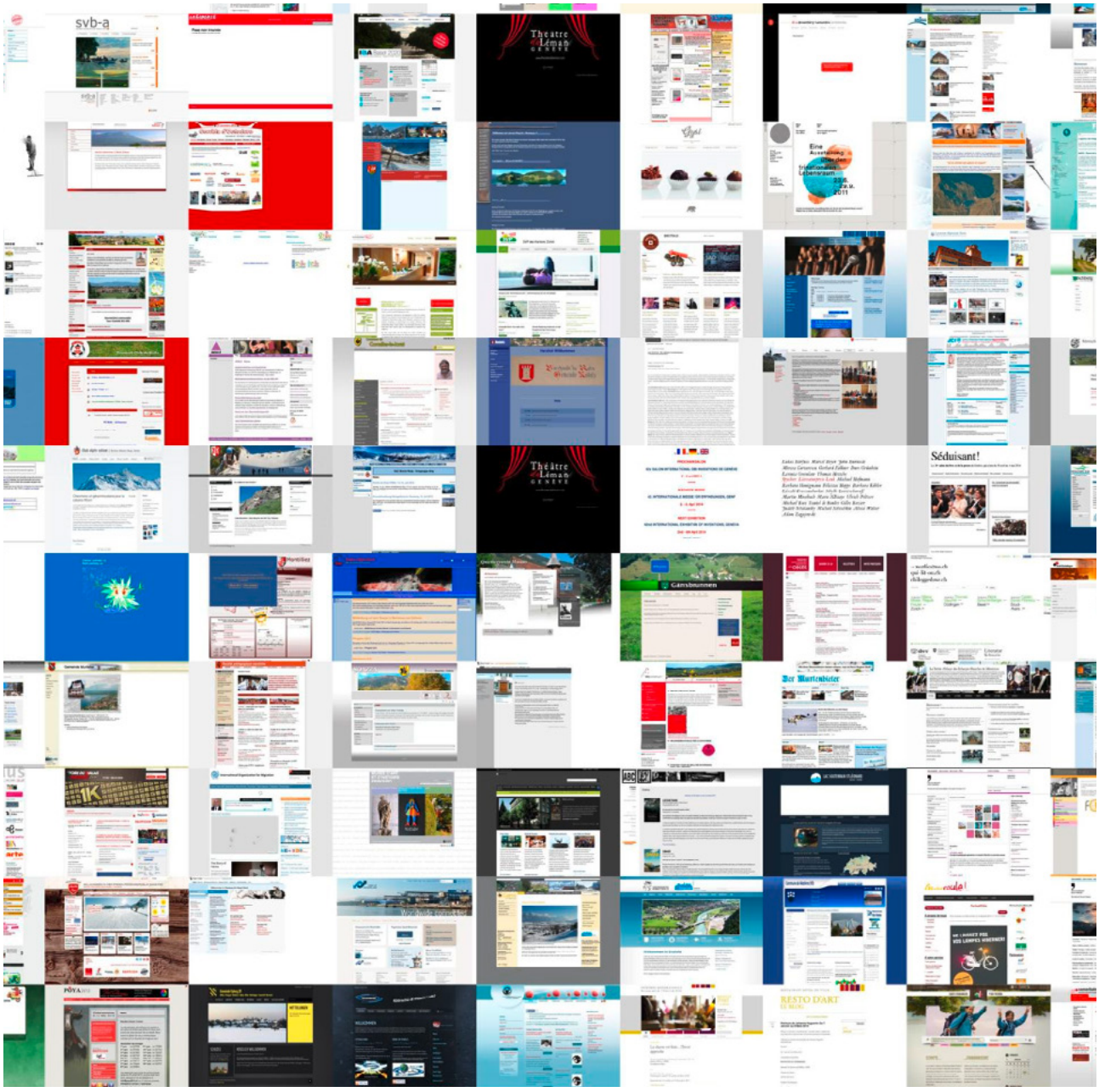
Norme minimale pour la sécurité des technologies de l'information et de la communication (TIC) relatives aux biens culturels numériques



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de la protection de la population OFPP

État au 19.02.2025

Couverture :
Archives Web Suisse, Bibliothèque nationale suisse (BN), page d'accueil sous forme de collage.
https://www.e-helvetica.nb.admin.ch/collage/

Auteur :
Tobias Wildi, Haute école spécialisée des Grisons, docuteam AG

Éditeur :
Office fédéral de la protection de la population (OFPP)
Division Protection civile et formation
Section Bases Protection civile et formation
Groupe Protection des biens culturels
kulturgueterschutz@babs.admin.ch
www.kgs.admin.ch

Les liens ont été testés pour la dernière fois le 8 juillet 2024.

Avant-propos

Dans sa Stratégie Suisse numérique , le Conseil fédéral souligne sa volonté d'exploiter au mieux les opportunités de la transformation numérique de la Suisse. Aujourd'hui, il est difficile d'imaginer la gestion de services d'archives sans les technologies de l'information et de la communication (TIC). La présente norme minimale pour la sécurité des technologies de l'information et de la communication (norme minimale TIC) a été élaborée sous forme de recommandation pour les organisations de conservation du patrimoine et met l'accent sur la sécurité de l'archivage numérique à long terme, en particulier la sauvegarde des données au repos dans le domaine des biens culturels numériques (voir le glossaire).

La Commission fédérale de la protection des biens culturels (CFPBC) contribue à l'amélioration de la résilience des biens culturels numériques en collaboration avec l'Office fédéral de la protection de la population (OFPP) et des experts externes. Il est nécessaire que les organisations concernées adhèrent à cette norme. La présente première version de la norme minimale TIC devra donc être régulièrement mise à jour et, si nécessaire, étendue.

En raison de la numérisation croissante de l'administration (gestion électronique des affaires GEVER, applications spécialisées), la quantité d'archives numériques a fortement augmenté au cours des dernières années. Parallèlement, la dématérialisation des processus crée de nouveaux risques dont il faut tenir compte. Les cyberattaques contre les infrastructures informatiques concernent aussi bien les organismes gouvernementaux que les exploitants d'infrastructures critiques et les institutions culturelles (musées, bibliothèques). La conservation du patrimoine culturel, même analogique, repose aujourd'hui sur des données numériques telles que des documents numérisés, des bases de données d'inventaires et de catalogues, ainsi que des documentations de sécurité ou des documents archéologiques numériques.

Les biens culturels numériques sont encore plus importants lorsque les biens culturels originaux ne sont plus disponibles ou que les objets ont été créés directement sous forme numérique. L'archivage à long terme de ces objets numériques soulève la question essentielle de la signification de *« long terme »*. Il s'agit de faire en sorte que les données restent utilisables sur plusieurs générations d'architectures de processeur, de systèmes d'exploitation et de formats de fichiers. Les mesures nécessaires à cet effet vont au-delà de la simple sauvegarde des données et des backups. La réflexion archivistique s'inscrit dans des périodes de plusieurs décennies et siècles. La présente norme minimale tient compte de ce contexte particulier.

1 Voir https://digital.swiss/fr/strategie/strategie-suisse-numerique.html

Résumé

La présente norme minimale TIC sert de recommandation et de guide pour améliorer la résilience TIC dans les organisations en charge de la maintenance et de la conservation des biens culturels numériques. Elle s'adresse en premier lieu aux exploitants d'infrastructures critiques, notamment aux directions et aux responsables TIC. L'objectif est d'identifier les risques et de les réduire à un niveau acceptable.

La norme minimale TIC propose un cadre axé sur la sécurité à long terme des biens culturels numériques et visant à atteindre un niveau de sécurité adéquat contre les cyberattaques ainsi que d'autres dangers. Après un incident, il doit être possible de revenir à la situation normale le plus rapidement possible. Pour la planification, on utilisera le « NIST Cybersecurity Framework »[2], permettant aux organisations d'évaluer systématiquement leurs risques et de faire le point sur l'état d'avancement de leurs mesures pour les contrer. La mise en œuvre d'une stratégie de « défense en profondeur », stratégie à plusieurs niveaux face aux cybermenaces, est au cœur de la recommandation.

De nombreux éléments concrets sont également mentionnés pour améliorer la résilience ; ils concernent les catégories suivantes : gestion de la sécurité, organisation et processus, modules du système et éléments physiques. La norme minimale s'adresse aussi bien aux grandes qu'aux petites organisations œuvrant pour la conservation du patrimoine culturel.

La présente norme est structurée sur le modèle de la « Norme minimale TIC – 2023 »[3] de l'Office fédéral pour l'approvisionnement économique du pays (OFAE).

2 La norme du National Institute of Standards and Technology (États-Unis) est disponible sous : https://www.nist.gov/cyberframework.

3 Le document est disponible sous : https://www.bwl.admin.ch/bwl/fr/home/bereiche/ikt/ikt_minimalstandard.html.

Table des matières

1 Contexte et objectifs

De nombreux biens culturels sont aujourd'hui produits, archivés et utilisés sous forme numérique. Font par exemple partie du patrimoine culturel numérique les archives publiques (archives fédérales, archives cantonales et archives communales), les collections des bibliothèques (archives photographiques, fonds d'auteurs, données de recherche) ou des musées (art vidéo et art en réseau, fonds photographiques). L'utilisation et la protection de ces biens culturels requièrent des outils numériques tels que des documentations de sécurité, des inventaires, des catalogues et des documents numérisés.

La conservation des biens culturels numériques est essentielle. En Suisse, certains biens culturels font partie des infrastructures critiques qui contribuent au fonctionnement de la société et au maintien de l'ordre et de la sécurité. Les fonds d'archives contribuent particulièrement à la sécurité juridique. On y trouve des documents importants tels que des textes de lois, des contrats, des actes et des décisions de justice.

Le présent rapport est principalement axé sur les archives, mais ses principes sont applicables à d'autres institutions qui gèrent des biens culturels numériques, comme les bibliothèques, les musées, les services de la conservation des monuments historiques, les services archéologiques et les centres de documentation, quel que soit leur mode d'organisation. Comme dans tous les secteurs, les biens culturels numériques sont exposés à de multiples dangers. La présente norme minimale TIC doit permettre aux institutions culturelles de renforcer leur infrastructure TIC. Basée sur les risques, la norme permet de mettre place différents niveaux de protection adaptés aux besoins spécifiques des organisations.

Le chapitre 3 du présent document propose une vue d'ensemble des systèmes et processus critiques à protéger. Le chapitre 4 présente le concept de la défense en profondeur, c'est-à-dire la défense à plusieurs niveaux contre les cyberdangers. Le chapitre 5 dédié au « NIST Cybersecurity Framework » propose ensuite une approche basée sur les risques pour analyser et gérer les cyberrisques. Enfin, le chapitre 6 propose des mesures de sécurité concrètes, réparties dans les catégories suivantes : gestion de la sécurité, organisation et processus, modules du système et éléments physiques.

1.1 Contexte et aperçu

Le Rapport sur la résilience dans le sous-secteur critique des biens culturels[4], mis à jour par l'OFPP en 2021, indique que les processus utilisés dans les archives et les bibliothèques sont aujourd'hui très dépendants des TIC. Compte tenu de ce fait, les cyberattaques contre ces institutions représentent un risque pour l'ensemble de la société.

À l'avenir, il faut s'attendre non seulement à une forte augmentation des fonds numériques dans les archives et les bibliothèques mais aussi à une croissance de la centralisation en matière de gestion des données, par exemple sous la forme de réseaux d'archivage, de coopérations ou de centres de calcul exploités en commun. Mentionnons à titre d'exemple le réseau d'archivage DIMAG[5] Suisse, auquel se sont associés plusieurs cantons. Si les réseaux numériques permettent de créer des synergies pour l'exploitation d'infrastructures nécessitant une lourde maintenance, ils représentent un risque accru en cas de cyberattaque ciblée ou de panne des systèmes TIC.

4 Rapport interne. Une fiche d'information est disponible sous : https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/b4b28e9b-a5e8-4ce0-8402-b374c5d6c928.pdf.

5 DIMAG (abréviation de Digitales Magazin) est un ensemble de solutions logicielles pour l'archivage numérique à long terme de documents de l'administration publique. DIMAG a été développé par les services d'archives des Länder allemands Bade-Wurtemberg et Hesse ainsi que de l'État libre de Bavière.
Les cantons de Soleure, de Schaffhouse et d'Argovie ont fondé en 2019 le réseau d'archives DIMAG Suisse. Voir aussi : https://www.eoperations.ch/fr/service/secretariat-dimag/.

L'analyse des risques détaillée effectuée dans le cadre du rapport précité a permis d'examiner le potentiel dommageable d'une cyberattaque ciblée sur des archives cantonales ou sur des systèmes TIC cantonaux pour les processus archivistiques. Le rapport montre clairement que les attaques et les pannes de l'infrastructure TIC qui en découlent peuvent affecter à long terme l'accès aux fonds et aux réseaux d'archives ainsi que leur disponibilité. En outre, on ne peut écarter le risque de destruction irréversible, de vol ou encore de publication intentionnelle ou involontaire d'informations sensibles.

1.2 Champ d'application et délimitations

La responsabilité de la protection des biens culturels numériques incombe en principe aux institutions qui les conservent et qui agissent sur la base d'un mandat légal ou à titre volontaire. Toutefois, lorsqu'il en va du bon fonctionnement des infrastructures critiques, il existe une responsabilité étatique en sus, fondée sur un mandat ancré dans la Constitution fédérale et dans la loi sur l'approvisionnement du pays (LAP)[6]. La présente norme minimale pour les TIC traduit cette responsabilité de l'État qui doit protéger ses citoyens, l'économie, les institutions et l'administration publique.

Cette norme s'adresse en premier lieu aux exploitants et aux responsables d'infrastructures critiques du sous-secteur des biens culturels, qui sont répertoriés dans l'Inventaire des infrastructures critiques (Inventaire PIC)[7]. Tous les objets de l'Inventaire PIC figurent également dans l'Inventaire PBC en tant qu'objets d'importance nationale (objets A)[8]. La recommandation de la branche se concentre sur les institutions (archives, bibliothèques, musées) disposant de fonds d'archives numériques, mais d'autres institutions au sein du sous-secteur des biens culturels peuvent également être concernées si elles disposent de fonds numériques. Il est recommandé aux exploitants d'infrastructures critiques de mettre en œuvre la norme minimale TIC. La norme offre en principe à tout acteur impliqué dans la conservation des biens culturels une aide et des éléments concrets pour améliorer la résilience des TIC.

Les biens culturels numériques sont souvent divisés en deux catégories : « born digital » et rétronumérisés. La présente norme minimale ne fait toutefois pas de distinction entre ces deux catégories, mais les considère équivalentes. Cela s'explique par le fait que la frontière entre ces concepts clairement délimités à l'origine est devenue de plus en plus floue au cours des dernières années. Outre la conversion analogique-numérique, la rétronumérisation est aujourd'hui généralement associée à des étapes de datafication. Il s'agit par exemple de la reconnaissance de texte ou de la reconnaissance vocale, de la « Named Entity Recognition » (NER) pour la conversion de texte en données structurées, de la vectorisation de plans, de la numérisation 3D dans le domaine de l'archéologie ou des objets de musée. En outre, les rétronumérisations servent de copies de sécurité pour les objets analogiques originaux et conservent un caractère original en cas de perte de ces derniers. Par conséquent, la valeur des biens culturels numériques ne dépend pas de la manière dont ils ont été créés, qu'ils soient « nés numériques » ou rétronumérisés.

