitions of terms:

- Glossary of Risk Terms, Federal Office for Civil Protection FOCP, 29.4.2013.
  Available in German, French and Italian
  https://www.babs.admin.ch/en/hazards-and-risks

- Glossary in the Critical Infrastructure Protection Guide, 2018.
  Available in German, French and Italian.
  https://www.babs.admin.ch/de/leitfaden-schutz-kritischer-infrastrukturen

8 Glossary and list of abbreviations

Authors and technical experts of the first edition

Surname	First name	Organisation	Position
Wildi	Tobias	FCPCP University of Applied Sciences of Graubünden	PM/Main author
Fornaro	Peter	Digital Humanities Lab, University of Basel	Review
Müller	Stefanie	University of Applied Sciences of Graubünden	Review

Timeline

Date	Brief description
2018	FCPCP decision to develop a Minimum ICT Standard
Jan – Jul 2023	Preparation of first draft
Aug – Nov 2023	Consultation with offices and cantons
Dec 2023	Revision and second draft
Jan – Mar 2024	Consultation with cantons
Apr – Jul 2024	Revision and final version
November 2024	Acceptance by FCPCP
Aug – Dec 2024	Translation and publication

Licence