Il existe déjà plusieurs normes en matière de sécurité informatique reconnues à l'échelle internationale (voir chap. 7 Références). La norme minimale TIC n'est pas en concurrence avec les normes existantes, mais est compatible avec elles, en étant toutefois plus succincte. Elle permet d'aborder plus facilement le sujet et constitue une aide pour prendre des mesures afin d'atteindre un niveau de protection adéquat. La recommandation se concentre sur les processus qui ont une influence directe sur la sécurité des biens culturels numériques, respectivement sur la sauvegarde des données au repos. Elle ne s'occupe pas ou seulement de manière très secondaire de la sécurité informatique administrative.

6 Loi fédérale du 17 juin 2016 sur l'approvisionnement économique du pays (LAP) ; RS 531 (état au 1er juillet 2023).

7 L'Inventaire PIC recense des éléments d'infrastructures critiques individuels qui revêtent une importance stratégique. L'inventaire de ces constructions et installations a été réalisé pour la première fois en 2012 en collaboration avec les cantons. Il est classifié et non accessible au public. Les services autorisés à y accéder (Confédération, cantons et exploitants) s'en servent comme base de planification et de priorisation dans le cadre de la gestion des risques et des événements.

8 L'Inventaire PBC 2021 est disponible sous : https://www.babs.admin.ch/fr/aufgabenbabs/kgs/inventar.html.

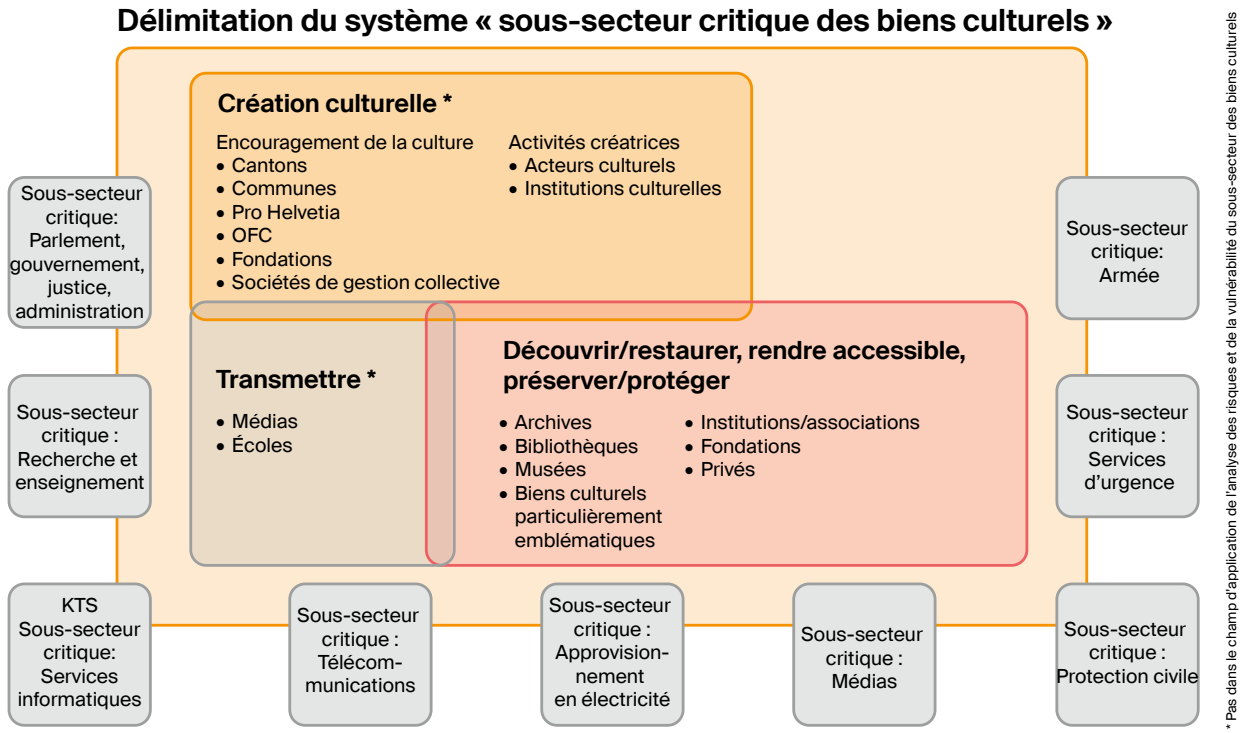


Figure : Limite du système du sous-secteur critique des biens culturels

1.3 Objectifs et structure de la norme minimale TIC

La présente norme minimale TIC est conçue comme une mesure préventive et formulée comme une recommandation sectorielle.

Le document se compose des chapitres suivants :

- Les chapitres 1 et 2 présentent les domaines de la protection des biens culturels concernés.
- Le chapitre 3 décrit les systèmes et processus critiques.
- Le chapitre 4 explique l'approche de défense en profondeur.
- Le chapitre 5 définit un cadre pour l'évaluation et la planification de la résilience.
- Le chapitre 6 formule des recommandations concrètes pour améliorer la résilience sous forme de modules organisationnels et techniques.

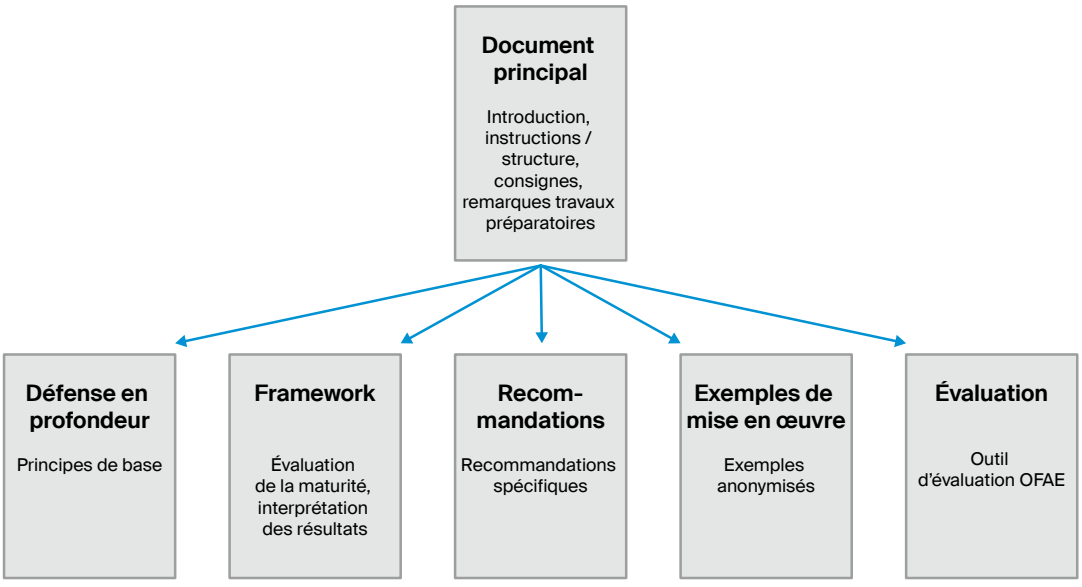


Figure : Aperçu des documents de la norme minimale TIC

Afin d'évaluer le niveau de maturité de l'entreprise ou de l'organisation, l'OFAE met à disposition un outil d'évaluation[9]. La norme minimale en matière de TIC est considérée comme appliquée si le niveau de maturité – selon le classement de l'outil d'évaluation – répond au moins aux exigences minimales de la cote globale, conformément à l'approche basée sur le risque propre à l'institution. Il est en principe recommandé d'adopter une approche basée sur les processus afin de garantir un contrôle et une amélioration réguliers et permanents.

1.4 Mise en œuvre de la norme minimale en matière de TIC

Le paysage institutionnel dans le domaine de la conservation des biens culturels est très hétérogène, notamment en ce qui concerne la taille, la mission et le type de financement. Toutes les institutions ne seront pas en mesure de mettre en œuvre la norme minimale TIC dans son intégralité. Les institutions plus petites et moins bien financées se concentreront sur quelques mesures de protection essentielles. Les propositions de mise en œuvre du chapitre 6, modulaires, constituent les éléments de base. Chaque institution peut donner la priorité aux modules qui la concernent en fonction de son profil (type de collection, risques). Selon la taille de l'institution, les recommandations de mise en œuvre suivantes s'appliquent :

Type d'institution	Exemples	Recommandations de mise en œuvre
Petite taille, ressources limitées, degré de professionnalisation bas.	Petites archives communales, archives spéciales avec un profil de collection ciblé.	Concentration sur les principaux éléments du chapitre 6.
Moyenne à grande taille, ressources assurées, degré de professionnalisation élevé.	Grandes archives communales, archives cantonales, archives fédérales, archives spéciales avec un profil de collections étendu.	Priorisation des éléments du chap. 6 en fonction du profil de risque, application de l'outil d'évaluation.

La mise en œuvre de la norme minimale TIC peut être abordée à l'aide du modèle de processus ci-dessous. Si les systèmes d'information des archives font partie de ceux de l'échelon supérieur (p. ex. ville, canton ou Confédération), la mise en œuvre peut se faire à ce niveau et englober d'autres infrastructures. Si ce n'est pas le cas ou si les archives doivent être sécurisées de manière autonome selon cette norme, l'étape suivante consiste à déterminer la catégorie d'institution : les petites institutions mettent en œuvre les éléments du chapitre 6 qui leur semblent prioritaires, les moyennes et grandes institutions appliquent intégralement la norme minimale TIC.

En principe, une approche basée sur les processus est recommandée, en particulier pour les grandes institutions. Cela signifie que la cybersécurité n'est pas une notion fixe. Il s'agit d'un processus évolutif à vérifier en permanence. La sécurité intégrale en matière de TIC n'est pas atteignable. Elle doit être constamment recherchée et faire l'objet de mises à jour périodiques.

1.5 Travaux préalables et bases légales

Selon la Constitution fédérale, les cantons sont souverains en matière de culture. Ils sont par ailleurs responsables des archives de droit public, conformément aux lois en la matière. La Confédération peut les soutenir à titre subsidiaire dans cette tâche. L'OFPP peut notamment soutenir et conseiller les cantons[10] dans le domaine de la protection des biens culturels.

Le 16 juin 2023, le Conseil fédéral a adopté la Stratégie nationale de protection des infrastructures critiques (stratégie PIC)[11], développée à partir des deux premières versions de 2012 et 2017, et a chargé l'OFPP de coordonner les tâches dans le domaine de la PIC. La stratégie PIC désigne 17 mesures visant à améliorer la résilience tant au niveau sectoriel qu'intersectoriel. La cyberstratégie nationale[12] indique clairement que, du point de vue de la politique économique et sociale, la Suisse doit absolument se protéger contre les cyberdangers afin de pouvoir exploiter de manière conséquente les opportunités offertes par la numérisation et de conserver son avantage en tant que pays sûr.

9 L'outil d'évaluation est disponible en format Excel sous : https://www.bwl.admin.ch/fr/normes-minimales-pour-les-tic

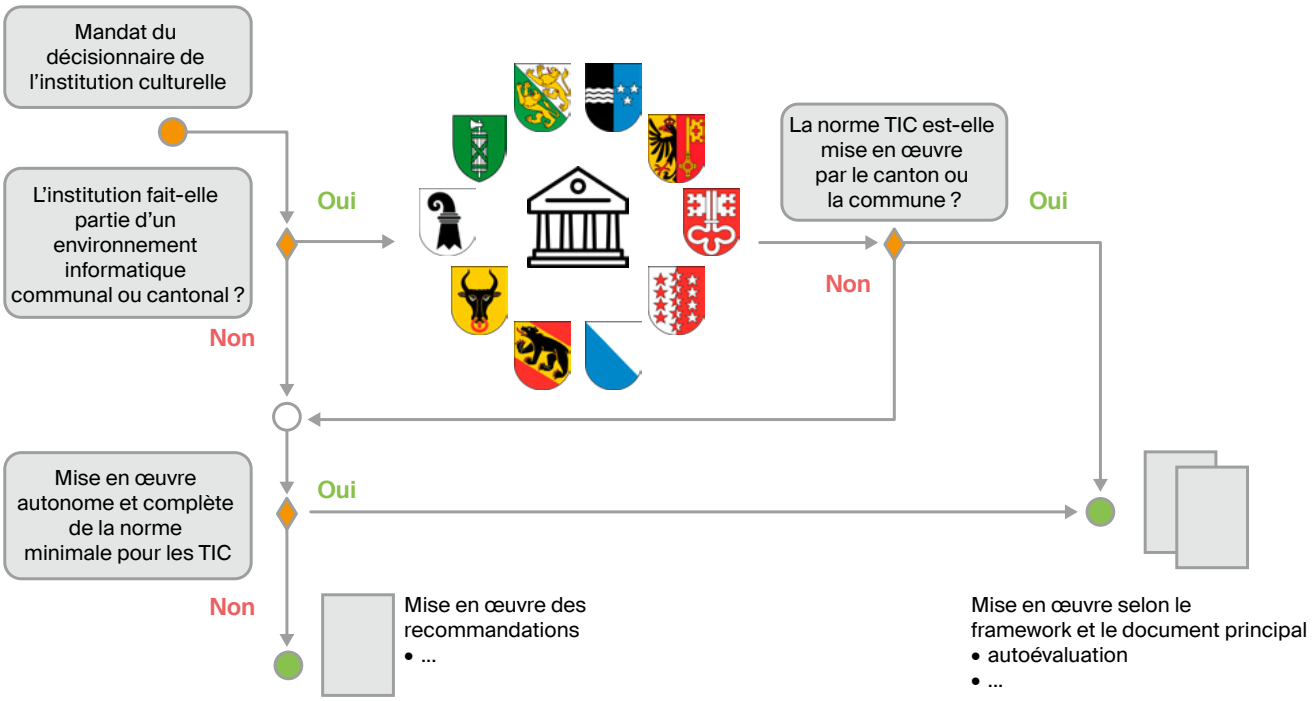


Figure : Aperçu du processus de mise en œuvre de la norme minimale TIC

Les travaux dans les domaines de la PIC et de la cybersécurité sont coordonnés entre la Confédération et les cantons. Dans le cadre de la mise en œuvre, le Centre national de cybersécurité (NCSC) a été créé et travaille en étroite collaboration avec le domaine Transformation numérique et pilotage des TIC (DTI) de la Chancellerie fédérale. De même, l'OFAE a publié à cette fin une norme minimale pour améliorer la résilience des TIC.

La CFPBC a adopté en 2020 une stratégie 2021–2025 « prévention / préparation – intervention – suivi » dans le domaine de la protection des biens culturels[13]. Cette stratégie définit les principales lignes directrices pour une protection des biens culturels optimale. Elle accorde une place importante à la numérisation et à la cybersécurité des biens culturels numériques. Les notions ont été précisées et une matrice d'évaluation pour l'introduction systématique des objets dans l'Inventaire PBC a été élaborée. La conservation à long terme et durable des objets numériques fait partie de la stratégie PBC.

Sur mandat de la CFPBC et de l'OFPP, le Digital Humanities Lab (DH Lab) de l'Université de Bâle a mené des enquêtes en ligne sur les biens culturels numériques et les a évaluées[14]. Les résultats des deux enquêtes menées par le DH Lab en 2016 et 2020 pour déterminer la quantité de biens culturels numériques et les besoins qui en découlent dans le domaine de la sécurité ont été utilisés comme base pour la norme minimale TIC.

10 Art. 4, let. b, de la loi fédérale du 20 juin 2014 sur la protection des biens culturels en cas de conflit armé, de catastrophe ou de situation d'urgence (LPBC, RS 520.3).

11 Stratégie nationale de protection des infrastructures critiques 2023. En 2012 et 2017 déjà, le Conseil fédéral a adopté deux premières versions de cette stratégie afin d'améliorer la résilience (capacité de résistance, d'adaptation et de régénération) de la Suisse dans le domaine des infrastructures critiques : https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/b4b28e9b-a5e8-4ce0-8402-b374c5d6c928.pdf

12 Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 : https://www.ncsc.admin.ch/ncsc/fr/home/strategie/strategie-ncss-2018-2022.html

13 Le document est disponible sous : https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/053ac33a-6351-48a9-b968-0ed877e06a46.pdf

14 Le rapport sur les résultats de l'enquête « Biens culturels numériques » de février 2017 peut être obtenu auprès du Groupe PBC de l'OFPP.

2 Le patrimoine culturel numérique de la Suisse

Selon les conventions de l'UNESCO[15], la notion de *patrimoine culturel* englobe l'ensemble des biens culturels meubles et immeubles ainsi que le patrimoine culturel immatériel.

- Les biens culturels **meubles (mobiles)** comprennent les collections des archives, des bibliothèques et des musées. Cette catégorie comprend non seulement le patrimoine culturel sur des supports d'information analogiques mais aussi le patrimoine culturel numérique, sous la forme de fonds numériques dans les archives de l'administration publique et dans les institutions mentionnées. Il s'agit par exemple d'art vidéo et d'art en réseau, de fonds d'auteurs, d'archives audiovisuelles, de banques de données, de données de recherche, etc.
- Les biens culturels **immeubles (immobiles)** comprennent les édifices, les monuments et les sites archéologiques. Pour ces biens culturels, il existe des documentations de sécurité sous forme de plans, de photographies et d'inventaires. Aujourd'hui, cette documentation est également créée sous forme numérique.
- Le patrimoine culturel **immatériel** comprend les traditions, les rituels, les événements festifs et les arts du spectacle[16]. Le patrimoine culturel immatériel est éphémère et ne peut pas être archivé, mais il peut être documenté. La documentation se fait en général sous forme d'enregistrements audiovisuels ou écrits, qui sont aujourd'hui en principe créés et archivés sous forme numérique.

Cet aperçu montre que les trois catégories comprennent des objets numériques dignes de protection. L'accent est toutefois mis sur les biens culturels meubles avec leurs collections et archives numériques. De telles collections sont actuellement gérées aussi bien par des entités privées que par des institutions publiques œuvrant dans la conservation du patrimoine. La présente norme minimale TIC se concentre en premier lieu sur la protection des archives, car celles-ci sont considérées comme particulièrement critiques en raison de leur fonction de garantie juridique.

15 Les conventions de l'UNESCO ratifiées par la Suisse sont disponibles sous : https://www.unesco.ch/culture/conventions/?lang=fr

16 Art. 2 de la Convention pour la sauvegarde du patrimoine culturel immatériel (RS 0.440.6), conclue à Paris le 17 octobre 2003.

2.1 Vue d'ensemble et parties prenantes

En Suisse, en raison d'une politique culturelle traditionnellement marquée par un fort fédéralisme, la conservation et l'entretien des biens culturels ne sont pas confiés à quelques institutions patrimoniales centralisées, mais sont assurés par une multitude d'organisations régionales, cantonales et nationales aux statuts juridiques variés. La conservation du patrimoine culturel en Suisse n'est donc pas gérée de manière centralisée.

Les acteurs, de droit public ou privé, peuvent être classés aux échelons suivants : Confédération (national) – canton – ville / commune / région. Parfois, ils sont actifs à plusieurs niveaux. Le tableau suivant illustre la diversité des acteurs :

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

Types principaux :

Public	**Hybride**	**Privé**

Les principales formes d'organisation des acteurs sont les suivantes :

- **Acteurs publics (étatiques) :** autorités, fondations aux niveaux de la Confédération, du canton, de la ville / de la commune.
- **Acteurs hybrides (privés / publics) :** fondations, associations aux niveaux international, national, cantonal, régional
- **Acteurs privés :** fondations, associations, entreprises aux niveaux international, national, cantonal, régional

Cet aperçu montre que le domaine de la conservation du patrimoine culturel se caractérise par une hétérogénéité prononcée, avec des acteurs de taille, de capacité financière et de champ d'action différents.

La plupart d'entre eux œuvrent à l'échelon cantonal et communal. La Confédération les soutient à titre subsidiaire et assume des tâches de coordination. Au niveau national, l'Office fédéral de la culture (OFC) est responsable de la conservation et de l'inventorisation des biens culturels et l'OFPP de la protection des biens culturels en cas catastrophe et de conflit armé. Au niveau cantonal et communal, les services respectifs sont compétents en matière de culture, de protection des biens culturels, de protection des sites, de conservation des monuments historiques et d'archéologie. De plus, de nombreux acteurs privés s'engagent pour la conservation et la protection des biens culturels en Suisse ; il s'agit la plupart du temps de fondations privées ou d'associations. Il existe aussi des acteurs hybrides, dont le mandat est public, mais qui sont régis par le droit privé[17].

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

La Confédération et les cantons sont responsables des biens culturels en leur possession. D'une manière générale, les responsabilités en matière de conservation et de mise en valeur des biens culturels sont régies au niveau fédéral par la loi fédérale sur la protection de la nature et du paysage (LPN)[18]. Il existe en outre une vaste législation cantonale en la matière (p. ex. droit des archives, conservation des monuments historiques et archéologie). La responsabilité des biens culturels en cas de conflit armé, de catastrophe et de situation d'urgence est réglée dans la loi fédérale sur la protection des biens culturels en cas de conflit armé, de catastrophe ou de situation d'urgence (LPBC)[19].

2.2 Archives et structure des archives en Suisse

La présente norme se concentre en premier lieu sur les archives, dont une partie en Suisse est classée comme infrastructure critique[20] en raison de leur contribution à la sécurité juridique. Dans le présent rapport, le terme archives ne désigne pas seulement un type d'organisation de la mémoire, mais plus généralement des fonctions et des systèmes de stockage et de conservation d'objets numériques ayant une valeur culturelle. La tâche des archives consiste à prendre en charge des biens culturels et à garantir la possibilité de leur utilisation à long terme. L'intégrité (absence de modification) et l'authenticité (fiabilité) des documents doivent être préservées. D'autres types d'acteurs, comme les bibliothèques ou les musées, peuvent également assumer cette fonction.

Il existe en Suisse plusieurs niveaux d'archives : fédérales, cantonales et communales, auxquelles s'ajoutent d'importantes archives ecclésiastiques, des archives d'entreprises et des archives spéciales, sans oublier les fonds d'archives des bibliothèques, des musées et des centres de documentation. L'inventaire PIC classe les archives des 26 cantons et de la Confédération parmi les ouvrages d'importance systémique.

Les archives de la Confédération, des cantons et des communes n'ont pas de structure centralisée. Aucune disposition constitutionnelle ne fixe le droit d'utilisation et les devoirs de conservation et de communication. Le droit des archives est réglementé sur un modèle fédéral : chaque canton a sa propre législation en la matière. Les 26 archives cantonales s'inscrivent donc dans une tradition juridico-historique propre.

Dans les années 1990, la législation sur la protection des données a exercé une forte influence sur l'évolution du droit des archives. Il a fallu alors régler en premier lieu l'obligation de proposer le versement des archives, le droit d'utilisation et la protection de la personnalité (protection des données). Actuellement, une grande partie des cantons ont adopté une loi sur les archives, en plus de la Confédération. En principe, toute personne en Suisse a le droit de consulter des documents officiels pour autant que des intérêts publics ou privés prépondérants ne s'y opposent pas.

La loi fédérale sur l'archivage (LAr)[21] règle l'archivage aux Archives fédérales des documents de la Confédération, considérés comme ayant une valeur juridique, politique, économique, historique, sociale ou culturelle. La LAr n'a toutefois pas de conséquences directes pour les cantons et les communes.

18 Loi fédérale du 1er juillet 1966 sur la protection de la nature et du paysage (LPN) ; RS 451.

19 Art. 3 et 5 la loi fédérale du 20 juin 2014 sur la protection des biens culturels en cas de conflit armé, de catastrophe ou de situation d'urgence (LPBC ; RS 520.3).

20 Voir https://www.babs.admin.ch/fr/aufgabenbabs/ski/kritisch.html.

21 Loi fédérale du 26 juin 1998 sur l'archivage (LAr ; RS 152.1).

3 Vue d'ensemble des systèmes et processus ayant une importance systémique

3.1 Archives d'importance systémique

Les archives d'importance systémique comprennent les Archives fédérales, les archives cantonales et certaines archives communales et spéciales.

Archives fédérales suisses (AFS)

Les Archives fédérales suisses (AFS) ont pour mission légale[22] de mettre à disposition de manière durable les informations pertinentes de la Confédération. L'administration rend ainsi compte de ses activités et est soutenue dans son travail. Les AFS fournissent aide et conseils à l'administration fédérale en ce qui concerne l'établissement, l'organisation et la gestion des données et des documents. En outre, les AFS sélectionnent avec les services administratifs les documents qui méritent d'être archivés et garantissent leur disponibilité et leur conservation à long terme. L'évaluation se base sur des critères systématiques et les décisions sont régulièrement publiées[23]. Les AFS numérisent en outre des documents d'archives analogiques et les mettent à la disposition du public. Elles participent à des recherches historiques sur certains sujets et assurent l'accès du grand public aux résultats.

Archives cantonales et communales

Les archives cantonales et communales remplissent à leur niveau essentiellement les mêmes tâches que les AFS au niveau national. Elles prennent en charge, inventorient et conservent les documents devant être archivés émanant des autorités tenues de leur en proposer le versement et sont responsables des mesures de conservation et de l'accessibilité. Elles contribuent à la transmission du savoir historique et à la recherche historique pour les besoins du canton, de la science et de la culture. Elles évaluent les documents en fonction de leur valeur archivistique, conseillent les autorités ainsi que les particuliers et édictent parfois des directives concernant le versement des documents et des instruments de recherche.

Archives spéciales

Les archives spéciales sont consacrées à des thèmes ou des domaines précis, au sujet desquels elles collectent et conservent des documents qu'elles mettent à disposition. Il peut s'agir d'art, de musique, d'histoire, de sciences naturelles, de techniques ou encore de médecine. Les archives spéciales servent à la recherche, à la formation et à la culture et représentent des sources importantes pour les scientifiques, les historiens, les journalistes, les artistes et le grand public. Elles jouent un rôle social important, car elles documentent les activités d'acteurs de la société civile et d'acteurs non gouvernementaux, en complément des archives publiques. Il s'agit de mouvements sociaux, de partis politiques, de communautés religieuses, d'associations, d'organisations non gouvernementales (ONG), etc.

3.2 Prestations des archives dans le sous-secteur des biens culturels

Les archives publiques jouent un rôle important pour garantir la sécurité juridique en Suisse. Elles conservent des documents qui sont d'une importance capitale pour la préservation et l'application des droits et des obligations, comme des textes de loi, des contrats, des actes, des décisions de justice ou des attestations de propriété foncière. Les archives veillent à ce que les documents soient archivés conformément aux lois, normes et standards en vigueur afin de garantir leur intégrité et leur authenticité.

En conservant durablement les documents issus de l'administration, les archives garantissent la traçabilité des décisions et des actions, notamment dans le domaine public. Elles contribuent à la transparence et à la responsabilité des processus gouvernementaux et administratifs et favorisent ainsi la confiance des citoyens dans leurs institutions et dans l'État de droit. Les Archives fédérales le résument parfaitement dans leur devise : **Pas de démocratie sans archives**.

22 Voir la loi fédérale sur l'archivage (LAr ; RS 152.1).

23 Les décisions d'évaluation des AFS sont disponibles sous : https://www.bar.admin.ch/bar/fr/home/gestion-de-l-information/valeur-archivistique/decisions-d-evaluation.html

Les archives spécialisées complètent les archives publiques. Leur utilité réside dans la conservation et la mise à disposition de biens culturels meubles dont la création n'est pas directement liée avec l'administration publique. Elles se concentrent sur des thèmes et des domaines spécifiques comme l'histoire sociale, l'histoire économique ou l'histoire des femmes. Les archives spéciales ont une grande valeur pour la formation de l'identité culturelle de notre pays et relèvent donc (au moins en partie) des infrastructures critiques.

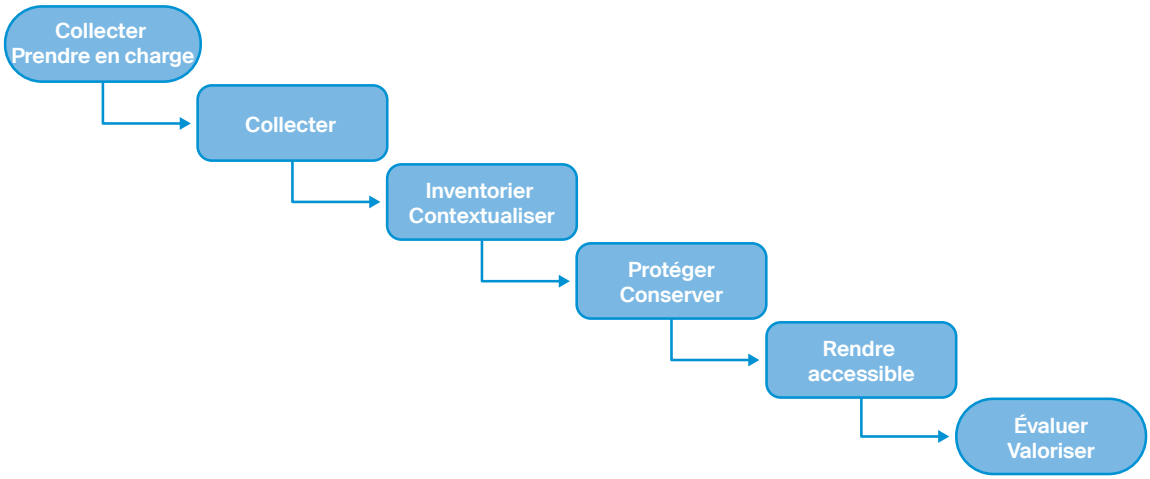
3.3 Vue d'ensemble des processus critiques

Les processus opérationnels mis en œuvre en principe par tous les acteurs impliqués dans la conservation et l'entretien du patrimoine culturel peuvent être décrits à l'aide du processus exposé ci-après. Les domaines d'activité sont désignés dans la mesure du possible par des termes généraux et le vocabulaire diffère selon le type d'acteur (archives, bibliothèque, musée, service de documentation, service de conservation du patrimoine) et de bien culturel (meuble, immeuble, immatériel). Le modèle laisse apparaître clairement la dépendance du sous-secteur critique des biens culturels par rapport aux systèmes TIC en particulier pour l'inventaire, la recherche, la protection et la conservation.

Dans le cadre de cette norme minimale TIC, certains champs d'action ne sont pas pris en compte ou font partie d'autres sous-secteurs d'infrastructures critiques :

- les systèmes en amont tels que GEVER, la gestion documentaire, le records management, les applications métier ;
- l'évaluation et la sélection de biens culturels à des fins d'archivage ;
- les systèmes en aval tels que les systèmes d'analyse, les infrastructures de recherche.

Le processus suivant règle la prise en charge, la protection et la transmission des biens culturels numériques :



Collecter
Prendre en charge et préparer les données et les métadonnées (ingest). Ce processus est soutenu par des systèmes basés sur le workflow qui automatisent et orchestrent des tâches telles que l'analyse antivirus, la validation, l'extraction de métadonnées, la migration de formats de fichiers, l'intégrité (écriture de sommes de contrôle), etc.

Inventorier et contextualiser
Créer des inventaires, répertorier et classer, documenter, cataloguer. Selon le type d'organisation, cette tâche est soutenue par des systèmes d'information archivistiques, des systèmes de gestion de bibliothèque ou de gestion des collections. En outre, des informations contextuelles et des indications sur la provenance et le contexte de création et d'utilisation sont collectées.

Protéger et conserver
Enregistrer (processus initial), sauvegarder (tâche permanente : entretenir et contrôler la mémoire) ; planifier la conservation (« preservation planning ») ; le cas échéant, mettre en œuvre des mesures de conservation.

Rendre accessible
Permettre les recherches (OPAC, salle de lecture virtuelle, accès web), diffusion (fournir des données pour une analyse automatique ou une utilisation ultérieure via des interfaces techniques).

Évaluer et valoriser
Transmettre et réactualiser sous la forme d'une médiation didactique et médiatique et par la pratique.

3.4 Contre quels dangers faut-il se protéger ?

Le rapport de l'OFPP de 2022 sur les menaces et la résilience dans le sous-secteur des biens culturels analyse les risques causés par la défaillance ou les perturbations de cette infrastructure critique. Les quatre principaux types de danger suivants ont été identifiés pour les biens culturels :

- Une **cyberattaque** et / ou une panne informatique affectent la disponibilité des fonds numériques d'un service d'archives, probablement pendant plusieurs semaines. En outre, une destruction irréversible, un vol ou une publication, intentionnelle ou non, d'informations sensibles sont également possibles. Les fonds d'archives ne peuvent être restaurés que si des mesures adéquates ont été prises au préalable. La publication de documents confidentiels peut causer des dommages considérables à la réputation des personnes et des organisations. Le risque de cyberattaque est notamment dû au fait que les institutions ont souvent des ressources limitées et n'ont pas les moyens de s'adapter au rythme effréné des progrès technologiques.
  Étapes du processus menacées : toutes les étapes sont menacées par une cyberattaque.
- Les **dangers naturels** comme les tremblements de terre et les inondations occasionnent des coûts considérables pour leur maîtrise et la remise en état. Ces dangers affectent plusieurs biens culturels dans la région concernée. La disponibilité des archives serait compromise pendant des mois, voire des années. Il en résulte des coûts consécutifs très importants pour la population, les collectivités publiques et la recherche.
  Étapes du processus menacées : l'étape « Protéger / Conserver » est particulièrement menacée par les dangers naturels.
- Un **attentat conventionnel** contre des archives ou un bien culturel est considéré comme une atteinte à l'identité d'un canton ou du pays et provoquerait des dommages importants en raison de l'insécurité ressentie par la population et les acteurs économiques. Un tel attentat dirigé contre un centre de calcul pourrait entraîner une perte de données considérable.
  Étapes du processus menacées : l'étape « Protéger / Conserver » est particulièrement menacée par un attentat conventionnel.
- Une **pandémie** entraînerait l'absence du personnel spécialisé nécessaire à la conservation et à l'exploitation des archives numériques. Ce risque est particulièrement marqué dans les petites institutions, dont le personnel spécialisé est restreint.
  Étapes du processus menacées : l'absence de personnel spécialisé met en danger l'intégralité du processus. L'étape « Protéger / Conserver » est particulièrement menacée.

Comme dans d'autres sous-secteurs, les cyberrisques représentent un risque considérable pour les biens culturels en raison de la dématérialisation croissante des processus opérationnels et de la centralisation des infrastructures informatiques. De plus, la fréquence de ces attaques a considérablement augmenté ces dernières années. Un potentiel de dommages plus élevé se dessine également en raison de l'émergence de réseaux régionaux et suprarégionaux d'archivage numérique, ainsi que de la plus grande quantité d'objets numériques pris en charge par les archives.

4 Défense en profondeur

La démarche dite « defense in depth » ou défense en profondeur vise à se protéger des dangers énumérés plus haut. Elle se fonde sur le principe qu'aucune mesure de sécurité n'est suffisante en soi pour protéger totalement les systèmes ou les réseaux. Il est préférable de suivre une approche globale reposant sur différentes mesures de sécurité mise en œuvre à plusieurs niveaux ou sur plusieurs couches. L'objectif de ce chapitre est d'expliquer plus en détail la défense en profondeur en matière de cybersécurité et de montrer avec quelles catégories de mesures les organisations peuvent mettre en œuvre cette approche. Sur la base de ces principes, le chapitre 6 mentionne ensuite des éléments concrets pour améliorer la sécurité de l'information.

4.1 Le concept de défense en profondeur

La stratégie de sécurité informatique d'une organisation doit viser à protéger les systèmes et applications nécessaires à ses champs d'activité et ses processus. Pour cela, il faut une approche à plusieurs niveaux, connue sous le nom de défense en profondeur. On entend par là la mise en œuvre coordonnée de plusieurs niveaux de protection, en vertu du principe qu'il est plus difficile de surmonter un système de défense échelonné et multicouche qu'une barrière unique. On observe en parallèle les méthodes et les manières de procéder de l'attaquant potentiel afin de préparer un dispositif de défense. Le concept de défense en profondeur vise à identifier les violations de la sécurité informatique afin de pouvoir y réagir en réduisant au minimum ou en atténuant leurs conséquences. La défense en profondeur suit une approche holistique qui tente de protéger tous les outils informatiques contre n'importe quel risque. Les ressources d'une organisation devraient être utilisées de manière à garantir une protection efficace contre les risques connus ainsi qu'une surveillance complète des risques potentiels. Celles-ci englobent les personnes, les processus, les objets, les données et les appareils. Un attaquant ne constitue une menace pour un système informatique qu'à partir du moment où il parvient à exploiter une vulnérabilité existante dans un de ces éléments. Les organisations et les entreprises sont tenues de surveiller en permanence les mesures et, si nécessaire, de les adapter aux nouvelles menaces.

De manière générale, les éléments d'une stratégie de défense en profondeur peuvent être répartis en mesures organisationnelles, techniques et physiques.

4.2 Mesures organisationnelles (processus)

Les éléments suivants font partie de ce groupe de mesures :

- la défense en tant que tâche permanente d'une organisation dans le cadre de la gestion de la sécurité ; la définition des responsabilités au sein de l'organisation ;
- l'élaboration d'un profil de risque ; l'identification des risques en matière de sécurité ;
- les aspects de la sécurité relevant de l'organisation et du personnel ;
- les concepts et procédures standardisés, par exemple en ce qui concerne la protection des données, l'effacement et la destruction de données et de leurs supports, l'échange d'informations en interne ou avec des tiers ;
- la gestion de l'inventaire des outils informatiques (Asset Management) ;
- la vue d'ensemble des objets numériques archivés ;
- les aspects de la sécurité dans le cadre opérationnel, à l'interne ou dans le cas d'une exploitation par des tiers (centre de calcul externe, cloud), la séparation de l'informatique administrative et du système d'archivage faisant également partie de ce domaine ;
- la gestion des correctifs et des points faibles ;
- les processus d'élaboration et de vérification des mesures de sécurité mises en œuvre, de détection des incidents de sécurité et de gestion des incidents ;
- l'organisation de la gestion de la continuité des activités ;
- la documentation.

4.3 Mesures techniques (systèmes)

Les éléments suivants font partie de ce groupe de mesures :

- la sécurisation des applications et des services, notamment dans les domaines de la communication, du stockage, des applications professionnelles et des applications client ;
- la sécurisation des différents systèmes informatiques tels que les serveurs et les ordinateurs de bureau ;
- la sécurisation du réseau, de ses connexions et de ses composants et de la communication via le réseau ; la répartition du réseau en segments et en zones de sécurité ;
- la sécurisation des composants actifs du réseau (pare-feux, routeurs, commutateurs, etc.).

4.4 Mesures physiques

La protection physique des fonds d'archives est surtout un sujet de préoccupation pour le matériel analogique, par la sécurisation des locaux contre le feu, l'eau ou le vandalisme. Pour les archives numériques, les domaines suivants jouent un rôle :

- la sécurisation de l'accès aux salles de serveurs et aux centres de données ;
- la protection des salles de serveurs et des centres de données contre les risques naturels ;
- la répartition géographique des systèmes de stockage et de sauvegarde ;
- la sauvegarde par stockage hors ligne ou à froid. Comme pour tous les types de stockage, un contrôle d'intégrité doit être régulièrement effectué.

4.5 Séparation de la bureautique et du système d'archivage

La séparation systématique et systémique de l'informatique administrative et des fonds d'archives numériques (système d'archivage), représente un aspect central de la stratégie de défense en profondeur. Un système d'archivage comprend en principe les tâches décrites dans la norme ISO 14721 (open archival information system, OAIS).

Le tableau suivant explique, à l'aide d'exemples, comment ces deux domaines fonctionnent selon des logiques et des processus de planification différents et doivent donc être considérés différemment. La présente norme minimale, et en particulier les modules d'amélioration de la sécurité de l'information au chapitre 6, se réfèrent en premier lieu à la protection des biens culturels numériques et non à la bureautique.

Thématique sécuritaire	TIC (p. ex. bureautique)	Système d'archivage basé sur OAIS
Bases normatives	Normes et standards	Législation nationale et cantonale sur les archives, convention de l'UNESCO pour la protection des biens culturels, normes et standards
Antivirus	Largement répandu. Facile à distribuer et à mettre à jour. Les utilisateurs ont la possibilité de le personnaliser. Une protection par antivirus peut être configurée au niveau de l'équipement ou d'une entreprise.	Les virus représentent un double défi : les serveurs du système d'archivage doivent être protégés et il faut éviter que des fichiers contaminés par des virus ne parviennent dans les archives à long terme via l'ingest.
Mises à jour de sécurité (gestion des mises à jour)	Précisément définies, appliquées à toute l'entreprise et automatisées grâce à des accès à distance.	Longue période de préparation et de planification jusqu'à la réussite de l'installation du correctif ; toujours spécifique au fabricant ; peut entraîner des interruptions (temporaires) dans l'OAIS. Nécessité de définir le risque acceptable à cet égard.
Cycles de vie de la technologie (Technology Support Lifecycle)	2 à 3 ans, plusieurs fournisseurs, développement et mises à niveau constants	10 à 20 ans, généralement le même fournisseur/prestataire de services tout au long du cycle de vie ; la fin du cycle de vie représente de nouvelles menaces pour la sécurité.

Thématique sécuritaire	TIC (p. ex. bureautique)	Système d'archivage basé sur OAIS
Méthodes de tests et d'audits (Testing and Audit Methods)	Utilisation de méthodes modernes (si possible automatisées). Les systèmes sont normalement suffisamment résilients et fiables pour supporter des évaluations (assessments) sans interrompre l'exploitation.	Les méthodes d'évaluation automatisées peuvent se révéler inappropriées, p. ex. en raison du degré élevé de développement individuel. La probabilité d'erreurs pendant l'évaluation est plus élevée. Les évaluations en cours d'exploitation ont donc tendance à être plus difficiles.
Gestion des modifications (Change Management)	Planifiées et périodiques. Respectant les exigences de l'entreprise : durées minimale + maximale de fonctionnement d'un appareil.	Processus complexe ayant un impact potentiel sur l'activité des archives. Nécessité d'une planification stratégique et individuelle
Classification des actifs (Asset Classification)	Se fait normalement chaque année. Les dépenses + investissements sont planifiés en fonction des résultats.	En ce qui concerne l'archivage, c'est surtout la classification des données qui pose problème. Sans inventaire ni connaissance de la sensibilité des données, il est difficile de planifier des contre-mesures efficaces.
Réaction et analyse en cas d'incidents (Incident Response and Forensics)	Facile à développer et à mettre en œuvre. Au besoin, se conformer aux prescriptions réglementaires (protection des données).	Se concentre principalement sur la reprise du système dans le cadre de la restauration des données et de la reprise après sinistre.
Sécurité physique (Physical Security)	Variable, allant de faible pour la bureautique à forte pour les centres de calcul protégés.	Typiquement, très bonne sécurité physique. Pour les archives cantonales, l'OAIS est généralement exploité dans des centres de calcul cantonaux.
Développement de logiciels sécurisés (Secure Software Development)	Partie intégrante du processus de développement.	Les premiers systèmes d'archivage numérique à long terme étaient souvent conçus comme des systèmes physiquement isolés et constituaient un corps étranger dans l'infrastructure informatique. Les OAIS modernes sont planifiés et mis en œuvre en tant que partie intégrante de l'infrastructure informatique cantonale en ce qui concerne la sécurité.
Règles de sécurité	Prescriptions réglementaires générales, selon le secteur (pas pour tous les secteurs).	Les contraintes de sécurité relatives aux normes sectorielles se concentrent sur la préservation à long terme des données et des métadonnées et n'abordent pas les questions de sécurité plus larges. Pour cela, il convient d'utiliser des normes générales (NIST, ISO 27001).

Tableau 1 : Différences entre la bureautique et un système d'archivage basé sur OAIS

5 Mesures relatives au NIST Framework Core

5.1 Vue d'ensemble

NIST Framework Core

L'objectif du cadre de cybersécurité[24] du National Institute of Standards and Technology (USA) est de mettre à la disposition des exploitants d'infrastructures critiques un outil leur permettant d'accroître, de manière autonome et responsable, leur résilience face aux cyberrisques. Ce faisant, il tient également compte de la recherche de rentabilité et d'efficacité ainsi que de la confidentialité et de la protection des données. Le cadre NIST se fonde sur un choix de normes, de directives et de règles de bonnes pratiques ; il est technologiquement neutre.

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

1. Identifier (Identify)
2. Protéger (Protect)
3. Détecter (Detect)
4. Réagir (Respond)
5. Récupérer (Recover)

Ensemble, ces cinq fonctions constituent la base du concept de sécurité.

Le NIST Framework comprend quatre niveaux appelés Implementation Tiers (niveaux d'implémentation). Ceux-ci décrivent le niveau de développement ou de protection qu'une entreprise a mis en œuvre. Ces niveaux vont de partiel (partial, tier 1) à adapté au danger (adaptive, tier 4). Pour déterminer son niveau de protection (tier level), une organisation devrait établir une vue d'ensemble de ses pratiques de gestion des risques, du genre de menaces plausibles et des exigences légales et réglementaires, de ses objectifs opérationnels et de ses besoins organisationnels. Ainsi elle pourra déterminer clairement contre quoi elle souhaite se protéger.

Le chapitre suivant est structuré selon les cinq fonctions du NIST Framework Core. Les tâches à effectuer sont catégorisées comme suit :

- Les deux premières lettres (p. ex. ID = Identify) désignent l'une des cinq fonctions.
- La deuxième paire de lettres désigne la catégorie (p. ex. AM = Asset Management).
- Enfin, le numéro désigne la tâche individuelle. Elles sont numérotées en continu à l'intérieur de la catégorie. Exemple de lecture : ID.AM-1 correspond à la première tâche de la catégorie Asset Management de la fonction Identify.

Le tableau suivant donne un aperçu des fonctions et des catégories du NIST Framework :

Abréviation	Français	Anglais
ID	**Identifier**	**Identify**
ID.AM	Gestion de l'inventaire	Asset Management
ID.BE	Environnement de l'entreprise	Business Environment
ID.GV	Règles	Governance
ID.RA	Analyse des risques	Risk Assessment

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

5 Mesures relatives au NIST Framework Core

Abréviation	Français	Anglais
ID.RM	Stratégie de gestion des risques	Risk Management Strategy
ID.SC	Gestion des risques liés à la chaîne d'approvisionnement	Supply Chain Riskmanagement
PR	**Protéger**	**Protect**
PR.AC	Gestion et contrôle des accès	Access Control
PR.AT	Sensibilisation et formation	Awareness and Training
PR.DS	Sécurité des données	Data Security
PR.IP	Protection des données	Information Protection Processes and Procedures
PR.MA	Maintenance	Maintenance
PR.PT	Technologie de protection	Protective Technology
DE	**Détecter**	**Detect**
DE.AE	Anomalies et incidents	Anomalies and Events
DE.CM	Surveillance	Security Continous Monitoring
DE.DP	Processus de détection	Detection Processes
RS	**Réagir**	**Respond**
RS.RP	Plan d'intervention	Response Planning
RS.CO	Communication	Communications
RS.AN	Analyses	Analysis
RS.MI	Circonscrire les dommages	Mitigation
RS.IM	Améliorations	Improvements
RC	**Récupérer**	**Recover**
RC.RP	Plan de récupération	Recovery Planning
RC.IM	Améliorations	Improvements
RC.CO	Communication	Communications

Tableau 2 : Aperçu des fonctions et des catégories du NIST Framework

Chaque tableau de tâches issues du NIST Framework Core est suivi d'un tableau de références à d'autres normes internationales. Chaque tableau fait référence à la catégorie, par exemple la gestion des actifs (Asset Management AM). Cela doit faciliter la compréhension pour les utilisateurs qui organisent leurs tâches de sécurité informatique selon d'autres normes. Pour le secteur des biens culturels numériques, il est également fait référence à la norme ISO 16363, voir paragraphe suivant.

NIST Framework et norme industrielle ISO 16363:2012
La norme ISO 16363:2012 « Audit and certification of trustworthy digital repositories » joue un rôle important dans l'évaluation de la fiabilité des archives numériques. Elle s'articule autour des trois parties suivantes :

- cadre organisationnel
- gestion des objets numériques
- gestion des risques liés à l'infrastructure et à la sécurité

Le tableau suivant montre comment les fonctions et les catégories du NIST Framework et de la norme ISO 16363 se rapportent les unes aux autres :

5 Mesures relatives au NIST Framework Core

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	

Tableau 3 : Rapport entre les catégories du NIST Framework et la norme ISO 16363:2012

Il s'avère que la norme sectorielle ISO 16363:2012 couvre largement les fonctions NIST Identify et Protect. D'une manière générale, on peut constater que les acteurs ont conscience de l'importance de ces deux domaines dans le secteur. Mais il apparaît aussi très clairement que les fonctions Detect, Respond et Recover ne sont pas couvertes. La même conclusion s'impose si l'on compare les catégories du NIST avec les critères nestor[25], un catalogue de critères d'archivage numérique fiable à long terme largement utilisé, du moins dans les pays germanophones. Ce catalogue de critères couvre les mêmes domaines que la norme ISO 16363:2012.

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

5.2 Identifier (Identify)

Gestion de l'inventaire (Asset Management)

Les données, les personnes, les appareils, les systèmes et les installations d'une entreprise sont identifiés, catalogués et évalués. L'évaluation se fait en fonction de leur criticité pour les processus opérationnels à mettre en place et de la stratégie de l'entreprise en matière de risque.

L'établissement d'inventaires est une mesure essentielle pour la protection des biens culturels numériques. Les inventaires n'offrent pas seulement une vue d'ensemble et un contrôle sur les biens à protéger, ils documentent également leur origine (provenance), l'histoire de leur création et contribuent à garantir leur authenticité. Il existe des inventaires généraux, comme l'Inventaire PBC, mais aussi des inventaires au sein des institutions, comme les systèmes d'information archivistiques, les catalogues de bibliothèque ou les bases de données pour la gestion des collections.

Désignation	Tâche
ID.AM-1	Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC (Assets / actifs).
ID.AM-2	Inventoriez toutes les plateformes, licences et applications dans votre organisation.
ID.AM-3	Listez tous les flux de communication et de transferts de données en interne.
ID.AM-4	Listez tous les systèmes TIC externes cruciaux pour votre organisation.
ID.AM-5	Hiérarchisez les ressources inventoriées (appareils, applications, données) en fonction de leur criticité.
ID.AM-6	Définissez des rôles et des responsabilités claires en matière de cybersécurité.

Tableau 4 : Tâches ID.AM

Norme	Référence
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

Tableau 5 : Références ID.AM

Environnement de l'entreprise (Business Environment)
Les objectifs, les tâches et les activités de l'entreprise sont hiérarchisés et évalués. Ces informations servent à répartir les responsabilités.

Désignation	Tâche
ID.BE-1	Le rôle de votre entreprise dans la chaîne d'approvisionnement (critique) est identifié, documenté et communiqué.
ID.BE-2	L'importance de l'entreprise en tant qu'infrastructure critique et sa position dans le secteur critique sont identifiées et communiquées.
ID.BE-3	Les objectifs, les tâches et les activités dans l'entreprise sont évalués et hiérarchisés.
ID.BE-4	Les interdépendances et les fonctions critiques pour la fourniture de services critiques sont définies.
ID.BE-5	Les exigences en matière de résilience pour soutenir la fourniture de services critiques sont définies pour tous les modes de fonctionnement (p. ex. sous contrainte / attaque, pendant le rétablissement, en fonctionnement normal).

Tableau 6 : Tâches ID.BE

Norme	Référence
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

Tableau 6 : Références ID.AM

Règles (Governance)
La gouvernance règle les responsabilités, surveille et garantit que les exigences réglementaires, légales et opérationnelles de l'environnement commercial sont respectées.

Désignation	Tâche
ID.GV-1	Les directives sur la sécurité informatique au sein de l'entreprise sont définies et communiquées.
ID.GV-2	Les rôles et les responsabilités en matière de sécurité de l'information entre les responsables internes (p. ex. gestion des risques) et les partenaires externes sont coordonnés.
ID.GV-3	Vérifiez que votre organisation respecte toutes les exigences légales et réglementaires en matière de cybersécurité, y compris au niveau de la protection des données.
ID.GV-4	Assurez-vous que les cyberrisques sont bien intégrés dans la gestion des risques pour toute l'entreprise.

Tableau 8 : Tâches ID.GV

Norme	Référence
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

Tableau 9 : Références ID.GV

Analyse des risques (Risk Assessment)
L'organisation connaît les effets des cyberrisques sur ses activités, ses équipements et son personnel, y compris les risques pour la réputation.

Désignation	Tâche
ID.RA-1	Identifiez les faiblesses (techniques) de vos équipements et documentez-les.
ID.RA-2	Des informations actuelles sur les cybermenaces sont obtenues grâce à des échanges réguliers sur des forums et lors de réunions d'experts.
ID.RA-3	Identifiez et documentez les cybermenaces, aussi bien internes qu'externes.
ID.RA-4	Identifiez l'impact potentiel des cybermenaces sur vos activités et évaluez leur probabilité d'occurrence.
ID.RA-5	Évaluez les risques pour votre organisation en fonction des menaces, des vulnérabilités, de l'impact (sur vos activités) et de leur probabilité d'occurrence.
ID.RA-6	Définissez les mesures à prendre immédiatement lorsqu'un risque se concrétise et fixez des priorités.

Tableau 10 : Tâches ID.RA

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

Tableau 11 : Références ID.RA

Stratégie de gestion des risques (Risk Management Strategy)
Les priorités, les restrictions et les risques maximaux supportables pour l'organisation sont définis. Les risques opérationnels sont évalués sur cette base.

Désignation	Tâche
ID.RM-1	Définissez les processus de gestion des risques, gérez-les activement et faites-les confirmer par les personnes impliquées ou les parties prenantes.
ID.RM-2	Définissez et communiquez la tolérance maximale au risque de pour votre entreprise.
ID.RM-3	Assurez-vous que la tolérance maximale au risque est évaluée en prenant en compte l'importance de votre organisation du fait qu'elle exploite une infrastructure critique. Prenez également en considération, dans votre analyse, les risques propres au secteur.

Tableau 12 : Tâches ID.RM

Norme	Référence
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

Tableau 13 : Références ID.RM

Gestion des risques liés à la chaîne d'approvisionnement (Supply Chain Risk Management)
Les priorités, les restrictions et les risques maximaux que l'organisation peut accepter par rapport à ses fournisseurs sont définis.

Désignation	Tâche
ID.SC-1	Les processus de gestion des risques dans la chaîne d'approvisionnement cyber sont identifiés, établis, évalués et gérés. Les parties prenantes impliquées sont d'accord sur les processus choisis.
ID.SC-2	Les fournisseurs et les prestataires pour les systèmes d'information, les composants et les services sont identifiés, hiérarchisés et évalués selon des processus de gestion des risques dans la chaîne d'approvisionnement cyber. Voir ID.SC-1.
ID.SC-3	Les fournisseurs et les prestataires tiers sont régulièrement contrôlés par des audits, des tests ou d'autres formes d'évaluation afin de s'assurer qu'ils respectent leurs obligations contractuelles.
ID.SC-4	Faites un suivi systématique pour vous assurer que tous vos fournisseurs et prestataires de services remplissent leurs obligations conformément aux exigences. Faites-le vérifier régulièrement par des rapports d'audit ou par les résultats des tests techniques.
ID.SC-5	Définissez avec vos fournisseurs et prestataires les processus pour réagir et récupérer après un incident de cybersécurité. Testez ces processus dans le cadre d'exercices.

Tableau 14 : Tâches ID.SC

Norme	Référence
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

Tableau 15 : Références ID.SC

5.3 Protéger (Protect)

Gestion et contrôle des accès (Access Control)

L'accès physique et logique aux équipements et installations TIC n'est possible que pour les personnes, processus et appareils autorisés. Seules les activités prévues sont permises.

Désignation	Tâche
PR.AC-1	Définissez un processus clair pour octroyer et gérer les autorisations et les données d'identification pour utilisateurs, appareils/machines et processus.
PR.AC-2	Assurez-vous que seules les personnes autorisées ont physiquement accès aux équipements TIC. Prenez des mesures concrètes, y compris au niveau de la construction des locaux, pour garantir que les ressources TIC sont protégées contre tout accès physique non autorisé.
PR.AC-3	Définissez les processus pour gérer les accès à distance.
PR.AC-4	Définissez les droits d'accès et les autorisations en tenant compte des principes de moindre privilège et de séparation des tâches.
PR.AC-5	Vérifiez que l'intégrité de votre réseau est protégée. Séparez votre réseau au niveau logique comme physique, là où c'est nécessaire et judicieux.
PR.AC-6	Veillez à ce que les identités numériques correspondent à des personnes ou à des processus clairement identifiés.
PR.AC-7	L'authentification d'utilisateurs, appareils et autres assets (p. ex. authentification à un ou plusieurs facteurs) est effectuée en fonction du risque de la transaction (p. ex. risques de sécurité ou protection des données pour des personnes et autres risques d'entreprise).

Tableau 16 : Tâches PR.AC

Norme	Référence
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

Tableau 17 : Références PR.AC

Sensibilisation et formation (Awareness and Training)
Les employés et les partenaires externes sont régulièrement et correctement formés dans le domaine de la cybersécurité. Ils exécutent les tâches impactant la sécurité conformément aux exigences et aux processus définis.

Désignation	Tâche
PR.AT-1	Veillez à ce que tous vos collaborateurs soient sensibilisés et formés en matière de cybersécurité.
PR.AT-2	Veillez à ce que les utilisateurs ayant des niveaux d'autorisation élevés soient conscients de leur rôle et de leurs responsabilités.
PR.AT-3	Veillez à ce que tous les acteurs extérieurs à votre entreprise (fournisseurs, clients, partenaires) soient conscients de leur rôle et de leurs responsabilités.
PR.AT-4	Veillez à ce que tous les cadres soient conscients de leurs rôles spécifiques et de leurs responsabilités.
PR.AT-5	Veillez à ce que les responsables de la sécurité physique et de la sécurité informatique soient conscients de leurs rôles spécifiques et de leurs responsabilités.

Tableau 18 : Tâches PR.AT

Norme	Référence
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

Tableau 19 : Références PR.AT

Sécurité des données (Data Security)
Les informations, les données et leurs supports sont gérés de manière à protéger la confidentialité, l'intégrité et la disponibilité des données, conformément à la stratégie de l'organisation pour gérer les risques.

Désignation	Tâche
PR.DS-1	Assurez-vous que les données stockées sont protégées (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).
PR.DS-2	Assurez-vous que les données sont protégées pendant leur transmission (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).
PR.DS-3	Veillez à ce qu'un processus formel soit défini pour votre matériel TIC afin de protéger les données lorsque des équipements sont supprimés, déplacés ou remplacés.
PR.DS-4	Veillez à ce que vos équipements TIC aient une réserve de capacité suffisante afin que vos données soient toujours disponibles.
PR.DS-5	Assurez-vous que des mesures appropriées sont mises en œuvre contre les fuites de données.
PR.DS-6	Définissez un processus pour vérifier l'intégrité des logiciels embarqués (firmwares), des systèmes d'exploitation, des logiciels d'application et des données.
PR.DS-7	Ayez un environnement informatique (IT) pour le développement et les tests qui soit totalement indépendant des systèmes de production.
PR.DS-8	Définissez un processus pour vérifier l'intégrité du matériel informatique utilisé.

Tableau 20 : Tâches PR.DS

Norme	Référence
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

Tableau 21 : Références PR.DS

Protection des données (Information Protection Processes and Procedures)
Des directives pour protéger les systèmes d'information et les équipements sont disponibles. Elles couvrent au minimum l'objectif, la portée, les rôles et les responsabilités et assurent la coordination au sein de l'organisation. Utilisez ces directives pour protéger les systèmes d'information et les équipements.

Désignation	Tâche
PR.IP-1	Générez une configuration standard pour l'infrastructure d'information et de communication, ainsi que pour les systèmes de contrôle industriels. Assurez-vous que cette configuration par défaut obéit aux règles usuelles de sécurité (p. ex. redondance N-1, configuration minimale, etc.).
PR.IP-2	Définissez un processus de cycle de vie pour l'utilisation des équipements TIC.
PR.IP-3	Définissez un processus pour contrôler les changements de configuration.
PR.IP-4	Assurez-vous que des sauvegardes informatiques de vos données (backups ou synchronisation) sont effectuées, gérées et testées régulièrement (possibilité de restaurer les données sauvegardées).
PR.IP-5	Veillez à ce que toutes les exigences (réglementaires) et les directives concernant les équipements physiques soient respectées.
PR.IP-6	Veillez à ce que les données soient toujours détruites selon les prescriptions.
PR.IP-7	Développez et améliorez régulièrement vos processus de sécurité informatique.
PR.IP-8	Discutez de l'efficacité des différentes technologies de protection avec vos partenaires.
PR.IP-9	Instaurez des processus pour réagir aux cyberincidents (Incident Response-Planning, Business Continuity Management, Incident Recovery, Disaster Recovery).
PR.IP-10	Testez les plans de réaction et de récupération.
PR.IP-11	Tenez compte de la cybersécurité dès le processus de recrutement (p. ex. en vérifiant les antécédents ou par des contrôles de sécurité relatifs aux personnes).
PR.IP-12	Développez et mettez en œuvre un processus pour traiter les failles repérées.

Tableau 22 : Tâches PR.IP

Norme	Référence
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

Tableau 23 : Références PR.IP

Maintenance
La maintenance et la réparation des composantes des systèmes TIC sont effectuées conformément aux directives et méthodes en vigueur.

Désignation	Tâche
PR.MA-1	Veillez à ce que le fonctionnement, la maintenance et les éventuelles réparations des équipements soient enregistrés et documentés (journalisation). Assurez-vous qu'elles sont effectuées rapidement et en ne recourant qu'à des moyens testés et approuvés.
PR.MA-2	Enregistrez et documentez également les travaux de maintenance de vos systèmes distants. Assurez-vous qu'aucun accès non autorisé n'est possible.

Tableau 24 : Tâches PR.MA

Norme	Référence
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

Tableau 25 : Références PR.MA

Technologie de protection (Protective Technology)
Installez des solutions techniques pour assurer la sécurité et la résilience de vos systèmes TIC et de vos données selon les exigences et processus.

Désignation	Tâche
PR.PT-1	Définissez les exigences pour les audits et les enregistrements des fichiers journaux (logs). Générez et vérifiez ces fichiers régulièrement, selon les exigences et les directives.
PR.PT-2	Assurez-vous que les supports amovibles sont protégés et que leur utilisation se fait dans le strict respect des directives.
PR.PT-3	Veillez à ce que votre système soit configuré pour assurer en tout temps une fonctionnalité minimale.
PR.PT-4	Assurez la protection de vos réseaux de communication et de contrôle.
PR.PT-5	Assurez-vous que des mécanismes (p. ex. résilience, équilibrage de charge, remplacement à chaud / Hot Swap) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.

Tableau 26 : Tâches PR.PT

Norme	Référence
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

Tableau 27 : Références PR.PT

5.4 Détecter (Detect)

Anomalies et incidents (Anomalies and Events)
Les anomalies et autres incidents de sécurité sont détectés à temps et le personnel est conscient de l'impact potentiel de ces événements.

Désignation	Tâche
DE.AE-1	Définissez des valeurs par défaut pour les opérations réseau licites et les flux de données prévus pour les utilisateurs et les systèmes. Gérez ces valeurs en permanence.
DE.AE-2	Assurez-vous que les incidents de cybersécurité détectés sont analysés quant à leurs objectifs et méthodes.
DE.AE-3	Assurez-vous que les informations sur les incidents de cybersécurité provenant de différentes sources et capteurs sont compilées et exploitées.
DE.AE-4	Déterminez les conséquences probables des incidents.
DE.AE-5	Définissez les valeurs limites au-delà desquelles les incidents de cybersécurité doivent générer des alertes.

Tableau 28 : Tâches DE.AE

Norme	Référence
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

Tableau 29 : Références DE.AE

Surveillance (Security Continuous Monitoring)
Le système TIC, équipements compris, est régulièrement contrôlé pour pouvoir détecter les incidents de cybersécurité d'une part et vérifier l'efficacité des mesures de protection d'autre part.

Désignation	Tâche
DE.CM-1	Mettez en place une surveillance permanente du réseau pour détecter les incidents de cybersécurité potentiels.
DE.CM-2	Mettez en place une surveillance / un monitoring continus de tous les équipements et des bâtiments pour détecter les incidents de cybersécurité.
DE.CM-3	L'utilisation des TIC par les employés est surveillée pour détecter les incidents de cybersécurité potentiels.
DE.CM-4	Veillez à pouvoir détecter les maliciels.
DE.CM-5	Veillez à pouvoir détecter les maliciels sur les appareils mobiles.
DE.CM-6	Assurez-vous que les activités des prestataires de services externes sont surveillées (monitorées) pour détecter d'éventuels incidents de cybersécurité.
DE.CM-7	Surveillez votre système en permanence pour être certain que des activités ou accès liés à des personnes, équipements ou logiciels non autorisés seront détectés.
DE.CM-8	Procédez à des scans de vulnérabilités.

Tableau 30 : Tâches DE.CM

Norme	Référence
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

Tableau 31 : Références DE.CM

Processus de détection (Detection Processes)
Les processus et les instructions pour détecter les incidents de cybersécurité sont maintenus, testés et entretenus.

Désignation	Tâche
DE.DP-1	Définissez clairement les rôles et les responsabilités pour que tous sachent bien qui est responsable de quoi et qui a telles ou telles compétences.
DE.DP-2	Assurez-vous que les processus de détection correspondent aux exigences et conditions fixées.
DE.DP-3	Testez vos processus de détection.
DE.DP-4	Communiquez aux personnes concernées (p. ex. fournisseurs, clients, partenaires, autorités) les incidents que vous avez détectés.
DE.DP-5	Améliorez en permanence vos processus de détection.

Tableau 32 : Tâches DE.DP

Norme	Référence
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

Tableau 33 : Références DE.DP

5.5 Réagir (Respond)

Plan d'intervention (Response Planning)
Un plan d'intervention pour traiter les incidents de cybersécurité détectés est disponible. Des mesures ont été prises pour qu'en cas d'incident ce plan d'intervention soit exécuté correctement et en temps utile.

Désignation	Tâche
RS.RP-1	Assurez-vous que le plan d'intervention est correctement suivi et rapidement exécuté si un incident de cybersécurité est détecté.

Tableau 34 : Tâches RS.RP

Norme	Référence
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

Tableau 35 : Références RS.RP

Communication
Contrôlez que vos processus de réaction sont coordonnés avec ceux des parties prenantes, internes et externes. Selon le type d'incident, veillez à pouvoir bénéficier du soutien des autorités si la situation l'exige.

Désignation	Tâche
RS.CO-1	Assurez-vous que toutes les personnes connaissent leurs tâches et la marche à suivre lorsqu'elles doivent réagir à un incident de cybersécurité.
RS.CO-2	Définissez des critères pour le signalement des incidents de cybersécurité et assurez-vous qu'ils soient signalés et traités conformément à ces critères.
RS.CO-3	Partagez les informations sur les incidents de cybersécurité relevés – ainsi que les enseignements qui en découlent – selon ces critères prédéfinis.
RS.CO-4	La coordination avec toutes les parties prenantes et les groupes d'intérêt se fait en accord avec les plans de réaction selon les critères prédéfinis.
RS.CO-5	Des informations sont régulièrement et volontairement échangées avec des acteurs externes afin d'accroître la sensibilisation à la situation actuelle en matière de cybersécurité.

Tableau 36 : Tâches RS.CO

Norme	Référence
COBIT 2019	Aucune
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

Tableau 37 : Références RS.CO

Analyses
Des analyses afin de réagir correctement en cas d'incident de cybersécurité sont régulièrement effectuées.

Désignation	Tâche
RS.AN-1	Assurez-vous que les alertes émanant de systèmes de détection sont prises en compte et déclenchent des enquêtes.
RS.AN-2	Veillez à ce que les impacts d'un incident de cybersécurité soient connus et compris.
RS.AN-3	Effectuez une analyse forensique après chaque incident.
RS.AN-4	Mettez en place des processus pour recevoir, analyser et réagir aux vulnérabilités portées à la connaissance de l'organisation par des sources internes et externes.

Tableau 38 : Tâches RS.AN

Norme	Référence
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

Tableau 39 : Références RS.AN

Circonscrire les dommages (Mitigation)
Faites tout pour éviter qu'un incident de cybersécurité se propage afin de limiter les éventuels dommages.

Désignation	Tâche
RS.MI-1	Assurez-vous que les incidents de cybersécurité peuvent être circonscrits et que vous pouvez stopper leur propagation.
RS.MI-2	Assurez-vous de pouvoir réduire l'impact des incidents de cybersécurité.
RS.MI-3	Veillez à réduire au maximum les failles récemment découvertes ou référencez-les comme des risques acceptables.

Tableau 40 : Tâches RS.MI

Norme	Référence
COBIT 2019	Aucune
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

Tableau 41 : Références RS.MI

Améliorations (Improvements)
La réactivité de l'organisation face aux incidents de cybersécurité est régulièrement améliorée grâce aux enseignements tirés des incidents précédents.

Désignation	Tâche
RS.IM-1	Assurez-vous que les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans de réaction.
RS.IM-2	Actualisez vos stratégies de réaction.

Tableau 42 : Tâches RS.IM

Norme	Référence
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

Tableau 43 : Références RS.IM

5.6 Récupérer (Recover)

Plan de récupération (Recovery Planning)

Les processus de récupération sont préparés puis exécutés de sorte à permettre une récupération rapide des systèmes.

Désignation	Tâche
RC.RP-1	Assurez-vous que le plan de récupération est suivi à la lettre en cas d'incident de cybersécurité.

Tableau 44 : Tâches RC.RP

Norme	Référence
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

Tableau 45 : Références RC.RP

Améliorations (Improvements)
Les processus de récupération sont constamment améliorés sur la base des enseignements tirés des incidents précédents.

Désignation	Tâche
RC.IM-1	Assurez-vous que les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans de récupération.
RC.IM-2	Actualisez vos stratégies de récupération.

Tableau 46 : Tâches RC.IM

Norme	Référence
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

Tableau 47 : Références RC.IM

Communication
Veillez à coordonner vos actions de récupération avec vos partenaires internes et externes (fournisseurs de services Internet, CERT, autorités, intégrateurs de systèmes, etc.).

Désignation	Tâche
RC.CO-1	Un plan de communication préalable a été élaboré pour les relations publiques en matière d'incident de cybersécurité.
RC.CO-2	L'organisation s'efforce de restaurer son image après un incident de cybersécurité.
RC.CO-3	Communication des activités de récupération aux groupes d'intérêt internes et externes, en particulier aux cadres et à la direction.

Tableau 48 : Tâches RC.CO

Norme	Référence
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

Tableau 49 : Références RC.CO

6 Éléments de base pour améliorer la sécurité de l'information

Le cadre d'évaluation utilisé au chapitre 5 offre un soutien complet pour le recensement et la planification de l'amélioration de la cybersécurité dans les institutions patrimoniales. Les grandes organisations disposant de ressources adéquates et d'un personnel formé (p. ex. au niveau cantonal ou fédéral) seront en mesure de mettre en œuvre cette recommandation dans son intégralité. Ces acteurs utilisent peut-être déjà le cadre proposé dans ce document ou une solution similaire. Le secteur de la conservation du patrimoine culturel est toutefois très hétérogène. La taille de certaines infrastructures critiques (effectifs et ressources disponibles pour la sécurité de l'information) est plutôt comparable à celle d'une petite entreprise, voire d'une microentreprise. Une mise en œuvre complète du cadre posera de grands défis à de telles institutions. Pour tenir compte de cette situation et mettre malgré tout en œuvre une stratégie de défense en profondeur efficace, les petites institutions devraient se concentrer sur les éléments essentiels d'amélioration de la sécurité de l'information mentionnés au chapitre suivant.

En règle générale, une petite institution ne dispose pas de vastes collections numériques, n'attire pas un grand public et ses ressources humaines et financières sont limitées. Ce serait par exemple le cas des archives communales d'une petite ville ou d'archives spécialisées rassemblant des fonds d'archives sur un thème particulier. Ce chapitre a pour but d'expliquer comment une telle institution peut mettre en œuvre les points centraux d'une stratégie de défense en profondeur (chap. 4) avec des ressources limitées. Les petites institutions patrimoniales étant souvent intégrées dans des organisations informatiques plus grandes (p. ex. services informatiques municipaux, cantonaux, universitaires), il faut tout mettre en œuvre pour utiliser les synergies et s'intégrer dans l'unité supérieure plus grande.

Chaque institution ne doit donc pas obligatoirement mettre en œuvre toutes les mesures, mais seulement celles qui sont nécessaires pour protéger ses propres processus critiques et systèmes informatiques. Les éléments pour améliorer la sécurité de l'information proposés par l'office fédéral allemand de la sécurité de l'information (Bundesamt für Sicherheit in der Informationstechnik, BSI)[26] présentent un panel de mesures et de recommandations. Ils sont répartis en trois catégories décrites au chap. 4 Défense en profondeur :

- mesures organisationnelles (gestion de la sécurité, organisation et processus)
- mesures techniques (systèmes)
- mesures physiques (bâtiments, locaux)

Le NIST Framework indique **les éléments à retenir** lors d'une démarche d'évaluation. Le chapitre suivant donne des idées sur la **manière de procéder**.

26 Les éléments peuvent être consultés sous : https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

6.1 Gestion de la sécurité

L'objectif de ce module est d'établir une gestion globale de la sécurité dans l'institution afin d'ancrer la sécurité de l'information comme un processus continu.

Parmi les mesures de ce module figurent la définition des objectifs et des exigences de sécurité, l'introduction de processus de sécurité, la définition des responsabilités et des compétences, la formation et la sensibilisation du personnel et la mise en place de plans d'urgence.

L'objectif de ce module est d'établir au sein de l'organisation une culture de l'amélioration systématique et continue de la sécurité de l'information. Une gestion globale de la sécurité doit permettre de réduire les risques au minimum et d'atteindre un niveau de sécurité adéquat pour les systèmes informatiques et les données.

Norme	Référence
BSI IT-G 2023	ISMS.1

6.2 Organisation et processus

Organisation

L'objectif du module **Organisation** est de créer une organisation efficace et efficiente, capable d'identifier et de réduire de manière proactive les risques dans le domaine de la sécurité informatique.

Parmi les mesures de ce module figurent notamment la définition de structures et de processus organisationnels en matière de sécurité de l'information, l'attribution de compétences et de responsabilités ainsi que l'élaboration de directives de sécurité. Étant donné que la plupart des archives sont intégrées dans une structure informatique gérée à l'échelon supérieur, il est important de clarifier les compétences spécifiques et techniques.

Le module **Organisation** met également l'accent sur une collaboration et une communication étroites entre les différents collaborateurs et unités d'une entreprise ou d'un service étatique. L'objectif est de créer une compréhension commune de l'importance de la sécurité de l'information et d'impliquer toutes les personnes concernées dans les processus de sécurité. Comme énoncé précédemment, ceci est très important pour l'harmonisation des besoins spécifiques et techniques entre les archives et les services informatiques.

En mettant en œuvre les mesures du module **Organisation**, une institution peut faire évoluer sa forme d'organisation de manière à ce que la sécurité de l'information devienne une partie intégrante des activités opérationnelles.

Norme	Référence
BSI IT-G 2023	ORP.1

Personnel

Ce module aborde le thème de la sécurité de l'information en rapport avec le personnel d'une institution. L'objectif est de s'assurer que le personnel est suffisamment sensibilisé et formé pour contribuer à la sécurité des systèmes informatiques et des données.

Parmi les mesures de ce module figurent notamment la définition d'exigences de sécurité pour le personnel, la sensibilisation et la formation à la sécurité de l'information et le respect des consignes de sécurité. Des dispositions doivent être prises pour réduire au minimum la perte de savoir-faire en cas d'absence de personnel, par exemple en cas de pandémie. En outre, il convient de développer de manière ciblée les qualifications de certaines personnes dans le domaine de la sécurité de l'information.

Une autre mesure pour les institutions contenant des données sensibles et importantes pour la sécurité est la réalisation d'un contrôle de sécurité des personnes lors de l'embauche[27].

Norme	Référence
BSI IT-G 2023	ORP.2

27 À l'échelon fédéral, c'est le Service spécialisé chargé des contrôles de sécurité relatifs aux personnes (CSP) du DDPS qui est responsable de ces contrôles : https://www.sepos.admin.ch/fr/controle-de-securite-relatif-aux-personnes

Sensibilisation et formation
Ce module a pour objectif de sensibiliser et de former les collaborateurs des entreprises et des services étatiques dans le domaine de la sécurité de l'information. Ce n'est qu'ainsi qu'ils pourront accomplir correctement leurs tâches en matière de sécurité de l'information et contribuer à réduire les risques.

Parmi les mesures de ce module figurent notamment la définition des objectifs de formation et de sensibilisation, le choix des formats et des méthodes de formation appropriés ainsi que la planification et la mise en œuvre des formations et des mesures de sensibilisation.

Les mesures de formation et de sensibilisation doivent être adaptées aux besoins et aux exigences spécifiques des employés, ainsi qu'aux risques spécifiques auxquels une institution est exposée. Les mesures doivent être mises en œuvre régulièrement, en particulier avec les nouveaux employés, et la direction doit également être impliquée afin de souligner l'importance de la sécurité de l'information dans l'institution.

Norme	Référence
BSI IT-G 2023	ORP.3

Gestion des données d'identification et des autorisations
Ce module traite de la gestion des données d'identification et des autorisations au sein d'une institution. L'objectif de ce module est de s'assurer que seules les personnes autorisées ont accès aux systèmes informatiques et aux données.

Parmi les mesures de ce module figurent notamment la définition des rôles et des autorisations pour les collaborateurs, la mise en œuvre de mécanismes de contrôle d'accès, la vérification des données d'identification et des autorisations ainsi que la réalisation d'audits relatifs au contrôle d'accès. Une mesure essentielle consiste à séparer la gestion des données d'identification et des autorisations de la bureautique et des archives numériques.

Le module Gestion des données **d'identification et des autorisations** comprend en outre la gestion appropriée des données d'accès et l'utilisation du système d'authentification à deux facteurs afin d'améliorer la sécurité des accès.

Norme	Référence
BSI IT-G 2023	ORP.4

Gestion de la conformité (compliance)
Ce module traite de la conformité aux exigences légales, réglementaires et contractuelles dans le domaine de la sécurité de l'information. L'objectif de ce module est de s'assurer que l'institution répond aux principales exigences et contribue ainsi à réduire les risques juridiques et réglementaires.

Parmi les mesures de ce module figurent notamment l'identification et le respect des exigences légales, réglementaires et contractuelles, l'intégration des exigences de conformité dans le concept de sécurité informatique et leur documentation ainsi que la réalisation de contrôles de conformité. Les normes et standards archivistiques ainsi que les bonnes pratiques (Best Practices) font notamment partie de ces exigences.

Le module Gestion **de la conformité** comprend également un contrôle régulier du respect des exigences ainsi que l'intégration des questions de conformité dans la planification et la réalisation des projets informatiques. On y trouve des interfaces avec le sous-secteur critique de l'administration, dans la mesure où l'archivage doit déjà être pris en compte lors de la planification et de l'introduction de nouveaux systèmes.

Norme	Référence
BSI IT-G 2023	ORP.5

Protection des données
Ce module traite de la protection des données personnelles au sein d'une organisation. L'objectif de ce module est de garantir que les données personnelles sont traitées et protégées conformément aux exigences légales.

Parmi les mesures de ce module figurent notamment la réalisation d'évaluations d'impact sur la protection des données, la mise en œuvre de mesures techniques et organisationnelles pour la protection des données personnelles, la formation du personnel au traitement des données personnelles et la vérification du respect des exigences en matière de protection des données.

Le module **Protection des données** se concentre sur le respect des principes de protection des données tels que la minimisation, les finalités et la transparence, ainsi que sur les droits des personnes concernées, tels que le droit d'accès, d'effacement ou de rectification des données.

En mettant en œuvre les mesures de ce module, les institutions s'assurent que les données personnelles sont traitées et protégées conformément aux exigences légales, ce qui renforce la confiance des fournisseurs de services et des utilisateurs et réduit les risques juridiques.

Norme	Référence
BSI IT-G 2023	CON.2

Concept de sauvegarde des données
Ce module porte sur la création et la mise en œuvre d'un concept de sauvegarde des données archivées et des métadonnées. L'objectif de ce module est de garantir la disponibilité et l'intégrité de ces données et de réduire le risque de perte de données.

Parmi les mesures de ce module figurent notamment la création d'un concept de sauvegarde des données qui comprend la fréquence et le type de sauvegarde, leur vérification ainsi que le stockage des copies de sécurité. En outre, la restauration et le contrôle d'intégrité des données après une perte ainsi que la mise en œuvre de procédures de sauvegarde sont également réglés.

Pour les archives numériques, il convient de choisir un concept de sauvegarde des données basé sur au moins trois copies indépendantes et synchronisées. En cas d'erreur sur l'une des copies, les données sont récupérées à partir d'une autre copie. Lors de la conception, les points suivants doivent notamment être pris en compte :

- systèmes de stockage géographiquement dispersés ;
- utilisation de différents pare-feux pour les systèmes de production et de sauvegarde ;
- stockage hors ligne ;
- systèmes de stockage avec mécanismes d'auto-réparation pour corriger les éventuelles erreurs ;
- déclenchement manuel plutôt qu'automatique des processus de sauvegarde et de réplication afin d'éviter la propagation des rançongiciels.

Le module **Concept de sauvegarde des données** comprend également l'identification et l'évaluation des risques liés à la sauvegarde des données, ainsi que l'adaptation du concept de sauvegarde des données à l'évolution des exigences et des risques au fil du temps.

Norme	Référence
BSI IT-G 2023	CON.3

Suppression et destruction de données
Il existe des cas où les données d'archives doivent être supprimées, notamment parce que leur format est devenu obsolète et qu'elles ont été migrées dans de nouveaux formats, ou parce qu'une réévaluation a révélé qu'elles ne sont plus adaptées pour l'archivage.

Ce module traite de la suppression sûre et définitive des données et de la destruction des supports de données d'une institution. L'objectif de ce module est de garantir que les données archivées (en particulier les données confidentielles ou personnelles) ne tombent pas entre de mauvaises mains et ne puissent pas être utilisées de manière non autorisée.

Parmi les mesures de ce module figurent notamment l'établissement de directives et de procédures pour la suppression sécurisée des données, l'identification précise des données et métadonnées à supprimer et la définition de procédures de destruction des supports de données. Cela inclut la documentation du processus de suppression. En outre, la formation des employés à la suppression sécurisée des données et la vérification du respect des procédures de suppression et de destruction sont également abordées.

Norme	Référence
BSI IT-G 2023	CON.6

Gestion individuelle
Ce module traite de la sécurisation des systèmes et infrastructures informatiques gérés par l'institution elle-même. L'objectif de ce module est de garantir la disponibilité, l'intégrité et la confidentialité des données et des systèmes informatiques, et donc de réduire les risques de pannes et d'attaques.

Parmi les mesures de ce module figurent notamment la création de directives de sécurité informatique, la mise en place de contrôles d'accès et d'autorisations, la surveillance des systèmes et réseaux informatiques et la réalisation d'audits réguliers relatifs à la sécurité informatique. En outre, la sécurisation physique des salles de serveurs et la planification d'urgence sont abordées.

Le module comprend la planification de ces mesures et renvoie aux éléments constitutifs du système nécessaires.

Le module **Gestion individuelle** prend également en compte les nouveaux développements et les nouvelles technologies ainsi que l'adaptation des mesures de sécurité informatique à l'évolution des risques et des menaces.

Les petites institutions, qui dépendent parfois du bénévolat, entrent souvent dans cette catégorie. Les exigences en matière de gestion individuelle sont élevées et il est recommandé à ces institutions d'examiner de manière plus approfondie la gestion par des tiers (cloud).

Norme	Référence
BSI IT-G 2023	OPS.1

Gestion par des tiers (Cloud)
Ce module traite de la sécurisation des systèmes et infrastructures informatiques gérés par un prestataire de services externe. L'objectif de ce module est de garantir la disponibilité, l'intégrité et la confidentialité des données et des systèmes informatiques, et donc de réduire les risques de pannes et d'attaques.

Parmi les mesures de ce module figurent notamment la définition d'exigences de sécurité pour le prestataire de services, la réalisation de contrôles de sécurité du prestataire de services, la définition des responsabilités et des obligations dans le cadre du contrat d'externalisation et la réalisation d'audits de sécurité informatique réguliers. En outre, le suivi des contrats de niveau de service (Service Level Agreement, SLA) et la planification d'urgence sont également abordés.

Le module accorde une grande importance à la sélection des prestataires de services appropriés et à la prise en compte des aspects de sécurité lors de l'établissement des contrats.

Norme	Référence
BSI IT-G 2023	OPS.2

6.3 Modules du système

Serveurs

Ce module traite de la sécurisation des serveurs et de leur environnement dans les systèmes informatiques. L'objectif de ce module est de garantir la disponibilité, l'intégrité et la confidentialité des données et des systèmes informatiques, et donc de réduire les risques de pannes et d'attaques.

Parmi les mesures de ce module figurent notamment la sécurisation physique des salles de serveurs, la mise en place de contrôles d'accès et d'autorisations, l'utilisation de communication cryptée, l'exécution de mises à jour de sécurité régulières et l'introduction de mécanismes de sauvegarde et de récupération. En outre, la surveillance des serveurs et la planification d'urgence sont également abordées.

Le module accorde une grande importance aux nouveaux développements et aux nouvelles technologies ainsi qu'à l'adaptation des mesures de sécurité informatique à l'évolution des risques et des menaces.

Norme	Référence
BSI IT-G 2023	SYS.1

Solutions de stockage

Ce module traite de la sécurisation des solutions de stockage dans les systèmes informatiques. L'objectif de ce module est de garantir la disponibilité, l'intégrité et la confidentialité des données et des systèmes informatiques, et donc de réduire les risques de pannes et d'attaques. Ce module met essentiellement en œuvre le concept de sauvegarde des données du module CON.3.

Parmi les mesures de ce module figurent notamment la sécurisation physique des systèmes de stockage, la mise en place de contrôles d'accès et d'autorisations, l'utilisation de communication cryptée, l'exécution de mises à jour de sécurité régulières et l'introduction de mécanismes de synchronisation et de sauvegarde.

La mise en œuvre des mesures vise à garantir que les solutions de stockage sont correctement protégées et que les pannes ou les attaques peuvent être rapidement détectées et traitées.

Norme	Référence
BSI IT-G 2023	SYS.1.8

Systèmes de bureau

Ce module traite de la sécurisation des systèmes de bureau dans l'environnement informatique. L'objectif de ce module est de garantir la disponibilité, l'intégrité et la confidentialité des données et des systèmes informatiques, et donc de réduire les risques de pannes et d'attaques.

Parmi les mesures de ce module figurent notamment la protection physique des postes de travail, la mise en place de contrôles d'accès et d'autorisations, l'utilisation de communication cryptée, l'exécution de mises à jour de sécurité régulières et l'introduction de mécanismes de sauvegarde et de récupération. Il faut veiller à la mise à jour du système d'exploitation et des logiciels installés ainsi qu'à l'installation et à la mise à jour d'une protection antivirus. Les logiciels obsolètes ou qui ne sont plus utilisés doivent être désinstallés. En outre, la surveillance des systèmes de bureau et la planification d'urgence sont également abordées.

Le module accorde une grande importance aux nouveaux développements et aux nouvelles technologies ainsi qu'à l'adaptation des mesures de sécurité informatique à l'évolution des risques et des menaces.

Norme	Référence
BSI IT-G 2023	SYS.2

Supports de données amovibles
Ce module traite de l'utilisation sécurisée des clés USB, des disques durs externes et d'autres supports de données amovibles dans les systèmes informatiques. L'objectif de ce module est de réduire le risque de perte, de vol ou d'altération des données par l'utilisation de supports de stockage amovibles et de garantir la confidentialité, l'intégrité et la disponibilité des données.

Parmi les mesures de ce module figurent la définition de directives pour l'utilisation des supports de stockage amovibles, la mise en œuvre de mécanismes de détection et de défense contre les logiciels malveillants sur les supports de stockage amovibles, ainsi que la formation et la sensibilisation des employés à une utilisation sûre de ces supports. La perte ou le vol d'un support de données peuvent arriver, mais grâce à des mesures appropriées telles que le cryptage, les conséquences peuvent être réduites. Il arrive que les supports amovibles soient défaillants. Ils peuvent être utilisés dans le cadre d'une stratégie de sauvegarde, mais jamais comme unique copie des données.

Le module **Supports de données amovibles** accorde une grande importance à la surveillance et à la documentation des activités liées aux supports de données amovibles, ainsi qu'à la vérification et à la mise à jour régulières des mesures de sécurité.

Norme	Référence
BSI IT-G 2023	SYS 4.5

Réseaux
Ce module traite de la sécurité des réseaux dans les systèmes informatiques. L'objectif de ce module est de garantir la disponibilité, l'intégrité et la confidentialité des données en réseaux et de réduire les risques d'attaques et de pertes de données.

Parmi les mesures de ce module figurent notamment la définition de directives et de processus pour l'architecture du réseau, sa segmentation et son administration. D'autres mesures comprennent l'implémentation de pare-feux, de systèmes de détection d'intrusion et le cryptage des connexions réseau. Une mesure centrale est la séparation de l'informatique bureautique et du système d'archivage électronique au niveau du réseau. En outre, au niveau du pare-feu, des règles doivent être établies non seulement pour le flux de données entrant, mais aussi pour le flux de données sortant, afin d'éviter toute fuite de données incontrôlée. En principe, toutes les connexions réseau entre les domaines et les ordinateurs individuels doivent être cryptées. Lors du transfert de données d'archives, l'intégrité des données doit être assurée en comparant les sommes de contrôle avant et après le transfert.

Le module **Réseaux** accorde une grande importance à la surveillance et à la documentation des activités liées aux réseaux, à la vérification et à la mise à jour régulières des équipements et des systèmes réseau, ainsi qu'à la formation et à la sensibilisation du personnel à l'utilisation sécurisée des réseaux.

Norme	Référence
BSI IT-G 2023	NET.1

6.4 Éléments physiques

Bâtiments
Ce module traite des aspects physiques de la sécurité des bâtiments dans lesquels sont exploités des systèmes informatiques. L'objectif de ce module est de garantir la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données par des mesures de sécurité appropriées au niveau du bâtiment. Il s'agit d'empêcher l'accès physique non autorisé à des lieux sensibles tels que les salles de serveurs ou les centres de données.

Parmi les mesures de ce module figurent la sécurisation des entrées, des fenêtres et des autres accès au bâtiment, le contrôle des visiteurs et des invités ainsi que l'installation d'équipements de sécurité tels que des caméras de surveillance, des systèmes d'alarme et des systèmes de contrôle d'accès.

Ce module comprend également la disponibilité de plans d'urgence et la formation des employés à la gestion des situations d'urgence telles que les incendies, les inondations et autres catastrophes naturelles.

Norme	Référence
BSI IT-G 2023	INF.1

Centres de données, salles de serveurs
Ce module traite des exigences spécifiques en matière de sécurité des centres de données et des salles de serveurs dans lesquels sont exploités des systèmes informatiques. L'objectif de ce module est de garantir la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données par des mesures de sécurité appropriées.

Parmi les mesures de ce module figurent la sécurisation des accès aux centres de données et aux salles de serveurs, le contrôle des visiteurs et des invités ainsi que l'installation d'équipements de sécurité tels que des caméras de surveillance, des systèmes d'alarme et des systèmes de contrôle d'accès.

Ce module comprend également une climatisation appropriée et des systèmes d'extinction d'incendie dans les centres de données ou les salles de serveurs afin d'éviter les dommages causés par une surchauffe ou un incendie.

À ces mesures générales viennent s'ajouter des mesures spécifiques aux archives numériques. Au moins trois copies des archives doivent être conservées sur au moins deux sites. Les sites doivent se trouver dans des zones sismiques différentes. Si seulement deux sites sont choisis pour les trois copies, le matériel informatique à double sur un site doit être placé dans différentes zones de protection contre les incendies.

En outre, le module **Centre de données, salle de serveurs** comprend également des recommandations pour la conception de l'infrastructure technique, comme l'alimentation électrique, l'architecture réseau et l'infrastructure des serveurs.

Norme	Référence
BSI IT-G 2023	INF.2

Archives de supports de données
Ce module traite de la conservation et de l'archivage sécurisés des supports de données dans les systèmes informatiques. L'objectif de ce module est de garantir la confidentialité, l'intégrité et la disponibilité des données sur les supports de données afin de réduire les risques de perte, de vol ou de manipulation. Les mesures des deux modules **Supports de données amovibles et Archives de supports de données** protègent les données même en cas de panne de courant et constituent un réseau de sécurité important pour la récupération après un sinistre (Disaster Recovery).

Parmi les mesures de ce module figurent notamment la définition de processus de contrôle d'accès physique et logique aux locaux d'archives des supports de données, la mise en œuvre de mesures de sécurité pour les supports de données eux-mêmes, telles que le cryptage et l'étiquetage (Labeling), ainsi que la définition de procédures de destruction sécurisée des supports de données en fin de vie.

Le module **Archives de supports de données** comprend également la vérification et la mise à jour régulières des mesures de sécurité ainsi que la formation et la sensibilisation du personnel ayant accès aux archives de supports de données.

Norme	Référence
BSI IT-G 2023	INF.6

7 Références et sources

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

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

CoreTrustSeal
La fondation CoreTrustSeal propose une certification des archives et des bases de données numériques selon le « 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
Système ouvert d'archivage d'information (SOAI / OAIS) — Modèle de référence
https://www.iso.org/standard/57284.html
Texte identique :
https://public.ccsds.org/pubs/650x0m2.pdf

ISO 16363
Audit et certification des référentiels numériques de confiance
https://www.iso.org/standard/56510.html
Texte identique :
https://public.ccsds.org/pubs/652x0m1.pdf

ISO 2700x
L'Organisation internationale de normalisation (International Organization for Standardization, ISO) met à disposition une douzaine de normes complémentaires sur la sécurité de l'information, appelées « famille 2700x ». La plus connue d'entre elles est la norme ISO 27001, qui spécifie les exigences pour l'établissement, la mise en œuvre, la mise à jour et l'amélioration continue d'un système de gestion de la sécurité de l'information documenté, en tenant compte du contexte de chaque organisation.
https://www.iso.org/fr/standard/73906.html

nestor (catalogue de critères)
Groupe de travail nestor sur l'archivage numérique fiable à long terme – Certification (2008). Catalogue de critères d'archivage numérique fiable à long terme.
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 Glossaire et liste des abréviations

AFS	Archives fédérales suisses
Ampleur des dommages	L'ampleur des dommages est l'estimation de l'impact sur la population et ses moyens de subsistance de la défaillance d'un ou plusieurs → processus critiques au moment où apparaît un → danger. Elle se compose de la somme des dommages au moment de l'événement et des dommages susceptibles de survenir pendant toute la phase de remise en état.
Archives AV	Archives audiovisuelles
Asset / actif	Dans ce contexte, données, personnes, appareils, systèmes et installations d'une organisation.
Authenticité	Dans le domaine de l'archivage numérique, ce terme est utilisé pour signifier qu'un fichier contient effectivement ce qu'il prétend. Il est largement utilisé comme synonyme de fiabilité.
Bien culturel	La Convention de La Haye pour la protection des biens culturels en cas de conflit armé de 1954 définit la notion comme suit : « biens, meubles ou immeubles, qui présentent une grande importance pour le patrimoine culturel des peuples, tels que les monuments d'architecture, d'art ou d'histoire, religieux ou laïques, les sites archéologiques, les ensembles de constructions qui, en tant que tels, présentent un intérêt historique ou artistique, les œuvres d'art, les manuscrits, livres et autres objets d'intérêt artistique, historique ou archéologique, ainsi que les collections scientifiques et les collections importantes de livres, d'archives ou de reproductions des biens définis ci-dessus »[28]. Il convient de souligner la distinction entre les biens culturels meubles et immeubles.
Bien culturel numérique	La notion de « bien culturel », telle qu'elle est définie à l'art. 1 de la Convention de La Haye pour la protection des biens culturels en cas de conflit armé de 1954, sert de critère central pour la sélection des objets. Par bien culturel numérique, nous entendons aussi bien les objets créés numériquement (born digital) que les objets numérisés (rétronumérisation). La notion de « collection » dans ce contexte est analogue à celle des archives, des bibliothèques et des musées. Il s'agit alors d'une collection d'archives numériques. Ces biens culturels créés numériquement comprennent non seulement des fonds d'archives numériques (p. ex. des journaux numérisés et des archives d'émissions audiovisuelles d'une bibliothèque cantonale), mais aussi de l'art numérique (p. ex. une collection de photographies créée numériquement dans un musée), des reproductions numériques d'œuvres d'art et des données de recherche (documentation relative à des fouilles d'un service archéologique cantonal sous forme de photos prises par des drones ou de modèles 3D), des documentations de sécurité créées numériquement, etc. Pour leur intégration dans l'Inventaire PBC, les objets numériques sont enregistrés et classés en tant que collections.

29 Art. 1 de la Convention de La Haye pour la protection des biens culturels en cas de conflit armé (RS 0.520.3), conclue à La Haye le 14 mai 1954.

8 Glossaire et liste des abréviations

Bitstream Preservation	Désigne le processus de préservation et de récupération à long terme du flux binaire afin de garantir l'intégrité et la reproductibilité du contenu numérique.
BN	Bibliothèque nationale suisse
CFPBC	Commission fédérale de la protection des biens culturels
Conformité	La conformité est le terme utilisé en économie et en droit pour désigner le respect des règles par les entreprises, c'est-à-dire le respect des lois, des directives et des codes volontaires.
Cybersécurité	La cybersécurité fait référence à la protection des ordinateurs, des réseaux et des données contre les attaques provenant d'internet ou d'autres réseaux. Elle comprend des mesures de défense contre les cybermenaces (→ danger) afin de sécuriser les infrastructures numériques.
Défense en profondeur	Approche de la cybersécurité proposant des mesures de sécurité à plusieurs niveaux afin de protéger les systèmes et les données. L'objectif est de créer des pare-feux redondants, de sorte que la défaillance d'une mesure de protection ne compromette pas l'ensemble du système de sécurité.
DH Lab	Digital Humanities Lab, Université de Bâle.
DIMAG	Digitales Magazin. Solution groupée pour l'archivage numérique dans les archives publiques.
Danger	Par « danger » on entend un risque concret existant pour un bien digne de protection. Le danger correspond par conséquent à un événement ou à un développement potentiel pouvant avoir des conséquences sur un bien digne de protection.
Données au repos	Les données au repos désignent les données qui sont hébergées sur un support de stockage physique ou électronique.
Données en transit	Les données en transit font référence aux données en cours de transmission sur les réseaux ou les canaux de communication.
GEVER	Gestion électronique des affaires
Infrastructures critiques	Les infrastructures critiques sont des processus, des systèmes et des installations essentiels au fonctionnement de l'économie ou au bien-être de la population.
Intégrité	Preuve que les données sont correctes et inchangées. Les sommes de contrôle sont un outil important à cet effet.
LAP	Loi fédérale du 17 juin 2016 sur l'approvisionnement économique du pays
LAr	Loi fédérale du 26 juin 1998 sur l'archivage (RS 152.1)
LPBC	Loi fédérale du 20 juin 2014 sur la protection des biens culturels en cas de conflit armé, de catastrophe ou de situation d'urgence (RS 520.3)
LPN	Loi fédérale du 1er juillet 1966 sur la protection de la nature et du paysage (RS 451)
NCSC	Centre national pour la cybersécurité
NIST	Le National Institute of Standards and Technology est une agence fédérale américaine qui a publié un cadre de gestion des cyberrisques.
OAIS	Open Archival Information System, ISO 14721. Modèle de référence pour les archives numériques.
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFC	Office fédéral de la culture
OFPP	Office fédéral de la protection de la population

8 Glossaire et liste des abréviations

OPAC	Open Public Access Catalog
Patrimoine culturel	Le patrimoine culturel est utilisé comme un terme générique et comprend l'ensemble des biens culturels meubles et immeubles ainsi que le patrimoine culturel immatériel.
Patrimoine culturel immatériel	On entend par « patrimoine culturel immatériel » les pratiques, représentations, expressions, connaissances et savoir-faire – ainsi que les instruments, objets, artefacts et espaces culturels qui leur sont associés – que les communautés, les groupes et, le cas échéant, les individus reconnaissent comme faisant partie de leur patrimoine culturel[29]. La convention de l'UNESCO désigne cinq domaines : A. les traditions et expressions orales, y compris la langue comme vecteur du patrimoine culturel immatériel ; B. les arts du spectacle ; C. les pratiques sociales, rituels et événements festifs ; D. les connaissances et pratiques concernant la nature et l'univers ; E. les savoir-faire liés à l'artisanat traditionnel.
PBC	Protection des biens culturels
Preservation Planning	La planification de la conservation dans un système d'archivage électronique selon OAIS a pour objectif de garantir la disponibilité dans le temps des contenus archivés.
Probabilité d'occurrence	On appelle « probabilité d'occurrence » la probabilité estimée ou calculée sur la base de statistiques qu'un événement se produise au cours d'une période donnée (p. ex. dans les 10 ans).
Processus critiques	Dans le contexte de la protection des infrastructures critiques, on entend par « processus critique » tout processus indispensable au fonctionnement de l'infrastructure critique et dont la défaillance aurait des répercussions graves sur la population et ses moyens de subsistance.
Protection des infrastructures critiques	La protection des infrastructures critiques englobe des mesures qui réduisent la → probabilité d'occurrence et / ou → l'ampleur des dommages d'un dérangement, d'une défaillance ou d'une destruction des → infrastructures critiques, ou qui réduisent le plus possible la durée de non-disponibilité.
Records management	Le records management consiste à gérer systématiquement les documents et les informations tout au long de leur cycle de vie, depuis leur création ou leur recensement jusqu'à leur archivage final ou leur destruction, en passant par leur classement et leur conservation.
Résilience	La résilience décrit la capacité d'un système, d'une organisation ou d'une société à surmonter des dysfonctionnements d'origine interne ou externe et à maintenir autant que possible ou à retrouver toute sa fonctionnalité. La résilience se compose de quatre éléments : 1. la robustesse des systèmes (p. ex. → infrastructures critiques, État, économie et société) ; 2. les redondances disponibles ; 3. la capacité à mobiliser des mesures auxiliaires efficaces ; 4. la rapidité et l'efficience des mesures auxiliaires.
Risque	Le risque est une mesure de l'ampleur d'un → danger et englobe la → probabilité d'occurrence et → l'ampleur des dommages d'un événement indésirable.

29 Art. 2 de la Convention pour la sauvegarde du patrimoine culturel immatériel (RS 0.440.6), conclue à Paris le 17 octobre 2003

8 Glossaire et liste des abréviations

RS	Recueil systématique
Sauvegarde	Une sauvegarde est une copie de données créée pour permettre leur récupération en cas de perte ou de corruption. Ces copies sont effectuées régulièrement et stockées en lieu sûr.
Sécurité de l'information	La sécurité de l'information protège les informations et les systèmes d'information des accès, de l'utilisation, de la publication, de la modification ou de la destruction non autorisés. L'objectif est de garantir la confidentialité, l'intégrité et la disponibilité des données.
Sous-secteur	Les → infrastructures critiques suisses ont été réparties en 27 sous-secteurs couvrant l'ensemble des branches, industries, secteurs économiques et autres divisions économiques. En Suisse, les infrastructures critiques appartiennent aux sous-secteurs suivants : déchets, eaux usées, armée, soins médicaux, services financiers, services d'urgence, chimie et produits thérapeutiques, approvisionnement en gaz naturel, approvisionnement en pétrole, recherche et enseignement, services informatiques, biens culturels, prestations de laboratoire, approvisionnement en denrées alimentaires, transport aérien, chauffage à distance et chaleur industrielle, médias, Parlement, gouvernement, justice et administration, services postaux, transport ferroviaire, transport fluvial, transport routier, approvisionnement en électricité, télécommunications, services d'assurance, approvisionnement en eau et protection civile.
Synchronisation	La synchronisation est le processus permettant d'accéder aux mêmes données d'un système à l'autre. Cette opération s'effectue soit en temps réel, soit à intervalles réguliers, afin de garantir la cohérence et l'actualité des données.
TIC	Technologies de l'information et de la communication
TNI	Transformation numérique et gouvernance de l'informatique, Chancellerie fédérale

Glossaires détaillés et définitions :

- Glossaire des risques, Office fédéral de la protection de la population, OFPP, 29.4.2013. https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/5b9f4356-9979-430b-b8cc-f6841f3d05e6.pdf

- Glossaire du Guide pour la protection des infrastructures critiques, 2018. https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/b2cce99d-4ccc-4cea-9e16-2fc5fde3d9e9.pdf

8 Glossaire et liste des abréviations

Auteurs et experts de la première édition

Nom	Prénom	Organisation	Fonction
Wildi	Tobias	CFPBC Haute école spécialisée Grisons	Chef de projet / auteur principal
Fornaro	Peter	Digital Humanities Lab, Université de Bâle	Révision
Müller	Stefanie	Haute école spécialisée Grisons	Révision

Calendrier

Date	Descriptif
2018	Décision CFPBC d'élaborer une norme minimale TIC
Janvier – juillet 2023	Élaboration, 1er projet
Août – novembre 2023	Consultation des offices et des cantons
Décembre 2023	Élaboration, 2e projet
Janvier – mars 2024	Consultation des cantons
Avril – juli 2024	Élaboration et version définitive
Novembre 2024	Approbation CFPBC
Août – décembre 2024	Traduction et publication

Licence